servicenow

Gestion de la sécurité Zurich

Dernière mise à jour: 10/11/2025

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La présente documentation a été traduite pour vous simplifier sa lecture, à l'aide d'un logiciel de traduction. Tous les efforts possibles ont été déployés pour fournir une traduction précise, toutefois, la traduction automatique ne peut en aucun cas remplacer les traducteurs humains. La traduction est fournie « en l'état ». Aucune garantie, quelle qu'elle soit, express ou implicite, n'est fournie concernant la précision, la fiabilité ou l'exactitude des traductions, quelle que soit la langue cible. En raison des limites inhérentes au logiciel de traduction, certaines traductions du contenu peuvent ne pas être exactes. La langue officielle de la présente documentation est l'anglais Toute déviation ou différence générée par la traduction ne peut en aucun cas être considérée comme juridiquement contraignante, et ne pourra avoir d'effet juridique sur la conformité ou l'application des dispositions de la documentation.

Certains des exemples et graphiques présentés ici sont fournis à des titres d'illustration uniquement.ªucune association ou connexion réelle à des produits ou services ServiceNow n'est voulue et ne devrait être inférée.

ServiceNow, le logo ServiceNow, Now et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. Les autres sociétés et noms de produits peuvent être des marques commerciales des sociétés respectives avec lesquelles ils sont associés.

Veuillez lire les Conditions d'utilisation du site Web de ServiceNow à l'adresse www.servicenow.fr/terms-of-use.html

Traduction automatique

Siège social de la société
2225 Lawson Lane
Santa Clara, CA 95054
États-Unis
(408) 501-8550

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sommaire

Opérations de sécurité **5**

Explorer Opérations de sécurité 7

Now Assist pour Réponse aux incidents de sécurité 14

Explorer 15

Configurer 19

Utiliser Now Assist pour fermer les incidents de sécurité 27

Utiliser des workflows agentiques 43

Now Assist pour Réponse aux vulnérabilités 58

Explorer 59

Configurer 63

Utiliser les compétences de l'IA générative 66

Utiliser des workflows agentiques 75

Référence 80

Applications de gestion de la surface d'attaque 82

Réponse aux vulnérabilités 84

Réponse aux vulnérabilités des applications 907

Réponse aux vulnérabilités pour conteneurs 1124

Conformité de la configuration 1203

Réponse aux vulnérabilités Espaces de travail 1479

Nomenclature logicielle 1689

Applications de gestion des tickets de sécurité d'entreprise 1734

Réponse aux incidents de sécurité 1735

Renseignements sur les menaces 3287

Contrôle de la posture de sécurité 3543

Explorer 3545

Utiliser l'espace de travail 3561

Utiliser des contrôles d'atténuation 3584

Référence 3608

Tableau de bord de direction de cybersécurité 3624

S'abonner aux scores de point de référence 3642

Définir des cibles 3643

Intégration de la simulation et de la formation de sécurité pour Security Operations 3643

Tableau de bord de risque et conformité pour GRC : Mesures 3646

Centre de sécurité des renseignements sur les menaces 3656

Explorer 3658

Configurer 3663

Intégrer 3666

Administrer 3754

Référence 3802

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser....3810
Data Loss Prevention Incident Response....4008
Explorer....4010
Configurer....4013
Administrer....4014
Gérer les incidents....4070
Intégration entrante....4092
Intégrer....4095
Opérations de sécurité Fonctionnalité commune....4166
Créer et définir des groupes de filtres dans Security Operations....4169
Transformation des données partagées....4170
Opérations de sécurité Traitement des e-mails....4174
Opérations de sécurité Mappage de champs....4185
Opérations de sécurité Transformations de valeurs de champs....4189
Opérations de sécurité Mappage des données d'enrichissement....4190
Opérations de sécurité Escalade définie par l'utilisateur....4193
Créer des remplacements de propriétés séparées par domaine....4194
Créer un groupe de systèmes d'exploitation....4195
Configurer des groupes de balises et des balises de sécurité....4197
Annotations de sécurité....4201
Composants installés avec Security Support Common....4203
Rechercher Opérations de sécurité....4204
Référence de Security Operations Integrations....4205
Opérations de sécurité Déclencheurs de workflow....4305
Orchestration de Security Operations....4307
Opérations de sécurité et le ServiceNow Store....4308
Télécharger une application à partir de ServiceNow Store pour la première fois....4309
Installer une Opérations de sécurité intégration....4314
Mettre à jour une application précédemment téléchargée à partir de ServiceNow Store....4318
Mettre à niveau votre instance vers la version de famille suivante....4319

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opérations de sécurité

ServiceNow® Opérations de sécurité Les applications importent les données d'incident de vos outils de sécurité dans un moteur de réponse structuré qui utilise des workflows intelligents, l'automatisation, des visualisations de données et une connexion profonde avec le service informatique pour hiérarchiser et résoudre les menaces en fonction de l'impact qu'elles représentent pour votre organisation.

Choisissez l'une des vignettes suivantes pour commencer.

Applications Security Operations et leurs espaces de travail



Découvrez comment les Opérations de sécurité applications peuvent vous aider à améliorer votre posture de sécurité.

Now Assist pour Réponse aux incidents de sécurité



Découvrez comment Now Assist pour Réponse aux incidents de sécurité prend en charge ServiceNow® les compétences d'IA générative (GenAI) dans l'espace de travail Réponse aux incidents de sécurité et dans l'interface utilisateur principale (UI16).

Now Assist pour Réponses aux vulnérabilités



Découvrez comment Now Assist pour Réponse aux vulnérabilités prend en charge ServiceNow® les compétences d'IA générative (GenAI) dans l'espace de travail Réponse aux vulnérabilités et dans l'interface utilisateur principale (UI16).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Applications de gestion de la surface d'attaque



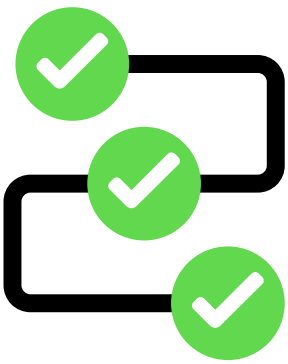
Découvrez les applications dans Vulnerability Response qui vous aident à identifier et à corriger les vulnérabilités sur votre surface de cyberattaque.

Applications de gestion des tickets de sécurité d'entreprise



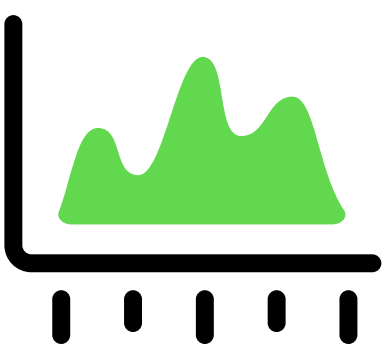
Découvrez les applications de Security Incident Response qui vous aident à analyser, isoler et résoudre les incidents de sécurité critiques au fur et à mesure de leur évolution.

Applications Contrôle de la posture de sécurité



Découvrez les applications qui vous aident à mieux comprendre votre posture de sécurité globale.

Tableau de bord de direction de cybersécurité



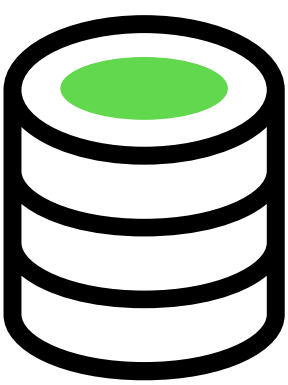
Découvrez comment le tableau de bord de direction de cybersécurité consolide les données des différents produits SecOps dans un tableau de bord unifié.

Centre de sécurité des renseignements sur les menaces



Découvrez comment la plateforme (TISC) fournit des solutions technologiques pour l'agrégation et la gestion des renseignements sur les Centre de sécurité des renseignements sur les menaces menaces.

Data Loss Prevention Incident Response

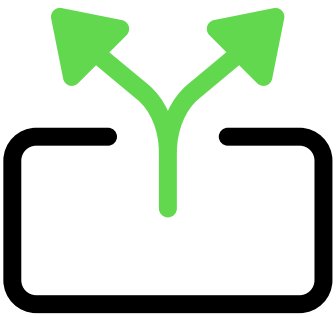


Découvrez comment gérer les informations sensibles de vos clients et identifier et protéger vos canaux de perte de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications partagées Security Operations



Découvrez les fonctionnalités et les modules qui fournissent des fonctionnalités communes dans .Opérations de sécurité

Scénarios et exemples d'opérations de sécurité



En savoir plus sur la façon d'obtenir Opérations de sécurité des applications à partir de et ServiceNow® Store des scénarios pour les applications que vous pouvez utiliser lors de l'utilisation des produits.

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Explorer Opérations de sécurité

Protégez vos actifs et votre environnement d'entreprise avec les applications ServiceNow Opérations de sécurité et la puissance du ServiceNow AI Platform®. Connectez vos équipes de sécurité et informatiques pour vous aider à hiérarchiser et à résoudre les menaces en fonction de l'impact qu'elles représentent pour votre organisation.

Vue d'ensemble de Opérations de sécurité

La Opérations de sécurité suite d'applications vous aide à protéger vos actifs en améliorant votre posture de sécurité globale. Par exemple, en intégrant des applications telles que Réponse aux incidents de sécurité, Réponse aux vulnérabilités et Contrôle de la posture de sécurité à vos outils de sécurité existants, vos analystes, gestionnaires et équipes informatiques de Security Operation Center (SOC) peuvent :

- Répondre à l'évolution rapide des menaces de cybersécurité et de sécurité
- Identifier, classer par ordre de priorité et corriger les vulnérabilités
- Afficher l'inventaire complet de vos actifs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

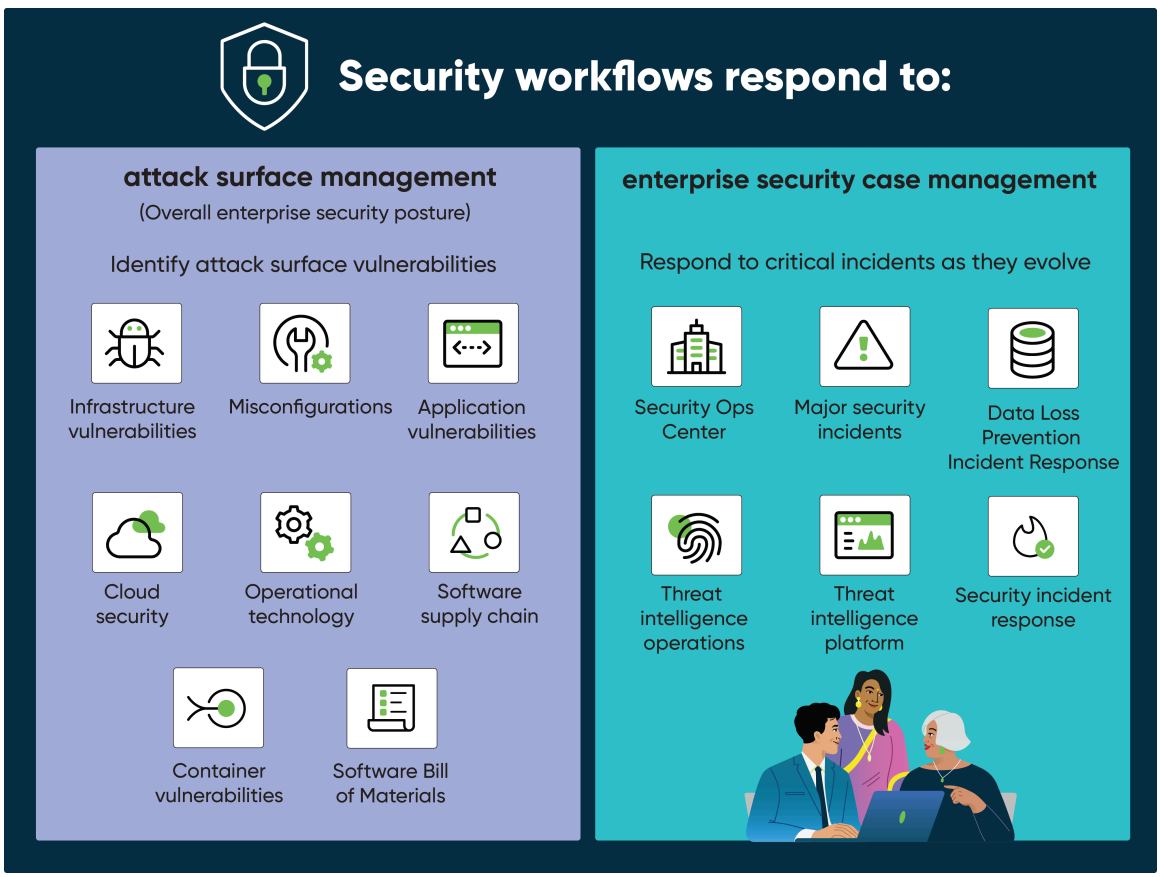
- Déterminer la couverture globale de votre outil de sécurité
- Résolvez les incidents de sécurité plus rapidement grâce à des workflows intelligents et ServiceNow à des compétences d'IA générative (GenAI). Consultez Now Assist pour Réponse aux incidents de sécurité pour plus d'informations.

Opérations de sécurité Applications pour les workflows

Les Opérations de sécurité applications se répartissent en deux grandes catégories de Opérations de sécurité flux de travail :

- Gestion de la surface d'attaque : applications et outils qui vous aident à anticiper, comprendre et fermer vos vulnérabilités.
- Gestion des tickets de sécurité d'entreprise : applications et outils qui vous aident à réagir rapidement pour répondre aux incidents critiques.

Workflows de sécurité



Les deux catégories d'applications Security Operations et les cas d'utilisation qu'elles vous aident à résoudre dans votre environnement d'entreprise.

Avantages des Opérations de sécurité applications

Affichez les Opérations de sécurité applications et les données avec des interfaces utilisateur de nouvelle génération (espaces de travail). Grâce aux espaces de travail, les analystes de sécurité, les responsables SOC (Security Operation Center) et les spécialistes de la remédiation de votre organisation peuvent surveiller et gérer les types de workflows suivants à partir d'un seul emplacement :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cycle de vie des incidents de sécurité, de l'analyse initiale au confinement, en passant par l'éradication et la récupération.
- Les vulnérabilités qui les intéressent le plus afin de pouvoir décider stratégiquement des vulnérabilités qu'ils envoient aux équipes informatiques pour correction.
- Aperçus clés et cas d'utilisation clés pour la couverture des outils de sécurité et l'hygiène des actifs qui signalent et surveillent les informations importées sur vos actifs.

Applications de gestion de la surface d'attaque

Applications qui vous aident à anticiper les menaces et à identifier les vulnérabilités

Application	Description	Utilisateurs
Contrôle de la posture de sécurité	Obtenez un aperçu de la façon dont les outils de sécurité sont déployés et couvrent vos actifs en fonction d'un inventaire des actifs et des données importées. Les connecteurs du graphe de services et les produits ServiceNow tels que Hardware Asset Management (HAM) et ITOM Discovery sont pris en charge pour les importations de données. Les audits basés sur des politiques vous aident à hiérarchiser le rattrapage des combinaisons à haut risque telles que l'exposition à Internet et les vulnérabilités connues. Créez des politiques et des aperçus personnalisés pour surveiller la conformité des actifs avec les normes de configuration de votre outil de sécurité interne.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Ingénieur des opérations informatiques • Propriétaire de service (profil du propriétaire de rattrapage)
Réponse aux vulnérabilités	Les scanners de vulnérabilité tiers et les outils d'évaluation vous aident à identifier les risques que les vulnérabilités posent aux types d'actifs suivants :	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications qui vous aident à anticiper les menaces et à identifier les vulnérabilités (suite)

Application	Description	Utilisateurs
	• Infrastructure (hôte) • Conteneur • Applications • Nomenclatures logicielles Les vulnérabilités identifiées par ces outils se traduisent par des risques pour les équipes de sécurité et informatiques responsables de la maintenance et de la sécurisation des actifs d'une organisation.	• Ingénieur des opérations informatiques • Propriétaire de service (profil du propriétaire de rattrapage)
Conformité de la configuration	Vérifiez votre conformité aux politiques de sécurité ou d'entreprise. Identifiez, classez par ordre de priorité et corrigez les éléments de configuration non conformes avec les résultats des tests obtenus à partir d'intégrations SCA (Secure Configuration Assessment) tierces.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Ingénieur des opérations informatiques • Propriétaire de service (profil du propriétaire de rattrapage)

Applications de gestion des tickets de sécurité d'entreprise

Applications qui vous aident à répondre aux violations et incidents de sécurité critiques

Application	Description	Utilisateurs
Réponse aux incidents de sécurité	Simplifiez le processus d'identification des incidents critiques en appliquant de puissants outils de workflow et d'automatisation qui accélèrent la correction. Intégrez vos outils SIEM (Security Information and Event Manager) existants aux Réponse aux incidents de sécurité applications Security Operations pour importer des données sur	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Analyste Threat Intelligence

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications qui vous aident à répondre aux violations et incidents de sécurité critiques (suite)

Application	Description	Utilisateurs
	les menaces provenant de diverses sources et créer automatiquement des incidents de sécurité prioritaires.	
Gestion des incidents de sécurité majeurs	Les principales options de gestion des incidents de sécurité fonctionnent avec les fonctionnalités existantes du produit Security Incident Response. Cela inclut la possibilité pour un analyste de sécurité d'escalader un incident de sécurité standard en un incident de sécurité majeur, afin que les nouvelles fonctionnalités du produit soient disponibles pour prendre en charge le processus de correction. Suivez la progression d'un incident de sécurité majeur (MSI), de la découverte à l'analyse. Proposer des solutions, promouvoir et lier les incidents de sécurité et la fermeture.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Ingénieur des opérations informatiques • Propriétaire de service (profil du propriétaire de rattrapage) • Conseil général
Data Loss Prevention Incident Response	Data Loss Prevention Incident Response (DLP IR) vous permet d'examiner et de gérer le workflow de rattrapage des incidents DLP à partir de plusieurs sources, telles que le point de terminaison, le réseau, la messagerie électronique et le cloud. Avec l'application DLP, vous pouvez identifier, répondre et protéger vos canaux de perte de données.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité
Renseignements sur les menaces	Permet aux équipes de réponse aux incidents d'automatiser les recherches de menaces, les recherches et la corrélation.	• CISO • Analyste de la sécurité de l'information

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications qui vous aident à répondre aux violations et incidents de sécurité critiques (suite)

Application	Description	Utilisateurs
	L'intégration avec MITRE ATT&CK vous permet de mesurer et de comprendre la couverture de détection et d'atténuation et facilite la chasse aux menaces.	• Responsable des opérations de sécurité • Analyste Threat Intelligence
Centre de sécurité des renseignements sur les menaces (TISC)	Regroupez, conservez et gérez les renseignements sur les menaces provenant de sources multiples et effectuez la gestion des tickets de renseignements sur les menaces. Suivez les campagnes, rendez opérationnels les renseignements sur les menaces et répondez aux renseignements exploitables.	• CISO • Analyste de la sécurité de l'information • Responsable des opérations de sécurité • Analyste Threat Intelligence

Ce qu'il faut explorer ensuite

Sélectionnez une tuile pour commencer avec les espaces de Opérations de sécurité travail.

Espace de travail Réponse aux incidents de sécurité



En savoir plus sur l'espace de travail Réponse aux incidents de sécurité

Espace de travail du gestionnaire de vulnérabilité



En savoir plus sur l'espace de travail du gestionnaire de vulnérabilité

Espace de travail Contrôle de la posture de sécurité



En savoir plus sur l'espace de travail Contrôle de la posture de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Espace de travail de l'évaluation de la vulnérabilité



En savoir plus sur l’espace de travail Évaluation de la vulnérabilité

Espace de travail de remédiation informatique



En savoir plus sur l’espace de travail de remédiation informatique

Espace de travail de nomenclature logicielle



En savoir plus sur l’espace de travail Nomenclature logicielle

Espace de travail du Centre de sécurité des renseignements sur les menaces (TISC)



En savoir plus sur l’espace de travail TISC

Espace de travail de la prévention de la perte de données (DLP) pour la réponse aux incidents



En savoir plus sur l’espace de travail DLP

Espace de travail Major Security Incident Management (MSIM)



En savoir plus sur l’espace de travail MSIM

Traduction automatique

Dépannage et demande d'aide

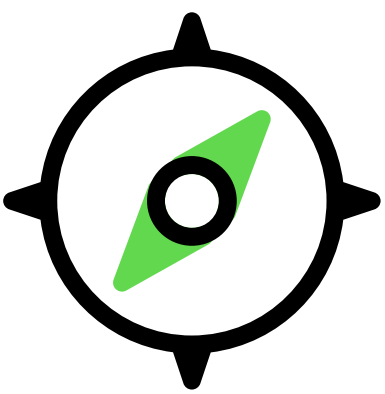
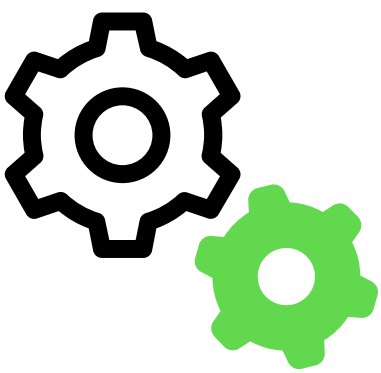
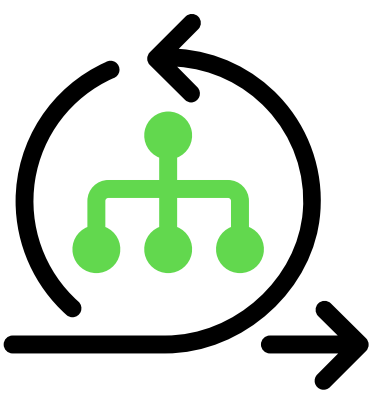
- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Now Assist pour Réponse aux incidents de sécurité

Les analystes de sécurité peuvent utiliser des workflows intelligents et ServiceNow des compétences d'IA générative pour les aider à résoudre les incidents de sécurité. Les responsables de la sécurité peuvent examiner rapidement le contexte des incidents de sécurité et des notes de fermeture dans un format concis et facile à lire, afficher les données d'analyse post-incident et consulter les étapes de rattrapage recommandées avec l'application Now Assist pour Réponse aux incidents de sécurité .

Premiers pas

Explorer	Configurer	Utiliser
		
En savoir plus Now Assist pour Réponse aux incidents de sécurité	Apprenez à configurer et à activer les compétences pour Now Assist pour Réponse aux incidents de sécurité	Découvrez comment résumer les détails et générer des notes de fermeture pour les incidents de sécurité avec l'IA générative et Now Assist pour Réponse aux incidents de sécurité

Important :

- Tous les fournisseurs de modèles ne sont pas disponibles pour les clients ayant des SKU dans le pays, et certains produits/fonctionnalités Now Assist ne sont actuellement pas disponibles pour les clients dans le pays. Pour plus d'informations, consultez l'article KB1584492 dans la base de connaissances Now Support. Assurez-vous de vérifier les mises à jour de disponibilité des fournisseurs de modèles dans les versions futures.
- Certains Now Assist produits/fonctionnalités ne sont actuellement pas disponibles pour les clients dans les centres de données FedRAMP, NSC DOD IL5 ou protégés par l'IRAP en Australie, les clients auto-hébergés ou dans d'autres environnements restreints. Pour en savoir plus, consultez l'article KB0743854 dans la Now Support Base de connaissances. Assurez-vous de consulter les mises à jour de disponibilité dans les versions futures.
- Certains Now Assist produits/fonctionnalités ne sont actuellement disponibles que pour les clients dans certaines régions. Assurez-vous de consulter les mises à jour de disponibilité dans les versions futures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Limitations de l'IA

Cette application utilise l'intelligence artificielle (IA) et l'apprentissage machine, des domaines d'étude à l'évolution rapide qui génèrent des prédictions basées sur des modèles de données. Par conséquent, cette application peut ne pas toujours produire des informations exactes, complètes ni appropriées. De plus, il n'y a aucune garantie que cette application ait été entièrement formée ou testée pour votre cas d'utilisation. Pour atténuer ces problèmes, il est de votre responsabilité de tester et d'évaluer l'exactitude, le préjudice et la pertinence de votre utilisation de cette application pour votre cas d'utilisation, d'utiliser une supervision humaine des résultats et de vous abstenir de vous fier uniquement aux résultats générés par l'IA à des fins de prise de décision. Cela est particulièrement important si vous déployez cette application dans des domaines ayant des impacts importants tels que la santé, la finance, le droit, l'emploi, la sécurité ou l'infrastructure. Vous acceptez de respecter la politique d'utilisation acceptable de l'IA de ServiceNow , qui peut être mise à jour par ServiceNow.

Traitement des données

Cette application nécessite que les données soient transférées des instances individuelles des clients ServiceNow vers un environnement ServiceNow centralisé, qui peut être situé dans une région du centre de données différente de celle où se trouve votre instance, et potentiellement vers un fournisseur de cloud tiers, comme Microsoft Azure. Ces données sont traitées conformément aux politiques et procédures internes de ServiceNow, y compris nos politiques disponibles via notre portail de conformité CORE .

Collecte de données

ServiceNow collecte et utilise les entrées, les sorties et les modifications des sorties de cette application pour développer et améliorer les technologies ServiceNow, y compris les modèles ServiceNow et les produits d'IA. En outre, cette application collecte Données provenant d'incidents de sécurité, d'incidents, de demandes de changement, de problèmes et d'éléments vulnérables. Les clients peuvent se désabonner de la collecte de données future à tout moment, comme décrit dans la page Now Assist Se désabonner .

Pour plus d'informations, consultez la documentation Now Assist .

Explorer Now Assist pour Réponse aux incidents de sécurité

Vos analystes de sécurité peuvent utiliser des workflows intelligents et ServiceNow des compétences d'IA générative pour les aider à trier, enquêter et fermer les incidents de sécurité dans le flux de travail avec l'application Now Assist pour Réponse aux incidents de sécurité .

Vue d'ensemble de Now Assist pour Réponse aux incidents de sécurité

Grâce aux compétences d'IA générative et aux workflows agentiques, vos analystes de sécurité ont la possibilité de :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Résumez les détails de l'incident de sécurité et passez rapidement en revue le contexte dans un format concis et facile à lire.
- Générer les prochaines étapes recommandées pour un incident de sécurité.
- Générer des données d'analyse post-incident.
- Générez des notes de fermeture.
- Générer des aperçus de corrélation

Les analystes de sécurité peuvent partager les résultats, les détails des incidents et les notes de fermeture avec d'autres analystes, responsables et personnes concernées clés.

Now Assist pour Réponse aux incidents de sécurité utilisateurs

Utilisateurs

Utilisateur	Description
Analystes et gestionnaires de la sécurité	Prévisualisez les détails des incidents de sécurité, voyez leur impact potentiel et affichez les principales actions de rattrapage déjà prises avec les résumés d'incidents de sécurité à l'aide de l'IA générative. Les résumés et les prochaines étapes recommandées (actions) donnent aux analystes et aux responsables une longueur d'avance dans leurs enquêtes et les aident à résoudre les incidents de sécurité. Générez automatiquement un brouillon de notes de fermeture à l'aide de l'IA générative. Les notes de fermeture des incidents de sécurité sont créées rapidement en fonction des activités de rattrapage et d'imbrication, en plus d'autres détails pertinents liés à leur fermeture.

Now Assist pour Réponse aux incidents de sécurité avantages

Fonctionnalités de Now Assist pour Réponse aux incidents de sécurité

Avantage	Fonctionnalité	Utilisateurs
Accélérez le triage des incidents de sécurité avec de longs flux d'activité en examinant rapidement les notes de travail et les informations contextuelles dans un format concis et facile à lire.	Générez des résumés pour les incidents de sécurité qui incluent les informations suivantes : • Problème • Détails • Observations • Principales mesures prises • Détails de fermeture	• Analystes de la sécurité • Gestionnaires de la sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalités de Now Assist pour Réponse aux incidents de sécurité (suite)

Avantage	Fonctionnalité	Utilisateurs
Générez automatiquement un brouillon de notes de fermeture pour un incident de sécurité lorsqu'il est prêt à être fermé. Les analystes peuvent modifier tout contenu généré par la compétence d'IA en le modifiant, en le supprimant ou en ajoutant leurs propres notes avant de fermer l'incident de sécurité.	Générer des notes de fermeture d'incident de sécurité	• Analystes de la sécurité • Gestionnaires de la sécurité
Générez les prochaines étapes recommandées dans le workflow sur demande pour vous aider à fermer un incident de sécurité.	Générer les actions recommandées en cas d'incident de sécurité	• Analystes de la sécurité • Gestionnaires de la sécurité
Générez une analyse post-incident qui comprend une analyse de la cause première, une évaluation de l'impact et les leçons apprises dans le cadre du workflow de clôture d'un incident de sécurité.	Générer une analyse post-incident	• Analystes de la sécurité • Gestionnaires de la sécurité
Connectez les incidents actuels aux événements passés qui impliquent les mêmes utilisateurs, éléments de configuration (CI) ou observables affectés.	Générer des aperçus de corrélation	• Analystes de la sécurité • Gestionnaires de la sécurité
Découvrez rapidement les détails d'un incident de sécurité en accédant aux résumés et aux notes de fermeture à partir du Now Assist panneau.	Accédez au résumé et aux notes de clôture de l'IA générative depuis le Now Assist panel. Saisissez des demandes d'informations plus basiques sur les incidents de sécurité dans le panneau.	• Analystes de la sécurité • Gestionnaires de la sécurité
Personnalisez les compétences de l'IA générative pour les résumés et les notes de clôture en fonction de vos besoins.	Copier une compétence et la modifier Sélectionnez les champs de la table connexe, définissez la disponibilité de la compétence et choisissez l'emplacement où afficher la compétence.	administrateur

Traduction automatique

Ce qu'il faut explorer ensuite

Pour en savoir plus sur la configuration et l'utilisation de Now Assist pour Réponse aux incidents de sécurité, consultez :

- Configurer Now Assist pour Réponse aux incidents de sécurité
- Résumer un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Générer des notes de fermeture pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité
- Générer des aperçus de corrélation dans le Now Assist panneau avec Now Assist pour Réponse aux incidents de sécurité
- Générer des actions recommandées pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité
- Générer une analyse post-incident pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité
- Entrées et déclencheurs pour Now Assist pour Réponse aux incidents de sécurité

Informations de prise en charge pour Now Assist pour Réponse aux incidents de sécurité

Obtenez une vue d'ensemble des informations importantes liées à l'application Now Assist pour Réponse aux incidents de sécurité.

Versions prises en charge

La version 2.0.1 de Now Assist pour Réponse aux incidents de sécurité prend en charge :

- legacy Interface utilisateur (UI16) : Réponse aux incidents de sécurité application principale, v13.6.4
- Espace de travail de la Réponse aux incidents de sécurité (Espace de travail SIR), v1.7.0
- Now Assist pour ServiceNow AI Platform® la version 6.0.1

Interfaces utilisateur prises en charge

Cela Now Assist pour Réponse aux incidents de sécurité inclut les compétences d'IA générative répertoriées dans le tableau suivant.

Now Assist pour Réponse aux incidents de sécurité Interfaces et compétences prises en charge

Interface	Fonctionnalités
Réponse aux incidents de sécurité	• Synthèse des incidents de sécurité. • Génération des prochaines étapes recommandées pour un incident de sécurité. • Génération d'une analyse post-incident qui comprend l'analyse de la cause première, l'évaluation de l'impact et les leçons apprises. • Now Assist panneau. • Génération de notes de fermeture. • Aperçus de corrélation à partir du Now Assist panneau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Now Assist pour Réponse aux incidents de sécurité Interfaces et compétences prises en charge (suite)

Interface	Fonctionnalités
Legacy UI16	• Synthèse des incidents de sécurité • Génération des prochaines étapes recommandées pour un incident de sécurité. • Génération d'une analyse post-incident qui comprend l'analyse de la cause première, l'évaluation de l'impact et les leçons apprises. • Now Assist panneau. • Génération de notes de fermeture. • Aperçus de corrélation à partir du Now Assist panneau.

Configurer Now Assist pour Réponse aux incidents de sécurité

L'application Now Assist pour Réponse aux incidents de sécurité est prise en charge dans et Espace de travail de la Réponse aux incidents de sécurité dans l'interface legacy utilisateur principale (UI16). Vous pouvez utiliser la configuration guidée dans la Administrateur Now Assist console pour configurer Now Assist pour Réponse aux incidents de sécurité.

Vue d'ensemble de la configuration

En partageant des données avec le programme de développement de l'IA, vous fournissez des données pertinentes pour aider à améliorer la ServiceNow® précision des prédictions, l'expérience utilisateur, adapter les produits à vos besoins professionnels et réduire les hallucinations pour vos compétences activées Now Assist .

Vous pouvez choisir de refuser le partage de données d'une ServiceNow instance à partir de la Administrateur Now Assist console si vous ne souhaitez pas participer. Consultez Refuser le partage de données pour Now Assist . Répétez le processus d'annulation de l'adhésion pour toutes les instances qui utilisent cette Now Assist fonctionnalité.

Utilisez la console Administrateur Now Assist pour configurer Now Assist pour Réponse aux incidents de sécurité. Cette console contient tout ce dont vous avez besoin pour installer les applications et configurer les compétences de l'IA générative. Pour en savoir plus, consultez Configuration des Now Assist paramètres et des fonctionnalités .

Le tableau suivant répertorie les fonctionnalités et les compétences auxquelles vous pouvez accéder à partir de la console Administrateur Now Assist.

Now Assist pour Réponse aux incidents de sécurité Fonctionnalités et compétences dans la Administrateur Now Assist console

Produit de technologie Now Assist	Compétences en matière d'incidents de sécurité
Now Assist pour Réponse aux incidents de sécurité	Synthèse des incidents de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Now Assist pour Réponse aux incidents de sécurité Fonctionnalités et compétences dans la Administrateur Now Assist console (suite)

Produit de technologie Now Assist	Compétences en matière d'incidents de sécurité
	Remarque : La synthèse des incidents prend en charge les incidents de sécurité dans tout état autre que **Brouillon**.
	Génération de notes de résolution.
	Actions recommandées en cas d'incident de sécurité La compétence d'actions recommandées en cas d'incident de sécurité prend en charge les incidents de sécurité dans tout état autre que **Fermé** et **Annulé**. **Remarque :** L'application Recherche IA doit être activée pour que la compétence Actions recommandées fonctionne pour les incidents de sécurité. Pour vérifier que Recherche IA est activé sur votre instance, accédez à **Tous** > **Recherche IA** > **État de Recherche IA**. Contactez l'assistance si la page indique que Recherche IA n'est pas activée. Les aperçus de corrélation prennent en charge les incidents de sécurité dans tous les états.
	Génération d'une analyse post-incident

1. Installer Now Assist modules d'extension .

   Installez les Now Assist pour Réponse aux incidents de sécurité applications (sn_sec_gen_ai) et Réponse aux incidents de sécurité Core [sn_si].

2. Configurer et activer une compétence pour Now Assist pour Réponse aux incidents de sécurité

   Configurez et examinez les détails d'une compétence. Vous activez une compétence à partir du Configuration guidée.

Utilisation pour Configuration guidée implémenter Now Assist pour Réponse aux incidents de sécurité

Configuration guidée fournit une séquence de tâches qui vous aident à configurer Now Assist pour Réponse aux incidents de sécurité sur votre ServiceNow instance. Pour ouvrir le Configuration guidée pour Now Assist pour Réponse aux incidents de sécurité, accédez à **Tous** > **Administrateur Now Assist** > **Fonctionnalités**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations, consultez Configurer et activer une compétence pour Now Assist pour Réponse aux incidents de sécurité.

Configurer et activer une compétence pour Now Assist pour Réponse aux incidents de sécurité

Configurez et examinez les détails d'une compétence dans le Configuration guidée. Vous pouvez activer une compétence à partir du Configuration guidée.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Administrateur Now Assist** > **Fonctionnalités**.
2. Une fois **Technologie** sélectionnée dans le panneau de navigation, sélectionnez **Opérations de sécurité** dans la liste.
   Les compétences d'incident de sécurité suivantes sont affichées sur la carte d'incident de sécurité :
   - Actions recommandées en cas d'incident de sécurité

     L'application Recherche IA doit être activée pour que la compétence Actions recommandées fonctionne pour les incidents de sécurité. Pour vérifier que Recherche IA est activé sur votre instance, accédez à **Tous** > **Recherche IA** > **État de Recherche IA**. Contactez l'assistance si la page indique que Recherche IA n'est pas activée.
   - Analyse post-incident
   - Génération d'aperçus de corrélation
   - Synthèse des incidents de sécurité
   - Génération de notes de résolution
3. Sélectionnez **Afficher les détails**.
   Vous ne pouvez pas modifier les compétences incluses dans l'application. Pour modifier les paramètres par défaut, vous devez en faire une copie. Pour plus d'informations sur la personnalisation d'une compétence, reportez-vous à la section Personnaliser une compétence Now Assist pour Réponse aux incidents de sécurité.
4. Sélectionnez **Activer la compétence** pour la compétence souhaitée.
5. Suivez les étapes pour configurer et activer une compétence à l'aide du Configuration guidée.

   Remarque : Certaines compétences ne nécessitent pas toutes les étapes de configuration énumérées ci-dessous. Sélectionnez les seules tâches affichées sur le panneau de gauche et suivez les invites. Une fois que vous avez terminé les tâches, activez la compétence.

   a. Dans le panneau de navigation, sélectionnez **Choisir une entrée** pour configurer les entrées ou les déclencheurs de la compétence sélectionnée.

      Certains ou tous les modèles d'entrée suivants pour la compétence sont répertoriés : **Travail en cours**, **Révision** et **Fermé**. Le modèle **Travail en cours** est sélectionné.

      Vous préférez peut-être conserver ces modèles d'entrée dans leurs paramètres par défaut jusqu'à ce que vous vous familiarisiez avec la façon dont les compétences de travail sont utilisées Now Assist pour Opérations de sécurité .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Toutefois, pour certaines compétences , vous pouvez modifier certains champs de table connexes, tester l'invite sur un incident de sécurité, définir la disponibilité de la compétence et choisir l'emplacement où afficher la compétence.

Si vous choisissez de modifier les champs, sélectionnez uniquement les options prises en charge dans les listes fournies dans le cadre de vos données d'entrée.

Si vous modifiez les entrées ou les déclencheurs d'une compétence, vous déterminez comment et quand une compétence est utilisée. Vous ne pouvez pas modifier la source de données d'entrée d'une compétence. La source de données contient les tables et les champs sur lesquels la compétence s'appuie. Toutefois, vous pouvez copier une compétence et la personnaliser. Pour plus d'informations, consultez Personnaliser une compétence Now Assist pour Réponse aux incidents de sécurité.

6. Sélectionnez **Enregistrer et passez** à l'étape suivante dans le Configuration guidée.
7. **Facultatif :** Testez l'invite sur un enregistrement d'incident de sécurité.
8. Sélectionnez **Enregistrer et passez** à l'étape suivante dans le Configuration guidée.
9. **Facultatif :** Choisissez l'une des options suivantes pour définir la disponibilité.

Option	Description
La compétence est toujours disponible	La compétence est toujours disponible pour les utilisateurs.
Personnaliser la disponibilité des compétences	La compétence n'est disponible que lorsque certaines conditions sont remplies (par défaut). (Optional) Utilisez le générateur de conditions pour définir vos conditions.

10. Sélectionnez **Enregistrer et passez** à l'étape suivante dans le Configuration guidée.
11. Choisissez **Sélectionner l'affichage** pour déterminer où vous souhaitez afficher la compétence.

Option	Description
Intégré au produit	Now Assist Les compétences sont affichées sur les formulaires et dans les espaces de travail.
Rôles d'utilisateur	Sélectionnez l'icône Développer ( )
Panneau Now Assist	Now Assist compétences sont disponibles dans le Now Assist panneau. **Remarque :** Si vous ne voyez pas cette option, vous devez activer le panneau Now Assist. Pour plus d'informations, consultez Activer le Now Assist panneau . Les actions recommandées en cas d'incident de sécurité et les compétences d'analyse post-incident ne sont pas disponibles dans le Now Assist panneau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

12. Sélectionnez **Enregistrer et continuer** pour passer à l'étape suivante.
13. **Facultatif :** Ajoutez ou supprimez des rôles.

    (Optional) Par défaut, les rôles sn_si.analyst et sn_si.manager sont ajoutés et peuvent voir les résultats de la génération automatisée de compétences. Vous pouvez ajouter ou supprimer des rôles uniquement si vous Personnaliser une compétence Now Assist pour Réponse aux incidents de sécurité.
14. Passez en revue vos choix et sélectionnez **Activer** pour terminer la configuration de la compétence.
15. Sélectionnez **Retourner à l'incident de sécurité**.
    La compétence est affichée dans la section Compétences actives.

Personnaliser une compétence Now Assist pour Réponse aux incidents de sécurité

Personnalisez certains champs d'entrée d'une compétence d'IA générative en fonction des exigences de votre environnement.

Avant de commencer

Rôles requis : admin

Procédure

1. Accédez au **Tous** > **Administrateur Now Assist** > **Fonctionnalités** de la Administrateur Now Assist console.
2. Une fois **Technologie** sélectionnée dans le panneau de navigation, sélectionnez **Opérations de sécurité** dans la liste.
   Ces compétences d'incident de sécurité sont affichées :
   - Actions recommandées en cas d'incident de sécurité
   - Analyse post-incident
   - Génération d'aperçus de corrélation
   - Synthèse des incidents de sécurité
   - Génération de notes de résolution
3. Créez une copie d'une compétence et personnalisez les champs d'entrée.

   a. Sur la carte de fonctionnalité Incident de sécurité, sélectionnez **Afficher les détails**.

   b. Dans la section Compétences actives, recherchez la compétence que vous souhaitez copier et sélectionnez l'icône Actions supplémentaires (icône

   c. Sélectionnez **Créer une copie**.

   d. Confirmez votre choix dans le modal.
   La configuration guidée s'affiche.

   e. Dans **Détails généraux**, saisissez un nom et une description uniques pour la compétence.

   f. Passez à l'étape suivante en sélectionnant **Enregistrer et continuer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

g. Sélectionnez **Choisir une entrée**.

Si **Choisir une entrée** est sélectionné, ces modèles d'entrée pour la compétence sont répertoriés : Travail en cours, Révision et Fermé. Le modèle Travail en cours est sélectionné.

Vous pouvez configurer certains champs de table d'entrée de base, les conditions et les listes connexes pour les modèles. Sélectionnez uniquement parmi les tables connexes prises en charge dans les listes pour vos données d'entrée.

Vous ne pouvez pas modifier la table d'entrée de base [sn_si_incident] ou ajouter une nouvelle source de données pour votre copie de la compétence de synthèse des incidents de sécurité.

h. Continuez à modifier les champs modifiables dans le modèle Travail en cours avec le générateur de conditions et les conditions de filtrage.

i. Passez à l'étape suivante dans le Configuration guidée modèle Travail en cours en sélectionnant **Enregistrer et continuer**.

- **Personnaliser l'invite** : modifiez l'invite en réorganisant ou en supprimant les sections prédéfinies. Vous pouvez examiner et tester l'invite sur un enregistrement d'incident de sécurité pour chaque configuration de modèle d'entrée.
- **Définir la disponibilité** :

Option	Description
La compétence est toujours disponible	La compétence est toujours disponible pour les utilisateurs.
Personnaliser la disponibilité des compétences	La compétence n'est disponible que lorsque les conditions sont remplies (par défaut). Utilisez le générateur de conditions pour définir vos conditions.

- **Sélectionner l'affichage** :

Option	Description
Intégré au produit	Affichez la synthèse des incidents de sécurité dans tous les produits de sécurité. Now Assist Les compétences sont affichées sur les formulaires et dans les espaces de travail.
Rôles d'utilisateur	Sélectionnez l'icône Développer ( )

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Panneau Now Assist	Now Assist compétences sont disponibles dans le Now Assist panneau. **Remarque :** Si vous ne voyez pas cette option, vous devez activer le panneau Now Assist. Pour plus d'informations, consultez Activer le Now Assist panneau .

j. Sélectionnez **Enregistrer le modèle** pour enregistrer vos modifications apportées au modèle Travail en cours.

k. Sélectionnez le modèle de révision.

l. Continuez à modifier les champs modifiables dans les modèles Révision et Fermé avec les conditions de filtrage décrites aux étapes précédentes.

m. Sélectionnez **Enregistrer et passez** à l'étape suivante dans le Configuration guidée.

n. Sélectionnez **Enregistrer le modèle** pour enregistrer vos modifications dans un modèle.

o. Sélectionnez **Examiner et activer** pour examiner votre compétence et apporter des modifications supplémentaires.

4. Sélectionnez **Activer**.
   Votre compétence est affichée sur la page Incident de sécurité dans la section Toutes les compétences d'incident de sécurité disponibles.
5. Sélectionnez **Activer la compétence**.

Entrées et déclencheurs pour Now Assist pour Réponse aux incidents de sécurité

Vous pouvez configurer certaines entrées ou certains des déclencheurs d'une compétence d'IA générative. Les entrées ou les déclencheurs vous permettent de déterminer comment et quand une compétence est utilisée.

Entrées et déclencheurs

Les entrées identifient les données utilisées pour une compétence. Les entrées comprennent la table et les champs utilisés pour générer un résumé d'incident de sécurité. Un déclencheur initie une action. Par exemple, les déclencheurs déterminent quand le système génère un résumé.

Vous pouvez modifier les entrées et les déclencheurs, mais vous ne pouvez pas modifier la source de données d'une compétence. La source de données contient les tables et les champs sur lesquels la compétence s'appuie.

Compétence de synthèse des incidents de sécurité

Les entrées de la compétence de synthèse des incidents de sécurité identifient la table et les champs utilisés lorsqu'un résumé d'incident de sécurité est généré. Le tableau suivant

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

répertorie les entrées pour la compétence de synthèse des incidents de sécurité à partir de la page Choisir une entrée dans la Administrateur Now Assist console.

Entrée	Description
Source de données	Table Incident de sécurité [sn_si_incident].
Champs d'entrée	• Brève description • Description • État • Priorité • Notes de travail • Commentaires supplémentaires
Tables d’entrée connexes	• CI affectés : élément de configuration • Utilisateurs affectés : utilisateurs • Réponse aux incidents de sécurité Tâche : description brève • État : tout état autre que **Annulé**. • Observables associés : le résultat de l’observable est malveillant ou suspect.

Compétence de génération de notes de résolution

Les entrées de la compétence de génération de notes de résolution identifient la table et les champs utilisés lorsque les notes de résolution sont générées pour un incident de sécurité. Le tableau suivant répertorie les entrées pour la compétence de génération de notes de résolution à partir de la page Choisir une entrée dans la Administrateur Now Assist console.

Entrée	Description
Source de données	Table Incident de sécurité [sn_si_incident].
Champs d'entrée	• Brève description • Description • Notes de travail • Commentaires supplémentaires

Incident de sécurité : compétence de génération d’actions recommandées

Entrée	Description
Source de données	Table Incident de sécurité [sn_si_incident].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Compétence de génération d'analyse post-incident

Entrée	Description
Source de données	Table Incident de sécurité [sn_si_incident].

Compétence de génération d'aperçus de corrélation

Vos aperçus de corrélation pour un incident de sécurité peuvent contenir des enregistrements des tables suivantes, mais vous devez avoir l'autorisation d'accéder à ces tables et enregistrements.

Entrée	Description
Source de données	Table Incident de sécurité [sn_si_incident]. Table des éléments de configuration [cmdb_ci]. Table Incident [incident]. Table de demande de changement [change_request]. Table Problème [problem]. Table des éléments vulnérables [sn_vul_vulnerable_item]. Table Associer l'observable [sn_ti_observable].

Utilisation Now Assist pour Réponse aux incidents de sécurité pour fermer les incidents de sécurité

Les analystes de sécurité peuvent fermer rapidement les incidents de sécurité à partir de leur flux de travail grâce aux compétences d'IA générative prises en charge par Now Assist pour Réponse aux incidents de sécurité.

Vue d'ensemble de Now Assist pour Réponse aux incidents de sécurité

Grâce aux compétences d'IA générative avec Now Assist pour Réponse aux incidents de sécurité, vos analystes de la sécurité ont la possibilité de :

- Résumez les détails de l'incident de sécurité et passez rapidement en revue le contexte dans un format concis et facile à lire.
- Générer des notes de clôture (résolution).
- Générer des actions recommandées pour un incident de sécurité
- Générer des données d'analyse post-incident
- Générez des aperçus de corrélation pour accélérer l'enquête sur les incidents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les gestionnaires et les analystes de sécurité peuvent demander des résumés des incidents de sécurité et des notes de fermeture aux emplacements suivants :

- Enregistrements d'incidents de sécurité
- Réponse aux incidents de sécurité Espace
- Le Now Assist panneau.

Remarque : Les actions recommandées en cas d'incident de sécurité et les compétences d'analyse post-incident ne sont pas disponibles dans le Now Assist panneau.

Les gestionnaires et les analystes de sécurité peuvent générer des prochaines étapes recommandées et des données d'analyse post-incident à partir des emplacements suivants :

- Enregistrements d'incidents de sécurité
- Réponse aux incidents de sécurité Espace

Les gestionnaires et les analystes de sécurité peuvent créer des tâches de rattrapage à partir des actions recommandées générées uniquement à partir d'incidents de sécurité dans l'espace Réponse aux incidents de sécurité de travail.

1. Résumer un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité

   Générez un résumé d'un incident de sécurité qui inclut le problème sous-jacent, les détails de l'incident, les données des listes connexes (observables) et les principales actions déjà effectuées.

2. Générer des actions recommandées pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité
3. Générer une analyse post-incident pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité
4. Générer des aperçus de corrélation dans le Now Assist panneau avec Now Assist pour Réponse aux incidents de sécurité
5. Générer des notes de fermeture pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité

   Générer automatiquement les notes de fermeture d'un incident de sécurité.

6. Demander des compétences d'IA générative dans le Now Assist panneau pour Now Assist pour Réponse aux incidents de sécurité

   Générez des résumés et des notes de fermeture à partir du Now Assist panneau.

   Remarque : Les actions recommandées en cas d'incident de sécurité et les compétences d'analyse post-incident ne sont pas disponibles dans le Now Assist panneau.

7. Personnaliser une compétence Now Assist pour Réponse aux incidents de sécurité

   Personnalisez les champs d'entrée d'une compétence en fonction des exigences de votre environnement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résumer un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité

Comprenez le contexte d'un incident de sécurité grâce à la compétence d'IA générative de synthèse des incidents de sécurité.

Avant de commencer

Vous pouvez résumer un incident de sécurité dans l'interface legacy utilisateur principale (UI16) et dans le .Espace de travail de la Réponse aux incidents de sécurité Les champs utilisés pour les données d'entrée afin de résumer un incident à l'aide de l'IA générative doivent comporter au moins 50 mots. Pour plus d'informations sur les champs d'entrée, reportez-vous à Entrées et déclencheurs pour Now Assist pour Réponse aux incidents de sécurité.

Rôles requis : sn_si.analyste, sn_si.manager ou sn_si.basic

Procédure

1. Dans l'interface legacy utilisateur principale, accédez à **Tous** > **Incident de sécurité** > **Incidents** et ouvrez un incident de sécurité qui vous est affecté.
2. Vous pouvez également accéder à **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité** et ouvrez un incident de sécurité qui vous est affecté.
3. Dans l'onglet **Vue d'ensemble** , sélectionnez **Résumer**.
   - Le résumé généré est affiché dans une bannière en haut de l'enregistrement d'incident de sécurité dans legacy Core UI16.
   - Le résumé généré est affiché dans l'onglet **Vue d'ensemble** dans le Espace de travail de la Réponse aux incidents de sécurité.
4. **Facultatif :** Sélectionnez l'une des options suivantes une fois le résumé généré.

   (Optional) Les résumés générés par l'IA peuvent manquer des détails clés. Vous préférez peut-être vérifier l'exactitude et l'exhaustivité du résumé avant de poursuivre.

Option	Description
Afficher les détails du résumé	Sélectionnez l'icône d'informations (ⓘ) en regard de l'incident de sécurité résumé par Now Assist.
Enregistrer les informations de résumé en les ajoutant aux notes de travail de l'incident	**a.** Sélectionnez **Partager dans les notes de travail**. **b.** Vérifiez l'exactitude du contenu généré par l'IA dans le modal et apportez des modifications. **c.** Sélectionnez **Enregistrer dans les notes de travail**.
Agrandir ou réduire le résumé	Sélectionnez l'icône de développement (⌄) ou l'icône de réduction (icône ⌃) en regard de **Partager dans les notes de travail** pour développer ou réduire le résumé.
Envoyer un commentaire	Sélectionnez l'icône Utile (👍) pour un commentaire positif. Sélectionnez l'icône Inutile (👎) si le résumé n'a pas été utile.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Les commentaires améliorent le modèle d'IA générative et peuvent contribuer à optimiser les futures versions de cet outil.
Copier le résumé	Sélectionnez l'icône de copie (icône pour copier le résumé dans le presse-papiers.

Générer des notes de fermeture pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité

Générez automatiquement un brouillon des notes de fermeture d'un incident de sécurité lorsque vous le fermez. Le brouillon est modifiable et sera examiné avant la fermeture de l'incident de sécurité. Il peut être utilisé ou modifié si nécessaire. Les notes de fermeture fournissent des informations sur la résolution d'un incident de sécurité à d'autres analystes, gestionnaires et personnes concernées clés.

Avant de commencer

Rôles requis : sn_si.analyste, sn_si.manager ou sn_si.basic

Remarque :

Si les champs Code de fermeture ou Notes de fermeture sont déjà mis à jour pour un incident de sécurité, Now Assist ne modifie pas ces champs, quel que soit l'état actuel de l'incident. Pour permettre à Now Assist de mettre à jour ces champs, assurez-vous que les champs Code de fermeture et Notes de fermeture sont laissés vides.

Procédure

1. Dans l'interface legacy utilisateur principale, accédez à **Tous** > **Incident de sécurité** > **Incidents** et ouvrez un incident de sécurité qui vous est affecté.
2. Vous pouvez également accéder à **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité** et ouvrez un incident de sécurité qui vous est affecté.
3. Fermez l'incident de sécurité.

Option	Description
Fermer l'incident de sécurité dans legacy l'interface utilisateur principale16	**a.** Modifiez le champ **État** sur **Fermé**. La fenêtre modale Fermeture s'affiche. **b.** Cliquez sur la section **Notes de fermeture** . Les notes de fermeture sont générées automatiquement si aucun texte n'existe, ou vous pouvez modifier le texte existant selon vos besoins en choisissant l'option requise dans NACM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Vous voudrez peut-être examiner le texte généré et vous assurer qu'il est exact avant de fermer l'incident de sécurité. Modifiez les notes ou supprimez-les pour fournir les vôtres. Vous pouvez également **élaborer** ou **raccourcir** le texte généré. **c.** Sélectionnez l'option requise dans le menu contextuel Now Assist. **Élaborer** vous aidera à élaborer le texte et remplace le texte de résolution sélectionné. Si vous souhaitez raccourcir le texte de résolution, vous pouvez sélectionner l'option **Raccourcir** dans le menu contextuel pour rendre le texte plus concis. **d.** Mettez à jour le code de fermeture et sélectionnez **Fermer l'incident**. Le résumé de la résolution est affiché dans la section Informations sur la résolution de l'enregistrement d'incident de sécurité. **Remarque :** À l'aide du menu contextuel Now Assist, vous pouvez directement ajouter ou générer les notes de résolution dans la section **Notes de fermeture** de l'enregistrement d'incident lui-même, lorsque l'incident est à l'état **Revue** . Pour plus d'informations, voir la capture d'écran ci-dessous.
Fermer l'incident de sécurité à partir de Espace de travail de la Réponse aux incidents de sécurité	**a.** Dans l'onglet **Détails** de l'espace de travail, définissez le champ **État** sur **Fermé**. La fenêtre modale de l'exécution pas à pas s'affiche. **b.** Examinez chaque étape et sélectionnez **Suivant**. **c.** Sélectionnez **Fournir les détails de la résolution** **d.** Cliquez sur la section **Notes de fermeture** . Les notes de fermeture sont générées automatiquement si aucun texte n'existe, ou vous pouvez modifier le texte existant selon vos besoins à l'aide des options Now Assist.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Vous voudrez peut-être examiner le texte généré et vous assurer qu'il est exact avant de fermer l'incident de sécurité. Modifiez les notes ou supprimez-les pour fournir les vôtres. Vous pouvez également **élaborer** ou **raccourcir** le texte généré.

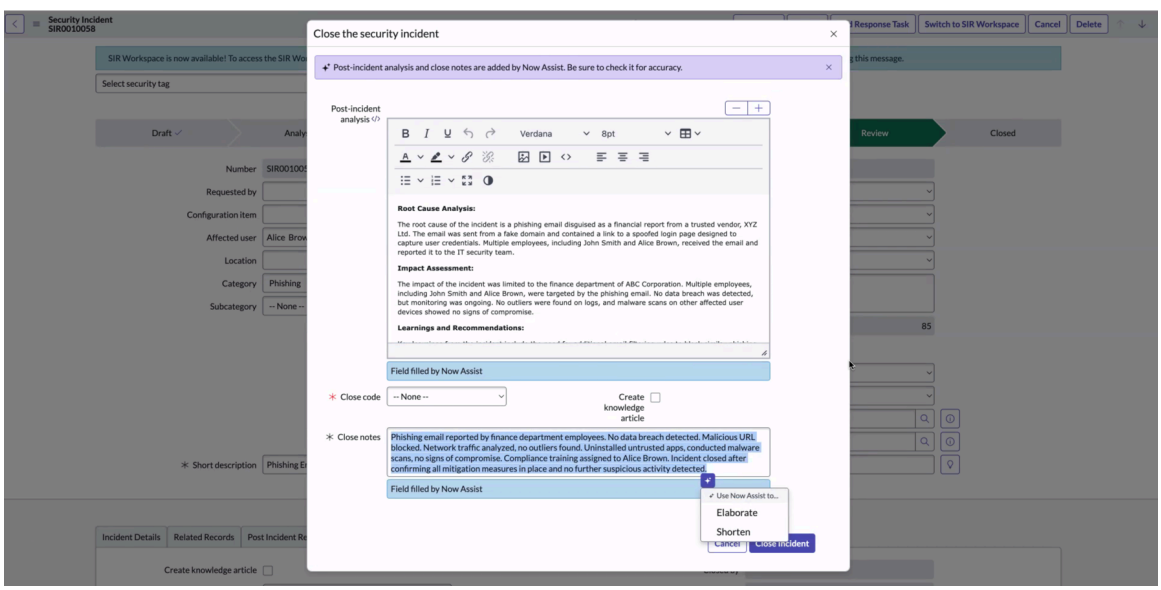
e. Sélectionnez l'option requise dans le menu contextuel Now Assist. **Élaborer** vous aidera à élaborer le texte et remplace le texte de résolution sélectionné. Si vous souhaitez raccourcir le texte de résolution, vous pouvez sélectionner l'option **Raccourcir** dans le menu contextuel pour rendre le texte plus concis.

f. Mettez à jour le code de fermeture et sélectionnez **Fermer l'incident**.

Le résumé de la résolution est affiché dans l'onglet **Détails** de l'enregistrement d'incident de sécurité dans l'espace de travail.

Remarque : À l'aide du menu contextuel Now Assist, vous pouvez directement ajouter ou générer les notes de résolution dans la section **Notes de fermeture** de l'enregistrement d'incident lui-même, lorsque l'incident est à l'état **Revue** . Pour plus d'informations, voir la capture d'écran ci-dessous.

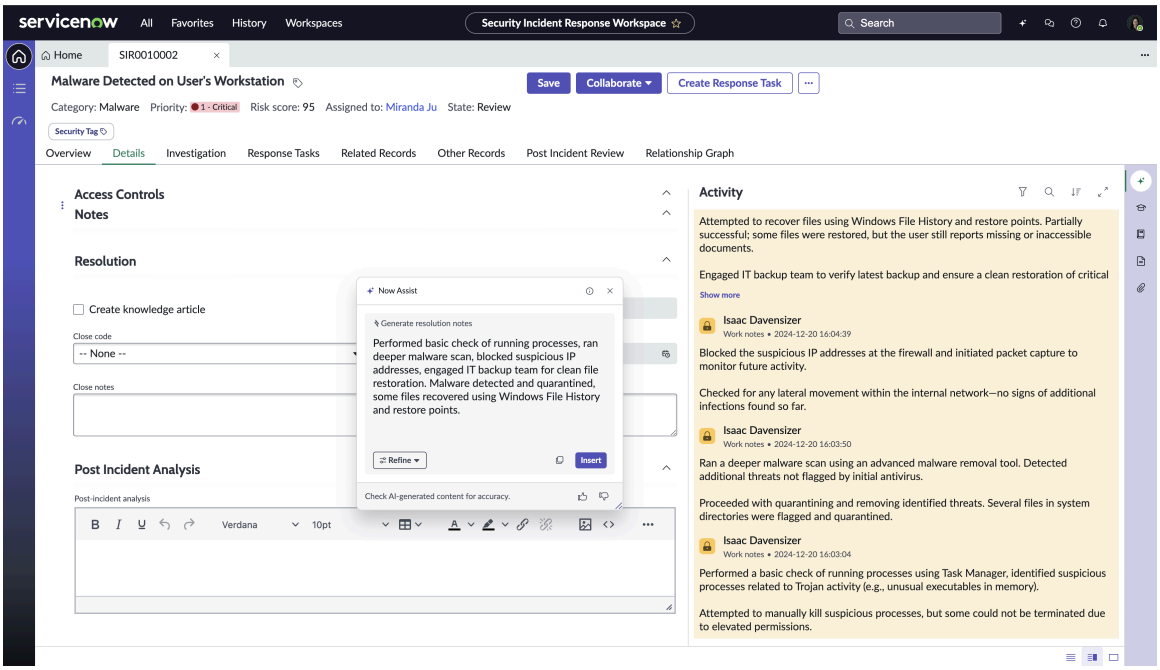
La capture d'écran suivante montre les notes de résolution générées pour fermer l'incident de sécurité dans l'interface utilisateur Core UI16.



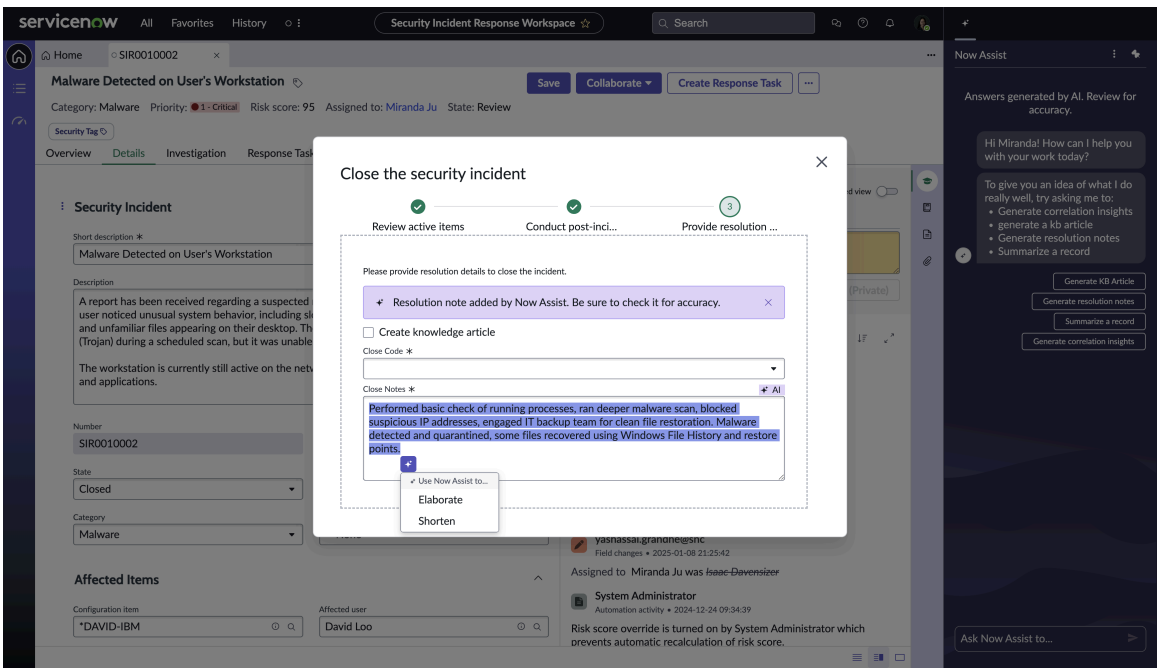
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notes de résolution générées automatiquement à partir de l'espace de travail Réponse aux incidents de sécurité.



Modifiez les notes de résolution générées à l'aide du menu contextuel Now Assist sur l'espace de travail Réponse aux incidents de sécurité.



Générer des actions recommandées pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité

Générez automatiquement les prochaines étapes que vos analystes peuvent suivre pour les aider à fermer un incident de sécurité dans l'espace de travail Réponse aux incidents de sécurité. Les étapes recommandées sont basées sur les incidents de sécurité existants et les articles de la base de connaissances.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Les prochaines étapes recommandées fonctionnent pour les incidents de sécurité actifs dans tout état autre que **Fermé** ou **Annulé**.

L'application Recherche IA doit être activée pour que la compétence Actions recommandées fonctionne pour les incidents de sécurité. Pour vérifier que Recherche IA est activé sur votre instance, accédez à **Tous** > **Recherche IA** > **État de Recherche IA**. Contactez l'assistance si la page indique que Recherche IA n'est pas activée.

Rôles requis : sn_si.analyste, sn_si.manager ou sn_si.basic

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité** et ouvrez un incident de sécurité qui vous est affecté.
2. Sélectionnez l'icône **Actions recommandées** ( ) dans la barre latérale contextuelle.



3. Sélectionnez **Obtenir des recommandations**.
4. Dans le modal Vérifier le contenu généré par l'IA, sélectionnez **Je reconnais**.
   Les actions recommandées générées sont affichées sous forme de cartes. Jusqu'à quatre références pour les actions sont affichées en haut. Ces références peuvent être n'importe quelle combinaison d'articles de la base de connaissances (KB) ou d'incidents de sécurité (SIR#).
5. Dans une carte, choisissez-en un.

Option	Description
Afficher les détails	Affichez les détails de cette action de rattrapage.
Enregistrer dans les notes de travail	Examinez les notes de travail et ayez la possibilité de les modifier avant de les enregistrer dans les notes de travail de l'incident de sécurité.
Sélectionner un lien de référence	Affichez l'incident de sécurité ou l'article de la base de connaissances utilisé comme source pour ces actions.

6. **Facultatif :** Sélectionnez l'icône d'actualisation dans le panneau Actions recommandées pour régénérer les actions recommandées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les actions recommandées restent en cache pendant une heure. Vous pouvez actualiser les étapes recommandées si :

- Vous pensez que les informations relatives à l'incident de sécurité ont changé depuis la dernière fois que vous avez généré les actions.
- Vous quittez la page, vous vous déconnectez, vous vous reconnectez et vous revenez à l'incident de sécurité dans l'heure qui suit.

Vous devez régénérer les actions en commençant par l'étape 3 pour les afficher au bout d'une heure.

7. Sélectionnez **Créer une tâche de réponse** sur une carte.
   Un nouvel onglet s'ouvre dans l'espace de travail. Les champs **Description brève** et **Description** sont renseignés automatiquement à partir des détails sur la carte d'action recommandée que vous avez sélectionnée.
8. Modifiez le formulaire selon vos besoins et sélectionnez **Enregistrer** pour créer la tâche de réponse.
   Jusqu'à ce que vous modifiiez la valeur de la propriété système, les deux options des actions recommandées que vous générez restent **Afficher les détails** et **Créer une tâche de réponse**.
9. **Facultatif :** Créez une tâche de réponse à partir des actions recommandées.
   Par défaut, le workflow vous offre la possibilité d'enregistrer les actions recommandées dans les notes de travail à partir des cartes. Si vous souhaitez avoir la possibilité de créer une tâche de réponse à partir d'une carte d'action au lieu de l'enregistrer dans des notes de travail, vous devez modifier le champ Valeur de la propriété système **Action recommandée SecOps** [sn_sec_ra.card_action_config].

   a. En tant qu'utilisateur disposant du rôle de gestionnaire d'incidents de sécurité [sn_si.manager], accédez à sys_properties. LISTE.

   b. Localisez la propriété système Action recommandée SecOps [sn_sec_ra.card_action_config] et ouvrez l'enregistrement.

   c. Remplacez la valeur share_to_work_notes par create_task.

   d. Enregistrez l'enregistrement.

   e. Revenez à l'enregistrement d'incident de sécurité et actualisez la page.
      Les cartes d'action vous fournissent les options Afficher les **détails** et **Créer une tâche de réponse**.

Générer une analyse post-incident pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité

Générez automatiquement une analyse post-incident pour un incident de sécurité qui comprend une analyse de la cause première, une évaluation de l'impact et des informations sur l'apprentissage et les recommandations.

Avant de commencer

Vous devez avoir activé la compétence d'analyse post-incident si vous souhaitez qu'une analyse post-incident soit générée automatiquement par Now Assist pour Réponse aux incidents de sécurité.

Si les notes de fermeture sont déjà remplies manuellement avant de fermer l'incident de sécurité, ce contenu n'est pas remplacé par Now Assist pour Réponse aux incidents de sécurité le moment où les analystes définissent le champ État sur **Fermé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

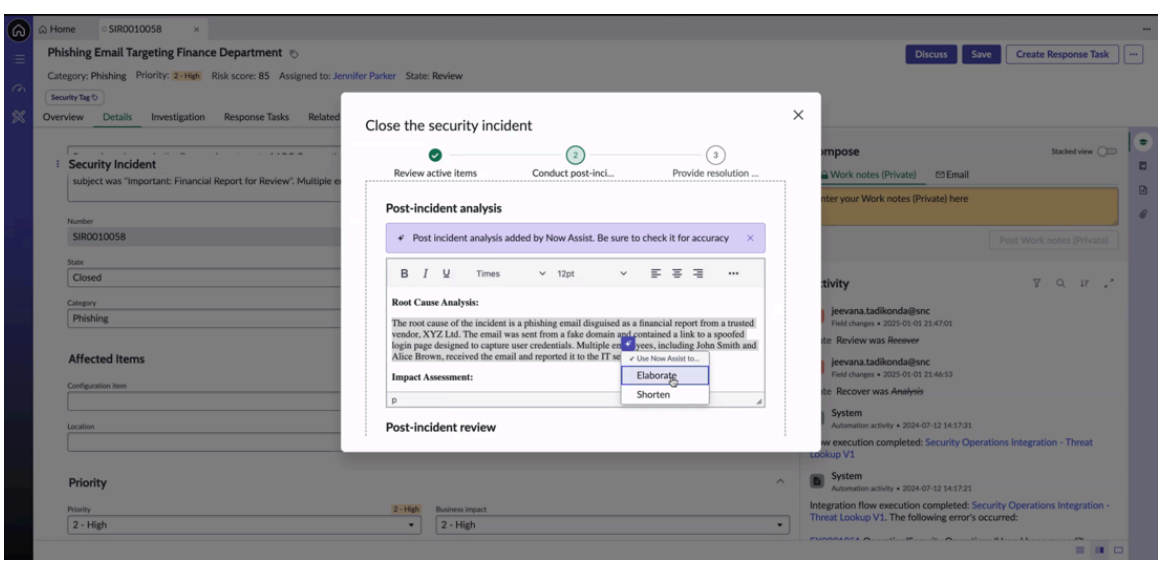
Rôles requis : sn_si.analyste, sn_si.manager ou sn_si.basic

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité** et ouvrez un incident de sécurité qui vous est affecté.
2. Dans l'onglet **Détails** , sélectionnez **Fermé** dans le champ État pour fermer l'incident de sécurité.
   La fenêtre modale Fermer l'incident de sécurité s'ouvre.
3. **Facultatif :** Sélectionnez **Examiner les tâches actives** pour examiner toutes les tâches de rattrapage actives associées à cet incident.
   Un nouvel onglet s'ouvre avec un ou des enregistrements à examiner. Utilisez cette option pour vérifier que vous êtes prêt à fermer l'incident de sécurité, car cette action annule tous les workflows et activités associés et ferme l'incident sur toutes les tâches de rattrapage associées.
4. Pour générer l'analyse post-incident, sélectionnez **Suivant**.
   L'analyse post-incident est affichée dans le modal avec trois sections. Remarque : l'icône Now Assist ( ) indique que le contenu est généré par Now Assist pour Réponse aux incidents de sécurité.
   - Analyse de la cause première
   - Évaluation de l'impact
   - Apprentissages et recommandations

   Remarque : Vous pouvez utiliser le menu contextuel Now Assist sur n'importe quelle option d'analyse post-incident et développer ou raccourcir l'analyse de la cause première/l'évaluation de l'impact/les apprentissages et les recommandations et remplacer le texte. **Élaborer** vous aidera à ajouter plus d'informations au texte existant. **Raccourcir** rendra le texte sélectionné plus concis.

   La capture d'écran suivante montre comment Menu contextuel Now Assist est utilisé pour élaborer ou raccourcir et remplacer le texte d'analyse post-incident souhaité.



5. Examinez le rapport pour en vérifier l'exactitude et apporter les modifications requises.
6. **Facultatif :** Sélectionnez **Effectuer une évaluation** et **Configurer/prévisualiser le rapport** pour effectuer l'examen post-incident.
   Toutes les modifications que vous apportez à la révision post-incident sont conservées pendant une heure si vous quittez cette page pour effectuer l'évaluation ou effectuer une autre action. Au bout d'une heure, vous devez redéfinir l'état sur **Fermé** sur l'incident pour régénérer l'analyse post-incident et fermer les notes.
7. Sélectionnez **Suivant** pour générer les notes de résolution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les notes de résolution s'affichent dans le champ Notes de fermeture.

8. Sélectionnez-en un dans la liste pour le code de fermeture.
9. Sélectionnez **Fermer l'incident**.
   L'analyse post-incident est enregistrée dans le champ Analyse post-incident de l'onglet Détails et dans l'onglet Vue d'ensemble sur les incidents de sécurité de l'espace de travail Réponse aux incidents de sécurité.

Explorer les aperçus de corrélation avec Now Assist pour Réponse aux incidents de sécurité

Vous pouvez générer des aperçus de corrélation pour éviter de dupliquer votre enquête sur les utilisateurs, les éléments de configuration et les observables affectés et pour vous aider à résoudre plus rapidement l'incident de sécurité sur lequel vous travaillez. Vous sélectionnez les critères d'un incident de sécurité sur lesquels vous souhaitez baser les aperçus de corrélation.

Génération d'aperçus de corrélation à partir de l'espace de travail Réponse aux incidents de sécurité

À partir de la version3.0.0 de , générez et affichez des aperçus de Now Assist pour Réponse aux incidents de sécurité corrélation et affichez les résultats dans le Espace de travail de la Réponse aux incidents de sécurité.

- Auparavant, si vous sélectionniez un élément de configuration (CI) ou un utilisateur affecté sur lequel baser vos informations, la recherche renvoyait l'utilisateur affecté principal ou le CI principal associé à un incident de sécurité. À partir de la version 3.0.0, l'agent vous demande avec quel CI ou utilisateur affecté vous souhaitez corréler l'incident de sécurité dans les listes connexes.
- Vous pouvez générer des aperçus de corrélation à partir de l'onglet **Examiner** pour un incident de sécurité dans n'importe quel état dans le Espace de travail de la Réponse aux incidents de sécurité.
- Vous pouvez générer des aperçus pour plusieurs éléments simultanément pour les **observables associés**, **les éléments de configuration** et **les utilisateurs affectés**.
- Les résultats sont affichés dans une boîte de dialogue non modale que vous pouvez redimensionner et déplacer.
- Votre plage de temps pour la recherche de corrélation est de 30 jours.

> **Remarque :** Une fois que vous avez généré un observable associé à un incident de sécurité, les aperçus sont stockés pour cet observable jusqu'à ce que vous le régénériez avec une plage horaire différente. Vos aperçus pour votre nouvelle plage horaire s'affichent.

La compétence de génération d'aperçus de corrélation doit être activée avant de pouvoir voir l'option **Générer des aperçus de corrélation** dans le Espace de travail de la Réponse aux incidents de sécurité. Pour plus d'informations, consultez Configurer et activer une compétence pour Now Assist pour Réponse aux incidents de sécurité.

Génération d'aperçus Now Assist de corrélation à partir du panneau dans et dans l'interface Espace de travail de la Réponse aux incidents de sécurité utilisateur (UI16)

La compétence de génération d'aperçus de corrélation doit être activée avant de pouvoir voir l'option **Générer des aperçus de corrélation** dans le Now Assist panneau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous ne voyez pas le Now Assist panneau, vous devez l'activer. Pour plus d'informations, consultez Activer le Now Assist panneau .

- Vous pouvez générer des aperçus de corrélation à partir d'un enregistrement d'incident de sécurité dans n'importe quel état dans ou Espace de travail de la Réponse aux incidents de sécurité dans l'interface legacy utilisateur (UI16).
- Par défaut, les aperçus de corrélation recherchent les enregistrements correspondants des 30 derniers jours.
- Vous pouvez localiser et examiner les valeurs des filtres **Élément de configuration**, **Utilisateur affecté** et **Observables** pour les aperçus de corrélation dans l'onglet **Détails** de ou Espace de travail de la Réponse aux incidents de sécurité sur les listes connexes Éléments de configuration, Utilisateurs affectés et Observables de l'interface legacy utilisateur (UI16).
- Vos critères de recherche et vos résultats restent affichés dans le Now Assist panneau jusqu'à ce que vous réinitialisiez la conversation. Pour réinitialiser votre conversation, sélectionnez l'icône Plus d'options (icône de Now Assist) dans le panneau et sélectionnez **Réinitialiser la conversation**.
- Vous devez avoir accès aux tables suivantes pour afficher ces enregistrements dans les aperçus de corrélation générés :
  - Table des éléments de configuration [cmdb_ci].
  - Table Incident [incident].
  - Table de demande de changement [change_request].
  - Table Problème [problem].
  - Table des éléments vulnérables [sn_vul_vulnerable_item].
  - Table Associer l'observable [sn_ti_observable].
- Vos résultats pour les aperçus de corrélation sont basés sur les tables auxquelles vous avez accès. Par exemple, si vous souhaitez afficher les éléments vulnérables (VIT) dans vos résultats d'aperçus de corrélation, vous devez avoir l'application Réponse aux vulnérabilités installée et le rôle d'accès en lecture (sn_vul.read_all).

Pour connaître les étapes de génération d'aperçus de corrélation, reportez-vous à la section Générer des aperçus de corrélation dans le Now Assist panneau avec Now Assist pour Réponse aux incidents de sécurité.

Générer des aperçus de corrélation à partir de avec Espace de travail de la Réponse aux incidents de sécuritéNow Assist pour Réponse aux incidents de sécurité

Générez et affichez des aperçus de corrélation dans pour Espace de travail de la Réponse aux incidents de sécurité vous aider à relier les événements passés à l'incident de sécurité sur lequel vous travaillez.

Avant de commencer

Rôles requis : sn_si.analyste, sn_si.manager ou sn_si.basic

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité** et ouvrez un incident de sécurité qui vous est affecté.
2. Sélectionnez l'onglet **Examiner** de l'enregistrement d'incident de sécurité.
3. Sélectionnez un ou plusieurs filtres sur lesquels vous souhaitez baser vos aperçus de corrélation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez sélectionner plusieurs observables.

- **Observables associés** : enregistrements liés par des observables partagés qui suggèrent des attaques potentielles en cours ou l'utilisation répétée d'infrastructures malveillantes. Les exemples peuvent inclure des adresses IP, des URL ou des hachages de fichiers.
- **Éléments de configuration** (CI) : enregistrements qui ont les mêmes CI pour vous aider à identifier les vulnérabilités potentielles dans des systèmes spécifiques. Un exemple pourrait être les ordinateurs portables des utilisateurs.
- **Utilisateurs affectés** : incidents passés qui ont les mêmes utilisateurs pour vous aider à voir des schémas tels que des tentatives d'hameçonnage fréquentes ou plusieurs tentatives d'accès non autorisé. Un exemple est le nom d'un utilisateur spécifique.

La liste des éléments correspondants s'affiche.

4. Sélectionnez les éléments de la liste pour lesquels vous souhaitez générer des aperçus.
5. Sélectionnez **Générer des aperçus**.
   Une boîte de dialogue s'ouvre. Après quelques instants, vos aperçus de corrélation s'affichent. Vous disposez des options suivantes dans cette boîte de dialogue :
   - Actualiser les) - Vous pouvez modifier les éléments de la liste après avoir généré vos aperçus initiaux et mettre à jour vos résultats.
   - Développer ( ) - Redimensionnez la boîte de dialogue et faites-la glisser sur la page.

   Vous disposez des options suivantes pour chaque entrée d'aperçu de corrélation dans la boîte de dialogue.

   - **Modifier la plage horaire** : sélectionnez une plage horaire pour recharger la boîte de dialogue avec les aperçus correspondants. Vos résultats pour cette entrée sont automatiquement régénérés si vous sélectionnez une nouvelle plage horaire. La plage horaire de chaque entrée s'affiche en regard de l'aperçu, par exemple, 35.35.35.35. (100 jours).
   - Dernière génération : date à laquelle l'aperçu a été généré pour la dernière fois.
   - Évaluer le contenu : (et (icône
   - Copier : (Copiez l'aperçu dans le presse-papiers.
   - **Partager dans les notes de travail** : modifiez le contenu et publiez-le dans les notes de travail sur l'incident de sécurité.

   Les aperçus de corrélation sont stockés pour les observables lorsque vous les générez pour la première fois en fonction de la période de recherche par défaut (30 jours). Ces aperçus sont stockés jusqu'à ce que vous régénériez des aperçus pour les observables avec une période de recherche différente. Modifiez la limite de 30 jours pour la requête en procédant comme suit :

   a. En tant qu'utilisateur disposant du rôle de gestionnaire d'incidents de sécurité [sn_si.manager], accédez à sys_properties. LISTE.
   b. Localisez la propriété système Période de vérification de corrélation [sn_sec_gen_ai.correlation_lookback_period] et ouvrez l'enregistrement.
   c. Saisissez un nombre dans le champ **Valeur** , jusqu'à 360.
   d. Enregistrez l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Revenez à l'enregistrement d'incident de sécurité et actualisez la page.

f. Générer des aperçus de corrélation. Vos résultats sont basés sur votre nouvelle période de recherche.

Générer des aperçus de corrélation dans le Now Assist panneau avec Now Assist pour Réponse aux incidents de sécurité

Générez des aperçus de corrélation à partir du Now Assist panneau pour vous aider à relier les événements passés à l'incident de sécurité sur lequel vous travaillez.

Avant de commencer

Rôles requis : sn_si.analyste, sn_si.manager ou sn_si.basic

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité** et ouvrez un incident de sécurité qui vous est affecté.
2. Sinon, dans l'interface legacy utilisateur (UI16), localisez un incident de sécurité dans la table Incidents de sécurité [sn_si_incident] et ouvrez-le.
3. Sélectionnez l'icône Now Assist ( ) dans l'en-tête supérieur pour ouvrir le Now Assist panneau.
4. Sélectionnez **Générer des aperçus de corrélation**.

   Des aperçus de corrélation sont générés si une ou plusieurs des valeurs suivantes peuvent être mises en correspondance. Les filtres suivants sur lesquels baser vos idées s'affichent dans le Now Assist panneau. Seuls les filtres qui présentent des correspondances avec d'autres incidents de sécurité sont affichés.

   Remarque : Si aucun enregistrement d'incident de sécurité n'est ouvert, vous êtes invité à saisir le numéro d'un enregistrement d'incident de sécurité après avoir sélectionné **Générer des aperçus de corrélation**.

   - **Élément de configuration** (CI) : enregistrements qui ont le même CI pour vous aider à identifier les vulnérabilités potentielles dans des systèmes spécifiques. Un exemple pourrait être l'ordinateur portable d'un utilisateur.
   - **Utilisateur affecté** : incidents passés qui ont le même utilisateur pour vous aider à voir des schémas tels que des tentatives d'hameçonnage fréquentes ou plusieurs tentatives d'accès non autorisé. Un exemple est le nom d'un utilisateur spécifique.
   - **Observables** : enregistrements liés par des observables partagés qui suggèrent des attaques potentielles en cours ou l'utilisation répétée d'infrastructures malveillantes. Les exemples peuvent inclure des adresses IP, des URL ou des hachages de fichiers. Vous devez saisir une valeur exacte pour un observable, par exemple, un hachage de fichier complet.

   Si aucune donnée correspondante n'existe pour l'un de ces filtres, aucune n'est affichée. Vous êtes invité à ajouter l'une de ces valeurs à l'incident de sécurité à partir duquel vous travaillez, à l'enregistrer, à réinitialiser votre conversation dans le panneau et à réessayer.

5. Réinitialisez votre conversation en sélectionnant l'icône du Now Assist menu Autres options ( ) dans le panneau et sélectionnez **Réinitialiser la conversation**.
6. Sélectionnez un filtre.

   Les résultats correspondants sont affichés dans le Now Assist panneau.

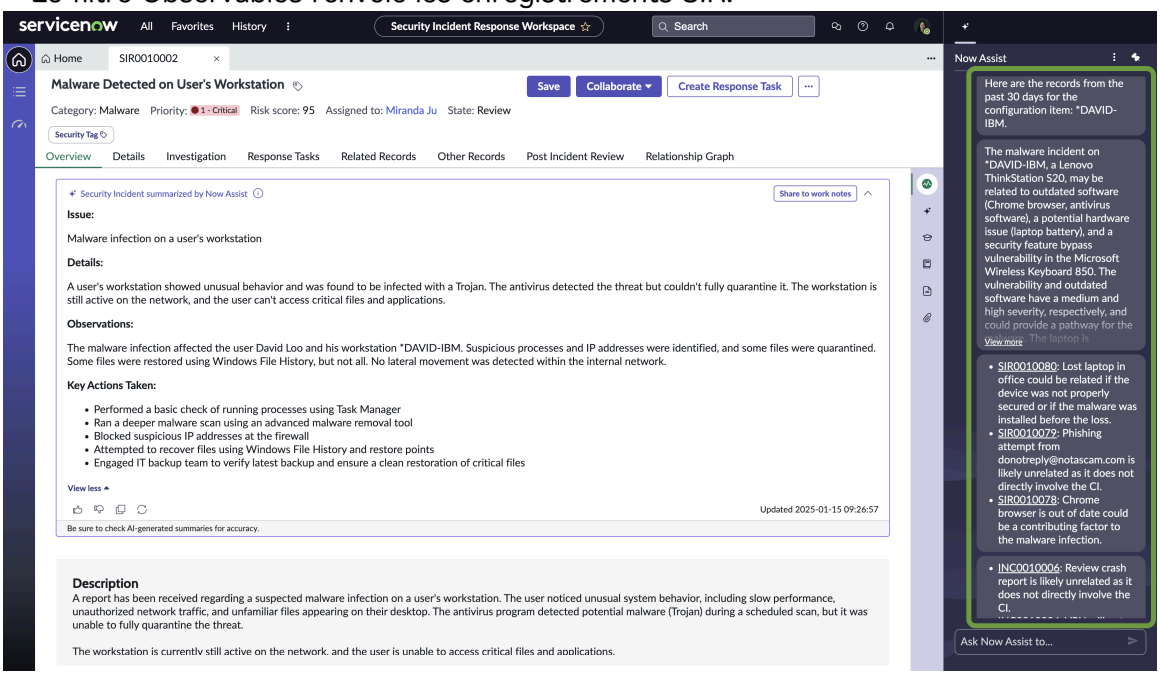
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'exemple suivant, **l'élément de configuration** a été demandé. La recherche a renvoyé un résumé de haut niveau et des liens vers les enregistrements qui ont un élément de configuration correspondant.

Les résultats sont regroupés par type d'enregistrement : enregistrement d'incident de sécurité (SIR), incident (INC), demande de changement (CHG), problème (PRB) et élément vulnérable (VIT).

- Le filtre Utilisateurs affectés renvoie les enregistrements SIR, INC et CHG.
- L'élément de filtre de configuration renvoie : les enregistrements SIR, INC, CHG, PRB et VIT.
- Le filtre Observables renvoie les enregistrements SIR.



7. **Facultatif :** Modifiez la limite de 30 jours pour la requête en procédant comme suit :
   a. En tant qu'utilisateur disposant du rôle de gestionnaire d'incidents de sécurité [sn_si.manager], accédez à sys_properties. LISTE.
   b. Localisez la propriété système Période de vérification de corrélation [sn_sec_gen_ai.correlation_lookback_period] et ouvrez l'enregistrement.
   c. Saisissez un nombre dans le champ **Valeur** , jusqu'à 360.
   d. Enregistrez l'enregistrement.
   e. Revenez à l'enregistrement d'incident de sécurité et actualisez la page.

Demander des compétences d'IA générative dans le Now Assist panneau pour Now Assist pour Réponse aux incidents de sécurité

Demandez un résumé de l'incident de sécurité ou des notes de fermeture à partir Now Assist du panneau.

Avant de commencer

Reportez-vous à la section Panneau Now Assist pour savoir comment activer le Now Assist panneau.

Rôles requis : si_analyst, si_manager ou sn_si.basic

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Connectez-vous à une instance sur laquelle l'application Now Assist pour Réponse aux incidents de sécurité est installée.
2. Dans l'interface legacy utilisateur principale, accédez à **Tous** > **Incident de sécurité** > **Incidents** et ouvrez un incident de sécurité qui vous est affecté.
3. Vous pouvez également accéder à **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité** et ouvrez un incident de sécurité qui vous est affecté.
4. Sélectionnez l'icône Now Assist ( ) dans la bannière supérieure.

Option	Description
Générer des notes de résolution	Dans le panneau Now Assist, sélectionnez **Générer des notes de résolution**. Les notes de fermeture générées dans le panneau sont identiques à celles générées lorsque vous fermez un incident de sécurité à partir d'un enregistrement. Les notes de fermeture des incidents de sécurité sont créées en fonction des mesures prises pour corriger et endiguer, ainsi que d'autres détails pertinents liés à leur fermeture. **Remarque :** Vous voudrez peut-être examiner le texte généré et vous assurer qu'il est exact avant de fermer l'incident de sécurité. Modifiez les notes ou supprimez-les pour fournir les vôtres. Consultez Générer des notes de fermeture pour un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité pour plus d'informations.
Résumer un incident de sécurité	Dans le panneau Now Assist, sélectionnez **Résumer un enregistrement**. Le résumé généré dans le panneau est identique à celui que vous générez à partir d'un enregistrement d'incident de sécurité. Les résumés générés par l'IA peuvent manquer des détails clés. Vous préférez peut-être vérifier l'exactitude et l'exhaustivité du résumé avant de poursuivre. Consultez Résumer un incident de sécurité avec Now Assist pour Réponse aux incidents de sécurité pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Générer des aperçus de corrélation	Dans le Now Assist panneau, sélectionnez **Générer des aperçus de corrélation**. Aperçus de corrélation du Now Assist panneau pour vous aider à relier les événements passés à l'incident de sécurité sur lequel vous travaillez. Voir Explorer les aperçus de corrélation avec Now Assist pour Réponse aux incidents de sécurité et Générer des aperçus de corrélation dans le Now Assist panneau avec Now Assist pour Réponse aux incidents de sécurité pour plus d'informations.

Utilisation des workflows agentiques IA dans Now Assist pour Réponse aux incidents de sécurité

Utilisez les Réponse aux incidents de sécurité agents IA pour accomplir vos tâches de manière autonome.

Workflows agentiques disponibles pour AI Agents pour Réponse aux incidents de sécurité

Nom du workflow agentique	Description	Agents IA disponibles
Fermer l'incident de sécurité	Ce workflow agentique aide les analystes de sécurité à fermer un incident de sécurité en langage naturel dans le Now Assist panneau.	Générateur de récapitulatif de l'incident de sécurité
Analyser les mesures des opérations de sécurité	Ce workflow agentique aide un responsable de centre d'opérations de sécurité (SOC) à analyser les performances de ses analystes de sécurité. Les mesures sont générées pour les enregistrements de réponse aux incidents de sécurité (SIR) pour le volume de tickets, le délai moyen d'affectation (MTTA) et le délai moyen de résolution (MTTR).	• Agent IA de la récupération des incidents de sécurité • Agent IA de l'analyse des mesures de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflows agentiques disponibles pour AI Agents pour Réponse aux incidents de sécurité (suite)

Nom du workflow agentique	Description	Agents IA disponibles
Résolution des incidents de sécurité	Ce workflow agentique aide les analystes de sécurité à identifier un chemin de résolution des incidents de sécurité. Ce workflow aide également les analystes de sécurité à fermer un incident de sécurité en langage naturel dans le Now Assist panneau.	• agent IA de la résolution des incidents de sécurité • Agent IA de gestion de l'intégration de Exchange Online • Agent IA du générateur de récapitulatif des incidents de sécurité • Agent IA de l'analyse des observables • Agent IA de gestion des activités d'incident de sécurité
Générer un rapport de transfert d'équipe SIR	Ce workflow agentique ajoute les détails d'un incident de sécurité au rapport de transfert d'équipe. L'agent remplit les différentes sections du transfert d'équipe avec le contenu approprié en identifiant les détails pertinents de l'incident de sécurité.	Transfert d'équipe de l'incident de sécurité : agent IA

Important : Par défaut, tous les workflows agentiques et les enregistrements d'agent IA sont en lecture seule.

Pour modifier un workflow agentique, vous devez d'abord Dupliquer un workflow agentique , puis procéder aux étapes suivantes :

- Activez le workflow.
- Activez tous les agents IA au sein du workflow.
- Si nécessaire, vous pouvez ajouter un déclencheur pour appeler automatiquement le workflow.

Vous recherchez un agent IA ?

- Il peut y avoir des agents IA installés avec l'application qui ne sont pas utilisés dans les Now Assist workflows agentiques. Pour savoir comment afficher tous les agents disponibles sur votre instance, consultez Rechercher des agents IA .
- Pour rechercher des agents qui ne peuvent pas être installés sur votre instance, visitez AI Agent Marketplace sur le ServiceNow Store.

Réponse aux incidents de sécurité Workflow agentique de fermeture de la collection d'agents IA

Le workflow agentique Fermer un incident de sécurité permet aux analystes de sécurité de fermer un incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble du workflow agentique Fermer un incident de sécurité

À l'aide du workflow agentique Fermer un incident de sécurité, annulez les tâches de réponse associées, générez des notes de résolution, des notes de fermeture, du code de fermeture et une analyse post-incident (PIA) lors de la fermeture d'un incident de sécurité, et fournissez des commentaires et ajustez le Now Assist contenu en langage naturel à partir du panneau.

Si vous souhaitez modifier ce workflow agentique, vous pouvez le dupliquer , ajuster les paramètres en fonction de vos besoins spécifiques et activer la version dupliquée du workflow agentique à la place.

Agent utilisé dans le workflow agentique Fermer un incident de sécurité

L'expert Générateur de récapitulatif d'incident de sécurité est utilisé dans le workflow agentique Fermer l'incident de sécurité.

Fermer un incident de sécurité

Discutez avec un agent IA dans le Now Assist panneau pour vous aider à fermer un incident de sécurité.

Avant de commencer
Rôle requis : sn_si.analyst ou sn_si.manager

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez l'incident de sécurité que vous souhaitez fermer à l'aide de l'agent IA.
3. Sélectionnez l'icône Now Assist (
   Le Now Assist panneau s'affiche.
4. Fermez l'incident de sécurité à l'aide de l'une des options suivantes.

Option	Description
Fermer un incident de sécurité	Dans le Now Assist panneau, demandez à l'agent de fermer l'incident de sécurité en langage naturel en saisissant `Fermer cet incident`, `Fermer cet incident de sécurité` ou `Fermer l'incident de sécurité : SIR0012345`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : ○ Lorsque vous entrez Fermer cet incident ou Fermer cet incident de sécurité, le Now Assist panneau sélectionne l'incident de sécurité en contexte. Lorsque vous fournissez un numéro d'incident de sécurité spécifique, tel que Fermer l'incident de sécurité : SIR0012345, le workflow agentique prend des mesures pour l'incident de sécurité suggéré. ○ Vous pouvez fermer n'importe quel incident de sécurité à partir du Now Assist panneau en fournissant le numéro de l'incident de sécurité dans votre texte. ○ Lorsque vous demandez la fermeture d'un incident de sécurité, le workflow agentique Fermer un incident de sécurité annule l'évaluation post-incident, les actions de flux, les actions de playbook, les actions de workflow et les tâches de réponse obligatoires. Toutefois, vous pouvez fermer ces actions manuellement avant de lancer la demande de fermeture de l'incident de sécurité. Le workflow agentique Fermer un incident de sécurité fournit du contenu pour chacun des champs suivants et vous demande vos commentaires. Le workflow agentique remplit vos commentaires acceptés. Une fois que vous avez accepté le contenu d'un champ, le workflow agentique fournit le contenu du champ suivant. ○ **Analyse post-incident** : acceptez le contenu suggéré en répondant par une réponse positive telle que Semble bien ou OK. Demandez au workflow agentique d'affiner le contenu et de suggérer les changements dont vous avez besoin. ○ **Fermer les notes** : acceptez le contenu suggéré en répondant par une réponse positive telle que « ça a l'air bien » ou « OK ». Vous pouvez demander au workflow agentique d'affiner le contenu et vous

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	pouvez également suggérer les changements dont vous avez besoin. ○ **Code de fermeture** : sur la base des détails de l'incident de sécurité, le workflow agentique suggère un code de fermeture. Vous pouvez accepter le code de fermeture ou suggérer un autre code de fermeture pour l'incident de sécurité. L'agent IA ferme l'incident de sécurité. **Remarque :** Lorsqu'un champ est modifié, le flux d'activité ajoute les mots « AGENT IA : » avec une description de la mise à jour effectuée par l'agent IA. Par exemple, AGENT IA : le code de fermeture est mis à jour.
Fermer un incident de sécurité en tant que faux positif	Dans le Now Assist panneau, vous pouvez demander à l'agent IA de fermer l'incident de sécurité en tant que faux positif. Par exemple, Fermer cet incident en tant que faux positif ou fermer cet incident de sécurité en tant que faux positif. Le workflow agentique fournit le résumé de l'incident de sécurité. Pour fermer l'incident de sécurité, saisissez des réponses positives telles que « semble bien » ou « OK ». L'agent IA ferme l'incident de sécurité. Elle met également à jour les notes de fermeture comme Fermé par l'agent IA comme Faux positif et le code de fermeture comme **Faux positif** et annule toutes les tâches de réponse actives.

Réponse aux incidents de sécurité Collection d'agent IA Workflow agentique de résolution d'incident de sécurité

Discutez avec un agent IA dans le Now Assist panneau pour vous aider à créer un plan de résolution d'un incident de sécurité et à le résoudre.

Résoudre un incident de sécurité Vue d'ensemble du workflow agentique

Utilisez le workflow agentique Résoudre un incident de sécurité pour extraire les détails de l'incident, extraire les articles de la base de connaissances et les incidents de sécurité fermés similaires, obtenir un plan de résolution et résoudre l'incident de sécurité.

Si vous souhaitez modifier ce workflow agentique, vous pouvez le dupliquer , ajuster les paramètres en fonction de vos besoins spécifiques et activer la version dupliquée du workflow agentique à la place.

Agents utilisés dans le workflow agentique Résoudre un incident de sécurité

Le workflow agentique Résoudre un incident de sécurité contient les agents suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- agent IA de la résolution des incidents de sécurité
- Agent IA de gestion de l'intégration de Exchange Online
- Agent IA du générateur de récapitulatif des incidents de sécurité
- Agent IA de l'analyse des observables
- Agent IA de gestion des activités d'incident de sécurité

Résoudre un incident de sécurité

Discutez avec un agent IA dans le Now Assist panneau pour résoudre un incident.

Avant de commencer

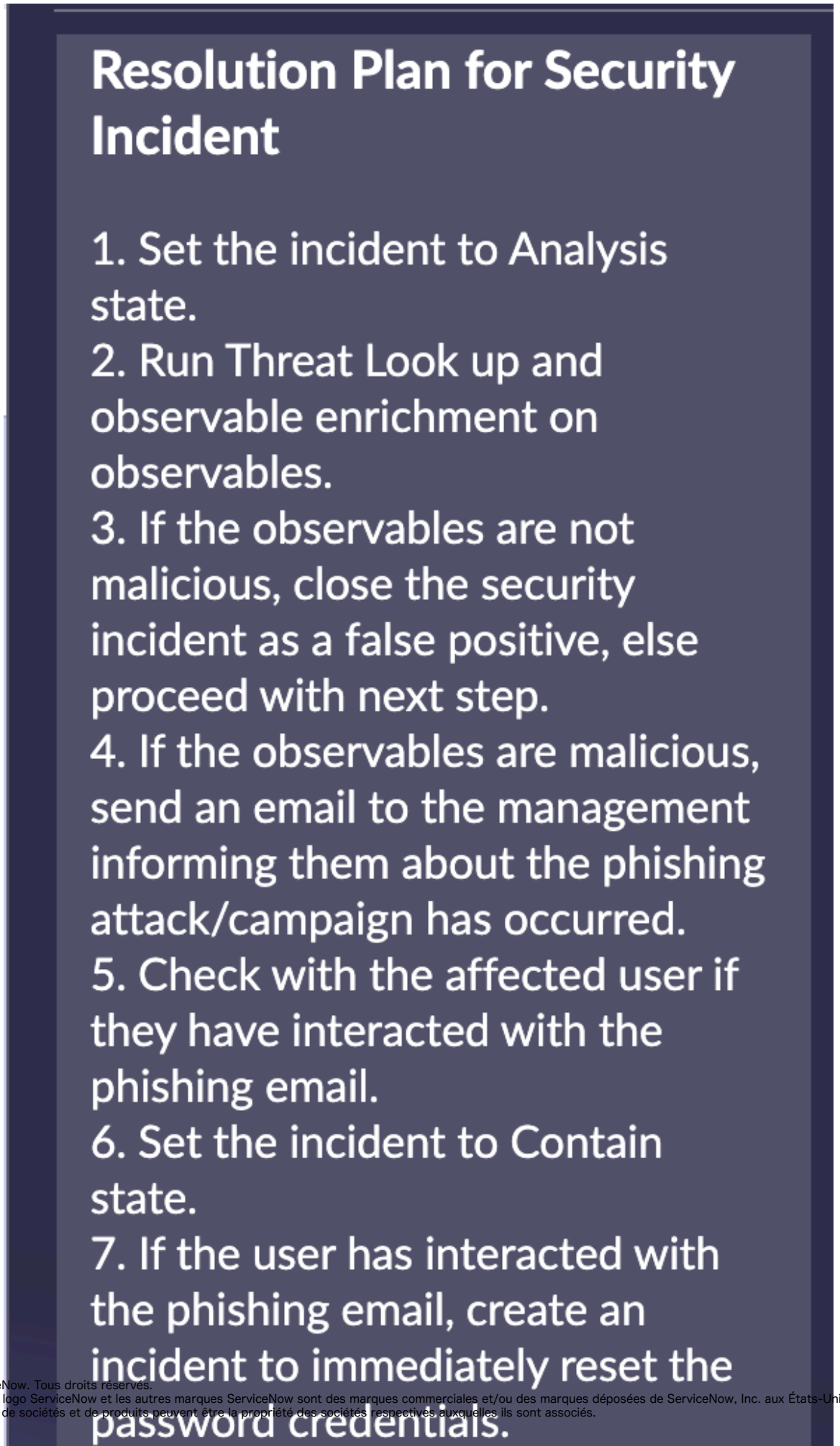
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez l'incident de sécurité que vous souhaitez résoudre à l'aide de l'agent IA.
3. Sélectionnez l'icône ( Now Assist IA).
   Le workflow agentique Résoudre un incident de sécurité est disponible sur demande. Vous pouvez entrer une requête en langage naturel pour résoudre un incident de sécurité à l'aide de ce workflow agentique.
4. Dans le Now Assist panneau, demandez à l'agent de résoudre l'incident de sécurité en saisissant Résoudre cet incident, Résoudre cet incident de sécurité ou Résoudre l'incident de sécurité : SIR0012345.
   Le Now Assist panneau fournit toutes les actions que vous pouvez effectuer sur l'incident de sécurité.
5. Sélectionnez **Résoudre un incident de sécurité**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’agent IA analyse l’incident de sécurité et fournit un résumé de l’incident ainsi que son état actuel. En outre, en utilisant les détails de l’incident, les articles de la base de connaissances et d’autres incidents de sécurité fermés similaires, l’agent IA fournit un plan de résolution.

6. Saisissez des réponses positives telles que Semble bien ou OK si vous acceptez le plan de résolution. Pour une réponse positive, l’agent IA examine chaque étape du plan de résolution et aide l’analyste (l’utilisateur disposant du rôle sn_si.analyst) à la résoudre. Pour chaque étape, l’agent IA fournit des commentaires et des demandes d’intervention de l’analyste. Par exemple, si l’agent IA identifie l’incident généré pour un e-mail d’hameçonnage, le workflow agentique suivant se produit :

Workflow agentique pour la résolution d’un incident d’hameçonnage par e-mail

Tâches de résolution d’un incident de sécurité	Description
Mettre à jour l’état de l’incident de sécurité	L’agent IA met à jour l’état de l’incident de sécurité. Par exemple, si l’état de l’incident de sécurité est Brouillon, l’agent IA le met à jour sur Analyse.
Exécuter une recherche de menace et un enrichissement d’observable sur l’observable	L’agent IA lance un processus de recherche de menaces et d’enrichissement des observables. Lorsque l’analyste confirme avec une entrée positive, l’agent IA fournit le résumé de l’analyse et de l’enrichissement des observables.
Pour les observables malveillants, envoyez un e-mail à la direction	L’analyste peut demander à l’agent IA d’envoyer un mail à la direction. L’agent IA fournit un brouillon d’e-mail et demande les destinataires de l’e-mail. **Remarque :** L’analyste peut vérifier l’e-mail envoyé dans l’onglet **Autres enregistrements** .
Vérifiez avec l’utilisateur affecté s’il a interagi avec l’e-mail d’hameçonnage	L’analyste vérifie manuellement auprès de l’utilisateur concerné s’il a interagi avec l’e-mail d’hameçonnage.
Si l’utilisateur a interagi avec l’e-mail d’hameçonnage, réinitialisez ses informations d’identification du mot de passe	Si l’utilisateur affecté a interagi avec l’e-mail d’hameçonnage, l’analyste peut demander à l’agent IA de créer un incident pour réinitialiser le mot de passe de l’utilisateur. L’agent IA fournit un résumé de l’incident et crée un incident lorsque l’analyste approuve le résumé.
Bloquer l’expéditeur/l’e-mail/l’URL sur la passerelle de messagerie	L’agent IA demande à l’analyste de bloquer l’expéditeur/l’e-mail/l’URL sur la passerelle de messagerie. L’analyste peut demander à l’agent IA de créer une tâche de réponse pour bloquer l’expéditeur/l’e-mail/l’URL sur la passerelle de messagerie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de résolution d'un incident de sécurité	Description
	L'agent IA fournit les informations pour les tâches de réponse et crée une tâche de réponse une fois approuvée par l'analyste. **Remarque :** L'analyste peut terminer la tâche de réponse et la marquer comme **Terminée** dans l'onglet **Tâches de réponse** . L'analyste confirme à l'agent IA que la tâche de réponse est terminée.
Rechercher et supprimer l'e-mail d'hameçonnage de toutes les boîtes de réception des utilisateurs	L'agent IA demande à l'analyste de supprimer l'e-mail d'hameçonnage de toutes les boîtes de réception des utilisateurs. L'analyste supprime l'e-mail d'hameçonnage et confirme à l'agent IA.
Inscrire l'utilisateur affecté à une formation obligatoire sur l'hameçonnage	Si l'utilisateur affecté a interagi avec l'e-mail d'hameçonnage, l'agent IA informe l'analyste d'inscrire l'utilisateur affecté à la formation obligatoire sur l'hameçonnage.
Réaliser l'audit de l'incident de sécurité	L'agent IA effectue l'audit de l'incident de sécurité et fournit le résumé.
Fermer l'incident de sécurité	L'agent IA ferme l'incident. Pour plus d'informations, consultez Fermer un incident de sécurité.

Réponse aux incidents de sécurité Collection d'agents IA pour le workflow agentique Analyser les mesures des opérations de sécurité

Le workflow agentique Analyser les mesures des opérations de sécurité aide les gestionnaires du centre des opérations de sécurité à analyser les performances de leurs équipes de sécurité.

Vue d'ensemble du workflow agentique Analyser les mesures d'opérations de sécurité

Les responsables des centres d'opérations de sécurité (SOC) peuvent analyser les mesures du volume global de tickets, du délai moyen d'affectation (MTTA) et du délai moyen de résolution (MTTR) sur les enregistrements Security Incident Response (SIR) afin d'avoir un aperçu des performances de leurs analystes de sécurité. Ils peuvent également demander des recommandations sur la façon d'améliorer les mesures.

Agents utilisés dans le workflow agentique Analyser les mesures d'opérations de sécurité

- Agent IA de la récupération des incidents de sécurité
- Agent IA de l'analyse des mesures de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Outils mappés au workflow agentique Analyser les mesures d'opérations de sécurité

Les outils suivants sont mappés aux agents IA utilisés dans le workflow agentique Analyser les mesures des opérations de sécurité.

Type d'outil	Mode d'exécution	Nom	Description
Script	Autonome	Rechercher des incidents de sécurité	Cet outil appelle le script avec l'entrée correcte de la requête de l'utilisateur pour récupérer les incidents de sécurité à partir de la base de données.
Script	Autonome	Analyse	Fournit une analyse plus approfondie pour un type de mesure, analyste, groupe, startDate, endDate et performances SOC spécifiés.
Script	Autonome	Calcul	Calcule les mesures de performance pour les gestionnaires SOC telles que le délai moyen de résolution (MTTR) et le délai moyen d'affectation (MTTA).
Script	Autonome	Recommander	Recommande des actions de gestion qui pourraient être entreprises sur la base de l'analyse d'une mesure.

Déclencheurs pour le workflow agentique Analyser les mesures des opérations de sécurité

Il n'existe aucun déclencheur pour ce cas d'utilisation. Si nécessaire, vous pouvez ajouter un déclencheur pour appeler automatiquement le cas d'utilisation.

Analyser les mesures d'opérations de sécurité : workflow agentique

Discutez avec un agent IA à partir du Now Assist panneau pour vous aider à mieux comprendre l'efficacité avec laquelle vos analystes de sécurité travaillent avec la résolution des incidents de sécurité.

Avant de commencer

Vous devez activer la compétence d'analyse des Now Assist mesures des opérations de sécurité avant de pouvoir utiliser les agents IA avec le workflow agentique Analyser les mesures des opérations de sécurité. Pour plus d'informations, consultez Configurer et activer une compétence pour Now Assist pour Réponse aux incidents de sécurité.

Rôle requis : sn_si.manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sélectionnez l'icône ( ) n'importe Now Assist où dans votre instance.
   Le Now Assist panneau s'affiche.
2. Sélectionnez **Analyser les mesures de Security Operations** dans le Now Assist panneau.
3. À l'invite, sélectionnez **Analyser les mesures d'incident de sécurité**.

   Le ticket de workflow agentique Analyser les mesures d'opérations de sécurité est disponible sur demande. Vous pouvez entrer n'importe quelle requête en langage naturel, mais vous pouvez envisager d'utiliser les invites décrites dans le tableau et les étapes suivants pour vous familiariser avec les données de mesures disponibles et ce que vous pouvez en faire.

Votre demande ou réponse	Description
Entrez un nom pour l'un de vos groupes d'analystes de sécurité et demandez des mesures, par exemple : ○ **Analyser les mesures des opérations de sécurité pour l'équipe d'analystes L1.** ○ **Mesures de sécurité pour l'équipe d'analystes L1 au cours des six derniers mois.** ○ **Comment s'est comportée l'équipe d'analystes L1 le mois dernier ?**	Spécifiez une équipe par son nom et indiquez une période.
Terminez la session ou **arrêtez-vous**.	Mettez fin à la conversation.

   Vous préférerez peut-être que l'espace de travail s'ouvre Réponse aux incidents de sécurité dans un autre onglet afin de pouvoir vous référer aux groupes d'affectation, aux dates et à d'autres informations pour vos invites.

   Votre conversation est enregistrée jusqu'à ce que vous démarriez une nouvelle messagerie instantanée. Pour lancer une nouvelle messagerie instantanée, sélectionnez l'icône Nouvelle messagerie ( ).

   Votre demande est répétée et affichée en surbrillance avec plus d'informations.

   Après quelques instants, vous êtes invité à fournir plus d'informations sur un analyste ou un groupe d'analystes spécifique.

4. Saisissez un nom de groupe d'affectation, par exemple, **Équipe d'analystes L1**.
5. À l'invite, saisissez une plage horaire, par exemple, **Les six derniers mois**.
   Les résultats pour le délai moyen de résolution (MTTR), le délai moyen d'affectation (MTTA) et le nombre total d'incidents de sécurité traités par votre équipe sont affichés. Sélectionnez le lien pour plus d'informations. Un nouvel onglet s'ouvre avec une liste dans UI16.
6. Développez la liste **Sources** et sélectionnez le lien Liste des **incidents de sécurité** .
   Une liste des incidents de sécurité affectés au groupe d'analystes L1 s'affiche dans un nouvel onglet de l'interface utilisateur 16. En haut de la liste, la plage de dates demandée (**6 mois**) s'affiche au format suivant : Ouvert > = 2024-09-23 > Ouvert < = 2025-03-23. Vous êtes invité à effectuer une analyse plus détaillée du MTTR, du MTTA ou du volume de tickets.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans cette liste, vous pouvez sélectionner un lien pour ouvrir des incidents de sécurité individuels à examiner. Vous pouvez entrer un numéro d'enregistrement dans la liste dans la messagerie instantanée pour que l'agent IA le résume.

7. Revenez à la messagerie instantanée et saisissez votre demande pour une mesure de performance en langage naturel, par exemple, `Oui, approfondir MTTR`.
   Des informations supplémentaires sont fournies pour votre demande, notamment un résumé et des données organisées en sections pour les champs relatifs à l'incident de sécurité.
   - Analyse des catégories : répartition par catégorie. Les exemples peuvent inclure un accès non autorisé, une vulnérabilité non corrigée, unfaux positif, etc.
   - Analyse des priorités : répartition par gravité : critique, élevée, modérée.
   - Analyse de l'équipe : répartition du MTTR par membres individuels de l'équipe.
   - Analyse des valeurs hors norme : répartition des incidents de sécurité qui ont des valeurs anormalement élevées, basses ou d'autres valeurs uniques.
8. À l'invite, saisissez une réponse affirmative à la demande de suggestions d'amélioration.
   Vos suggestions s'affichent. En fonction des résultats de l'évaluation, vous souhaiterez peut-être rechercher plus d'informations sur des types spécifiques d'incidents de sécurité.
9. À l'invite, par exemple, demandez en langage naturel tous les incidents de sécurité de la catégorie hameçonnage dont l'état est **Analyse**.
10. Sélectionnez le lien **Afficher les résultats** .
    Une liste des incidents de sécurité qui correspondent à votre demande est fournie dans un nouvel onglet dans UI16.

    À partir de cette liste, vous pouvez ouvrir des incidents individuels et demander des résumés à l'agent IA.
11. **Facultatif :** Modifiez les propriétés système pour les champs sources utilisés pour l'analyse des mesures et la valeur du facteur aberrant.
    - sn_sec_gen_ai.aia_metric_analysis_dimensions : l'agent IA décompose l'analyse en fonction des champs suivants lors de l'analyse des mesures MTTR et MTTA : **catégorie**, **priorité**, **close_code**, **assigned_toalert_sensor**. Les utilisateurs disposant des rôles sn_si.manager et sn_si.admin peuvent modifier cette liste.
    - sn_sec_gen_ai.aia_metric_analysis_outlier_factor : cette propriété détermine le facteur de valeur hors norme pour MTTR et MTTA. La valeur hors norme par défaut est 2. Par défaut, un enregistrement est une valeur aberrante si son MTTR dépasse 2 fois le temps moyen qu'il faut à un groupe d'affectation pour résoudre les incidents de sécurité pour la période que vous avez demandée. Les utilisateurs disposant des rôles sn_si.manager et sn_si.admin peuvent modifier cette valeur.

Générer un rapport de transfert d'équipe SIR

Discutez avec un agent IA dans le Now Assist panneau pour utiliser le workflow agentique Générer un rapport de transfert d'équipe SIR afin de vous aider à ajouter les détails d'un incident de sécurité à un rapport de transfert d'équipe.

Générer un rapport de transfert d'équipe SIR Vue d'ensemble

Utilisez le workflow agentique Générer un rapport de transfert d'équipe SIR pour ajouter les détails d'un incident de sécurité au rapport de transfert d'équipe. L'agent remplit les différentes sections du transfert d'équipe avec le contenu approprié en identifiant les détails pertinents de l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'agent IA identifie si l'analyste a accès à un enregistrement de transfert d'équipe, génère du contenu à partir des détails de l'incident de sécurité pour chaque section du rapport de transfert d'équipe. L'analyste peut fournir des commentaires sur le contenu, et l'agent IA génère le contenu mis à jour et enregistre le contenu dans le rapport de transfert d'équipe lorsque l'analyste approuve.

Si vous souhaitez modifier ce workflow agentique, vous pouvez le dupliquer , ajuster les paramètres en fonction de vos besoins spécifiques et activer la version dupliquée du workflow agentique à la place.

Agents utilisés dans la vue d'ensemble Générer le rapport de transfert d'équipe SIR

Le workflow agentique Générer un rapport de transfert d'équipe SIR contient les agents suivants : Agent IA de transfert d'équipe d'incident de sécurité.

Ajouter un incident de sécurité au rapport de transfert d'équipe

Discutez avec un agent IA dans le panneau pour ajouter les détails d'un Now Assist incident de sécurité à un rapport de transfert d'équipe.

Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez l'incident de sécurité que vous souhaitez ajouter à un rapport de transfert d'équipe à l'aide de l'agent IA.
3. Sélectionnez l'icône (Now Assist IA).
   Le workflow agentique Générer un rapport de transfert d'équipe SIR est sur demande. Vous pouvez entrer une requête en langage naturel pour ajouter un incident de sécurité à un rapport de transfert d'équipe.
4. Dans le Now Assist panneau, demandez à l'agent d'ajouter un incident de sécurité à un rapport de transfert d'équipe Ajoutez cet incident de sécurité au transfert d'équipe, ou Ajoutez cet incident au transfert d'équipe : SIR0012345 et appuyez sur la touche Entrée.
   Le Now Assist panneau déclenche le workflow « Ajouter un incident de sécurité pour le transfert d'équipe ». Ce workflow récupère les détails de l'incident de sécurité.

   L'agent IA trouve l'enregistrement de transfert d'équipe en cours auquel l'analyste a accès et y ajoute les détails de l'incident de sécurité. S'il existe plusieurs enregistrements de transfert d'équipe en cours auxquels l'analyste a accès, l'agent IA répertorie les cinq premiers enregistrements de transfert d'équipe que l'analyste doit sélectionner.

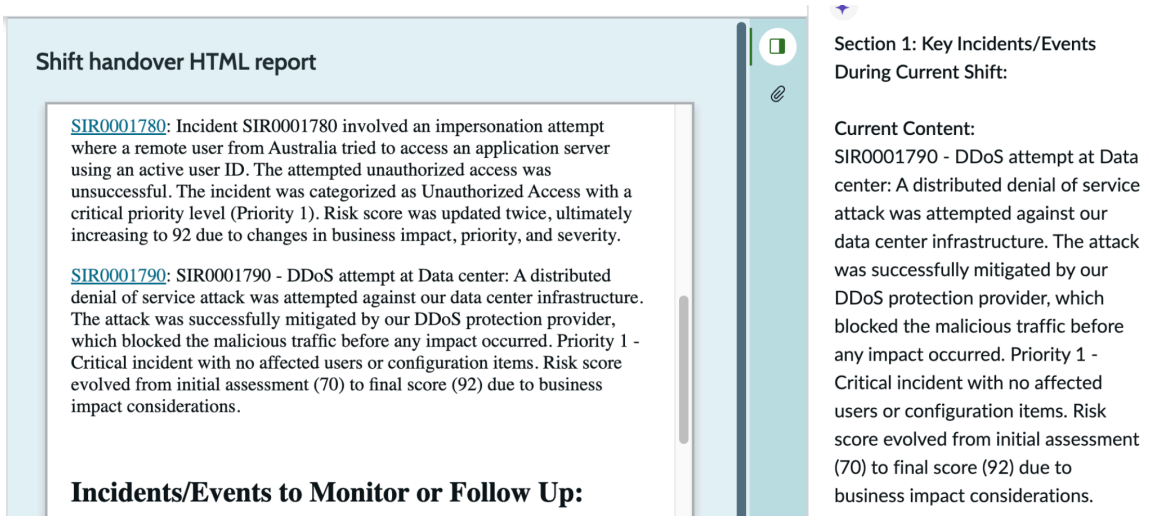
   S'il n'existe aucun enregistrement de transfert d'équipe à l'état « en cours » et affecté au groupe de l'utilisateur, ou s'il n'existe aucun enregistrement de transfert d'équipe, un message de notification s'affiche indiquant qu'il n'existe aucun enregistrement de transfert d'équipe actif pour l'utilisateur.
5. Fournissez le numéro d'enregistrement du transfert d'équipe et appuyez sur la touche Entrée.
   L'agent IA valide l'enregistrement de transfert d'équipe pour déterminer si l'enregistrement est valide et en cours, l'analyste connecté a accès à l'enregistrement de transfert d'équipe. Une fois la validation réussie, l'agent IA génère le contenu de l'enregistrement de transfert d'équipe et le fournit pour approbation.
6. Saisissez des réponses positives telles que Semble bien, Approuvé ou OK si vous êtes d'accord avec le contenu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’agent IA enregistre le contenu approuvé dans la section appropriée du rapport de transfert d’équipe.

Pour chaque section du rapport de transfert d’équipe, l’agent IA fournit le contenu et demande des commentaires à l’analyste. Si nécessaire, vous pouvez ignorer pour mettre à jour n’importe quelle section.



Résultats

L’agent IA affiche le résumé de toutes les sections mises à jour et ignorées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Shift Handover Report Update Complete

Security incident **SIR0051335** has been successfully added to shift handover report **SHR0001013**.

Summary of Processing:

Sections Saved (7 total):

1. ✅ Key Incidents/Events During Current Shift
2. ✅ Incidents/Events to Monitor or Follow Up
3. ✅ System/Infrastructure Updates
4. ✅ Outstanding Action Items
5. ✅ Shift Notes/Comments
6. ✅ Next Steps for Incoming Shift
7. ✅ References

Sections Skipped: None

All sections have been successfully

Traduction automatique

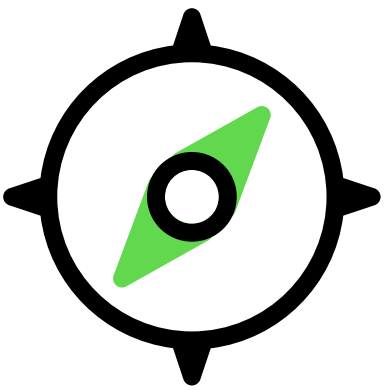
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Now Assist pour Réponse aux vulnérabilités

Utilisez l'application pour aider vos gestionnaires de vulnérabilités et vos analystes à évaluer votre exposition potentielle aux vulnérabilités critiques et à obtenir un aperçu de la conformité de votre accord sur les Now Assist pour Réponse aux vulnérabilités niveaux de service (SLA) pour les éléments vulnérables.

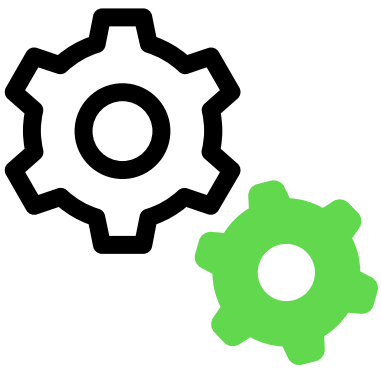
Premiers pas

Explorer



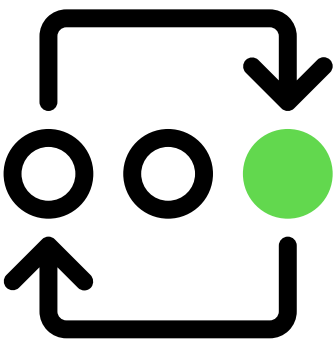
En savoir plus Now Assist pour Réponse aux vulnérabilités

Configurer



Découvrez comment configurer et activer les compétences d'IA générative et les workflows agentiques pour Now Assist pour Réponse aux vulnérabilités

Utiliser



Apprendre à utiliser Now Assist pour Réponse aux vulnérabilités

Collection d'agents



IA

Obtenir des informations sur les agents IA et les workflows agentiques pour Now Assist pour Réponse aux vulnérabilités

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

- Tous les fournisseurs de modèles ne sont pas disponibles pour les clients ayant des SKU dans le pays, et certains produits/fonctionnalités Now Assist ne sont actuellement pas disponibles pour les clients dans le pays. Pour plus d'informations, consultez l'article KB1584492 dans la base de connaissances Now Support. Assurez-vous de vérifier les mises à jour de disponibilité des fournisseurs de modèles dans les versions futures.
- Certains Now Assist produits/fonctionnalités ne sont actuellement pas disponibles pour les clients dans les centres de données FedRAMP, NSC DOD IL5 ou protégés par l'IRAP en Australie, les clients auto-hébergés ou dans d'autres environnements restreints. Pour en savoir plus, consultez l'article KB0743854 dans la Now Support Base de connaissances. Assurez-vous de consulter les mises à jour de disponibilité dans les versions futures.
- Certains Now Assist produits/fonctionnalités ne sont actuellement disponibles que pour les clients dans certaines régions. Assurez-vous de consulter les mises à jour de disponibilité dans les versions futures.

Ressources utiles

Voici quelques ServiceNow ressources qui peuvent vous fournir des informations utiles :

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Traitement des données

Cette application nécessite que les données soient transférées des instances individuelles des clients ServiceNow vers un environnement ServiceNow centralisé, qui peut être situé dans une région du centre de données différente de celle où se trouve votre instance, et potentiellement vers un fournisseur de cloud tiers, comme Microsoft Azure. Ces données sont traitées conformément aux politiques et procédures internes de ServiceNow, y compris nos politiques disponibles via notre portail de conformité CORE .

Collecte de données

ServiceNow collecte et utilise les entrées, les sorties et les modifications des sorties de cette application pour développer et améliorer les technologies ServiceNow, y compris les modèles ServiceNow et les produits d'IA. En outre, cette application collecte les données de vulnérabilité que vous importez ainsi que des informations sur les éléments de configuration dans votre CMDB. Les clients peuvent se désabonner de la collecte de données future à tout moment, comme décrit dans la page Now Assist Se désabonner .

Pour plus d'informations, consultez le Now Assist documentation .

Explorer Now Assist pour Réponse aux vulnérabilités

Obtenez des informations sur la façon dont vos gestionnaires et analystes de vulnérabilités peuvent utiliser les Now Assist compétences et les agents IA avec Now Assist pour Réponse aux vulnérabilités.

Vue d'ensemble de Now Assist pour Réponse aux vulnérabilités

Grâce Now Assist aux compétences fournies avec l'application Now Assist pour Réponse aux vulnérabilités , vos responsables de vulnérabilité et vos analystes ont la possibilité d'identifier,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d’examiner et de fermer les éléments vulnérables en double importés de vos scanners de vulnérabilité.

Les gestionnaires et les analystes ont également la possibilité d’obtenir des conseils clairs sur la façon de résoudre les éléments vulnérables, notamment en fournissant des solutions potentielles préférées importées des compétences de fournisseurs Now Assist tiers.

Grâce aux agents IA et aux workflows agentiques fournis avec l’application, vos gestionnaires et analystes de vulnérabilité ont la possibilité de déterminer l’exposition potentielle de votre environnement aux vulnérabilités récentes et connues et de voir dans quelle mesure vos cibles de rattrapage sont conformes à vos accords sur les Now Assist pour Réponse aux vulnérabilités niveaux de service (SLA).

Now Assist pour Réponse aux vulnérabilités utilisateurs

Utilisateurs

Utilisateur	Description
Responsables et analystes des vulnérabilités	Déterminez votre exposition aux vulnérabilités de votre environnement et leur impact potentiel sur vos éléments de configuration (CI) et services aux entreprises.
Responsables et analystes des vulnérabilités	Obtenez un aperçu de la façon dont vous atteignez vos cibles de rattrapage des vulnérabilités conformément à vos accords sur les niveaux de service (SLA).
Responsables et analystes des vulnérabilités	Fournissez des étapes aux analystes pour corriger les éléments vulnérables (VIT) qui leur sont affectés avec des rubriques de surveillance et des efforts de rattrapage.
Responsables et analystes des vulnérabilités	Obtenez une assistance claire sur la résolution des tâches de rattrapage, y compris les solutions potentielles préférées, le cas échéant.
Responsables et analystes des vulnérabilités	Identifiez et examinez les éléments vulnérables en double importés par vos scanners de vulnérabilité. Identifiez l’élément vulnérable primaire associé à un élément de configuration.

Now Assist pour Réponse aux vulnérabilités avantages

Fonctionnalités de Now Assist pour Réponse aux vulnérabilités

Avantage	Fonctionnalité	Utilisateurs
Identifiez l’élément vulnérable primaire (premier trouvé) pour un élément de configuration et supprimez les éléments vulnérables d’hôte (VIT) en double.	Compétence de déduplication d’élément vulnérable	Responsables et analystes des vulnérabilités
Obtenez des conseils sur la façon de résoudre les tâches de rattrapage qui incluent les solutions potentielles et préférées disponibles auprès de fournisseurs tiers.	Recommander la solution privilégiée pour la compétence VIT	Responsables et analystes des vulnérabilités

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalités de Now Assist pour Réponse aux vulnérabilités (suite)

Avantage	Fonctionnalité	Utilisateurs
• Identifiez les actifs avec des vulnérabilités et des expositions communes (CVE). • Déterminez le nombre d'éléments de vulnérabilité actifs (VIT) qui correspondent à des CVE. • Identifier les services d'entreprise présentant des vulnérabilités connues. • Créez des rubriques de surveillance pour le rattrapage des éléments vulnérables (VIT) en fonction des informations fournies. L'agent IA peut créer un effort de rattrapage pour les VIT actifs associés à la rubrique de surveillance.	Évaluer l'exposition à la vulnérabilité workflow agentique	Responsables et analystes des vulnérabilités
Obtenez un aperçu de la progression du résumé de conformité de votre accord sur les niveaux de service (SLA) au cours des 30 derniers jours. Affichez les groupes et les types d'actifs qui ont manqué les SLA pour vous aider à suivre et à ajuster les cibles.	Analyser le workflow agentique d'état du rattrapage de vulnérabilité	Responsables et analystes des vulnérabilités
Récupérez le contexte et les détails pertinents pour les éléments vulnérables qui vous sont affectés. Analysez, planifiez et créez des étapes de correction.	Étapes pour la résolution des problèmes	Analystes de vulnérabilité

Ce qu'il faut explorer ensuite

Pour en savoir plus sur la configuration et l'utilisation de Now Assist pour Réponse aux vulnérabilités, consultez :

- Configurer Now Assist pour Réponse aux vulnérabilités
- Utiliser des workflows agentiques dans Now Assist pour Réponse aux vulnérabilités

Informations de prise en charge pour Now Assist pour Réponse aux vulnérabilités

Obtenez une vue d'ensemble des informations importantes liées à l'application Now Assist pour Réponse aux vulnérabilités.

Versions prises en charge et applications requises

Les applications suivantes sont requises :

Application	Version
Now Assist pour Réponse aux vulnérabilités	1.0.4
Now Assist pour la plateforme [sn_genai_platform]	9.1.0
Réponse aux vulnérabilités Intégration dans CISA [sn_vul_cisa]	1.5.1

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application	Version
Réponse aux vulnérabilités [sn_vul]	26.2.1
Réponse aux vulnérabilités Gestion des licences et utilisation [sn_vul_licensing] (installé avec [sn_vul])	2.7.1
Réponse aux vulnérabilités Espace de travail commun [sn_vul_cmn_ws] (installé avec [sn_vul])	1.7.0
Cadre de travail d'intégration de Vulnerability Response [sn_vul_int_fw]	1.1.2
Gestion des solutions de vulnérabilité [sn_vul_solution]	10.4.3

Interfaces utilisateur prises en charge

Now Assist pour Réponse aux vulnérabilités inclut les compétences d'IA générative répertoriées dans le tableau suivant.

Interfaces prises en charge par Now Assist pour Réponse aux vulnérabilités

Interface	Fonctionnalités
Espace de travail du gestionnaire de vulnérabilité	Now Assist Compétences: • Déduplication des éléments vulnérables de l'hôte (VIT). • Assistance à la correction qui comprend la fourniture de solutions potentielles privilégiées de fournisseurs tiers. Agents IA : Les gestionnaires de vulnérabilité et les analystes peuvent évaluer si vos éléments de configuration (CI) et vos services d'entreprise sont exposés à des vulnérabilités. Vérifiez toutes les nouvelles vulnérabilités exploitables connues de la CISA (Cybersecurity and Infrastructure Security Agency) et évaluez leur impact potentiel sur votre environnement. Les responsables des vulnérabilités et les analystes peuvent en savoir plus sur vos mesures de conformité afin de comprendre dans quelle mesure votre organisation atteint ses objectifs de correction des vulnérabilités basés sur les accords sur les niveaux de service (SLA).
UI6	Les liens dans les réponses duNow Assist panneau ouvrent de nouveaux onglets dans votre navigateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Now Assist pour Réponse aux vulnérabilités

L'application Now Assist pour Réponse aux vulnérabilités est prise en charge dans le Now Assist panneau et disponible à la demande.

Vue d'ensemble de la configuration

En partageant des données avec le programme de développement de l'IA, vous fournissez des données pertinentes pour aider à améliorer la ServiceNow® précision des prédictions, l'expérience utilisateur, adapter les produits à vos besoins professionnels et réduire les hallucinations pour vos compétences activées Now Assist .

Vous pouvez choisir de refuser le partage de données d'une ServiceNow instance à partir de la Administrateur Now Assist console si vous ne souhaitez pas participer. Pour plus d'informations, consultez Refuser le partage de données pour Now Assist . Répétez le processus d'annulation de l'adhésion pour toutes les instances qui utilisent cette Now Assist fonctionnalité.

Avant la version 1.0.4, utilisez le pour configurer Now Assist pour Réponse aux vulnérabilités.Studio d'agents IA

À partir de la version 1.0.4, utilisez la console pour configurer Now Assist pour Réponse aux vulnérabilités.Administrateur Now Assist Cette console contient tout ce dont vous avez besoin pour installer les applications et configurer les compétences de l'IA générative. Pour en savoir plus, consultez Configuration des Now Assist paramètres et des fonctionnalités .

Le Now Assist panneau doit être activé. Pour plus d'informations, consultez Activer le Now Assist panneau .

- Installer Now Assist modules d'extension .

  Installez l'application Now Assist pour Réponse aux vulnérabilités (sn_vul_ai).

- Configurer et activer une compétence pour Now Assist pour Réponse aux vulnérabilités

  Configurez et examinez les détails d'une compétence dans le Configuration guidée. Vous pouvez activer une compétence à partir du Configuration guidée.

- Activer un workflow agentique pour Now Assist pour Réponse aux vulnérabilités

  Les Now Assist pour Réponse aux vulnérabilités agents IA inclus dans l'application sont activés par défaut. Vous devez activer les workflows agentiques à partir de pour Studio d'agents IA utiliser Now Assist pour Réponse aux vulnérabilités. Consultez Activer un workflow agentique pour Now Assist pour Réponse aux vulnérabilités pour plus d'informations.

  Configurez et activez un workflow agentique à partir du Configuration guidée.

Configurer et activer une compétence pour Now Assist pour Réponse aux vulnérabilités

Configurez et examinez les détails d'une compétence dans le Configuration guidée. Vous pouvez activer une compétence à partir du Configuration guidée.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Administrateur Now Assist** > **Compétences**.
2. Une fois **Technologie** sélectionnée dans le panneau de navigation, sélectionnez **Opérations de sécurité** dans la liste.
   La page Compétences Now Assist pour Security Operations s'affiche. Ces Now Assist pour Réponse aux vulnérabilités compétences sont prises en charge pour Now Assist pour Réponse aux vulnérabilités:
   - Recommander la solution privilégiée pour VIT
   - Déduplication de l'élément vulnérable
3. Sélectionnez **Activer la compétence** pour la compétence souhaitée.
4. Suivez les étapes pour configurer et activer une compétence à l'aide du Configuration guidée.

   Remarque : Certaines compétences ne nécessitent pas toutes les étapes de configuration énumérées ci-dessous. Sélectionnez les seules tâches affichées sur le panneau de gauche et suivez les invites. Une fois que vous avez terminé les tâches, activez la compétence.

5. Sur la page Détails généraux, sélectionnez **Enregistrer et continuer**.
   Cette page est en lecture seule.
6. **Facultatif :** Choisissez l'une des options suivantes pour définir la disponibilité.

Option	Description
La compétence est toujours disponible	La compétence est toujours disponible pour les utilisateurs (par défaut).
Personnaliser la disponibilité des compétences	La compétence n'est disponible que lorsque certaines conditions sont remplies. (Optional) Utilisez le générateur de conditions pour définir vos conditions.

7. Sélectionnez **Enregistrer et continuer**.
8. Définir l'accès.

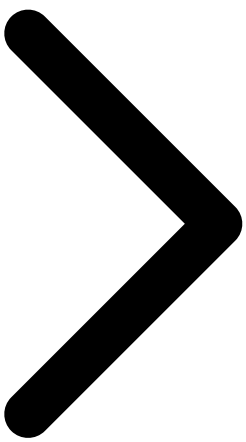
   Remarque :
   - Pour la compétence de déduplication d'élément vulnérable, le rôle sn_vul_ai.run_vi_dedup_job s'affiche. Ce rôle est requis pour exécuter les tâches de déduplication à partir de l'espace de travail.
   - Pour la compétence Recommander la solution préférée pour VIT, le rôle sn_vul_ai.run_suggest_solution s'affiche. Ce rôle est nécessaire pour exécuter la fonctionnalité de solution recommandée pour les éléments vulnérables.
   - Le rôle sn_vul_ai.read_suggest_solution_job est nécessaire pour exécuter la tâche planifiée pour les tâches de rattrapage, afficher la table Tâche de solution recommandée [sn_vul_ai_suggest_solution_job] et afficher l'état d'exécution.

   Vous pouvez modifier ces rôles, mais vous préférez peut-être les conserver comme paramètres par défaut pour cette étape.

9. Sélectionnez **Enregistrer et continuer**.
10. Déterminez où vous souhaitez afficher la compétence et qui peut la consulter dans l'espace de travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Bureau intégré au produit	Now Assist Les compétences sont affichées sur les formulaires et dans les espaces de travail.
Rôles d'utilisateur	Sélectionnez l’icône  de développement) Le rôle de l’étape Définir l’accès s’affiche dans la liste.

11. Sélectionnez **Enregistrer et continuer**.
12. Passez en revue vos choix et sélectionnez **Activer** pour terminer la configuration de la compétence.
13. Sélectionnez **Retourner à Security** Operations pour revenir à la page Compétences Now Assist pour Security Operations.
    Vous êtes maintenant prêt à passer en revue Utilisation pour le Now Assist pour Réponse aux vulnérabilités rattrapage d’éléments vulnérables.

Activer un workflow agentique pour Now Assist pour Réponse aux vulnérabilités

Vous devez activer les workflows agentiques à partir du Studio d’agent IA. Les Now Assist pour Réponse aux vulnérabilités agents IA inclus dans l’application et utilisés dans les workflows agentiques sont activés par défaut.

Avant de commencer

Le Now Assist panneau doit être activé. Consultez Activer le Now Assist panneau pour plus d'informations.

Rôle requis : aia-admin

Procédure

1. Accédez à la **Tous** > **Studio d'agent IA** > **Vue d'ensemble**.
2. Sélectionnez la carte du workflow agentique que vous souhaitez configurer et activer.
   - **Cas d’utilisation Évaluer l’exposition à la vulnérabilité**
   - **Cas d’utilisation : Analyser l’état du rattrapage des vulnérabilités**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous souhaitez modifier ce workflow agentique, vous pouvez le dupliquer , ajuster les paramètres en fonction de vos besoins spécifiques et activer le doublon.

La configuration guidée s'affiche. La page Décrire et connecter est en lecture seule.

3. Sélectionnez **Continuer**.
4. Pour Définir le déclencheur, sélectionnez **Continuer**.

   La page Définir le déclencheur est en lecture seule.
5. Sélectionnez le bouton bascule **Affichage** de la page Sélectionner l'affichage afin que la conversation avec l'agent IA s'affiche dans le Now Assist panneau.
6. Sélectionnez l'icône de flèche pour développer la section.
   Les rôles sn_vul.vulnerability_admin et sn_vul.vulnerability_analyst s'affichent. Ces rôles sont pris en charge pour les workflows agentiques dans l'application Now Assist pour Réponse aux vulnérabilités .
7. Pour activer le workflow agentique, sélectionnez **Enregistrer et tester**.
   Vous pouvez maintenant invoquer les workflows agentiques sur demande.
8. **Facultatif :** Sélectionnez **Cas d'utilisation** (workflow agentique) et saisissez les informations que vous souhaitez tester, puis sélectionnez **Démarrer le test**.

Utilisation pour le Now Assist pour Réponse aux vulnérabilités rattrapage d'éléments vulnérables

Les gestionnaires et les analystes de vulnérabilité peuvent résoudre les tâches de rattrapage à partir de leur flux de travail avec les compétences d'IA générative prises en charge par Now Assist pour Réponse aux vulnérabilités.

Vue d'ensemble des Now Assist pour Réponse aux vulnérabilités compétences

Grâce aux compétences d'IA générative avec Now Assist pour Réponse aux vulnérabilités, vos gestionnaires de vulnérabilités et vos analystes ont la possibilité de :

Identifiez et fermez les éléments vulnérables en double.

Remarque : La déduplication n'est prise en charge que pour les éléments vulnérables de l'hôte (VIT) actifs.

Afficher les solutions de vulnérabilité préférées recommandées pour les éléments vulnérables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Vous devez installer et activer Gestion des solutions pour vulnérabilités [sn_vul_solution] pour importer et afficher les solutions de vulnérabilité préférées et disponibles. Cette application vous fournit des solutions actuelles avec des importations planifiées. Gestion des solutions pour vulnérabilités est disponible sur le .ServiceNow® Store
- Cette compétence d'IA générative ne prend en charge que les éléments vulnérables d'hôte actifs (VIT). Les VIT doivent être **à** l'état **Ouvert, En cours d'examen**, En **attente d'implémentation** ou **En cours de révision** .
- Les solutions actuelles qui traitent le mieux les vulnérabilités, également appelées solutions de priorité maximale, doivent être disponibles pour que vous puissiez les importer auprès de fournisseurs tiers. Consultez la rubrique Gestion des solutions pour vulnérabilités pour plus d'informations sur Gestion des solutions pour vulnérabilités les intégrations prises en charge pour plus d'informations.
- Le champ **Élément de configuration** d'un VIT doit être renseigné avec une valeur de la table Élément de configuration [cmdb_ci].
- Le champ **Vulnérabilité** d'un VIT doit être renseigné.

- Identifier les éléments vulnérables en double avec Now Assist pour Réponse aux vulnérabilités

  Identifiez et regroupez les éléments vulnérables en double (VIT) créés à partir de plusieurs analyseurs. Identifiez l'élément vulnérable primaire et supprimez (fermez) les doublons.

- Suggérer des solutions de vulnérabilité préférées avec Now Assist pour Réponse aux vulnérabilités

  Identifiez la solution privilégiée la plus appropriée pour un élément vulnérable (VIT) donné.

Identifier les éléments vulnérables en double avec Now Assist pour Réponse aux vulnérabilités

Créez ou exécutez une tâche pour identifier les éléments vulnérables primaires (premiers trouvés) pour les éléments de configuration ainsi que les éléments vulnérables en double importés par vos scanners de vulnérabilité.

Avant de commencer

Consultez la rubrique Utilisation pour le Now Assist pour Réponse aux vulnérabilités rattrapage d'éléments vulnérables pour en savoir plus sur les exigences de cette Now Assist compétence. Consultez la section Configurer et activer une compétence pour Now Assist pour Réponse aux vulnérabilités pour plus d'informations sur la façon de l'activer.

Rôles requis :

Remarque : Les sn_vul.vulnerability_admin et sn_vul.vulnerability_analyst héritent des rôles suivants lorsque vous installez l'application Now Assist pour Réponse aux vulnérabilités .

- Afficher le module de déduplication des éléments vulnérables dans l'espace de travail : sn_vul_ai.now_assist_user
- Créer des configurations de tâche de déduplication : sn_vul_ai.configure_vi_dedup
- Exécuter les tâches de déduplication : sn_vul_ai.run_vi_dedup_job
- Examiner les enregistrements de tâches en double : sn_vul_ai.review_duplicate_vi

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sélectionnez Now Assist dans le panneau de navigation.
   Les onglets **Toutes les configurations de tâches**, **Toutes les tâches** et **Toutes les révisions en double** s'affichent sur la Now Assist page. Vous devez créer une tâche de déduplication comme première étape pour la déduplication des éléments vulnérables (VIT).

   Remarque : Vous devez disposer du rôle sn_vul_ai.configure_vi_dedup pour créer des tâches.

3. Pour créer une tâche, sélectionnez **Nouveau** et renseignez les champs.

Champ	Description
Titre	Nom unique pour vous aider à identifier cette tâche parmi d'autres tâches.
Notification par e-mail	Cochez cette case pour recevoir des notifications par e-mail lorsque cette tâche est terminée. Si cette option est sélectionnée, vous pouvez voir les informations suivantes dans un e-mail : ○ Éléments vulnérables en double trouvés ○ Nombre total d'éléments vulnérables traités ○ Éléments de configuration impactés ○ Sélectionnez le lien **Examiner les doublons** pour afficher la liste des doublons dans l'espace de travail. Vous pouvez également sélectionner l'icône Afficher les notifications (cloche) dans la bannière supérieure pour afficher les messages contenant les éléments vulnérables en double trouvés pour les tâches terminées.
Définir les conditions	a. Sélectionnez le lien **Définir les conditions** pour filtrer les éléments vulnérables que vous souhaitez examiner à la recherche de doublons. Un exemple pourrait être : **[Élément de configuration] [contient] [VI-serveur-based]**. Le lien **Définir les conditions** est actualisé et affiche un décompte avec vos résultats correspondants. Vous préférerez peut-être renommer votre tâche en fonction des résultats que vous avez retournés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Vous pouvez sélectionner le lien **Afficher les résultats correspondants** pour afficher les éléments vulnérables qui répondent à vos conditions et plus de détails tels qu'un résumé, des éléments de configuration et des évaluations de risque dans le modal Condition. **b.** Lorsque vous êtes satisfait des résultats, sélectionnez **Enregistrer**.

4. Une fois la tâche enregistrée, le bouton **Exécuter la tâche** s'affiche et est activé sur l'enregistrement.

Vous êtes prêt à exécuter une tâche.

Remarque : Vous devez disposer du rôle sn_vul_ai.run_vi_dedup_job pour afficher le bouton **Exécuter la tâche** et lancer des tâches.

a. Pour exécuter une tâche, accédez à **Tous** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Now Assist** > **Toutes les configurations de tâches**.

b. Localisez la tâche souhaitée, sélectionnez l'enregistrement dans la colonne Numéro pour l'ouvrir, puis sélectionnez **Exécuter la tâche**.
Un message indiquant que la tâche est en cours d'exécution en arrière-plan s'affiche. Pour plus d'informations sur l'état de votre tâche, sélectionnez le lien **Afficher la progression** .

Une fois que vous avez sélectionné la tâche Exécuter, la tâche d'achèvement de la tâche de déduplication Vérifier l'élément vulnérable est lancée et s'exécute en arrière-plan.

Il existe une autre tâche qui s'exécute toutes les 30 minutes pour vérifier que les tâches actives ont été effectuées.

Une fois votre tâche terminée, vous pouvez examiner, évaluer et fermer les VIT en double trouvés par votre tâche.

Remarque : Vous devez disposer du rôle sn_vul_ai.review_duplicate_vi pour examiner les VIT en double.

5. Examinez les VIT en double.

a. Pour passer en revue les tâches terminées et les listes des éléments vulnérables en double, accédez à **Tous** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Now Assist** > **Toutes les tâches**.

b. Ouvrez un enregistrement (**JOB#**) et sélectionnez la liste connexe **Revues des éléments vulnérables en double** .

c. Facultatif : Sélectionnez les liens pour ouvrir les enregistrements d'éléments vulnérables (**VIT#**) pour examen avant de déterminer si les VIT sur l'enregistrement sont des doublons.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Pour une comparaison côte à côte des enregistrements VIT en double, sélectionnez un enregistrement (**DUP#**) pour l'ouvrir.

- Le numéro et l'état de la tâche (**Requiert une revue**) s'affichent.
- Les champs Confiance et Motif vous fournissent plus d'informations. La colonne Motif affiche le raisonnement de l'IA générative et du service Now LLM expliquant pourquoi ces VIT sont considérés comme des doublons.
- Les informations sur le VIT principal et le VIT en double sont côte à côte dans la section Détails de l'élément vulnérable.
- Date de premier résultat pour le VIT primaire et les doublons. Un VIT principal comporte généralement la date de premier résultat la plus ancienne.
- Sélectionnez l'icône ⓘ minuscule dans les champs Détails de l'élément vulnérable primaire et Doublons si vous souhaitez ouvrir les enregistrements VIT à partir de cette page.

e. Choisissez-en un.

Option	Description
Marquer comme non dupliqué	Il s'agit de deux éléments vulnérables distincts qui représentent au moins deux vulnérabilités uniques. Ces deux éléments vulnérables ne seront pas considérés comme des doublons dans les tâches que vous créerez à l'avenir. L'état passe de **Requiert une revue** à**Non dupliqué** pour l'enregistrement **DUP#** .
Confirmer un doublon	Votre avis indique que ces deux VIT sont des doublons. L'enregistrement VIT qui s'affiche sur l'enregistrement Dupliqué intitulé Dupliquer passe à **Fermé**. Une note de travail avec des notes de fermeture est ajoutée à l'enregistrement VIT fermé. Toutes les détections associées sur le VIT fermé sont déplacées vers l'enregistrement VIT principal. Des notes de travail sont ajoutées au VIT principal pour indiquer qu'un doublon a été fermé et que ses détections ont été liées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : La propriété système sn_vul_ai.duplicate_vi_confidence_threshold automatise le workflow de déduplication des éléments vulnérables. Cette propriété système est activée par défaut, mais elle n'a pas de valeur de seuil pour un score de confiance. En l'absence de valeur pour le seuil, le workflow automatisé ne ferme aucun doublon. **Remarque :** Les scores de confiance de 100 pour les VIT ne sont pas calculés par la Now Assist compétence. Ce score est calculé par correspondance avec une logique déterministe. Si vous saisissez une valeur de seuil, tous les doublons dont le score de confiance est supérieur à la valeur que vous spécifiez sont automatiquement fermés et leurs détections sont déployées sur l'élément vulnérable primaire. Vous préférez peut-être laisser cette propriété système dans son paramètre par défaut sans valeur de seuil jusqu'à ce que vous soyez familiarisé avec le workflow et que vous ayez le temps d'établir une valeur précise. Dans son paramètre par défaut, vous pouvez garder le contrôle sur les conditions dans lesquelles vos VIT en double sont examinés, marqués et traités. Vous devez disposer du rôle sn_vul_ai.configure_vi_dedup ou sn_vul_ai.review_duplicate_vi pour modifier cette propriété système.

f. Facultatif : Vous pouvez également examiner les éléments en double à partir de l'onglet de liste **Toutes les révisions en double** à partir d'un enregistrement **DUP#** .
Cette liste vous permet d'effectuer une modification en bloc des enregistrements dupliqués et de leurs enregistrements VIT associés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suggérer des solutions de vulnérabilité préférées avec Now Assist pour Réponse aux vulnérabilités

Utilisez le raisonnement de l'IA générative avec Now Assist pour Réponse aux vulnérabilités (Now Assist avec la réalité virtuelle) pour aider vos analystes à trouver des solutions privilégiées potentielles auprès de fournisseurs tiers pour les vulnérabilités de vos actifs.

Avant de commencer

Consultez la rubrique Utilisation pour le Now Assist pour Réponse aux vulnérabilités rattrapage d'éléments vulnérables pour en savoir plus sur les exigences de cette Now Assist compétence. Consultez la section Configurer et activer une compétence pour Now Assist pour Réponse aux vulnérabilités pour plus d'informations sur la façon de l'activer.

Rôles requis :

Remarque : Les sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst et sn_vul.remediation_owner héritent des rôles suivants lorsque vous installez l'application Now Assist pour Réponse aux vulnérabilités .

- sn_vul_ai.run_suggest_solution : nécessaire pour exécuter la fonctionnalité de solution recommandée sur les éléments vulnérables.
- sn_vul_ai.read_suggest_solution_job : nécessaire pour exécuter la tâche planifiée pour les tâches de rattrapage, afficher la table Recommander la tâche de solution [sn_vul_ai_suggest_solution_job] et l'état d'exécution.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Ouvrez un enregistrement d'élément vulnérable de l'hôte (VIT) et sélectionnez l'onglet **Détails** .
3. À utiliser Now Assist avec le raisonnement VR pour trouver les solutions qui correspondent le mieux à vos vulnérabilités, sélectionnez **Recommander une solution**.
4. Vous pouvez également ouvrir une tâche de rattrapage (RT) qui vous est affectée et sélectionner **Recommander une solution**.

   Les tableaux suivants décrivent les messages et les notifications qui s'affichent et où les données sont renseignées une fois que vous avez sélectionné **Recommander une solution** sur les enregistrements de tâches VIT et de rattrapage.

   Remarque : Now Assist avec la RV ne génère pas de solutions de vulnérabilité. Les solutions sont importées d'intégrations tierces. Pour que le bouton **Recommander une solution** s'affiche sur les enregistrements de VIT et de tâche de rattrapage, il doit y avoir au moins une solution de la plus haute priorité disponible pour la vulnérabilité associée à ce VIT.

Enregistrements d'éléments vulnérables (VIT)

Message ou notification	Description
Une solution potentielle a été trouvée par Now Assist for VR pour vous aider à corriger cette vulnérabilité. Pour plus d'informations, consultez la section Rattrapage et le flux d'activité de l'onglet Détails.	Les informations sur une solution privilégiée sont renseignées dans l'onglet Détails d'un VIT dans les champs Solution préférée et Résumé de la section Correction. Les notes de travail sont saisies dans le flux d'activité. Assurez-vous de vérifier l'exactitude des solutions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Message ou notification	Description
	Remarque : Si un VIT a une solution fournie par Now Assist pour la réalité virtuelle, la solution peut changer si vous importez plus de solutions et réexécutez la tâche (sélectionner **Recommander une solution**).
Une solution à cette vulnérabilité a été trouvée à l'aide de Now Assist pour VR sur la base du raisonnement suivant.	Détails dans le flux d'activité sur les VIT sur les raisons pour lesquelles cette solution a été déterminée par Now Assist la RV comme solution privilégiée. Le raisonnement n'est affiché que sur les VIT. Les solutions préférées trouvées par la compétence sont déployées dans l'onglet Solutions sur les tâches de rattrapage. Assurez-vous de vérifier l'exactitude des solutions.
Aucune solution n'a été trouvée. Pour plus d'informations, consultez la section Rattrapage et le flux d'activité de l'onglet Détails.	Résumé dans le flux d'activité de l'onglet Détails sur les VIT expliquant pourquoi aucune solution n'a été trouvée. Le raisonnement n'est affiché que sur les VIT.

Enregistrements de tâches de rattrapage (RT)

Message ou notification	Description
Utilisez Now Assist pour VR pour vous aider à trouver des solutions privilégiées potentielles pour les éléments vulnérables de cette tâche de rattrapage. Vos performances peuvent être affectées si la tâche de rattrapage comporte un grand nombre de VIT.	○ Le RT doit avoir au moins un VIT. La valeur par défaut pour le nombre maximum de VIT sur un RT est de 1 000. Vous préférez peut-être conserver cette valeur dans son paramètre par défaut. **Remarque :** Vous pouvez modifier la valeur maximale avec la propriété système sn_vul_ai.max_vits_allowed_for_suggest_solution. ○ Passe en revue tous les VIT dans la tâche de rattrapage, mais les solutions ne sont recommandées que pour les VIT dans la tâche de rattrapage qui sont dans des états actifs, qui ont des solutions de la plus haute priorité et qui n'ont pas encore de solution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Message ou notification	Description
	Remarque : Si vous réexécutez la tâche (sélectionner **Recommander une solution**) pour une tâche de rattrapage, par défaut, la tâche évalue uniquement les VIT sans solution (vrai). Pour évaluer les VIT avec des solutions, vous devez modifier la propriété système sn_vul_ai.exclude_vits_with_solution sur false. ○ Fournit un résumé de la solution préférée dans le flux d'activité dans l'onglet Détails de la tâche de rattrapage. ○ Les solutions préférées trouvées par la compétence sont déployées dans l'onglet Solutions sur les tâches de rattrapage. ○ Répète les informations de solution pour faire correspondre les VIT dans la tâche de rattrapage. Les informations sur la solution sont renseignées dans les champs Solution privilégiée et Résumé, ainsi que dans le flux d'activité des onglets Détails. ○ Si une tâche en arrière-plan est en cours et évalue des solutions pour cet enregistrement, le bouton **Recommander une solution** n'est pas visible sur la tâche de rattrapage. Vous pouvez afficher le bouton une fois la tâche terminée. Assurez-vous de vérifier l'exactitude des solutions.
Rassemble actuellement des solutions pour les VIT. Sélectionnez ce lien pour suivre la progression.	Consultez l'état de la tâche et un résumé comprenant les informations suivantes : ○ Nombre total de VIT dans la tâche de rattrapage : n ○ Nombre de VIT traités : n ○ VIT avec solutions : n VIT S'il n'y a pas assez d'informations pour suggérer une solution en toute confiance, aucune solution n'est fournie pour les VIT. Le résumé est également fourni dans le flux d'activité une fois la tâche terminée.
Des solutions ne sont pas fournies aux VIT s'il n'y a pas suffisamment d'informations pour suggérer une solution en toute confiance.	Des solutions n'ont pas été trouvées pour certains VIT, car il n'y a pas assez d'informations ou aucune

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Message ou notification	Description
	solution de la plus haute importance n’a été fournie Now Assist pour déterminer une solution. ○ Les champs Solution privilégiée et Résumé restent vides sur le VIT. ○ Les notes de travail sont saisies dans le flux d’activité de la tâche VIT et de rattrapage. ○ Le raisonnement n’est affiché que sur les VIT.

Utiliser des workflows agentiques dans Now Assist pour Réponse aux vulnérabilités

Utilisez les Réponse aux vulnérabilités agents IA pour accomplir vos tâches de manière autonome.

Workflows agentiques disponibles pour AI Agents pour Réponse aux vulnérabilités

Nom du workflow agentique	Description	Agents IA disponibles
Évaluer l'exposition à la vulnérabilité	• Déterminez si vos éléments de configuration (CI) et vos services d’entreprise sont exposés à des vulnérabilités connues. • Déterminez l’impact potentiel qu’une vulnérabilité spécifique peut avoir sur l’ensemble de votre environnement. • Vérifiez si les CI présentent de nouvelles vulnérabilités exploitables (zero-day) par la Cybersecurity and Infrastructure Security Agency (CISA). • Créez des rubriques de visualisation dans l’espace de travail du gestionnaire de vulnérabilité pour corriger les éléments vulnérables.	• Agent IA de l'analyse de vulnérabilité CISA • Agent IA de l'analyse de l'exposition à la vulnérabilité • Agent IA de création de rubrique de surveillance
Analyser le statut de remédiation des vulnérabilités	• Obtenez un aperçu de vos mesures et statistiques de conformité pour savoir dans quelle mesure vous respectez les dates	Agent IA de l'analyse de conformité du rattrapage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflows agentiques disponibles pour AI Agents pour Réponse aux vulnérabilités (suite)

Nom du workflow agentique	Description	Agents IA disponibles
	cibles de rattrapage sur les enregistrements d'éléments vulnérables (VIT). • Affichez les totaux de rattrapage de vos enregistrements VIT mensuels et identifiez les cibles manquées. • Répartissez les données de rattrapage sur les VIT par **gravité**, **groupe d'affectation**, **élément de configuration** et **vulnérabilité** pour vos examens mensuels de conformité à l'accord sur les niveaux de service (SLA).	

Important : Par défaut, tous les workflows agentiques et les enregistrements d'agent IA sont en lecture seule.

Pour modifier un workflow agentique, vous devez d'abord Dupliquer un workflow agentique , puis procéder aux étapes suivantes :

- Activez le workflow agentique. Les Now Assist pour Réponse aux vulnérabilités agents IA inclus dans l'application sont activés par défaut.
- Si nécessaire, vous pouvez ajouter un déclencheur pour appeler automatiquement le workflow agentique.

Vous recherchez un agent IA ?

- Il peut y avoir des agents IA installés avec l'application qui ne sont pas utilisés dans les Now Assist workflows agentiques. Pour savoir comment afficher tous les agents disponibles sur votre instance, consultez Rechercher des agents IA .
- Pour rechercher des agents qui ne peuvent pas être installés sur votre instance, visitez AI Agent Marketplace sur le ServiceNow Store.

- Évaluer l'exposition à la vulnérabilité workflow agentique.

  Discutez avec un agent IA à partir du Now Assist panneau pour vous aider à évaluer si vos éléments de configuration et vos services d'entreprise sont exposés à des vulnérabilités.

- Analyser le workflow agentique d'état du rattrapage de vulnérabilité.

  Discutez avec un agent IA à partir du Now Assist panneau pour vous aider à mieux comprendre vos mesures de conformité pour résoudre les éléments vulnérables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluer l'exposition à la vulnérabilité workflow agentique

Discutez avec un agent IA à partir du Now Assist panneau pour vous aider à évaluer l'exposition potentielle de vos éléments de configuration et de vos services d'entreprise aux vulnérabilités.

Avant de commencer

Le Now Assist panneau doit être activé. Pour plus d'informations, consultez Activer le Now Assist panneau .

Rôles requis : sn_vul.vulnerability_admin ou sn_vul.vulnerability_analyst

Procédure

1. Sélectionnez l'icône ( ) n'importe Now Assist où dans votre instance.
   Le Now Assist panneau s'affiche.

   Le workflow agentique Évaluer l'exposition des vulnérabilités est disponible à la demande. Vous pouvez entrer n'importe quelle requête en langage naturel, mais vous pouvez envisager d'utiliser les invites décrites dans le tableau suivant et les étapes pour commencer pour vous familiariser avec les données de vulnérabilité disponibles et ce que vous pouvez en faire. Les étapes suivantes vous montrent comment demander des données de vulnérabilité actuelles, créer une rubrique de visualisation basée sur les résultats retournés et déterminer l'impact global qu'une vulnérabilité peut avoir sur votre environnement.

Votre demande ou réponse	Description
Quelles sont les vulnérabilités récentes de CISA ?	**Récent** dans votre question fait référence aux nouvelles vulnérabilités qui sont apparues au cours des sept derniers jours. Sept jours (une semaine) est la période par défaut pour le workflow agentique. Si vous souhaitez rechercher de nouvelles vulnérabilités pour une période spécifique autre que sept jours, tapez une demande avec une valeur qui se produit dans le passé, par exemple Quelles **sont les vulnérabilités récentes pour les 30 derniers jours ?**
Oui, créer une rubrique de surveillance pour la vulnérabilité CVE-2018-9065.	Lorsqu'on vous demande si vous souhaitez créer une rubrique de visualisation, vous préférerez peut-être être précis dans votre réponse. Par exemple, confirmez la demande et saisissez une vulnérabilité spécifique au format : **CVE-2018-9065**.
Pouvez-vous me fournir une analyse d'impact détaillée de la vulnérabilité CVE-2018-9065 ?	L'analyse de l'impact potentiel des vulnérabilités n'est prise en charge que pour les services aux entreprises et les classes d'éléments de configuration affectés.
Affichez les résultats de la question précédente.	Demandez à l'agent de revoir votre question précédente si elle ne vous donne pas de réponse.
Terminez la session ou **arrêtez-vous**.	Mettez fin à la conversation.

Votre conversation est enregistrée jusqu'à ce que vous démarriez une nouvelle messagerie instantanée. Si la conversation se termine de manière inattendue, démarrez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

une nouvelle messagerie instantanée. Pour lancer une nouvelle messagerie instantanée, sélectionnez l'icône Nouvelle messagerie (+).

2. Saisissez une demande en langage naturel pour voir si vous êtes exposé à des vulnérabilités récentes, par exemple, **Quelles sont les vulnérabilités CISA récentes ?**

   Étant donné que votre entrée ne spécifie pas de plage, l'agent rassemble par défaut les données de vulnérabilité exploitables de la CISA (Cybersecurity and Infrastructure Security Agency) sur vos actifs et renvoie les informations des sept derniers jours.

   Les vulnérabilités et expositions courantes (CVE) qui ont un impact sur vos actifs et auxquelles des éléments vulnérables sont associés dans votre environnement sont répertoriées.

   Vous pouvez voir que l'agent renvoie également des alias qui correspondent aux CVE. Les alias sont signalés si vous utilisez des scanners tiers pour importer vos données de vulnérabilité. Par exemple, CVE-2018-8627 (alias : TEN-119686, TEN-119596) de gravité moyenne comporte 4 éléments vulnérables (VIT). Cette réponse indique que la vulnérabilité a été détectée et importée par le produit de scanner Tenable (TEN).

3. **Facultatif :** Sélectionnez le lien CISA Known Exploitable Vulnerabilities pour obtenir des informations sur toutes les CVE qui ont été renvoyées.
   La liste s'ouvre dans un nouvel onglet dans UI16.

4. Revenez à la messagerie instantanée et demandez à l'agent de créer une rubrique de surveillance pour un CVE à l'invite, par exemple, **Oui, créer une rubrique de surveillance pour la vulnérabilité CVE-2018-9065.**
   L'agent propose un nom pour votre rubrique de surveillance et demande confirmation. Vous pouvez modifier le nom.

5. Entrez **OK**.

6. Sélectionnez le lien pour afficher la rubrique de surveillance dans l'espace de travail du gestionnaire de vulnérabilité et afficher plus de détails ainsi que les éléments vulnérables associés aux CVE.
   La liste s'ouvre dans un nouvel onglet dans UI16. Après avoir examiné les données, vous pouvez décider de vouloir plus d'informations sur l'impact des CVE sur vos autres actifs.

7. Revenez au Now Assist panneau et saisissez et demandez à l'agent une analyse d'impact détaillée, par exemple, **Pouvez-vous me fournir une analyse d'impact détaillée pour la vulnérabilité CVE-2018-9065 ?**
   Cette demande renvoie des informations sur vos éléments de configuration et les services aux entreprises qui sont affectés par cette CVE. Il fournit une répartition de criticité, une liste des services aux entreprises impactés et une liste des classes d'éléments de configuration affectés. Il y a aussi un lien pour des informations plus détaillées.

8. **Facultatif :** Demandez une évaluation globale de l'exposition à la vulnérabilité pour un service d'entreprise spécifique.
   Les informations sur le service d'entreprise comprennent les éléments vulnérables associés, la criticité (risque) et les éléments de configuration par classe sont répertoriés.

Analyser le workflow agentique d'état du rattrapage de vulnérabilité

Discutez avec un agent IA à partir du Now Assist panneau pour vous aider à obtenir des informations sur vos mesures mensuelles de conformité du rattrapage pour les éléments vulnérables.

Avant de commencer

Le Now Assist panneau doit être activé. Pour plus d'informations, consultez Activer le Now Assist panneau .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles requis : administrateur sn_vul.vulnerability_admin ou sn_vul.vulnerability_analyst

Procédure

1. Sélectionnez l'icône Now Assist ( ).
   Le Now Assist panneau s'affiche.

   Le workflow agentique Analyser l'état du rattrapage de vulnérabilité est disponible sur demande. Vous pouvez entrer n'importe quelle requête en langage naturel, mais vous pouvez envisager d'utiliser les invites décrites dans le tableau et les étapes suivants pour vous familiariser avec les données disponibles et ce que vous pouvez en faire.

   Ces étapes vous donnent un aperçu de vos mesures de conformité concernant la façon dont vos équipes respectent leurs dates cibles mensuelles de rattrapage pour les enregistrements d'éléments vulnérables, telles qu'indiquées dans votre accord sur les niveaux de service (SLA).

Votre demande ou réponse	Description
Quelle est ma conformité pour le rattrapage pour le mois d'octobre 2024 ?	Par défaut, la recherche est basée sur le groupe d'affectation. Si vous ne spécifiez pas de mois, l'agent IA recherche le mois en cours, puis commence à remonter dans le temps, un mois à la fois. Vous pouvez également demander à l'agent une répartition par classe d'élément de configuration ou vulnérabilité. Par exemple, tapez **Quelle est ma conformité pour le mois d'octobre 2024 pour les serveurs Windows ?**
Quels types d'actifs ont représenté le plus grand nombre de SLA manqués ?	Les résultats sont organisés en fonction des données du mois de votre demande d'origine par type d'actif.
Quel groupe d'affectation a eu le moins de SLA critiques manqués ?	Obtenez le groupe d'affectation qui avait le plus ou le moins de SLA manqués en fonction de la gravité de l'élément vulnérable (VIT) : Critique, Élevée, Moyenne et Faible. En outre, vous pouvez demander à l'agent IA de rechercher les SLA manqués par catégorie de VIT.
Affichez les résultats de la question précédente.	Demandez à l'agent de revoir votre question précédente si elle ne vous donne pas de réponse.
Terminez la session ou **arrêtez-vous**.	Mettez fin à la conversation.

   Votre conversation est enregistrée jusqu'à ce que vous démarriez une nouvelle messagerie instantanée. Si la conversation se termine de manière inattendue, démarrez une nouvelle messagerie instantanée. Pour démarrer une nouvelle messagerie instantanée, sélectionnez l'icône Nouvelle messagerie ( ).

2. Saisissez une demande en langage naturel pour afficher vos mesures de rattrapage pour un mois et une année donnés, par exemple, Quelle est ma conformité pour le rattrapage pour le mois d'octobre 2024 ?

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les résultats sont organisés en sections.

- Résumé : nombre total d'enregistrements ayant des cibles de rattrapage de SLA pour le mois et l'année que vous avez demandés, ainsi que les totaux en pourcentage pour les dates cibles manquées ou atteintes.
- Répartition par gravité : les éléments vulnérables qui n'ont pas atteint les cibles de rattrapage sont répartis par gravité critique, élevée, moyenne et faible.
- Répartition par groupes d'affectation : pourcentage du total des enregistrements avec des cibles manquées, répartis par groupes d'affectation.
- Pour plus d'informations : Lien Conformité à la remédiation pour octobre 2024 - Afficher plus d'informations sur les données. Un nouvel onglet s'ouvre dans UI16.

3. Vous pouvez demander des informations plus spécifiques sur les SLA manqués, par exemple, `Quels types d'actifs ont représenté le plus grand nombre de SLA manqués ?`
   Les résultats sont organisés pour les données du mois de votre demande d'origine par type d'actif, par exemple, Windows Server, Base de données, Serveur Linux, et ainsi de suite.
4. Vous pouvez demander des informations plus spécifiques sur la productivité de vos équipes au cours de ce mois, par exemple : `Quel groupe d'affectation a eu le moins de SLA critiques manqués ?`
   Le groupe d'affectation est retourné qui avait le moins de VIT critiques pour lesquels le SLA a manqué.
5. Vous pouvez comparer ces résultats à un autre mois, par exemple, `Comment ces données se comparent-elles à celles de novembre 2024 ?`
   Les résultats sont organisés en sections.
   - Résumé de la comparaison : nombre total d'enregistrements ayant des cibles de rattrapage de SLA pour la période que vous avez demandée pour la première fois (**octobre 2024**) par rapport à votre dernière demande (**novembre 2024**).
   - Répartition par gravité : les éléments vulnérables qui ont manqué les cibles de rattrapage sont répartis par gravité : critique, élevée, moyenne et faible.
   - Observations : analyse des données et aperçu des tendances des données sur la base de la comparaison.
   - Pour plus d'informations : Lien Conformité au rattrapage pour novembre 2024 - Afficher plus d'informations sur les données utilisées pour la comparaison. Un nouvel onglet s'ouvre dans UI16.

Now Assist pour Réponse aux vulnérabilités Informations de référence

Outils, agents et informations de collecte d'agents IA pour Now Assist pour Réponse aux vulnérabilités.

Références

Affichez les vues d'ensemble des workflows agentiques suivants.

- Réponse aux vulnérabilités Collection d'agents IA pour le workflow agentique Évaluer l'exposition à la vulnérabilité
- Réponse aux vulnérabilités Collection d'agents IA pour le workflow agentique Analyser l'état du rattrapage de vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités Collection d'agents IA pour le workflow agentique Évaluer l'exposition à la vulnérabilité

Les outils et les agents IA pour le workflow agentique Évaluer l'exposition des vulnérabilités.

Vue d'ensemble du workflow agentique

Les workflows agentiques suivants sont inclus dans l'application Now Assist pour Réponse aux vulnérabilités :

- Évaluer l'exposition à la vulnérabilité workflow agentique
- Analyser le workflow d'état du rattrapage de vulnérabilité

Si vous souhaitez modifier ce workflow agentique, vous pouvez le dupliquer , ajuster les paramètres en fonction de vos besoins spécifiques et activer la version dupliquée du workflow agentique.

Évaluer l'exposition à la vulnérabilité workflow agentique Vue d'ensemble du workflow agentique

Utilisez le workflow agentique Évaluer l'exposition à la vulnérabilité du Now Assist panneau pour vous aider à :

- Déterminez si vos éléments de configuration (CI) et vos services d'entreprise sont exposés à des vulnérabilités connues.
- Déterminez l'impact potentiel qu'une vulnérabilité spécifique peut avoir sur l'ensemble de votre environnement.
- Vérifiez si les CI présentent de nouvelles vulnérabilités exploitables (zero-day) par la Cybersecurity and Infrastructure Security Agency (CISA).
- Créez des rubriques de visualisation dans l'espace de travail du gestionnaire de vulnérabilité pour corriger les éléments vulnérables.
- Ajustez le contenu en langage naturel.

Agents utilisés dans le workflow agentique Évaluer l'exposition de la vulnérabilité

- Exécuteur d'action de Vulnerability Response
- Analyseur de vulnérabilités exploitées connues CISA
- Conseiller en évaluation de l'exposition aux vulnérabilités

Réponse aux vulnérabilités Collection d'agents IA pour le workflow agentique Analyser l'état du rattrapage de vulnérabilité

Les outils et les agents IA pour le workflow agentique Analyser l'état du rattrapage des vulnérabilités.

Analyser l'état du rattrapage de vulnérabilité Vue d'ensemble du workflow agentique

Utilisez le workflow agentique Analyser l'état du rattrapage des vulnérabilités du Now Assist panneau pour vous aider à :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Obtenez un aperçu de vos mesures et statistiques de conformité pour savoir dans quelle mesure vous respectez les dates cibles de rattrapage sur les enregistrements d'éléments vulnérables (VIT).
- Affichez les totaux de rattrapage de vos enregistrements VIT mensuels et identifiez les cibles manquées.
- Répartissez les données de rattrapage sur les VIT par **gravité**, **groupe d'affectation**, **élément de configuration** et **vulnérabilité** pour vos examens mensuels de conformité à l'accord sur les niveaux de service (SLA).

Si vous souhaitez modifier ce workflow agentique, vous pouvez le dupliquer , ajuster les paramètres en fonction de vos besoins spécifiques et activer la version dupliquée du workflow agentique.

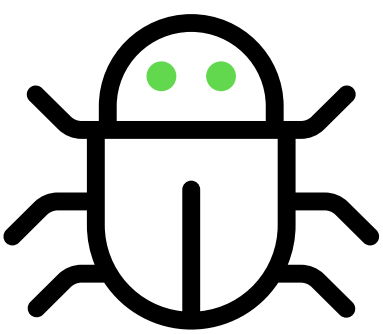
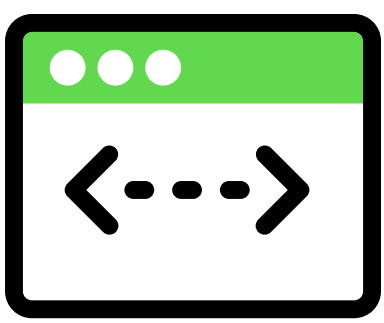
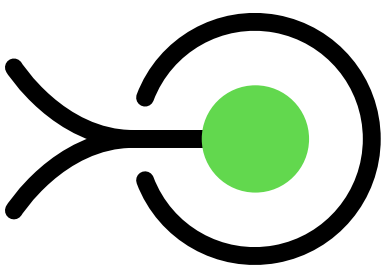
Agent utilisé dans le workflow agentique Analyser l'état du rattrapage de vulnérabilité

Le fournisseur d'aperçus de conformité du rattrapage est utilisé par le workflow agentique Analyser l'état du rattrapage de vulnérabilité.

Applications de gestion de la surface d'attaque

Les Réponse aux vulnérabilités applications et autres qui composent la gestion de la surface d'attaque vous aident à hiérarchiser vos actifs vulnérables et à ajouter du contexte pour vous aider à déterminer quand les systèmes critiques de l'entreprise sont menacés. Grâce à la CMDB, vos équipes de sécurité peuvent également identifier facilement les dépendances entre les systèmes et évaluer rapidement l'impact des changements ou des temps d'arrêt sur l'entreprise.

Réponse aux vulnérabilités applications

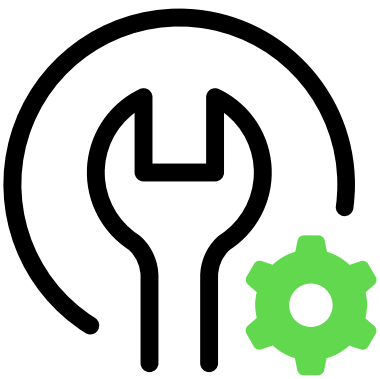
Réponse aux vulnérabilités	Réponse aux vulnérabilités de l'application	Réponse aux vulnérabilités du conteneur
		
En savoir plus sur l'application Vulnerability Response	En savoir plus sur l'application Application Vulnerability Response	En savoir plus sur l'application Container Vulnerability Response

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités applications (suite)

Configuration Compliance



En savoir plus sur l’application Configuration Compliance

Nomenclature logicielle



En savoir plus sur les applications de nomenclature logicielle

Réponse aux vulnérabilités Espaces de travail

Espace de travail du gestionnaire de vulnérabilité



En savoir plus sur l’espace de travail du gestionnaire de vulnérabilité

Espace de travail de remédiation informatique



En savoir plus sur l’espace de travail de remédiation informatique

Espace de travail de l'évaluation de la vulnérabilité



En savoir plus sur l’espace de travail Évaluation de la vulnérabilité

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations

Traduction automatique

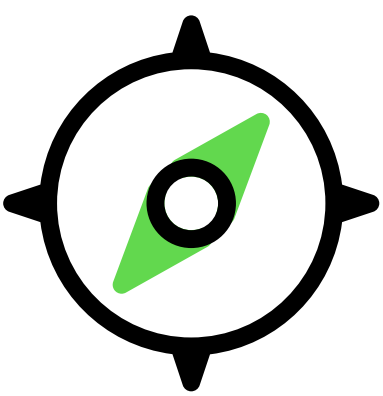
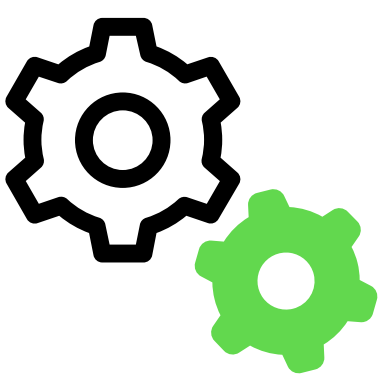
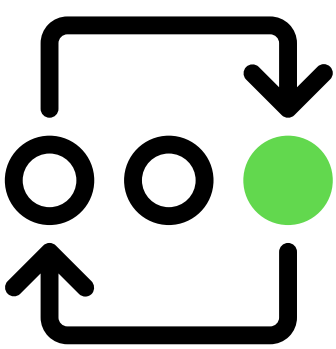
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Réponse aux vulnérabilités

La base de données de vulnérabilité nationale (NVD) et d'autres sources collectent des informations sur les vulnérabilités connues. Ces vulnérabilités peuvent inclure des faiblesses dans les logiciels, les systèmes d'exploitation que les logiciels malveillants peuvent exploiter et d'autres attaques. L'application ServiceNow® Réponse aux vulnérabilités vous aide à suivre, classer par ordre de priorité et résoudre ces vulnérabilités.

Réponse aux vulnérabilités

Explorer	Mettre en place et configurer	Intégrer
		
En savoir plus sur les fonctionnalités de Vulnerability Response	Installez et configurez votre application Vulnerability Response	Étendre Vulnerability Response en l'intégrant à d'autres applications

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

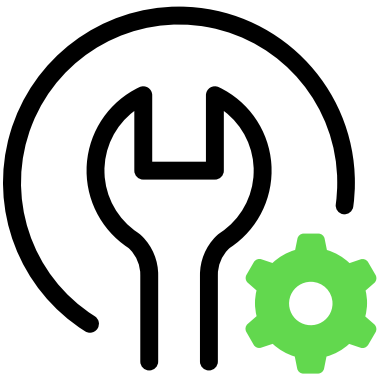
Réponse aux vulnérabilités (suite)

Utiliser les espaces de travail Vulnerability Response



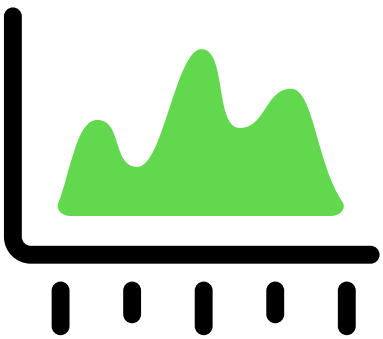
Découvrez comment surveiller, gérer et corriger les VIT dans les espaces de travail Gestionnaire des vulnérabilités, Rattrapage informatique et Évaluation de la vulnérabilité.

Corriger



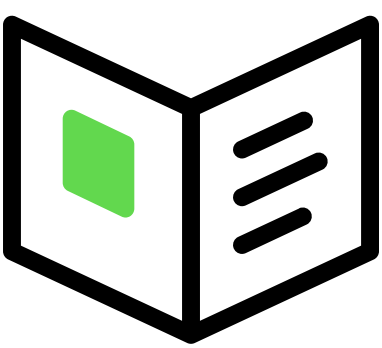
Utilisez les fonctionnalités de Vulnerability Response pour corriger vos vulnérabilités et protéger vos actifs

Analyses et rapports



Surveiller la progression du rattrapage

Référence



Obtenez plus de détails sur les notes de version, les composants et les informations de référence de Vulnerability Response sur les champs, les tables et les propriétés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Explorer l'application Réponse aux vulnérabilités

L'application ServiceNow® Réponse aux vulnérabilités importe et regroupe automatiquement les éléments vulnérables selon des règles qui vous permettent de corriger rapidement les vulnérabilités. Les données de vulnérabilité sont extraites de sources externes, telles que la base de données de vulnérabilité nationale (NVD) et des intégrations tierces, et traitées avec des applications développées par ServiceNow®.

Regardez une vue d'ensemble de Vulnerability Response qui définit les éléments vulnérables, les tâches de rattrapage et leurs cycles de vie.

Vue d'ensemble de la réponse aux vulnérabilités classique au sein d'une entreprise par rapport à la réponse aux vulnérabilités avec ServiceNow, et définit les éléments vulnérables, les groupes de vulnérabilité et leurs cycles de vie.

Réponse aux vulnérabilités et votre environnement d'entreprise

En règle générale, dans un environnement d'entreprise, les organisations utilisent des scanners de vulnérabilité et des outils d'évaluation pour identifier et gérer les risques que les vulnérabilités font peser sur leurs actifs. Les vulnérabilités identifiées par ces outils se traduisent par des risques pour les équipes de sécurité et informatiques responsables de la maintenance et de la sécurisation des actifs d'une organisation. Certains risques peuvent inclure, sans s'y limiter, les types de vulnérabilités identifiés suivants :

- Dépendance à des logiciels obsolètes ou à des systèmes mal configurés
- Protocoles réseau non sécurisés
- Dépendance à l'égard de bibliothèques logicielles tierces défectueuses
- Hygiène de l'administration système médiocre ou incohérente
- Images système de base de référence qui ne sont pas renforcées

À mesure que ces risques potentiels sont exposés, les équipes de sécurité et informatiques sont généralement confrontées à des défis dans le traitement et la gestion du volume d'informations sur les vulnérabilités générées par leurs outils d'analyse et d'évaluation. Plus précisément, ces équipes se retrouvent dépassées lorsqu'elles gèrent un volume élevé de vulnérabilités identifiées et élaborent des efforts de réponse exploitables pour atténuer les risques potentiels auxquels leurs organisations sont confrontées.

Vous pouvez identifier ces défis pour votre propre posture de sécurité en vous posant les questions suivantes :

- Quelles vulnérabilités identifiées doivent être examinées en premier ?
- Que signifient ces vulnérabilités identifiées pour notre organisation ?
- Qui doit être responsable des risques identifiés et s'approprier ?
- Qui devrait mettre la main à la pâte pour résoudre/atténuer ces risques ?

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Comment atténuer efficacement les vulnérabilités identifiées avec les ressources dont nous disposons ?
- Quels sont les résultats inattendus potentiels de la réduction des vulnérabilités identifiées ?
- Quel processus suivons-nous pour corriger les vulnérabilités, suivre les mesures que nous avons prises et assurer un suivi pour nous assurer que nos actions ont fonctionné ?
- Comment savoir si nous faisons des progrès dans la réduction de notre position globale vis-à-vis du risque ?

Réponse aux vulnérabilités et Opérations de sécurité le ServiceNow AI Platform®

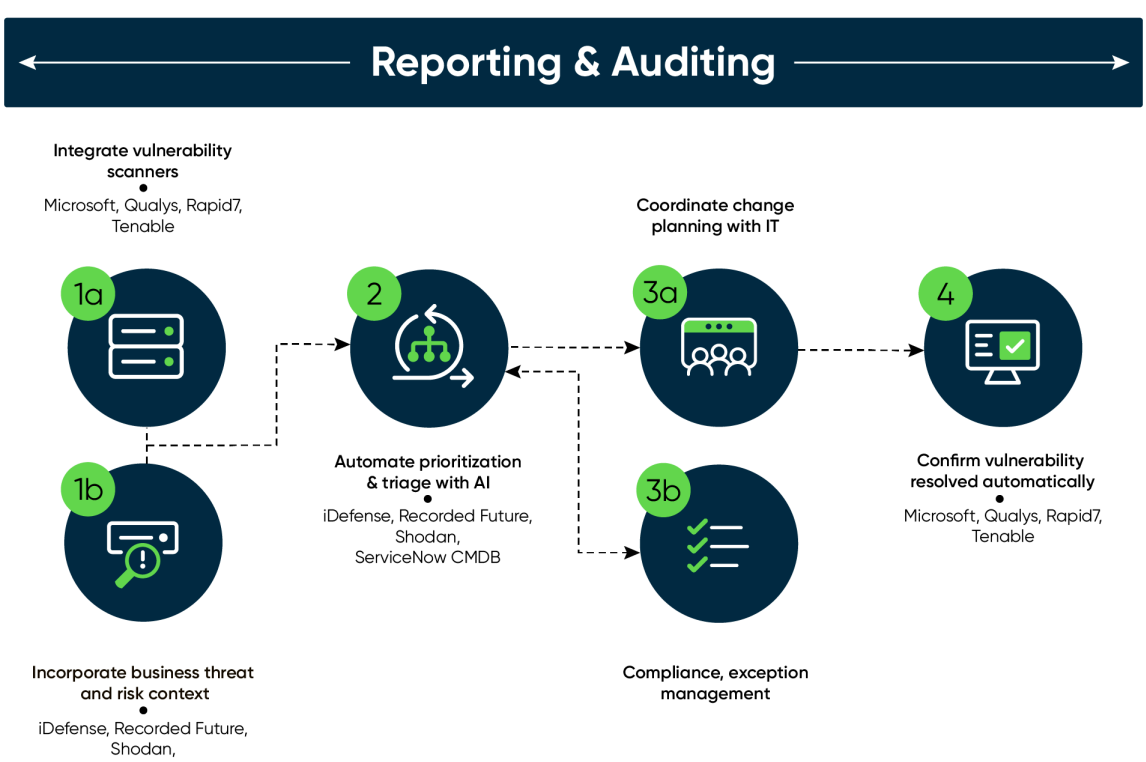
L'application Réponse aux vulnérabilités fait partie de la suite Security Operations . Ensemble, ces applications vous aident à protéger vos actifs en améliorant votre posture de sécurité globale.

L'application ServiceNow Réponse aux vulnérabilités a deux objectifs principaux :

- Aidez les équipes de sécurité confrontées à la gestion d'énormes quantités de données de vulnérabilité.
- Aider les équipes opérationnelles chargées de résoudre les vulnérabilités.

Vous pouvez ainsi utiliser l'application Réponse aux vulnérabilités pour automatiser le flux d'informations, de l'intégration à la résolution, en passant par l'enquête.

Le processus de gestion des vulnérabilités dans le ServiceNow AI Platform® peut impliquer des processus, des données, des rapports et l'automatisation avec le CMDB.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Intégrez des scanners et ServiceNow® des applications tiers à l'application Réponse aux vulnérabilités pour ingérer des données de vulnérabilité connues.
- Améliorez vos données de vulnérabilité ingérées avec l'exploit, la connaissance des menaces, le risque et le contexte métier. Utilisez ces données pour vous aider avec les stratégies d'application de correctif et de rattrapage.
- Les vulnérabilités importées à partir du NVD et les données de détection des produits tiers sont rapprochées avec les actifs de votre CMDB. Le triage peut inclure : la création de tâches de rattrapage composées de plusieurs éléments vulnérables, c'est-à-dire vos actifs qui présentent des vulnérabilités, le regroupement de ces tâches par catégorie, leur classement par ordre de priorité et leur affectation aux équipes.
- Utilisez une gestion coordonnée des changements et des exceptions pour vous aider à résoudre les vulnérabilités qui peuvent nécessiter une intervention manuelle supplémentaire, plus de temps de résolution ou des recherches approfondies.
- Vérifiez que les vulnérabilités sont résolues et mises à jour automatiquement par les détections de vos produits de scanner.

Qui pourrait utiliser Réponse aux vulnérabilités dans votre organisation

Réponse aux vulnérabilités Les utilisateurs se divisent généralement en deux personnages.

Analyste de vulnérabilité

Le profil d'analyste de vulnérabilité se situe généralement dans les domaines de la sécurité, des risques et de la conformité ou de la gestion. Ces utilisateurs surveillent les vulnérabilités et déterminent quand lancer les processus de rattrapage.

Important : L'analyste de vulnérabilité utilise principalement le Espace de travail du gestionnaire de vulnérabilités pour surveiller et créer des tâches de correction.

Propriétaire de la résolution

Le profil du propriétaire de rattrapage fait généralement partie des opérations informatiques, de DevOps/ingénierie ou d'un propriétaire de service. Ces utilisateurs effectuent les tâches de rattrapage nécessaires pour corriger les vulnérabilités. Ils peuvent soumettre des demandes d'exception ou de changement si des processus contrôlés sont nécessaires pour la maintenance ou la suppression des actifs.

Important : Le propriétaire de rattrapage travaille principalement sur les tâches de rattrapage à partir de .Espace de travail de remédiation IT

Réponse aux vulnérabilités des applications

La Réponse aux vulnérabilités des applications fonctionnalité (AVR) de l'application importe les éléments vulnérables de l'application ServiceNow® Réponse aux vulnérabilités (AVIT) et, selon des règles, vous permet de corriger les vulnérabilités de l'application. Il est disponible par abonnement séparé. Pour Réponse aux vulnérabilités des applications plus de documentation, reportez-vous à Explorer Réponse aux vulnérabilités des applications.

Versions disponibles

Pour obtenir un glossaire des termes et d'autres références comprenant des liens, des dépannages, des articles de la base de connaissances, en plus des données de champ sur les formulaires et les enregistrements trouvés dans , reportez-vous Réponse aux vulnérabilités Informations de référenceà Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Version de mise en production	Notes de publication
Réponse aux vulnérabilités v23.0	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Réponse aux vulnérabilités applications et CSDM tables

Réponse aux vulnérabilités des applications Les Réponse aux vulnérabilités intégrations et Nomenclature logicielle applications de vulnérabilité tierces gèrent les tables (y contribuent des données). CSDM Ces applications utilisent également des données provenant de CSDM tables générées par d'autres applications. Plusieurs ServiceNow produits bénéficient donc de ces Opérations de sécurité applications et y ajoutent de la valeur. Consultez Réponse aux vulnérabilités applications et CSDM tables pour plus d'informations.

Installation et prise en charge des Réponse aux vulnérabilités applications

L'application Réponse aux vulnérabilités est disponible à partir du ServiceNow Store. L'application prend en charge d'autres ServiceNow applications et intégrations tierces que vous téléchargez également à partir du ServiceNow Store. D'autres options sont également disponibles pour étendre la configuration de base.

Tâches pour la configuration de base

L'application Réponse aux vulnérabilités est requise dans un premier temps. Pour plus d'informations sur son installation, consultez Liste de vérification d'implémentation pour l'application Réponse aux vulnérabilités et Installer l'application Vulnerability Response .

- Une fois l'installation terminée, vous pouvez configurer Vulnerability Response à l'aide de l'assistant de configuration.

  Avec l'Assistant de configuration, affectez des utilisateurs et des groupes pour accéder à l'application, créez ou modifiez des règles d'affectation, des règles de tâche de rattrapage et des dates cibles, et configurez des calculateurs de risque.

- Vous pouvez également sélectionner, installer et configurer une ou plusieurs intégrations tierces prises en charge à partir de l'assistant de configuration. Ces intégrations récupèrent les données de vulnérabilité des systèmes externes et des fournisseurs. Pour en savoir plus sur le fonctionnement des intégrations et sur les intégrations prises en charge par , reportez-vous à Réponse aux vulnérabilités la section Intégrations de Réponse aux vulnérabilités.

- Avant d'implémenter des intégrations tierces, exécutez l'intégration NVD et la tâche planifiée CWE dans le cadre de votre configuration initiale de Réponse aux vulnérabilités.

  Consultez Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces et Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE pour plus d'informations sur l'installation, la configuration et l'affichage des bibliothèques NVD et CWE.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sélectionnez une application d'analyse, le cas échéant. Pack de contenu Performance Analytics pour l'application Vulnerability Response contient des rapports qui couvrent toutes les étapes du cycle de vie de la gestion de la vulnérabilité.

  [Facultatif] Installer et configurer l'application Analyse des performances pour Réponse aux vulnérabilités [PA] application.

- Sélectionnez une application de solutions, le cas échéant. Gestion des solutions vous aide à corréler les vulnérabilités de votre environnement avec les solutions susceptibles de les corriger. [Facultatif] Installer l'application Gestion des solutions pour Réponse aux vulnérabilités.

  Remarque :

  - Lorsque l'application Gestion des solutions pour vulnérabilités est activée, les et le Microsoft Security Response Center Solution Integration sont disponibles pour modification dans l'Assistant Intégration de solution Red Hat de configuration.

  - Gestion des solutions pour vulnérabilités nécessite un abonnement distinct. Pour plus d'informations, consultez Gestion des solutions pour vulnérabilités.

- [Facultatif] Installez l'application ServiceNow Agent et Réponse aux vulnérabilités l'application Mobile pour .Expérience mobile pour Réponse aux vulnérabilités

Autres tâches de configuration que vous pouvez effectuer

Ces tâches de configuration supplémentaires s'ajoutent à votre configuration de base et prennent en charge le rattrapage avec des options de reporting, de notifications par e-mail, de configuration d'intégration native et d'utilisation des éléments vulnérables. La plupart de ces tâches sont effectuées en dehors de l'assistant de configuration. Consultez Tâches d'installation et de configuration supplémentaires Réponse aux vulnérabilités.

Tâches avancées en dehors de la configuration de base

Ces tâches de configuration facultatives sont effectuées en dehors de l'assistant de configuration et nécessitent du codage ou une expertise avancée ServiceNow et ne sont pas considérées comme faisant partie de la configuration de base. Consultez Tâches de configuration avancée Réponse aux vulnérabilités.

Réponse aux vulnérabilités Profils et rôles granulaires

Avant de pouvoir corriger des vulnérabilités avec l'application Réponse aux vulnérabilités , vous devez affecter des profils et des rôles à vos utilisateurs et groupes dans l'Assistant de configuration.

L'une des premières étapes de configuration requises pour l'application Réponse aux vulnérabilités consiste à affecter des rôles aux utilisateurs et aux groupes. Les rôles définissent ce que les utilisateurs et les groupes peuvent voir et effectuer dans Réponse aux vulnérabilités, Analyse des performances pour Réponse aux vulnérabilités et toutes les intégrations tierces avec Réponse aux vulnérabilités.

Vous affectez des rôles de profil à des utilisateurs et à des groupes existants dans l'Assistant de configuration. Consultez Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Si vous êtes un client de mise à niveau, vous pouvez continuer à utiliser vos rôles existants pour l'application Réponse aux vulnérabilités . L'accès des utilisateurs et des groupes affectés aux autorisations sn_vul.vulnerability_read et sn_vul.vulnerability_write et au propriétaire de la résolution avant la version 10.3 n'a pas changé.

Toutefois, pour plus de contrôle sur ce que les utilisateurs et les groupes peuvent faire et voir dans l'application Réponse aux vulnérabilités au niveau de la tâche, vous pouvez préférer utiliser des rôles granulaires. Pour plus d'informations, consultez Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Si vous avez déjà affecté des rôles à l'aide de l'Assistant de configuration et que vous souhaitez gérer les affectations de rôles granulaires pour tous les utilisateurs et groupes à partir du module Administration utilisateurs, voir Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités pour plus d'informations.

Rôles de profil et rôles granulaires à partir de

Termes clés.

Rôle

Les rôles définissent ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités .

Groupe

Un ensemble d'utilisateurs qui partagent certains rôles et un objectif commun.

Rôle de profil

Un rôle préconfiguré dans l'application qui est composé de plusieurs rôles granulaires. Les rôles de profil dans Assistant de configuration, Administrateur de vulnérabilité, Analyste de vulnérabilité, Propriétaire du rattrapage, Gestionnaire d'élément de configuration et Gestionnaire d'exceptions sont conçus pour correspondre aux titres de poste courants des gestionnaires, des analystes et des propriétaires de services d'une organisation informatique ou d'un groupe de rattrapage de vulnérabilité.

Rôles hérités

Terme qui décrit les rôles que les utilisateurs acquièrent automatiquement lorsqu'ils sont affectés à d'autres rôles. Par exemple, tous les utilisateurs ou groupes affectés au rôle de profil sn_vul.remediation_owner héritent également des rôles granulaires sn_vul.read_assigned,sn_vul.write_assigned.

Liste de contrôle d'accès (ACL)

Les listes de contrôle d'accès restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

À partir de la Réponse aux vulnérabilités version 16.5, pour protéger les rapports contre l'exposition, définissez **toutes les ACL report_view** sur `active=true`. Cette ACL garantit que les données protégées ne sont disponibles que pour les utilisateurs autorisés.

Vous affectez des groupes et des utilisateurs à des rôles de profil dans l'Assistant de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Dans l'Assistant de configuration, le rôle d'administrateur système (admin) est requis pour les tâches de la première section, l'affectation des rôles et l'installation des intégrations. Après avoir affecté des rôles de profil dans l'assistant de configuration et installé les intégrations, vous préférerez peut-être affecter un utilisateur ou un groupe avec le rôle sn_vul.vulnerability_admin pour terminer toutes les tâches restantes dans l'assistant de configuration et gérer l'application Réponse aux vulnérabilités .

La table suivante répertorie Réponse aux vulnérabilités les rôles de profil installés avec l'application.

Rôles de profil pour Réponse aux vulnérabilités	Description
Affectez sn_vul.vulnerability_admin - Administrateur de vulnérabilité aux utilisateurs ou aux groupes.	Les utilisateurs disposant de ce rôle ont un accès complet à l'application Vulnerability Response (VR) et à ses enregistrements. Les utilisateurs disposant de ce rôle configurent toutes les applications et règles VR et installent des intégrations tierces.
Affectez sn_vul.vulnerability_analyst - Analyste de vulnérabilité aux utilisateurs et aux groupes.	Les utilisateurs et les groupes disposant de ce rôle affichent et mettent à jour tous les enregistrements pour le rattrapage des VI.
Affecter sn_vul.remediation_owner : propriétaire du rattrapage aux utilisateurs et aux groupes.	Les utilisateurs et les groupes dotés de ce rôle corrigent les vulnérabilités qui leur sont affectées ou qui sont affectées à un groupe auquel ils appartiennent. Les groupes ou les utilisateurs dotés de ce rôle voient et mettent à jour les enregistrements qui leur sont affectés ou qui sont affectés à un groupe auquel ils appartiennent.
Affectez sn_vul.ci_manager aux utilisateurs et aux groupes.	Les utilisateurs et les groupes dotés de ce rôle gèrent la reclassification des éléments de configuration (CI) sans correspondance qui ne se trouvent pas dans la Base de données de gestion des configurations (CMDB).
Affectez un accès en lecture à des zones spécifiques de l'application par tâche.	Par exemple, affectez sn_vul.read_all afin qu'un utilisateur puisse afficher tous les enregistrements VR. Pour un accès en lecture à l'affichage des règles de tâche de rattrapage, affectez sn_vul.read_group_rules. Les utilisateurs et les groupes ayant ce rôle ne mettent pas à jour les enregistrements.

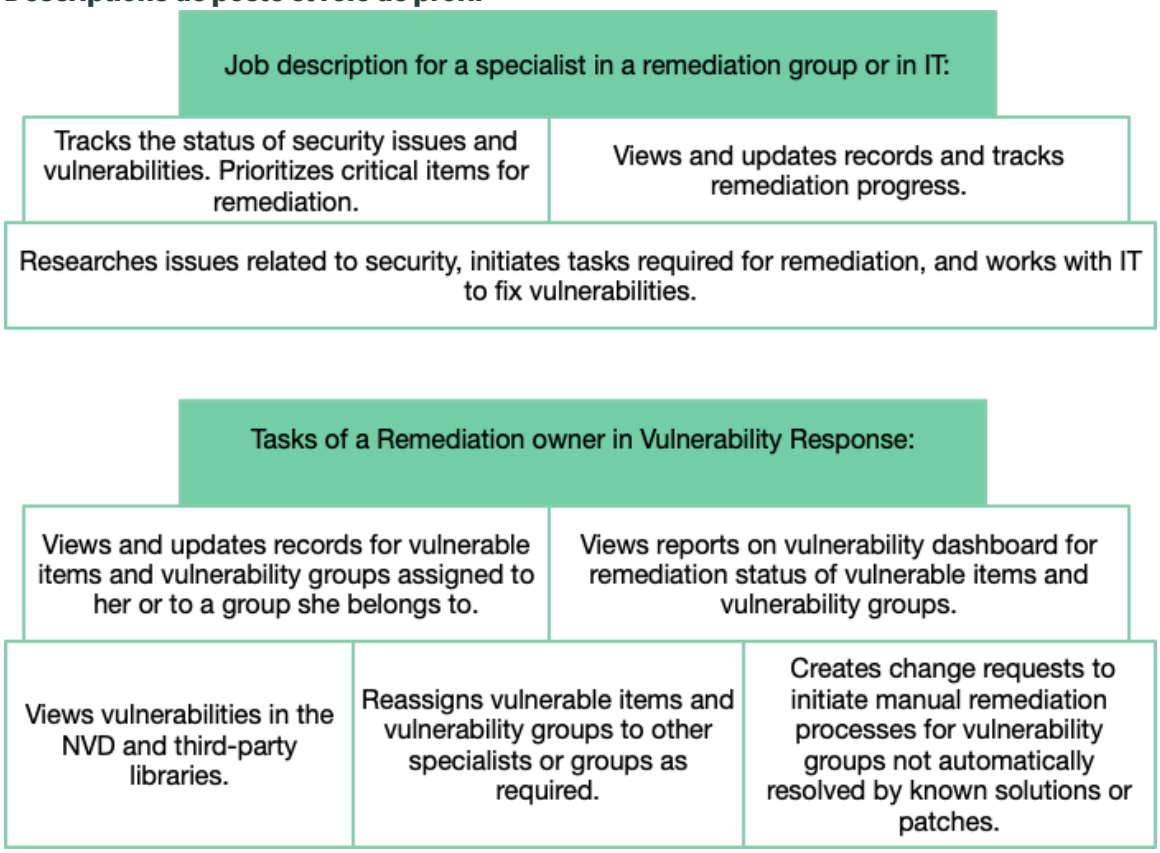
Rôles granulaires et rôles de profil

Une façon de penser aux rôles de profil est de considérer comment leurs descriptions peuvent être liées aux descriptions de poste pour divers postes informatiques ou de rattrapage de vulnérabilité dans votre organisation. La figure suivante illustre une description de poste possible pour un spécialiste du rattrapage dans l'informatique, et la façon dont les tâches associées à ce poste sont liées aux tâches d'un rôle de profil du propriétaire du rattrapage dans l'application Réponse aux vulnérabilités .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Descriptions de poste et rôle de profil



La description de tâche et le rôle de profil du propriétaire de rattrapage peuvent être définis comme une série de tâches de rattrapage. Dans l'image précédente, une description de poste et un rôle de profil dans les blocs verts se trouvent au-dessus des tâches qui les décrivent. Dans cet exemple, certaines des exigences professionnelles typiques d'un spécialiste dans un groupe de rattrapage correspondent directement aux tâches qui constituent le profil du propriétaire de rattrapage dans Réponse aux vulnérabilités: Examiner et mettre à jour les enregistrements, suivre l'état de rattrapage des vulnérabilités, classer les éléments à corriger par ordre de priorité et appliquer des correctifs et des correctifs avec le service informatique.

Parfois, cependant, les emplois de votre organisation peuvent ne pas correspondre directement aux tâches qui composent l'un des cinq rôles de profil dans l'application Réponse aux vulnérabilités . Pour diverses raisons, telles que la protection des données sensibles ou le respect de la réglementation, vous devez limiter l'accès étendu que certains rôles de profil fournissent à vos utilisateurs et groupes. Ou, inversement, vous êtes tenu de fournir aux utilisateurs et aux groupes plus d'accès afin qu'ils puissent effectuer leur travail. À l'aide de rôles granulaires, vous pouvez facilement personnaliser les rôles et contrôler l'accès des utilisateurs et des groupes à , ainsi qu'aux Réponse aux vulnérabilitésAnalyse des performances pour Réponse aux vulnérabilités intégrations tierces.

Les rôles granulaires définissent les tâches

Les noms des rôles granulaires dans Réponse aux vulnérabilités décrivent généralement ce que les utilisateurs peuvent faire et voir dans l'application Réponse aux vulnérabilités . Par exemple, dans l'image précédente, les utilisateurs et les groupes avec le profil de propriétaire de rattrapage affecté ont les rôles granulaires sn_vul.read_assigned et sn_vul.write_assigned. Ces rôles granulaires permettent aux utilisateurs ou aux groupes d'afficher et de mettre à jour les éléments vulnérables et les enregistrements de tâches de rattrapage qui leur sont affectés. Pour afficher les descriptions de rôles granulaires spécifiques, en tant

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

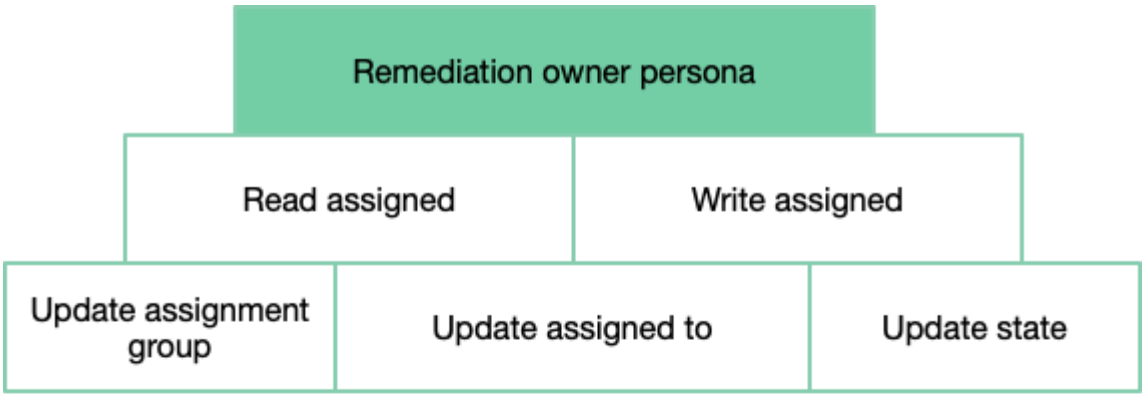
qu'utilisateur ayant le rôle d'administrateur système, accédez à **Administration utilisateurs** > **Rôles** et localisez le rôle souhaité. Les rôles qui sont automatiquement hérités lorsqu'un rôle est affecté sont répertoriés. En outre, lorsqu'un rôle dépend d'autres affectations de rôles, tous les rôles requis sont également répertoriés.

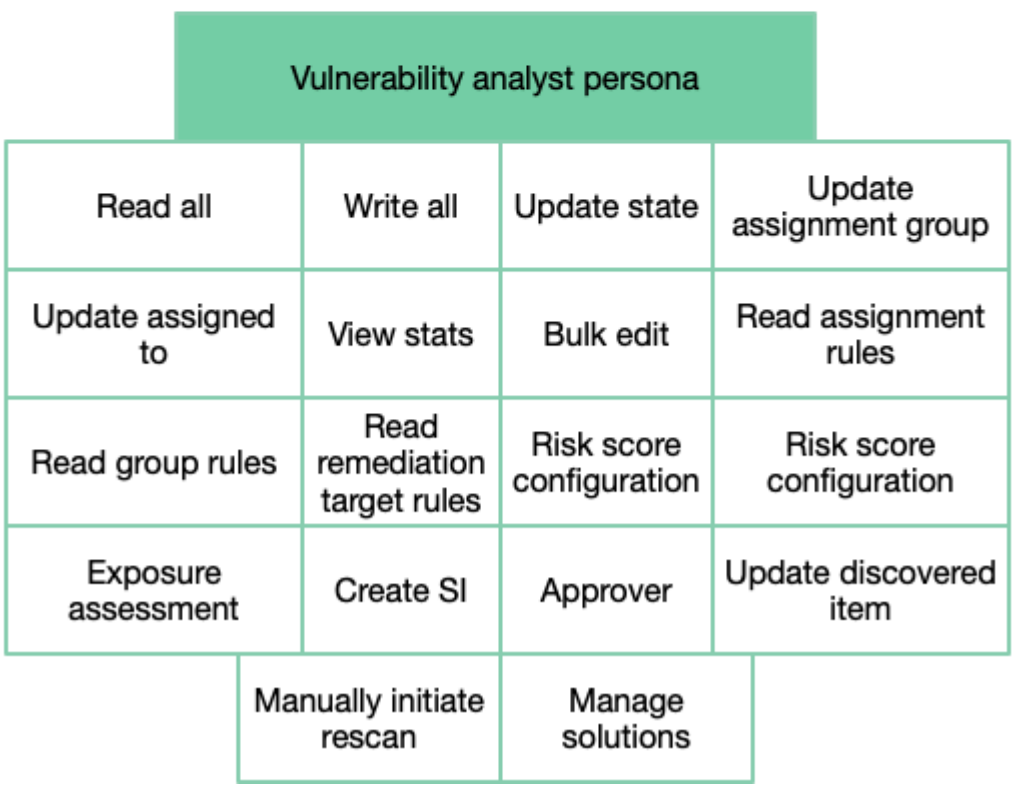
L'image suivante illustre les rôles granulaires du profil du propriétaire du rattrapage et du profil d'analyste de vulnérabilité. Notez que le profil du propriétaire de rattrapage n'inclut pas les autorisations read_all et write_all du profil de l'analyste de vulnérabilité. Les rôles granulaires, read_all et write_all, sont requis pour que les utilisateurs et les groupes puissent lire et modifier tous les enregistrements d'éléments vulnérables et de tâches de rattrapage. Pour personnaliser ces rôles, il suffit d'ajouter ou de supprimer des rôles granulaires pour développer ou limiter l'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles granulaires et profils du propriétaire de la remédiation et de l'analyste de vulnérabilité





Si vous souhaitez que vos utilisateurs et vos groupes aient plus d'accès que ne le permettent les rôles de profil, vous pouvez ajouter des rôles plus granulaires aux utilisateurs et aux groupes. Inversement, si vous souhaitez limiter l'accès à des utilisateurs et à des groupes spécifiques au niveau de la tâche, vous pouvez supprimer les rôles granulaires.

Remarque : Le rôle d'administrateur système est requis pour affecter et modifier des rôles granulaires dans le module Administration utilisateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles granulaires avec accès aux scripts

Les rôles suivants fournissent un accès de scripting aux tables répertoriées :

Rôle	Table	Application
sn_vul.manage_auto_close_stale_vi	sn_vul_cmn_auto_close_rule	Réponse aux vulnérabilités
sn_vul.app_manage_auto_close_rule		Réponse aux vulnérabilités
sn_vul_container.manage_auto_close_stale_vi		Réponse aux vulnérabilités du conteneur
sn_vul_container.manage_assignment_rules	sn_vul_assignment_rule	Réponse aux vulnérabilités du conteneur
sn_vul.app_manage_assignment_rules		Réponse aux vulnérabilités de l'application
sn_vul.manage_assignment_rules		Réponse aux vulnérabilités
sn_vul_agile.write	sn_vul_agile_tool	Réponse aux vulnérabilités
sn_vul_int_fw.configure_integrations	sn_vul_int_fw_integration	Réponse aux vulnérabilités

Rôles granulaires dans le module Administration utilisateurs

Pour obtenir un exemple de gestion des rôles granulaires d'un utilisateur ou d'un groupe, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pour affecter des rôles de profil, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation

Définissez les critères selon lesquels les éléments vulnérables (VIT) sont automatiquement affectés à un groupe d'affectation pour le rattrapage.

Une règle d'affectation par défaut, **Affecter au groupe de support CI**, est incluse dans l'affectation des éléments vulnérables au **groupe de support CI** par le système de base. La règle Affecter à un groupe de support CI affecte un VIT au groupe de support défini pour l'élément de configuration (CI) associé au VIT.

Remarque : Les règles d'affectation ne réévaluent pas les affectations créées manuellement.

Le type d'affectation, **manuel** ou **règle** , est disponible dans le formulaire VIT et la vue de liste. Tout VIT qui a été affecté à l'origine par une règle, mais qui a ensuite été réaffecté manuellement contient une référence à la règle d'origine.

Utilisez les informations de règle d'affectation et de type d'affectation pour identifier les tickets pour lesquels les règles d'affectation n'ont pas trouvé de correspondance appropriée pour le destinataire prévu. Vous pouvez également utiliser les informations pour identifier les règles qui ont connu le plus de réaffectations.

Les groupes d'affectation définis par les règles d'affectation sont utilisés par **les règles de tâche de rattrapage** pour affecter des propriétaires à des tâches de rattrapage (VUL).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Pour que Rapid7 InsightVM des balises d'actifs puissent être utilisées dans le filtre de condition pour les règles d'affectation, vous devez exécuter l'intégration de la Rapid7 InsightVM liste des actifs avant les autres Rapid7 InsightVM intégrations.

La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.

Affectation automatique des éléments vulnérables

Il existe trois façons différentes d'affecter des éléments vulnérables à l'aide de **l'option Affecter à l'aide de** :

- Groupe d'utilisateurs : cette option vous permet de sélectionner n'importe quel groupe d'utilisateurs existant ServiceNow AI Platform® .
- Champ de groupe d'utilisateurs : cette option vous permet de choisir n'importe quel champ de groupe d'affectation disponible à l'aide de la table cmdb_ci. Par défaut, les trois champs de groupe suivants s'affichent :
  - Aucune : n'indique aucune valeur par défaut pour ce champ obligatoire
  - Élément de configuration : groupe d'approbation
  - Élément de configuration : groupe d'affectation
  - Élément de configuration : groupe de support
- Script : cette option vous permet de définir les conditions à l'aide d'un script. Cette option nécessite un codage ou une expertise avancée ServiceNow . Pour plus d'informations sur l'utilisation de l'éditeur de script pour définir des conditions complexes, consultez l'article de la base de connaissances KB0965240 .

Exécutez d'abord les règles de priorité élevée (éléments nécessitant une gestion spéciale, lorsque le risque est critique ou qu'un VIT doit être géré par la conformité réglementaire). Ensuite, exécutez vos règles générales, où aucune manipulation spéciale n'est requise, et vous savez qui doit en être responsable. Enfin, créez une règle par défaut pour affecter des VIT au groupe qui déterminera à quel groupe d'affectation ils doivent appartenir. Ce groupe pourrait ajouter une autre règle pour couvrir ses décisions. Cette règle par défaut s'exécute en dernier.

Processus d'évaluation des règles d'affectation

Les règles d'affectation sont utilisées pour évaluer et affecter un VIT lorsqu'un nouveau VIT est ouvert, c'est-à-dire importé, créé manuellement ou rouvert. À moins que vous ne réappliquiez manuellement des règles d'affectation après que le VIT ou son état a changé, un VI est évalué une fois.

Le processus suivant est utilisé pour chaque VIT nouveau, mis à jour ou rouvert :

- Pour chaque règle d'affectation de vulnérabilité, la VIT est comparée au filtre d'affectation, en commençant par la règle d'ordre le plus bas.
- Lorsque la condition est remplie, le VIT se voit affecter un groupe d'affectation. La recherche s'arrête.
- Lorsque les conditions ne trouvent pas de correspondance parmi toutes les autres règles, le VIT est affecté au groupe d'affectation par défaut, s'il en existe une.

  Une fois l'élément vulnérable affecté, la règle de tâche de rattrapage appropriée utilise l'affectation comme l'un de ses critères pour placer les éléments vulnérables dans une

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

tâche de rattrapage. Voir Réponse aux vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage et Filtrage au sein de Réponse aux vulnérabilités pour plus d'informations.

Remarque : La règle par défaut est celle qui présente la valeur d'ordre d'exécution la plus élevée. Une règle finale à utiliser qui est un bon contact de secours est active=true. S'il n'y a pas de règle par défaut, le VIT reste désaffecté lorsque la règle de la tâche de rattrapage effectue l'affectation.

Réapplication des règles d'affectation

Lorsque vous modifiez une règle d'affectation, utilisez le bouton **Appliquer les modifications** sur la page de liste Règles d'affectation pour réexécuter toutes les règles modifiées sur tous les VI ouverts actifs, à l'exception de ceux qui ont été affectés manuellement.

Remarque :

Si la tâche planifiée ne s'est *Reapply all vulnerability assignment rules* pas exécutée avant la première fois que vous utilisez **Appliquer des changements**, elle exécute toutes les règles d'affectation sur tous les VIT ouverts, à l'exception des VI qui ont été affectés manuellement. Ensuite, toutes les utilisations ultérieures de **l'application Appliquer les modifications** réexécutent uniquement les règles modifiées et les règles dépendantes. Les changements apportés à une règle peuvent entraîner la correspondance d'un VIT avec une autre règle non modifiée. La réapplication des règles d'affectation ne regroupe pas les éléments vulnérables.

La tâche planifiée [*Reapply all vulnerability assignment rules*] est inactive par défaut. Lorsqu'elle est activée, elle applique toutes les règles à tous les VIT ouverts, à l'exception de ceux qui sont affectés manuellement. Il peut s'exécuter **quotidiennement**, **hebdomadairement**, **mensuellement**, **périodiquement**, **une fois** ou **sur demande**. En fonction du nombre de VI actifs que vous avez dans votre environnement, n'oubliez pas de définir le champ **Exécuter** de manière appropriée après l'exécution initiale pour éviter les impacts sur les performances.

Les clients de mise à niveau doivent consulter les Réponse aux vulnérabilités notes de version pour plus d'informations sur l'impact de cette fonctionnalité sur les VIT existants.

Important : En tant qu'administrateur et analyste des vulnérabilités, vous pouvez obtenir les dernières affectations pour les éléments vulnérables sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités. Cette méthode est plus efficace que l'exécution des règles d'affectation pour tous les éléments vulnérables dans l'interface utilisateur classique, qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Lorsqu'un groupe d'affectation sur une règle d'affectation change, les éléments vulnérables peuvent être automatiquement réévalués et regroupés en activant la propriété système sn_vul.rerun_task_rules et la règle métier Lien vers les tâches de rattrapage.

Pour activer la propriété système :

1. Accédez à la **Tous** > **Propriétés système** > **Toutes les propriétés**.
2. Ouvrez la propriété système sn_vul.rerun_task_rules.
3. Dans le champ **Valeur** , définissez la valeur sur vrai.

Lorsque la propriété système est définie sur vrai et que les règles d'affectation sont réappliquées, les éléments vulnérables sont dissociés des tâches de rattrapage, où la condition ne correspond plus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Par défaut, la propriété système sn_vul.rerun_task_rules est définie sur false.

Pour automatiser le regroupement des éléments vulnérables, vous devez activer la règle métier Lier les tâches de rattrapage.

Pour activer la règle métier :

1. Accédez à la **Tous** > **Définition du système** > **Règles métier**.
2. Ouvrez la règle métier Lien vers les tâches de remédiation.
3. Cochez la case **Actif** pour activer la règle métier.

La règle métier lorsqu'elle est activée regroupe les éléments vulnérables en les déplaçant vers le groupe approprié ou en créant un groupe s'ils ne peuvent pas être regroupés dans un groupe existant.

Remarque :

- Les éléments vulnérables sont supprimés des groupes sans supprimer les groupes.
- Seuls sont supprimés les éléments créés à l'aide des règles de tâche de rattrapage ou d'un effort de rattrapage.
- Le regroupement est effectué automatiquement uniquement lorsque le groupe d'affectation change dans le cadre d'une règle d'affectation et non lorsqu'il est modifié manuellement.
- Les règles d'affectation ne s'appliquent pas aux VIT à l'état Différé. Si un VIT est reporté, vous devez l'affecter manuellement si nécessaire.

Le regroupement dans les espaces de travail est effectué pour les tâches de rattrapage, qui sont créées à partir d'un effort de rattrapage.

Réponse aux vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage

Configurez les tâches de rattrapage (VUL) pour aider les analystes et les spécialistes du rattrapage à organiser les éléments vulnérables (VI) et à les analyser en bloc. Les critères selon lesquels les tâches de rattrapage sont formées sont configurés de manière à ce que vous n'ayez pas à affecter manuellement les éléments vulnérables aux tâches de rattrapage. Les tâches de rattrapage vous permettent de surveiller la progression et de piloter le processus de rattrapage plus efficacement.

Suivi du nombre de reports pour les éléments vulnérables et les tâches de remédiation

Suivez le nombre de reports d'un élément vulnérable, d'un élément vulnérable d'application, d'un élément vulnérable de conteneur ou d'une tâche de rattrapage. Une tâche planifiée, **Définir les nombres de reports**, s'exécute quotidiennement pour valider les nombres des enregistrements qui sont différés plusieurs fois dans la colonne Nombre de reports. Les enregistrements sont affichés dans les modules Reports multiples pour VR, AVR et CVR.

Actualisation automatique des éléments vulnérables

Remarque : L'automatisation de l'actualisation des éléments vulnérables s'applique uniquement aux tâches de rattrapage créées à l'aide du filtre de condition ou du groupe de filtres. L'automatisation ne s'applique pas aux éléments vulnérables qui ont été ajoutés manuellement ou regroupés à l'aide des règles de tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque la case **Mettre automatiquement à jour les éléments vulnérables connexes** est cochée, les nouveaux éléments vulnérables correspondant aux critères de filtre de la tâche de rattrapage sont automatiquement ajoutés à la tâche. Les éléments vulnérables de la tâche de rattrapage qui ne correspondent plus aux critères de filtre sont automatiquement supprimés de la tâche.

Par défaut, lorsque la tâche de rattrapage quitte l'état **Ouvert** , la case est décochée. Si vous voulez que les éléments vulnérables continuent d'être ajoutés à la tâche de rattrapage, quel que soit leur état, désactivez la *`Set auto refresh vulnerable items`* règle métier.

Vous pouvez sélectionner à nouveau la case à cocher manuellement à partir de l'état En cours d'examen. **L'option Mettre automatiquement à jour les éléments vulnérables connexes** n'est pas désactivée lorsque la tâche de rattrapage passe à l'état **En attente d'implémentation** . Une fois dans l'état En attente d'implémentation, aucun nouvel élément vulnérable ne peut être ajouté à la tâche existante, et les éléments vulnérables existants ne peuvent pas être supprimés.

Remarque : Lorsqu'une tâche de rattrapage est créée manuellement et que les VI sont ajoutés à l'aide du filtre **Condition** ou du **groupe de filtres**, la case n'est pas cochée. Vous avez le choix de cocher la case ou non.

Actualisation manuelle des éléments vulnérables

Pour les tâches de rattrapage créées manuellement avec un filtre **de groupe de filtres** ou de **condition** , lorsque vous cliquez sur le lien connexe **Actualiser** les éléments vulnérables associés sur la page **Tâche de rattrapage** , tous les éléments vulnérables qui correspondent aux critères de filtre sont ajoutés. Les éléments ne correspondant plus aux critères sont supprimés. Cette action permet une mise à jour immédiate de la liste des éléments vulnérables et est utilisée que la case **Mettre à jour automatiquement les éléments vulnérables connexes** soit cochée ou non.

Les types de filtres des tâches de rattrapage créées manuellement à l'aide d'une **condition** ou **d'un groupe de filtres** sont actualisés une fois par heure.

Comprendre les règles de tâche de rattrapage

Les règles de tâche de rattrapage vous permettent de définir comment les éléments vulnérables sont automatiquement regroupés et affectés. Une règle par défaut, **Vulnérabilité**, est incluse dans le système de base qui rassemble les éléments vulnérables en fonction de leurs vulnérabilités. Toutefois, vous pouvez effectuer un regroupement par tout autre ensemble de valeurs dans des colonnes accessibles à partir de l'élément vulnérable. Ces valeurs peuvent inclure l'élément de configuration (CI), le groupe de support, la gravité de la vulnérabilité, etc.

Vous pouvez créer n'importe quel nombre de conditions. Une fois que vous avez défini une sélection Grouper par, une autre ligne apparaît. Vous pouvez avoir jusqu'à six sélections **Grouper par** . Vous pouvez également automatiser l'affectation de groupe. Voir Créer ou modifier des Réponse aux vulnérabilités règles de tâche de rattrapage et Filtrage au sein de Réponse aux vulnérabilités pour plus d'informations.

Remarque : Pour que Rapid7 InsightVM des balises d'actifs puissent être utilisées dans le filtre de condition pour les règles de tâche de rattrapage, vous devez exécuter l'intégration de la Rapid7 InsightVM liste des actifs avant les autres Rapid7 InsightVM intégrations.

Par exemple, vous pouvez regrouper vos éléments vulnérables par centre de coûts du CI vulnérable ou par vecteur d'attaque de la vulnérabilité. Vous pouvez avoir une règle de

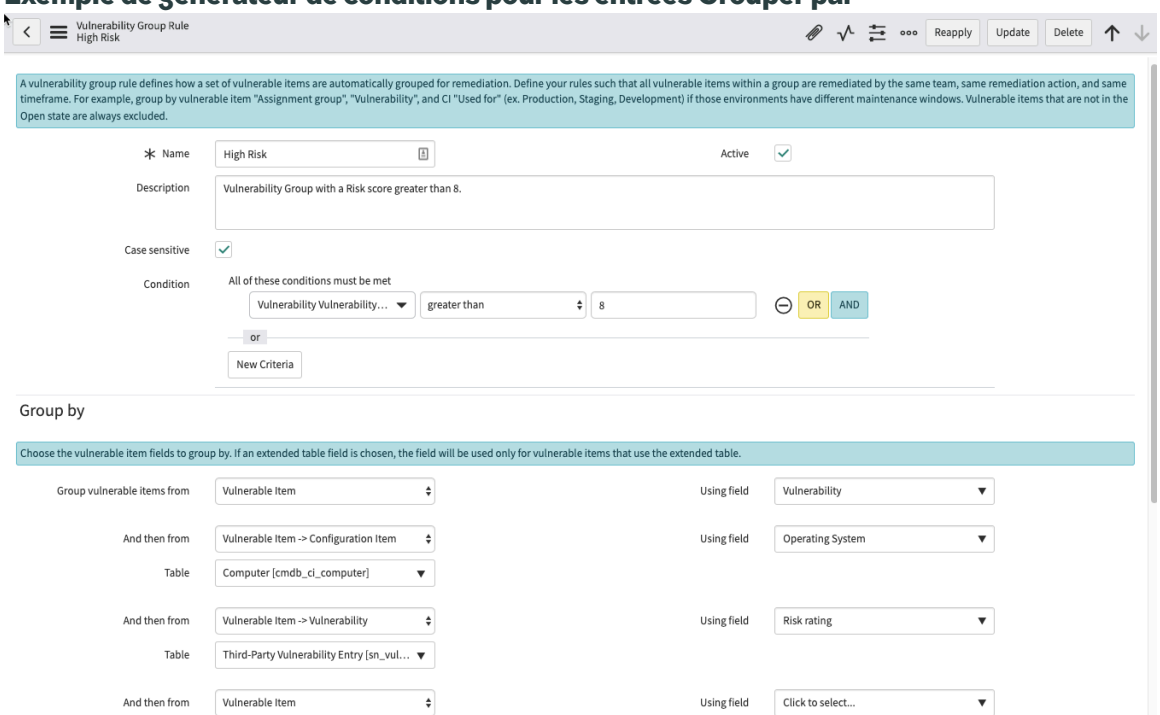
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

tâche unique pour les vulnérabilités de faible gravité ou les CI à faible risque. Vous pouvez avoir une autre règle de tâche pour les serveurs critiques et les vulnérabilités avec des exploits, des éléments vulnérables qui exposent l'entreprise à plus de risques.

Un autre ensemble de règles peut être utilisé pour les éléments vulnérables qui exposent l'entreprise à davantage de risques. Le nom de la tâche de rattrapage est ajouté à la règle de tâche de rattrapage **Grouper par** valeurs pour faire la brève description du nouvel enregistrement. Consultez la rubrique Créer manuellement une tâche de rattrapage dans Réponse aux vulnérabilités pour plus d'informations sur les champs disponibles.

Exemple de générateur de conditions pour les entrées Grouper par



Lorsqu'un nouvel élément vulnérable est créé, importé ou rouvert après avoir été fermé, les règles de vulnérabilité sont évaluées en fonction de celui-ci. Un VI n'est évalué qu'une seule fois, automatiquement, à moins qu'il ne soit rouvert après avoir été fermé ou que les règles ne soient réappliquées manuellement.

Le processus suivant est utilisé pour chaque VI nouveau ou rouvert :

- Pour chaque règle de tâche de rattrapage, le VI est comparé au filtre de règle de tâche de rattrapage.
- Pour chaque règle dans laquelle la condition de la règle de tâche de rattrapage est vérifiée, la règle extrait les données des sélections **Grouper par** sur le VI. Il génère un nom de groupe et un champ. Dans ce cas, **Risque élevé : QID-32342 :** *`Résumé de QID-3242`* (Nom : ID de vulnérabilité : résumé de la vulnérabilité).

  Remarque : Le champ Description brève est limité à 160 caractères. Les résumés de vulnérabilité plus longs sont tronqués.

  La règle vérifie s'il existe une tâche de rattrapage **ouverte** correspondante affectée au même groupe d'affectation que le VI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si la tâche est trouvée, l'élément vulnérable est ajouté à la tâche existante à l'état **Ouvert** .
- Si aucune tâche à l'état **Ouvert** n'est trouvée, la règle crée une tâche **Risque élevé : QID-32342** , l'affecte au même groupe d'affectation que le VI et place le VI dans la tâche de rattrapage.

Plusieurs règles de tâche de rattrapage peuvent être définies, pour regrouper différents types de vulnérabilités. Étant donné que chaque vulnérabilité est comparée aux conditions de la règle de tâche de rattrapage avant de la placer dans une tâche de rattrapage, trop de règles peuvent avoir un impact sur les performances.

Par défaut, les règles de tâche de rattrapage utilisent le groupe d'affectation défini par les **règles d'affectation** sur l'élément vulnérable lors du regroupement des éléments vulnérables et affectent la tâche de rattrapage pour correspondre aux éléments vulnérables.

Dans le cadre de la règle de tâche par défaut, l'affectation de ces tâches de rattrapage est contrôlée par les règles du module **Règles d'affectation** . Pour plus d'informations sur les règles d'affectation, reportez-vous à Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Lorsqu'une règle de tâche est supprimée, vous pouvez supprimer, à partir de la vue de formulaire ou de liste, toutes les tâches **ouvertes** créées par cette règle. Les tâches non **ouvertes** sont exclues.

Réapplication des règles de tâche de rattrapage

Lorsque vous souhaitez modifier une règle de tâche de rattrapage, utilisez le bouton **Réappliquer** sur la page de règle de tâche de rattrapage pour réexécuter la règle modifiée sur toutes les tâches de rattrapage **ouvertes** actives créées par cette règle. Elle supprime et recrée automatiquement les tâches de rattrapage en fonction de la règle modifiée.

Important : En tant qu'administrateur et analyste des vulnérabilités, vous pouvez évaluer les règles de tâche de rattrapage pour les éléments vulnérables sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités. Cette méthode est plus efficace que la réapplication des règles de tâche de rattrapage dans l'interface utilisateur classique, qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Réponse aux vulnérabilités Règles de cibles de rattrapage

Les règles de cible de rattrapage définissent le délai prévu pour le rattrapage des éléments vulnérables (VI), tout comme les SLA fournissent un délai pour le rattrapage de la vulnérabilité elle-même. Par exemple, si un actif contient des données PCI (données de carte de crédit), la vulnérabilité de cet élément doit être corrigée dans les 30 jours, conformément à la norme PCI DSS.

Les gestionnaires de vulnérabilité peuvent créer des règles de cible de rattrapage en définissant :

- La cible de rattrapage
- La cible de rappel
- Les destinataires des rappels et des notifications : qui doit être notifié lorsque les éléments vulnérables (VI) ont dépassé la date cible de rappel ou de rattrapage et n'ont pas été corrigés ?

Les analystes et les gestionnaires de vulnérabilité peuvent voir la date cible de rattrapage dans le formulaire d'élément de vulnérabilité et les vues de liste, tant que les éléments

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérables ne sont pas à l'état **Différé**, **Résolu** ou **Fermé** . Les règles de cibles de rattrapage sont exécutées lors de l'importation et réexécutées si un VI est rouvert.

La **date cible de rattrapage** est codée par couleur sur la vue de liste des VI sous forme de points, comme suit :

- Les éléments vulnérables qui n'ont pas encore atteint leur date de notification sont affichés en vert.
- Les éléments vulnérables approchant de la date cible de rattrapage sont affichés en orange.
- Les éléments vulnérables dépassant la date cible de rattrapage sont affichés en rouge.

Un e-mail récapitulatif, par règle de cible de rattrapage, est envoyé lorsqu'un ou plusieurs VI approchent de leur date cible de rattrapage ou que la date cible de rattrapage est dépassée.

Les règles de cibles de rattrapage peuvent être désactivées ou supprimées

Lorsqu'une règle est désactivée, les dates cibles de rattrapage actuelles pour les éléments vulnérables auxquels elle s'applique sont effacées. Si un VI satisfait à une règle active, cette règle est appliquée, sinon le VI n'a pas de règle ni de date cible, et son état est **Aucune cible**.

Lorsque des règles sont supprimées, la date **cible de rattrapage** et les champs connexes sur les VI fermés, différés ou résolus sont conservés. La date **cible de rattrapage** et les champs connexes sur les VI non fermés sont effacés et toutes les règles dépendantes sont réappliquées.

Scénario de règle de cible de rattrapage

Lorsque plusieurs règles cibles de rattrapage sont appliquées au même élément vulnérable, la règle la plus restrictive s'applique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les cibles de rattrapage sont calculées à partir de la **dernière date d'ouverture** additionnée au nombre de jours (mesurés par incréments de 24 heures).

À partir de la version 17.1, les cibles de rattrapage sont calculées à partir **de la cible à partir du (date).** La valeur par défaut reste **Dernière date d'ouverture**.

Par exemple, si un élément vulnérable répond à la condition de deux règles de cible de rattrapage :

Scénario : l'élément vulnérable a été ouvert pour la dernière fois le 03/01/2018 à 10:00:00.

- Règle de cible de rattrapage 1 : Dernière ouverture le 03/07/2018 ; la cible de rattrapage est de 15 jours depuis sa dernière ouverture ; La date cible de rattrapage calculée est le 16/03/2018 10:00:00.
- Règle de cible de rattrapage 2 : Dernière ouverture le 10/03/2018 ; la cible de rattrapage est de 10 jours à compter de sa dernière ouverture ; La date cible de rattrapage calculée est le 11/03/2018 10:00:00.

Dans ce scénario, la règle de cible de rattrapage 2 s'applique à l'élément vulnérable, car il a la date la plus restrictive. 10 jours depuis la première identification de l'élément vulnérable par rapport à 15 jours.

Remarque : Une fois la règle de cible de rattrapage définie, les dates cibles de rattrapage sont calculées par la *`Evaluate remediation targets`* tâche planifiée.

À propos de la tâche planifiée Évaluer les cibles de rattrapage

`Evaluate remediation targets` s'exécute une fois à 4:00:00 tous les jours.

Il itère toutes les règles de vulnérabilité actives, en commençant par celles dont la date cible de rattrapage est la plus ancienne. Il examine tous les éléments vulnérables qui :

- ne sont pas à l'état **Fermé**, **Différé** ou **Résolu** .
- N'ont pas de date cible de rattrapage.
- Avoir une date cible de rattrapage ultérieure à la date de la règle de cible de rattrapage.

`Evaluate remediation targets` Ajoute une date cible de rattrapage, s'il n'en existe pas, ou si une règle aboutit à une date antérieure à celle de l'enregistrement, il met à jour la date cible existante. Enfin, il met à jour les champs **Cible de rattrapage** et **État du rattrapage** dans le formulaire d'élément vulnérable.

Une fois la *`Evaluate remediation targets`* tâche exécutée, les notifications disponibles sont envoyées.

`Evaluate remediation targets` efface les champs de rattrapage sur le VI et arrête l'envoi de notifications.

Lorsqu'elle est activée, cette *`sn_sec_cmn.evaluate_targetmissed_records`* propriété empêche la tâche planifiée d'évaluer *`Remediation Target Rules`* les VI manqués. Cette propriété est activée par défaut.

Réapplication des règles de cibles de rattrapage

Lorsque vous modifiez une règle de cible de rattrapage, utilisez le bouton **Appliquer les changements** de la page de liste des règles de cibles de rattrapage pour réexécuter toutes les règles modifiées sur tous les VI ouverts actifs, à l'exception de ceux dont l'état est

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fermé, **Différé** ou **Résolu** . Selon le nombre d'EV que vous avez, cette opération peut prendre un certain temps.

Remarque :

Si la tâche planifiée *`Evaluate remediation targets`* est en cours d'exécution, vous ne pouvez pas lancer un processus de nouvelle demande. Toutefois, si un processus de réapplication est déjà en cours d'exécution et le travail planifié qu'il a déclenché, ils s'exécutent en parallèle.

Les processus de réapplication sont Réponse aux vulnérabilitésRéponse aux vulnérabilités des applications indépendants et peuvent s'exécuter en parallèle.

Important : En tant qu'administrateur et analyste des vulnérabilités, vous pouvez obtenir la dernière date cible de rattrapage pour les éléments vulnérables sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités. Cette méthode est plus efficace que l'exécution des règles de cibles de rattrapage pour tous les éléments vulnérables de l'interface classique utilisateur, qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Information associée

Créer ou modifier Réponse aux vulnérabilités des règles de cibles de rattrapage

Afficher l'état de la cible de rattrapage d'un Réponse aux vulnérabilités élément vulnérable

Créer ou modifier des notifications de cible de rattrapage

Groupes et règles de classification des vulnérabilités

Les groupes de classification automatisent la classification des valeurs d'une table en fonction des règles de classification définies dans le groupe. La condition de chaque règle est évaluée dans l'ordre, et la première règle correspondante est utilisée.

Le système de base de Vulnerability Response comprend les deux groupes de classification suivants, qui classent respectivement les éléments découverts et les vulnérabilités :

- Classification des éléments détectés
- Classification de l'entrée de vulnérabilité

Chaque fois que des vulnérabilités et des éléments détectés sont importés, les règles de classification des vulnérabilités dans les groupes respectifs sont exécutées. En fonction des conditions définies dans la règle, les enregistrements sont classés dans le groupe de classification approprié. Vous pouvez créer, modifier, supprimer ou réappliquer ces règles à une vulnérabilité existante.

Remarque :

- Pour une table sélectionnée, il ne peut y avoir qu'un seul groupe de classification actif.
- Une fois que vous avez créé un groupe, vous ne pouvez pas le supprimer.

Pour en savoir plus, consultez Créer et modifier une règle de classification, Appliquer une règle à une vulnérabilité existante et Désactiver ou supprimer une règle de classification.

Solutions d'apprentissage machine pour Réponse aux vulnérabilités

Recommandations d'affectation de vulnérabilité utilise ServiceNow® Intelligence prédictive l'apprentissage machine pour recommander des groupes d'affectation pour les éléments vulnérables (VI) et les tâches de rattrapage (VUL ou RT). Vous pouvez réduire le temps que

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vous consacrez à l'identification des propriétaires des résultats de vulnérabilité non affectés ou mal affectés. En outre, vous pouvez voir un score de confiance généré par le système qui évalue si le groupe d'affectation recommandé est adapté pour résoudre la vulnérabilité.

Les Intelligence prédictive options sont utilisées pour Réponse aux vulnérabilités offrir une meilleure expérience professionnelle en créant et en formant un modèle de définition de solution capable de prédire le groupe d'affectation en fonction des données existantes.

Pour en savoir plus, consultez Intelligence prédictive .

Recommandations d'affectation de vulnérabilité

Avec l'application Recommandations d'affectation de vulnérabilité (com.snc.vulnerability.recom), le système peut affecter des recommandations à Réponse aux vulnérabilités l'aide de ServiceNow Intelligence prédictive. Ce module d'extension nécessite :

- Réponse aux vulnérabilités (com.snc.vulnerability)
- Intelligence prédictive (com.glide.platform_ml)

Pour en savoir plus, consultez Intelligence prédictive .

Scores de confiance

Utilisez l'application Recommandations d'affectation de vulnérabilité pour générer le score de confiance qui indique le niveau de confiance des groupes d'affectation recommandés pour les RT ou VI sélectionnés. Le score de confiance évalue si le système est sûr que le groupe d'affectation recommandé est adapté pour résoudre la vulnérabilité. Jusqu'à 10 recommandations s'affichent. Ces recommandations sont basées sur la probabilité la plus élevée de réussite. La première recommandation de la liste signifie que le système a le plus haut niveau de confiance dans le fait qu'il s'agit du bon groupe d'affectation.

Par exemple, sur une échelle de 0 à 100, pour chaque groupe d'affectation, le score de confiance suggère la probabilité qu'un VI ou un RT appartienne à ce groupe particulier.

Information associée

Intelligence prédictive

Créer et former une solution de classification

Créer et former une solution de similarité

Créer et former une solution de mise en grappe

Configuration de paramètres avancés pour vos solutions ML

Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces

Lorsque les données sont importées à partir d'une intégration tierce, Réponse aux vulnérabilités utilise automatiquement les données de l'hôte pour rechercher des correspondances dans le Base de données de gestion des configurations (CMDB). Pour ce faire, il utilise les **règles de recherche de CI**. Ces règles sont utilisées pour identifier les éléments de configuration (CI) et les ajouter à l'enregistrement d'élément vulnérable pour faciliter le rattrapage.

À partir de la version 19.0, accédez à **Security Operations** > **CMDB** > **Règles de recherche** pour localiser la liste dans votre instance.

Au fur et à mesure que les actifs sont importés, une recherche est d'abord effectuée sur la liste **des éléments détectés** à l'aide d'ID tiers afin de trouver des correspondances avec les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

éléments de configuration (CI) des importations précédentes. Lorsqu'une correspondance d'ID d'hôte est trouvée, elle est utilisée comme champ **d'élément de configuration** dans l'enregistrement de l'élément vulnérable.

Vous pouvez voir comment les actifs importés sont mappés aux CI à l'aide de la liste **des éléments détectés** . Si aucune correspondance n'est trouvée ou si le champ ID d'hôte est vide, les règles utilisent les autres informations de l'hôte pour tenter d'identifier correctement le CI. Si aucune correspondance n'est toujours trouvée, un CI d'espace réservé est créé et désigné comme **CI sans correspondance**. Consultez la rubrique Ci sans correspondance pour plus d'informations sur la façon dont ces CI sont gérés.

Les règles de recherche de CI peuvent être séparées par domaine et sont spécifiques à la source. Chaque source peut avoir plusieurs déploiements.

Remarque : Les règles de recherche de CI sont partagées par tous les déploiements de l'intégration de source de vulnérabilité. Si une règle est supprimée ou modifiée, la suppression ou les changements affectent tous les déploiements de l'intégration de vulnérabilité.

Lors d'une tentative de correspondance, la première étape consiste à rechercher un ID de fournisseur pour trouver une correspondance exacte entre la source, le source_instance et l'ID du fournisseur. Ensuite, les règles de recherche sont exécutées dans l'ordre, de la plus basse à la plus élevée, et s'arrêtent lorsqu'une règle ne renvoie qu'un seul CI comme correspondance. Si une règle est créée de telle sorte qu'elle renvoie plusieurs CI, seule la première correspondance est utilisée.

Remarque : Pour éviter la mise en correspondance sur des éléments de réseau de bas niveau, si un CI correspondant est l'un des dscy_switchport, cmdb_ci_network_adapter, cmdb_ci_nic ou cmdb_ci_ip_address, le CI parent est renvoyé.

Une propriété système permettant d'exclure des classes CI est disponible. Cette propriété n'est pas disponible avec la mise à niveau. Pour plus d'informations et d'instructions sur la mise à niveau, reportez-vous Ignorer les classes CI à la section Configurer la propriété.

Pour faciliter la recherche de problèmes correspondants, lorsqu'une correspondance est trouvée, la règle de recherche de CI utilisée pour la trouver est ajoutée à l'enregistrement d'élément détecté dans le champ de **règle de correspondance CI** . Les règles de recherche sont évaluées en fonction **de la valeur d'ordre** la plus faible en premier.

Les règles de recherche de CI sont fournies avec les modules d'extension d'intégration correspondants.

Voici quelques-unes des règles de recherche de Qualys CI :

- ID D'HÔTE QUALYS
- FQDN
- NetBIOS
- DNS
- IP

Voici quelques-unes des règles de recherche de Rapid7 CI :

- MacAddress
- FQDN

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Nom d'hôte
- IP

Voici quelques-unes des règles de recherche de CI Tenable.io :

- FQDN
- NETBIOS
- NOM D'HÔTE
- MacAddress
- DNS

Remarque : Les règles de recherche de CI Tenable.io classent par ordre de priorité et renseignent les valeurs d'interface réseau non vides (FDQN, IPV4 et MacAddress) par rapport aux valeurs FDQN, IPV4 et MacAddress normales d'un élément détecté. Lorsque ces valeurs d'interface réseau sont vides, les valeurs FDQN, IPV4 et MacAddress normales sont renseignées pour un élément détecté.

Voici quelques-unes des règles de recherche de CI Tenable.sc :

- MacAddress
- FQDN
- NETBIOS

Remarque : Une fois supprimées, les règles ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

L'importation de données de vulnérabilité peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer la correspondance dans peut entraîner de longs délais de CMDB traitement. Pour éviter toute dégradation potentielle des ressources ou toute complication des performances, testez toutes les règles de recherche de CI écrites sur mesure ou les modifications apportées aux **règles de recherche de CI prédéfinies**. Consultez Étapes pour empêcher les enregistrements dupliqués ou orphelins après l'exécution Réponse aux vulnérabilités de règles de recherche de CI pour plus d'informations sur la prévention des enregistrements orphelins en double, la suppression des données et le nettoyage des données.

Remarque : Pour plus d'informations sur la correspondance de CI, voir KB0998706 .

Réapplication des règles de recherche de CI mises à jour

Lorsque vous modifiez une règle de recherche de CI, cliquez sur **Appliquer les modifications** sur la page de liste Règles de recherche de CI pour réexécuter toutes les règles sur les éléments détectés qui :

- Ont été mis à jour et correspondent aux règles
- Ne correspondent à aucune règle

Si l'élément de configuration (CI) change après la réapplication des règles de recherche, les éléments détectés sont mis à jour avec le nouveau CI. Les détections impactées et les éléments vulnérables sont également mis à jour. Pour plus d'informations, consultez Réappliquer des règles de recherche de CI sur les éléments détectés sélectionnés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Matériel non classé

Si un actif ne trouve pas de correspondance dans les Base de données de gestion des configurations (CMDB) règles de recherche par CI, l'actif est qualifié de matériel non classé.

Lorsque les données sont importées à partir d'intégrations créées, Réponse aux vulnérabilités utilise automatiquement les données de ServiceNow l'hôte pour rechercher des correspondances dans le CMDB. Les règles de recherche de CI sont utilisées pour identifier les éléments de configuration (CI) et les ajouter à l'enregistrement d'élément vulnérable pour faciliter le rattrapage. Si les actifs sont introuvables dans le CMDB, le moteur Identification et rapprochement (IRE) exécute ses propres règles d'identification définies sur la classe de matériel et tous ses enfants et crée un CI dans une classe de matériel non classée. Lorsque Découverte cet actif est trouvé, au lieu de reclasser le matériel non classé existant, il crée un CI. Cela est dû au fait que la règle d'identification repose sur le nom du CI matériel.

Si le moteur Identification et réconciliation (IRE) est activé, l'option de reclassification à partir des éléments détectés n'est pas prise en charge.

Les extraits suivants montrent la charge utile IRE pour la création d'un CI dans un matériel non classé via Réponse aux vulnérabilités et Découverte respectivement.

```
"className": "cmdb_ci_unclassed_hardware",

"values": {
      "name": "asset01.company.com",//from NetBios,
      "mac_address": "1a:5e:2c:0e:42:f3",
      "fqdn": "asset01.company.com",
      "ip_address": "133.10.3.123"
   }

"settings": {
      "updateWithoutSwitch": true
   }
```

```
"className": "cmdb_ci_cmdb_ci_win_server"

"values": {
      "name": "asset01",
      "mac_address": "1a:5e:2c:0e:42:f3",
      "fqdn": "asset01.company.com",
      "ip_address": "133.10.3.123",
      "os_domain": "company"
   }

"settings": {
      "updateWithoutSwitch": false
   }
```

Dans ce cas, le CI matériel non classé existant n'est pas reclassé vers le serveur Windows, mais un nouveau CI sous le serveur Windows est créé. La raison en est que la règle d'identification repose sur le nom du CI matériel. Si vous remarquez les charges utiles, le nom dans la charge utile à partir de Réponse aux vulnérabilités est le même que FQDN/NETBIOS, mais il s'agit simplement du nom d'hôte pour la charge utile à partir de Découverte.

Information associée

Reclassifier le matériel non classé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ci sans correspondance

Les éléments de configuration (CI) sont automatiquement mis en correspondance avec les CI lors de leur Base de données de gestion des configurations (CMDB) importation. Par défaut, le paramètre **Security Operations** > **CMDB** > **Éléments détectés** Le module répertorie ces éléments de configuration sans correspondance.

Si vous pensez qu'un CI sans correspondance appartient à une classe existante dans la CMDB, passez en revue vos règles de recherche de CI. Sinon, envisagez de reclassifier l'élément de configuration.

Remarque : Le filtre par défaut de cette liste est défini sur **Sans correspondance**. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Si le moteur Identification et réconciliation (IRE) est activé, l'option de reclassification à partir des éléments détectés n'est pas prise en charge.

Information associée

- Afficher et reclasser les éléments de configuration sans correspondance
- Rapprocher les éléments détectés sans correspondance
- Étapes pour empêcher les enregistrements dupliqués ou orphelins après l'exécution Réponse aux vulnérabilités de règles de recherche de CI
- Déduplication des éléments de configuration existants

Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation

Vous pouvez créer des éléments de configuration (CI) à l'aide de l'API Base de données de gestion des configurations (CMDB) du moteur Identification et réconciliation (IRE). En utilisant l'API IRE pour créer des CI, vous pouvez empêcher la création de CI en double et vous pouvez rapprocher les attributs de CI en autorisant uniquement les sources de données de référence à écrire CMDB.

Une classe CI (table) est le nom de table d'origine dans la base de données d'instance. CMDB contient des classes système de base qui stockent des données sur les CI.

Utilisation d'IRE pour la création de CI

Réponse aux vulnérabilités Avant la version v12.2, si aucun CI correspondant n'était trouvé dans la liste des éléments détectés ou CMDB, un CI était créé dans la classe de CI sans correspondance (sn_sec_cmn_unmatched_ci). Pour plus d'informations, voir CI sans correspondance.

À partir de la version 24.0.6 du Réponse aux vulnérabilités, si IRE rencontre des exceptions qui empêchent la création de CI, les spécificités de ces exceptions sont enregistrées dans le champ Information supplémentaire. En examinant les détails de ce champ, vous pouvez déterminer la cause première et implémenter les corrections nécessaires pour vous assurer que le CI est créé avec succès.

Réponse aux vulnérabilités De la version 12.2 à la version 18.0, si aucune correspondance n'est trouvée lors de l'application des règles de recherche de CI, les informations sur l'actif sont envoyées à IRE et un CI est créé dans l'une des classes `Matériel non classé` et `Adresse IP incomplète des appareils identifiés`. À partir de la Réponse aux vulnérabilités version 18.0, une nouvelle classe, `Cloud Resource` est également incluse. Pour plus d'informations sur la configuration de la catégorisation des ressources cloud sans correspondance dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

CMDB Classes CI

Remarque : Pour utiliser les nouvelles classes, activez le module d'extension Modèles de CMDB classe CI. Dans le cas contraire, les CI sont créés dans la classe de CI sans correspondance.

Si l'hôte que vous avez importé à partir d'un scanner tiers est introuvable dans la liste des éléments détectés ou CMDB, il est créé dans l'une des nouvelles CMDB classes de CI suivantes.

CMDB Classes CI

CMDB Classe CI	Description
Adresse IP incomplète de l'appareil identifié (*cmdb_ci_incomplete_ip*)	Le CI est créé dans cette table si seule l'adresse IP est disponible dans les informations hôte reçues du scanner.
Matériel non classé (*cmdb_ci_unclassed_hardware*)	Le CI est créé dans cette table si l'une des informations suivantes est disponible dans les informations hôtes reçues du scanner : • Nom d'hôte • Adresse IP • DNS • NETBIOS • Adresse MAC **Remarque :** Si l'adresse MAC est disponible, l'entrée de carte réseau est créée et associée au CI matériel non classé. Si les adresses IP et MAC sont disponibles, le CI d'adresse IP est également créé et associé au CI matériel non classé.
Ressource du cloud (*cmdb_ci_cmp_resource*)	Le CI est créé dans cette table s'il *Cloud Resource ID* est disponible dans les informations hôtes reçues du scanner. **Remarque :** Si le Type d'actif d'une intégration d'analyse est *Hybride* et que la *sn_sec_cmn.unmatched_cloud_resource_enabled* propriété système est définie sur faux, les CI sont créés dans la classe *Matériel non classé* , mais pas dans la classe *Ressource* cloud.

Si le moteur Identification et réconciliation (IRE) est activé, l'option de reclassification à partir des éléments détectés n'est pas prise en charge.

Le système utilise automatiquement une classe CI sans correspondance si l'une des situations suivantes se produit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le module d'extension CMDB Classe CI n'est pas activé.
- IRE émet une exception lors de la création d'un CI.

Pour plus d'informations, voir CI sans correspondance.

Information associée

Application de stockage CMDB CI Class Models

Moteur Identification et réconciliation (IRE)

Mise à jour de la classe CI pour les actifs cloud sans correspondance

Réponse aux vulnérabilités À partir de la version 20.0, vous pouvez classer les actifs cloud sans correspondance des scanners , Rapid7 et Tenable dans *Matériel non classé* à l'aide de Qualys la *sn_sec_cmn.unmatched_cloud_resource_enabled* propriété système.

Cette propriété système dont la valeur par défaut est false est fournie avec le système de base. Il classe les actifs cloud sans correspondance dans une classe *de matériel* (*cmdb_ci_unclassed_hardware*) ou *de ressource dans le cloud* () non classée (*cmdb_ci_cmp_resource*) pour les intégrations qui intègrent à la fois des actifs d'infrastructure et des actifs cloud.

Réponse aux vulnérabilités À partir de la version 20.0, la colonne Type d'actif est ajoutée dans la table Intégrations tierces (sn_sec_int_integration) pour identifier les intégrations qui prennent en charge à la fois l'infrastructure et les actifs cloud. La colonne Type d'actif contient la valeur *Hybride* pour les scanners qui intègrent à la fois des actifs d'infrastructure et des actifs cloud. Par exemple, Qualys les intégrations , Rapid7 et Tenable ont la valeur *Hybride* dans la colonne Type d'actif.

- Pour les nouvelles installations de Réponse aux vulnérabilités la version 20.0 et supérieure, tous les actifs cloud sans correspondance sont classés dans les catégories suivantes :
  - *Classe de matériel non classée* par défaut.
  - *Classe des ressources dans le cloud* , si vous changez la *sn_sec_cmn.unmatched_cloud_resource_enabled* propriété système sur true.
- Pour les mises à niveau vers la Réponse aux vulnérabilités version 20.0 :
  - Si la classe de *ressources cloud* contient des actifs, la propriété système *sn_sec_cmn.unmatched_cloud_resource_enabled* est définie sur vrai afin que les actifs cloud sans correspondance continuent de s'ajouter à la classe de *ressources cloud* (*cmdb_ci_cmp_resource*).
  - Dans le cas contraire, la propriété système *sn_sec_cmn.unmatched_cloud_resource_enabled* est définie sur faux, de sorte que les actifs cloud sans correspondance sont classés dans la classe *Matériel non classé* .

Remarque : Si vous modifiez la valeur de la *sn_sec_cmn.unmatched_cloud_resource_enabled* propriété système, assurez-vous de supprimer les éléments de configuration sans correspondance dans la classe CI précédemment ciblée et réappliquez les règles de recherche. Pour en savoir plus sur la suppression des CI existants et la réapplication des règles de recherche de CI afin que les nouveaux CI soient créés dans la bonne classe, consultez KB1533376 .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Éléments détectés

Les actifs sont automatiquement mis en correspondance avec les éléments de configuration (CI) lorsqu'ils Base de données de gestion des configurations (CMDB) sont importés à **l'aide des règles de recherche de CI**. Les éléments détectés vous donnent une visibilité sur la façon dont l'identification des actifs est mappée sur les CI dans le CMDB.

Les éléments détectés sont considérés comme **ayant une correspondance**, **sans correspondance** ou **reclassés**. Les CI identifiés sont dans l'état **Correspondance** .

Pour faciliter la recherche de problèmes de correspondance potentiels, la règle de recherche de CI correspondant au CI apparaît dans le champ Règle de **correspondance de CI** .

Par défaut, le paramètre **Security Operations** > **CMDB** > **Éléments détectés** Le module répertorie les éléments de configuration sans correspondance Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour obtenir une description des champs dans les éléments détectés, reportez-vous à la section Champs du formulaire Éléments détectés. Pour plus d'informations sur le rapprochement des éléments détectés sans correspondance et sur la réapplication de règles de recherche de CI sur les éléments détectés sélectionnés, consultez Rapprocher les éléments détectés sans correspondanceRéappliquer des règles de recherche de CI sur les éléments découverts sélectionnés et respectivement.

Changements de CI pour les éléments détectés

Lorsqu'un élément de configuration (CI) sur un élément détecté (DI) change, les détections impactées et les éléments vulnérables (VI) sont mis à jour. Le score de risque, les règles d'affectation, les règles de groupe et la règle de cible de rattrapage sont réévalués.

À partir de la version 24.0.6 de , vous pouvez afficher les mises à jour d'un Réponse aux vulnérabilités CI dans la table Élément détecté. Les informations, y compris le CI précédent, le CI mis à jour et l'utilisateur qui a effectué les changements, sont documentées dans la liste connexe Historique des audits.

Si un VI existe avec la même vulnérabilité et le même CI, les détections sont mises à jour avec le VI existant et le VI actuel est fermé avec le sous-état de CI non valide. Des notes de travail sont ajoutées pour les raisons suivantes :

- Lorsque les détections sont déplacées d'un VI à un autre.
- Lorsqu'un VI en double est fermé.

Si vous ne souhaitez pas mettre à jour le CI pour le VI existant, définissez la propriété sn_sec_cmn.update_on_ci_change sur faux. Ensuite, lorsqu'un CI change, un nouvel élément vulnérable est créé et l'élément existant est fermé en tant que CI non valide.

La valeur par défaut de la propriété sn_sec_cmn.update_on_ci_change est vrai.

Réévaluation des éléments détectés

Lorsque de nouvelles données sont reçues sur un élément détecté, l'élément détecté n'est pas immédiatement réévalué. Lors de la réception de *`true`* nouvelles données, l'option *`reevaluate_ci`* est définie sur Par défaut.

La tâche *`Re-apply CI Lookup Rules on the Changed Discovered items`* planifiée évalue tous les éléments détectés dont les données sources sont en cours de modification par le scanner. Il retraite à nouveau les éléments détectés et met à jour les éléments

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérables associés à l'élément détecté dont les données sources sont modifiées. La valeur de cette tâche planifiée est *On Demand* par défaut.

Remarque : Vous pouvez également choisir d'exécuter cette tâche planifiée quotidiennement. Pour plus d'informations sur le mode d'initiation de cette tâche, la fréquence de la tâche et l'affichage du nombre d'enregistrements qu'elle traite, consultez KB1695110 Réponse aux vulnérabilités : réappliquer des règles de recherche de CI sur les éléments découverts modifiés .

Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables

Avec l'application Réponse aux vulnérabilités , vous pouvez utiliser le modèle d'état pour voir l'état d'une tâche de rattrapage, à un moment donné. Savoir comment chaque état est lié et s'affecte les uns les autres vous aide à déterminer quand et comment corriger vos éléments vulnérables (VI).

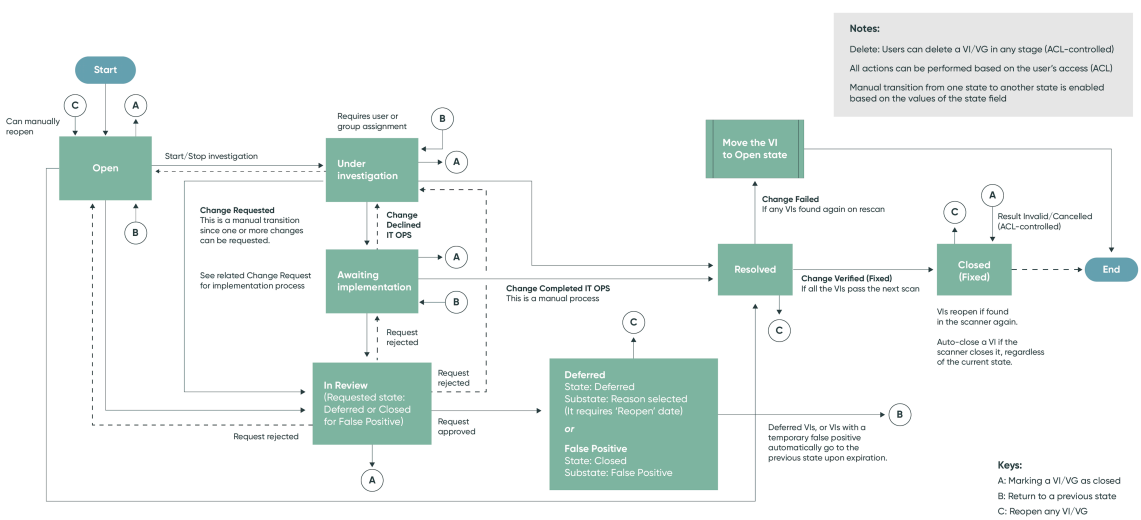
États des tâches de rattrapage

Les cas d'utilisation complexes peuvent parfois entraîner un élément vulnérable dans un état différent de celui de sa tâche de rattrapage. Comprendre le fonctionnement des états permet d'expliquer ce comportement et peut aider à créer des tâches de rattrapage et à créer ou modifier des règles de tâche de rattrapage.

Remarque : À partir de la version 23.0 de , le workflow Approbation de Réponse aux vulnérabilités**l'état de l'élément vulnérable** est déconseillé et remplacé par le changement d'approbation de l'état de vulnérabilité de flux dans le concepteur de flux.

Les tâches de rattrapage ont de nombreux états possibles, comme illustré dans le diagramme suivant.

Flux d'état de Vulnerability Response



Remarque : Chaque formulaire de tâche contient des boutons **Suivre** et **Mettre à jour** standard pour ServiceNow les tâches.

Pour plus d'informations sur les états de la tâche de rattrapage et les actions que vous pouvez effectuer sur celle-ci à un état respectif, reportez-vous à la section Réponse aux vulnérabilités États des tâches de rattrapage.

Pour plus d'informations sur les détections, les tâches de rattrapage et les états des éléments vulnérables, reportez-vous à la section Détections, tâches de rattrapage et états des éléments vulnérables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les états des tâches et des VI de rattrapage, reportez-vous à la section Tâches de rattrapage et états des éléments vulnérables.

Pour plus d'informations sur l'état de la tâche de rattrapage pour les VI de plusieurs groupes, reportez-vous à la section État de la tâche de rattrapage pour les éléments vulnérables (VIT) dans plusieurs groupes.

Calcul et affichage de l'âge de l'élément vulnérable

L'âge des éléments vulnérables (VI) est affiché dans l'application Réponse aux vulnérabilités avec plus de détails.

L'âge de l'élément vulnérable (EV) est affiché au format Jours/Heures/Minutes dans la colonne Âge de la vue de liste Éléments vulnérables et dans les champs Âge et Âge fermé des enregistrements de VI (VIT). L'âge affiché en chiffres plus significatifs peut vous aider à effectuer les activités suivantes avec plus de précision :

- Configurez des règles dans le module Règles de suppression automatique pour cibler et supprimer des enregistrements de VI spécifiques par jour/heures/minutes. Supprimer des enregistrements avec plus de précision peut augmenter vos performances, surtout si vous avez un grand nombre d'enregistrements de VI dans votre instance.
- Affichez les rapports avec des détails plus spécifiques dans Analyse des performances de l'application Réponse aux vulnérabilités .
- Créez des filtres qui identifient uniquement les VI souhaités.
- Élaguez les vues de listes pour afficher uniquement les VI souhaités.
- Remonter pas à pas plus facilement.

Une tâche planifiée a calculé l'âge et mis à jour tous les VI actifs. Dans les instances comportant un grand nombre d'enregistrements de VI, ce processus peut être lent et avoir un impact négatif sur les performances. L'âge VI est calculé plus efficacement à la demande et affiché avec des chiffres plus significatifs avec une colonne Âge améliorée. La colonne Âge améliorée est automatiquement ajoutée lorsque vous installez ou mettez à niveau l'application Réponse aux vulnérabilités .

Remarque : Si vous effectuez une mise à niveau et que l'âge du VI n'est pas affiché dans la vue de liste Éléments vulnérables et dans les champs Âge et Âge fermé des enregistrements de VI actifs (VIT) au format Jours/Heures/Minutes (9 jours, 18 heures, 29 minutes), la colonne d'âge n'est pas à jour dans votre instance. Pour en savoir plus sur la résolution de ce problème après une mise à niveau, reportez-vous à la rubrique KB0749231 .

La colonne et les champs d'âge ne sont pas modifiables. Un gestionnaire des vulnérabilités disposant de l'autorisation sn_vul.vulnerability_read ou du profil administrateur de vulnérabilité peut afficher cette valeur, et les propriétaires de rattrapage informatique disposant du rôle sn_vul.remediation_owner peuvent l'afficher sur les enregistrements qui leur sont affectés.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

L'âge VI est affiché comme illustré dans les images suivantes.

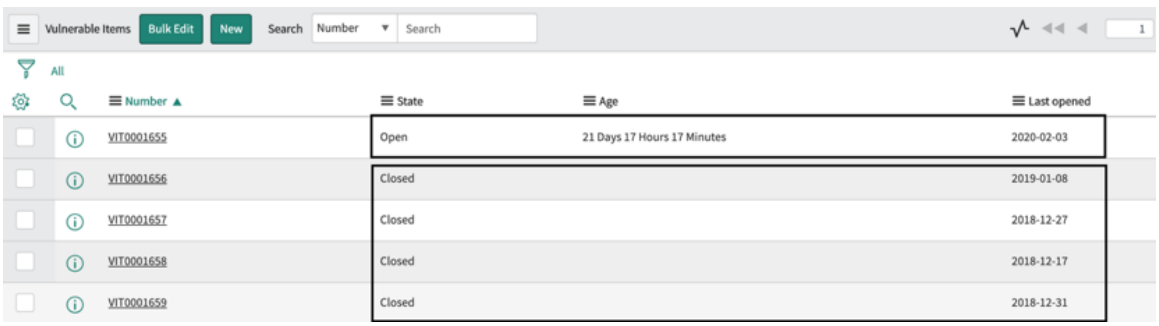
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste des éléments vulnérables

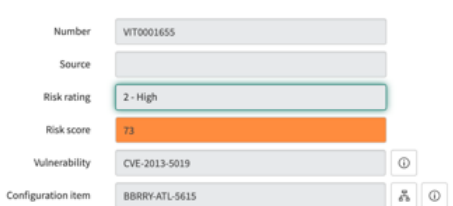
Comme le montre la figure suivante, dans la vue de liste Éléments vulnérables, l'âge est affiché dans la colonne Âge en jours/heures/minutes (21 jours 17 heures 17 minutes) uniquement pour les VI actifs. Les VI actifs sont des VI dans un état autre que « Fermé ». Cette valeur d'âge représente le nombre de jours pendant lesquels le VI a été actif.

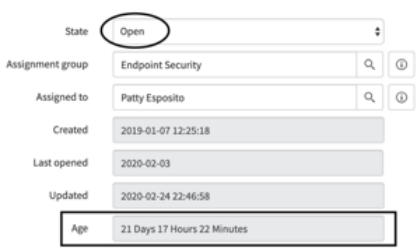
L'âge n'est pas affiché pour les VI à l'état « Fermé ». Pour les VI précédemment dans un état « Fermé », puis rouverts, la valeur représente le nombre de jours pendant lesquels le VI a été actif depuis la date de sa dernière ouverture.



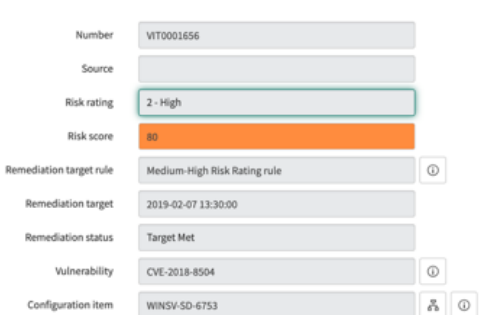
Âge sur les enregistrements de VI

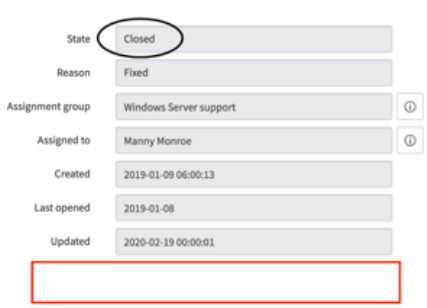
Sur les enregistrements de VI, la valeur de la colonne Âge dans la vue de liste est visible pour les VI actifs dans le champ Âge.





La valeur de la colonne Âge ne s'affiche pas pour les enregistrements VI à l'état « Fermé ».





Âge sur la liste des éléments vulnérables et les enregistrements de VI lorsqu'un VI est mis à jour

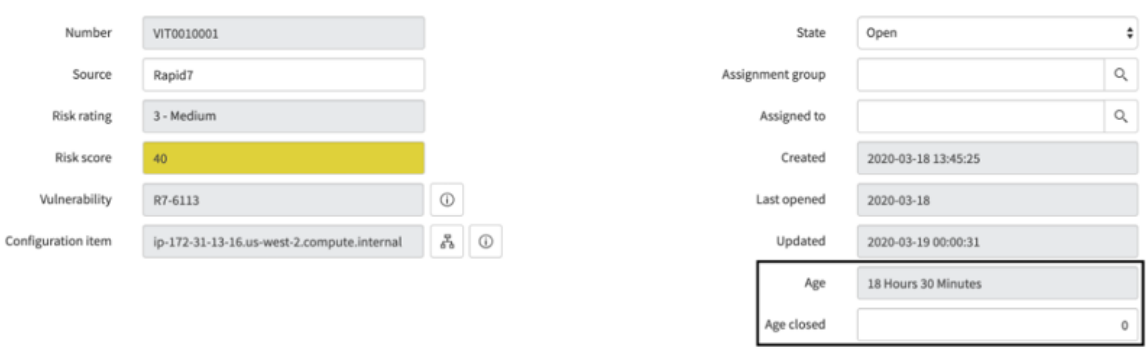
Lorsqu'un VI est à l'état « Fermé », le champ Âge n'est pas affiché. Lorsque le VI passe à « Fermé », la valeur en nombre de jours de la colonne Âge s'affiche dans le champ Âge fermé (9), comme illustré dans la figure suivante. Cette valeur représente le nombre de jours pendant lesquels le VI était actif avant de passer à « Fermé ». Par exemple, dans l'image suivante, ce VI a été actif pendant 9 jours, 18 heures et 29 minutes, mais seul le nombre de jours (9) est affiché sur l'enregistrement Fermé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Si ce VI est rouvert, lorsque l'état du VI revient à « Ouvert », le champ Âge fermé est remis à 0. Étant donné que le VI est à nouveau actif, l'âge en jours/heures/minutes est affiché dans la vue de liste dans la colonne Âge et dans le champ Âge du VIT.



Pour plus d'informations sur la personnalisation des calculs d'âge et d'âge fermé, consultez l'article KB1703270 .

Suppression des affectations des éléments vulnérables et des tâches de rattrapage

Vous pouvez effacer les champs **Affecté à** et **Groupe d'affectation** des éléments vulnérables directement à partir des enregistrements d'élément vulnérable et de tâche de rattrapage que vous déterminez comme susceptibles d'être incorrectement affectés à vous ou à vos groupes.

Vue d'ensemble du workflow

Les propriétaires de rattrapage et les analystes de vulnérabilité peuvent effacer les champs **Affecté à** et **Groupe d'affectation** et mettre à jour les enregistrements à réaffecter avec l'action d'interface utilisateur **Annuler l'affectation** .

Cas d'utilisation

Si vous déterminez que des enregistrements ne se trouvent pas dans votre périmètre pour le rattrapage, ou si vous pensez qu'ils vous ont été affectés de manière incorrecte ou ont été affectés à vos groupes, vous pouvez vous supprimer ou supprimer vos groupes des champs **Affecté à** et **Groupe d'affectation** sur les enregistrements d'élément vulnérable et de tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'action d'interface utilisateur Annuler l'affectation et le menu Plus d'options

Vous pouvez **annuler l'affectation** des enregistrements suivants avec une action d'interface utilisateur ou à partir du menu Autres options () dans un état autre que Fermé ou Résolu :

- Tâches de rattrapage (VUL, AVUL ET CVUL) dans l'environnement classique comme dans les espaces de travail.

  Si une tâche de rattrapage est mise à jour avec cette fonctionnalité, les champs **Affecté à** et **Groupe d'affectation** sur tous ses VIT associés qui ont les mêmes groupes d'affectation sont également effacés.

  Remarque : Si un VIT, AVIT ou CVIT d'une tâche de rattrapage a un groupe d'affectation différent de celui de sa tâche de rattrapage, il n'est pas désaffecté. Dans la plupart des cas, ces éléments vulnérables ont été affectés manuellement.

- Éléments vulnérables (VIT, AVIT et CVIT) dans l'environnement classique et les espaces de travail.

Tous les enregistrements pour lesquels vous mettez à jour les affectations avec l'action d'interface utilisateur ou manuellement s'affichent dans le module Non affecté sous leurs modules de produit respectifs.

Pour connaître les étapes permettant d'effacer les champs **Affecté à** et **Groupe d'affectation** sur les enregistrements avec l'action d'interface utilisateur, consultez Supprimer les affectations des éléments vulnérables et des tâches de rattrapage pour plus d'informations*Unassigned*.

Propriété système et notifications

Si vous sélectionnez **Annuler l'affectation** sur un enregistrement, par défaut, la *sn_vul.unassign_vr.approval_required* propriété système and déclenche le flux d'approbation et crée un enregistrement d'approbation de changement d'état à l'état Révision et une demande d'approbation est émise pour l'approbateur qui s'affiche dans la liste **Mes approbations** .

Remarque : En tant qu'administrateur de vulnérabilité [sn_vul.vulnerability_admin], vous pouvez définir la *sn_vul.unassign_vr.approval_required* propriété système sur **false** pour désactiver le processus d'approbation.

- Si la demande est approuvée, *sn_vul.default_assignment_group* efface les champs **Affecté à** et **Groupe d'affectation** et renseigne le champ **Type d'affectation** avec **Non affecté**. En tant qu'administrateur de vulnérabilités, vous pouvez modifier la valeur de la *sn_vul.default_assignment_group* propriété système afin que les champs d'affectation soient effacés et qu'un groupe spécifique soit ensuite affecté. Par exemple, si un utilisateur clique sur **Annuler l'affectation** d'un enregistrement et que vous souhaitez le rediriger vers un groupe spécifique pour révision, vous pouvez ajouter un ID système pour le groupe de votre choix dans le champ Valeur de la propriété système.

  Remarque : Si vous modifiez cette valeur, les notifications pour tous les VIT, AVIT et CVIT qui ne sont pas affectés sont envoyées au groupe que vous spécifiez.

- Si votre demande est rejetée, le motif est affiché dans l'onglet **Notes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sinon, si n'est `sn_vul.default_assignment_group` pas configuré pour un groupe spécifique, par défaut, les utilisateurs que vous ajoutez au groupe d'utilisateurs de notification Désaffecter sont alertés lorsque des enregistrements sont désaffectés. La `sn_vul.default_assignment_group` propriété système détermine les notifications à ce groupe.

Le type d'affectation, qu'il soit **Manuel**, **Règle** ou **Non affecté**, est disponible dans les enregistrements VIT et la vue de liste. Le type d'affectation **non affecté** s'affiche dans les enregistrements après que la propriété système a désactivé les champs **Affecté à** et **Groupe d'affectation** .

Consultez pour Approuver ou rejeter une demande de désaffectation dans Réponse aux vulnérabilités plus d'informations sur l'approbation des demandes.

Surveillance de vos règles d'affectation avec la tâche planifiée pour cette fonctionnalité

Une tâche planifiée quotidienne compte les enregistrements lorsqu'elle passe au type d'affectation **Non affecté** . Avec ce nombre, les analystes de vulnérabilité peuvent surveiller et ajuster toutes les règles d'affectation susceptibles de ne pas fonctionner correctement en fonction des règles d'affectation qui ont un nombre plus élevé de VI non affectés.

La `Reassignment count for assignment rules` tâche planifiée s'exécute quotidiennement et publie le nombre total de VI désaffectés par cette fonctionnalité pour une règle d'affectation particulière.

Les dénombrements recueillis par cette tâche s'appliquent aux éléments vulnérables et aux règles d'affectation uniques pour Réponse aux vulnérabilités et Réponse aux vulnérabilités des applications. Les nombres sont affichés par règle d'affectation dans chaque liste de règles d'affectation pour chaque module.

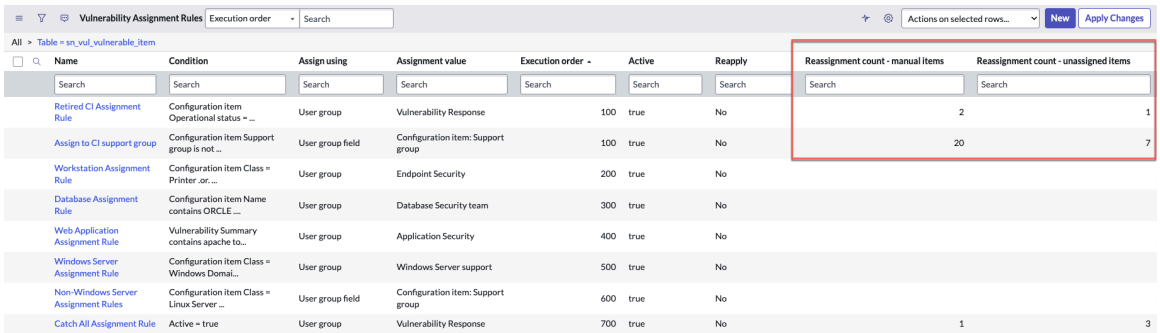
La tâche compte également tous les enregistrements qui ne sont pas affectés manuellement. Les décomptes manuels et les décomptes collectés par cette fonctionnalité sont publiés dans la liste Règles d'affectation de vulnérabilité dans deux colonnes : `Reassignment count - manual items` et `Reassignment count - unassigned items`.

1. En tant qu'administrateur des vulnérabilités, pour afficher ces nombres, accédez à **Réponse aux vulnérabilités** > **Administration** > **Règles d'affectation**.
2. Cliquez sur l'icône en forme d'engrenage dans l'angle supérieur droit de la liste, puis sélectionnez , et `Reassignment count - unassigned items` pour l'affichage`Reassignment count - manual items`.
3. Tout élément vulnérable initialement affecté par une règle, mais réaffecté automatiquement ou manuellement par la suite, contient une référence à la règle d'origine dans la vue de liste.

L'exemple suivant montre les nombres de réaffectations pour deux règles d'affectation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité

Les calculateurs de vulnérabilité automatisent le calcul des valeurs initiales pour les champs des éléments vulnérables. La condition de chaque calculateur est évaluée dans l'ordre, et le premier calculateur correspondant est utilisé.

Calculateurs de vulnérabilités

Le Réponse aux vulnérabilités système de base comprend deux calculateurs de vulnérabilité qui définissent le **score de risque** de base sur l'élément vulnérable.

- **Calculateur de risque par défaut**
- **Gravité de la vulnérabilité**

Les calculateurs de vulnérabilité peuvent être créés pour hiérarchiser et évaluer l'impact des éléments vulnérables en fonction de n'importe quel critère à l'aide de filtres de condition. Qu'il s'agisse de l'impact de la vulnérabilité sur l'entreprise, de la classe de l'élément de configuration (CI) ou de l'âge de l'élément vulnérable, vous pouvez créer des calculateurs de vulnérabilité supplémentaires pour définir d'autres champs sur les éléments vulnérables. Vous pouvez également personnaliser les calculateurs de vulnérabilité existants. Une calculatrice peut être rédigée pour refléter n'importe quel ensemble de priorités. Voir Créer un Réponse aux vulnérabilités calculateur et Filtrage au sein de Réponse aux vulnérabilités pour plus d'informations.

En outre, vous pouvez utiliser des attributs dans le configuration_item [cmdb_ci] dans la Base de données de gestion des configurations (CMDB) pour vous aider à créer une logique pour vos calculateurs de risque de Vulnerability Response. Si, par exemple, vous déterminez que les CI orientés vers l'extérieur de votre organisation sont plus vulnérables et peuvent nécessiter une correction immédiate, vous pouvez affecter des attributs tels que `Internet Facing` pour ces CI. Cet attribut, ainsi que d'autres, sont répertoriés dans les notes de version de Common Service Data Model . Pour obtenir des renseignements et des conseils à jour sur le CMDB, consultez les rubriques suivantes :

- Modèle conceptuel du modèle de données de service commun
- Modèle de schéma CMDB
- Réponse aux vulnérabilités : calcul du score de risque (KB1169927)

Chaque calculateur contient une liste de règles du calculateur, avec une condition déterminant quand l'appliquer. Lorsque le calculateur est exécuté, la condition de chaque règle est évaluée dans l'ordre et la première règle correspondante est utilisée.

Le calculateur de gravité de la **vulnérabilité** calcule le **score de risque** pour les éléments vulnérables en utilisant la gravité de vulnérabilité normalisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Un seul calculateur par champ cible (**score de risque**) peut être actif à la fois. **La gravité de la vulnérabilité** est désactivée par défaut.
- Chaque fois que le score de risque est mis à jour sur un VIT, la section **Notes** est mise à jour avec les détails suivants :
  - Nom du groupe de calculateurs
  - Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre crochets. Pour modifier ou afficher la base de la règle du calculateur, cliquez sur une règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. Si Modèle est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si Script est sélectionné, vous pouvez ajouter ou mettre à jour le script existant.

    La propriété *sn_sec_cmn.risk_score_changes_add_worknotes* système permet de renseigner la section des notes de travail. À partir de la version 25.0.3 de Réponse aux vulnérabilités, la propriété système est inactive par défaut. Si vous l'activez, vous pouvez alors seulement voir tous les changements liés au score de risque.

Tous les calculateurs de vulnérabilité activés définissent les champs sélectionnés chaque fois qu'un élément vulnérable est créé, lorsqu'un CI ou une vulnérabilité associé change ou lorsque le lien connexe **Calculer le score de risque** d'un élément vulnérable est utilisé. Par exemple, le score de risque est automatiquement mis à jour sur les enregistrements d'éléments vulnérables lorsque la valeur de gravité est mise à jour sur une vulnérabilité importée. Une fois qu'une importation de vulnérabilité a mis à jour un score de vulnérabilité, le marqueur recalculer est activé pour cette vulnérabilité. Les scores de risque pour les éléments vulnérables pour lesquels le marqueur de recalcul est activé (vrai) avec cette vulnérabilité sont recalculés.

À partir d'un élément vulnérable existant, si vous cliquez sur le lien connexe **Calculer le score de risque** et que l'un des calculateurs est activé, le champ Score de **risque** de l'élément vulnérable est mis à jour.

Remarque :

- Le lien connexe **Calculer le score de risque** n'est visible que lorsqu'au moins un calculateur de vulnérabilité est activé.
- Vous pouvez mettre à jour le score de risque d'un élément vulnérable dans le et Espace de travail de remédiation IT en sélectionnant le bouton **Calculer le score de risque** dans sa vue d'enregistrement.Espace de travail du gestionnaire de vulnérabilités
- Chaque fois que le score de risque d'un VIT change, les détails suivants sont documentés dans la section Notes du VIT :
  - Nom du groupe de calculateurs
  - Nom du calculateur
  - Valeurs des champs avec leur pondération et leur contribution au score de risque
  - Score de risque final

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règle du calculateur de vulnérabilité

Le calculateur du système de base **Calculateur de risque par défaut** contient la règle**Règle de risque par défaut**, une règle de calcul de vulnérabilité spécialisée appelée **règle de risque**. Il calcule le **score de risque** en fonction de plusieurs valeurs :

- Gravité de la vulnérabilité
- Informations sur l'exploitation
- Criticité
- Exposition externe du CI avec la vulnérabilité
- Scores de l'EPSS

Vous pouvez ajuster les valeurs à utiliser dans la **règle de risque par défaut** et le poids à donner à chacune de ces valeurs. Les poids sont utilisés pour ajuster le nombre de chaque élément lors de la définition du **score de risque** de base.

Vous pouvez personnaliser les critères de la règle de risque par défaut. Pour plus d'informations, consultez Définir les champs et les poids de la règle de risque pour les calculateurs de risque de Vulnerability Response.

Pour obtenir un exemple sur la façon dont les scores de risque sont déterminés pour les calculateurs de règles de risque, reportez-vous à la section Exemple de calcul de score de risque pour Réponse aux vulnérabilités.

Affectation d'un pourcentage de pondération

Vous pouvez également affecter un pourcentage de pondération (0-100) au niveau de la valeur du champ. Par exemple, vous pouvez affecter un pourcentage de pondération à chaque niveau de gravité (Aucun à Critique).

Si la pondération de gravité est de 50 pour la règle de risque, et que les valeurs de pondération suivantes sont affectées au niveau de gravité :

Gravité de la vulnérabilité	Score du risque
Critique	100
Élevé	50
Moyen	20
Aucun	0

Si la gravité est critique, la pondération équivalente est 50. Si la gravité est élevée, la pondération équivalente est 25, et si la sévérité est moyenne, la pondération équivalente est 10. Si la gravité est Aucune, la pondération équivalente est 0. Pour plus d'informations, reportez-vous à la section Exemple de calcul de score de risque pour Réponse aux vulnérabilités.

Paramètres des règles du calculateur de vulnérabilité

Chaque règle a un paramètre **d'ordre** . Toutefois, le premier à correspondre aux conditions met à jour le champ de **score de risque** de l'élément vulnérable. Pour en savoir plus sur les paramètres des règles du calculateur de vulnérabilité, reportez-vous à la section Créer un Réponse aux vulnérabilités calculateur. Les règles de calculateur non scriptées ont généralement un impact moindre sur les performances que les règles de calculateur scriptées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le calculateur de **gravité de la vulnérabilité** du système de base contient des règles de calcul qui attribuent à chaque niveau de gravité (Aucun à Critique) une valeur (0-100) pour le **score de risque** en fonction de la gravité. Un score de **risque de 100** est automatiquement affecté à la gravité inconnue. Ces valeurs peuvent être ajustées et, comme le **calculateur de risque par défaut**, de nouvelles règles de calcul ou de nouvelles règles de risque peuvent être créées.

Poids du score de risque de vulnérabilité

Toutes les vulnérabilités se voient attribuer un score de risque et une cote de risque en fonction de facteurs tels que la gravité, la criticité, les informations sur l'exploitation, et ainsi de suite. La règle *`Update Risk Rating from Risk Score`* métier de la table des éléments vulnérables est responsable du calcul de la cote de risque. Chaque fois que le score de risque change, la cote de risque est calculée et renseignée pour les éléments vulnérables.

Valeur (cote de risque)	Poids (score de risque)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

- Les types de cote de risque sont expédiés dans la table de base sous forme de vr_risk_rating. Ces types sont transmis dans le cadre de la règle métier sur chaque table où la cote de risque est calculée.
- Le script a été modifié afin que vous puissiez interroger les entrées des valeurs de la table Poids du score de risque pour le calcul de la cote de risque.
- Ajoutez des entrées supplémentaires pour un type existant ou créez-en un nouveau. Lorsque vous créez un nouveau type, assurez-vous d'ajouter les étiquettes pour la nouvelle cote de risque et de modifier les scripts et les règles métier associés. Vous devez également ajouter un nouveau style pour le nouveau score de risque.
- Modifiez le script pour interroger les enregistrements dans la table de base.

Vous pouvez accéder à la table des pondérations des scores de risque en saisissant sn_sec_cmn_risk_score_weight dans le navigateur de filtre.

En outre, le score de risque est automatiquement recalculé lorsque les vulnérabilités et expositions communes (CVE) ou les entrées tierces (TPE) associées sur les éléments de vulnérabilité (VI) sont liées à une vulnérabilité d'exploitation connue (KEV) CVE.

Intégration des vulnérabilités tenable et règle de risque tenable

La règle de risque tenable est disponible avec le Tenable Vulnerability Integration. L'évaluation de priorité de vulnérabilité (VPR) est un attribut du produit Tenable qui est importé et utilisé avec un nouveau calculateur de risque par défaut dans Réponse aux vulnérabilités. La règle de risque Tenable est installée avec l'application dans le Vulnerability Response integration with Tenable cadre du calculateur de risque par défaut dans les calculateurs de vulnérabilité de Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette règle de risque est désactivée par défaut. Consultez Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration.

Réponse aux vulnérabilités Détections d'éléments vulnérables à partir d'intégrations tierces

Affichez toutes les informations collectées par les analyses tierces dans votre ServiceNow AI Platform® instance. Affichez les résultats renvoyés des analyses sur les enregistrements de détection et d'éléments vulnérables (VI) dans votre instance tels que ces résultats sont affichés sur les scanners.

Vue d'ensemble

L'application Réponse aux vulnérabilités prend en charge les intégrations tierces qui récupèrent les données des éléments vulnérables de votre environnement d'entreprise. Les données détaillées sur les détections, c'est-à-dire les occurrences uniques et distinctes de vulnérabilités signalées par les analyseurs de vos intégrations tierces, sont importées et affichées sur les enregistrements de détection et les enregistrements d'éléments vulnérables de votre ServiceNow AI Platform instance.

Les intégrations tierces récupèrent les données de détection des éléments vulnérables. Les détections sont des occurrences distinctes de vulnérabilités telles que signalées par les scanners. Les données de détection sont associées aux éléments vulnérables et l'état du VI est mis à jour en fonction de l'état des détections. Si aucun VI n'est trouvé, un nouveau VI est créé. Les détections ne sont ouvertes ou fermées que par les données trouvées directement par un scanner.

Dans les versions précédentes des détections d'éléments Réponse aux vulnérabilités vulnérables, la relation entre un CI (actif) de votre environnement et une vulnérabilité importée à partir d'un scanner tiers créait un élément vulnérable unique dans votre ServiceNow AI Platform instance.

La granularité des données d'origine fournies par le scanner est préservée. Avec les détections, les données de détection sont associées à des éléments vulnérables. Lors d'une ingestion, un nouvel élément vulnérable est créé si aucun élément vulnérable n'est trouvé.

À partir de la version 21.1.2 de Réponse aux vulnérabilités, une propriété `sn_vul.show_last_open_detection` système est fournie dans le système de base. Par défaut, la valeur de cette propriété est définie sur faux, et le comportement actuel d'agrégation des valeurs de la détection initiale à l'élément vulnérable reste inchangé. Toutefois, s'il est défini sur vrai, un élément vulnérable est automatiquement mis à jour avec la dernière détection ouverte après une ingestion. Les champs tels que Adresse IP, SSL, Port, Protocole, NetBIOS et Preuve sont mis à jour pour les détections de VI. Si nécessaire, vous pouvez personnaliser les champs de détection qui doivent être mis à jour en modifiant le script DetectionBase .

Pour afficher les valeurs de la dernière détection ouverte, accédez à l'onglet **Dernière détection ouverte** sur la vue de formulaire VI. Pour mettre à jour tous les VI ouverts au cours de l'année écoulée avec les dernières valeurs de détection ouvertes, vous pouvez exécuter la tâche `Update Last Open Detection Value To VITs` planifiée sur demande. Cette tâche planifiée est également fournie dans le système de base.

Remarque : Lorsqu'un élément de configuration (CI) change sur un élément détecté, les mises à jour correspondantes sont également reflétées dans les détections. Par conséquent, les détections peuvent être déplacées d'un élément vulnérable à un autre. En fonction de ce changement et de la valeur de la `sn_vul.show_last_open_detection` propriété, les valeurs des détections sont déployées sur les VI source et cible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions prises en charge de Réponse aux vulnérabilités

Pour plus d'informations sur l'installation ou la mise à jour de l'application Réponse aux vulnérabilités , reportez-vous à la section Installer Réponse aux vulnérabilités.

Intégrations tierces prises en charge

Une intégration tierce prise en charge à votre Réponse aux vulnérabilités application est requise pour les détections d'éléments vulnérables. Les intégrations tierces suivantes sont prises en charge par l'application pour les Réponse aux vulnérabilités détections d'éléments vulnérables :

- Intégration de la détection d'hôte Qualys
- Entrepôt de données Rapid7 :
  - Intégration d'élément vulnérable
  - Intégration de résolution de l'élément vulnérable
- Intégration de résolution d'élément vulnérable Rapid7 (InsightVM)
  - Intégration de VM Aperçu
  - Intégration de l'élément vulnérable : API
- Tenable Vulnerability Integration
- Microsoft Defender Gestion des vulnérabilités

Ces intégrations tierces sont disponibles avec un abonnement distinct de .ServiceNow Store Pour plus d'informations sur ces intégrations, consultez Intégrations de Réponse aux vulnérabilités et Opérations de sécurité et le ServiceNow Store pour plus d'informations sur l'obtention d'une autorisation.

Pour vérifier que votre scanner tiers est configuré pour l'importation, reportez-vous aux rubriques Installer et configurer l'application Rapid7 Integration pour Security Operations et Installer Qualys Vulnerability Integration.

Termes clés pour les détections d'éléments vulnérables

Vulnérabilité

Données sur les faiblesses des logiciels, des systèmes d'exploitation et des actifs importés de sources internes et externes. Ces données sont importées et comparées aux actifs existants (éléments de configuration, CI) répertoriés dans la CMDB.

Élément vulnérable

Un élément vulnérable est créé ou mis à jour lorsqu'une vulnérabilité importée correspond à un CI dans la CMDB.

Détection

Une occurrence unique et distincte d'une vulnérabilité signalée par un scanner appelée détection d'élément vulnérable dans l'environnement ServiceNow AI Platform . Une détection comprend des données enrichies sur une vulnérabilité et tous les éléments vulnérables correspondants. Ces données sont affichées sur l'enregistrement de détection (VID#) et la vue de liste des éléments vulnérables, qui incluent les détails suivants :

- Premier trouvé (données)
- Dernière occurrence trouvée (date)
- Nom DNS

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Nom du BIOS réseau
- Adresse IP
- Port
- Protocole
- Preuve
- SSL
- Durées trouvées

Remarque : L’ajout d’une règle métier sur la table de détection aura un impact sur les performances de l’ingestion.

Clé de détection

Combinaison hachée de champs qui permet d’identifier et de lier une détection à un élément vulnérable. Les clés de détection sont spécifiques à l’intégration.

Configurations des clés de détection

Scanner	Vulnérabilité	Port	Protocole	ID de l'actif	Preuve	Carte réseau
Qualys	Oui	Oui	Oui	Oui	Non	N/A
Tenable	Oui	Oui	Oui	Oui	Non	N/A
Rapid7	Oui	Oui	Oui	Oui	Oui (il n’est pas sensible à la casse)	Oui

Remarque :

- Si la clé de détection n’est pas spécifiée, ou pour les versions antérieures à Réponse aux vulnérabilités 14.0, elle est une combinaison d’entrée de vulnérabilité, de port, de protocole, d’ID d’actif et de preuve.
- À partir de la version 19.0 sur Réponse aux vulnérabilités, une nouvelle clé de détection NIC est ajoutée pour Rapid7 InsightVM, qui est activée par défaut. Les détections existantes sans carte réseau sont mises à jour avec la première carte réseau entrante dans la charge utile à partir de Rapid7. La clé de détection est recalculée et remplie à nouveau sur la carte réseau incluant la détection. De nouvelles détections sont créées si des détections similaires sont observées avec des valeurs de carte réseau différentes. Ces données ne sont pas déployées sur la table Élément vulnérable. La valeur de carte réseau est stockée dans une nouvelle colonne sur la table sn_vul_detection_key_config et sn_vul_detection.

De dup

Processus utilisé par l’application Réponse aux vulnérabilités de la réduction des détections individuelles en un seul VI lorsque les données répondent à certains critères codés en dur.

ID externe VI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur stockée dans le champ ID externe de la table des VI. Cette valeur est un hachage composé de la combinaison de clés au sein d'un VI qui représente ce qui le rend unique dans l'application. Il est composé d'un CI et d'une entrée vulnérable.

Rouvrir les éléments vulnérables résolus

Les éléments vulnérables définis sur **Résolu** dans votre ServiceNow AI Platform instance, mais pas transitionnés à l'état **Fermé/Corrigé** par les exécutions d'intégration suivantes sont rouverts s'ils sont détectés lors des nouvelles analyses.

Les VI fermés avec un sous-état **fixe** ou **périmé** sont rouverts si une nouvelle détection est créée et que les VI peuvent être mis en correspondance avec la nouvelle vulnérabilité.

Selon le script include, *`DetectionBase`*, méthode , *`_shouldReOpenVI()`*si le VIT était précédemment **fermé** avec le sous-état **Fixe**, **Périmé** ou **CI désactivé**, il est rouvert et la détection est mappée au VIT existant.

Par exemple, supposons que la date de fermeture d'un VIT est postérieure à la date de last_found d'une détection. On peut s'attendre à ce que ces enregistrements VIT restent fermés. Toutefois, si vous voyez un VIT précédemment fermé rouvert, cela signifie que le VIT a été fermé par une détection antérieure et que la vulnérabilité a été retrouvée lors d'une analyse ultérieure. Lorsqu'une nouvelle détection correspond au VIT fermé qui présente la même vulnérabilité sur l'élément de configuration du VIT, le VIT est rouvert.

Pour Rapid7 les détections, une option est maintenant disponible sur la page de configuration Rapid7 de votre instance pour rouvrir les VI résolus par âge. Si cette option est activée, les VI définis sur **Résolu** , mais ne sont pas transitionnés à **l'état Fermé/Corrigé** par les analyses suivantes et reviennent à **l'état Ouvert** après le nombre de jours que vous entrez.

En ce Qualys qui concerne les détections, si le scanner continue de trouver des VI qui ont été définis sur **Résolu** , mais qui ne sont pas passés à **l'état Fermé/Corrigé** par les analyses suivantes, ces VI retournent à **l'état Ouvert** lorsque la dernière date trouvée est postérieure à la date de résolution.

Afficher les données de détection

Vous affichez les données importées à partir des détections d'éléments vulnérables sur l'enregistrement du VI. Pour plus d'informations, consultez Afficher les Réponse aux vulnérabilités données de détection des éléments vulnérables et Vérifier les Réponse aux vulnérabilités données de détection d'éléments vulnérables sur les enregistrements de l'exécution de l'intégration (VINTRUN).

Gestion des solutions pour vulnérabilités

Corrélez automatiquement les vulnérabilités de votre environnement avec les solutions qui pourraient les corriger. Identifiez les actions de rattrapage qui s'appliquent à vos vulnérabilités et hiérarchisez-les en fonction de la meilleure réduction du risque de vulnérabilité.

Gestion des solutions pour vulnérabilités

Les équipes informatiques et de sécurité passent souvent beaucoup de temps à rechercher les résultats des vulnérabilités afin d'identifier les traitements les plus efficaces pour leur environnement. Compte tenu du volume et de la complexité des vulnérabilités dans les grandes organisations, la traduction des résultats de vulnérabilité en tâches de rattrapage est un processus manuel, fastidieux et sujet aux erreurs.

Grâce Gestion des solutions pour vulnérabilitésà , vous pouvez automatiquement corréler vos résultats de vulnérabilité avec les solutions qui les corrigent. Identifiez les correctifs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

logiciels, les mises à jour de configuration et les autres contrôles qui ont le plus d'impact pour votre organisation sans frais manuels.

Configuration requise pour le Gestion des solutions pour vulnérabilités

Gestion des solutions pour vulnérabilités est une fonctionnalité disponible au sein de l'application Réponse aux vulnérabilités . Gestion des solutions pour vulnérabilités Nécessite un abonnement distinct.

Pour en savoir plus sur l'obtention d'autorisations pour les applications à partir de , reportez-vous à la ServiceNow Store section Obtenir une autorisation pour un produit ou une Opérations de sécurité application. Pour plus d'informations sur l'installation de l'application après l'avoir téléchargée sur votre instance, reportez-vous Installer l'application Gestion des solutions pour Réponse aux vulnérabilités à la section .

Une fois installé, Gestion des solutions pour vulnérabilités il vous permet d'accéder aux données de la Red Hat solution à partir de Réponse aux vulnérabilités.Microsoft Security Response Center

Remarque :

Vous pouvez configurer les deux applications de solution à partir de l'assistant de configuration. Consultez Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'assistant de configuration.

Consultez Microsoft Security Response Center Solution Integration et Intégration de solution Red Hat pour plus d'informations sur les solutions importées.

Versions disponibles

Pour la version la plus récente de Gestion des solutions pour vulnérabilités, vérifiez que la version la plus récente de Réponse aux vulnérabilités est installée.

Version de Gestion des solutions pour vulnérabilités	Versions compatibles de Réponse aux vulnérabilités	Notes de publication
Gestion des solutions pour vulnérabilités v10.3	Réponse aux vulnérabilités v18.0	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

À propos des solutions et du remplacement

Une mise à jour remplacée est un remplacement complet d'une ou de plusieurs versions précédentes. Par exemple, une mise à jour de correctif peut être remplacée par un Service Pack. Les solutions sont liées aux vulnérabilités. Les solutions peuvent également se rapporter à d'autres solutions d'une chaîne de remplacement. Les solutions traitent les vulnérabilités des solutions précédentes et elles sont cumulatives. Gestion des solutions pour vulnérabilités associe automatiquement les vulnérabilités des solutions précédentes aux solutions de remplacement. Si une vulnérabilité plus ancienne est trouvée, n'importe quelle solution de remplacement supérieure peut la résoudre, mais la solution de remplacement la plus élevée est préférée, car elle est la plus cumulative.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Solutions potentielles et solutions privilégiées

Une solution potentielle est une solution qui pourrait remédier à une vulnérabilité. Les vulnérabilités ont souvent de nombreuses solutions potentielles. Une solution privilégiée est la solution unique ciblée pour corriger une vulnérabilité ou un élément vulnérable (VI). Il communique l'intention et permet d'obtenir des mesures de déploiement plus détaillées.

Solutions privilégiées

Gestion des solutions pour vulnérabilités Définit automatiquement la solution la plus efficace (**solution privilégiée**) pour la vulnérabilité détectée en fonction de la priorité la plus élevée lorsqu'il n'existe qu'une seule solution de priorité la plus élevée. S'il existe plus d'un remplacement le plus élevé pour la vulnérabilité, aucune valeur n'est fixée. Dans Réponse aux vulnérabilités, une **solution privilégiée** est la Microsoft Security Response Center solution OU Red Hat avec la plus haute substitution dérivée des solutions associées à la vulnérabilité.

Les valeurs de solution privilégiée peuvent être définies sur l'élément vulnérable ou la vulnérabilité. Lorsqu'ils sont définis directement sur la vulnérabilité, tous les éléments vulnérables associés à la vulnérabilité héritent de cette solution. Modifiez les valeurs de **solution préférée** pour plusieurs éléments vulnérables à l'aide de la fonctionnalité de modification en bloc. Lors de la modification en bloc, seule la **solution privilégiée** sur l'élément vulnérable est mise à jour, car définir la **solution privilégiée** au niveau d'entrée de vulnérabilité définirait la **solution privilégiée** pour tous les nouveaux VI à l'avenir. La modification en bloc s'applique uniquement aux éléments vulnérables actuels.

Remarque : S'il existe plusieurs solutions de remplacement les plus élevées pour une vulnérabilité, les valeurs de **solution privilégiée** au niveau de la vulnérabilité sont effacées, car cette solution dépend de l'actif affecté. Lorsqu'il existe plusieurs solutions de remplacement les plus élevées pour une vulnérabilité, définissez une **solution privilégiée** sur l'élément vulnérable. Vous pouvez définir une solution différente à **l'aide** de la liste de recherche sur le formulaire **d'élément vulnérable** .

Toutes les solutions privilégiées pour les éléments vulnérables dans les tâches de rattrapage figurent dans une liste connexe sur l'enregistrement de la **tâche de rattrapage** .

Les importations de solutions n'entraînent pas toutes des actualisations complètes des données. Le processus de remplacement est mis à jour lorsque :

- Un élément vulnérable est créé.
- Les données ont changé sur un VI actif.

Remarque : À partir de la version 22.0 de Réponse aux vulnérabilités, les solutions ne sont pas mises en file d'attente dans les deux cas ci-dessus.

- Un nouveau mappage est créé pour une entrée tierce avec les CVE.
- De nouvelles données de solution ont été publiées depuis la dernière importation, une solution existante est mise à jour.

À partir de la version 24.0.6 de Réponse aux vulnérabilités, vous pouvez ingérer des solutions à partir de scanners en plus des solutions des fournisseurs. Les données de rattrapage des scanners tels que Tenable Qualys et Microsoft TVM sont exploitées pour créer les solutions. Ces solutions de scanner sont importées à l'aide des intégrations suivantes :

- Tenable.sc Intégration de module d'extension
- Tenable.io Intégration de module d'extension
- Qualys Base de connaissances (remplissage)

Traduction automatique

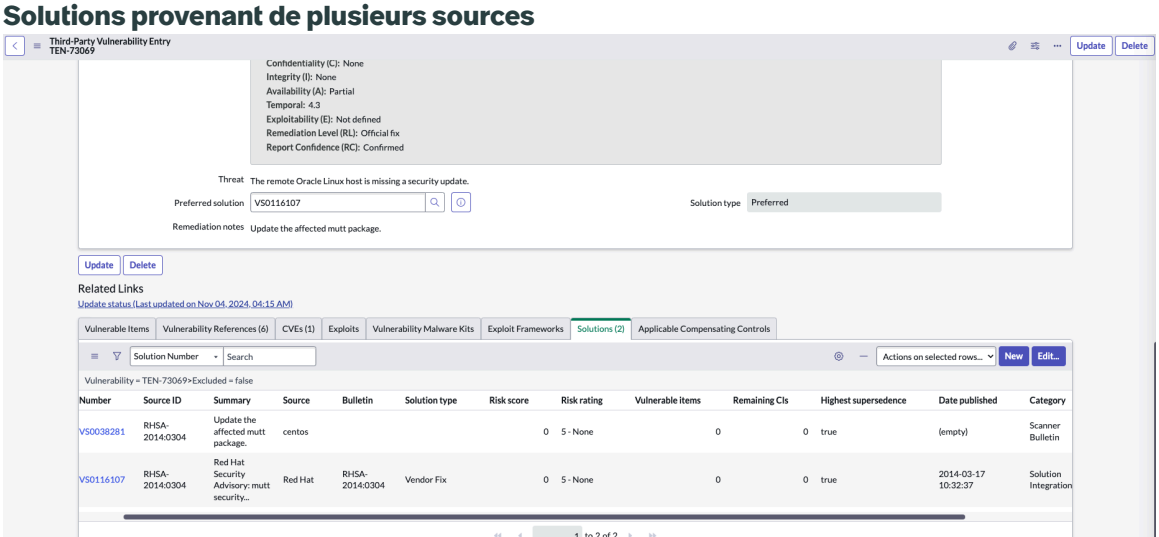
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Intégration des vulnérabilités de la machine Microsoft TVM (importation complète)
- Intégration des vulnérabilités des ordinateurs Microsoft TVM (importation Delta)

Lorsque les intégrations de vulnérabilité s'exécutent, une charge utile d'informations de rattrapage est créée avant de traiter les entrées tierces. Pour Tenable et Qualys, les données de rattrapage sont reçues au niveau d'entrée de la vulnérabilité ou du tiers. À l'inverse, pour Microsoft TVM, les solutions sont créées au niveau de la détection, ce qui permet de renseigner directement les solutions préférées sur les éléments vulnérables sans avoir besoin d'un traitement supplémentaire. Ces solutions sont créées sur la base de ces informations de rattrapage et traitées selon les besoins. Lors du traitement, la solution privilégiée est renseignée sur les vulnérabilités et déployée sur les éléments vulnérables. La solution privilégiée est renseignée dans l'ordre suivant :

- Sélection manuelle : si vous sélectionnez une solution manuellement, elle n'est pas remplacée.
- Solutions de fournisseurs (importations Microsoft, RedHat, CVRF et CSAF) : si vous ne sélectionnez pas une solution manuellement, elle est sélectionnée automatiquement.
- Solutions les plus récentes (si activées) : s'il existe plusieurs solutions de remplacement supérieures disponibles pour une vulnérabilité, le champ Solution **privilégiée** reste vide. Dans ce cas, si vous activez la propriété `sn_vul.latest_solutions`, la solution de fournisseur de remplacement la plus récente est renseignée en tant que solution préférée.
- Solutions de bulletins de scanner (si activées) : si vous ne sélectionnez pas une solution manuellement ou si les solutions du fournisseur ne sont pas disponibles, le champ **Solution privilégiée** est renseigné avec les solutions de scanner à condition qu'il n'y ait qu'une seule solution de scanner. Vous devez activer la propriété `sn_vul.populate_scanner_solutions` pour remplir les solutions de scanner.

Solutions provenant de plusieurs sources

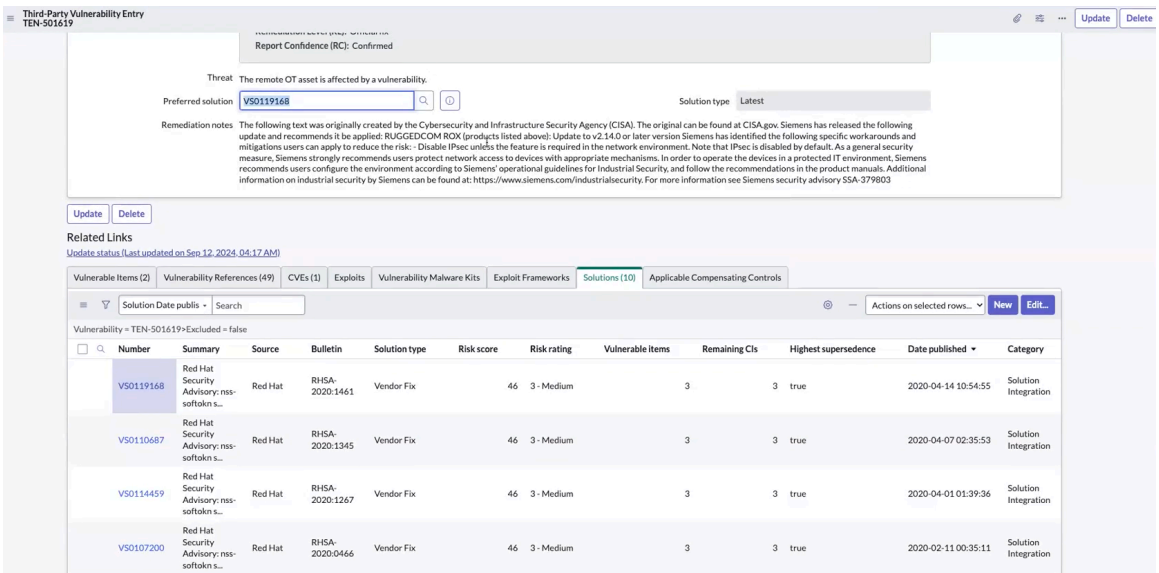


Cet exemple illustre la sélection d'une solution si plusieurs solutions sont disponibles à partir de différentes sources. Dans ce cas, il existe deux solutions pour une vulnérabilité : l'une provenant d'un fournisseur et l'autre provenant d'un scanner. Lorsque la solution VS0116107 est reçue d'un fournisseur, par exemple Redhat, qui a une préférence plus élevée, elle est sélectionnée comme solution préférée.

Traduction automatique

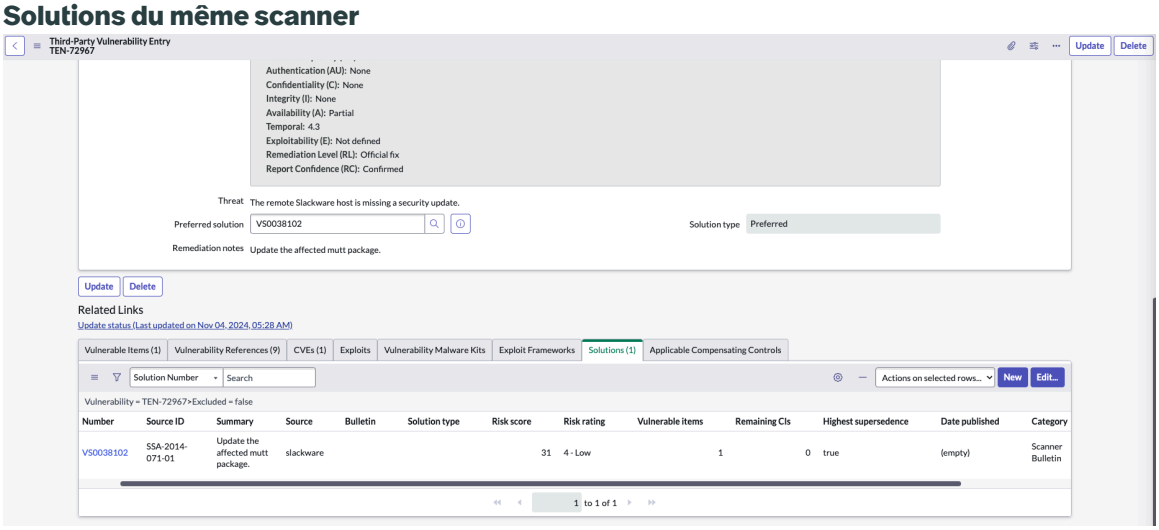
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Solutions du même fournisseur



Cet exemple illustre la sélection d'une solution si plusieurs solutions sont disponibles auprès du même fournisseur, c'est-à-dire Redhat dans ce cas. Si la *sn_vul.latest_solutions* propriété est activée et qu'aucune autre solution de fournisseur n'est disponible pour une vulnérabilité spécifique, ces solutions sont traitées, renseignant les solutions préférées sur les vulnérabilités, puis sur les éléments vulnérables. Si vous activez la propriété *sn_vul.latest_solutions*, la solution la plus récente est sélectionnée comme solution préférée.

Solutions du même scanner



Cet exemple illustre la sélection d'une solution si une seule solution de scanner est disponible à partir des scanners. Si la *sn_vul.populate_scanner_solutions* propriété est activée, les solutions sont traitées, renseignant les solutions préférées sur les vulnérabilités, puis sur les éléments vulnérables. S'il existe plusieurs solutions d'analyse, le champ **Solution privilégiée** est laissé vide en raison d'une ambiguïté.

Améliorer la gestion des solutions et l'optimisation des performances

Les solutions proviennent de diverses intégrations, notamment Microsoft et Redhat. Le premier fournit des mises à jour mensuelles et établit une chaîne de dépendances pour suivre la solution préférée pour détecter les vulnérabilités. Toutefois, d'autres intégrations ne suivent pas ce format de mise à jour et n'ont pas besoin d'établir une chaîne de dépendances pour elles. Auparavant, une logique de traitement était utilisée qui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

impliquait la création d'un graphique pour maintenir la priorité et identifier les solutions de remplacement les plus élevées. Ces solutions ont été suggérées comme solution privilégiée pour les vulnérabilités. Cependant, comme la construction du graphique prend du temps, les autres intégrations sont exclues de ce processus. Pour améliorer les performances, à partir de la version 22.0 de Réponse aux vulnérabilités, la méthode `utility.processNonGraphSolutions()` est appelée dans la `Process Vulnerability Solutions Metrics Queue` tâche planifiée. Cette méthode gère les solutions provenant d'intégrations autres que Microsoft.

Deuxièmement, les solutions sont mises en file d'attente à partir de diverses sources à l'aide de la tâche `Process Vulnerability Solutions Metrics Queue`planifiée. Cette tâche planifiée implique le déploiement de solutions à partir d'entrées NVD vers des entrées tierces, le remplissage des solutions préférées sur les vulnérabilités et la mise à jour des mesures d'état du rattrapage sur les solutions. Dans les scénarios suivants, seules les mesures d'état de rattrapage doivent être mises à jour :

- Lorsque la solution privilégiée change sur les vulnérabilités
- Lorsque les VIT sont créés ou supprimés
- Lorsqu'une importation VIT est terminée

Bien que les solutions soient mises en file d'attente pour mettre à jour uniquement les mesures d'état de rattrapage, elles tentent toujours de déployer des solutions des entrées NVD vers les entrées tierces et de renseigner les solutions préférées. Pour optimiser ce processus, dans la table Solution de vulnérabilité, la colonne Mettre **à jour le statut** est introduite. Lorsque les mesures d'état du rattrapage sur les solutions doivent être mises à jour sans nécessiter le déploiement ou le remplissage des solutions préférées, les solutions ne sont plus mises en file d'attente. Au lieu de cela, la colonne **État de la mise à jour** est directement mise à jour avec la valeur vrai. Cette approche permet de gérer les tickets où seules les mesures d'état de rattrapage doivent être mises à jour, ce qui permet de réaliser des économies de temps et de ressources. Dans la tâche planifiée, une fois le traitement des solutions en file d'attente terminé, les solutions marquées avec un état de mise à jour comme vrai sont identifiées. Ensuite, elles sont itérées à travers ces solutions, en calculant les nombres et en mettant à jour les mesures d'état de rattrapage en conséquence. Cette étape joue un rôle important dans l'amélioration des performances de la tâche planifiée, car le nombre de solutions à mettre en file d'attente est réduit. Pour afficher les mesures de l'état du rattrapage, accédez à la table Solution de vulnérabilité [sn_vul_solution] et sélectionnez une solution de vulnérabilité. Sélectionnez ensuite l'onglet **État du rattrapage** . L'onglet contient les champs suivants :

Mesures de l'état de rattrapage

Champ	Description
Cibles de solution préférées : état du rattrapage pour les éléments vulnérables pour lesquels il s'agit de la solution préférée	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
CI restants	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures de l'état de rattrapage (suite)

Champ	Description
VI totaux	Nombre d'éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
CI totaux	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
% des VI rattrapés	Pourcentage complet pour le rattrapage d'éléments vulnérables (VI). S'applique aux éléments vulnérables pour lesquels cette solution est préférée. Ce nombre exclut les éléments vulnérables différés.
% des CI rattrapés	Pourcentage complet pour le rattrapage de CI. S'applique aux éléments vulnérables pour lesquels cette solution est préférée. Ce nombre exclut les éléments vulnérables différés.
Cibles de solutions préférées (inclut les éléments différés) : état du rattrapage pour les éléments vulnérables, y compris les éléments différés, pour lesquels il s'agit de la solution préférée	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est préférée pour le rattrapage.
CI restants	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre d'éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage.
CI totaux	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage.
% des VI rattrapés	Pourcentage complet pour le rattrapage d'éléments vulnérables (VI). S'applique aux éléments vulnérables pour lesquels cette solution est préférée.
% des CI rattrapés	Pourcentage complet pour le rattrapage de CI. S'applique aux éléments vulnérables pour lesquels cette solution est préférée.
Cibles de solutions potentielles : état du rattrapage pour tous les VI avec une vulnérabilité liée à cette solution	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est une solution possible pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
CI restants	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est une solution possible pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures de l'état de rattrapage (suite)

Champ	Description
Cibles de solutions potentielles (inclut les éléments différés) : état du rattrapage pour tous les éléments vulnérables, y compris les éléments différés, avec une vulnérabilité associée à cette solution	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est une solution possible pour le rattrapage.
CI restants	Nombre de CI associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est une solution possible pour le rattrapage.

Troisièmement, la disponibilité d'une solution privilégiée pour les vulnérabilités et les VIT doit être assurée pour remédier aux vulnérabilités. Toutefois, dans les situations où il existe plusieurs solutions de remplacement supérieures pour une vulnérabilité, la solution privilégiée n'est pas renseignée en raison de l'ambiguïté. Pour résoudre ce scénario, une approche est mise en œuvre qui consiste à exécuter la logique de traitement et à renseigner la solution préférée lorsqu'elle est disponible. Dans les cas où il n'existe qu'une seule solution de remplacement supérieure, elle est renseignée en tant que solution privilégiée. Lorsqu'il existe plusieurs solutions de remplacement supérieures, le champ de solution privilégiée reste vide. Cependant, l'objectif est de renseigner la solution de remplacement la plus élevée, qui est publiée comme la plus récente, comme la solution préférée. Pour ce faire, une propriété *sn_vul.latest_solutions* système est introduite. Par défaut, cette propriété est définie sur faux. Si vous souhaitez activer la possibilité de renseigner les solutions les plus récentes en tant que solution préférée lorsqu'aucune solution privilégiée n'est disponible, vous pouvez activer cette propriété. Une fois activée, la colonne **Type de solution** est mise à jour dans la table de vulnérabilité avec les options suivantes :

- Préféré : lorsque la solution préférée est renseignée
- Le plus récent : lorsqu'aucune solution privilégiée n'est disponible, la solution la plus récente de l'ensemble des solutions de remplacement les plus élevées est sélectionnée en fonction de la valeur de la date de publication. Le champ à sélectionner en tant que solution la plus récente peut être personnalisé à l'aide de la *sn_vul.latest_solutions* propriété système. Par défaut, la valeur est définie sur « date de publication », mais elle peut être changée en « dernière modification » pour sélectionner la solution en fonction de la colonne Dernière modification dans les solutions.
- Manuel : lorsque le type de solution préféré est mis à jour manuellement. La priorité pour ce type de solution est la plus élevée.

Dans certains scénarios, la solution privilégiée sur un élément vulnérable (VIT) peut différer de la solution privilégiée sur la vulnérabilité correspondante. Cela se produit lorsque la solution préférée est mise à jour manuellement sur un VIT et non sur la vulnérabilité. Dans ce cas, le champ **Type de solution** est masqué sur le VIT.

Que fait Gestion des solutions pour vulnérabilités

- Associe automatiquement les nouveaux éléments vulnérables (VIT) et les tâches de rattrapage aux solutions pendant Microsoft Security Response Center Solution Integration l'importation Intégration de solution Red Hat .

  MSRC Les solutions sont associées au dernier bulletin dans lequel la solution apparaît.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Associe automatiquement les éléments vulnérables et les tâches de rattrapage aux solutions lorsque les enregistrements de vulnérabilité sont associés manuellement aux solutions.

  Remarque : Les éléments vulnérables réaffectés manuellement à une autre solution ne sont pas automatiquement mis à jour avec les changements de solution au niveau de vulnérabilité.

- MSRC: crée des chaînes de remplacement pendant l'importation que vous pouvez afficher dans la liste connexe de la solution.
- Indique si une solution est une solution de priorité élevée ou non.
- Répertorie le **score de risque** de solution associé à chaque solution pour vous fournir les plus grandes opportunités de réduction des risques.
- Gère **l'état du rattrapage** pour les solutions sur **les entrées de vulnérabilité**, **les tâches de rattrapage** et les enregistrements de **solutions de vulnérabilité** tiers afin que vous puissiez suivre la progression du rattrapage.

  Il contient :

  - Nombre d'éléments vulnérables corrigés en pourcentage, pour les VI avec des solutions privilégiées, avec et sans les VI à l'état Différé.
  - Nombres d'éléments de configuration (CI) corrigés en pourcentage, pour les VI avec des solutions privilégiées, avec et sans ces VI à l'état Différé.
  - Nombre d'éléments vulnérables corrigés en pourcentage, pour les éléments vulnérables avec des solutions potentielles, avec et sans les VI à l'état Différé.
  - Nombre d'éléments de configuration corrigés en pourcentage, pour les VI avec des solutions privilégiées, avec et sans ces VI à l'état Différé.

Ce que vous pouvez faire avec Gestion des solutions pour vulnérabilités

- Créez, mettez à jour, affichez ou supprimez des solutions associées à des vulnérabilités, afin de pouvoir suivre les solutions en matière de vulnérabilité qui ne sont pas couvertes par le contenu de solutions tierces. L'intégration de la solution avec l'entrepôt de données Rapid7 n'est pas prise en charge.
- Associez les vulnérabilités tierces et les entrées NVD à un enregistrement de solution.
- Supprimez et associez à nouveau des éléments vulnérables et des tâches de rattrapage à une solution.
- Affichez la **solution privilégiée** applicable à une vulnérabilité donnée sur les formulaires de vulnérabilité et d'éléments vulnérables.
- Consultez une liste connexe **de solutions privilégiées** sur les formulaires de tâche de rattrapage, qui répertorie toutes les solutions qui ont été préférées par au moins un VI actif au sein de ce groupe.
- Affichez les détails de **l'état du rattrapage** d'une solution qui montrent la réduction du risque associée au déploiement de la **solution préférée** sur la vulnérabilité, l'élément vulnérable, les tâches de rattrapage et les formulaires de solution.
- Affichez les vulnérabilités applicables à une solution donnée sur le formulaire de solution.
- MSRC: affichez les solutions de remplacement d'une solution donnée sur une vulnérabilité, afin de trouver la dernière mise à jour à déployer ou une mise à jour antérieure, plus ciblée et efficace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Affichez des listes de solutions triées en fonction de différentes caractéristiques.
  - Toutes : solutions triées par date de publication et par numéro.
  - MSRC: priorité la plus élevée : solutions comportant des éléments vulnérables actifs et non différés. Trié par **Priorité la plus élevée**, **Date de publication** et **Nombre**.
  - Avec éléments vulnérables : solutions avec des éléments vulnérables actifs et non différés. Trié par **Priorité ou Priorité la plus élevée**, **Score de risque** et **Nombre**. Si elles sont déployées, les premières entrées de la liste offrent la réduction de risque la plus importante pour les actifs de votre environnement.

Enregistrement de solution Score de risque et cote de risque

Remarque : Le score de **risque** et la **cote de risque de l'enregistrement de la** solution sont distincts des champs utilisés pour les vulnérabilités, les éléments vulnérables et les tâches de rattrapage.

Le score de **risque** de l'enregistrement de solution est un calcul pondéré basé sur le **score de risque** de l'élément vulnérable et un nombre d'éléments vulnérables actifs avec cette solution comme **solution potentielle**. Le **score de risque** de la solution fournit une estimation de la réduction du risque attendue de la solution.

Le **score de risque** de l'enregistrement de solution est calculé comme suit :

- Cela commence par prendre 85 % du **score de risque** le plus élevé ou maximum d'un élément vulnérable actif avec cette solution potentielle.
- Le score de **risque** de l'enregistrement de solution totalise ensuite le nombre total d'éléments vulnérables avec cette solution potentielle. Pour chaque plage du nombre d'éléments vulnérables, il ajoute des points et arrive à un total.
  - 0 à 09 éléments vulnérables n'ajoutent aucun point
  - 10 à 99 éléments vulnérables ajoutent 5 points
  - 100 à 999 éléments vulnérables ajoutent 10 points
  - 1 000 et plus d'éléments vulnérables ajoutent 15 points

  Par exemple, pour un score de **risque** d'élément vulnérable de 80, le **score de risque** de l'enregistrement de solution commencerait à 68. S'il y avait 200 éléments vulnérables actifs au total avec cette solution potentielle, le **score** final de risque de la solution serait de 78.

La cote de **risque** de l'enregistrement de solution sépare le **score de risque** de l'enregistrement de solution en plages allant de Critique à Aucun. La **cote de risque** de la solution évalue la réduction du risque pour les éléments vulnérables que cette solution corrige.

Jusqu'à VR v16.1, les évaluations des risques séparaient le **score de risque** de la solution résultante dans les plages suivantes :

- 1 – Critique (**score de risque** de la solution de 90+)
- 2 – Élevé (70-89, enregistrement de solution, **score de risque**)
- 3 - Moyen (30-69 Enregistrement de solution **Score du risque**)
- 4 – Faible (1-29, enregistrement de la solution **Score du risque**)
- 5 — Aucun (0, Enregistrement de solution, **Score du risque**)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de VR v16.1, les évaluations des risques séparent le **score de risque** de la solution résultant dans les plages suivantes pour Solution Management :

- 1 – Critique (**score de risque** de la solution de 90+)
- 2 – Élevé (70-89, enregistrement de solution, **score de risque**)
- 3 - Moyen (40-69 Enregistrement de la solution **Score du risque**)
- 4 – Faible (1-39, enregistrement de la solution **Score du risque**)
- 5 — Aucun (0, Enregistrement de solution, **Score du risque**)

Cas d'utilisation

Affichez la progression du déploiement de l'état d'un cycle de correctifs actuel à l'aide du module de priorité la plus élevée, trié par date.

Affichez les solutions à plus forte valeur à l'aide du module Avec éléments vulnérables, triées par score de risque.

Les listes de solutions communiquent les détails clés de la solution, les scores de risque et les mesures de déploiement. Utilisez **le score de risque** et les nombres de VI actifs pour la hiérarchisation. Découvrez quelles solutions du cycle de correctifs actuel ne progressent pas, ce qui peut indiquer un prérequis de déploiement manqué.

Remarque : Ajoutez **%VI rattrapés(percent_nd_pref_vis_remediated)** à partir du menu **Personnaliser les colonnes de liste** pour la progression du rattrapage sur le formulaire Solutions de vulnérabilité.

Microsoft Security Response Center Solution Integration

Examiner et mettre en œuvre les solutions de rattrapage proposées fournies par le Microsoft Security Response Center Solution Integration.

Microsoft Security Response Center Solution Integration est inclus dans la Gestion des solutions pour vulnérabilités fonctionnalité de Réponse aux vulnérabilités, disponible par abonnement séparé. Consultez la section Gestion des solutions pour vulnérabilités pour plus d'informations sur la façon d'intégrer des Réponse aux vulnérabilités solutions.

Microsoft Security Response Center examine les rapports de vulnérabilités de sécurité affectant les produits et services Microsoft et fournit des informations sur les solutions pour aider à gérer les risques de sécurité. Les solutions sont des rattrapages connus importés dans votre Microsoft Security Response Center Solution Integration à partir du Microsoft Security Response Center produit.

Le Microsoft Security Response Center Solution Integration contient des points d'entrée vers le Microsoft Security Response Center produit, invoqués en tant que travaux planifiés. Les travaux planifiés simplifient le cycle de vie du rattrapage de la vulnérabilité en maintenant l'instance synchronisée avec d'autres systèmes de gestion de la vulnérabilité. Les travaux planifiés s'exécutent automatiquement et dans l'ordre spécifié. Vous pouvez également exécuter manuellement des travaux planifiés individuels.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles

Pour connaître la version la plus récente de Gestion des solutions pour vulnérabilités et Microsoft Security Response Center les solutions, vérifiez que la version la plus récente est Réponse aux vulnérabilités installée.

Pour plus d'informations sur l'installation et la configuration Gestion des solutions pour vulnérabilités des intégrations de solutions, reportez-vous aux sections Installer l'application Gestion des solutions pour Réponse aux vulnérabilités et Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'assistant de configuration.

Version de Réponse aux vulnérabilités	Version de Gestion des solutions pour vulnérabilités	Notes de publication
Réponse aux vulnérabilités v15.0	v10.3	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Rôles

Microsoft Security Response Center Solution Integration Les tâches impliquent les rôles suivants.

- sn_vul.vulnerability_admin ou sn_vul.admin (obsolète) : autorisation de lecture, d'écriture et de suppression d'enregistrements.
- sn_vul.vulnerability_write : autorisation de lecture et d'écriture d'enregistrements.
- sn_vul.vulnerability.read : autorisation de lecture des enregistrements.
- sn_vul.remediation_owner : peut lire et écrire des notes internes sur les enregistrements affectés au groupe ou à la personne du spécialiste du rattrapage. (Contenu dans le rôle itil.)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Microsoft Security Response Center Solution Integration

Pour afficher le Microsoft Security Response Center Solution Integration, accédez à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.

L'intégration suivante est incluse dans le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Microsoft Security Response Center Solution Integration

Intégration	Description
Microsoft Security Response Center Solution Integration	Récupère les solutions et le mappage de base de données de vulnérabilité nationale (NVD) pour associer les solutions aux vulnérabilités, aux éléments vulnérables et aux tâches de remédiation. **Remarque :** Le Microsoft Security Response Center Solution Integration ne fournit pas de solutions avant 2016.

Solutions

Pour afficher les solutions importées dans une liste, reportez-vous à la section Afficher une solution.

Intégration de solution Red Hat

Vous pouvez examiner et implémenter les solutions de rattrapage proposées par l'dans Intégration de solution Red Hat l'application Réponse aux vulnérabilités .

Intégration de solution Red Hat est inclus dans la Gestion des solutions pour vulnérabilités fonctionnalité de Réponse aux vulnérabilités, disponible par abonnement séparé. Consultez la section Gestion des solutions pour vulnérabilités pour plus d'informations sur la façon d'intégrer des Réponse aux vulnérabilités solutions.

Intégration de solution Red Hat enquête sur les rapports de vulnérabilités de sécurité affectant Red Hat les produits et services et fournit des informations sur les solutions pour aider à gérer les risques de sécurité. Les solutions connues sous le nom de rattrapages sont importées dans votre Intégration de solution Red Hat à partir de Red Hat.

À partir de la version 21.0 de Réponse aux vulnérabilités, Red Hat transmet les charges utiles au format CSAF (Common Security Advisory Framework) plutôt qu'au format CVRF (Common Vulnerability Reporting Framework). CSAF, une norme basée sur XML, diffère à la fois par sa structure et son format de CVRF. Pour tenir compte de ce changement, un nouvel analyseur CSAF a été développé. Cet analyseur interprète le format CSAF en extrayant les champs requis pour remplir les tables en conséquence.

Remarque : Par défaut, vous recevrez la charge utile au format CSAF.

Les extraits suivants montrent le script d'intégration permettant d'analyser Red Hat la charge utile reçue respectivement dans les formats CSAF et CVRF.

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
return new sn_vul.RedHatSolutionIntegration(true);
})(integrationProcessGr);
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
return new sn_vul.RedHatSolutionIntegration(false);
})(integrationProcessGr);
```

Intégration de solution Red Hat contient des points d'entrée vers le produit Red Hat, invoqué en tant que tâche planifiée. La tâche planifiée simplifie le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités. Il s'exécute automatiquement. Vous pouvez également exécuter le travail planifié manuellement.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Versions disponibles

Pour connaître la version la plus récente de Gestion des solutions pour vulnérabilités et Red Hat les solutions, vérifiez que la version la plus récente est Réponse aux vulnérabilités installée.

Pour plus d'informations sur l'installation et la configuration Gestion des solutions pour vulnérabilités des intégrations de solutions, reportez-vous aux sections Installer l'application Gestion des solutions pour Réponse aux vulnérabilités et Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'assistant de configuration.

Version de Réponse aux vulnérabilités	**Version de** Gestion des solutions pour vulnérabilités	**Notes de publication**
Réponse aux vulnérabilités v15.0	v10.3	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Rôles

Intégration de solution Red Hat Les tâches impliquent le rôle suivant : sn_vul.configure_rhsa_integration

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration de solution Red Hat

Pour afficher le Intégration de solution Red Hat, accédez à **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.

L'intégration suivante est incluse dans le système de base.

Intégration Red Hat

Intégration	Description
Intégration de solution Red Hat	Récupère les solutions et le mappage de base de données de vulnérabilité nationale (NVD) pour associer les solutions aux vulnérabilités, aux éléments vulnérables et aux tâches de remédiation.

Solutions

Pour afficher les solutions importées dans une liste, reportez-vous à la section Afficher une solution.

Rapid7 Gestion des solutions

Les solutions sont des rattrapages connus qui sont importés dans Ur Intégration des vulnérabilités Rapid7 à partir de l'entrepôt Rapid7 de données ou Rapid7 InsightVM Rapid7 de . L'entrepôt de données importe à la fois les solutions et les solutions de remplacement. Avec Rapid7 InsightVM, vous obtenez des solutions dans le cadre de l'API Rapid7 Vulnerable Item Integration.

À partir de la version 21.0 de Réponse aux vulnérabilités, il y a un changement dans la façon dont les solutions sont créées par Rapid7 InsightVM. Au lieu de s'appuyer sur des champs **solution_summary**, **solution_fix** ou **solution_type** , Rapid7 InsightVM Now crée des solutions à l'aide des solution_id fournis par le scanner. Cela signifie que même si ces champs sont vides, une solution est créée tant qu'un ID de solution est disponible.

Pour afficher les solutions importées sous forme de liste, accédez à **Rapid7** > **Solutions**.

Si le module d'extension Gestion des solutions pour vulnérabilités est activé, la dernière version de Intégration des vulnérabilités Rapid7 fournit les fonctionnalités clés suivantes concernant les solutions :

- La gestion de la Rapid7 solution est déplacée vers la gestion des solutions de vulnérabilité.
- Une nouvelle intégration de Rapid7 Prerequisite Solution Management pour l'entrepôt de données est introduite. L'intégration récupère la solution prérequise à partir de l'entrepôt Rapid7 de données.
- La liste connexe de Rapid7 (solution) sur les entrées tierces (TPE) est masquée.
- Les données précédemment importées peuvent être visualisées dans le nouveau modèle de données. Les solutions Rapid7, Remplacement de solution et Carte de solution de vulnérabilité sont réimportées et le champ **Importer depuis** est défini sur vide. Le champ est renseigné dans Gestion des solutions.
- Les détections sont mises à jour pour renseigner le champ de solution. Les détections affichent les solutions telles qu'elles font partie de Vulnerability Solution Management.
- Rapid7 obtient une préférence plus élevée par rapport aux autres solutions lors de la définition de la solution préférée sur TPE pour Rapid7 l'entrepôt de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les solutions se déploient jusqu'aux éléments vulnérables (VI) à partir des détections pour Rapid7 InsightVM.

Remarque : Si vous n'avez pas activé le module d'extension Gestion des solutions pour vulnérabilités , l'application fonctionne en l'état.

Gestion de la solution de vulnérabilité

Si vous avez activé le module d'extension Gestion des solutions pour vulnérabilités , les solutions pour l'entrepôt Rapid7 de Rapid7 données et Rapid7 InsightVM la table Solutions en matière de vulnérabilité [sn_vul_solution]. Toutefois, si vous n'avez pas activé le module d'extension Gestion des solutions pour vulnérabilités , il Intégration des vulnérabilités Rapid7 fonctionne tel quel et importe les solutions dans la table personnalisée [sn_vul_r7_solution].

Pour afficher la table des solutions en matière de vulnérabilité, accédez à **Tous** > **Réponse aux vulnérabilités** > **Solutions en matière de vulnérabilité** où vous pouvez afficher et comparer les solutions de différents fournisseurs. Pour afficher les solutions importées dans la table personnalisée, accédez à **Tous** > **Rapid7 Vulnerability Integration** > **Solutions**.

Remarque : Regrouper par source pour afficher les solutions en fonction des fournisseurs.

Intégration de Rapid7 Prerequisite Solution Management

Si vous avez activé le module d'extension Gestion des solutions pour vulnérabilités , un script correctif est exécuté et modifie l'ordre des intégrations. La nouvelle intégration de la solution préalable Rapid7 pour Rapid7 l'entrepôt de données mappe les solutions avec les solutions préalables. Les intégrations s'exécutent dans l'ordre suivant :

1. Rapid7 Intégration de solution
2. Rapid7 Solution prérequise
3. Rapid7 Intégration de solution de remplacement
4. Rapid7 Intégration de la carte de solution de vulnérabilité
5. Rapid7 Intégration de solution VI (à partir de la version 19.0 sur Réponse aux vulnérabilités)

Remarque : Si vous exécutez les intégrations manuellement, commencez par l'intégration de la Rapid7 solution. Ne modifiez pas la chaîne d'intégration suivante dans l'intégration Rapid7 . La séquence est définie dans la colonne Intégration suivante.

Liste connexe Rapid7 (Solutions) sur TPE

Si vous avez activé le module d'extension Gestion des solutions pour vulnérabilités , vous pouvez procéder comme suit :

- Vous pouvez afficher les TPE en accédant à **Tous** > **Réponse aux vulnérabilités** > **Tiers**.
- Vous ne pouvez pas voir la liste connexe Solutions (Rapid7), qui était disponible dans les versions antérieures.
- Vous pouvez voir les solutions connexes Rapid7 dans la liste connexe Solutions ainsi que les solutions d'autres sources, telles que RedHat, Microsoft (MSRC), etc.

Si vous n'avez pas activé le module d'extension Gestion des solutions pour vulnérabilités , les événements suivants se produisent :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La fonctionnalité de listes connexes reste la même.
- Vous pouvez afficher la liste connexe Solutions (Rapid7).
- La liste connexe Solutions est masquée.

Solution privilégiée sur les TPE et les VI

Rapid7 Obtient la solution de l'entrepôt de données au niveau de l'entrée tierce (TPE) et pour Rapid7 InsightVM au niveau de la détection.

Pour un Rapid7 entrepôt de données, la solution est gérée de la manière suivante :

- La solution privilégiée est définie sur le TPE en fonction du mappage des vulnérabilités et des solutions.
- Si la vulnérabilité de Rapid7 a une solution de remplacement unique la plus élevée de Rapid7, elle est définie comme la solution privilégiée, quelles que soient les autres solutions des fournisseurs attachés à cette vulnérabilité.
- Dans tous les autres cas, le flux de la solution préférée reste le même. Pour plus d'informations sur le comportement par défaut des solutions préférées, reportez-vous à la section Gestion des solutions pour vulnérabilités.

Pour Rapid7 InsightVM, la solution est gérée de la manière suivante :

- La solution privilégiée est déployée des détections vers les VI.
- S'il existe une seule détection et une seule solution de Rapid7, la solution est déployée sur VI.
- S'il y a plusieurs détections et que toutes ont la même solution de Rapid7, la solution est déployée sur VI.
- Si plusieurs détections ont plusieurs solutions de Rapid7, la dernière solution est déployée sur le VI.

À partir de la version 19.0 de Réponse aux vulnérabilités, la solution privilégiée, générée par Rapid7 Data Warehouse, est directement renseignée sur les éléments vulnérables en Rapid7 contournant la nécessité de Gestion des solutions pour vulnérabilités. Ce changement permet d'éliminer toute incertitude concernant les solutions potentielles pour ces éléments vulnérables.

Pour atteindre cette population directe grâce à Rapid7, les mesures suivantes sont prises :

- Une nouvelle intégration, Rapid7 VI Solution Integration, est établie et intégrée au workflow existant d'intégration de vulnérabilité Rapid7.
- Une nouvelle table [sn_vul_r7_rapid7_vi_solution_import] est créée.
- Une nouvelle carte de transformation Transformation de solution VI Rapid7 est créée.
- L'include de script Rapid7AssetsImportProcessor est modifié pour exclure le traitement des solutions générées par Rapid7 dans Gestion des solutions pour vulnérabilités.

Lors de l'exécution de l'intégration de la solution Rapid7 VI, les données non traitées obtenues Rapid7 sont stockées dans la table nouvellement créée. Ensuite, la transformation de solution VI Rapid7 est déclenchée, traitant ces données et renseignant la solution préférée directement dans la table Élément vulnérable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'intégration de la solution Rapid7 VI remplit la solution préférée exclusivement lorsque le module d'extension Gestion des solutions pour vulnérabilités a été installé.

À partir de la version 22.0 de , les solutions de Rapid7 ne sont plus mises en file d'attente lors de Réponse aux vulnérabilités l'exécution de la tâche *Process Vulnerability Solutions Metrics Queue*planifiée . Cette tâche planifiée implique le déploiement des solutions des entrées NVD vers les entrées tierces, le remplissage des solutions préférées sur les vulnérabilités et la mise à jour des mesures d'état du rattrapage sur les solutions. Dans les scénarios suivants, seules les mesures d'état de rattrapage doivent être mises à jour :

- Lorsque la solution privilégiée change sur les vulnérabilités
- Lorsque les VIT sont créés ou supprimés
- Lorsqu'une importation VIT est terminée

Bien que les solutions soient mises en file d'attente pour mettre à jour uniquement les mesures d'état de rattrapage, elles tentent toujours de déployer des solutions des entrées NVD vers les entrées tierces et de renseigner les solutions préférées. Pour optimiser ce processus, dans la table Solution de vulnérabilité, la colonne Mettre **à jour le statut** est introduite. Lorsque les mesures d'état du rattrapage sur les solutions doivent être mises à jour sans nécessiter le déploiement de solutions des entrées NVD vers les entrées tierces ou le remplissage des solutions préférées, elles ne sont plus mises en file d'attente. Au lieu de cela, la colonne **État de la mise à jour** est directement mise à jour avec la valeur vrai. Cette approche permet de gérer les tickets où seules les mesures d'état de rattrapage doivent être mises à jour, ce qui permet de réaliser des économies de temps et de ressources. Dans la tâche planifiée, une fois le traitement des solutions en file d'attente terminé, les solutions marquées avec un état de mise à jour comme vrai sont identifiées. Ensuite, elles sont itérées à travers ces solutions, en calculant les nombres et en mettant à jour les mesures d'état de rattrapage en conséquence. Cette étape joue un rôle important dans l'amélioration des performances de la tâche planifiée, car le nombre de solutions à mettre en file d'attente est réduit.

Chaîne de remplacement de solution importée de l'entrepôt de données Rapid7 pour une vulnérabilité

Vous pouvez afficher les solutions de remplacement d'une solution en sélectionnant une solution de vulnérabilité et en sélectionnant la liste connexe Solutions de remplacement. Vous pouvez afficher les solutions précédentes en sélectionnant la liste connexe Solutions précédentes. Lorsque vous attachez une solution au TPE, la solution de remplacement de cette solution est attachée à ce TPE.

Modifier la profondeur maximale de la chaîne de remplacement de solution dans un graphique par propriété système

La chaîne de remplacement de solution reçue dans le modèle de Rapid7 données est trop longue pour créer le graphique pendant le remplissage de la solution préférée. Ainsi, pour limiter la profondeur de la chaîne, une propriété système nommée *sn_vul.max_recursion_depth* avec une valeur 500 est créée. Si la profondeur de la chaîne est supérieure à 500, le reste de la chaîne est ignoré. Pour modifier la profondeur maximale de la chaîne, accédez à la table [sys_properties] et modifiez la valeur de la propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise à niveau de l'application Rapid7

Si vous mettez à niveau le Intégration des vulnérabilités Rapid7 module d'extension et que vous ne l'avez Gestion des solutions pour vulnérabilités pas encore activé, l'application fonctionne en l'état.

Que vous activiez le module d'extension Gestion des solutions pour vulnérabilités avant ou après la mise à niveau de l'application Rapid7 , le champ **Importer depuis** reste vide pour les intégrations suivantes :

- Intégration de solution de remplacement Rapid7
- Intégration de la carte de solution de vulnérabilité Rapid7
- Intégration de solution Rapid7

> **Remarque :** À partir de l'exécution de l'intégration suivante, les données sont renseignées dans la table de solutions de vulnérabilité.

Pour Rapid7 InsightVM, les données sont reçues au niveau de détection. Lorsque l'intégration s'exécute Rapid7 InsightVM , les solutions sont importées dans la table des solutions de vulnérabilité.

Cadre de travail générique pour ingérer des données de n'importe quel fournisseur de solution

Un cadre de travail générique pour l'intégration de l'intelligence des solutions est disponible pour prendre en charge l'ingestion de données dans différents formats de fichier à partir des fournisseurs de solutions. Ces formats accélèrent l'échange et le traitement de l'information et facilitent le partage d'informations critiques relatives à la sécurité dans un format de rapport normalisé.

Les formats de fichier pris en charge sont les suivants :

Cadre commun de génération de rapports sur les vulnérabilités (CVRF)

Le Cadre commun de génération de rapports sur les vulnérabilités (CVRF) est un langage XML. Les principaux fournisseurs tels que Oracle, Red Hat, Cisco et Microsoft prennent en charge le format CVRF.

Cadre de travail consultatif de sécurité commun (CSAF)

Le Cadre de travail consultatif de sécurité commun (CSAF) est une norme open source qui fournit des avis de sécurité structurés et lisibles par machine basés sur JSON. Les principaux fournisseurs tels que Siemens, Red Hat Hitachi et Schneider prennent en charge le format CSAF.

La gestion des solutions prise en charge par CVRF ou CSAF comprend les fonctionnalités clés suivantes :

- Configuration via l'assistant de configuration
- Prise en charge de l'importation de données CVRF ou CSAF via l'importation de fichiers
- Prise en charge de l'importation de données CVRF ou CSAF via l'URL CVRF ou CSAF
- Prise en charge de l'importation de données CVRF ou CSAF par le biais de conseils
- Mappage des solutions avec les vulnérabilités associées

Le module d'extension Vulnerability Response se charge de mettre à jour les états des mesures de la solution créée.

Pour plus d'informations sur la configuration des fournisseurs de solutions, reportez-vous à la section Configurer les fournisseurs de solutions de vulnérabilité.

Traduction automatique

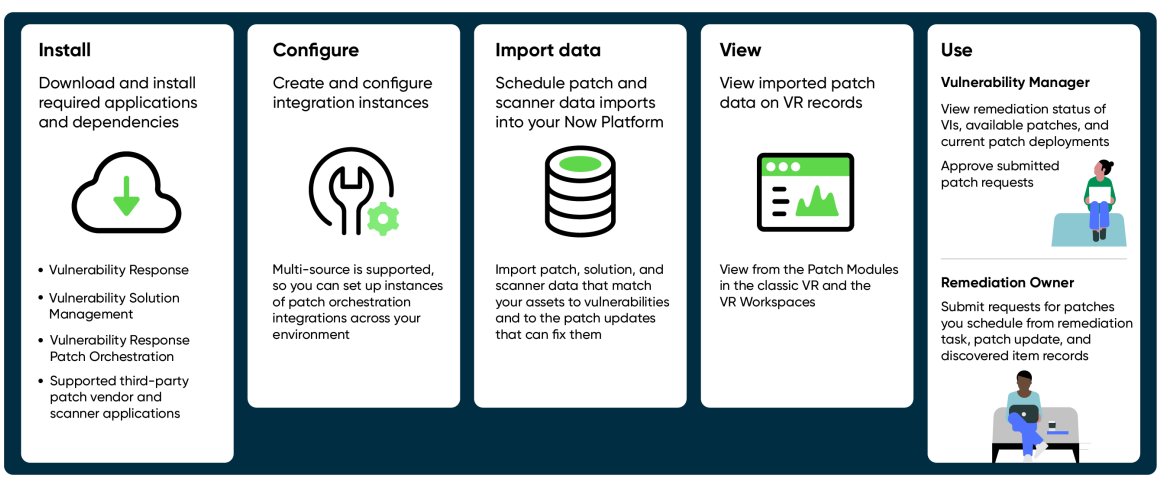
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Orchestration de correctifs avec Réponse aux vulnérabilités

Vous pouvez gérer les correctifs et les déploiements de correctifs pour les vulnérabilités critiques pour de grands groupes de vos actifs avec l'orchestration de correctifs avec Réponse aux vulnérabilités. Réponse aux vulnérabilités L'orchestration des correctifs et les intégrations de l'orchestration des correctifs sont disponibles sur le .ServiceNow® Store

Présentation de l'orchestration des correctifs avec Réponse aux vulnérabilités

L'orchestration des correctifs utilise Réponse aux vulnérabilités les données des importations planifiées à partir d'intégrations de solutions tierces, de fournisseurs de correctifs et de scanners de vulnérabilité. Ces données sont corrélées dans l'application Réponse aux vulnérabilités . Cette organisation des données vous permet de terminer les étapes du cycle de rattrapage de la vulnérabilité. Commencez par identifier les vulnérabilités, puis appliquez des correctifs et des mises à jour, et enfin fermez les éléments vulnérables à l'aide de données d'analyseurs tiers, le tout à partir de votre ServiceNow AI Platform® instance.



L'orchestration des correctifs avec Réponse aux vulnérabilités est prise en charge à la fois dans l'environnement classique et dans les espaces de Réponse aux vulnérabilités travail.

Pour plus d'informations sur l'orchestration des correctifs dans les espaces de travail, reportez-vous à la section Orchestration de correctifs avec les Réponse aux vulnérabilités espaces de travail.

Avec l'orchestration des correctifs dans Réponse aux vulnérabilités, les gestionnaires et analystes des vulnérabilités ainsi que les spécialistes de la remédiation informatique peuvent effectuer les tâches de rattrapage suivantes :

- Voir plus de contexte et d'informations sur les types de correctifs et les fournisseurs qui composent leurs solutions (correctifs).
- Affichez et surveillez les données de vulnérabilité et de solution, ainsi que la progression du rattrapage de la vulnérabilité à partir des enregistrements dans les espaces de Réponse aux vulnérabilités travail ou dans l'environnement classique.
- Déployez des correctifs pris en charge par des fournisseurs de solutions tiers pour leurs Windows, CentOS, MacOS, Oracle et d'autres actifs à intervalles réguliers et planifiés. Vous pouvez planifier des correctifs en dehors des heures de travail pour éviter les conflits avec les personnes au travail.
- À l'aide des données de détection importées fournies par des analyseurs tiers, identifiez les actifs qui présentent des vulnérabilités et qui ne sont pas corrigés ou qui ne sont pas mis à jour avec succès par les correctifs planifiés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lancez et planifiez les correctifs disponibles pour les actifs qui nécessitent des mises à jour à partir de la mise à jour du correctif, de la tâche de rattrapage et des enregistrements d'éléments détectés dans l'application Réponse aux vulnérabilités .
- Surveillez les déploiements de correctifs avec un processus d'approbation facultatif pour les demandes de correctifs soumises par vos spécialistes du rattrapage.

Termes clés

Élément de configuration (CI)

Les CI correspondent aux actifs existants répertoriés dans votre Configuration Management Database (CMDB).

Élément vulnérable (VI)

Une vulnérabilité importée qui correspond à un actif existant dans votre CMDB. Les éléments vulnérables (VIT) sont regroupés en tâches de rattrapage, ou listes, en fonction de certains critères qui spécifient les actions de rattrapage pour les VI.

Instance

Désigne un compte distinct d'une application d'un fournisseur de solution. Par exemple, chaque compte d'utilisateur peut être une instance de l'application HCL BigFix. Ce terme fait également référence à une adresse Web unique et sécurisée pour une ServiceNow AI Platform® instance.

Solution

Il existe deux types de solutions dans le cadre de cette intégration, potentielle et préférée. Une solution potentielle est une solution qui pourrait remédier à une vulnérabilité. Les vulnérabilités ont souvent de nombreuses solutions potentielles. #Une solution privilégiée correspond à la solution la plus efficace pour une vulnérabilité spécifique détectée.

Correctif

Mises à jour logicielles qui corrigent les vulnérabilités. Les fournisseurs de correctifs utilisent leurs propres noms pour les correctifs, par exemple, dans l'application HCL BigFix, les correctifs sont appelés Fixlets.

Correctif préféré

Les correctifs préférés sont des mises à jour logicielles destinées à corriger des vulnérabilités spécifiques. Une fois déployés, les correctifs sont mappés aux éléments vulnérables liés à des vulnérabilités spécifiques et les corrigent.

Déploiement

Aux fins de cette intégration, le déploiement désigne l'application, le lancement ou la planification d'un correctif sur un ordinateur.

Le déploiement dans peut ServiceNow AI Platform également faire référence à une intégration qui prend en charge le multisource. Une existence d'intégration unique est appelée un déploiement de votre intégration. Un déploiement fait référence aux intégrations et aux produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements d'un scanner tiers ou l'intégration d'un fournisseur de solution dans votre environnement.

Versions disponibles des applications et dépendances requises pour l'intégration de l'orchestration des correctifs

- L'application Vulnerability Response et les modules d'extension de dépendance, Security Support Common et Security Support Orchestration.
- Gestion des solutions pour vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Réponse aux vulnérabilités Application Patch Orchestration disponible dans le ServiceNow® Store.
- Une application de fournisseur de correctifs tiers prise en charge, telle que l'intégration de l'orchestration des correctifs Vulnerability Response avec HCL BigFix ou l'intégration de l'orchestration des correctifs Vulnerability Response avec Microsoft SCCM.
- Intégrations de scanners tiers prises en charge avec Vulnerability Response.

Rôles requis

Les utilisateurs ont besoin de rôles spécifiques à l'intégration d'orchestration de correctifs qu'ils utilisent pour afficher les données et planifier les correctifs à partir de l'application Réponse aux vulnérabilités . Consultez les informations de configuration pour les intégrations prises en charge que vous utilisez répertoriées ci-dessous pour en savoir plus.

- Présentation de l'intégration de l'orchestration de correctifs HCL BigFix avec Réponse aux vulnérabilités et l'intégration de l'orchestration des correctifs Vulnerability Response avec Microsoft SCCM.
- Dans les espaces de Réponse aux vulnérabilités travail et l'environnement classique, le rôle sn_vul_patch_orch.read_patch, qui permet aux utilisateurs d'afficher mais pas de modifier les données, est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst.

  Les rôles que vous devez affecter et qui sont nécessaires pour configurer les connexions aux fournisseurs de correctifs et planifier les correctifs sont spécifiques à l'intégration. Pour plus d'informations, consultez et configurez Vulnerability Response Patch Orchestration with MS SCCM.Configurer l'intégration de l'orchestration des Réponse aux vulnérabilités correctifs avec HCL BigFix

Il existe un processus de soumission et d'approbation pour les demandes de correctifs incluses avec les applications. Par défaut, une propriété système est activée [**sn_vul_patch_orch.patch_approval_required**] dans l'application Vulnerability Response Patch Orchestration de votre ServiceNow AI Platform instance.

Cette propriété système est activée de sorte que, lorsque des déploiements de correctifs sont planifiés, ils sont soumis pour révision et approbation aux utilisateurs affectés au groupe d'approbation de mise à jour de correctif de niveau 1. Si vous souhaitez que les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch planifient des correctifs sans approbation, vous pouvez désactiver la propriété [**sn_vul_patch_orch.patch_approval_required**]. Vous préférez peut-être laisser les approbations activées afin que les correctifs planifiés n'entrent pas en conflit avec les heures de travail normales. Si vous désactivez la propriété système d'approbation, tout utilisateur disposant du rôle sn_vul_patch_orch.configure_patch peut planifier et déployer des correctifs sans examen ni approbation.

Pour plus d'informations et pour savoir comment désactiver cette propriété système, consultez la rubrique de configuration de votre intégration prise en charge.

- Configurer l'intégration de l'orchestration des Réponse aux vulnérabilités correctifs avec HCL BigFix.
- Configurer Vulnerability Response Patch Orchestration avec Microsoft l'intégration SCCM.

Planifier des correctifs à partir d'enregistrements Réponse aux vulnérabilités

Les spécialistes du rattrapage peuvent planifier des mises à jour de correctifs pour résoudre les éléments vulnérables et surveiller la progression du rattrapage, le tout à partir des enregistrements de l'application Réponse aux vulnérabilités .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- Mise à jour du correctif
- Tâche de rattrapage
- Élément découvert

Enregistrements qui recupèrent les nombres de VI actifs dans Réponse aux vulnérabilités

Pour éviter d'éventuels problèmes de performances liés au déploiement de tous les correctifs sur toutes les vulnérabilités, la tâche planifiée qui récupère les changements modifie uniquement le nombre de VI actifs. Ces changements de nombre et les données connexes sont déployés dans les enregistrements suivants de l'application Réponse aux vulnérabilités :

- VIT (élément vulnérable)
- RT (tâche de rattrapage)
- Solution de vulnérabilité
- Mise à jour du correctif

Pour plus d'informations sur l'affichage des données de correctif et du déploiement des données de correctif dans les enregistrements, et sur l'affichage des correctifs sans solutions, consultez les rubriques suivantes.

- Données de correctif et déploiement d'état pour l'orchestration de correctifs dans Réponse aux vulnérabilités.
- Affichage des données de correctifs et planification des correctifs dans Réponse aux vulnérabilités.
- Afficher les correctifs sans solutions dans Réponse aux vulnérabilités.

Modifier en bloc des éléments vulnérables avec des correctifs

Vous pouvez modifier en bloc des éléments vulnérables dans l'environnement classique qui ont des correctifs de l'environnement classique. Pour plus d'informations sur le fonctionnement de la modification en bloc, reportez-vous à la section Modifier des éléments vulnérables en bloc dans Réponse aux vulnérabilités. Correctifs préférés pour tous les VI sélectionnés pour la modification en bloc. Cette option de modification ne fonctionne que si des correctifs préférés sont mappés à tous les VI sélectionnés.

Améliorations du modèle de données de gestion des correctifs

Le module d'extension Patch Management Data Model, un module d'extension autonome et gratuit qui encapsule le modèle de données actuellement utilisé dans l'application VR Patch Orchestration. Cela inclut des tables clés telles que Collection, Mise à jour de correctif, Déploiement de correctif et autres.

Ce module d'extension peut être utilisé par les outils de gestion des correctifs pour ingérer les données de gestion des correctifs devant être utilisées par des applications telles que ITSM, Vulnerability Response et ainsi de suite pour les workflows existants.

Principales améliorations :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les tables telles que Appareil de collecte, Mise à jour de correctif et Déploiement de correctif tables dans le module d'extension Orchestration de correctif existant seront déplacées vers le nouveau module d'extension Modèle de données.
- Les données de l'ancienne table seront migrées vers les nouvelles tables pour la fonctionnalité d'orchestration de correctifs VR existante.

Vue d'ensemble de la gestion des exceptions

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive publiée en matière de gestion des vulnérabilités ou de sécurité, vous pouvez demander une exception. La gestion des exceptions implique de demander, de réviser, d'approuver ou de rejeter des exceptions à un élément vulnérable (VI) ou à une tâche de rattrapage (RT) qui ne peuvent pas être corrigées conformément à la politique.

Certaines vulnérabilités peuvent ne pas avoir de correctif, de correctif ou de solution existant. Lorsqu'une exception est approuvée, cela signifie également que vous acceptez un risque, car vous reconnaissez et acceptez les conséquences d'une non-correction de la vulnérabilité.

Cycle de vie d'une exception

Définition d'une exception

Une exception est une demande de différer le rattrapage d'un VI ou d'un RT pour une période spécifiée. Par exemple, en tant que propriétaire de rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine.

Demande d'exception

En tant que propriétaire du rattrapage, vous pouvez demander une exemption pour un VI ou un RT à l'aide du processus de gestion des exceptions. Une fois que l'approbateur d'exception a approuvé cette demande, le VI ou le RT passe à un état **Différé** .

Approbation d'une demande d'exception

Les VI ou RT qui ne peuvent pas être corrigés immédiatement sont examinés par des analystes de vulnérabilité, évalués pour le risque et approuvés pour le report jusqu'à ce qu'ils puissent être corrigés. L'approbation d'une demande d'exception peut être un workflow à deux niveaux. Si seul l'approbateur de premier niveau est présent, l'exception peut être demandée et approuvée. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Consultez Ajouter un approbateur d'exception pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- À partir de la version 15.0, si vous déployez l'application VR pour la première fois, le concepteur de Réponse aux vulnérabilités flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et les faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

  Une fois qu'une demande d'exception pour un VI ou un RT est approuvée, vous pouvez effectuer les actions suivantes :

  - Rouvrir
  - Supprimer
  - Mettre à jour les champs Affectation à ou **Groupes d'affectation**
- À partir de la version 23.0 du , le workflow **Approbation de l'état de la règle d'exception**Réponse aux vulnérabilités est déconseillé et remplacé par l'approbation de la règle d'exception de flux dans le concepteur de flux.

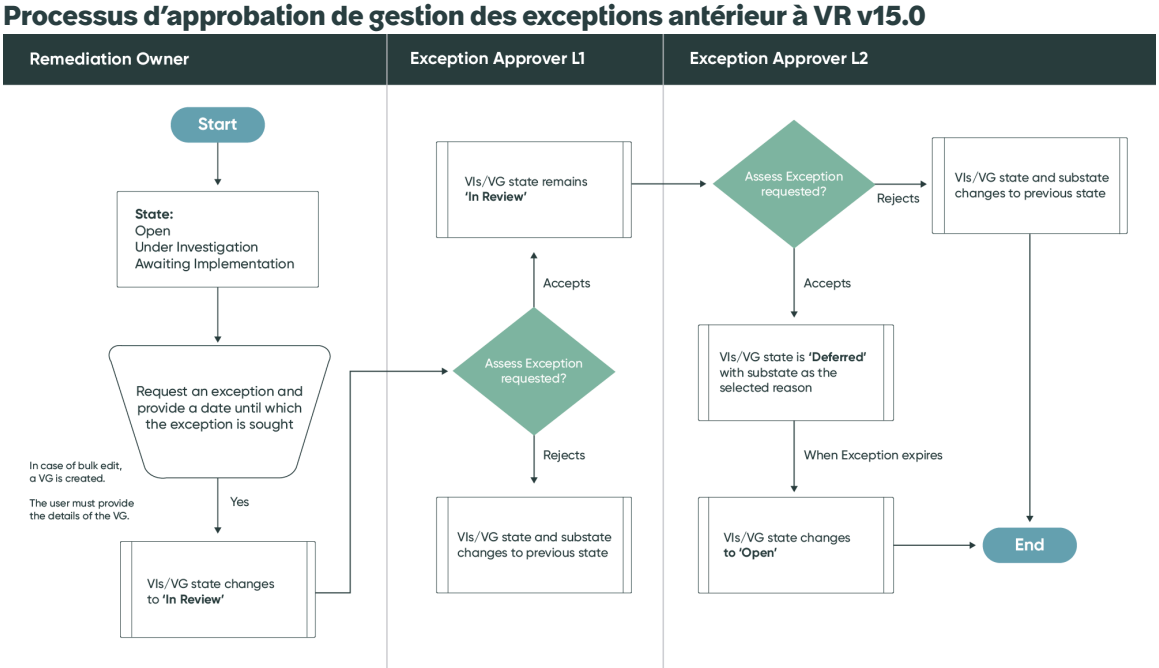
Suivi d'une demande d'exception

Après avoir levé l'exception, vous pouvez suivre son état à l'aide de l'onglet **Approbations de changement d'état** du VI ou du RT. Si une action est effectuée sur un RT, vous ne pouvez pas suivre l'état des VI individuels dans ce RT.

Expiration d'une demande d'exception

Lorsqu'une demande d'exception pour un VI ou un RT particulier expire, le VI ou le RT impacté revient à son état **Ouvert** .

Processus d'approbation de gestion des exceptions antérieur à VR v15.0



Si un seul VI ou tous les VI d'un RT réussissent lors de l'analyse suivante, les VI et, le cas échéant, le champ **État** RT passent à **Fermé** avec le sous-état **Corrigé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Reports multiples

Suivre le nombre de fois où un enregistrement ou une tâche de rattrapage est reporté. Une tâche planifiée, `set deferral counts`, s'exécute quotidiennement pour valider les nombres des enregistrements qui sont reportés plusieurs fois dans la colonne Nombre de reports du module Reports multiples pour VR. Tous les décomptes des enregistrements associés à une tâche de rattrapage sont collectés et publiés si une tâche de rattrapage est reportée plus d'une fois.

Information associée

Demander des exceptions pour les tâches et les enregistrements de rattrapage dans Espace de travail du gestionnaire de vulnérabilités

Demander une exception dans le Espace de travail de remédiation IT

Demander une exception à l'aide de GRC : Gestion de la politique et de la conformitéEspace de travail de remédiation IT

Vue d'ensemble des règles d'exception

Règles d'exception pour Réponse aux vulnérabilités vous permettre d'automatiser le processus de report pour les éléments vulnérables (VI). Demandez une exception pour les éléments vulnérables (VI) qui ne peuvent pas être corrigés ou différés immédiatement, en identifiant les vulnérabilités, les éléments de configuration (CI) ou les VI impactés. Différez les VI correspondants en fonction de la règle lorsque le système les identifie en automatisant le processus de report de VI.

Utilisation de règles d'exception dans votre organisation

Utilisez des règles d'exception pour différer automatiquement les VI nouveaux et existants pour une période spécifique s'ils correspondent à la condition de règle approuvée. L'automatisation minimise le risque de manquer des accords sur les niveaux de service et facilite la gestion de plusieurs éléments, car vous éliminez toute intervention manuelle.

Les règles de report prennent en charge l'ordonnancement, c'est-à-dire que la règle ayant la priorité la plus élevée est exécutée en premier. Lorsqu'une règle de priorité élevée est appliquée à un élément vulnérable, aucune règle suivante ne lui est appliquée, même si la condition correspond au VI.

Remarque :

- Vous ne pouvez créer des règles que si vous sélectionnez une option Réponse aux vulnérabilités dans la configuration Gestion de l'exception. Pour plus de détails, voir Configurer la gestion des exceptions pour Réponse aux vulnérabilités.
- Lorsque des éléments vulnérables sont différés par une règle d'exception, ils sont copiés dans la tâche de rattrapage (RT) de report qui est créée. Les VI continuent de faire partie des RT dont ils faisaient partie auparavant.

Le cycle de vie d'une règle d'exception est le suivant :

- Création d'une règle d'exception
- Approbation d'une demande de règle d'exception
- Activation d'une règle d'exception
- Différer une règle d'exception
- Expiration d'une règle d'exception

Création d'une règle d'exception

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez créer une règle d'exception pour différer automatiquement les VI qui correspondent aux conditions définies pour la période spécifiée. Après avoir créé une règle d'exception, soumettez-la pour approbation.

Approbation d'une demande de règle d'exception

L'approbation d'une demande de règle d'exception est un processus à deux niveaux. Si seul l'approbateur de premier niveau est présent, la règle d'exception peut être évaluée et approuvée par une seule approbation. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une approbation de règle d'exception ne peut pas être approuvée. Une fois la règle approuvée, une tâche de rattrapage (RT) est créée. Consultez Approuver une demande de règle d'exception pour plus d'informations.

Remarque :

À partir de la version 15.0, si vous déployez l'application VR pour la première fois, le concepteur de Réponse aux vulnérabilités flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et les faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Une fois qu'une demande de règle d'exception est approuvée, vous pouvez effectuer les actions suivantes :

- Annuler
- Supprimer

Activation d'une règle d'exception

Une fois qu'une règle d'exception est approuvée, une tâche de rattrapage est créée par défaut dans un état Différé. À partir de la date de début de validité, la règle d'exception s'exécute sur tous les éléments vulnérables créés, ainsi que sur ceux qui sont déplacés de l'état Fermé à l'état Ouvert.

Remarque : Si vous activez l'option Exécuter sur les données existantes, une tâche planifiée s'exécute une fois sur les données existantes à la date de début de validité.

Différer une règle d'exception

Vous pouvez différer les VI qui correspondent aux conditions définies dans cette règle d'exception, jusqu'à la date « Reporté jusqu'à » qui est définie pour la règle. À cette date, la tâche de rattrapage que vous avez créée pour la règle d'exception est fermée et tous les VI de ce groupe repassent à l'état Ouvert. Des règles de groupe leur sont appliquées à nouveau pour les affecter aux thérapeutes en temps réel.

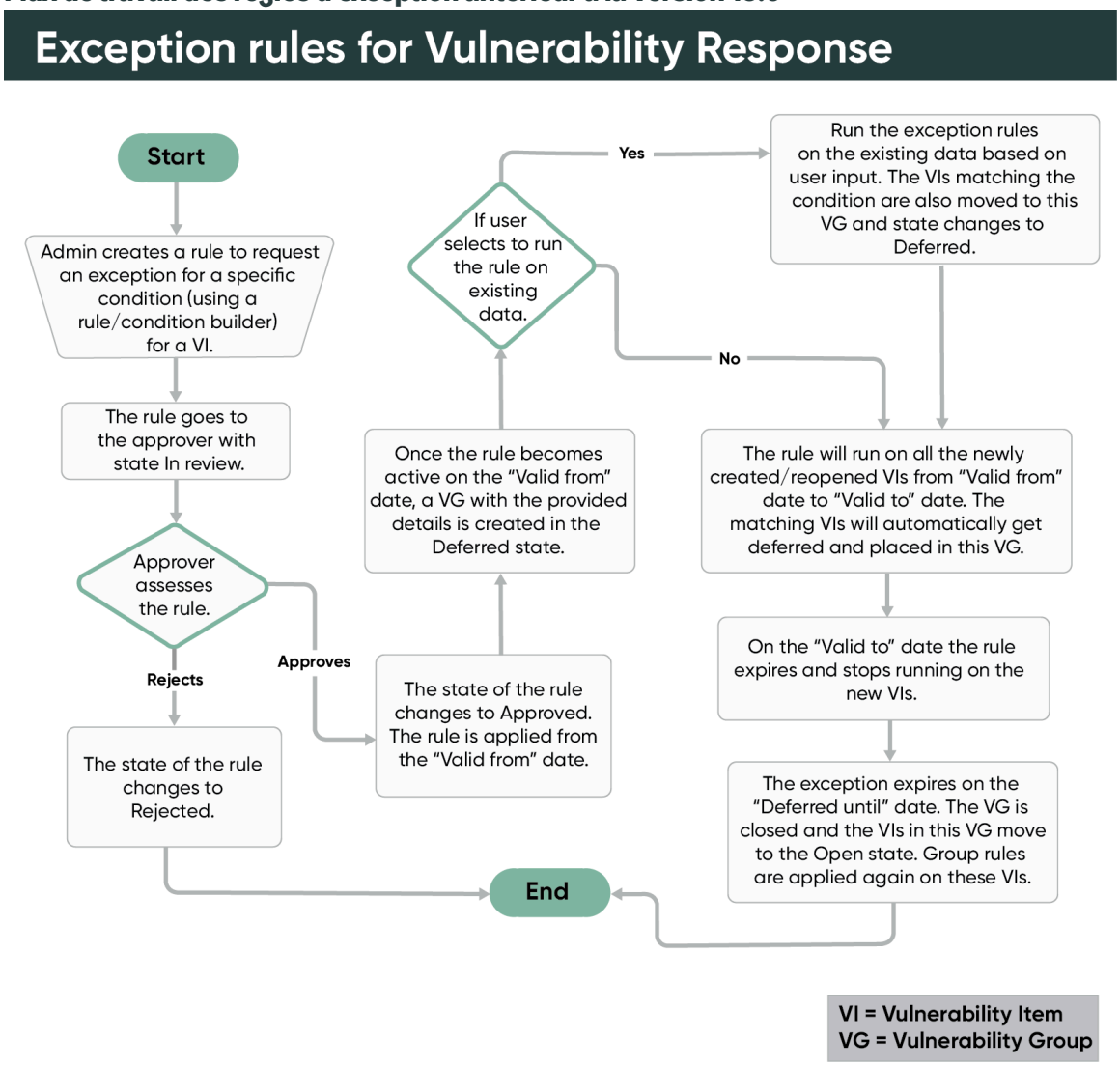
Expiration d'une règle d'exception

Après l'expiration de la règle d'exception, elle ne s'exécute plus sur les nouveaux VI ou les VI rouverts. Le RT associé reste à l'état Différé jusqu'à la date « Différé jusqu'à ».

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de travail des règles d'exception antérieur à la version 15.0



Traduction automatique

Vue d'ensemble des règles d'exclusion

Les règles d'exclusion permettent de filtrer ou d'empêcher que des détections ne soient converties en éléments vulnérables (VIT) au cours du processus d'ingestion dans Réponse aux vulnérabilités.

Ces règles peuvent être configurées pour gérer divers scénarios tels que :

- À l'exclusion des vulnérabilités de faible gravité ou à faible risque qui ne nécessitent pas de correction immédiate.
- Améliorer le processus de rattrapage en hiérarchisant les VIT les plus critiques pour une action.
- Réduction du temps de traitement pendant l'importation des données en excluant un pourcentage de détections de la conversion VIT.

Au cours du processus d'ingestion des données, il existe des approches distinctes pour gérer les détections nouvelles et existantes.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour les nouvelles détections :
  - Si une nouvelle détection ne répond pas aux conditions d'une règle d'exclusion, une détection est créée avec les VIT.
  - Si une nouvelle détection répond aux conditions d'une règle d'exclusion, la règle est associée à la détection, mais VIT n'est pas créée. Renseignez la référence de la règle d'exclusion correspondante sur l'enregistrement de détection. La colonne Règle d'exclusion est renseignée avec la référence à la règle d'exclusion sur l'enregistrement de détection en conséquence.
- Pour les détections existantes :
  - Si la détection ne répond aux conditions d'aucune règle d'exclusion, elle poursuit le workflow normal.
  - Si une détection existante correspond aux conditions d'une règle d'exclusion, le VIT associé à cette détection reste dans son état actuel, mais la règle est associée à la détection. L'état de la VIT est régi par la valeur définie dans la *sn_vul.close_vit_with_excluded_detections* propriété. Par défaut, la valeur de cette propriété est définie sur Faux. Si la valeur est définie sur Faux, les détections sous un VIT sont exclues et l'état des VIT reste dans son état actuel. Toutefois, si la valeur est définie sur Vrai, les scénarios suivants peuvent se produire :
    - Si toutes les détections sous un VIT sont exclues, l'état du VIT est mis à jour sur Fermé exclu.

      Remarque : À partir de la v22.1.2 d'un Réponse aux vulnérabilités nouveau sous-état appelé Exclu a été ajouté,

    - Si une détection est marquée comme fermée tandis que les autres sont exclues, la VIT est désignée comme fermée fixe.
    - Si le VIT comporte des détections ouvertes, il reste ouvert.

Information associée

Créer une règle d'exclusion

Vue d'ensemble des faux positifs

Un faux positif est une condition dans laquelle le scanner signale qu'une vulnérabilité existe dans le système, mais en réalité il n'y a pas de vulnérabilité. Il peut y avoir plusieurs raisons, comme une classification incorrecte, une logique ou un algorithme incorrect dans le scanner. Le propriétaire du rattrapage peut marquer les éléments vulnérables (VI) ou les tâches de rattrapage (RT) comme des faux positifs.

Important : Vous pouvez marquer les éléments vulnérables de l'hôte comme faux positif en bloc dans le Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations sur le marquage des éléments vulnérables de l'hôte comme faux positif en bloc, reportez-vous à la section Modifier en bloc le faux positif dans l'espace de travail du gestionnaire de vulnérabilité.

Cycle de vie d'un faux positif

Signification de faux positif

Le scanner donne parfois un avertissement, alors qu'en réalité il n'y a pas de vulnérabilité. Par exemple, si un élément de configuration a été mis hors service, mais que le scanner soulève toujours un problème connexe, marquez-le comme faux positif.

Marquage comme faux positif

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus de détails sur le marquage d'un VI ou d'un RT comme faux positif, reportez-vous à la section Marquer comme faux positif.

Utiliser le faux positif

Une fois qu'un VI ou un RT est marqué comme faux positif, l'état est mis à jour sur Fermé et le sous-état passe à Faux positif. Les actions suivantes peuvent être effectuées :

- Rouvrir
- Supprimer
- Mettez à jour la date dans le champ **Jusqu'à** . Cette date est ensuite utilisée comme date d'expiration du faux positif.

Remarque : S'il n'est pas approuvé, le VI ou le RT revient à son état précédent.

Approbation d'un faux positif

L'approbateur peut approuver le faux positif à partir de son workflow d'approbation.

Remarque :

À partir de Vulnerability Response v15.0, si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et les faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Réouverture d'un faux positif

Un VI ou RT dans un sous-état de faux positif peut être rouvert à tout moment.

Suivi d'un faux positif

Utilisez la section **Approbations de changement de l'état** pour suivre l'état du faux positif. Une fois approuvé, l'état du VI ou du RT est mis à jour sur Fermé et le motif est Faux positif.

Expiration d'un faux positif

Seul l'approbateur du faux positif peut définir une date de fin pour le faux positif, pour l'expiration du VI ou du RT. En outre, seuls les faux positifs pour lesquels l'approbateur a fourni une date de fin peuvent expirer. Cette date peut être fournie une fois le faux positif approuvé.

Un faux positif sans date de fin est un faux positif permanent. Après l'expiration du faux positif, l'état du VI ou du VR revient à Ouvert.

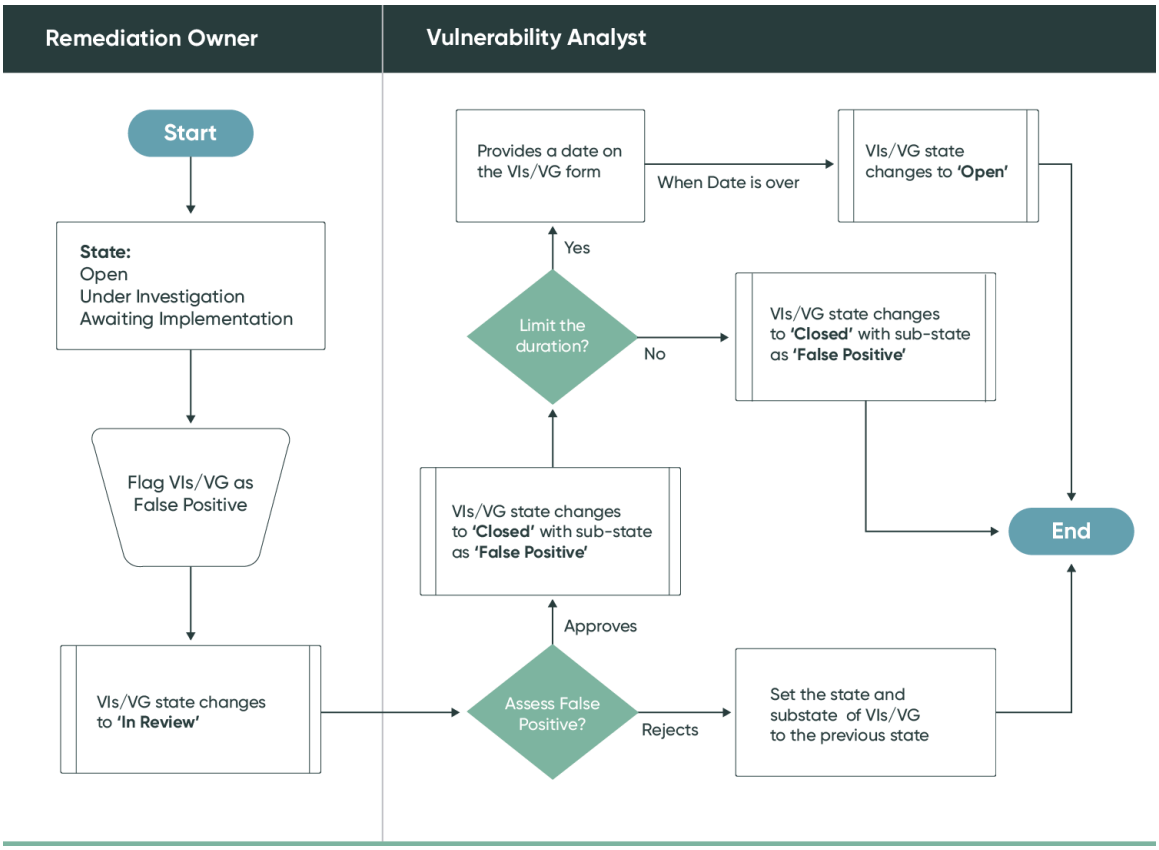
Remarque :

À partir de la version 21.0 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Processus d'approbation des faux positifs antérieur à la version 15.0



Le processus d'approbation est automatique si tous les VI passent l'analyse suivante. Les VI se ferment automatiquement, quel que soit leur état actuel. Les champs des VI ou, le cas échéant, de **l'état de** RT basculent sur **Fermé** avec le sous-état **Fixe.**

Pour plus d'informations, consultez Marquer et approuver un faux positif.

Information associée

Demander un faux positif pour un élément vulnérable ou une tâche de rattrapage

Prise en charge des questionnaires dans la gestion des exceptions via l'évaluation intelligente

Configurez des questionnaires avancés dans le cadre du processus de gestion des exceptions à l'aide de l'évaluation intelligente. Cela permet aux propriétaires de rattrapages de fournir un contexte plus détaillé pour les demandes d'exception et aux approbateurs de configurer des questions conditionnelles pour recueillir des informations afin de prendre des décisions éclairées.

Rôles requis

Lecteur de modèle d'évaluation intelligente : **sn_vul_cmn.smart_assessment_template_manager** (administrateur de vulnérabilité et lecteur de modèle) permet aux administrateurs de créer et de modifier des modèles.

Acteur d'évaluation intelligente : **sn_vul_cmn.smart_assessment_actor** vous permet (propriétaires et administrateurs de rattrapage) de remplir les questionnaires/évaluations.

Lecteur d'évaluation intelligente : **sn_vul_cmn.smart_assessment_reader** vous permet (Approbateur) de lire les réponses au questionnaire soumises.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Condition préalable : les modules d'extension d'évaluation intelligente doivent être installés, car l'évaluation intelligente est une dépendance de Vulnerability Response.

Vous pouvez maintenant configurer les questionnaires dans le cadre du processus de gestion des exceptions à l'aide de l'Évaluation intelligente. Elle permet aux administrateurs/gestionnaires de vulnérabilité de configurer des questions conditionnelles afin de recueillir les bonnes informations nécessaires à une prise de décision éclairée, tout en permettant aux propriétaires de rattrapage de fournir un contexte plus détaillé pour les demandes d'exception. Cela améliore la collaboration entre les équipes de gestion des vulnérabilités et de rattrapage en rationalisant le processus d'approbation et en garantissant la clarté et l'exhaustivité des justifications d'exception.

Les questionnaires et les évaluations intelligentes sont accessibles dans Workspace ainsi que dans l'interface utilisateur classique, car certains workflows nécessitent toujours les anciens questionnaires de style, tandis que la nouvelle évaluation est plus conviviale et n'est prise en charge que dans Workspace.

Dans l'écran **de configuration de la gestion des exceptions** , vous pouvez maintenant sélectionner l'évaluation pour les enregistrements de contrôle de compensation, de demande d'exception et de faux positif.

Remarque : Si vous choisissez de remplir le champ « Évaluation pour demander une exception », le système vous permet d'examiner le modèle d'évaluation intelligente, ou bien les questionnaires classiques sont pris en compte.

Vous pouvez utiliser les deux options fournies ci-dessous :

- **Évaluation intelligente** : gérez les questionnaires dans l'espace de travail de vulnérabilité.
- **Questionnaire existant** : vous pouvez accéder au questionnaire existant à la fois dans l'espace de travail et dans l'expérience classique.

Les modèles ci-dessus peuvent être consultés/modifiés par le lecteur de modèle d'évaluation intelligente : **sn_vul_cmn.smart_assessment_template_manager**.

Configurer le modèle d'évaluation

Les modèles d'évaluation contiennent les questions qui vous seront posées au cours du processus de demande (par exemple, lors de la demande d'une exception). Les modèles préconfigurés mentionnés ci-dessus sont fournis avec une évaluation intelligente. Vous pouvez également créer vos propres modèles selon vos besoins.

Avant de commencer

Rôle requis :

Rôle de lecteur de modèle : **sn_vul_cmn.smart_assessment_reader** vous permet (en tant qu'approbateur) de lire les réponses au questionnaire soumises.

Rôle d'acteur de modèle : **sn_vul_cmn.smart_assessment_actor** Vous permet (propriétaire et administrateur du rattrapage) de remplir les questionnaires/évaluations.

Pourquoi et quand exécuter cette tâche

Dans l'espace de travail Réponse aux vulnérabilités, vous pouvez sélectionner le modèle avec la cible d'évaluation comme VCA, à utiliser pour la demande d'exception (par exemple, Exception pour Vulnerability Response, Faux positif pour Vulnerability Response). Si vous sélectionnez le modèle par défaut, les questions sont automatiquement remplies. Si vous choisissez de créer votre propre modèle, il peut être modifié.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à l'espace de travail d'évaluation.
2. Sélectionner un **modèle d'évaluation** existant ou sélectionner un**nouveau modèle**
3. Renseignez les champs suivants :
   - **Nom du modèle** : nom unique pour le modèle
   - **Nom de l'évaluation** : nom affiché dans le système lors de l'affichage de l'évaluation.
   - **Catégories de modèles** : les modèles sont catégorisés pour faciliter la gestion. Certaines catégories de modèles sont fournies prêtes à l'emploi. Par exemple, les modèles de questionnaire de réponse aux vulnérabilités. Vous pouvez créer les modèles de votre choix.
   - **Cibles d'évaluation** : spécifie la table à laquelle le modèle est associé. Pour la VR, il s'agit de la table VCA (Vulnerability Change Approval table).

Workflow d'évaluation intelligente

Les propriétaires de rattrapage doivent remplir le questionnaire avant de soumettre pour approbation. Les approbateurs examinent le questionnaire et prennent des décisions d'approbation ou de rejet en fonction des informations fournies.

Avant de commencer

Rôle requis : **sn_vul_cmn.smart_assessment_reader**

Pourquoi et quand exécuter cette tâche

Voici le flux de travail de l'adaptation d'évaluation intelligente :

- **Demande d'exception/faux positif** Lorsque vous demandez une exception ou marquez un élément comme faux positif, le système vérifie si un questionnaire est nécessaire.
- Si **l'option de questionnaire est activée**, un **message obligatoire** invite l'utilisateur à remplir le questionnaire avant de poursuivre le processus d'approbation.
- **État Brouillon** : l'enregistrement **d'approbation de changement d'état de la vulnérabilité** (VCA) restera à l'état de brouillon jusqu'à ce que le questionnaire soit soumis, et l'élément de vulnérabilité (VIT) sera à l'état ouvert.
- **Vue de l'approbateur** : une fois que les propriétaires de rattrapage ont rempli le questionnaire et l'ont soumis, les enregistrements d'approbation de changement d'état de la vulnérabilité (VCA) et d'élément de vulnérabilité (VIT) passent à l'état En cours de révision. Les approbateurs peuvent consulter les questionnaires à partir de « Toutes les > mes approbations ». La VIT passera à l'état Différé lors de l'approbation des enregistrements. Vous pouvez afficher le questionnaire via un lien soumis par les propriétaires des rattrapages dans l'en-tête du formulaire d'enregistrement.

Procédure

1. Naviguer **Tous** > **Mes approbations**pour afficher le questionnaire.
2. Une fois l'enregistrement **approuvé**, VIT passe à l'état Différé.
3. Vous pouvez afficher le questionnaire via un lien soumis par les propriétaires des rattrapages dans l'en-tête du formulaire d'enregistrement.

Questionnaire pour faux positif ou demande d'exception

Lorsque le questionnaire pour un faux positif ou une demande d'exception est soumis mais n'est pas rempli de manière appropriée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si un questionnaire pour un faux positif ou une exception de demande est rempli mais pas complètement, l'enregistrement VCA passe à l'état « Brouillon ». Si vous souhaitez émettre une exception à partir de la même catégorie, vous serez redirigé vers le questionnaire précédent après une note contextuelle à ce sujet. Si vous souhaitez soumettre un enregistrement de faux positif au lieu d'une exception de demande existante, le système remplace l'approbation de changement d'état de vulnérabilité (VCA) et crée un nouvel enregistrement d'approbation de changement d'état de vulnérabilité (VCA) faux positif.

Si le questionnaire est rempli à moitié et que le même élément de vulnérabilité (VIT)/ou qu'un ÉLÉMENT est ouvert dans la vue classique, vous serez redirigé vers le questionnaire de l'espace de travail pour remplir les données restantes si le même type de demande est émis à nouveau. Si le questionnaire de la vue classique est rempli de manière sélective et que le même élément est ouvert dans l'espace de travail, le questionnaire de vue classique s'ouvre dans l'espace de travail.

Chien de garde pour Réponse aux vulnérabilités

Le chien de garde est utilisé pour suivre les tables en fonction des conditions que vous spécifiez. Par exemple, il peut être utilisé pour consigner les détails des échecs d'exécution de l'intégration dans Réponse aux vulnérabilités.

Vous pouvez choisir d'être informé de ces échecs. Sur la base de cette notification, vous pouvez planifier le rattrapage. Les chiens de garde par défaut sont les suivants :

- Échec de l'exécution de l'intégration : si l'état de l'exécution de l'intégration est défini sur Terminé et que le sous-état est défini sur Échec, les utilisateurs et les groupes d'utilisateurs sont informés si la condition renvoie un nombre supérieur à 0, c'est-à-dire si l'exécution de l'intégration échoue.
- Intégrations à exécution longue : script pour vérifier si l'exécution de l'intégration dépasse la durée définie. Cet organisme de surveillance vous alerte de manière proactive chaque fois qu'il y a un retard dans l'exécution de l'intégration.
- Exécutions périodiques qui se chevauchent : script pour vérifier les exécutions d'intégration récurrentes qui continuent de s'exécuter pendant leur prochaine occurrence. Il génère un lien contenant la liste de ces exécutions d'intégration.

Journal de surveillance

Le chien de garde est livré avec un journal de surveillance, qui fournit un compte du nombre de fois où la condition a été remplie.

Tableau de bord de vue d'ensemble

Utilisez le tableau de bord Vue d'ensemble pour surveiller l'organisme de surveillance au cours des 30 derniers jours. Vous pouvez créer plusieurs widgets pour suivre d'autres rubriques de surveillance que vous surveillez.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Rapport

Nom	Description

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapport (suite)

Échec de WatchDog au cours des 30 derniers jours	Toutes les conditions sont remplies au cours des 30 derniers jours.

Pour plus d'informations, consultez Configurer WatchDog et Gestion des erreurs pour les détections.

Change Management pour Réponse aux vulnérabilités

En tant que propriétaire d'un rattrapage informatique, vous pouvez créer et gérer des demandes de changement (CHG) directement à partir des tâches de rattrapage (RT) dans l'application Réponse aux vulnérabilités . Les demandes de changement vous aident à initier et à suivre les activités de changement sur vos actifs afin que vous puissiez corriger vos tâches de rattrapage et leurs éléments vulnérables correspondants.

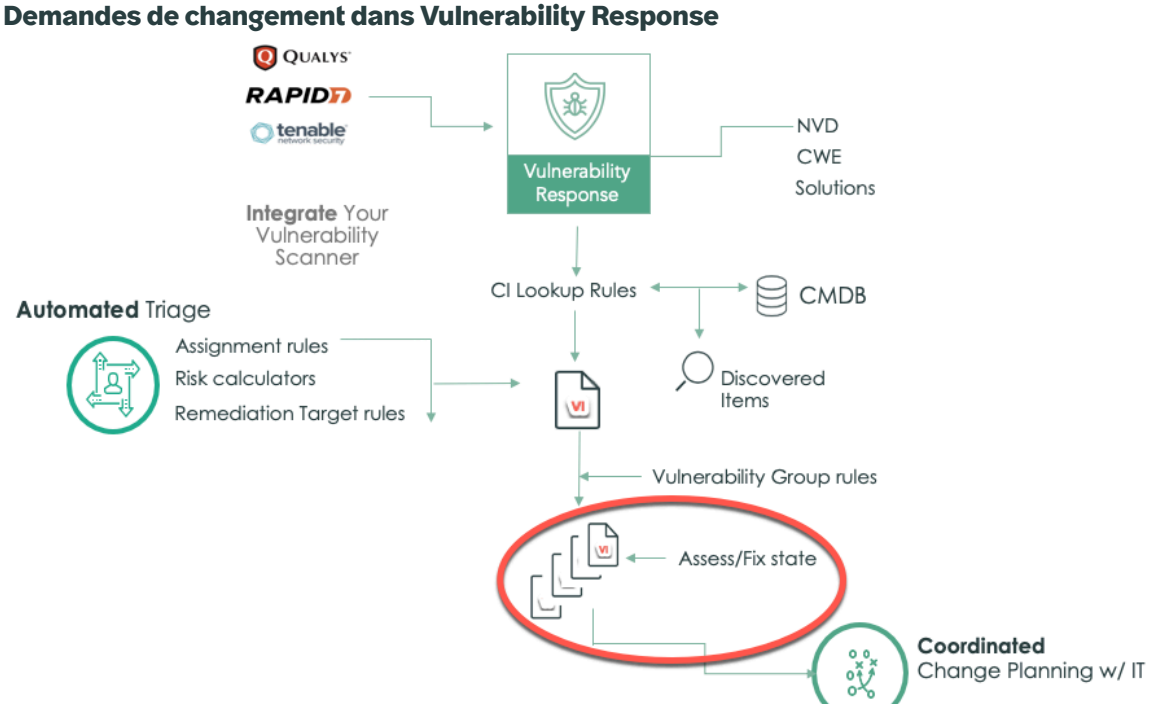
Les demandes de changement et le workflow de vulnérabilité

Si vous n'êtes pas familier avec l'application Vulnerability Response, reportez-vous à la section Explorer l'application Réponse aux vulnérabilités.

L'image suivante illustre le flux d'informations pour Réponse aux vulnérabilités, de l'intégration (scanner) configurée au triage automatisé et à l'enquête.

Les demandes de changement et la gestion des changements font partie du processus de rattrapage (état Évaluer/Corriger) dans le Réponse aux vulnérabilités workflow illustré dans la figure suivante. Au cours de cette phase, vous pouvez utiliser les demandes de changement pour lancer et suivre le rattrapage des vulnérabilités. Vous pouvez créer et gérer des demandes de changement directement à partir de la tâche de rattrapage et répertorier les tâches d'enquête et de rattrapage qui incluent des solutions pour les actifs impactés pour les éléments de configuration (CI) dans votre CMDB.

Demandes de changement dans Vulnerability Response



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Quand utiliser les demandes de changement dans Vulnerability Response

En tant que propriétaire d'un rattrapage informatique, vous pouvez créer des demandes de changement à partir d'une tâche de rattrapage si un processus manuel et contrôlé de quelque nature que ce soit est nécessaire pour modifier ou supprimer des éléments de configuration (CI) pris en charge dans votre CMDB. La création et la gestion des demandes de changement directement à partir d'un enregistrement de tâche de rattrapage vous aident à enquêter et à résoudre rapidement les vulnérabilités. Les éléments vulnérables d'une tâche de rattrapage résolue peuvent être analysés et vérifiés lors de la prochaine analyse planifiée dans votre ServiceNow AI Platform et renvoyés au triage automatisé du Réponse aux vulnérabilités workflow. Les interventions manuelles qui peuvent nécessiter des demandes de changement comprennent les exemples suivants :

- Un correctif logiciel, un correctif ou une autre tâche informatique requise sur les éléments vulnérables avant la résolution RT.
- Vous déterminez qu'un sous-ensemble des éléments vulnérables dans une tâche de rattrapage nécessite une enquête plus approfondie ou une réaffectation à un autre département.
- Vous déterminez qu'un sous-ensemble d'éléments vulnérables dans un RT avec un grand ensemble d'éléments vulnérables peut être déplacé vers une nouvelle tâche de rattrapage.
- Vous pouvez associer une tâche de rattrapage à une demande de changement existante pour éviter la duplication des tâches de rattrapage.

Types de demandes de changement pour un RT

L'application Réponse aux vulnérabilités utilise les trois types de changements de service pris en charge par le ITSM Gestion des changements produit sur votre ServiceNow AI Platform® instance : standard, urgent et normal. Le type de changement que vous sélectionnez détermine le modèle d'état invoqué et le processus de changement à suivre. Les demandes de changement enregistrent les informations détaillées sur le changement, telles que la raison du changement, la priorité, le risque, le type et la catégorie du changement. Voir Types de changement .

Réponse aux vulnérabilités En tant que propriétaire d'un rattrapage informatique, vous disposez des options suivantes pour créer des demandes de changement normal, standard et urgent directement à partir d'une tâche de rattrapage :

- Vous pouvez créer des demandes de changement qui contiennent des informations pré-remplies de la tâche de rattrapage pour rationaliser le processus et gagner du temps.
- Vous pouvez associer une tâche de rattrapage à une demande de changement existante pour éviter de créer des demandes de changement en double qui partagent des informations similaires et des éléments vulnérables.
- À l'aide d'un ensemble de conditions, vous pouvez filtrer un sous-ensemble d'éléments vulnérables et diviser une tâche de rattrapage. Les éléments que vous sélectionnez sont automatiquement déplacés vers un nouveau RT.

Vous pouvez filtrer les éléments vulnérables à l'aide des valeurs de n'importe quel champ d'une tâche de rattrapage et appliquer la demande de changement uniquement aux éléments qui correspondent à vos critères de filtre.

Information associée

Créer une demande de changement à partir d'une tâche de rattrapage

Associer une tâche de rattrapage à une demande de changement existante

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fractionner une tâche de rattrapage

Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage

Évaluation de l'exposition logicielle à l'aide de Gestion des actifs logiciels (SAM Foundation)

Utilisez l'application Évaluation de l'exposition aux vulnérabilités ServiceNow® pour déterminer le nombre total de logiciels installés pour un package logiciel spécifique sur vos actifs. Lorsqu'il est utilisé avec l'application ServiceNow® Software Asset Management (SAM) Foundation, évaluez votre exposition, créez des éléments vulnérables et gérez le rattrapage des logiciels vulnérables détectés.

Important : Vous pouvez effectuer l'évaluation de l'exposition à l'aide des vulnérabilités et expositions courantes (CVE) et du logiciel pour tirer parti des options supplémentaires de l'espace de travail Évaluation de la vulnérabilité. Pour plus d'informations, consultez Explorer l'espace de travail de l'évaluation de la vulnérabilité.

Déterminez votre exposition aux logiciels vulnérables en fournissant les informations sur les logiciels vulnérables (éditeur, produit, édition et version) sans utiliser la base de données des vulnérabilités et expositions communes (CVE). Évaluez les cas de vulnérabilités logicielles zero-day (jour courant) pour les cas suivants :

- Lorsque les produits ne disposent pas encore de données CVE.
- Lorsqu'il y a un décalage entre le moment où une vulnérabilité est connue du public et le moment où les données CVE avec la vulnérabilité sont mises à jour dans le NVD.
- Lorsque vous en apprenez davantage sur la vulnérabilité entre les analyses planifiées de votre analyseur de vulnérabilité.

Avec l'application Évaluation de l'exposition aux vulnérabilités , si vous connaissez l'éditeur et le produit des logiciels vulnérables, en utilisant les enregistrements qui répertorient les logiciels installés dans votre réseau créés par l'application, vous pouvez évaluer votre exposition aux packages logiciels potentiellement malveillants à la SAM Foundation demande.

Connaître l'ampleur de votre exposition à ce type de vulnérabilité vous permet de réagir de manière proactive en mettant en place une alerte rouge et en désinstallant le logiciel, ou en informant votre centre d'opérations de sécurité (SOC) de rechercher un correctif spécifique. Vous pouvez créer des éléments vulnérables et affecter des tâches au spécialiste du rattrapage pour un rattrapage plus approfondi. Affichez une liste de tâches de rattrapage (VUL) pour vérifier que les éléments vulnérables que vous souhaitez sont créés et associés correctement à la VUL.

Information associée

Configurer l'évaluation de l'exposition à la vulnérabilité

Évaluez votre exposition aux logiciels vulnérables

Gestion de crise de vulnérabilité

Créez et suivez les événements de vulnérabilité critiques via le workflow Gestion de crise de vulnérabilité (VCM). Créez des enregistrements d'évaluation des vulnérabilités, enregistrez les attributs clés de la vulnérabilité pour calculer le risque, effectuez une évaluation pour identifier le niveau d'exposition et impliquez les personnes concernées pour une réponse coordonnée et rapide aux vulnérabilités.

Gestion des événements de crise de vulnérabilité

Vulnerability Crisis Management est un workflow complet pour gérer les événements de crise de vulnérabilité avec les fonctionnalités suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Identifiez efficacement les éléments de configuration vulnérables en corrélant les vulnérabilités critiques avec l'inventaire des installations logicielles à partir de l'inventaire Nomenclature logicielle (Gestion des actifs logiciels SBOM), les vulnérabilités signalées par les scanners et Base de données de gestion des configurations (CMDB).
- Convertissez les résultats de l'évaluation en éléments vulnérables pour le rattrapage.
- Déclencher un incident de sécurité majeur pour garantir une réponse rapide et coordonnée à la menace.
- Engagez et collaborez avec les équipes de l'ensemble de l'organisation pour faciliter une réponse unifiée aux vulnérabilités.
- Fournir des rapports d'étape réguliers aux parties prenantes interfonctionnelles et aux équipes impliquées afin de maintenir la transparence et la communication tout au long de la crise.

Gestion de crise de vulnérabilité à l'aide de l'espace de travail Évaluation de la vulnérabilité

Remarque : À partir de la version 1.0.1 de Vulnerability Crisis Management, l'application est disponible sous forme d'abonnement distinct dans la boutique. Vous pouvez accéder à Vulnerability Crisis Management à partir de l'espace de travail Évaluation de la vulnérabilité uniquement si vous disposez d'une autorisation affinée ou si vous avez installé l'application à partir de la boutique. Auparavant, Vulnerability Crisis Management était inclus dans le module d'extension Vulnerability Emergency Response. À partir de la version 3.2.2, le module d'extension Vulnerability Emergency Response a été renommé Vulnerability Exposure Assessment.

Lors de l'identification d'une vulnérabilité d'intérêt, le gestionnaire d'événements de vulnérabilité crée un enregistrement d'évaluation de la vulnérabilité avec des informations sur la source des renseignements sur les menaces, les caractéristiques de vulnérabilité et les produits affectés. Ces informations sont utilisées pour une analyse plus approfondie de l'impact et de l'exposition.

Une fois l'enregistrement d'une vulnérabilité d'intérêt créé, une évaluation des risques est effectuée. Cette évaluation comprend la notation structurée des risques, l'examen de l'enregistrement et les observations de l'analyste qui exécute la tâche. Le score de risque initial pour une vulnérabilité d'intérêt est calculé à l'aide des attributs disponibles au moment de la création de l'événement. Le score de risque pour l'évaluation peut changer à mesure que des informations supplémentaires deviennent disponibles. Utilisez le score de risque pour déterminer l'impact potentiel de l'exploitation et établir les priorités de réponse.

Une fois que l'évaluation d'une vulnérabilité d'intérêt a été créée et déterminée comme présentant un risque pour l'infrastructure de l'organisation, vous pouvez analyser la menace plus en détail en mettant à jour l'évaluation des risques avec une évaluation approfondie de l'exposition avec l'inventaire des installations logicielles de (Nomenclature logicielle SBOM) inventaireGestion des actifs logiciels, les vulnérabilités signalées par les scanners et Base de données de gestion des configurations (CMDB). Les éléments de configuration et les applications impactés sont automatiquement identifiés par évaluation. Des éléments concernés supplémentaires peuvent être ajoutés manuellement.

Une fois l'évaluation terminée, des éléments vulnérables ou des éléments vulnérables d'applications peuvent être créés pour les résultats d'exposition qui n'ont pas déjà d'élément vulnérable associé. Le calculateur de score de risque des éléments vulnérables peut être exploité/configuré pour ajuster le score de risque pour les éléments vulnérables liés aux enregistrements d'évaluation de vulnérabilité. L'enregistrement d'évaluation de vulnérabilité peut être affecté au niveau d'exposition et à la priorité d'événement. En fonction de la priorité de l'événement, le gestionnaire d'événements de vulnérabilité peut

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

choisir de proposer, de promouvoir ou de lier l'évaluation de la vulnérabilité à un incident de sécurité majeur.

Utilisez cette fonction Gestion des incidents de sécurité majeurs pour suivre et gérer les activités de rattrapage, lier les incidents de sécurité en cours, créer des tâches ad hoc, impliquer les équipes affectées, envoyer des rapports d'état et collaborer à l'aide des intégrations de collaboration disponibles dans Gestion des incidents de sécurité majeurs.

ServiceNow® Gestion des actifs logiciels et Nomenclature logicielle (SBOM) une logique d'évaluation et de traitement

À l'aide Gestion des actifs logiciels des données, les CPE provenant de NVD pour les CVE, puis les modèles de détection sont récupérés à l'aide de la logique de correspondance de chaîne. Une fois les modèles de détection extraits, une analyse des installations connexes est exécutée, les éléments de configuration connexes sont récupérés et la table Élément de configuration affecté est renseignée. Vous pouvez fournir des détails supplémentaires tels que l'éditeur, le produit, la version et l'édition. En fonction de ces éléments, tous les modèles de détection et les installations de logiciels correspondants pour l'enregistrement sont récupérés. Ensuite, les éléments de configuration connexes sont récupérés et la table Élément de configuration affecté est remplie à nouveau.

Pour SBOM, le logiciel associé pour les CVE à partir de la table connexe (m2m) (entre CVE et le logiciel) est récupéré. Après avoir extrait les détails logiciels, les composants SBOM connexes sont identifiés en faisant correspondre le produit et la version du composant SBOM au produit et à la version du logiciel identifiés.

Une fois les composants associés trouvés, les entités associées aux composants sont extraites. Le modèle de produit des entités et le CI associé (s'il est trouvé) sont récupérés et l'élément de configuration est enregistré dans la table Élément de configuration affecté. Si l'élément de configuration est exempt d'éléments vulnérables, vous pouvez l'utiliser pour créer l'élément vulnérable. Si aucun élément de configuration n'est trouvé, le modèle de produit est enregistré dans la table Modèle logiciel affecté et peut être utilisé pour créer des éléments vulnérables de l'application.

Pour plus d'informations sur l'utilisation du workflow Gestion de crise de vulnérabilité, consultez Utilisation de l'espace de travail Évaluation de la vulnérabilité.

Information associée

Explorer l'évaluation des vulnérabilités

Explorer l'espace de travail de l'évaluation de la vulnérabilité

Onglet Évaluation

Séparation de domaine et Réponse aux vulnérabilités

L'application Séparation de domaine est prise en charge dans Réponse aux vulnérabilités. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Standard

- Inclut tous les aspects du support de niveau **basique** .
- Les propriétés d'application sont sensibles au domaine selon les besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Comment fonctionne Séparation de domaine dans Réponse aux vulnérabilités

Grâce à Séparation de domaine, vous pouvez standardiser les procédures VR (Réponse aux vulnérabilités) pour l'ensemble de la clientèle que vous servez, avec des coûts opérationnels réduits et une meilleure qualité de service.

Séparer les espaces de travail des clients pour les workflows, les tableaux de bord, les rapports, etc., garantit que les données client sont séparées et ne sont jamais exposées à d'autres clients.

Prise en charge de Domain Separation dans Vulnerability Response par version.

Mise en production	Niveau de prise en charge	Notes
Orlando	Standard	
Paris	Standard	
Québec	Standard	
Rome	Standard	
San Diego	Standard	
Tokyo	Standard	
Utah	Standard	
Vancouver	Standard	
Washingtondc	Standard	

Séparation de domaine pour l'application Réponse aux vulnérabilités couvre les fonctionnalités de produit suivantes :

- Ingère les éléments vulnérables à partir d'analyseurs tiers (par exemple, Qualys, Rapid 7 ou Tenable) dans le domaine approprié. Les données sont ingérées dans le même domaine que celui de l'utilisateur d'intégration, dont les informations d'identification sont utilisées pour l'intégration.
- Scanne à nouveau des actifs Réponse aux vulnérabilités spécifiques dans le domaine à partir duquel ils ont été demandés.
- Utilise le processus de recherche de CI CMDB pour s'assurer que les informations CI provenant des scanners correspondent aux CI dans la CMDB du domaine de l'utilisateur d'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Calcule les scores de risque au niveau de l'élément vulnérable selon le calculateur de score de risque défini dans le même domaine que celui de l'utilisateur d'intégration.
- Les règles de cibles de rattrapage sont exécutées sur les éléments vulnérables conformément aux règles de cibles de rattrapage définies dans le même domaine que celui de l'utilisateur d'intégration.
- La ou les règles de tâche de rattrapage peuvent être définies et rester dans le même domaine que le domaine de l'utilisateur d'intégration.
- Les tâches de rattrapage créées à l'aide des règles de tâche de rattrapage restent dans le même domaine que celui dans lequel les règles de groupe sont créées.
- Le workflow de report passe par le processus d'approbation dans le domaine pour lequel le report est demandé.
- Les rapports et les tableaux de bord affichent les états des éléments vulnérables tels que l'âge de l'élément vulnérable, les éléments vulnérables ouverts par CI, les vulnérabilités par impact et l'état de la date cible de rattrapage dans le domaine auquel il appartient.
- Les connaissances provenant de scanners tiers ou de la base de données de vulnérabilité nationale (NVD) peuvent être ingérées dans le domaine mondial et les données peuvent être partagées entre plusieurs clients.

Remarque : Dans tous les cas ci-dessus, les principes généraux de la séparation dans des domaines séparés s'appliquent dans la Now Platform.

Pour plus d'informations sur la création et la prise en charge des importations séparées par domaine, consultez Créer des importations séparées par domaine pour une intégration et Créer et prendre en charge plusieurs domaines dans le cadre des tâches en arrière-plan.

Cas d'utilisation

L'application Réponse aux vulnérabilités gère le cycle de vie d'un élément de vulnérabilité de bout en bout. Les cas d'utilisation suivants sont sensibles à la séparation de domaine :

- **Ingérer** des éléments vulnérables (vulnérabilités sur l'actif) à partir de votre intégration tierce.
  - Ingérer des données à partir de plusieurs instances
  - Dédupliquer l'élément vulnérable
  - Correspondance avec le CI CMDB
- **Enrichissement** de l'élément vulnérable avec les scores de risque et les dates cibles de rattrapage
  - Enrichissement des actifs (CMDB)
  - Enrichissement du score de risque et de la date cible de rattrapage
- **Regrouper** les éléments vulnérables et affecter la tâche de rattrapage
  - Regroupement automatique des éléments vulnérables
  - Affecter automatiquement la tâche de rattrapage
- **Rattraper**
  - Tâches de rattrapage
  - Cycle de vie complet des rattrapages
  - Workflow du report

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Mesurer** la posture de sécurité de l'organisation et le programme de gestion des vulnérabilités
  - Tendance de vulnérabilité, actif le plus vulnérable, vulnérabilité par âge
  - État du rattrapage à la date cible de rattrapage

Configuration

La configuration de Séparation de domaine pour Réponse aux vulnérabilités ne nécessite aucune étape supplémentaire. Toutes les Réponse aux vulnérabilités tables acquièrent la colonne Domaine une fois que l'instance est séparée par domaine. Vous pouvez diriger les données d'importation d'intégration de vulnérabilité vers des domaines spécifiques. Consultez Créer des importations séparées par domaine pour une intégration pour plus d'informations.

Données séparées par domaine

Les données peuvent être séparées par domaine, ce qui signifie :

- L'élément vulnérable ingéré à partir d'analyses tierces reste dans le même domaine que le domaine de l'utilisateur d'intégration et n'est accessible à partir d'aucun autre domaine.
- Les vulnérabilités, les éléments vulnérables (instances) ou les actifs d'un domaine ne peuvent pas être consultés à partir d'autres domaines.
- L'algorithme de notation des risques, les règles de tâche de rattrapage et les règles de cibles de rattrapage ne peuvent être consultés par personne en dehors du domaine.
- Les informations de vulnérabilité du NVD peuvent exister dans le domaine global et être partagées avec tous les clients.
- Les tâches de rattrapage dans un domaine ne peuvent pas être visualisées à partir d'un autre domaine.
- Les workflows de report créés dans un domaine ne sont pas visibles dans un autre domaine.
- Toutes les notifications par e-mail sont contenues dans le domaine auquel elles appartiennent.

Remarque :

Les modèles d'importation planifiée disponibles sur l'instance sont définis par défaut sur « Domaine : global ». Ainsi, pour éviter tout conflit lorsqu'il y a plusieurs domaines sur les instances, adaptez la pratique suivante :

- Répartissez les modèles d'importation disponibles sur l'instance dans le nombre de domaines impliqués dans l'intégration.
- Mettez à jour le domaine de l'enregistrement de modèle d'importation vers la sys_id du domaine cible.
- Si nécessaire, créez des modèles d'importation pour chaque domaine.
- Assurez-vous que chaque domaine possède 2 modèles d'importation.
- sn_vul_sched_import_pool : les enregistrements de cette table doivent être séparés par domaine si la séparation de domaine est présente sur l'instance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment les analystes de vulnérabilité gèrent leurs propres données d'application

- Les analystes créent leurs propres règles d'installation d'application, de gestion des applications multisources et de recherche de CI.
- Les analystes peuvent configurer des intégrations spécifiques exclusivement pour une utilisation dans le domaine.
- Les analystes peuvent créer leurs propres workflows de gestion des reports et des changements.
- Les analystes peuvent créer leurs propres règles de tâche de rattrapage, leur propre logique de notation des risques pour hiérarchiser avec précision les vulnérabilités, affecter automatiquement des tâches de rattrapage et les affecter au groupe d'affectation approprié.
- Les utilisateurs du domaine créent un élément de vulnérabilité manuel, puis le ferment.

Logique métier et processus pouvant être séparés par domaine par le propriétaire de l'instance

- Réponse aux vulnérabilités Utilisateurs et groupes
- Intégrations de Réponse aux vulnérabilités
- Configuration complète de la configuration (gestion des utilisateurs et des groupes, installation d'applications, gestion des applications multisources, règles de recherche de CI, règles de tâche de rattrapage, calculateurs de risque, règles de cibles de rattrapage, etc.)
- Cycle de vie complet du rattrapage, y compris le report
- Planifier des travaux

Information associée

Séparation de domaine pour les fournisseurs de services

Mappage des services dans Réponse aux vulnérabilités

Service Mapping aide les organisations à acquérir une compréhension complète de votre infrastructure informatique et des relations entre les différents composants. Elle active la découverte et le mappage automatiques des services, des applications et des composants d'infrastructure, fournissant une représentation visuelle des dépendances et des relations.

Dans Réponse aux vulnérabilités, la tâche *`Set related CI services`* planifiée établit des connexions entre les services d'entreprise affectés et les éléments de configuration (CI) associés aux éléments vulnérables (VIT). Le processus de liaison a lieu une fois l'importation de l'intégration terminée et à un moment désigné. Pour améliorer les performances de cette tâche planifiée, plusieurs changements ont été implémentés à partir de la version 21.1.2 de Réponse aux vulnérabilités. Les voici :

- Calcul du score de risque : le processus de calcul des scores de risque implique l'utilisation de la *`Set related CI services`* tâche planifiée. Une fois le CI traité, cette tâche stocke les données nécessaires dans la table Services associés [sn_vul_m2m_ci_services]. Auparavant, dans , le Conformité de la configuration calcul du risque impliquait d'accéder directement aux *`CIUtils`* de l'interface de programmation d'application (API) afin de récupérer les services de chaque résultat de test pendant l'importationBase de données de gestion des configurations (CMDB). Toutefois, le processus actuel s'appuie sur la sortie de la tâche planifiée de la table Services associés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

[sn_vul_m2m_ci_services] pour calculer le score de risque dans Conformité de la configuration. En outre, le calculateur du système de base a été modifié pour utiliser la table Services associés [sn_vul_m2m_ci_services].

- Taille des services : la valeur de service dans la propriété *sn_sec_cmn.services_affected_by_CI_max_size*système, qui est liée à la *Set related CI services* tâche planifiée, est réduite de 1 000 à 500.
- Profondeur des services : la profondeur de la propriété *sn_sec_cmn.services_affected_by_CI_max_depth*système, qui est liée à la *Set related CI services* tâche planifiée, est réduite de 10 à 5. La valeur du service est également réduite de 1000 à 500.
- Exclusion de CMDB classes : une propriété *sn_sec_cmn.ignoreCIClassForService* système a été introduite pour permettre la configuration des classes pour lesquelles le calcul de CMDB service doit être ignoré. Dans le système de base, cette propriété est définie sur *cmdb_ci_unclassed_hardware*, *cmdb_ci_incomplete_ipsn_sec_cmn_unmatched_ci* car ces classes sont créées par Réponse aux vulnérabilités et peuvent ne pas avoir de mappage de services. Auparavant, le calcul du service était basé sur le VIT. Toutefois, la logique a été modifiée pour utiliser l'élément détecté à la place. L'élément détecté est utilisé pour calculer le service, qui est ensuite associé au CI dans la même table.
- Tâche planifiée pour l'actualisation complète des services : une tâche *Full refresh-related CI services for VI*planifiée à la demande a été introduite pour effectuer une actualisation complète des services. Lorsque vous effectuez une mise à niveau vers la version 21.0 de Réponse aux vulnérabilités, la tâche s'exécute d'abord *Set related CI services* pour une durée plus longue, car la table de base utilise des éléments détectés au lieu d'éléments vulnérables. Par conséquent, la tâche doit traiter tous les éléments détectés qui ont été analysés au cours des 90 derniers jours. De plus, si vous avez besoin d'actualisations de service plus fréquentes, vous pouvez y répondre en programmant des actualisations périodiques hebdomadaires ou en effectuant une actualisation complète. Si vous avez effectué des activités qui ont entraîné des changements dans les services associés à vos CI et que vous souhaitez Réponse aux vulnérabilités refléter ces changements, vous pouvez exécuter le travail *Full refresh related CI services for VI*planifié à la demande. Cette tâche prend en charge tous les éléments détectés enregistrés au cours des 90 derniers jours et actualise les services associés en conséquence.

Information associée

Mappage des services

CIUtils : global

Implémentation de Réponse aux vulnérabilités

Suivez les étapes décrites dans les images suivantes pour télécharger l'application Réponse aux vulnérabilités à partir de , ServiceNow Store installez-la sur votre ServiceNow AI Platform® instance et configurez-la à l'aide de l'assistant de configuration.

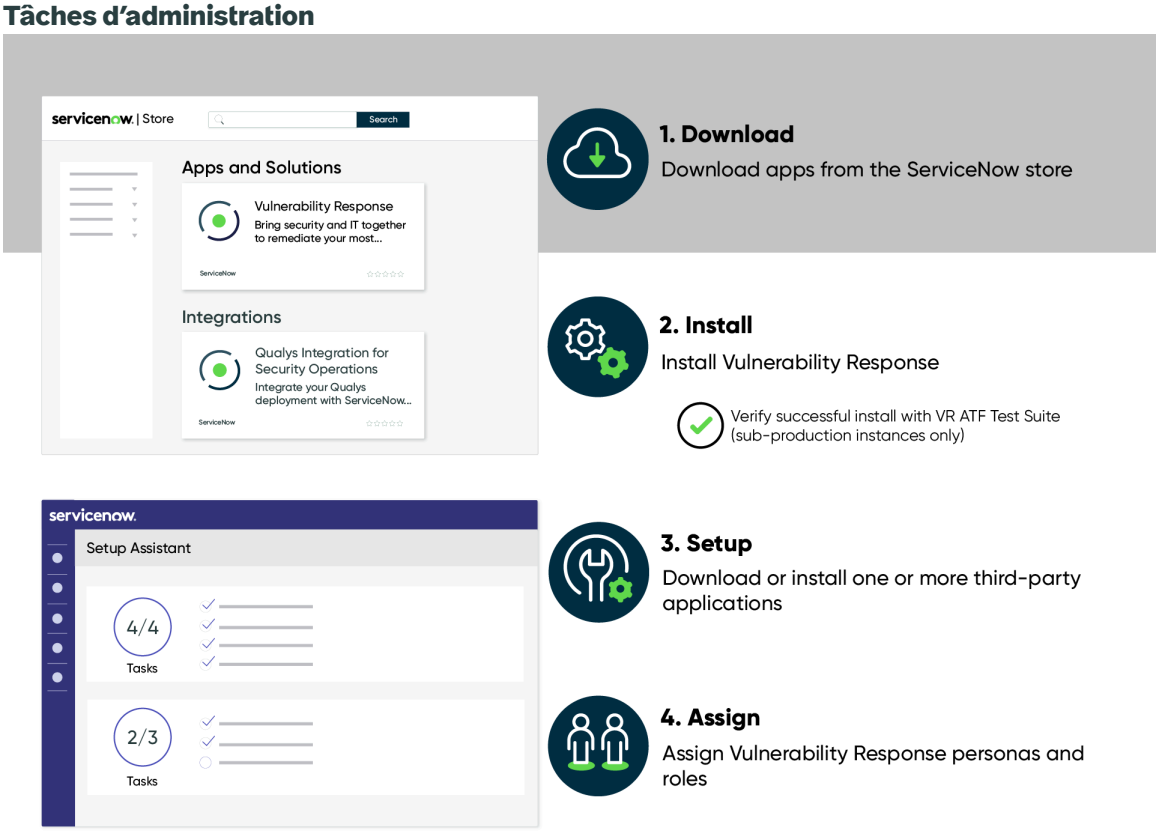
Un exemple d'installation et de configuration pour l'installation du système de base, de l'application Réponse aux vulnérabilités et d'une application d'analyse tierce, l'application Qualys , est illustré dans les images suivantes. Les rôles requis et les tâches obligatoires, ainsi que les étapes facultatives, sont également répertoriés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour en savoir plus sur chaque étape illustrée dans les images suivantes et sur une liste de contrôle contenant des liens vers la documentation associée, reportez-vous à la section Liste de vérification d'implémentation pour l'application Réponse aux vulnérabilités.
- Vous pouvez étendre les concepts et la séquence d'étapes présentés dans cet exemple à l'installation et à la configuration d'autres applications prises en charge pour Réponse aux vulnérabilités. Pour obtenir la liste des applications de support, reportez-vous à la section Installation et prise en charge des Réponse aux vulnérabilités applications.
- Le rôle administrateur est requis pour télécharger et installer l'application et l'application Réponse aux vulnérabilitésQualys Vulnérabilité utilisées dans cet exemple.
- Le rôle d'administrateur affecte également le profil Administrateur de vulnérabilité [sn_vul.vulnerability_admin] et d'autres rôles de Réponse aux vulnérabilités profil aux utilisateurs et aux groupes.

Tâches d'administration



Le rôle sn_vul.vulnerability_admin configure les applications et Qualys dans l'Assistant Réponse aux vulnérabilités de configuration et vérifie les résultats attendus.

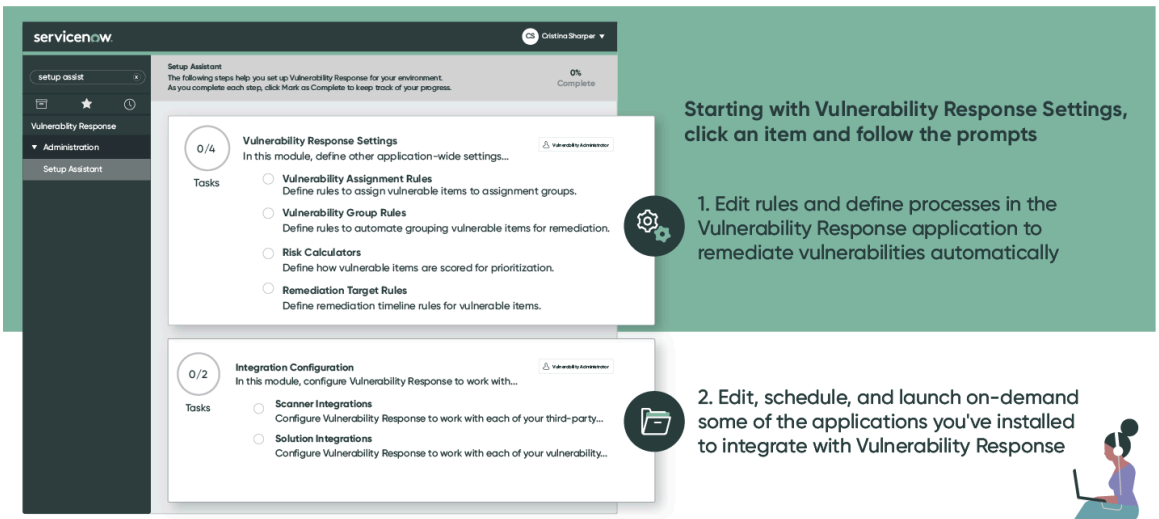
Suivez les étapes et les invites de l'Assistant de configuration, en commençant par la section Paramètres de Vulnerability Response pour poursuivre l'installation et la configuration. L'examen de ces paramètres vous aide à comprendre et à vérifier les processus à Réponse aux vulnérabilités mesure que vous continuez à configurer votre environnement.

Rôle requis : sn_vul.vulnerability_admin ou admin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de l'administrateur de vulnérabilité



Roles required: sn_vul.vulnerability_admin or admin

Passez en revue les descriptions, les paramètres par défaut et les données de démonstration que vous avez installés avec les applications dans les sections suivantes :

- Règles d'affectation de vulnérabilité : affecter automatiquement les éléments vulnérables (VI) au groupe d'affectation approprié.
- Règles de la tâche de rattrapage : regroupez automatiquement les éléments vulnérables (VI) à mesure qu'ils sont importés en fonction de certaines conditions.
- Calculateurs de risque : le calculateur de risque par défaut est activé.
- Règles de cibles de rattrapage : définissez des chronologies de rattrapage pour les éléments vulnérables et les tâches de rattrapage (RT).
- Examinez et modifiez les paramètres des applications tierces et des solutions installées que vous avez installées, et définissez des conditions pour vos importations de données. Saisissez les informations de votre compte de tiers et configurez les paramètres d'importation, les calendriers, les règles de recherche d'éléments de configuration (CI), ainsi que d'autres paramètres.

Consultez Liste de vérification d'implémentation pour l'application Réponse aux vulnérabilités pour plus d'informations.

Pour plus d'informations sur la personnalisation ou l'implémentation de l'application Réponse aux vulnérabilités , consultez KB1000704 .

Installer Réponse aux vulnérabilités

Avant d'exécuter l'application Réponse aux vulnérabilités dans votre ServiceNow AI Platform instance, vous devez obtenir une autorisation et télécharger l'application à partir de , ServiceNow Store l'installer sur votre ServiceNow AI Platform instance, puis effectuer quelques étapes d'installation dans l'Assistant de configuration.

Avant de commencer

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

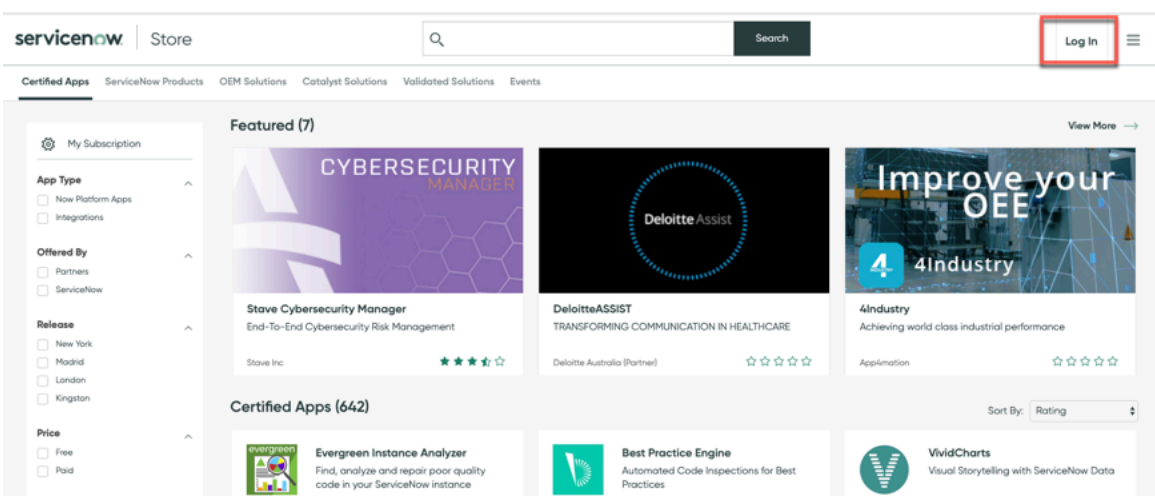
- Vérifiez que les rôles requis ServiceNow sont affectés à votre instance.
- Le rôle administrateur est requis pour l'installation et l'affectation des rôles.

Rôle requis : admin

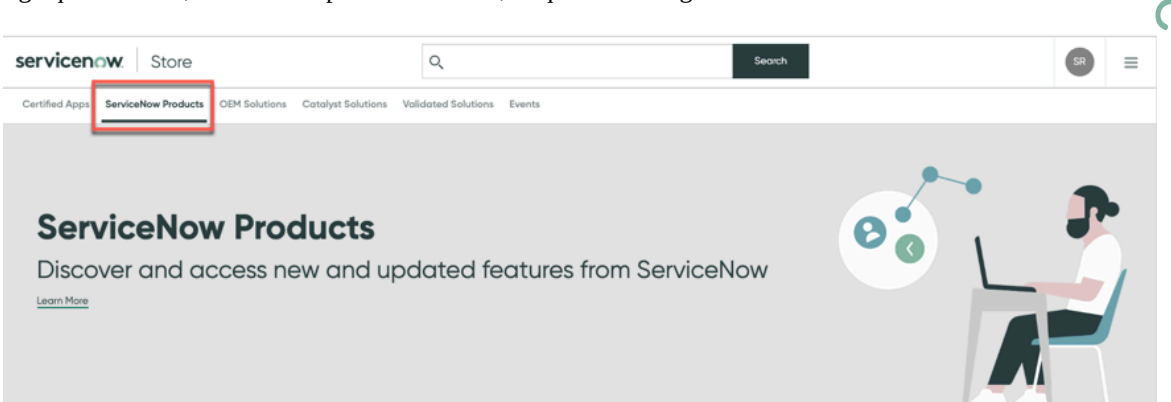
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Pour obtenir une autorisation et télécharger l'application Réponse aux vulnérabilités principale, accédez au ServiceNow Store.
2. En haut à droite de la page, cliquez sur **Se connecter**.



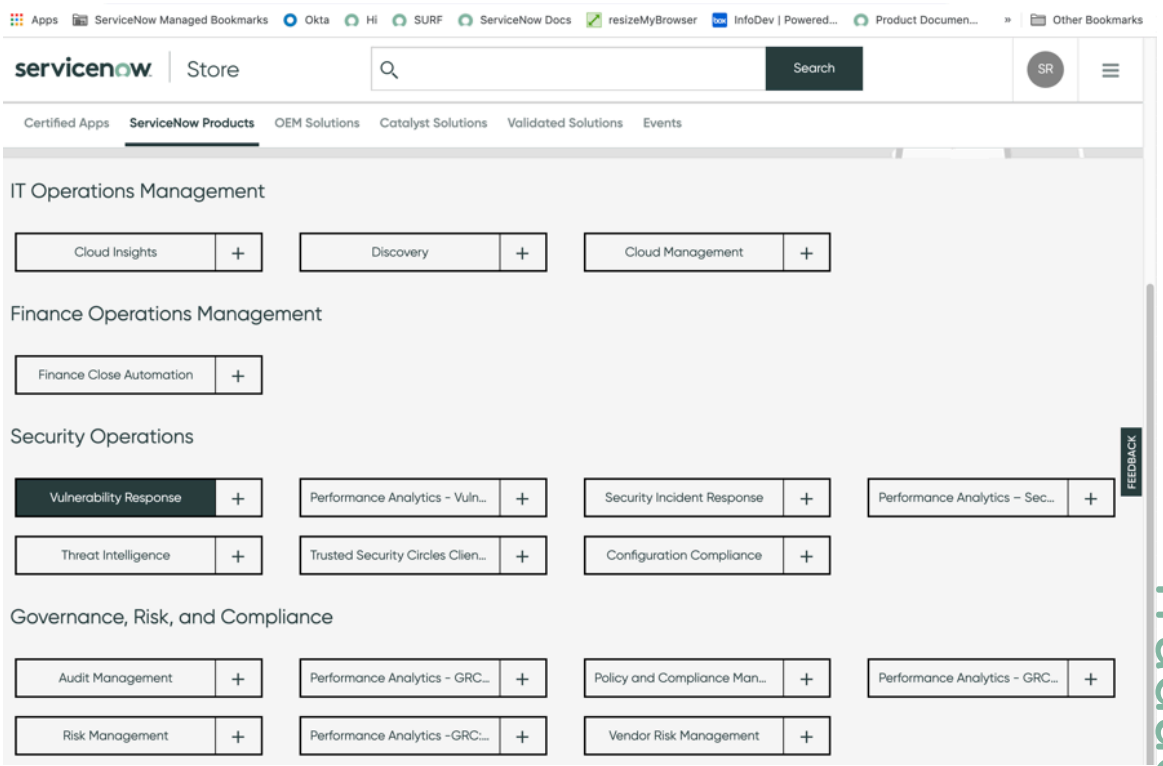
3. Dans la boîte de dialogue qui s'affiche, saisissez vos informations d'identification HI et cliquez sur **Connexion**.
4. Sur la page qui s'affiche, si elle n'est pas sélectionnée, cliquez sur l'onglet **Produits ServiceNow** .



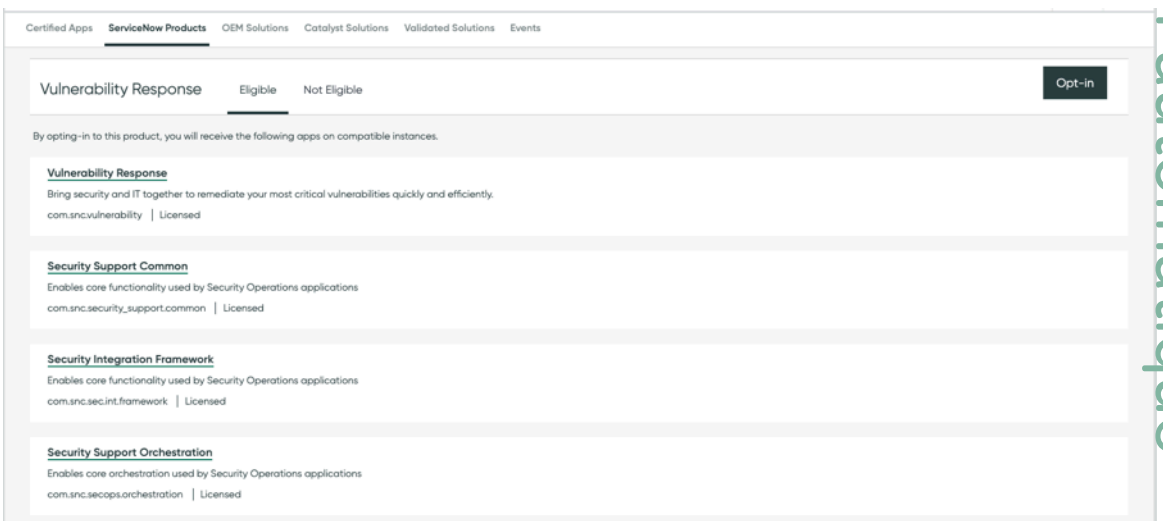
5. Pour afficher les applications associées auxquelles vous êtes éligible avec l'application Réponse aux vulnérabilités , sur la page de liste des produits, cliquez sur le produit **Vulnerability Response** .

Traduction automatique

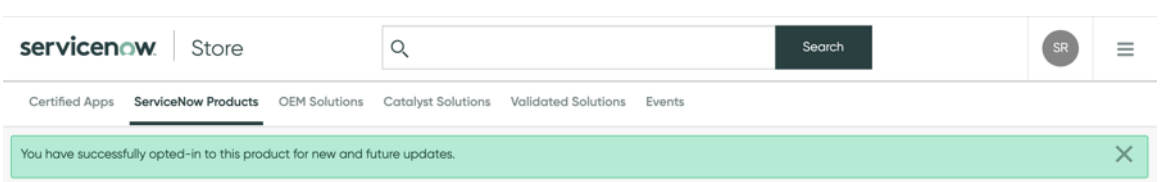
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L’onglet Éligible répertorie toutes les applications auxquelles vous êtes éligible si vous vous abonnez. Pour plus d’informations sur une application, cliquez sur un lien.



6. Pour obtenir l’application Réponse aux vulnérabilités principale, cliquez sur **Adhérer**.
7. Pour accepter les termes et conditions, à l’invite, cochez la case et cliquez sur **Accepter**.
   Un message s’affiche pour indiquer que vous êtes abonné à l’application.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois l'onglet ServiceNow Produits sélectionné et affiché, une coche verte remplace le signe plus à droite de l'application Réponse aux vulnérabilités , comme illustré dans la figure suivante.

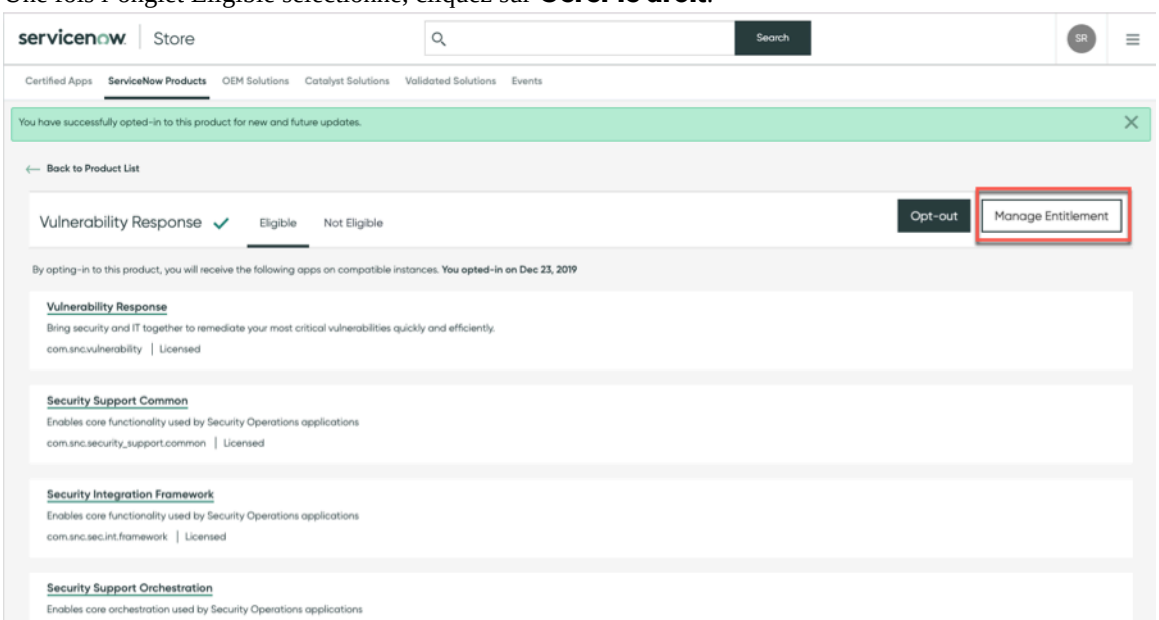


Une fois que vous avez accepté les termes et conditions et géré les autorisations pour l'une des applications de l'onglet **Produits ServiceNow** , sur la page Liste des produits, vous pouvez cliquer sur le signe plus (+) pour obtenir l'autorisation et vous abonner aux autres applications de cette page en un seul clic.

8. Passez à l'étape 10 pour installer l'application sur votre ServiceNow AI Platform instance.
9. **Facultatif :** Pour gérer votre droit pour l'application Réponse aux vulnérabilités sur d'autres ServiceNow AI Platform instances, procédez comme suit.

   a. Si le bouton Gérer le droit n'est pas affiché, cliquez sur l'application Réponse aux vulnérabilités dans la Liste de produits pour l'afficher.

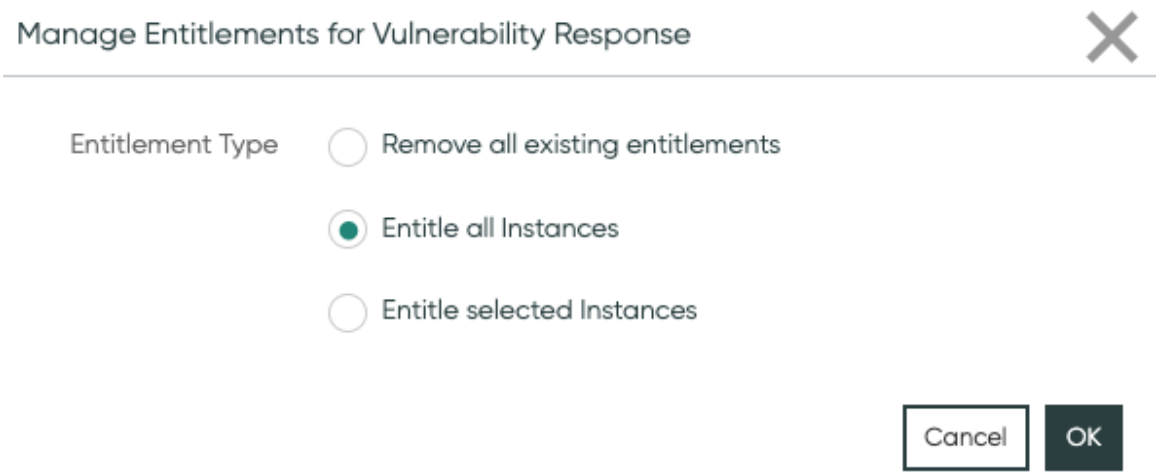
   b. Une fois l'onglet Éligible sélectionné, cliquez sur **Gérer le droit**.



   c. Dans la boîte de dialogue Gérer les autorisations pour Vulnerability Response qui s'affiche, choisissez l'une des options suivantes :

Traduction automatique

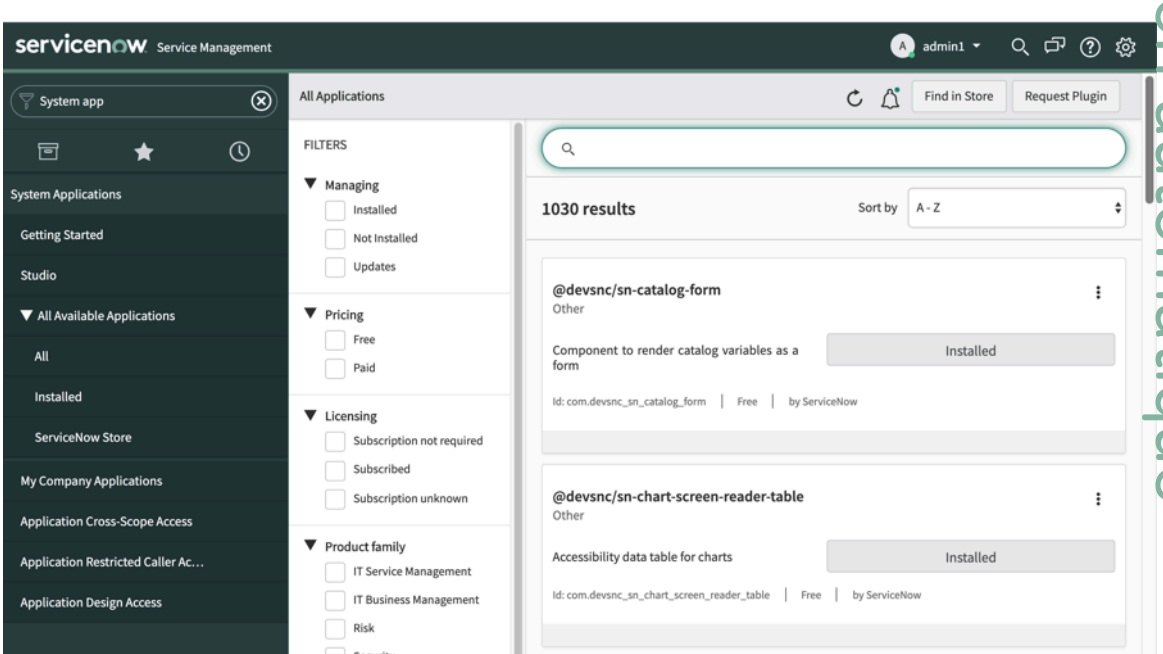
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Cliquez sur **OK** ou **sur Annuler** pour continuer.
Vous êtes prêt à activer les modules d'extension et à installer l'application sur votre ou vos ServiceNow AI Platform instances.

10. Connectez-vous à l'instance ServiceNow AI Platform sur laquelle vous souhaitez installer l'application Réponse aux vulnérabilités .

11. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.



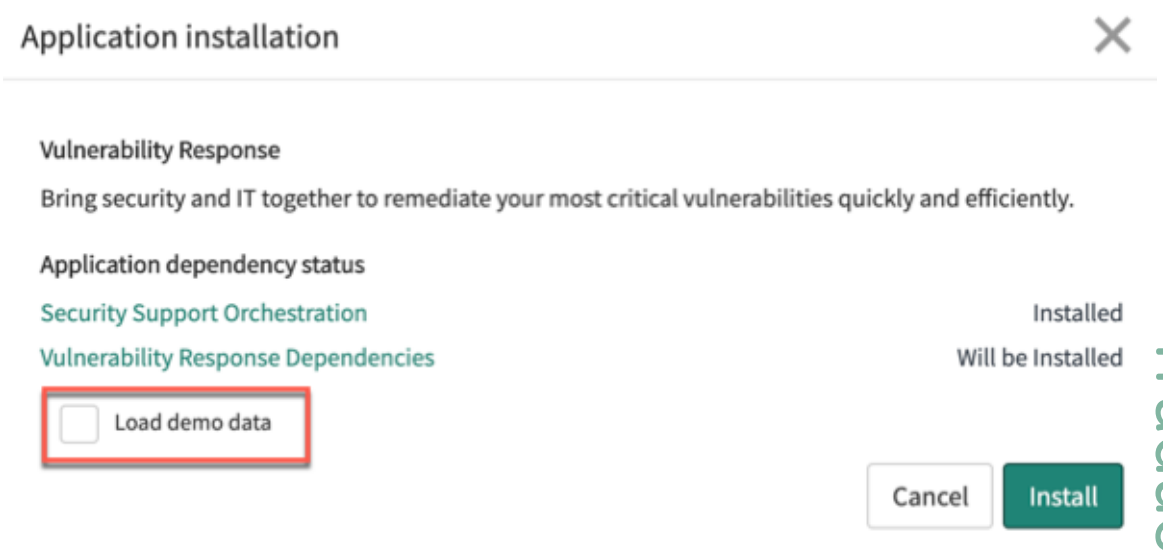
12. Dans les applications répertoriées, localisez l'application Vulnerability Response (sn_vul), sélectionnez une version dans la liste de choix, puis cliquez sur **Installer**.
La boîte de dialogue d'installation de l'application s'affiche. Toutes les dépendances qui seront installées s'affichent.

13. **Facultatif :** Si vous souhaitez des données de démonstration, cochez la case Charger les données de démonstration et cliquez sur **Installer**.

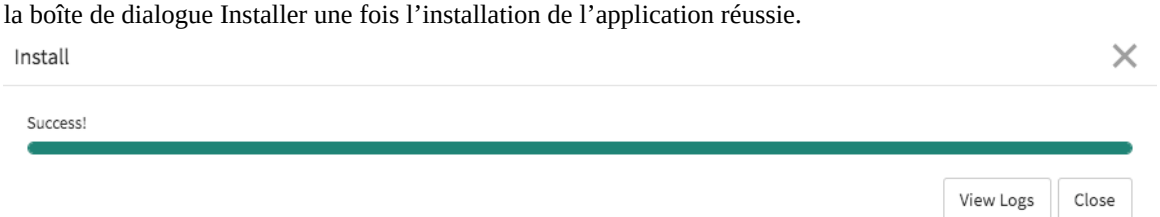
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous ne cochez pas la case **Charger les données de démonstration**, les données de démonstration ne sont pas disponibles pour une installation ultérieure à partir du gestionnaire d'applications. Pour plus d'informations sur l'installation ou la réinstallation des données de démonstration après l'installation initiale, consultez l'article Solution de contournement pour installer les données de démonstration si l'application est déjà installée [KB0722909] dans la base de Now Support connaissances.



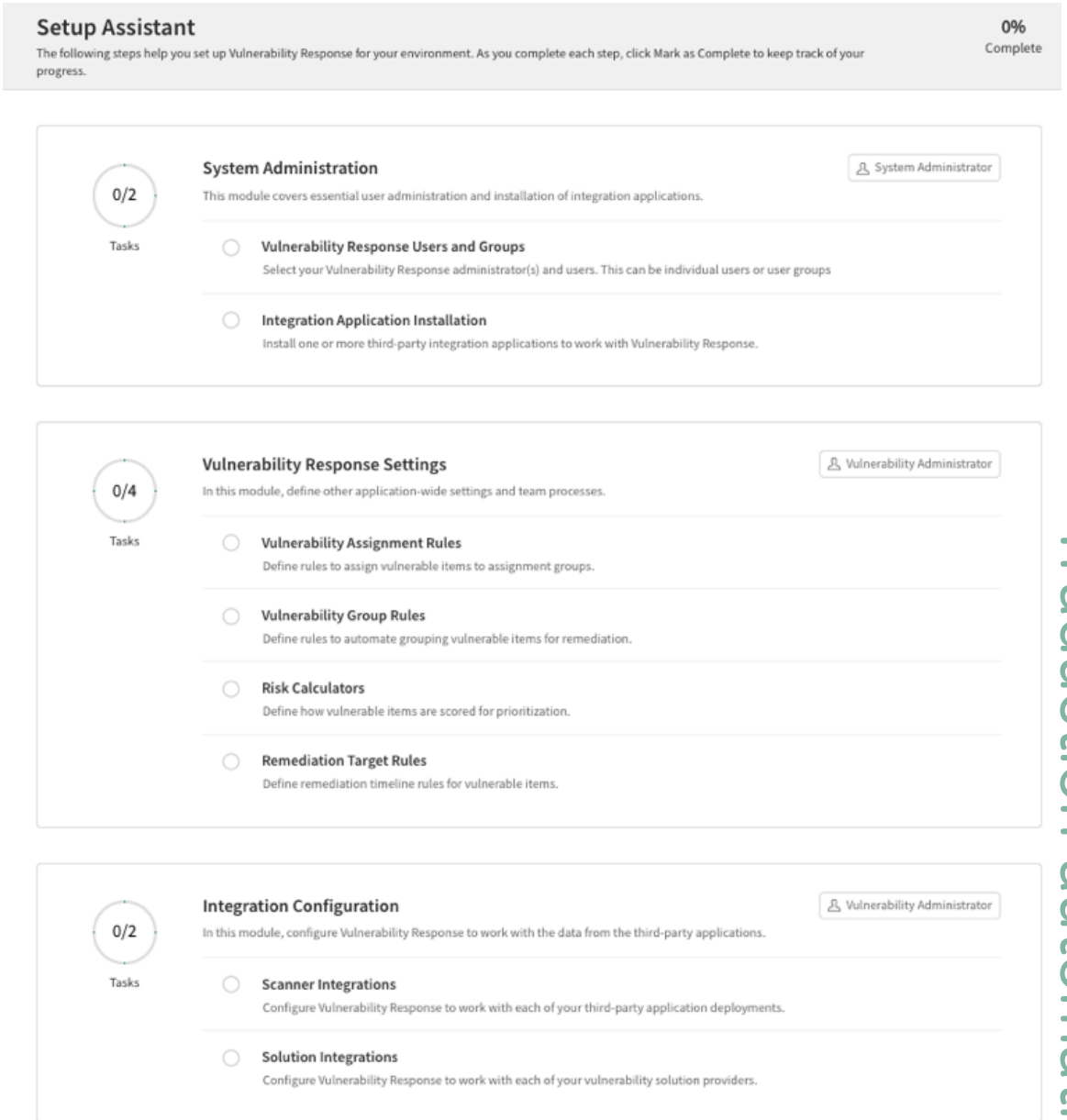
Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'installation de l'application réussie.



14. Cliquez sur **Fermer**.
15. Une fois l'installation terminée, accédez à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



16. Suivez les instructions sur les formulaires dans chaque section.

Que faire ensuite

Pour plus d'informations sur les paramètres, l'installation des applications, la configuration, les intégrations, les règles de groupe, les calculateurs de risque et les règles de cibles de rattrapage, reportez-vous à Réponse aux vulnérabilités la section Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration.

Composants installés avec Réponse aux vulnérabilités

Plusieurs types de composants sont installés lors de l'activation de l'application Réponse aux vulnérabilités, notamment des tables, des rôles d'utilisateur et des tâches planifiées.

Afficher les listes filtrées des composants installés avec une application

À partir de la version 24.0.6 de Réponse aux vulnérabilités, les propriétés système les plus fréquemment utilisées sont désormais accessibles dans l'application Réponse aux vulnérabilités . Pour afficher ces propriétés système, accédez à **Tous**Réponse aux vulnérabilités**Propriétés**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Filtrez la table Fichiers d'applications afin de n'afficher que les rôles, les travaux planifiés et les tables installés avec une application. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés dans l'instance et dans la table de métadonnées. Suivez ces étapes pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application. Par exemple : **Application** > **est** > **Réponse aux vulnérabilités**.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, sélectionnez **ET,** puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rôles installés

Remarque : Les rôles, les travaux planifiés et les tables de Réponse aux vulnérabilités des applications se trouvent dans Composants installés avec Réponse aux vulnérabilités des applications.

Titre du rôle [name]	Description	Contient des rôles
sn_vul_prisma.configure_prisma_integration	Sécurise les opérations CRUD + report_view sur sn_vul_prisma_hosts_import table et report_view opération sur sn_vul_prisma_host_attrb table.	
sn_vul.view_manager_workspace	Vues Espace de travail du gestionnaire de vulnérabilités.	
sn_vul.supprimer	Supprime les enregistrements sources et les éléments vulnérables. Avant la version 23.0, le rôle d'administrateur avait le privilège de supprimer les enregistrements sources.	• sn_vul_cmn.supprimer • sn_vul.delete_vulnerable_items
sn_vul_cmn.supprimer	Supprime les enregistrements sources.	
sn_vulc.modifier_du_bloc	Effectue une opération de modification en bloc sur les résultats des tests.	
sn_vul.app_modification_du_bloc	Effectue une opération de modification en bloc sur les éléments vulnérables de l'application (AVIT).	sn_vul.app_écrire_tout
sn_vul_container.container_bulk_edit	Effectue une opération de modification en bloc sur les	sn_vul_container.écrire_tout

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	éléments vulnérables de conteneur (CVIT).	
sn_vul_cisa.configure_intelligence_integration	Configure les intégrations d'intelligence.	
Responsables des vulnérabilités et analystes principaux [sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)]	Mettez à jour les propriétés et les intégrations de vulnérabilité. Le rôle sn_vul.vulnerability_admin ou sn_vul.admin (obsolète) est requis pour Réponse aux vulnérabilités l'administration, y compris les intégrations de vulnérabilités, les règles de tâche de rattrapage, les calculateurs, les règles et les tâches de cibles de rattrapage, les rapports et la configuration d'intégration tierce.	• sn_vul.vulnerability_write • sn_vul.ciso_write • sn_sec_cmn.admin • sn_vul_qualys.admin (lorsque Qual Vulnerability Integration est install • sn_vul_r7.admin (lorsque Rapid7 Vulnerability Integration est install • sn_vul_shodan.admin (lorsque Sho Exploit Integration est installée.) • sn_vul.configure_nvd_integration (lorsque les intégrations NVD sont installées.) • treemap_admin (lorsque l'applicati Performance Analytics est installé
Orchestration de correctifs	Configure les intégrations de fournisseurs de correctifs tiers prises en charge. Afficher et appliquer les données et les enregistrements de correctifs.	• sn_vul_patch_orch.configure_patc Configurer et appliquer des correc • sn_vul_patch_orch.read_patch Peut afficher les enregistrements données de correctifs. • sn_vul_bigfix.configure_integration Configure l'application BigFix Patc Orchestration Integration. Ce rôle contient les rôles granulaires sn_vul_bigfix.read_integration et connection_admin qui permettent l'utilisateur de se connecter à la c BigFix. • sn_vul_sccm.configure_integration Ce rôle contient les rôles granulair sn_vul_sccm.read_integration et connection_admin qui permettent l'utilisateur de se connecter à la c SCCM. • sn_vul_bigfix.read_integration Les utilisateurs disposant de ce rô peuvent afficher (en lecture seule) les enregistrements de Vulnerabili

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
		Response et de l'application BigFi Patch Orchestration Integration, a que les données d'orchestration d correctifs. • sn_vul_sccm.read_integration Les utilisateurs disposant de ce rô peuvent afficher (en lecture seule) les enregistrements de Vulnerabili Response et de l'application Micro SCCM Patch Orchestration Integr ainsi que les données d'orchestrat de correctifs.
Analystes de vulnérabilité [sn_vul.vulnérabilité_écriture]	Le rôle sn_vul.vulnerability_write est requis pour gérer les tâches de rattrapage et les éléments vulnérables, ainsi que pour surveiller la progression du rattrapage.	• sn_vul.lire_tout • sn_sc_cmn.écriture • sn_vul_qualys.user (lorsque Qualys Vulnerability Integration est install • sn_vul_shodan.write (lorsque Shod Exploit Integration est installée.)
V19.0 : Gestionnaire des événements de vulnérabilité [sn_vul_analyst.vul_event_manager]	Le rôle sn_vul_analyst.vul_event_manager est utilisé pour évaluer l'impact d'une nouvelle vulnérabilité ou d'un nouveau logiciel, ou pour ajouter une vulnérabilité zero-day pour identifier les actifs impactés et créer des éléments vulnérables (VI).	• sn_sec_cmn.lire • canvas_user • sn_vul_analyst.emergency_respons • sn_vul.Gérer_l'évaluation_de_l'exp
Autres [sn_vul.lire_tout] Le rôle sn_vul.vulnerability_read est déconseillé.	Le rôle sn_vul.read_all est requis pour toute personne ayant besoin d'une visibilité sur la gestion des vulnérabilités. Par exemple, les responsables informatiques et de sécurité ou toute personne qui souhaite explorer les éléments qui composent les visuels du tableau de bord à partir des tableaux de bord de haut niveau. **Important :** À partir de la version 24.0.6 de Réponse aux vulnérabilités, le rôle sn_vul.read_all a le privilège d'accéder Espace de travail du gestionnaire de vulnérabilités au .	• sn_sec_cmn.lire • sn_vul_qualys.read (lorsque Qualys Vulnerability Integration est install • sn_vul_shodan.read (lorsque Shod Exploit Integration est installée.) • pa_viewer (lorsque l'application An des performances est installée). • sn_vul_tenable.read_integration (lo l'intégration de vulnérabilité Tenab installée.) • sn_vul.view_manager_workspace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
sn_vul.read_assigned	Affichez les éléments vulnérables qui vous sont affectés ou qui sont affectés à vos groupes d'affectation dans l'interface utilisateur classique et Espace de travail de remédiation IT. **Important :** À partir de la version 24.0.6 de Réponse aux vulnérabilités, le rôle sn_vul.read_assigned a le privilège d'accéder Espace de travail de remédiation IT au .	sn_vul.view_rem_workspace
Administrateur d'importation système VR [sn_vul.vr_import_admin]	Exécution du système en tant qu'utilisateur. Exécute les travaux planifiés. **Remarque :** Cet utilisateur est l'utilisateur d'exécution par défaut pour chaque enregistrement d'intégration. Ne changez pas.	• import_admin • sn_vul.vulnerability_write
Propriétaire du rattrapage [sn_vul.remediation_owner]	Affichez et mettez à jour l'autorisation pour les éléments vulnérables et les tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe. Peut afficher toutes les vulnérabilités et solutions. Dispose d'un accès en écriture au**champ Notes internes** de l'enregistrement de solution.	Contenu dans le rôle itil.
RSSI et responsables des vulnérabilités [sn_vul.vulnérabilité_ciso]	Affichez le tableau de bord CISO dans Analyse des performances pour Vulnerability Response.	• sn_vul.ciso_read • sn_vul.lire_tout
Approbateur de faux positif [sn_vul.approbateur_faux_positif]	Approuve/rejette les demandes de faux positif.	sn_vul.view_manager_workspace
Approbateur d'exception [sn_vul.exception_approver]	Approuve/rejette les demandes d'exception.	sn_vul.view_manager_workspace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Travaux planifiés installés

Tâche planifiée	Description
Renseigner les filtres enregistrés prêts à l'emploi pour l'hôte et le module d'application	Migre les modules associés au module d'hôte et d'application.
Renseigner les filtres enregistrés prêts à l'emploi pour le module CC	Migre les modules associés au module CC.
Renseigner les filtres enregistrés prêts à l'emploi pour le module Conteneur	Migre les modules associés au module de conteneur.
Actualiser les filtres enregistrés associés à l'hôte	Actualise toutes les données d'agrégation associées aux filtres enregistrés du module hôte.
Actualiser les filtres enregistrés associés à CC	Actualise toutes les données d'agrégation associées aux filtres enregistrés du module CC.
Actualiser le conteneur Filtres enregistrés connexes	Actualise toutes les données d'agrégation associées aux filtres enregistrés du module Conteneur.
Actualiser les filtres enregistrés associés à l'application	Actualise toutes les données d'agrégation associées aux filtres enregistrés du module d'application.
Déclencher la création et l'exécution de l'agrégation pour le filtre enregistré	Crée, met à jour, exécute et actualise les agrégations associées au filtre enregistré.
Version 19.0 de Vulnerability Response et v4.0 de Veracode Vulnerability Integration	L'intégration CWE de Veracode récupère des données spécifiques de Common Weakness Enumeration (CWE) pour obtenir des informations sur les menaces et des Veracode recommandations de correction. L'intégration des SBOM Veracode ingère les informations de version, de version et de vulnérabilité provenant Veracode des composants de vos projets logiciels. L'intégration génère des SBOM au format JSON CycloneDx et les télécharge dans votre instance L'intégration des catégories Veracode récupère les données de catégories améliorées à partir de Veracode. L'intégration Veracode DevOps permet aux utilisateurs DevOps d'afficher les détails récapitulatifs des analyses de vulnérabilité tierces sans licence SecOps. API basées sur JSON pour les intégrations Veracode suivantes : élément vulnérable de l'application, résumé de l'analyse, liste

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
	des applications. Les versions d'API basées sur XML de ces intégrations sont déconseillées.
Associer les VI existants à la règle d'exception automatique	Associe automatiquement la règle d'exception automatique aux VI existants.
Fermer automatiquement les détections vulnérables	Ferme automatiquement les détections vulnérables périmées en fonction de la configuration définie dans la table « sn_vul_auto_close_config ».
Version 16.1 : HCL : BigFix Collection, Fixlet et intégrations d'actions.	Gérez les correctifs et les déploiements de correctifs pour les vulnérabilités avec des correctifs du produit HCL BigFix.
Calculer les nombres connexes pour toutes les solutions	Inactif par défaut. Traite les données des solutions une fois tous les soirs au lieu de manière continue. À partir de la version 22.0, vous pouvez exécuter cette tâche uniquement sur demande. Comme cette tâche planifiée traite toutes les solutions, elle peut avoir un impact sur les performances. Par conséquent, il est recommandé d'exécuter cette tâche une seule fois si les données de la solution sont corrompues.
Calculer le nombre de VI associés pour la tâche de vulnérabilité et de rattrapage	Capture les changements d'importation manuelle et VI pour la journée. Rapproche les relations de vulnérabilité et de solution et recalcule les totaux. Les données de solutions sont mises en file d'attente et traitées séparément par la tâche planifiée File **d'attente des mesures de la solution de vulnérabilité du processus** .
Vérifier le délai d'expiration du serveur MID	Envoie un ping au serveur MID et des erreurs apparaissent au bout de 30 secondes.
V19.0 : vérifier l'exposition potentielle à la vulnérabilité	Traite les CVE delta, les logiciels et les installations pour obtenir l'exposition.
Vérifier l'état d'exécution WaitComplete	Marque une exécution d'intégration comme terminée une fois qu'elle a été vérifiée comme terminée.
Vérifier l'expiration du report des éléments vulnérables et des groupes	Envoie des notifications si les éléments vulnérables ou les vulnérabilités ont expiré (et s'ils expirent dans une semaine). Vérifie si une règle d'exception est applicable sur un VI différé et met à jour les champs **Motif etJusqu'à** en fonction de la règle

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
	d'exception. L'état du VI reste Différé jusqu'à la dernière date d'expiration.
Fermer annuler les VIT qui n'ont pas de CI associé	Ferme automatiquement les éléments vulnérables qui n'ont pas d'élément de configuration (CI) associé et qui n'ont pas été mis à jour depuis trois jours. L'état est défini sur Fermé/Annulé.
Fermer le VI à la suppression de l'enregistrement d'expérience	Ferme un VI lorsqu'il est supprimé.
Intégration des résultats de la conformité	Importe les résultats des tests, ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources faisant autorité pour traitement dans l'application Configuration Compliance.
Intégration du remplissage des résultats de la conformité	Dans le cadre d'une intégration chaînée exécutée avec l'intégration des actifs, importe les données d'évaluation de configuration pour les actifs ignorés qui sont découverts (importés via l'intégration Tenable.io des actifs).
Synchronisation de l'état CR	Le script adapte automatiquement toutes les tâches de rattrapage existantes aux relations CHG afin qu'elles soient synchronisées. Active la synchronisation à l'avenir.
Version 15.0 Intégration des informations d'identification de numérisation	Importe et stocke temporairement Tenable.io en toute sécurité les informations d'identification utilisées pour accéder au scanner pour des nouvelles analyses à la demande.
Intégration complète CWE 2000	Intégration de vulnérabilité qui extrait les informations sur les vulnérabilités de l'ensemble de données CWE (Common Weakness Enumeration), géré par MITRE Corporation.
V18.0 : Supprimer les enregistrements d'actions de division périmés	Tâche quotidienne pour nettoyer les enregistrements périmés dans les tables intermédiaires de tâches fractionnées.
Désactiver les solutions VR lorsque l'application de solutions n'est pas active	Désactive et masque la Gestion des solutions pour vulnérabilités fonctionnalité lorsque l'application Gestion des solutions pour Réponse aux vulnérabilités n'est pas installée.
Évaluer les cibles de rattrapage	Définit ou met à jour les dates cibles de rattrapage sur tous les éléments vulnérables. Détermine l'état des dates cibles de rattrapage par rapport aux règles.
• Correction des détections pour la clé mise à jour pour Rapid7 • Correction des détections de la clé mise à jour pour Qualys	Nettoie automatiquement les données de détection par une tâche planifiée spécifique à l'intégration qui est déclenchée après la mise à niveau vers Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
• Résolution des détections pour la clé mise à jour pour Tenable	
Version 16.1 : Générer une synthèse de rattrapage	Cette tâche génère automatiquement une synthèse d'e-mail pour tous les utilisateurs du groupe d'utilisateurs Propriétaire de rattrapage. La tâche est activée par défaut.
V19.0 : Insertion de CVE exploité par CISA dans la configuration d'exposition	Insère les CVE CISA dans la table Configuration de l'exposition pour calculer l'exposition.
V18.0 : Insérer des tâches de remédiation classiques dans la tâche de remédiation unifiée	Tâche planifiée ponctuelle pour insérer toutes les tâches de rattrapage créées dans l'interface utilisateur classique dans la tâche de rattrapage unifiée (sn_vul_remediation_task).
Intégration de solution Microsoft Security Response Center	Gestion des solutions pour vulnérabilités qui récupère les solutions à partir du Microsoft Security Response Center.
Version 16.1 : collections Microsoft SCCM, mises à jour de correctifs et intégrations de déploiements	Gérez les correctifs et les déploiements de correctifs pour détecter les vulnérabilités à l'aide Microsoft de correctifs SCCM.
Processus d'intégration limitée de reprise	Crée le processus d'intégration pour le Intégration d'exploit Shodan.
Renseigner le texte des produits affectés	Après la mise à niveau, gère les solutions existantes pour renseigner le texte des produits affectés. Cette tâche ne s'exécute qu'une seule fois.
Remplir la nouvelle colonne Nombre de CR	Remplit automatiquement la nouvelle colonne Nombre de CR pour les clients avec des données existantes dans la table de tâches de rattrapage [sn_vul_vulnerability].
File d'attente des mesures de la solution de vulnérabilité du processus	Traite les données des solutions en file d'attente par : • Solutions de déploiement des entrées NVD vers les entrées tierces • Remplissage des solutions privilégiées sur les vulnérabilités, et • Mise à jour des mesures d'état du rattrapage sur les solutions En outre, il traite également les solutions marquées pour les états de mise à jour. **Remarque :** Si vous utilisez uniquement Rapid7, vous pouvez désactiver cette tâche planifiée pour améliorer les performances.
Remplir les enregistrements dans la table de mappage du fournisseur de vulnérabilités	Insère les enregistrements dans la table de mappage des fournisseurs de vulnérabilités pour les vulnérabilités existantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Remplir les enregistrements dans la table de mappage des fournisseurs de vulnérabilités pour les vulnérabilités Rapid7	
Rouvrir les groupes de vulnérabilité différés	Rouvre les tâches de rattrapage différées lorsque la date de report est passée.
Réappliquer toutes les règles d'affectation de vulnérabilité	Réévalue les règles d'affectation par rapport à tous les VI **ouverts** .
Version 16.5 : Nombre de réaffectations pour les règles d'affectation	S'exécute quotidiennement et publie le nombre total de VI et de tâches de rattrapage qui ne sont pas affectés par cette fonctionnalité pour une règle d'affectation particulière.
Intégration de solution Red Hat	Gestion des solutions pour vulnérabilités qui récupère les solutions à partir du Avis de sécurité Red Hat.
V17.1 : Actualiser et résoudre les VIT en double sur la tâche de rattrapage	Trouve des éléments vulnérables en double pour les éléments de la tâche de rattrapage avec l'option « Actualiser automatiquement les VI en double » active.
Actualiser les éléments vulnérables associés pour la tâche de rattrapage non basée sur des règles	Met à jour la tâche de rattrapage avec des éléments vulnérables correspondant aux critères Groupe de filtres et Groupes de conditions.
Réparer les éléments vulnérables erronés Dernières ouvertures et fermetures	Répare les données d'interface utilisateur existantes corrompues par des défauts précédemment corrigés.
Réexécuter les calculateurs	Réapplique les calculateurs à tous les éléments vulnérables affectés par le changement. Cela déclenche un recalcul des scores de risque cumulés de leurs tâchesde rattrapage. **Remarque :** La réexécution des calculateurs peut prendre beaucoup de temps en fonction de votre environnement.
Nouvelle tentative annulée Ensembles de données à importer d'intégration	Nouveaux essais Ensembles de données à importer d'intégration annulés. Nouveaux essais 5 fois avant de renvoyer une erreur.
Réessayer les processus d'intégration	Retente les processus d'intégration. Nouveaux essais 5 fois avant de renvoyer une erreur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Déployer les valeurs d'éléments vulnérables sur la vulnérabilité et le groupe	Calcule le score de risque, le nombre d'éléments vulnérables et l'état de la cible de rattrapage pour les tâches de rattrapage, à l'aide du calculateur de déploiement. **Remarque :** À partir de la version 23.0 de Réponse aux vulnérabilités, la tâche planifiée est améliorée pour créer des tâches en arrière-plan avec des options de multithreading. Cette mise à niveau implique de segmenter la tâche en plusieurs tâches enfants plus petites, qui sont exécutées en parallèle ou simultanément. Cette modification permet de traiter plusieurs enregistrements simultanément, ce qui accélère considérablement la tâche globale.
Exécuter le calculateur de gravité après la promotion de l'entrée de vulnérabilité	Exécute le calculateur de gravité après la mise à jour d'une vulnérabilité précédemment manquante avec son score et d'autres données provenant d'un fournisseur tiers, tel que Qualys Cloud Platform. Rapid7 Nexpose **Remarque :** À partir de la version 25.0.3 de Réponse aux vulnérabilités, la tâche planifiée est améliorée pour créer des tâches en arrière-plan avec des options de multithreading. Cette mise à niveau implique de segmenter la tâche en plusieurs tâches enfants plus petites, qui sont exécutées en parallèle ou simultanément. Cette modification permet de traiter plusieurs enregistrements simultanément, ce qui accélère considérablement la tâche globale.
V19.0 : exécuter l'évaluation de l'exposition pour les CVE configurées	Calcule l'exposition pour tous les enregistrements CVE dans la table Configuration de l'exposition.
V19.0 : exécuter l'exposition logicielle	Calcule l'exposition de tous les enregistrements logiciels dans la table Configuration de l'exposition.
Processeur de source de données de vulnérabilité planifiée	Vérifie la file d'attente d'importation pour les entrées à traiter et attribue une tâche d'importation planifiée en fonction des ressources disponibles.
Nettoyage des pièces jointes du processus d'intégration de vulnérabilité planifiée	Supprime les pièces jointes XML d'intégration une fois qu'elles ont 14 jours. Cette durée de conservation n'est pas configurable.
Vérificateur du délai d'expiration de l'intégration de vulnérabilité planifiée	Annule les exécutions d'intégration qui prennent plus de 60 minutes.
Définir les services CI associés pour VI	Une fois l'importation de l'intégration terminée, elle relie les services aux entreprises affectés aux CI connectés aux éléments vulnérables, à l'heure spécifiée. Pour plus d'informations, consultez Mappage des services dans Réponse aux vulnérabilités.
Définir les nombres de reports	Collecte le nombre de fois où un élément vulnérable, un élément vulnérable d'application, un élément vulnérable de conteneur ou une tâche de rattrapage est reporté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Déclencher l'intégration suivante	Déclenche l'intégration suivante dans une exécution d'intégration chaînée.
Intégration de modèles	Un seul enregistrement de modèle est envoyé lors de la Tenable.io nouvelle analyse.
Mettre à jour les éléments vulnérables non groupés	Détermine si un élément vulnérable se trouve dans une tâche derattrapage et l'ajoute ou le supprime de la liste **des éléments vulnérables dégroupés**. **Remarque :** Cette tâche s'exécute après la mise à niveau et, selon votre ensemble de données, peut prendre beaucoup de temps.
Mettre à jour la vulnérabilité sur VG	Met à jour le champ **Vulnérabilité** de la table Tâche de rattrapage (sn_vul_vulnerabilty) après la mise à niveau. Cette tâche est déclenchée une fois et inactive par la suite.
Modèle d'importation de vulnérabilité	Moteur qui traite la file d'attente d'importation. L'un des 10.
Âge de la réponse aux vulnérabilités Mise à jour fermée	Met à jour la colonne Âge fermé sur la table des VI.
Nombre de CI de réponse aux vulnérabilités	Calcule le nombre de CI analysés par des analyseurs tiers au cours des 30 derniers jours.
Mise à niveau du risque et de l'état du rattrapage de Vulnerability Response	Met à jour la cote de risque sur les données lors de la mise à niveau.
v20.0 : vérifier l'expiration de l'atténuation du risque	Vérifie si les contrôles compensatoires ont expiré pour un élément vulnérable et une tâche de rattrapage. S'ils ont expiré, le score de risque revient au score de risque d'origine et envoie une notification par e-mail indiquant que les contrôles de compensation ont expiré. Envoie également une notification par e-mail si les contrôles compensatoires doivent expirer dans les 7 jours.

Tables installées

Table	Description
v24.0.6 Importation des hôtes Prisma [sn_vul_prisma_hosts_import]	Table des ensembles de données à importer pour les hôtes.
v24.0.6 Attributs de l'hôte Prisma [sn_vul_prisma_host_attrb]	Table d'attributs d'actif pour l'intégration d'hôtes.
v22.0	Ferme automatiquement les détections obsolètes en fonction des conditions de filtre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
sn_vul_cmn_auto_close_rule	
sn_vul_cmn_ws_saved_filter	Stocke les données du filtre enregistré.
sn_vul_licensing_usage	Contient l'actif dupliqué, l'actif IP incomplet, le nombre total d'actifs de scanner et l'utilisation finale.
sn_vul_m2m_entry_compensating_control	Représente l'association entre les entrées de vulnérabilité et les contrôles de compensation.
v21.0 Moteur d'analyse Rapid7 [sn_vul_r7_scan_engine)	Stocke les enregistrements importés Données du moteur d'analyse chargé de découvrir les actifs au cours d'une analyse et de vérifier leur vulnérabilité.
v21.0 Importation du moteur d'analyse Rapid7 [sn_vul_r7_scan_engine_import]	Utilisé par l'intégration du moteur d'analyse Rapid7 pour organiser l'importation des données avant leur traitement.
Version 19.0 : [sn_vul_veracode_cwe_import]	Étend la table des catégories Veracode pour les recommandations de rattrapage CWE.
Version 19.0 : [sn_vul_veracode_category_import]	Stocke les données des catégories importées.
Version 19.0 : [sn_vul_veracode_sbom_import]	Stocke les données SBOM importées provenant de Veracode.
V17.1 : Ajouter une preuve à la clé de VI [sn_vul_proof_key_vulnerability]	Vulnérabilités Rapid7 dont la preuve doit être incluse dans la clé de VI. À partir de la version 24.0.6 de Réponse aux vulnérabilités, une colonne « Expression régulière pour diviser les VIT Tenable » est ajoutée. Il stocke l'expression régulière saisie par un utilisateur qui est utilisée pour analyser la preuve à partir de la charge utile.
Éléments vulnérables évalués [sn_vul_m2m_exp_sw_vi]	Affecte une tâche de rattrapage à un groupe d'affectation lors de la création de la tâche de rattrapage.
Règle d'affectation [sn_vul_vgr_assignment_rule]	Affecte une tâche de rattrapage à un groupe d'affectation lors de la création de la tâche de rattrapage. Avant la version 15.0 : affecte une tâche de rattrapage à un groupe d'affectation lors de la création de la tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Demande de changement associée [sn_vul_action_associate_cr]	Table intermédiaire utilisée pour traiter les nouvelles associations tâche-CHG de rattrapage. Avant la version 15.0 : Table intermédiaire utilisée pour traiter les nouvelles associations VG-CHG.
Tâche d'élément vulnérable asynchrone [sn_vul_async_vi_job]	Contient des tâches en arrière-plan qui traitent les éléments vulnérables. Un seul type de tâche est pris en charge ; Utilisé pour modifier les vulnérabilités en bloc.
Type de tâche d'élément vulnérable asynchrone [sn_vul_async_vi_job_type]	Contient les types de tâches en arrière-plan et fait référence au script pertinent. Il n'a qu'un seul processeur, le **VulnerabilityBulkEditProcessor**
Fermer automatiquement les détections obsolètes [sn_vul_auto_close_config]	Stocke la configuration de fermeture automatique des détections périmées.
Configurer la granularité des éléments vulnérables [sn_vul_action_vi_granularity_config]	Stocke le formulaire d'interface utilisateur utilisé pour activer ou désactiver Inclure le port à partir de la page de configuration dans le module Configurer la granularité VI.
Création d'une demande de changement [sn_vul_action_create_cr]	Utilisé pour créer des demandes de changement à partir d'une tâche de rattrapage.
Créer des éléments vulnérables [sn_vul_action_create_vi]	Table intermédiaire utilisée comme espace réservé pour les informations. Cette table ne stocke aucun enregistrement.
Collection [sn_vul_patch_orch_collection]	Stocke les données de collecte d'instances distinctes.
CWE [sn_vul_cwe]	Catalogue des vulnérabilités logicielles courantes de Weakness and Enumeration (CWE).
Plateforme CWE applicable [sn_vul_cwe_m2m_cwe_platform]	Contient les données de plateforme applicables CWE importées.
Catégorie CWE [sn_vul_cwe_category]	Contient les données de catégorie CWE importées.
Conséquence courante CWE	Contient les données des conséquences courantes CWE importées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vul_cwe_consquence]	
Référence externe CWE [sn_vul_cwe_reference]	Contient les données de référence externe CWE importées.
Exemple observé de CWE [sn_vul_m2m_cwe_cve]	Contient les données CVE CWE importées.
Plateforme CWE [sn_vul_cwe_platform]	Contient les données de plateforme CWE importées.
Référence externe CWE [sn_vul_cwe_reference]	Contient les données de référence externes liées à CWE importées.
Relation CWE [sn_vul_m2m_cwe_relation]	Contient les données de relation CWE importées.
Vue CWE [sn_vul_cwe_view]	Contient les données de vue CWE importées.
Faiblesse CWE [sn_vul_cwe_weakness]	Contient les données de faiblesse CWE importées.
Version 16.1 : collection d'appareils [sn_vul_patch_orch_m2m_src_ci_collection]	Stocke les données des collections sur les éléments découverts.
Version 16.1 : Mise à jour de l'appareil [sn_vul_patch_orch_m2m_src_ci_update]	Stocke les données relatives aux correctifs déployés, ainsi que l'état de déploiement, qui sont affichés sur les enregistrements d'éléments détectés.
Correspondance de logiciel vulnérable de modèle de Découverte [sn_vul_discovery_model_software_match]	Complète la mise en correspondance des logiciels vulnérables avec un modèle de détection.
Configuration de gestion de l'exception [sn_vul_exception_config]	Stocke les paramètres de configuration de la fonctionnalité de gestion des exceptions.
Règle d'exception	Contient l'ensemble des règles évaluées pour la gestion des exceptions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vul_auto_exception_rule]	
Exploit [sn_vul_exploit]	Contient les définitions des exploits : code accessible au public qui tire parti d'une vulnérabilité.
Cadre de travail de l'exploit sn_vul_exploit_framework	Contient les noms de frameworks d'exploits : des packages logiciels complets capables d'exécuter de nombreux exploits.
Modèles de découverte exposés [sn_vul_m2m_exp_sw_model]	Stocke le mappage entre le modèle de découverte et l'évaluation de l'exposition à la vulnérabilité .
Évaluation de l'exposition [sn_vul_exp_by_sw]	Stocke les enregistrements pour l'évaluation de l'exposition.
V19.0 : manifeste d'exposition sn_vul_analyst_exposure_manifest	Table de manifeste pour le traitement delta.
Entrées de vulnérabilité d'exposition [sn_vul_m2m_entry_exp]	Stocke le mappage entre Vulnérabilité (sn_vul_entry) et Évaluation de l'exposition.
Kit malware [sn_vul_malware_kit]	Contient les détails des kits de logiciels malveillants : des outils pré-écrits qui facilitent l'exécution d'un exploit ou d'un ensemble d'exploits connexes sans effectuer de travail de codage ou de configuration supplémentaire
Table d'actifs manquante [sn_vul_tenable_missing_asset]	Contient des ID d'actifs temporaires pour les données d'évaluation de la conformité de la configuration ignorées avec des actifs sans correspondance.
Mise à jour de la solution du Microsoft Security Response Center [sn_vul_msrc_update]	Contient la dernière fois que les données de la solution ont été mises à jour par Microsoft. Utilisé pour comparer l'importation nocturne afin de déterminer les données delta à télécharger.
Microsoft Security Response Center Importation de solution [sn_vul_msrc_solution_import]	Utilisé par l'intégration de la solution Microsoft Security Response Center pour organiser l'importation des données avant leur traitement.
Microsoft Security Response Center Solution Integration [sn_vul_msrc_integration]	Étend la table d'intégration de vulnérabilité [sn_vul_integration] pour le Microsoft Security Response Center Solution Integration.
Entrée de base de données de vulnérabilité nationa [sn_vul_nvd_entry]	Vulnérabilité documentée à partir de la base de données de vulnérabilité nationale du NIST.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Importation NVD CVSS [sn_vul_nvd_cvss_import]	Contient des données intermédiaires qui n'ont pas encore été transformées en schéma lors de l'importation Réponse aux vulnérabilités NVD.
Version 16.1 [sn_vul_patch_orch.patch_approval_required]	Lorsque les déploiements de correctifs sont planifiés à partir d'une intégration de correctifs, les demandes sont soumises pour révision et approbation aux utilisateurs affectés au groupe d'approbation de mise à jour de correctif de niveau 1. Cette propriété est activée par défaut.
Version 16.1 : Déploiement de correctif [sn_vul_patch_orch_deployment]	Stocke des informations sur les correctifs déployés sur les collections et les CI.
Version 16.1 : Mise à jour du correctif [sn_vul_patch_orch_update]	Stocke des informations sur les correctifs disponibles sur des instances distinctes.
Version 16.1 : Correctif potentiel [sn_vul_patch_orch_m2m_vuln_patch]	Stocke des données sur les correctifs et les vulnérabilités qui identifient les correctifs qui peuvent être utilisés pour résoudre une vulnérabilité.
V19.0 : Exposition potentielle à la vulnérabilité sn_vul_analyst_m2m_pot_exp_sw_model	Table d'évaluation de l'exposition pour CVE.
Catégorie de produits [sn_vul_product_category]	Contient les données de catégorie de produits importées.
Avis de sécurité Red Hat [sn_vul_rhsa_update]	Compare les solutions à la Red Hat tâche de nuit afin de déterminer les données delta pour l'importation.
Red Hat Importations de solutions [sn_vul_rh_solution_import]	Utilisé par pour organiser l'importation Intégration de solution Red Hat de données avant leur traitement.
Intégration de solution Red Hat [sn_vul_rh_integration]	Étend la table d'intégration de vulnérabilité [sn_vul_integration] pour le Intégration de solution Red Hat.
Services d'entreprise associés [sn_vul_m2m_ci_services]	Relie les CI aux services d'entreprise pour la recherche des services concernés. Contient un marqueur indiquant s'il a été ajouté par Mappage des services.
V18.0 : Nombre d'efforts de rattrapage [sn_vul_daily_count_re]	Nombre quotidien d'efforts de rattrapage. Cette table est mise à jour quotidiennement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
V18.0 : Enregistrement de l'effort de rattrapage [sn_vul_remediation_effort_record]	Suit la progression du rattrapage pour les efforts de rattrapage (RE). Contient des références aux RE.
Règle de cible de rattrapage [sn_vul_ttr_rule]	Définit le délai prévu pour le rattrapage d'un élément vulnérable. Étend le fichier d'application.
V18.0 : tâche de rattrapage [sn_vul_remediation_task]	Stocke toutes les tâches de rattrapage pour la réalité virtuelle, l'AVR, le CVR et les groupes de résultats des tests. Se compose d'informations relatives aux enregistrements de table [sn_vul_vulnerability]. Les utilisateurs qui ne peuvent pas afficher les enregistrements dans la vue de liste de table [sn_vul_vulnerability] peuvent voir ces informations d'enregistrements dans la vue de liste de table [sn_vul_remediation_task]. Cette table est accessible aux utilisateurs dans l'espace de travail Gestionnaire de vulnérabilité ou l'espace de travail de rattrapage informatique
Intégrations REST [sn_vul_rest_integration]	Étend la table d'intégration de vulnérabilité [sn_vul_integration] pour les intégrations basées sur REST.
Détection de vulnérabilité NVD SAM [sn_vul_sam_config]	Contient les CI et les vulnérabilités surveillés avec NVD SAM et indique si la détection des vulnérabilités NVD SAM est activée ou non.
Pool d'importation planifiée [sn_vul_sched_import_pool]	Collection des enregistrements d'ensembles de données à importer planifiées utilisée pour faciliter les importations simultanées de sources de données.
Sélectionner l'élément vulnérable [sn_vul_action_select_vi]	Table intermédiaire de base utilisée pour gérer les VG divisés, créer des CHG et associer des CHG
État de la configuration [sn_vul_setup_status]	Interne uniquement : utilisé par l'assistant de configuration. Chaque fois que l'Assistant de configuration est ouvert, il affiche l'état des étapes Terminé, et le pourcentage dans le coin supérieur droit provient de cette table.
Carte de gravité [sn_vul_severity_map]	Contient les mappages de la gravité de la source à la gravité normalisée.
Mappage de l'analyse de la solution	Mappe le fournisseur, le scanner et les mots clés pour l'exclusion ou l'inclusion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vul_solution_scanner_mapping]	
Diviser la tâche de rattrapage [sn_vul_action_split_vg]	Table intermédiaire utilisée pour diviser les tâches de rattrapage.
Entrée de vulnérabilité tierce [sn_vul_third_party_entry]	Vulnérabilité documentée provenant d'une source tierce.
[sn_vul_tenable_io_template	Un enregistrement de modèle est envoyé, Tenable.io puis importé pendant la nouvelle analyse pour les éléments qui ont Tenable.io comme source.
Mettre à jour le manifeste [sn_vul_update_manifest]	Liste des tâches de rattrapage qui ont été mises à jour et qui doivent être recalculées par le calculateur de déploiement.
V17.1 : Utilisation par classes CI [sn_vul_licensing_usage_by_ci_classes]	Contient le nombre d'utilisations agrégé par classe CI.
Nombre d'éléments de configuration VR [sn_vul_vr_configuration_item_count]	Contient la moyenne cumulative mobile de 90 jours des éléments de configuration importés à partir d'intégrations tierces.
Règle d'affectation de vulnérabilité [sn_vul_assignment_rule]	Contient l'ensemble des règles évaluées pour définir le groupe d'affectation sur les VI.
Calculateur de vulnérabilité [sn_vul_calculator_group]	Contient les règles du calculateur de vulnérabilité. L'ordre du calculateur détermine quel calculateur est évalué en premier, et dans chaque calculateur, une règle de calculateur, au maximum, est utilisée.
Règle du calculateur de vulnérabilité [sn_vul_calculator]	Contient les règles de tous les calculateurs. Pour chaque calculatrice, les règles de la calculatrice sont passées en revue dans l'ordre. Le premier calculateur correspondant à la condition utilise les valeurs de cette règle.
CVE de vulnérabilité [sn_vul_m2m_entry_cve]	Relie les données d'expositions courantes aux vulnérabilités (CVE) NVD aux entrées vulnérables.
Entrée de file d'attente d'importation de la sourc [sn_vul_ds_import_q_entry]	Mettez les pièces jointes en file d'attente avant qu'elles ne soient traitées par une source de données. Utilisé par les intégrations de vulnérabilité
Entrée de vulnérabilité [sn_vul_entry]	Vulnérabilité documentée.
Analyse de l'entrée de vulnérabilité [sn_vul_entry_scan]	Stocke la relation entre une analyse et une entrée de vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Cadre de travail de l'exploit de vulnérabilité [sn_vul_m2m_framework_vul]	Contient la relation entre les cadres de travail de l'exploit et les vulnérabilités.
V19.0 : Évaluation de l'exposition aux vulnérabilités sn_vul_analyst_sam_config	Table de configuration de l'évaluation de l'exposition pour CVE.
Configuration de la granularité des vulnérabilités [sn_vul_granularity_config]	Stocke et gère l'état du port d'inclusion ou d'exclusion pour le module Configurer la granularité des VI.
Tâches de remédiation [sn_vul_vulnerability]	Collecte d'éléments vulnérables organisés pour la correction.
Demandes de changement de tâche de rattrapage [sn_vul_m2m_vg_change_request]	Stocke l'association des tâches de rattrapage et des demandes CHG.
Éléments de tâche de rattrapage [sn_vul_m2m_vul_group_item]	Association des tâches de rattrapage et des éléments vulnérables.
Règles de la tâche de rattrapage [sn_vul_grouping_rule]	Contient les règles qui définissent les critères avec lesquels les groupes sont automatiquement créés pour un ensemble d'éléments vulnérables.
Intégration de vulnérabilité [sn_vul_integration]	Enregistrement programmable pour importer des données de vulnérabilité à partir d'une source externe. Prolonge l'exécution de script planifiée.
Source de données d'intégration de vulnérabilité [sn_vul_int_data_src]	Source de données à utiliser avec une intégration de vulnérabilité.
Journal d'intégration de vulnérabilité [sn_vul_integration_log]	Enregistre la sortie d'informations de journal par exécution d'intégration de vulnérabilité.
Processus d'intégration de vulnérabilité [sn_vul_integration_process]	Occurrence de processus unique pour une intégration de vulnérabilité.
File d'attente d'intégration de vulnérabilité [sn_vul_integration_queue]	Met en file d'attente les demandes d'importation pour une exécution d'intégration lorsque toutes les sources de données sont utilisées.
Exécution de l'intégration de vulnérabilité [sn_vul_integration_run]	Invocations d'intégration de vulnérabilité. **Remarque :** Si une exécution d'intégration est en cours, une seule intégration peut être à l'état Prêt dans les backlogs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Statistiques d'exécutions de l'intégration de vulnérabilité [sn_vul_integration_stats]	Stocke la répartition de chaque étape : par exemple, l'heure de l'API REST, l'heure de création du VI, et ainsi de suite pour une exécution d'intégration
Tâche d'élément de vulnérabilité [sn_vul_m2m_item_task]	Éléments vulnérables associés à des problèmes, des changements et des incidents de sécurité.
Kit malware de vulnérabilité [sn_vul_m2m_malware_kit_vul]	Contient les relations entre les vulnérabilités et les kits de logiciels malveillants.
Solution prérequise de vulnérabilité [sn_vul_m2m_solution_prerequisite]	Contient les prérequis spécifiques à la source pour appliquer une solution, lorsqu'elle est disponible.
Limite du taux de vulnérabilité [sn_vul_rate_limit]	Définit une limite de taux à utiliser sur un scanner.
Référence de vulnérabilité [sn_vul_reference]	Références externes pour les vulnérabilités connues.
État du rattrapage des vulnérabilités [sn_vul_m2m_ttr_status]	État de l'élément vulnérable par rapport à la règle de cible de rattrapage appliquée la plus proche.
Règle du groupe de vulnérabilité [sn_vul_calc_risk]	Règle de calcul spécialisée utilisée avec les calculateurs de score de risque. Prend des poids indiquant les valeurs, liées à un VI, à utiliser pour calculer le score de risque.
Calculateur de déploiement de vulnérabilité [sn_vul_rollup]	Liste des calculateurs de déploiement de vulnérabilité.
Analyse de vulnérabilité [sn_vul_scan]	Analyse de vulnérabilité. Contient ce qu'il faut analyser, avec quel scanner et un résumé des résultats de l'analyse.
Élément de configuration de l'analyse de vulnérabilité [sn_vul_m2m_scan_configuration_item]	Associe les CI CMDB qui sont mis en file d'attente pour être analysés.
Entrée de la file d'attente de l'analyse de vulnérabilité [sn_vul_scan_q_entry]	Enregistrement de l'analyse mis en file d'attente pour l'analyse ou le traitement. Facilite les demandes dans les limites de débit indiquées.
Source de l'analyse de vulnérabilité [sn_vul_m2m_scan_source]	Associe des sources à un enregistrement d'analyse et signifie que tous les enregistrements qui sont mis en file d'attente doivent être analysés.
Tâche d'analyse de vulnérabilité [sn_vul_m2m_scan_vulnerability]	Associe les tâches de vulnérabilité aux sources d'un enregistrement d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Scanner de vulnérabilité [sn_vul_scanner]	Définit les scanners tiers à utiliser dans les analyses.
Limite de taux du scanner de vulnérabilité [sn_cmn_scanner_rate_limit]	Associe un scanner à une limite de taux.
Logiciel de vulnérabilité [sn_vul_m2m_entry_software]	Contient des associations entre les vulnérabilités et les logiciels vulnérables.
Solution de vulnérabilité [sn_vul_solution]	Contient les données de relation entre la vulnérabilité et les solutions possibles. À partir de la version 24.0.6 de , une nouvelle colonne intitulée Bulletin du Réponse aux vulnérabilités scanner est ajoutée à cette table.
Solution de vulnérabilité [sn_vul_m2m_vulnerability_solution]	Relie la table Entrée de vulnérabilité (sn_vul_entry) à la table Solution de vulnérabilité (sn_vul_solution).
Approbation de changement d'état de la vulnérabilité [sn_vul_change_approval]	Suit le processus d'approbation des vulnérabilités.
Solution de remplacement à la vulnérabilité [sn_vul_m2m_solution_supersedence]	Contient la relation spécifique à la source entre les solutions.
Manifeste de mise à jour de vulnérabilité [sn_vul_vuln_update]	Contient une liste des vulnérabilités dont les données de déploiement doivent être mises à jour après la mise à jour, la fermeture de leurs éléments vulnérables ou des changements de score de risque.
Mappage du fournisseur de vulnérabilités [sun_vul_vulnerability_vendor_mapping]	Contient une liste des vulnérabilités et de leurs fournisseurs.
Élément vulnérable [sn_vul_vulnerable_item]	Contient l'occurrence d'une vulnérabilité sur un élément de configuration.
Détection d'éléments vulnérables [sn_vul_detection]	Contient les détections d'éléments vulnérables provenant d'intégrations tierces.
Logiciel vulnérable [sn_vul_software]	Logiciel connu pour avoir certaines vulnérabilités.

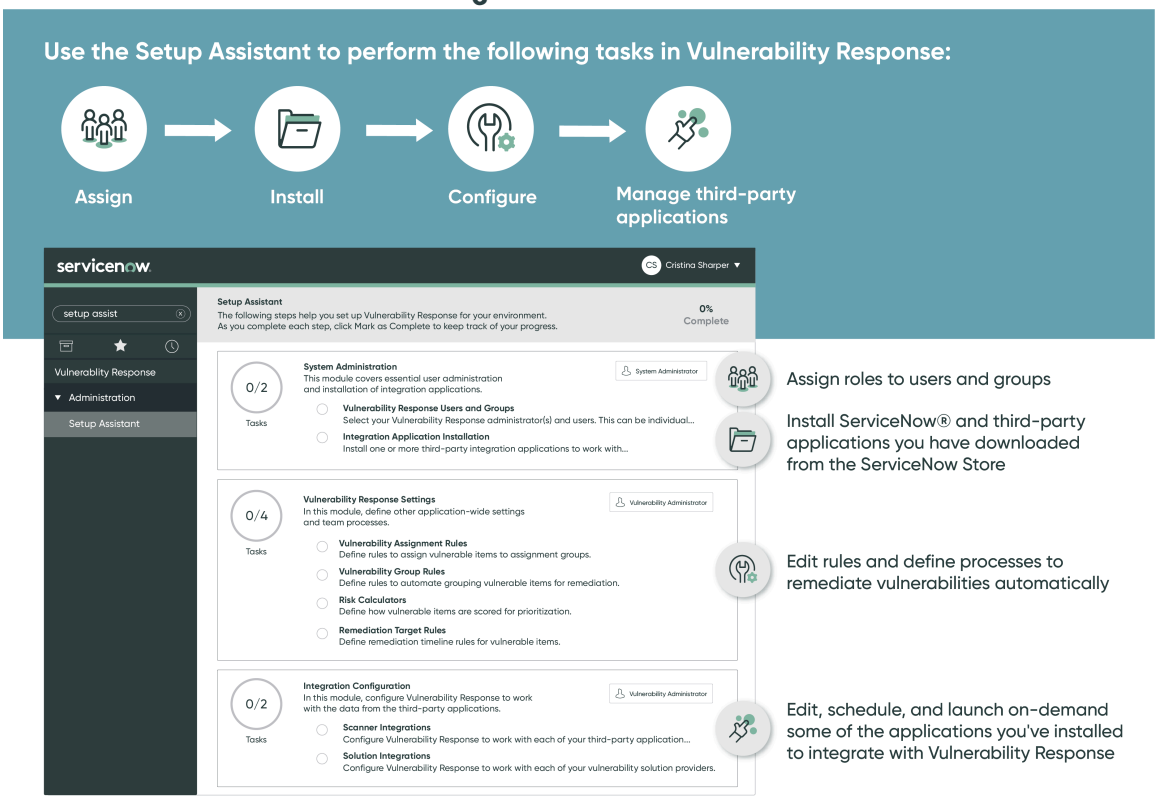
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration

L'Assistant de configuration vous guide tout au long de la Réponse aux vulnérabilités configuration et de certaines intégrations tierces pour votre environnement. L'assistant de configuration fournit presque tout ce dont vous avez besoin pour installer et configurer votre environnement afin que vous puissiez utiliser Réponse aux vulnérabilités.

Fonctionnalité de l'assistant de configuration



Now Platform® roles: admin and vulnerability admin

L'utilisation de l'assistant de configuration nécessite deux rôles différents ServiceNow AI Platform® : administrateur et administrateur de vulnérabilité.

Reportez-vous aux sections suivantes pour compléter les instructions et les invites fournies dans l'assistant de configuration.

Administration système : affecter des utilisateurs et des groupes et installer des applications d'intégration

Rôle requis : administrateur

Une liste des utilisateurs et des intégrations doit être obtenue auprès du gestionnaire de vulnérabilité avant de commencer ces tâches.

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.
2. Dans la première section, Administration système, l'administrateur attribue des rôles aux utilisateurs et aux groupes et installe les intégrations prises en charge.

   Affectez Réponse aux vulnérabilités des profils et des rôles aux utilisateurs et aux groupes dans l'Assistant de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

3. Affectez des rôles dans l'Assistant de configuration.
   - Affectez le rôle de sn_vul.admin à des utilisateurs ou à des groupes.
   - Affectez le rôle sn_vul.admin pour l'administration et la configuration de Vulnerability Response, y compris les intégrations de vulnérabilité, les règles de tâche de rattrapage, les calculateurs et les règles de délai de correction.
   - Affectez le rôle de sn_vul_vulnerability_write pour la création et la mise à jour des tâches de rattrapage et des éléments vulnérables.

     Remarque : Tous les autres utilisateurs bénéficient automatiquement d'un accès en écriture uniquement aux tâches de rattrapage qui leur sont affectées.

   - Affectez le rôle sn_vul_vulnerability_read pour afficher les tâches de rattrapage, les éléments vulnérables et d'autres informations sur la vulnérabilité.

     Remarque : Les utilisateurs disposant du rôle itil se voient automatiquement attribuer le rôle sn_vul.remediation_owner, ce qui leur permet de voir les tâches de rattrapage et les éléments vulnérables qui leur sont affectés, les entrées de vulnérabilité et les solutions dans l'application Réponse aux vulnérabilités sur leur instance et dans l'application Agent mobile . Aucune affectation supplémentaire n'est nécessaire.

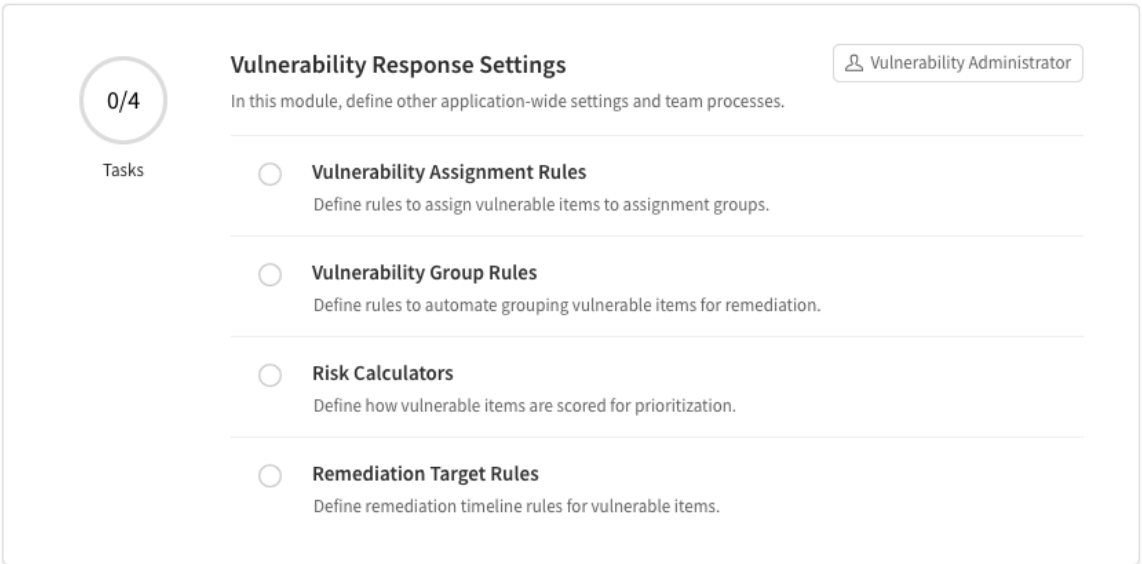
4. Installez des applications d'intégration tierces.
   - Consultez Installation et prise en charge des Réponse aux vulnérabilités applications et Intégrations de Réponse aux vulnérabilités pour plus d'informations sur les applications prises en charge par Réponse aux vulnérabilités.
   - Pour plus d'informations sur l'utilisation de l'assistant de configuration pour installer les applications prises en charge, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.

Réponse aux vulnérabilités Paramètres

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Dans les paramètres de Vulnerability Response, l'administrateur de vulnérabilité définit les paramètres à l'échelle de l'application et définit des règles pour Réponse aux vulnérabilités. L'administrateur peut également effectuer ces tâches.

1. Créer des règles d'affectation de vulnérabilité.

Créez des règles qui définissent l'affectation automatique des tâches de rattrapage pour résolution. Au moins une règle est fournie avec le système de base. Consultez Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation pour plus d'informations.

Remarque :

La fonctionnalité de réapplication nécessite une application de base des règles. Une fois vos règles créées, activez la tâche planifiée pour qu'elle s'exécute `Reapply all vulnerability assignment rules` , à votre convenance. Sinon, vous devrez réappliquer toutes les règles à tous les VI ouverts avant de les modifier.

Lorsque la tâche est terminée, définissez le champ **Exécuter** de la tâche planifiée en fonction de votre environnement. Selon le nombre de VI actifs dont vous disposez, leur évaluation et leur mise à jour quotidienne peuvent avoir un impact non négligeable sur les performances. Pour les environnements plus grands, envisagez de mettre à jour une fois par semaine, voire une fois par mois.

La réapplication des règles d'affectation ne regroupe pas les éléments vulnérables.

2. Créez des règles de tâche de rattrapage.

Créez des règles qui définissent la création automatique de tâches de rattrapage pour la résolution. Au moins une règle, **Vulnérabilité,** est fournie avec le système de base. Vous pouvez réappliquer les règles à partir de la vue de formulaire ou de liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lorsqu'une règle de groupe est supprimée, à partir de la vue de formulaire ou de liste, vous pouvez supprimer tous les groupes **ouverts** créés par cette règle. Les groupes dont l'état n'est pas **Ouvert** sont exclus.
- Pour plus d'informations sur la création de règles pour votre environnement, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces .
- Reportez-vous à la section Explorer l'application Réponse aux vulnérabilités pour plus d'informations sur l'utilisation Réponse aux vulnérabilités pour corriger les vulnérabilités.

3. Créez et activez des calculateurs de risque.

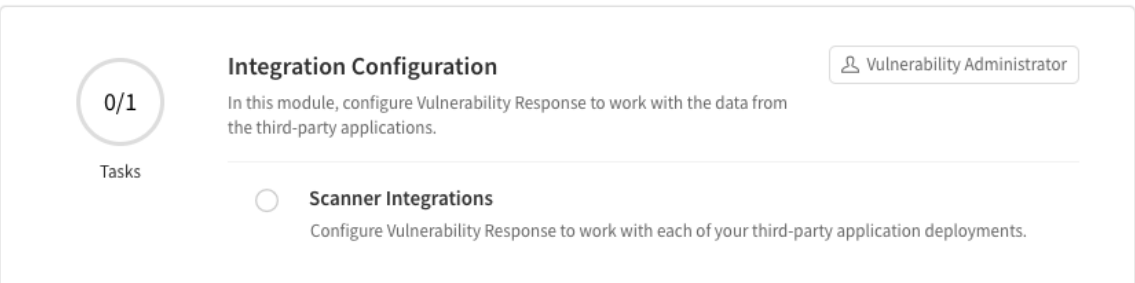
   Activez les calculateurs de risque qui définissent la notation des éléments vulnérables pour déterminer leur ordre de priorité. Plusieurs calculateurs de risque sont fournis avec le système de base. Consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité les informations sur la création ou la modification des calculateurs de risque pour votre environnement.

4. Créez des règles de cibles de rattrapage.

   Créez des règles de cible de rattrapage pour les catégories de rattrapage. Au moins une règle est fournie avec le système de base. Pour plus d'informations sur la création de règles pour votre environnement, reportez-vous à la section Réponse aux vulnérabilités Règles de cibles de rattrapage .

Configuration de l'intégration

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou administrateur.



Dans la section Configuration de l'intégration, configurez, planifiez, modifiez et lancez sur demande les intégrations de scanners de vulnérabilité tiers suivantes et, si l'application est installée, les fournisseurs de Gestion des solutions pour Réponse aux vulnérabilités solutions.

- Pour Configurer l'utilisation de l'assistant Qualys Vulnerability Integration de configuration plus d'informations sur la configuration du fichier Qualys Vulnerability Integration.
- La configuration de l'application Vulnerability Response integration with Tenable est prise en charge. Reportez-vous à Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration.
- Après avoir installé l'application Gestion des solutions pour vulnérabilités , l'option **Intégrations de solutions** s'affiche sous **Intégrations de scanners**. Cliquez sur **Intégrations de solutions** pour configurer vos fournisseurs de solutions de vulnérabilité installés à partir de cette section de l'Assistant de configuration. Les Intégration de solution Red Hat et Microsoft Security Response Center Solution Integration sont pris en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur les solutions installées, reportez-vous à la section Gestion des solutions pour vulnérabilités . Voir Installer l'application Gestion des solutions pour Réponse aux vulnérabilités pour plus d'informations sur l'installation.

Pour plus d'informations sur la configuration de vos solutions installées, reportez-vous à la section Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'assistant de configuration .

- Si une intégration est multisources, vous pouvez avoir plusieurs déploiements de la même intégration tierce.
- Les paramètres de votre intégration tierce d'origine servent de modèle pour les paramètres de chaque nouvelle intégration.

Remarque : Si vous supprimez l'intégration de vulnérabilité d'origine, vous devez sélectionner une autre intégration à utiliser comme modèle. Envisagez de désactiver l'intégration au lieu de la supprimer. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

Les données de chaque intégration tierce sont identifiées de manière unique et disponibles dans une seule instance de Réponse aux vulnérabilités.

Remarque : Plusieurs intégrations de Rapid7 InsightVM vulnérabilité pour ne sont pas disponibles dans l'assistant de configuration. Pour plus d'informations sur la configuration et la création de plusieurs Rapid7 InsightVM intégrations, reportez-vous à la section Créer des importations séparées par domaine pour une intégration .

Tâches supplémentaires

Consultez Tâches d'installation et de configuration supplémentaires Réponse aux vulnérabilités pour en savoir plus sur les tâches de configuration non incluses dans l'assistant de configuration.

Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration

Affectez les rôles de personnage à des groupes ou à des utilisateurs avec l'Assistant Réponse aux vulnérabilités de configuration.

Avant de commencer

Si vous avez déjà affecté des rôles de profil à Réponse aux vulnérabilités l'aide de l'Assistant de configuration et que vous souhaitez plus d'informations sur la modification et la gestion de vos rôles granulaires et de vos affectations de rôles dans le module Administration utilisateurs, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Si vous êtes un client de mise à niveau, vous pouvez continuer à utiliser vos rôles existants pour l'application Vulnerability Response. L'accès des utilisateurs et des groupes affectés aux autorisations sn_vul.vulnerability_read et sn_vul.vulnerability_write et aux rôles de propriétaire de rattrapage disponibles dans les versions précédentes de n'a Réponse aux vulnérabilités pas changé.

Toutefois, pour plus de contrôle sur ce que les utilisateurs et les groupes peuvent faire et voir dans l'application Réponse aux vulnérabilités au niveau de la tâche, vous préférerez peut-être utiliser des rôles de profil et granulaires.

Si vous n'avez pas encore affecté le rôle de profil sn_vul.vulnerability_admin à l'aide de l'Assistant de configuration, suivez les étapes ci-dessous pour l'affecter. Une fois affecté, l'administrateur de vulnérabilité disposant de ce rôle de profil a la permission d'effectuer les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

tâches de l'assistant de configuration après la première section et de gérer les règles et les intégrations tierces dans l'application Réponse aux vulnérabilités .

Pour une présentation des rôles de profil et des rôles granulaires, reportez-vous à la section Réponse aux vulnérabilités Profils et rôles granulaires.

Si vous êtes un client de mise à niveau, utilisez le tableau suivant comme référence.

Affectation précédente	Affectation recommandée [Profil de l'utilisateur]	Description
sn_vul.admin	sn_vul.vulnerability_admin [Administrateur de vulnérabilité]	Fournit un accès complet à l'application Vulnerability Response (VR). Les utilisateurs disposant de ce rôle configurent des applications et des règles de réalité virtuelle et installent des intégrations tierces.
sn_vulnerability_write	sn_vul.vulnerability_analyst [Analyste de vulnérabilité]	Permet l'affichage et la mise à jour de tous les enregistrements pour le rattrapage VIT.
sn_vul.remediation_owner	sn_vul.remediation_owner [Propriétaire du rattrapage]	Permet aux utilisateurs et aux groupes de corriger les vulnérabilités qui leur sont affectées ou qui sont affectées à leur groupe et de mettre à jour les enregistrements connexes.
sn_vul.admin	sn_vul.ci [Gestionnaire CI]	Permet de gérer les éléments de configuration sans correspondance introuvables dans la CMDB, y compris la mise à jour des éléments détectés.
sn_vul.admin	sn_vul.exception_approver [Approbateur d'exception]	Permet d'approuver des exceptions, des reports et des fermetures de tâches de rattrapage et d'éléments vulnérables.
sn_vul.vulnerability_read	sn_vul.read_all ou sn_vul.read_group_rules	Accorde un accès en lecture seule à des zones spécifiques de l'application. Utilisez sn_vul.read_all pour afficher tous les enregistrements VR ou sn_vul.read_group_rules pour afficher les règles de tâche de rattrapage. Les utilisateurs ayant ces rôles ne peuvent pas mettre à jour les enregistrements. **Remarque :** Plusieurs autres rôles de lecture sont disponibles dans le champ d'application Réponse aux vulnérabilités pour un accès plus précis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher les rôles granulaires dont un utilisateur ou des groupes dotés d'un rôle de profil héritent par défaut, accédez à **Tous** > **Administration utilisateurs** > **Rôles**. Recherchez le rôle souhaité et cliquez dessus pour ouvrir l'enregistrement. L'onglet Contient les rôles répertorie tous les rôles granulaires du rôle de profil, ainsi que tous les rôles hérités.

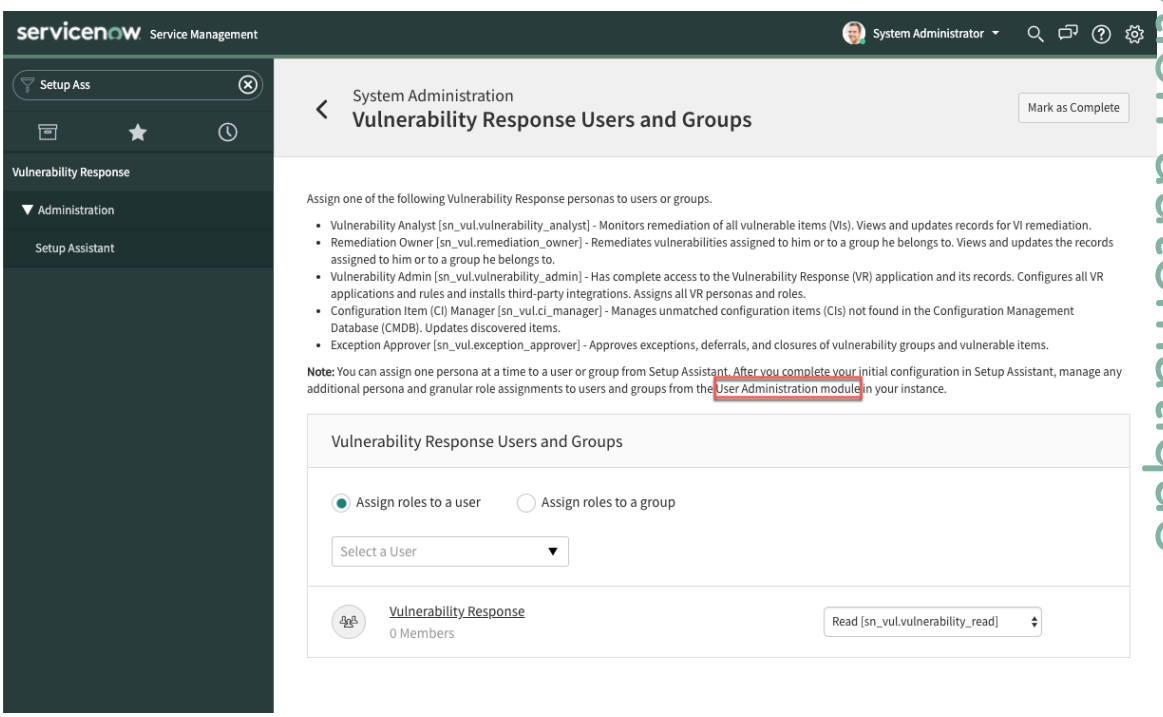
Vous préférez peut-être vérifier que tous les utilisateurs et groupes requis sont créés avant d'affecter des rôles dans l'Assistant de configuration. Pour ajouter de nouveaux utilisateurs et groupes à partir de l'Assistant de configuration, vous pouvez également cliquer sur le lien du **module Administration utilisateurs** dans le formulaire illustré dans la figure suivante.

Pour l'exemple suivant, pour limiter l'accès à l'application Réponse aux vulnérabilités , cet exemple montre comment affecter un utilisateur avec le profil d'administrateur de vulnérabilité. En règle générale, vous préférez affecter des rôles de profil autres que sn_vul.vulnerability_admin à des groupes.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration Assistant de configuration**.
   La page Assistant de configuration s'affiche.
2. Cliquez sur Utilisateur et groupes de Vulnerability Response.
   La page Utilisateurs et groupes de Vulnerability Response d'administration système s'affiche.



3. Une fois l'option Affecter des rôles à un utilisateur sélectionnée, choisissez un utilisateur existant dans la liste.

   Vous ne pouvez affecter qu'un utilisateur ou un groupe avec un rôle de profil.

   À droite du formulaire, une fois que vous avez sélectionné un utilisateur ou un groupe, le profil par défaut, Propriétaire de rattrapage [sn_vul.remediation_owner] est affecté par défaut et reste affiché dans la liste jusqu'à ce que vous le modifiiez.

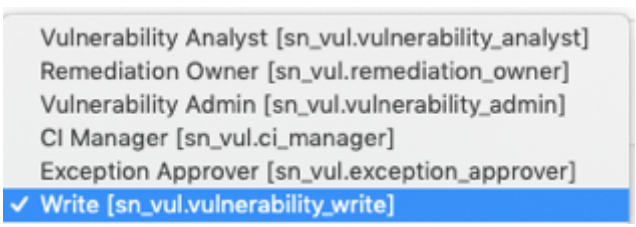
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous effectuez une mise à niveau vers une version plus récente et Réponse aux vulnérabilités que vous avez précédemment affecté le rôle sn_vul.vulnerability_read ou sn_vul.vulnerability_write à un utilisateur ou à un groupe avant la mise à niveau, il s'affiche avec les nouveaux rôles de profil, comme illustré dans la figure suivante.

Si vous êtes un client de mise à niveau, vous pouvez continuer à utiliser vos rôles existants pour l'application Vulnerability Response. L'accès des utilisateurs et des groupes affectés aux autorisations sn_vul.vulnerability_read et sn_vul.vulnerability_write et au propriétaire de la résolution avant la version 10.3 n'a pas changé.

Notez que pour les utilisateurs existants ou les groupes actuellement affectés aux rôles sn_vul.vulnerability_read ou sn_vul.vulnerability_write, ces rôles sont affichés avec les rôles de profil dans la liste. Une fois que vous avez affecté un rôle de profil, l'ancien rôle n'est plus disponible à l'avenir. Par exemple, comme le montre la figure suivante, le rôle Écrire [sn_vul.vulnerability_write] n'est plus affiché en tant qu'option pour cet utilisateur ou ce groupe après qu'il a été affecté à l'un des rôles de profil.

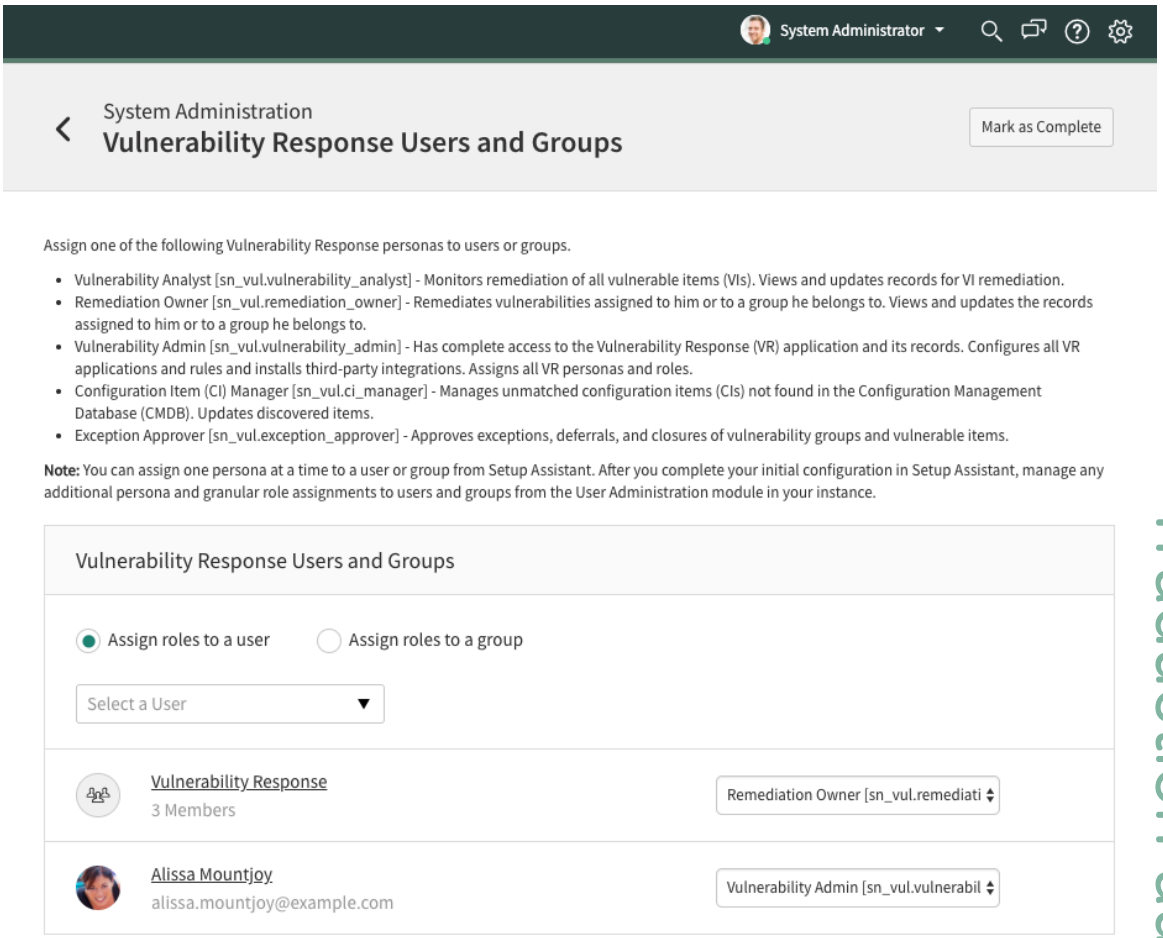


4. Dans la liste située à droite du formulaire, sélectionnez **Administrateur de vulnérabilité [sn_vul.vulnerability_admin].**
   Un message s'affiche indiquant que l'utilisateur ou le groupe est affecté avec succès au profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Profil du propriétaire de la résolution affecté à un groupe et profil d'administrateur de vulnérabilité affecté à un utilisateur



5. À l'aide des descriptions des rôles de profil répertoriées ci-dessus, continuez à affecter des utilisateurs et des groupes aux rôles de profil restants : propriétaire du rattrapage, analyste de vulnérabilité, gestionnaire de CI et approbateur d'exception.
   Vous avez terminé avec succès l'affectation de rôles de profil à des utilisateurs et à des groupes à l'aide de l'Assistant de configuration.
6. **Facultatif :** Pour modifier les utilisateurs d'un groupe à partir de l'Assistant de configuration, procédez comme suit.

   a. Une fois le groupe affiché sur le formulaire, cliquez sur le nom du groupe que vous souhaitez modifier. L'enregistrement du groupe s'affiche.

   b. Une fois l'onglet Membres du groupe sélectionné, cliquez sur **Modifier**. Le formulaire Modifier les membres s'affiche

   c. Utilisez la zone de liste double pour sélectionner ou supprimer des utilisateurs.

   d. Cliquez sur **Enregistrer** pour enregistrer vos modifications et revenir à l'enregistrement du groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Cliquez sur **Mettre à jour** pour revenir à l'assistant de configuration.

f. Sur la page de l'assistant de configuration, cliquez sur **Utilisateurs et groupes de Vulnerability Response** pour poursuivre votre configuration dans l'assistant de configuration.

Que faire ensuite

En tant qu'administrateur système, poursuivez la configuration dans l'assistant de Réponse aux vulnérabilités configuration. Notez qu'une fois la première section terminée, vous pouvez demander à un utilisateur auquel vous avez affecté le rôle de profil d'administrateur de vulnérabilité d'effectuer les tâches dans l'Assistant de configuration. Pour plus d'informations sur la gestion des rôles granulaires et des exemples, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités

Une fois que vous avez terminé votre affectation initiale de rôles de profil à l'aide de l'Assistant de configuration, gérez les affectations de rôles granulaires supplémentaires à des utilisateurs ou à des groupes à partir du module Administration utilisateurs de votre instance.

Avant de commencer

Si vous n'avez pas encore terminé l'installation et la configuration initiales de Réponse aux vulnérabilités l'utilisation de l'assistant d'installation, ou affecté des rôles de profil aux utilisateurs et aux groupes, accédez à **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**. Consultez Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

Pour les termes clés et une vue d'ensemble des rôles de profil, reportez-vous à la section Réponse aux vulnérabilités Profils et rôles granulaires.

Un rôle de profil est un rôle préconfiguré dans l'application qui est composé de plusieurs rôles granulaires. Les rôles de profil dans Assistant de configuration, Administrateur de vulnérabilité, Analyste de vulnérabilité, Propriétaire du rattrapage, Gestionnaire d'élément de configuration et Gestionnaire d'exceptions sont conçus pour correspondre aux titres de poste courants des gestionnaires, des analystes et des propriétaires de services d'une organisation informatique ou d'un groupe de rattrapage de vulnérabilité.

Si vous souhaitez que vos utilisateurs et vos groupes aient plus d'accès qu'un des rôles ne le permet, vous pouvez ajouter des rôles plus granulaires aux utilisateurs et aux groupes. Inversement, si vous souhaitez limiter l'accès à des utilisateurs et à des groupes spécifiques au niveau de la tâche, vous pouvez supprimer les rôles granulaires. Vous pouvez également créer des rôles personnalisés en fonction de vos besoins.

Rôle requis : admin

Procédure

1. Pour gérer les rôles granulaires pour les utilisateurs et les groupes, choisissez-en un pour continuer.

Option	Description
Modifier les rôles granulaires d'un utilisateur ou d'un groupe	Affectez ou supprimez des rôles granulaires pour les utilisateurs ou les groupes, ou modifiez les rôles granulaires afin que seuls certains utilisateurs d'un groupe disposent d'autorisations étendues ou limitées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Un exemple suit le tableau.
Créer un nouveau rôle	Créez un rôle à l'aide d'un ou de plusieurs rôles granulaires de la bibliothèque pour un titre de poste spécifique ou pour répondre à un besoin spécifique. Un exemple suit le tableau.

Les noms des rôles granulaires dans Réponse aux vulnérabilités décrivent généralement ce que les utilisateurs peuvent faire et voir. Pour afficher les descriptions de rôles granulaires spécifiques, accédez à **Tous** > **Administration utilisateurs** > **Rôles** et localisez le rôle souhaité. La description du rôle, les rôles qui sont automatiquement hérités lorsqu'un rôle est affecté et tous les rôles qui dépendent d'autres rôles sont également répertoriés.

2. Pour affecter ou supprimer un rôle granulaire à un utilisateur ou à un groupe, procédez comme suit.
   Par exemple, supposons que vous souhaitiez affecter un gestionnaire informatique avec un rôle qui permet à ce gestionnaire de visualiser des enregistrements, mais pas de les mettre à jour ou de les modifier. Pour afficher des enregistrements dans Réponse aux vulnérabilités, Analyse des performances pour Réponse aux vulnérabilités et pour toutes les intégrations tierces, vous devez affecter à cet utilisateur le rôle granulaire sn_vul.read_all.

   a. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs**.

   b. Localisez l'utilisateur et, dans la colonne Nom, cliquez sur l'enregistrement pour l'ouvrir.
      L'enregistrement de l'utilisateur s'affiche.

   c. Si elle est décochée, sélectionnez l'onglet Rôles.
      Les rôles actuellement affectés à l'utilisateur s'affichent.

   d. Cliquez sur **Modifier**.
      Le formulaire Modifier les membres s'affiche.

   e. Dans le champ Collection de la zone de liste double, saisissez le nom du rôle si vous le connaissez, ou saisissez `*sn_vul` pour afficher uniquement les rôles granulaires disponibles pour Vulnerability Response.

   f. Localisez et déplacez sn_vul.read_all vers la liste des rôles.

      Remarque : Utilisez le même processus pour supprimer des rôles granulaires spécifiques des utilisateurs dans la zone de liste double en déplaçant le rôle de la liste Rôles vers la liste de collecte.

   g. Cliquez sur **Enregistrer**.
      L'enregistrement utilisateur s'affiche avec le nouveau rôle granulaire.

   h. Cliquez sur **Mettre à jour** pour enregistrer vos modifications et revenir à la liste Utilisateurs.
      Vous avez fourni à un utilisateur l'autorisation de lire des enregistrements dans , mais pas de les mettre à jour, Analyse des performances pour Réponse aux vulnérabilités ainsi que Réponse aux vulnérabilités pour les intégrations tierces.

3. Pour modifier un groupe afin que seuls certains membres aient un accès étendu avec des rôles plus granulaires, procédez comme suit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, supposons que vous souhaitiez autoriser certains utilisateurs du groupe du propriétaire de rattrapage (sn_vul.remediation_owner) à créer manuellement des éléments vulnérables, mais que vous ne souhaitez pas étendre cette autorisation à tous les utilisateurs du groupe. L'autorisation de créer manuellement des éléments vulnérables est accordée par le rôle granulaire sn_vul.create_vulnerable_items. Pour accorder cette autorisation à certains utilisateurs de ce groupe, procédez comme suit.

a. Accédez à la **Tous** > **Administration utilisateurs** > **Groupes**.

b. Localisez le groupe du propriétaire du rattrapage et, dans la colonne Nom, cliquez sur le groupe pour ouvrir l'enregistrement.
L'enregistrement du groupe s'affiche.

c. Si elle n'est pas sélectionnée, sélectionnez l'onglet Membres du groupe.
Les membres actuels du groupe s'affichent.

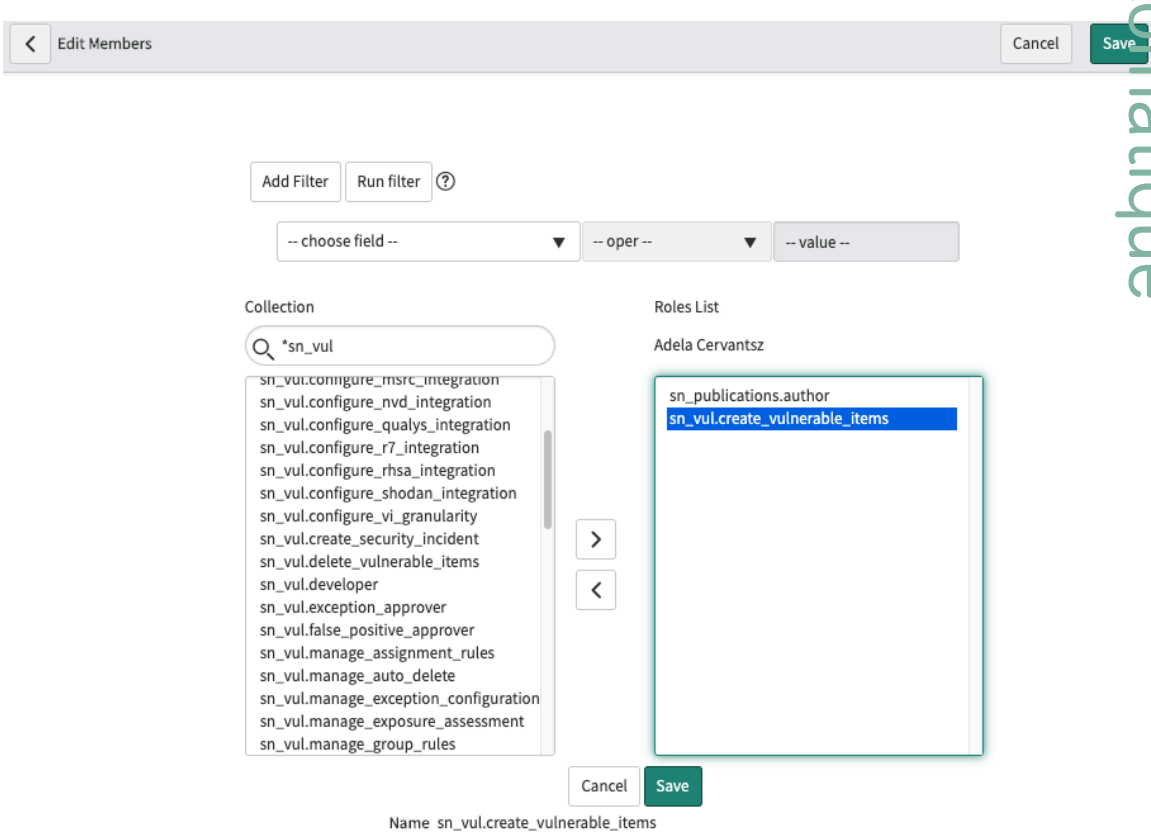
d. Cliquez sur un nom dans la liste à laquelle vous souhaitez affecter le rôle granulaire et ouvrez l'enregistrement.

e. Sur l'enregistrement, faites défiler jusqu'à l'onglet Rôles et sélectionnez-le.
Les rôles affectés à l'utilisateur s'affichent.

f. Cliquez sur **Modifier**.
Le formulaire Modifier les membres s'affiche.

g. Dans le champ Collecte, saisissez le nom du rôle si vous le connaissez, ou saisissez `*sn_vul` pour afficher tous les rôles granulaires disponibles pour Vulnerability Response.

h. Localisez et déplacez sn_vul.create_vulnerable_items vers la liste des rôles.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Cliquez sur **Enregistrer**.
L'enregistrement utilisateur s'affiche avec le nouveau rôle granulaire.

j. Cliquez sur la flèche de retour pour revenir à l'affichage des utilisateurs dans l'enregistrement pour le groupe de propriétaires de rattrapage

k. Cliquez sur les noms dans la liste à laquelle vous souhaitez affecter ce rôle granulaire, ouvrez leurs enregistrements et utilisez la zone de liste double pour affecter le rôle.

l. Une fois vos modifications terminées, cliquez sur **Mettre à jour** pour enregistrer vos modifications et revenir à la liste des groupes.
Vous avez donné à certains utilisateurs du groupe Propriétaire de rattrapage (sn_vul.remediation_owner) l'autorisation de créer manuellement des éléments vulnérables.

4. Pour créer un nouveau rôle en utilisant uniquement les rôles granulaires que vous sélectionnez, procédez comme suit.
Pour cet exemple, supposons que vous souhaitiez créer un rôle pour un auditeur de conformité. Ce rôle travaille en étroite collaboration avec Gouvernance, risque et conformité (GRC), et le travail nécessite les autorisations et tâches suivantes dans Réponse aux vulnérabilités:
   - Gère les délais de rattrapage pour les éléments vulnérables et les groupes vulnérables
   - Approuve les demandes d'exception pour prolonger les délais ou différer le rattrapage
   - Gère le nettoyage des éléments vulnérables plus anciens avec suppression automatique
   - Définir les scores de risque
   - Lit tous les enregistrements, Réponse aux vulnérabilités mais n'est pas autorisé à les modifier.

a. Accédez à la **Tous** > **Administration utilisateurs** > **Rôles**.

b. Dans la liste Rôles, cliquez sur **Nouveau**.

c. Dans l'enregistrement de rôle, renseignez les champs.

Créez un nom, sélectionnez l'application qui contient cet enregistrement et entrez une description brève de votre nouveau rôle. Pour plus d'informations sur les autres champs du formulaire, voir Créer un rôle

Remarque : Lors de la création d'un nom pour votre nouveau rôle, vous préférerez peut-être utiliser un nom facilement reconnaissable dans la liste des rôles et qui décrit la fonctionnalité du rôle. Pour cet exemple, vous préférerez peut-être un titre tel que Auditeur de conformité - GRC-VR.

d. Cliquez sur **Envoyer**.
La liste Rôles s'affiche.

e. Localisez votre nouveau rôle et cliquez dessus pour ouvrir l'enregistrement.

f. Cliquez sur **Modifier**.
Le formulaire Modifier les membres s'affiche.

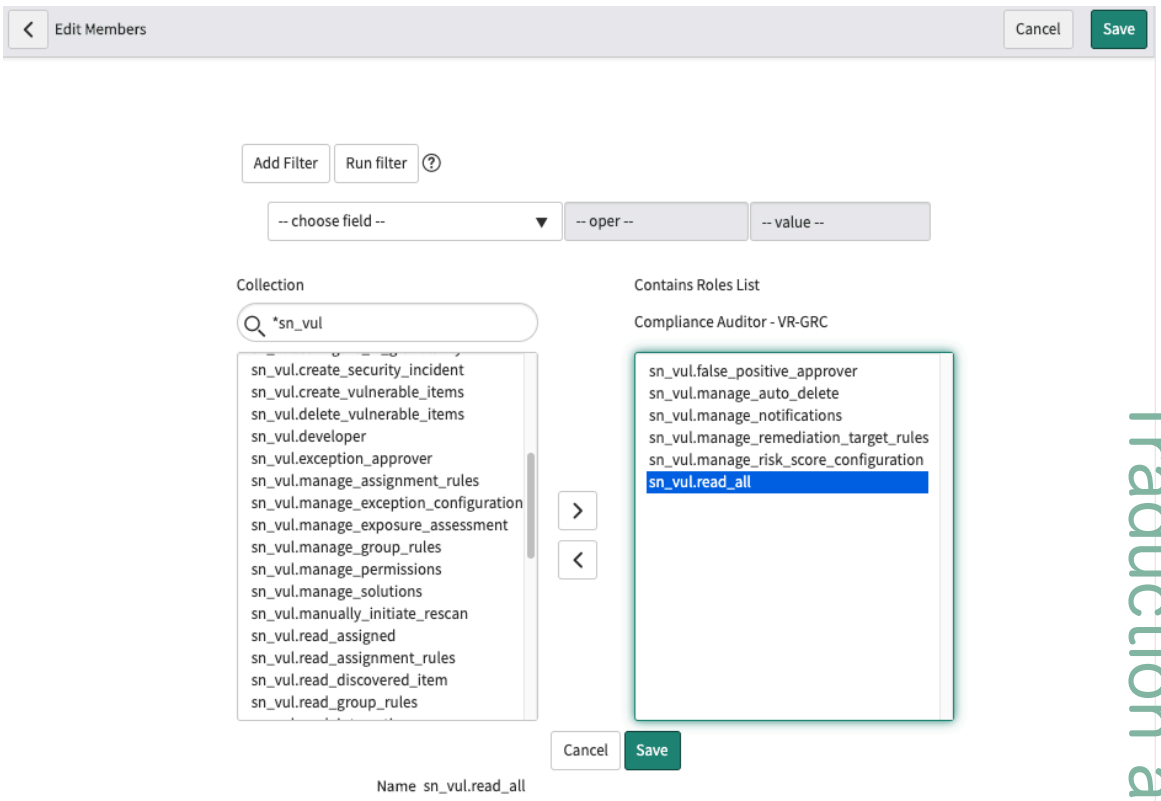
g. Utilisez la zone de liste double pour ajouter des rôles granulaires à votre nouveau rôle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour cet exemple, les rôles requis pour ce nouveau rôle sont affichés dans la colonne de droite de la figure suivante.

Pour afficher uniquement les rôles granulaires pour Vulnerability Response, dans le champ Collecte, saisissez `*sn_vul`.



h. Cliquez sur **Enregistrer**.
L'enregistrement de votre nouveau rôle s'affiche. À partir de l'onglet Contient les rôles, continuez à modifier le rôle au besoin.

i. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
Votre nouveau rôle s'affiche dans la liste Rôles.

Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration

Installez les applications d'intégration tierces pour lesquelles vous avez droit à l'aide de l'Assistant Réponse aux vulnérabilités de configuration.

Avant de commencer

L'Assistant de configuration prend en charge l'installation de la plupart des applications d'intégration tierces avec Réponse aux vulnérabilités, mais vous poursuivez la configuration pour certaines applications que vous installez à partir des modules de configuration de votre instance. Consultez la liste Intégrations de Réponse aux vulnérabilités des applications prises en charge par Réponse aux vulnérabilités.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Une fois installée, la Gestion des solutions pour vulnérabilités fonctionnalité vous permet d'accéder Réponse aux vulnérabilités à l'assistant Microsoft Security Response Center Solution IntegrationIntégration de solution Red Hat de configuration intégré.
- Gestion des solutions pour vulnérabilités est disponible par abonnement séparé. Consultez la section Gestion des solutions pour vulnérabilités pour plus d'informations sur la façon d'intégrer des Réponse aux vulnérabilités solutions.

Avant de pouvoir installer et activer des applications tierces à partir de l'Assistant de configuration, effectuez les tâches suivantes pour garantir une installation fluide :

Configurer les tâches	Description
Vérifiez que vous disposez des autorisations valides ServiceNow pour les applications d'intégration que vous souhaitez installer.	Accédez à la **Gestion des abonnements** > **Abonnements** dans votre instance pour vérifier les droits. La liste affiche les abonnements que votre organisation a achetés. Pour plus d'informations sur l'obtention d'autorisations pour une Opérations de sécurité application à partir de , reportez-vous à la ServiceNow Store section Obtenir une autorisation pour un produit ou une Opérations de sécurité application.
(Facultatif) Si elle n'est pas déjà installée et activée, vous préférerez peut-être installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce.	Pour plus d'informations sur l'installation et l'activation de l'application Réponse aux vulnérabilités , consultez Installer et configurer Vulnerability Response.
Si ce n'est pas déjà fait depuis l'installation et l'activation, vous devez activer et importer les données de vulnérabilité avec l'intégration NVD et la tâche planifiée CWE avant d'exécuter une application d'analyse tierce pour importer les données.	Exécutez les intégrations NVD et CWE dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit d'analyse tiers. Consultez Présentation des intégrations NVD pour plus d'informations.
Vérifiez que vous avez effectué toutes les tâches de configuration requises pour les intégrations tierces pour Réponse aux vulnérabilités.	Passez en revue toutes les tâches de configuration requises pour chaque intégration que vous souhaitez installer à .Intégrations de Réponse aux vulnérabilités

Rôle requis : admin

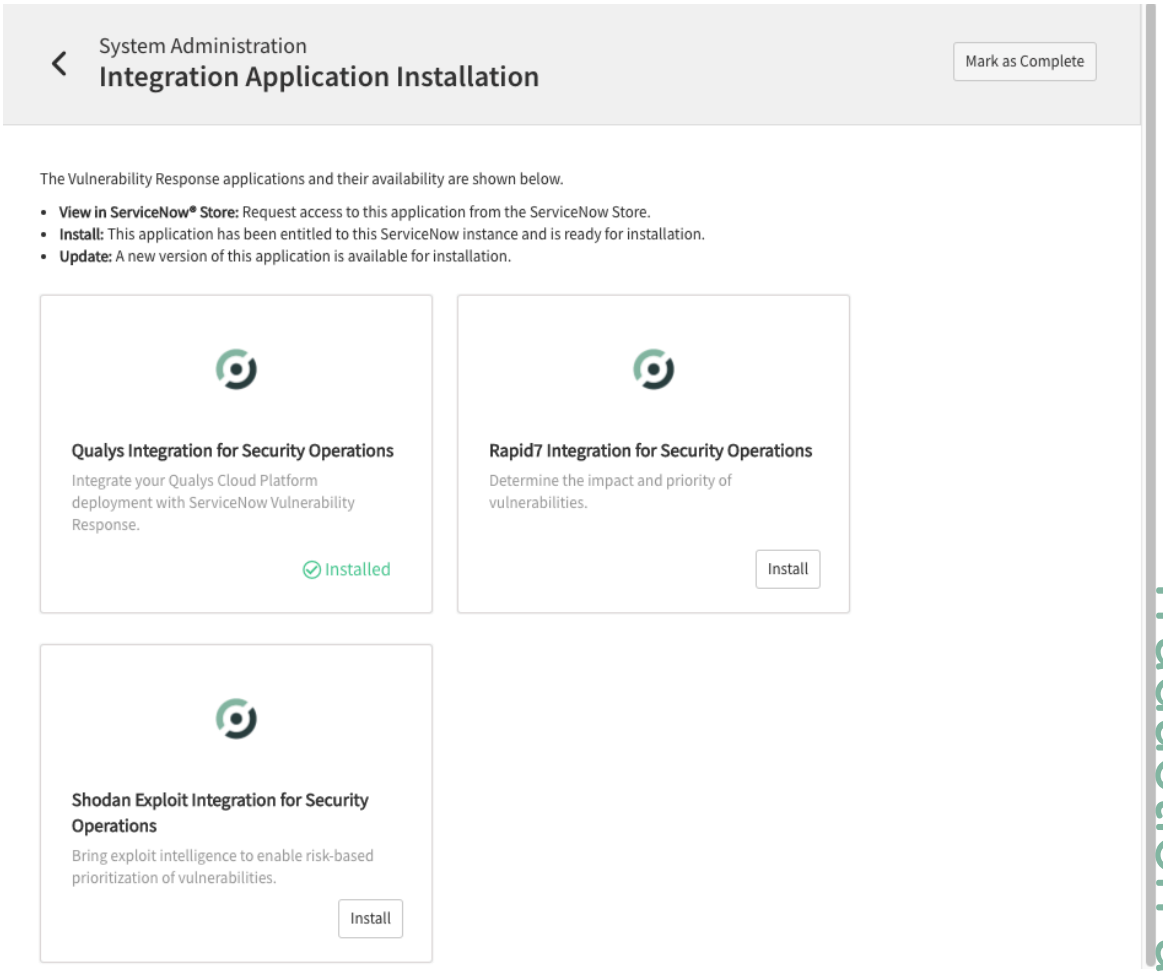
Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Administration système** > **Installation d'application d'intégration**.

   Après quelques instants, les applications pour lesquelles vous avez droit et qui sont disponibles pour installation sur votre instance s'affichent.

Traduction automatique

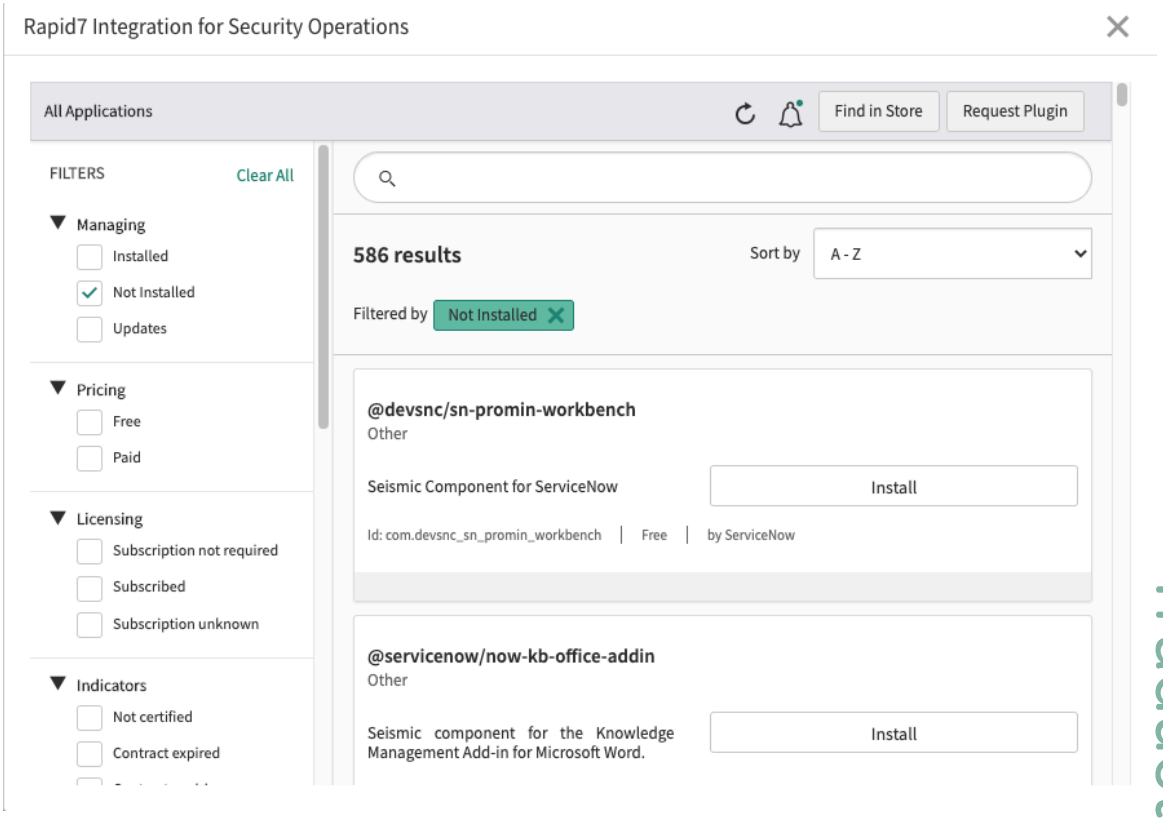
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Localisez l'application que vous voulez installer, puis cliquez sur **Installer** dans la vignette de l'application. La boîte de dialogue Toutes les applications s'affiche avec le nom de la vignette d'application sur laquelle vous avez cliqué, par exemple, Intégration Rapid7 pour Security Operations, comme illustré dans la figure suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

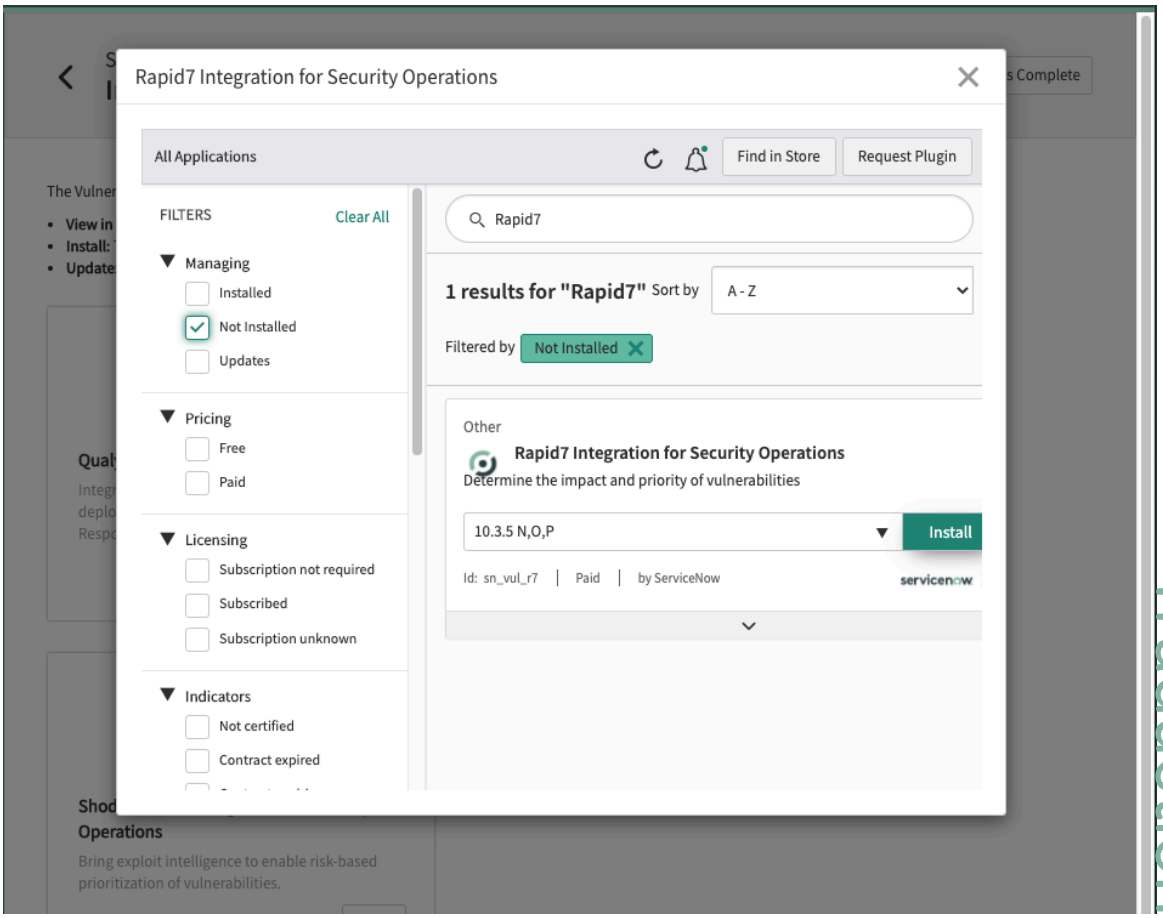


3. Localisez l'application, sélectionnez une version dans la liste de choix, puis cliquez sur **Installer**.

Si une mise à jour est disponible pour l'application, le bouton **Mettre à jour** s'affiche.

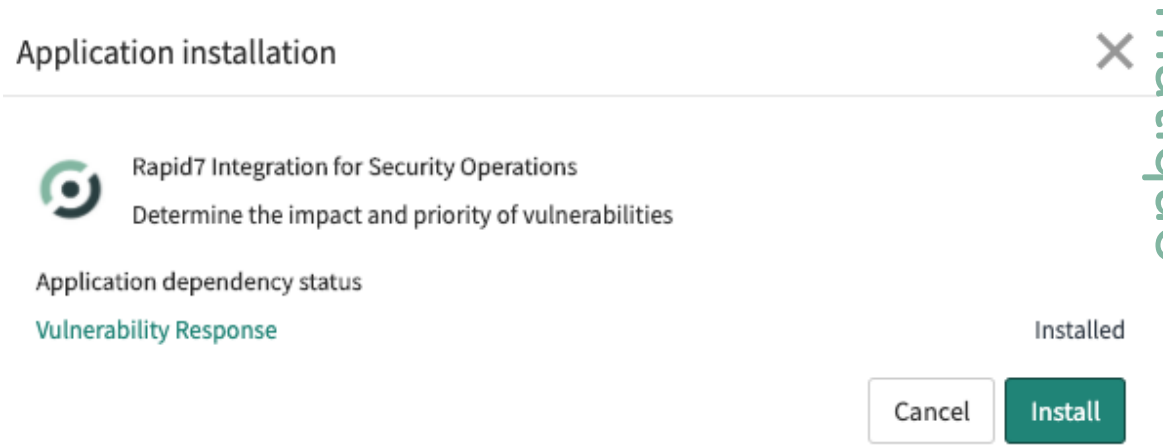
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La boîte de dialogue d'installation de l'application affiche l'état de dépendance de l'application. Toutes les dépendances requises qui ne sont pas déjà installées sont automatiquement installées avec l'application.

4. Dans la boîte de dialogue d'installation de l'application, cliquez sur **Installer**.



La boîte de dialogue Installer indique que l'installation est terminée.

5. Fermez la boîte de dialogue.
La page Toutes les applications s'affiche et affiche que votre application est installée avec succès.

Après l'installation et l'activation, vous pouvez configurer, programmer et lancer les applications et solutions installées suivantes directement à partir de la section Configuration de l'intégration de l'Assistant de configuration :

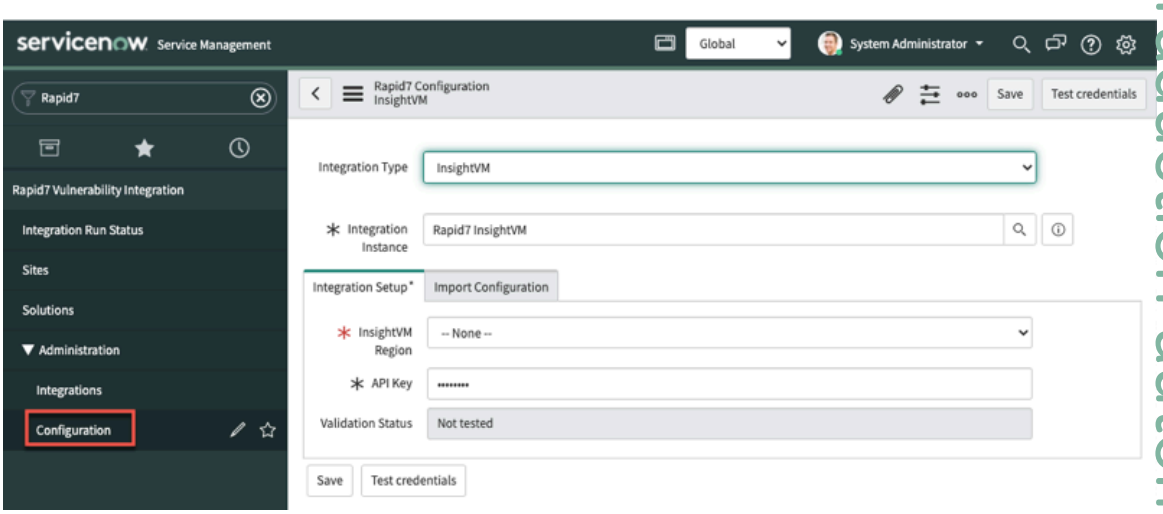
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le Qualys Vulnerability Integration
- Le Vulnerability Response integration with Tenable.
- Le Microsoft Security Response Center Solution Integration
- Le Intégration de solution Red Hat
- Microsoft Security Response Center Solution Integration
- L'intégration Microsoft Defender Gestion des vulnérabilités

Pour les autres applications non répertoriées ci-dessus, accédez directement au module de configuration de l'application pour poursuivre la configuration et saisir toutes les informations d'identification tierces requises. Par exemple, l'image suivante montre l'emplacement de la configuration et du module de l'application Rapid7 .

Pour plus d'informations sur la configuration d'applications spécifiques, consultez la documentation produit d'installation et de configuration par nom de produit fourni pour chaque application.



Que faire ensuite
Poursuivez la configuration de votre application dans l'Assistant de configuration si votre application est prise en charge.

Si votre application n'est pas prise en charge pour la configuration dans l'Assistant de configuration, accédez directement au module de configuration de l'application pour poursuivre la configuration. Pour afficher les applications prises en charge dans l'Assistant de configuration, reportez-vous à la section Installation et prise en charge des Réponse aux vulnérabilités applications.

Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces

Si ce n'est pas déjà fait, téléchargez et exécutez l'intégration NVD et exécutez la tâche planifiée CWE dans le cadre de votre configuration initiale de Vulnerability Response et avant d'importer des données de vulnérabilité dans votre instance avec un produit d'analyse tiers. L'intégration de Vulnerability Response avec NVD est disponible sur le ServiceNow Store.

Ingestion de données CWE et NVD

Les données importées à partir des intégrations NVD et CWE sont utilisées pour enrichir les données de vulnérabilité de votre instance et vous aider à décider s'il faut escalader le rattrapage pour une vulnérabilité, un élément vulnérable ou une tâche de rattrapage. Après

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

une importation initiale, vous pouvez mettre à jour les enregistrements de bibliothèque à la demande ou configurer une tâche planifiée pour mettre à jour les enregistrements régulièrement. Réponse aux vulnérabilités les stocke dans les **bibliothèques**.

Le système commun de notation des vulnérabilités (CVSS), inclus dans NVD et les entrées tierces, capture les principales caractéristiques d'une vulnérabilité. Réponse aux vulnérabilités utilise les données CVSS pour produire une valeur normalisée reflétant la gravité de la vulnérabilité. Lorsque la gravité est calculée, la vulnérabilité permet de mieux comprendre le risque posé par cette vulnérabilité pour votre organisation. La gravité vous aide à évaluer et à classer par ordre de priorité le rattrapage de vulnérabilité.

S'il s'agit de votre première installation de Réponse aux vulnérabilités, ou avant d'ingérer des données pour la première fois avec un produit de scanner tiers :

1. Effectuez une importation initiale des données CWE avec l'intégration complète CWE 2000.

   Consultez Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE pour plus d'informations. Vous effectuez des mises à jour CWE **sur demande** à partir de l'enregistrement d'intégration par défaut, et vous devez le configurer si vous souhaitez qu'il s'exécute en tant que tâche planifiée.

   Remarque : Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. Le jour par défaut pour la mise à jour NVD est le **lundi**, **chaque semaine**.

2. Vérifiez que l'intégration avec l'application Réponse aux vulnérabilités NVD est installée et que les données de l'API (CVE uniquement) ou de l'API (CVE et CPE) sont importées.

   L'activation de ce module d'extension pour les instances de production peut nécessiter une licence distincte. Après son installation, l'intégration NIST National Vulnerability Database Integration : API (CVE uniquement) est activée par défaut. Il fonctionne quotidiennement. Voir Présentation des intégrations NVD et Installer l'intégration Réponse aux vulnérabilités avec la base de données de vulnérabilité nationale NIST pour plus d'informations.

3. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Consultez la documentation de votre intégration à l'adresse Intégrations de Réponse aux vulnérabilités pour plus d'informations sur les intégrations tierces.

Affichage des données de vulnérabilité et des éléments vulnérables importés

Les bibliothèques suivantes sont disponibles :

Bibliothèques	Description
NVD	Liste des vulnérabilités trouvées par NVD et comprend des listes de vérification de sécurité, des failles logicielles liées à la sécurité, des erreurs de configuration, des noms de produits et des mesures d'impact, y compris les exploits.
CWE	Liste des types de faiblesses logicielles développés par la communauté. Chaque enregistrement CWE comprend également un article de la base de connaissances associé qui décrit la faiblesse. Vous ne pouvez pas escalader une vulnérabilité à partir de l'écran Common Weakness Enumerations, à titre de référence uniquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bibliothèques	Description
Tiers	Liste des vulnérabilités tierces importées dans votre instance. Contient une liste des références, des éléments vulnérables, des exploits et des CVE connexes.

Information associée

Afficher les Réponse aux vulnérabilités bibliothèques de vulnérabilités

Installer l'application Gestion des solutions pour Réponse aux vulnérabilités

Avant de pouvoir utiliser la Gestion des solutions pour Réponse aux vulnérabilités fonctionnalité de Réponse aux vulnérabilités dans votre instance, vous devez terminer l'installation de l'application Gestion des solutions pour vulnérabilités . Cette application est disponible sous forme d'abonnement distinct dans le ServiceNow Store.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Effectuez ces tâches de configuration pour une installation fluide.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Les Microsoft Security Response Center Solution Integration et Intégration de solution Red Hat sont les applications de solutions disponibles dans Gestion des solutions pour Réponse aux vulnérabilités après l'installation Gestion des solutions pour vulnérabilités de .

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Gestion des solutions pour Réponse aux vulnérabilités nécessite l'application Réponse aux vulnérabilités . Pour la version la plus récente de Gestion des solutions pour vulnérabilités, vérifiez que la version la plus récente de Réponse aux vulnérabilités est installée. Consultez KB0856498 les changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response . Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que vous disposez des droits d'accès à l'application.	Pour vérifier que vous disposez des droits d'accès à l'application Gestion des solutions pour vulnérabilités , accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Pour obtenir l'autorisation pour l'application Gestion des solutions pour vulnérabilités à partir de et ServiceNow Store la télécharger sur votre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	ServiceNow AI Platform instance, reportez-vous à la section Obtenir une autorisation pour un produit ou une Opérations de sécurité application.
Assurez-vous que vos dossiers NVD sont à jour depuis 10 ans.	Consultez Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.
Assurez-vous que vos vulnérabilités tierces sont à jour.	Consultez la section Intégrations de Réponse aux vulnérabilités pour plus d'informations sur les intégrations de vulnérabilité tierces.
Vérifiez que les rôles requis ServiceNow AI Platform sont affectés à votre instance.	Les rôles suivants sont requis pour l'installation et la vérification des résultats attendus : Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités. • L'administrateur système [admin] installe l'application. S'il n'est pas déjà affecté, l'administrateur affecte le rôle d'administrateur de vulnérabilité [sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)]. • L'administrateur de vulnérabilité supervise la configuration et vérifie les résultats attendus.

Rôles requis : administrateur pour installer l'application Gestion des solutions pour vulnérabilités et administrateur de vulnérabilité pour la configurer.

Procédure

1. Accédez au ServiceNow Store.
2. Cliquez sur **Connexion** et saisissez vos informations d'identification HI.
3. Cliquez sur l'onglet **Produits ServiceNow** pour afficher les produits disponibles ServiceNow .
4. Cliquez sur le signe plus (**+**) à côté **de Gestion des solutions de vulnérabilité** pour afficher toutes les applications associées auxquelles vous êtes éligible.
5. Cliquez sur **S'abonner** pour vérifier que vous avez droit à Gestion des solutions pour vulnérabilités l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Si vous disposez déjà d'une autorisation, passez à l'étape 10 pour installer l'application sur votre ServiceNow AI Platform instance.
7. Cochez la case et cliquez sur **Accepter** pour accepter les termes et conditions à l'invite.
   Un message s'affiche pour indiquer que vous êtes abonné à l'application.
8. **Facultatif :** Cliquez sur Gérer le droit si vous souhaitez gérer votre droit pour Gestion des solutions pour vulnérabilités d'autres ServiceNow AI Platform instances.

   Remarque : Si le bouton **Gérer le droit** n'est pas affiché, cliquez sur l'application **Gestion des solutions de vulnérabilité** dans la Liste de produits pour l'afficher.

   a. Choisir une option

   b. Cliquez sur **OK** ou **sur Annuler** pour continuer.
      Vous pouvez activer les modules d'extension et installer l'application sur vos instances.

9. Connectez-vous à l'instance ServiceNow AI Platform sur laquelle vous souhaitez installer l'application Gestion des solutions pour vulnérabilités .
10. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.
11. Localisez l'application Gestion des solutions pour vulnérabilités (sn_vul_solution) et cliquez sur **Installer**.
    La boîte de dialogue d'installation de l'application affiche l'état du module d'extension de dépendance d'application. Toutes les dépendances requises qui ne sont pas déjà installées sont automatiquement installées avec l'application.
12. Cliquez sur **Installer**.
    Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'application et ses dépendances installées.

    L'administrateur de vulnérabilité peut maintenant configurer l'application à partir de l'assistant de configuration.
13. Cliquez sur **Fermer**.

    Les Microsoft Security Response Center Solution Integration et Intégration de solution Red Hat sont les applications de solutions disponibles dans Gestion des solutions pour Réponse aux vulnérabilités après l'installation Gestion des solutions pour vulnérabilités de .

    Affichez les solutions de vulnérabilité en accédant à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions**. Consultez Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'assistant de configuration pour plus d'informations.

Que faire ensuite

Après avoir configuré l'application et les solutions disponibles, vérifiez que les CVE et les solutions s'accordent à l'aide de la table Solution de vulnérabilité [sn_vul_m2m_vulnerability_solution].

Installer et configurer l'application Analyse des performances pour Réponse aux vulnérabilités [PA]

Avant de pouvoir utiliser l'application, vous devez obtenir une Analyse des performances pour Réponse aux vulnérabilités autorisation et télécharger l'application à partir de , ServiceNow Store l'installer sur votre ServiceNow AI Platform® instance, puis effectuer quelques étapes d'installation et de configuration. L'application PA n'est pas installée avec l'application Réponse aux vulnérabilités . Elle est disponible sous la forme d'un abonnement distinct.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Si vous avez déjà l'application sur votre instance et que vous effectuez la mise à jour vers une version plus récente de l'application, passez à l'étape 8 des étapes suivantes pour poursuivre la mise à jour et la configuration.

Pour une nouvelle installation, effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Pour vérifier que les modules d'extension et les applications sont installés et activés, accédez à **Tous** > **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que le module d'extension Vulnerability Response dependencies (com.snc.vul_dep) est installé et activé.	**Dépendances de Vulnerability Response** Ce module d'extension contient tous les modules d'extension de dépendance requis pour prendre en charge l'application. Pour vérifier que le module d'extension est installé et activé, dans votre instance vous souhaitez que l'application accède à **Applications système** > **Toutes les applications disponibles** > **Tous**. Si vous êtes invité à mettre à jour d'autres modules d'extension de dépendance, cliquez sur les liens dans les boîtes de dialogue et suivez les invites pour continuer.
Vérifiez que l'application ServiceNow Réponse aux vulnérabilités (sn_vul) est installée et activée.	**Réponse aux vulnérabilités** Pour vérifier que le module d'extension est installé et activé, dans votre instance vous souhaitez que l'application accède à **Applications système** > **Toutes les applications disponibles** > **Tous**. Si vous êtes invité à mettre à jour d'autres modules d'extension de dépendance, cliquez sur les liens dans les boîtes de dialogue et suivez les invites pour continuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	L'activation de ce module d'extension pour les instances de production peut nécessiter une licence distincte. Contactez ServiceNow pour plus de détails.
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance. Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur Performance Analytics [pa_admin] ou le système [admin] installe l'application et vérifie les résultats attendus. • L'administrateur de vulnérabilité [sn_vul.vulnerability_admin ou sn_vul.admin (obsolète)] supervise la configuration et vérifie les résultats attendus avec les tableaux de bord PA. • Le propriétaire du rattrapage [sn_vul.remediation_owner] supervise les tâches de gestion des changements et lit et met à jour les enregistrements affectés. Le rôle sn_vul.remediation_owner est également affecté automatiquement lorsqu'un utilisateur est affecté au rôle itil.
Vérifiez que Performance Analytics et Réponse aux vulnérabilités les applications sont compatibles.	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

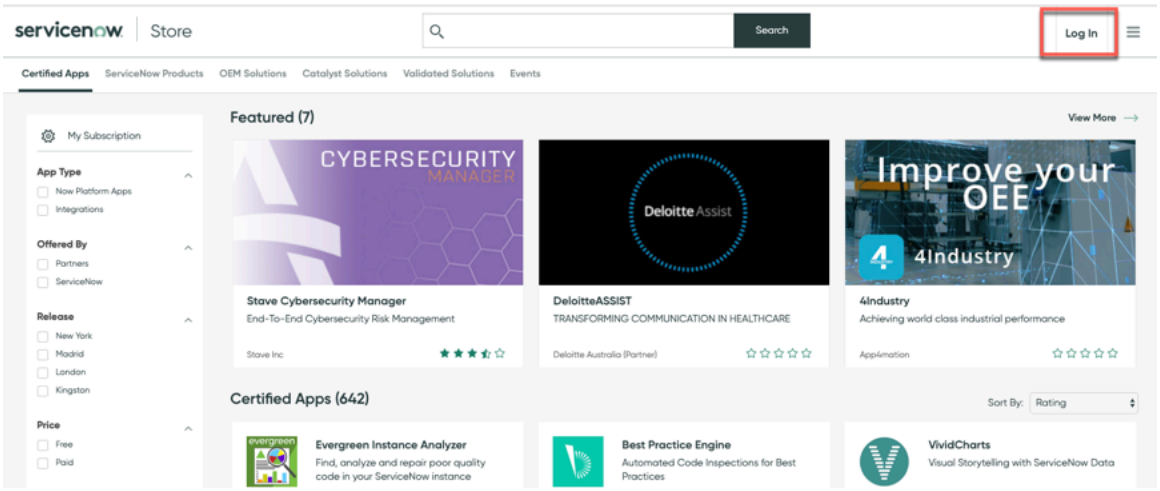
Rôle requis : admin ou pa_admin

Procédure

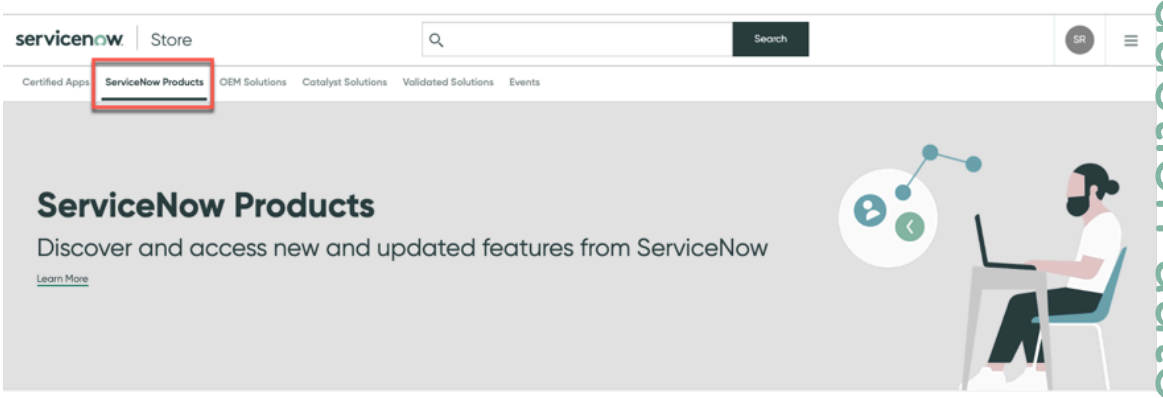
1. Pour obtenir une autorisation et télécharger l'application sur votre ServiceNow AI Platform instance, accédez au .ServiceNow Store
2. En haut à droite de la page, cliquez sur **Se connecter**.

Traduction automatique

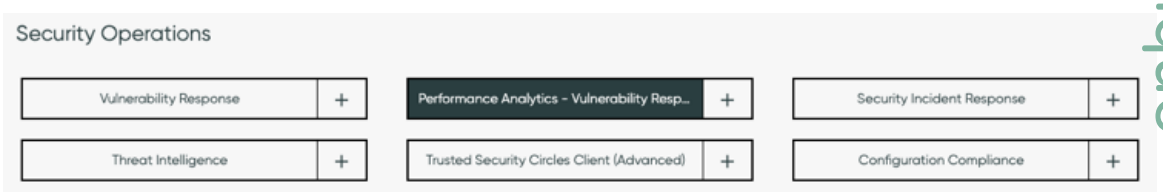
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



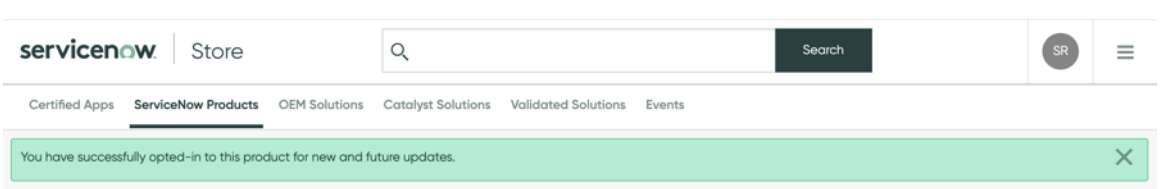
3. Dans la boîte de dialogue qui s'affiche, saisissez vos informations d'identification HI et cliquez sur **Connexion**.
4. Sur la page qui s'affiche, si elle n'est pas sélectionnée, cliquez sur l'onglet **Produits ServiceNow** .



5. Sur la page de liste de produits, cliquez sur **Analyse des performances - Réponse aux vulnérabilités**.



6. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
   Une page avec le bouton Opt-in s'affiche.
7. Pour obtenir l'application, cliquez sur **S'inscrire**Analyse des performances pour Réponse aux vulnérabilités.
8. Pour accepter les termes et conditions, à l'invite, cochez la case et cliquez sur **Accepter**.



Traduction automatique

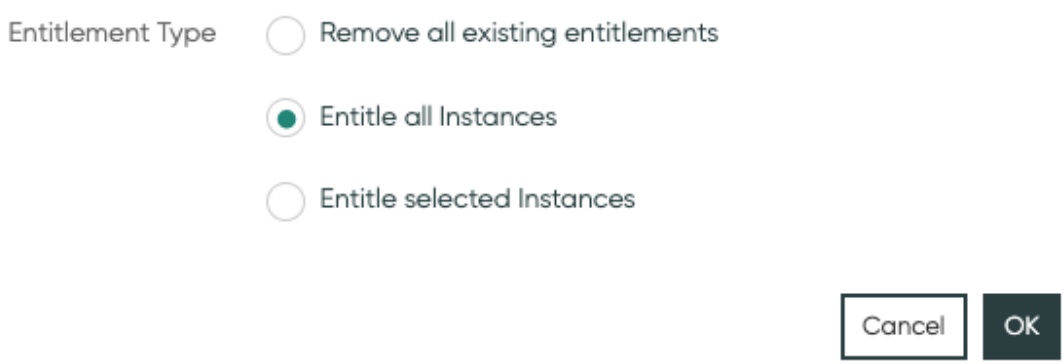
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. **Facultatif :** Pour gérer votre droit pour l'application sur d'autres ServiceNow AI Platform instances, procédez comme suit.

   a. Si le bouton Gérer le droit n'est pas affiché, cliquez sur l'application Analyse des performances pour Réponse aux vulnérabilités dans la Liste de produits pour l'afficher.

   b. Une fois l'onglet Éligible sélectionné, cliquez sur **Gérer le droit**.

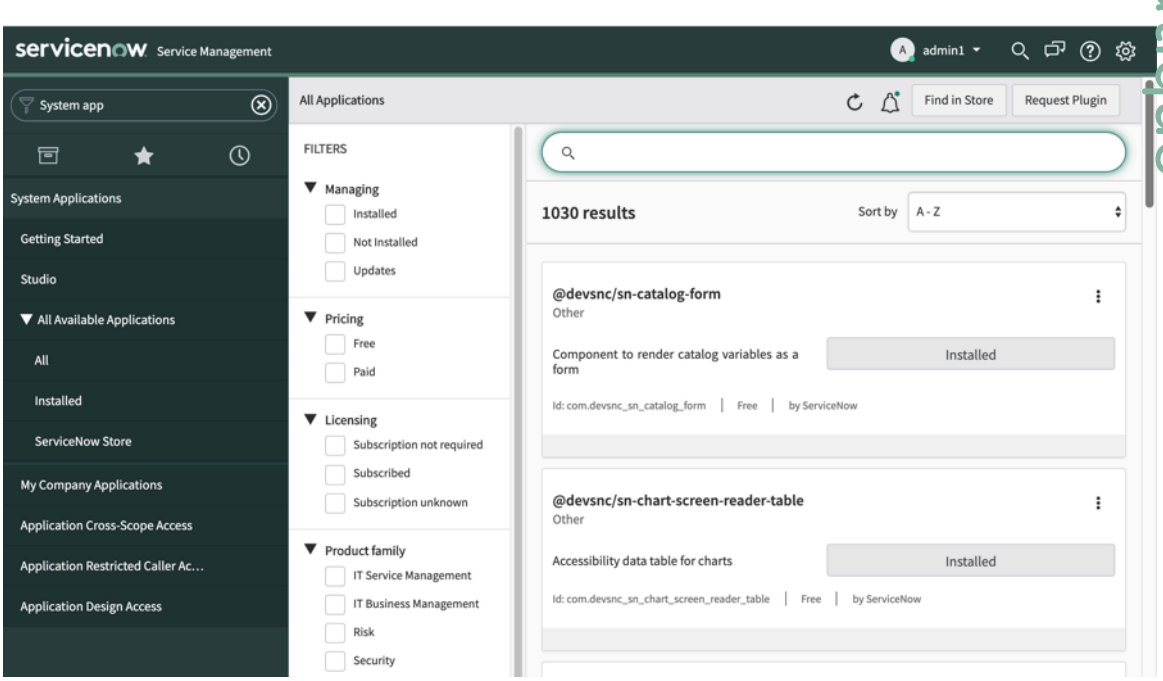
   c. Dans la boîte de dialogue Gérer les autorisations pour Vulnerability Response qui s'affiche, choisissez l'une des options suivantes :



   d. Cliquez sur **OK** ou **sur Annuler** pour continuer.
   Vous êtes prêt à activer les modules d'extension et à installer l'application sur votre ou vos ServiceNow AI Platform instances.

10. Connectez-vous à l'instance ServiceNow AI Platform sur laquelle vous souhaitez installer l'application Réponse aux vulnérabilités .

11. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

12. Parmi les applications répertoriées, localisez l'application Analyse des performances - Content Pack - Réponse aux vulnérabilités (sn_vul_analytics) et cliquez sur **Installer**.

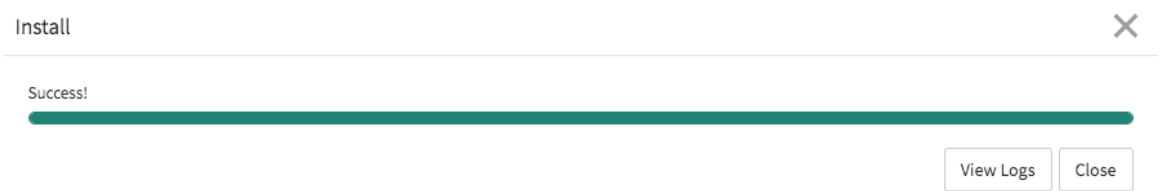
    Remarque : Si vous effectuez une mise à jour vers une nouvelle version, sélectionnez la version souhaitée dans la liste de choix.

    et cliquez sur **Mettre à jour**.
    La boîte de dialogue d'installation de l'application s'affiche. Toutes les dépendances qui seront installées automatiquement avec l'application sont également affichées.

13. **Facultatif :** Si vous souhaitez des données de démonstration, cochez la case Charger les données de démonstration et cliquez sur **Installer**.

    Remarque : Si vous ne cochez pas la case **Charger les données de démonstration**, les données de démonstration ne sont pas disponibles pour une installation ultérieure à partir du gestionnaire d'applications. Pour plus d'informations sur l'installation ou la réinstallation des données de démonstration après l'installation initiale, consultez l'article Solution de contournement pour installer les données de démonstration si l'application est déjà installée [KB0722909] dans la base de Now Support connaissances.

    Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'installation de l'application réussie.



14. Cliquez sur **Fermer**.

15. **Facultatif :** Si vous prévoyez un grand nombre d'éléments vulnérables actifs dans votre environnement, vous préférerez peut-être modifier le paramètre par défaut pour le nombre maximal d'enregistrements collectés, activer les travaux planifiés et définir les heures de collecte en dehors des heures de travail.
    Pour modifier ces paramètres et d'autres paramètres de l'application après son installation, procédez comme suit.

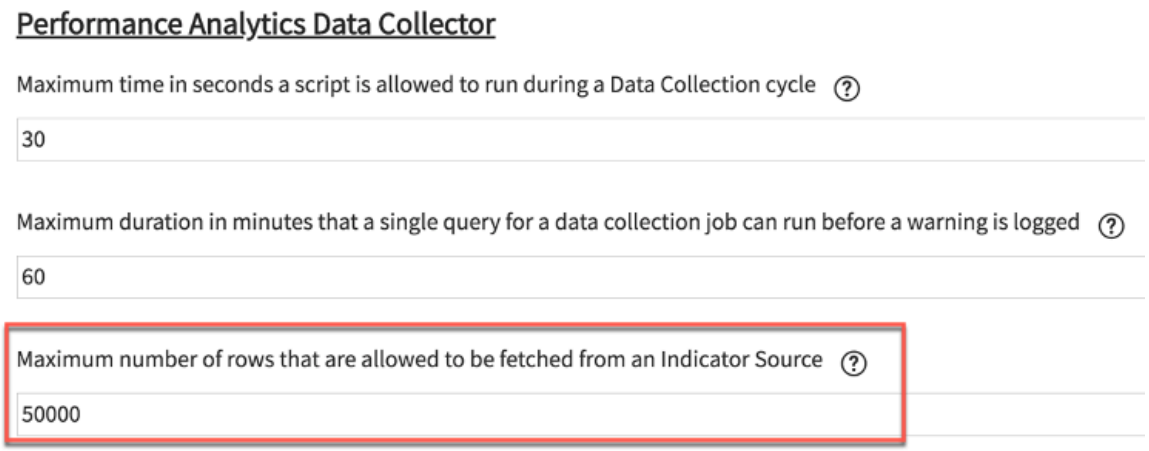
    a. Accédez à la **Tous** > **Analyse des performances** > **Console d'administration**.

    b. Dans la vignette Configuration avancée, cliquez sur le lien **Propriétés de Performance Analytics** .

    c. Sur la page Console d'administration [Analyse des performances], accédez à la section Collecteur de données d'Analyse des performances.
    Le paramètre par défaut (50 000 enregistrements) s'affiche pour le Nombre maximal de lignes pouvant être extraites d'une source d'indicateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

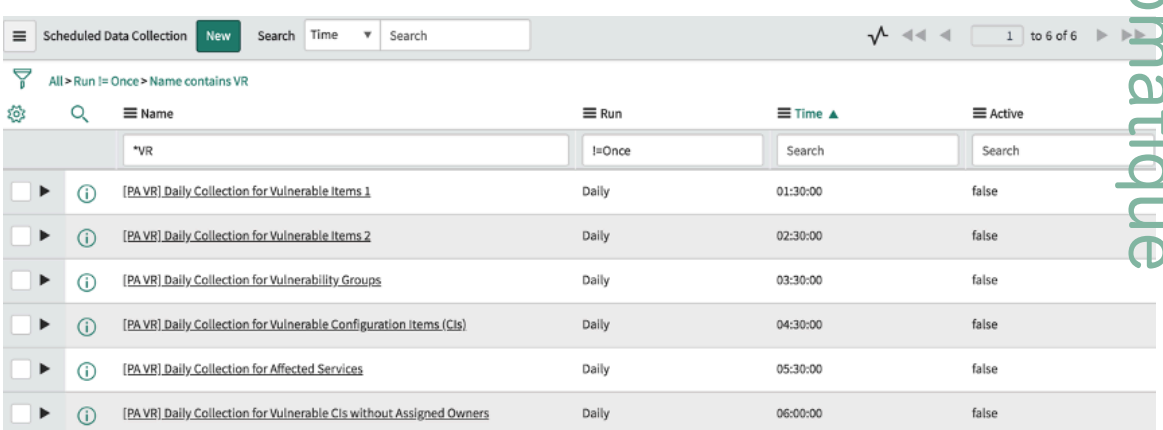


d. Vous préférerez peut-être augmenter ce nombre à une valeur supérieure d'environ 20 % au nombre total d'éléments vulnérables actifs (VI) que vous prévoyez dans votre environnement.

e. Cliquez sur **Enregistrer**.

f. Pour activer les travaux planifiés, accédez à **Analyse des performances** > **Collecteur de données** > **Tâches**.
La liste Collecte de données planifiée s'affiche. Dans la colonne Actif, les travaux planifiés répertoriés dans la colonne Application pour Analyse des performances - Pack de contenu - Réponse aux vulnérabilités sont désactivés par défaut (faux).

Remarque : Une tâche planifiée pour la collecte de données historiques ne s'affiche pas dans la liste des tâches. Pour les jeux de données volumineux, vous préférez peut-être commencer à collecter des données et des tendances au fil du temps en activant vos tâches quotidiennes lorsque vous configurez Analyse des performances pour Réponse aux vulnérabilités l'application.



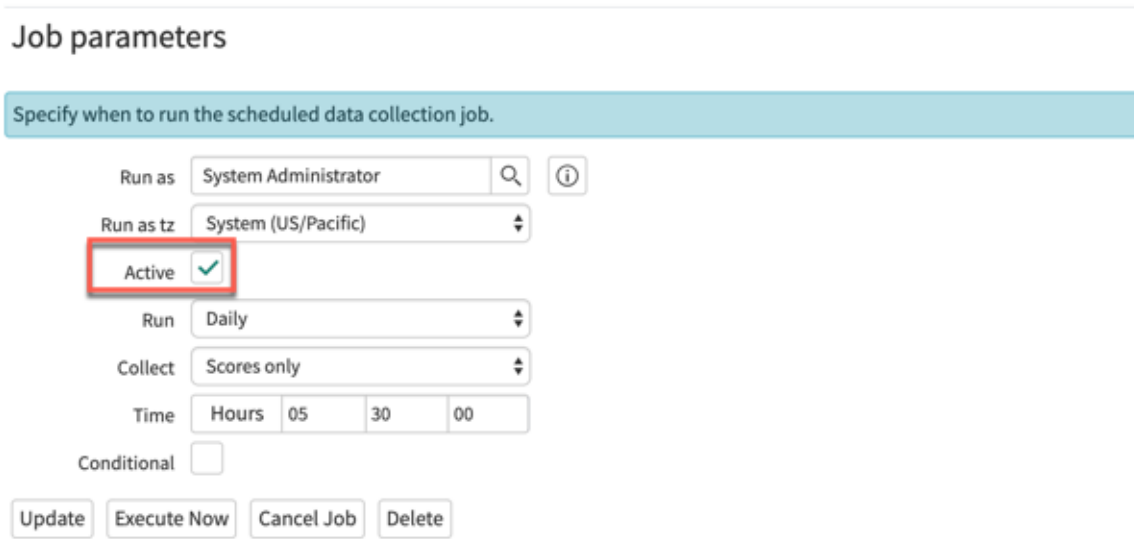
g. Dans la colonne Nom, cliquez sur un lien pour ouvrir un enregistrement de tâche PA_VR.

h. Si les champs ne sont pas modifiables, cliquez sur le lien **ici** pour les modifier.

i. Dans la section Paramètres de la tâche, cochez la case Actif pour planifier une tâche.
Les champs Heure s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



j. Saisissez l'heure de début de la tâche.
Si vous prévoyez un volume important, vous préférerez peut-être définir des heures de collecte en dehors des heures de travail. Si vous prévoyez 10 millions d'EV actifs ou plus dans votre environnement, contactez votre ServiceNow® partenaire d'implémentation pour plus d'informations sur la configuration de votre environnement de collecte de données.

Pour plus d'informations sur les indicateurs utilisés pour la collecte de données, reportez-vous à la section Afficher les Analyse des performances indicateurs pour Réponse aux vulnérabilités [PA].

k. Une fois que vous avez activé toutes les tâches souhaitées, cliquez sur **Mettre à jour**.
La liste Collecte de données planifiée s'affiche. Pour plus d'informations, consultez les propriétés d'Analyse des performances .

Que faire ensuite

Accédez à la **Réponse aux vulnérabilités** > **Vue d'ensemble** pour afficher le tableau de bord.

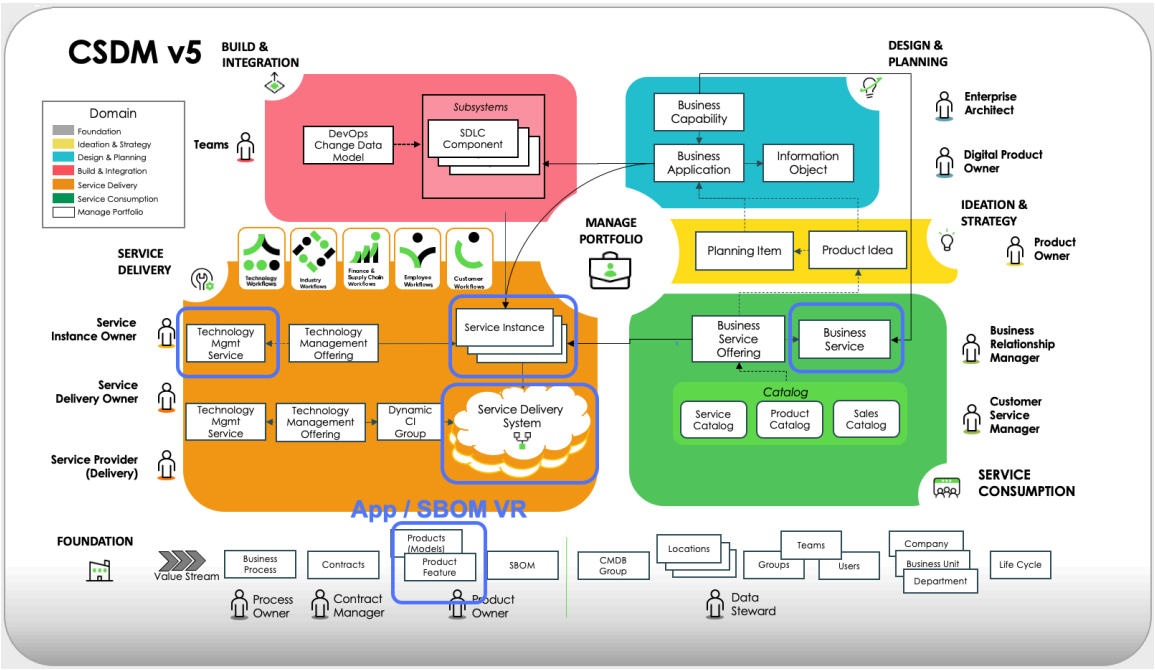
Réponse aux vulnérabilités applications et CSDM tables

Réponse aux vulnérabilités des applications Les Réponse aux vulnérabilités intégrations et Nomenclature logicielle applications de vulnérabilité tierces gèrent les tables (y contribuent des données). CSDM Ces applications utilisent également des données provenant de CSDM tables générées par d'autres applications. Plusieurs ServiceNow produits bénéficient donc de ces Opérations de sécurité applications et y ajoutent de la valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le CSDM cadre de travail et Réponse aux vulnérabilités les applications de données



CSDM Tables référencées par Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, intégrations et Nomenclature logicielle applications de vulnérabilité tierces

À mesure que les actifs sont importés à partir de scanners de vulnérabilité tiers (intégrations), ils sont intégrés Réponse aux vulnérabilités et représentés dans des tables spécifiques :

- Éléments détectés par l'hôte Réponse aux vulnérabilités .
- Images dans le cloud et Réponse aux vulnérabilités pour conteneurs détectées
- Réponse aux vulnérabilités des applications Applications détectées (modèle de produit)

Dans le cadre de la Opérations de sécurité recherche d'élément de configuration (CI) CMDB, une recherche est effectuée pour faire correspondre un enregistrement (CI) des données importées avec les enregistrements existants dans la CMDB.

Chaque enregistrement CI spécifique peut contenir des attributs non détectables, par exemple, Groupe de support ou Classification, qui sont renseignés sur le CI et qui peuvent être utilisés comme entrée pour les règles d'affectation d'éléments vulnérables. Ces attributs peuvent être renseignés à partir de synchronisations CSDM (Common Service Data Model) basées sur les offres de services techniques en amont.

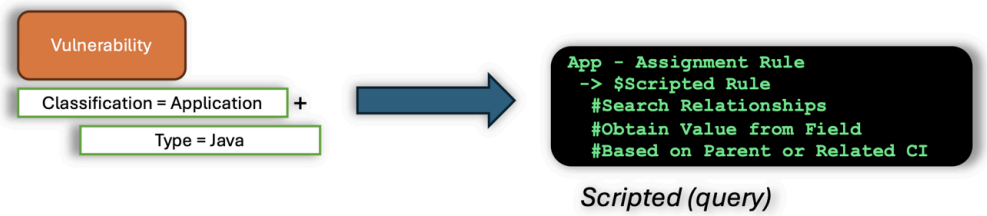
Si vous souhaitez exploiter les objets CSDM associés pour Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, les intégrations de vulnérabilité tierces et Nomenclature logicielle les applications, vous devez utiliser des règles scriptées.

Par exemple, pour affecter automatiquement des éléments vulnérables pour rattrapage à l'aide de règles d'affectation d'éléments vulnérables, vous pouvez créer une règle qui exploite les valeurs de classification des éléments de configuration lorsqu'elles sont mises à jour sur les entrées de vulnérabilité importées. Dans ce cas, vous avez besoin d'une règle scriptée pour interroger la valeur cible souhaitée à partir de l'objet CSDM connexe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous trouverez ci-dessous un exemple de requête scriptée que vous pouvez utiliser pour voir si un CI contient Java et est lié à une entrée de vulnérabilité.



Scripted (query)

Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, les intégrations et Nomenclature logicielle applications de vulnérabilité tierces font référence aux tables suivantes. Pour plus d'informations, reportez-vous à l'image du CSDM cadre de travail des données et Réponse aux vulnérabilités des applications.

- Table Modèle de produit [cmdb_model] (référencée par Réponse aux vulnérabilités des applications et Nomenclature logicielle).
- La table Modèle d'application [cmdb_application_product_model] (référencée par Réponse aux vulnérabilités des applications et Nomenclature logicielle).
- La table Élément de configuration [cmdb_ci].
- Table Service d'entreprise [cmdb_ci_service_business].
- La table Service [cmdb_ci_service].
- Table Groupe CMDB [cmdb_group].
- Table Groupe de CI dynamique [cmdb_ci_query_based_service].

CSDM Tables utilisées par Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, intégrations et Nomenclature logicielle applications de vulnérabilité tierces

1. Table Modèle de produit [cmdb_model] (utilisée par Réponse aux vulnérabilités des applications et Nomenclature logicielle).
2. Table de modèle d'application [cmdb_application_product_model] (utilisée par Réponse aux vulnérabilités des applications et Nomenclature logicielle).
3. La table Élément de configuration [cmdb_ci].
4. Application d'entreprise [cmdb_ci_business_app] (utilisée par Réponse aux vulnérabilités des applications et Nomenclature logicielle).
5. Service d'entreprise [cmdb_ci_service_business].
6. Table Service de gestion des technologies [cmdb_ci_service_technical] (anciennement Service technique).

Remarque :

Lorsque vous chargez Nomenclature logicielle des fichiers, les applications SBOM tentent de faire correspondre les modèles de produits et les applications métier que vous chargez à ceux qui existent déjà dans votre CMDB. Vous pouvez lier des instances de service (anciennement appelées services d'application) ou des applications d'entreprise à un modèle de produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Produits qui apportent une valeur ajoutée aux intégrations et Nomenclature logicielle applications Réponse aux vulnérabilitésRéponse aux vulnérabilités des applications de vulnérabilité tierces

L'utilisation des Réponse aux vulnérabilités applications avec les produits suivants ServiceNow peut être bénéfique pour votre organisation.

Scanners de vulnérabilité tiers et intégrations

Les vulnérabilités importées de la base de données de vulnérabilité nationale (NVD) et les données de détection provenant d'analyseurs tiers sont rapprochées avec les actifs de votre CMDB. Lorsqu'une vulnérabilité importée correspond à un actif existant, un élément vulnérable est créé. Les éléments vulnérables sont automatiquement regroupés en tâches à corriger, notés en fonction du risque en fonction du contexte métier, classés par ordre de priorité et affectés aux équipes appropriées pour la correction. Pour plus d'informations et une liste des intégrations, reportez-vous à Intégrations de Réponse aux vulnérabilités.

Intégrations CWE Comprehensive 2000 et NVD

Les données importées à partir des intégrations NIST National Vulnerability Database (NVD) et Common Weakness Enumeration (CWE) sont utilisées pour enrichir les données de vulnérabilité de votre instance et vous aider à décider s'il faut escalader le rattrapage pour une vulnérabilité, un élément vulnérable ou une tâche de rattrapage. Voir Présentation des intégrations NVD et Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE pour plus d'informations.

Produits qui bénéficient de l'intégration avec Nomenclature logicielle

Contrôle de la posture de sécurité

Contrôle de la posture de sécurité permet aux équipes de cybersécurité d'obtenir une visibilité sur l'ensemble de leur inventaire d'actifs d'entreprise et de déterminer leur posture de sécurité globale. Les politiques peuvent SPC vous aider à détecter les actifs présentant des vulnérabilités que vous importez avec les Réponse aux vulnérabilités applications pour vous aider à localiser les lacunes de couverture des outils de sécurité.

Gouvernance, risque et conformité

Connectez la sécurité et l'informatique à un programme de gestion des risques intégré offrant une surveillance, une hiérarchisation et une automatisation continues.

DevOps

Protégez vos environnements contre les composants potentiellement dangereux pendant les cycles de développement logiciel avec GitHub Actions que vous lancez à partir de votre environnement GitHub. Chargez des ServiceNow AI Platform fichiers SBOM à partir de vos référentiels GitHub.

Créer ou modifier Réponse aux vulnérabilités des règles d'affectation

Une fois que vous avez terminé votre évaluation initiale des règles d'affectation à l'aide de l'Assistant de configuration, vous pouvez créer des règles pour affecter automatiquement des éléments vulnérables en fonction des conditions de filtre. Ces règles affectent des éléments vulnérables à mesure qu'ils sont importés ou créés manuellement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Le système de base est fourni avec une règle d'affectation de vulnérabilité, **Affecter au groupe de support CI**, qui affecte les éléments vulnérables au même groupe d'affectation que le groupe de support CI. Cette règle peut être modifiée à l'aide des conditions de filtre ou vous pouvez créer une nouvelle règle. Les règles d'affectation vous permettent de définir la ou les conditions d'affectation et l'ordre d'exécution. Une fois qu'un VI correspond à une condition de règle, la recherche d'affectation s'arrête.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'affectation**.
2. Ouvrez la règle **Affecter au groupe de support CI** ou cliquez sur **Nouveau**.
3. S'il s'agit **d'un nouveau**, renseignez les champs du formulaire comme il convient.

Règle d'affectation de vulnérabilité

Champ	Description
Nom	Nom de la règle de groupe.
Actif	Indique si la règle d'affectation est active.
Ordre d'exécution	Ordre dans lequel les règles sont évaluées. Les règles de priorité élevée, les éléments qui nécessitent une gestion spéciale, où le risque est critique ou un élément vulnérable doit être géré par la conformité réglementaire, à exécuter en premier. Ensuite, exécutez vos règles générales, où aucune manipulation spéciale n'est requise, et vous savez qui devrait en être responsable. Enfin, créez une règle par défaut pour affecter des VI au groupe qui déterminera à quel groupe d'affectation ils doivent appartenir. Ce groupe pourrait ajouter une autre règle pour couvrir ses décisions. Cette règle par défaut s'exécute en dernier.
Description	Description de la règle d'affectation.
Condition	
Aperçu	Affiche le nombre de résultats renvoyés par cette requête.
Champs de condition	Conditions à remplir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Pour que Rapid7 InsightVM des balises d'actifs puissent être utilisées dans le filtre de condition pour les règles d'affectation, vous devez exécuter l'intégration de la Rapid7 InsightVM liste des actifs avant les autres Rapid7 InsightVM intégrations. La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.
Nouveau critère	Ajoute d'autres champs de filtre de condition à choisir.
Affecter à l'aide de	Pour automatiser l'affectation des groupes créés en fonction de cette règle, choisissez l'une des options disponibles. ◦ Groupe d'utilisateurs : sélectionnez un groupe d'utilisateurs dans la table de recherche. ◦ Champ de groupe d'utilisateurs : sélectionnez un champ de groupe d'utilisateurs dans le menu déroulant. ◦ Script : créez ou modifiez un script. **Remarque :** La création ou la modification d'un script nécessite une ServiceNow expertise.

4. Cliquez sur **Envoyer**.
   Les règles nouvelles ou mises à jour sont évaluées lors de l'importation suivante.

Remarque :

La fonctionnalité de réapplication nécessite une application de base des règles. Une fois vos règles créées, si vous ne l'avez pas déjà fait, activez le *`Reapply all vulnerability assignment rules`* travail planifié pour qu'il s'exécute, à votre convenance. Elle applique toutes les règles à tous les VI ouverts, à l'exception de ceux affectés manuellement. En fonction du nombre de VI actifs que vous avez dans votre environnement, n'oubliez pas de définir le champ **Exécuter** de manière appropriée après l'exécution initiale pour éviter les impacts sur les performances.

Si vous n'avez pas exécuté cette tâche planifiée, lorsque vous essayez d'utiliser le bouton **Appliquer les modifications** sur le formulaire Règles d'affectation, vous devez le faire. La réapplication des règles d'affectation ne regroupe pas les éléments vulnérables.

Créer une règle d'affectation Réponse aux vulnérabilités à l'aide de ML

Utilisez le script suivant pour créer une règle d'affectation de contact de secours pour les éléments vulnérables qui utilise les recommandations ML d'Intelligence prédictive pour les affecter automatiquement à la correction.

Avant de commencer
Les recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités l'application doivent être installées et activées. Cette application est disponible sur le ServiceNow Store.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une solution de classification doit être définie, active et formée. Vous utilisez ce modèle pour vous aider à prédire le groupe d'affectation approprié pour les éléments vulnérables (VI) dans les cas où vos règles d'affectation n'ont pas trouvé de correspondance correcte pour les destinataires prévus.

Cette règle peut vous aider à réduire le nombre de VI non affectés une fois que d'autres règles d'affectation ont déjà été appliquées.

Voir Installer Recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités et Créer et former une définition de solution pour Réponse aux vulnérabilités pour plus d'informations.

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Vous préférerez peut-être effectuer cette tâche uniquement si vous avez une expérience avancée du codage ou si vous avez des connaissances approfondies sur le ServiceNow AI Platform, ses fonctionnalités Predictive Intelligence et le fonctionnement des règles d'affectation.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'affectation**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Consultez la rubrique Créer ou modifier Réponse aux vulnérabilités des règles d'affectation pour plus d'informations sur ces champs.
4. Dans la liste de choix Affecter, sélectionnez **Script**.
5. Dans l'éditeur, copiez et collez le script suivant.

```
  /*
  * Catch-all assignment rule using ML recommendation
  * NOTE: Requires Vulnerability Assignment Recommendations for Vulnerability Response
  * Classification Solution must be active and trained
  */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
  var ARU = new sn_vul.AssignmentRecommendationUtils();
  ARU.initialize();

  var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
  /*
  *returns object containing array of predictions
  *payload structure:
  *
  {
    "predictions": [
      {
        "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
        "name": "Windows Server support ",
        "confidence_score": "57.54"
      },
      ...
    ],
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    "exception": ""
  }
  */
  var viPredictionArray = viPredictionObj['predictions'];
  var topPredictionObj = viPredictionArray.shift();

  return topPredictionObj['sys_id'];
}
```

6. Sélectionnez **Soumettre**.

Que faire ensuite

Consultez pour Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation obtenir des informations plus générales sur les règles d'affectation et la *`Reapply all vulnerability assignment rules`* tâche planifiée.

Créer une règle d'affectation pour l'assistance Réponse aux vulnérabilités de service

Utilisez le script suivant pour créer une règle qui affecte des éléments vulnérables à corriger en fonction des services aux entreprises sur lesquels ils ont un impact.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Vous préférerez peut-être effectuer cette tâche uniquement si vous avez une expérience avancée du codage ou si vous avez une connaissance approfondie du fonctionnement des règles d'affectation ServiceNow AI Platform .

Avec cette règle, les VI sont affectés en fonction de leur pertinence par rapport aux services d'entreprise répertoriés dans votre CMDB. Si aucun service, département ou groupe de support associé n'est apparié, les VI sont affectés au groupe d'analystes de vulnérabilité.

Cette règle peut vous aider à réduire le nombre de VI qui sont incorrectement affectés ou qui ne le sont pas après que d'autres règles d'affectation ont déjà été appliquées.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'affectation**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Consultez la rubrique Créer ou modifier Réponse aux vulnérabilités des règles d'affectation pour plus d'informations sur ces champs.
4. Dans la liste de choix Affecter, sélectionnez **Script**.
5. Dans l'éditeur, copiez et collez le script suivant.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business Service
*/
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
  var ci = vitGR.getValue('cmdb_ci');
  var defaultAssignmentGroup = 'Vulnerability Analyst';
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
  var defaultGR = new GlideRecord('sys_user_group');
  defaultGR.get('name', defaultAssignmentGroup);
  var defaultAssignmentGroupID = defaultGR.sys_id;

  var maxSizeValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_size", 1000);
  var maxDepthValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_depth", 10);
  var customValues = {
     "maxDepth": maxDepthValue,
     "maxSize": maxSizeValue
  };
  var ciu = new global.CIUtils();
  var services = ciu.servicesAffectedByCI(ci, customValues);
  var svc = new GlideRecord("cmdb_ci_service");
  var hasSvc = false;
  if (services && services.length > 0) {
     svc.addQuery("sys_id", "IN", services.join(",")); // returns the service with highest
business criticality. Implement alternate logic here.
     svc.addNotNullQuery("busines_criticality"); // typo intended
     svc.orderBy("busines_criticality");
     svc.setLimit(1);
     svc.query();
     hasSvc = svc.next();
  }
  if (!hasSvc) {
     // If there are no services it should be assigned to a default assignent group
     return defaultAssignmentGroupID;
  } else {
     var serviceAssignmentGroup = hasSvc.getValue('support_group'); //Also consider
managed_by_group, assignment_group, change_control
     return !gs.nil(serviceAssignmentGroup) ? serviceAssignmentGroup :
defaultAssignmentGroupID; //Return the Service assignment group if it is not empty, return
the default assignment group otherwise.
  }
}
```

6. Sélectionnez **Soumettre**.

Que faire ensuite

Consultez pour Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation obtenir des informations plus générales sur les règles d'affectation et la *`Reapply all vulnerability assignment rules`* tâche planifiée.

Créer ou modifier des Réponse aux vulnérabilités règles de tâche de rattrapage

Une fois que vous avez terminé votre évaluation initiale des règles de tâche de rattrapage à l'aide de l'Assistant de configuration, vous pouvez créer des règles pour regrouper automatiquement les éléments vulnérables en fonction des conditions de filtre. Ces règles regroupent automatiquement les éléments vulnérables à mesure qu'ils sont importés ou créés manuellement. Utilisez le filtre pour limiter les éléments vulnérables regroupés par cette règle, comme la sélection de tous les éléments vulnérables avec des exploits.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Le système de base est fourni avec une règle de tâche de rattrapage, **Vulnérabilité**, qui regroupe les éléments vulnérables par vulnérabilité et groupe d'affectation (à partir des **règles d'affectation**). Vous pouvez réappliquer les règles à partir de la vue de formulaire ou de liste. Pour quelques exemples d'entrées, Réponse aux vulnérabilités Exemples de règles de tâches de rattrapage.

Cette règle peut être modifiée comme suit :

En utilisant des conditions de filtre et Grouper par choix.

Par défaut, les tâches de rattrapage utilisent des **règles d'affectation**, lorsqu'elles sont disponibles, dans le cadre de leurs critères de filtre.

Remarque : S'il n'existe aucune règle d'affectation, vous pouvez sélectionner un groupe à l'aide du champ **Groupe d'utilisateurs** .

À partir de la version 18.0 de , la règle de la tâche de rattrapage de Réponse aux vulnérabilités**vulnérabilité** est désactivée dans Réponse aux vulnérabilités pour les nouvelles implémentations.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles de la tâche de rattrapage**.
2. Ouvrez la règle ou cliquez sur **Nouveau**.
3. S'il s'agit **d'un nouveau**, renseignez les champs du formulaire comme il convient.

Règle de la tâche de rattrapage

Champ	Description
Nom	Nom de la règle de tâche.
Actif	Indique si la tâche est active.
Description	Description de la règle.
Sensible à la casse	Détermine si une condition est sensible à la casse ou non. **Remarque :** La valeur par défaut est insensible à la casse.
Condition	Conditions de filtre facultatives pour la règle. **Remarque :** Pour que Rapid7 InsightVM des balises d'actifs puissent être utilisées dans le filtre de condition pour les règles de tâche de rattrapage, vous devez exécuter l'intégration de la Rapid7 InsightVM liste des actifs avant les autres Rapid7 InsightVM intégrations. Par défaut (case **sensible** à la casse désactivée), le texte de recherche que vous saisissez dans le générateur de conditions sur les enregistrements de règles de tâches et les formulaires n'est pas sensible à la casse. Vous pouvez activer les recherches sensibles à la casse sur les enregistrements de tâches et les formulaires.
Grouper par (jusqu'à six ensembles de conditions sont disponibles)	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Regrouper les éléments vulnérables à partir de	La table que la règle utilise pour regrouper les VI. Vous pouvez avoir jusqu'à six filtres. Les choix possibles sont les suivants : ○ Élément vulnérable [sn_vul_vulnerable_item] ○ Élément vulnérable → Élément de configuration [cmdb_ci] ○ Élément vulnérable → Vulnérabilité [sn_vul_third_party_entry] **Remarque :** Si vous choisissez une table étendue, le **champ Utilisation** n'est appliqué qu'aux éléments vulnérables qui utilisent cette table étendue.
Utilisation du champ	Champ de la table que la règle utilise pour regrouper les VI.
Affectation	
Affecter la tâche de rattrapage par	Lors de l'affectation automatique des tâches de rattrapage, le choix Affectation est utilisé en plus des choix **Grouper par** pour regrouper les éléments vulnérables. De nouvelles tâches sont créées, selon les besoins, pour s'assurer que chaque élément vulnérable est placé dans une tâche avec un groupe d'affectation correspondant défini. Pour automatiser l'affectation des tâches créées en fonction de cette règle, choisissez l'une des options disponibles. ○ Regrouper par champ : si vous avez sélectionné un champ de groupe d'utilisateurs dans les valeurs **de champ Utilisation** de la section **Grouper par**, elles apparaissent dans le menu déroulant. ○ Groupe d'utilisateurs : utilisez la liste de recherche pour sélectionner un groupe d'utilisateurs statique.

Remarque : Si vous changez d'avis sur l'un des paramètres **Grouper par** , le lien connexe **Effacer le regroupement par champs** réinitialise les champs **Grouper par** sur le formulaire.

Lorsqu'une règle de groupe est supprimée, à partir de la vue de formulaire ou de liste, vous pouvez supprimer tous les groupes **ouverts** créés par cette règle. Les groupes dont l'état n'est pas **Ouvert** sont exclus.

Pour quelques exemples d'entrées, reportez-vous à la section Réponse aux vulnérabilités Exemples de règles de tâches de rattrapage.

Définir les champs et les poids de la règle de risque pour les calculateurs de risque de Vulnerability Response

Personnalisez les paramètres et les pondérations de la règle de risque afin de pouvoir générer des scores de risque qui utilisent les données de vulnérabilité et d'actif propres à votre organisation. En sélectionnant les champs qui sont inclus dans la règle de risque, vous pouvez définir un cadre de travail de notation des risques efficace.

Avant de commencer

En outre, vous pouvez utiliser des attributs dans le configuration_item [cmdb_ci] dans la Base de données de gestion des configurations (CMDB) pour vous aider à créer une logique pour vos calculateurs de risque de Vulnerability Response. Si, par exemple, vous déterminez que les CI orientés vers l'extérieur de votre organisation sont plus vulnérables et peuvent nécessiter une correction immédiate, vous pouvez affecter des attributs tels que

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Internet Facing pour ces CI. Cet attribut, ainsi que d'autres, sont répertoriés dans les notes de version de Common Service Data Model pour la version de la famille Orlando. Pour obtenir des renseignements et des conseils à jour sur le CMDB, consultez les rubriques suivantes :

- Modèle conceptuel du modèle de données de service commun
- Modèle de schéma CMDB

Rôle requis : sn_vul.manage_risk_score_configuration

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Calculateurs de vulnérabilités**.
2. Sur la page Calculateurs de vulnérabilité, sélectionnez **Calculateur de risque par défaut**.
3. Accédez à la **Page Calculateur de vulnérabilité** > **Onglet Règles du calculateur de vulnérabilité** > **Règle sur les risques par défaut**.
4. **Facultatif :** Dans la section Critères du calculateur de risque de la page Règle de risque de vulnérabilité, définissez le poids de chaque critère en fonction de son importance dans le calcul du score de risque global.
5. Pour désactiver la règle, vous devez décocher la case **Actif** .
6. Pour ajouter des champs de règles de risque aux critères du calculateur de risque, sélectionnez **Ajouter des critères**.
7. Remplissez les champs du formulaire.

Formulaire de champ de règle de risque

Champ	Description
Choisir la table de référence	Table que vous utilisez pour définir la pondération du score de risque. Vous pouvez sélectionner l'une des options suivantes : ○ **Élément vulnérable** : ajoutez des champs qui peuvent être remontés pas à pas à partir de l'élément vulnérable (VI). ○ **Élément vulnérable : élément de configuration** : ajoutez des champs parcourables par point qui font partie des extensions de table de base, telles que la table Matériel. Ces champs ne font pas partie de la table de base (cmdb_ci). ○ **Élément vulnérable : vulnérabilité** : ajoutez des champs parcourables par point qui font partie des tables qui étendent la table de base, par exemple, Entrée tierce. Ces champs ne font pas partie de la table de base Entrée de vulnérabilité. ○ **Table de référence de l'élément vulnérable** : ajoutez des champs qui font partie des tables connexes (m2m)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ou des tables qui font référence à l'élément vulnérable. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du VI. ○ **Table de référence d'élément de configuration** : ajoutez des champs qui font partie des tables connexes (m2m) de cmdb_ci ou des tables qui ont une référence à cmdb_ci. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du VI. ○ **Table de référence de vulnérabilité** : ajoutez des champs qui font partie des tables connexes (m2m) des sn_vul_entry ou des tables qui ont une référence à sn_vul_entry. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du VI. ○ **Conditions personnalisées** : utilisez cette option pour affecter des poids à la règle en évaluant la condition. Par exemple, le filtre orienté vers Internet détermine si un élément de configuration (CI) est externe ou interne.
Table	Champ qui s'affiche uniquement lorsque l'une des options suivantes est sélectionnée dans la table Choisir une référence : ○ **Élément vulnérable -> Élément de configuration** ○ **Élément vulnérable -> Vulnérabilité** ○ **Table de référence de l'élément vulnérable** ○ **Table de référence de l'élément de configuration** ○ **Table de référence de vulnérabilité**
Champ	Champ à utiliser pour le calcul du score de risque pour cette règle.
Agrégation	Champ qui s'affiche uniquement lorsqu'une table de référence est sélectionnée dans la table Choisir une référence. Sélectionnez la valeur minimale ou maximale à prendre en compte pour les calculs lorsque le champ est sélectionné dans les tables connexes (m2m).
Pondération	Pondération de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
Définir la pondération de la valeur	Composant permettant d'attribuer des poids à chaque valeur de champ. Pour les champs numériques, les valeurs de champ peuvent être

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	définies comme une plage (par exemple, 1 à 5). Les pondérations doivent être un nombre entier compris entre 0 et 100. **Remarque :** Ce champ n'apparaît pas si l'option Conditions personnalisées est sélectionnée dans la table Choisir la référence.
Table de condition	Champ qui s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans la table Choisir la référence. Sélectionnez une condition dans la liste.
Nom de champ	Champ qui s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans la table Choisir la référence. Entrez un nom pour les critères de risque.
Condition	Champ qui s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans la table Choisir la référence. Prévisualisez les éléments de cette table qui correspondent aux conditions définies.

8. Sélectionnez **Soumettre**.
9. Sur la page Règle, activez et réappliquez la règle pour réévaluer le score de risque des éléments vulnérables actifs.

Remarque : À partir de la version 23.0 de Réponse aux vulnérabilités, dans le cas de :

- **Règle du calculateur de risque par défaut** : chaque fois que le score de risque d'un élément vulnérable (VIT) change, les détails suivants sont documentés dans la section Notes du VIT :
  - Nom du groupe de calculateurs
  - Nom du calculateur
  - Valeurs de champ dont la pondération est supérieure à 1 et dont la contribution au score de risque est supérieure à 1.
  - Score de risque final
- **Règle de risque de gravité** de la vulnérabilité : chaque fois que le score de risque est mis à jour sur un VIT, la section **Notes** est mise à jour avec les détails suivants :
  - Nom du groupe de calculateurs
  - Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre crochets. Pour modifier ou afficher la base de la règle du calculateur, sélectionnez une règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. **Si Modèle** est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si **Script** est sélectionné, vous pouvez ajouter ou mettre à jour le script existant.

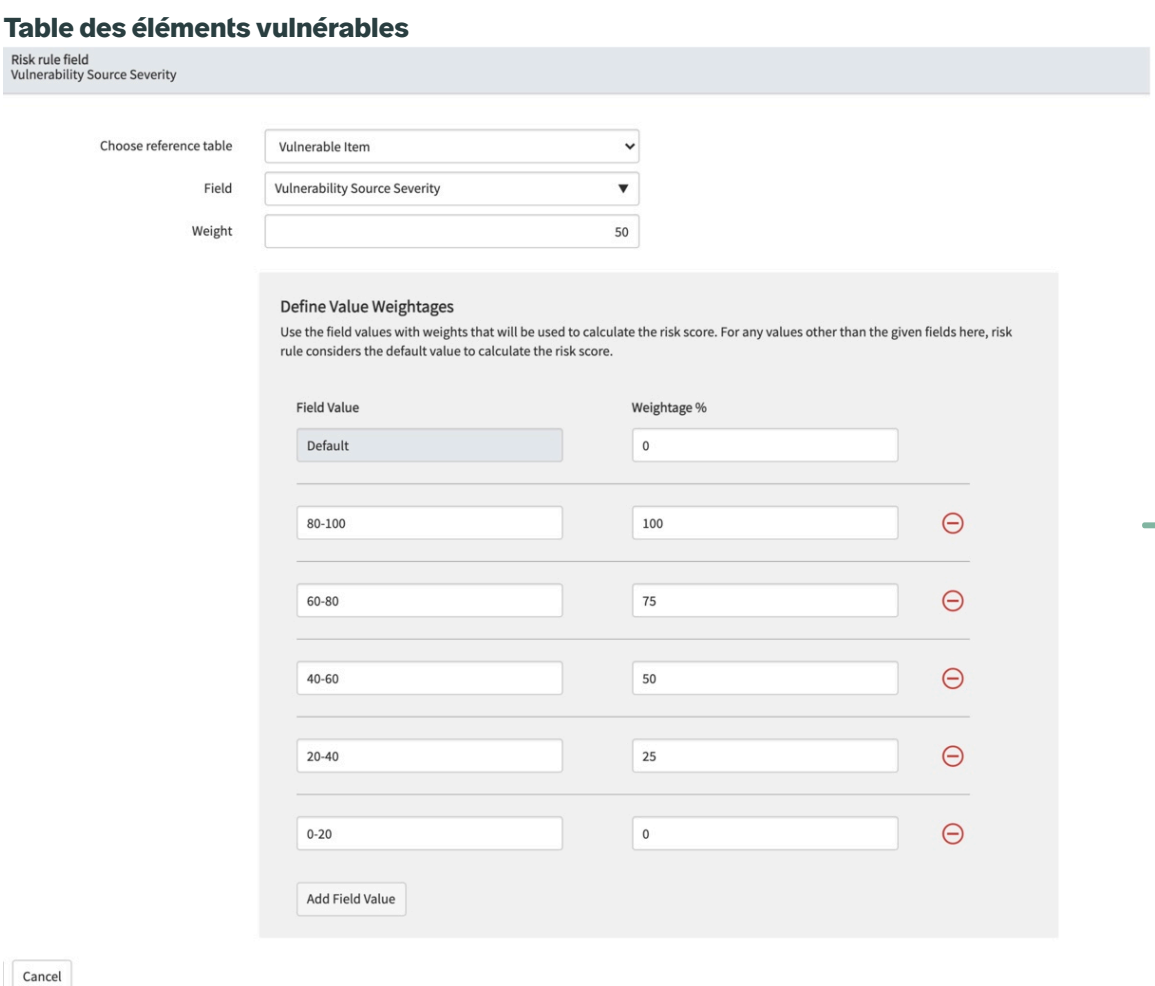
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example:
Exemple 1 : Ajouter une gravité de la source comme critère pour une règle de risque.

Cas d'utilisation : les fournisseurs tiers, comme Qualys et Tenable, fournissent leurs propres scores. Ces scores sont renseignés dans le champ Gravité de la **source** de la table sn_vul_entry. Utilisez ce champ pour les calculs de score de risque. Pour utiliser ce score afin de calculer le score de risque, procédez comme suit :

1. Accédez à la page Règle de risque.
2. Pour désactiver la règle, décochez la case **Actif** .
3. Pour ajouter des champs de règles de risque aux critères du calculateur de risque, sélectionnez **Ajouter des critères**.
4. Dans la liste Choisir la table de référence, sélectionnez **Élément vulnérable**.
5. Dans la liste Champ, sélectionnez **Vulnérabilité.Gravité de la source**.
6. Dans le champ **Poids** , entrez l'importance relative de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
7. Dans la section Définir la pondération de la valeur, ajoutez des valeurs de champ et attribuez-leur une pondération.



8. Sélectionnez **Soumettre**.

Exemple 2 : Ajouter une criticité opérationnelle comme critère pour une règle de risque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation : supposons que votre organisation dispose de nombreux services aux entreprises. L'élément de configuration (CI) LINUX-SF-6381 est utilisé par les services suivants :

Criticité des services aux entreprises

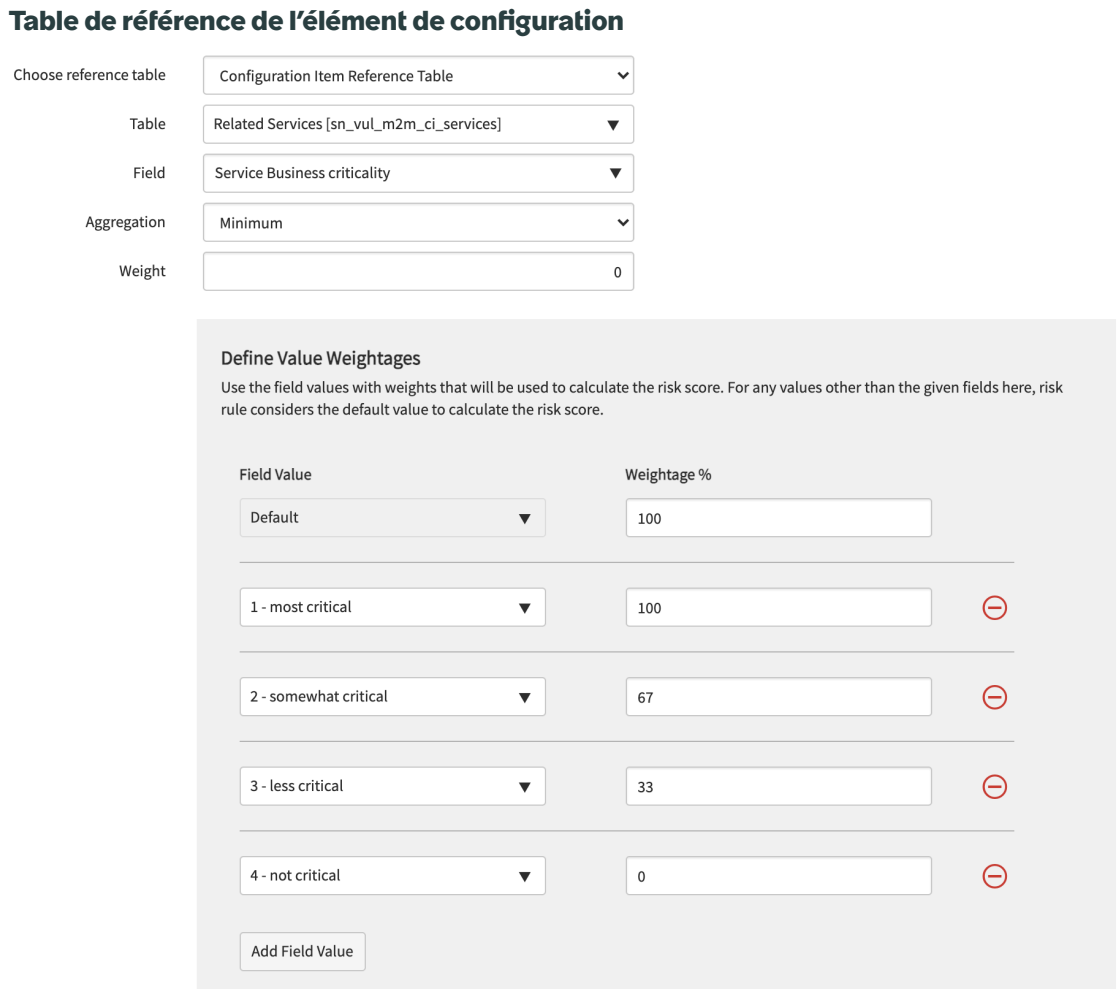
Service d'entreprise	Criticité
Gestion cloud	1 – Très critique
Commerce électronique	2 – Assez critique
Services aux clients	3 – Peu critique
Déplacements et dépenses	4 – Non critique

Le mappage entre le CI et les services est stocké dans la table Services associés [sn_vul_m2m_ci_services]. Lorsqu'une vulnérabilité est détectée dans l'actif LINUX-SF-6381, un élément vulnérable (VI) est créé. Vous pouvez utiliser la valeur de la criticité opérationnelle des services affectés pour calculer le score de risque pour ce VI. Pour utiliser la valeur de criticité de ces services pour calculer le score de risque, procédez comme suit :

1. Accédez à la page Règle de risque.
2. Pour désactiver la règle, décochez la case **Actif** .
3. Pour ajouter des champs de règles de risque aux critères du calculateur de risque, sélectionnez **Ajouter des critères**.
4. Dans la liste Choisir la table de référence, sélectionnez **Table de référence de l'élément de configuration**.
5. Dans la liste Table, sélectionnez **Services associés [sn_vul_m2m_ci_services].**
6. Dans la liste Champ, sélectionnez **Service.Criticité opérationnelle**.
7. Dans le champ **Agrégation** , sélectionnez **Minimum** pour récupérer le service le plus critique pour ce cas d'utilisation (**1 : valeur la plus critique**) ou Maximum pour récupérer le service le moins critique pour ce cas d'utilisation (**4 – Valeur non critique**) pour ce cas d'utilisation.
8. Dans le champ **Poids** , entrez l'importance relative de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
9. Dans la section Définir les pondérations des valeurs, ajoutez des valeurs de champ et attribuez-leur un poids.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Sélectionnez **Soumettre**.

Exemple 3 : Ajouter un critère conditionnel au calculateur de risque.

Supposons qu'une organisation dispose de plusieurs éléments de configuration (CI), dont seuls quelques-uns peuvent être consultés par un utilisateur externe. Les utilisateurs peuvent ajouter des pondérations de score de risque pour ces CI orientés vers l'extérieur.

Remarque : Vous pouvez identifier ces CI par leur nom. Les noms commencent par « externe ».

Pour ajouter un critère conditionnel à la règle de risque, procédez comme suit :

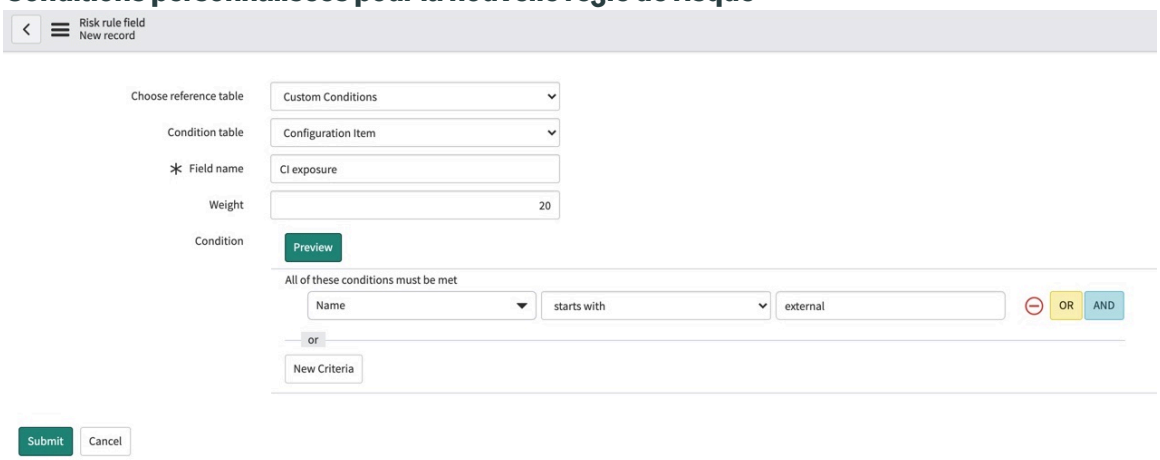
1. Accédez à la page Règle de risque.
2. Pour désactiver la règle, décochez la case **Actif** .
3. Pour ajouter des champs de règles de risque aux critères du calculateur de risque, sélectionnez **Ajouter des critères**.
4. Dans la liste Choisir la table de référence, sélectionnez **Conditions personnalisées**.
5. Dans la liste Table de condition, sélectionnez **Élément de configuration**.
6. Dans le champ **Nom du champ** , entrez le nom **Exposition CI**.
7. Dans le champ **Poids** , entrez l'importance relative de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Dans le champ **Condition** , sélectionnez **Nom** > **commence par** et entrez la valeur **externe**.

Conditions personnalisées pour la nouvelle règle de risque



9. Sélectionnez **Soumettre**.

Remarque : L'ajout de critères conditionnels à votre règle de risque peut dégrader les performances.

Information associée

Calculateurs de Vulnerability Response et règles du calculateur de vulnérabilité

Créer un calculateur de Vulnerability Response

Filtrage dans Vulnerability Response

Réponse aux vulnérabilités Calculateurs de cumul

Après votre évaluation initiale des calculateurs de risque dans l'assistant de configuration, utilisez les calculateurs de déploiement de vulnérabilité pour configurer le mode de calcul du score de risque cumulé pour les tâches de rattrapage et les vulnérabilités importées.

Utilisez les calculateurs de déploiement de vulnérabilité pour configurer le mode de calcul du score de risque cumulatif pour les tâches de rattrapage et les vulnérabilités importées. Les calculateurs de déploiement suivants sont fournis avec le système de base :

- *`Remediation Task Rollup`*: cumule les scores de risque pour tous les éléments vulnérables dans une tâche de correction afin de fournir un score de risque global pour l'ensemble du groupe d'éléments vulnérables.
- *`Patch Update Rollup`*: regroupe les scores de risque pour tous les éléments vulnérables avec la même mise à jour de correctif afin de fournir un score de risque global pour la mise à jour du correctif.
- *`Organization Risk Score Rollup`*: cumule les scores de risque pour tous les éléments vulnérables d'hôte, d'application, de conteneur et de configuration dans une organisation afin de fournir un score de risque global pour l'ensemble de l'organisation dans le tableau de bord unifié.

Remarque : À partir de la version 22.0 de Réponse aux vulnérabilités, vous pouvez configurer les poids de cumul pour le score organisationnel. De plus, les calculateurs de cumul individuels ont été supprimés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *Vulnerable Item Rollup*: cumule les scores de risque pour tous les éléments vulnérables de l'hôte dans une organisation afin de contribuer au score de risque global de l'organisation pour le tableau de bord unifié.
- *Vulnerability Entry Rollup*: cumule les scores de risque pour tous les éléments vulnérables dans la même entrée de vulnérabilité afin de fournir un score de risque global pour l'entrée de vulnérabilité.
- *Rollup EPSS Scores from NVD to TPEs*: cumule les scores EPSS de tous les éléments vulnérables/CVE répertoriés dans la table NVD sur les TPE existants, afin de fournir une probabilité globale d'exploitation de la vulnérabilité.
- *Remediation Effort Rollup*: regroupe les scores de risque pour tous les enregistrements dans le cadre d'un effort de correction afin de fournir un score de risque global de l'effort de rattrapage.

Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Calculateur de déploiement de vulnérabilité**.

Configurez le calculateur de déploiement pour spécifier le poids à donner à chacune de ces valeurs calculées dans la définition du score de risque cumulatif. Plus le poids est élevé, plus cette valeur est utilisée pour déterminer le score de risque déployé dans les tâches de vulnérabilité ou de rattrapage.

Remarque : Lorsque **l'option Inclure les éléments différés** est sélectionnée, tous les éléments vulnérables différés sont inclus dans le calcul de déploiement pour les tâches de rattrapage. Assurez-vous de bien comprendre l'impact sur le calcul du total avant de sélectionner cette option.

Les calculateurs de déploiement exécutent la tâche planifiée, *Rollup vulnerable item values to vulnerability and groups*, toutes les 15 minutes pour détecter les changements et déployer les détails et les scores de risque sur les tâches de rattrapage et les vulnérabilités. Ces travaux planifiés calculent également les valeurs cumulatives pour le nombre de VI, le score de risque maximal, la date cible de rattrapage et l'état des tâches de rattrapage.

Remarque : Les valeurs calculées pour les entrées de vulnérabilité n'incluent pas les données cibles de rattrapage.

Le score de risque est calculé quand :

- Le score de risque, la cible de rattrapage, l'état du rattrapage ou les changements de vulnérabilité des éléments vulnérables.
- L'état de l'élément vulnérable passe à Ouvert, Différé, Fermé ou passe de Fermé à Différé.
- Les éléments vulnérables sont supprimés.
- Les éléments vulnérables sont ajoutés ou supprimés de la tâche de rattrapage.

Exemple de calculateur de déploiement de vulnérabilité : Considérez une tâche de rattrapage VUL324567, qui comporte les éléments vulnérables suivants :

- VIT1001 avec un score de risque de 30
- VIT1002 avec un score de risque de 40
- VIT1003 avec un score de risque de 50

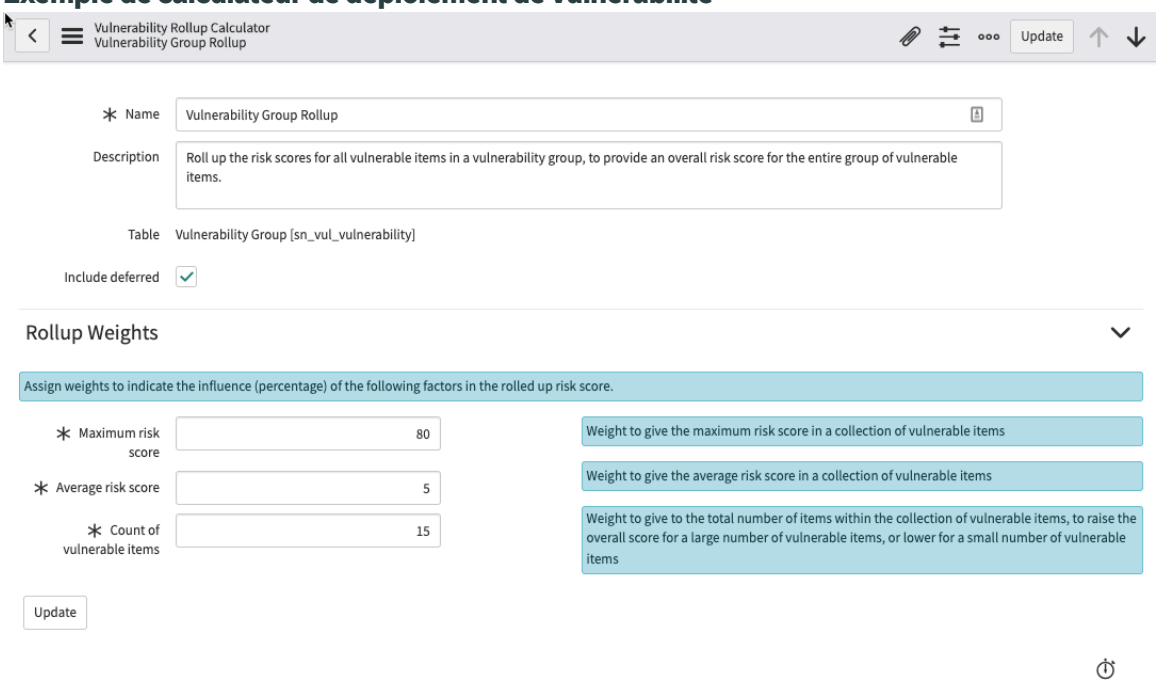
Prenez également en compte les pondérations suivantes dans le calculateur de déploiement de vulnérabilité :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Score de risque maximal : 80
- Score de risque moyen : 5
- Nombre d'éléments vulnérables : 15

Exemple de calculateur de déploiement de vulnérabilité



Dans l'exemple du calculateur de déploiement de vulnérabilité, la formule pour déterminer le **score de risque** de la tâche de rattrapage est la suivante :

(**score de risque maximal**/100) * 80 + (**score de risque moyen** /100) * 5 + (facteur * 15)

Le facteur est déterminé comme suit :

Nombre VI	Facteur
<10	0,2
10-100	0,4
101-1000	0,6
1001-10000	0,8
> 10000	1

Donc, pour la tâche de rattrapage, VUL324567 :

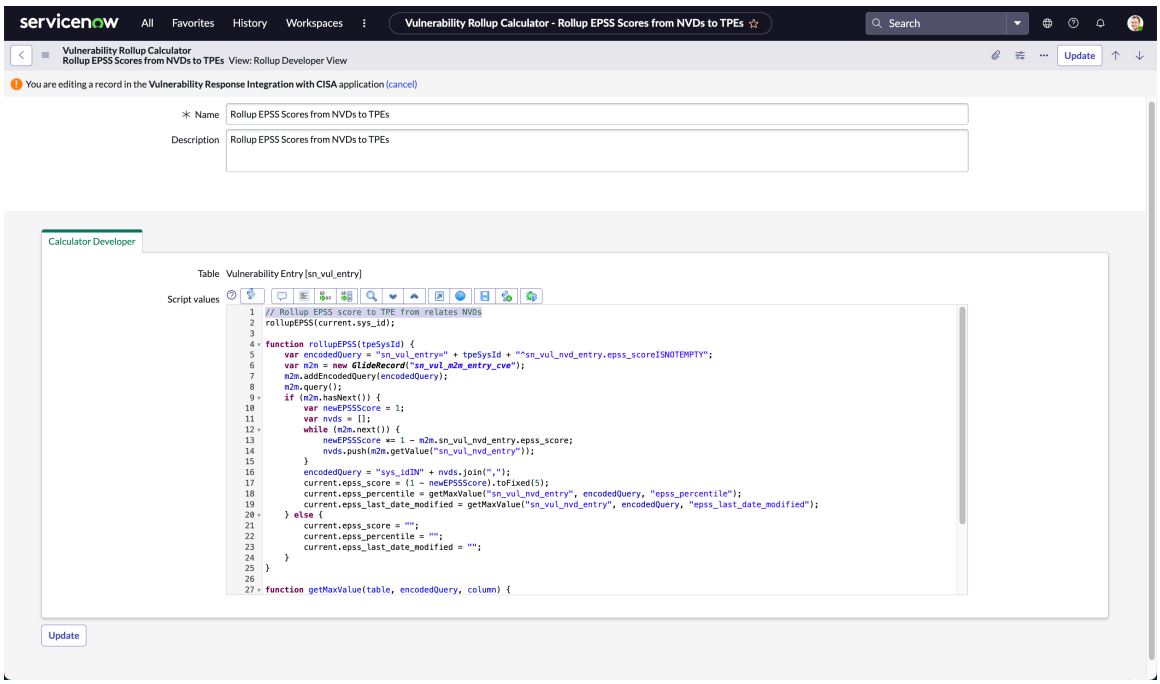
- Le score de risque moyen est de 40
- Le score de risque maximal est de 50
- 50 (score du risque maximal)
- Le facteur est de 0,2

Le **score de risque** serait de 45 [(50/100) * 80 + (40/100) * 5 + 0,2 * 15 = 40 + 2 + 3 = 45]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cumul des scores de l'EPSS des NVD aux TPE



Calculateur de déploiement de l'EPSS : exemple

Prenons l'exemple d'une organisation qui compte 100 vulnérabilités, chacune ayant 5 % de chances d'être exploitée. La question qui intéresse beaucoup un défenseur de réseau pourrait être la suivante : quelle est la probabilité qu'au moins une de ces vulnérabilités soit exploitée, et donc quelle est ma menace globale ? La probabilité qu'au moins un événement se produise est simplement le complément (opposé) de l'absence d'événements, c'est-à-dire :

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are exploited)
```

Où la probabilité qu'aucune vulnérabilité ne soit exploitée est le produit linéaire de chaque vulnérabilité non exploitée. Dans cet exemple, puisque chaque vulnérabilité a 5 % de chances d'être exploitée, elles ont chacune 95 % de chances de ne pas l'être. Et comme il y en a 100, nous pouvons écrire ceci comme suit :

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 - P(one vuln not
 exploited)^100 = 1 - 0.95^100 = 0.994
```

Ce qui signifie que la probabilité qu'au moins une des vulnérabilités soit exploitée est de 99,4 %.

Important : Pour modifier le *`Rollup EPSS Scores from NVD to TPEs`*, vous devez basculer la vue du menu contextuel du formulaire vers la **vue Développeur de déploiement** à partir de la **vue Par défaut**.

Créer ou modifier Réponse aux vulnérabilités des règles de cibles de rattrapage

Après l'évaluation initiale des règles de cibles de rattrapage dans l'Assistant de configuration, les gestionnaires de vulnérabilité peuvent configurer une règle de cible de rattrapage au niveau de l'élément vulnérable pour piloter la correction des vulnérabilités à haut risque en temps opportun. Lorsque la date de rattrapage d'un élément vulnérable approche, une notification est envoyée aux utilisateurs ou groupes spécifiés dans la règle.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles de cibles de remédiation**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom de la règle.
Cible (jours)	Spécifiez le nombre de jours pendant lesquels les éléments vulnérables doivent être corrigés, depuis leur dernière ouverture.
V17.1 : (date) de la cible	Date à partir de laquelle les SLA cibles sont calculés. Vous pouvez spécifier uniquement les champs de date ou le type de date et d'heure. La valeur par défaut est Dernière date d'ouverture. Pour personnaliser les valeurs de ce champ, consultez KB1642413 .
Actif	Par défaut, la case **Actif** est cochée, ce qui signifie que la règle de cible de rattrapage est active. Si cette case n'est pas cochée, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Notifier (jours avant l'échéance)	Nombre de jours avant le délai de rattrapage ciblé pour l'envoi d'une notification. La date de notification calculée à l'aide de cette valeur est utilisée pour afficher l'état du rattrapage et le code couleur. Si la date est antérieure à la date de notification, l'état du rattrapage est « En cours ». S'il a dépassé la date de notification et est antérieur à la date cible de rattrapage, l'état indique que la cible approche. **Remarque :** Si ce champ est défini sur 0, seule une notification **de cible manquée** est envoyée.
Description	Texte décrivant la règle de cible de rattrapage.
Condition	À l'aide du filtre de condition, sélectionnez les critères d'application de la règle aux éléments vulnérables. Pour éviter l'impact sur les performances, testez vos conditions à l'échelle de la production. Les tests vous permettent de déterminer la durée d'exécution de la tâche **Évaluer les cibles de rattrapage** , compte tenu des conditions et de la taille de votre Base de données de gestion des configurations (CMDB). La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.
Notifications	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Remarque : Le nombre indiqué dans l'e-mail de notification n'inclut pas les éléments vulnérables à l'état **Différé**, **Résolu** ou **Fermé** .	
Utilisateurs	Personnes à notifier lorsque l'élément vulnérable sélectionné approche ou dépasse l'heure cible de rattrapage prévue.
Groupe	Groupe à notifier quand l'élément vulnérable sélectionné approche ou dépasse l'heure cible de rattrapage prévue.
Historique des mises à jour	
	Non utilisé lors de la création initiale d'une règle. Ensuite, les notes de travail du système sont consignées ici.

4. Cliquez sur **Envoyer**.
   Cette règle entre en vigueur lors de la prochaine exécution du travail *`Evaluate remediation targets`* planifié ou lors de l'utilisation du bouton **Appliquer les changements** dans la vue de liste Règles de cibles de rattrapage. Il en va de même lorsqu'une règle existante est mise à jour. Pour plus d'informations sur la tâche planifiée et sur **l'application des changements**, reportez-vous à la section Réponse aux vulnérabilités Règles de cibles de rattrapage.

Configurer les intégrations tierces installées à l'aide de l'assistant de configuration

Configurez Vulnerability Response pour qu'elle fonctionne avec chacun de vos déploiements d'applications tierces installées.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration**.
2. Sélectionnez **Intégrations de scanners pour configurer les déploiements** d'applications tierces installées.
3. S'il Gestion des solutions pour Réponse aux vulnérabilités est installé, vous pouvez sélectionner **Intégrations de solutions** pour configurer vos fournisseurs de solutions de vulnérabilité.

Configurer les intégrations de solutions installées pour Gestion des solutions pour vulnérabilités l'utilisation de l'assistant de configuration

Après avoir installé l'application Gestion des solutions de vulnérabilité, vous pouvez configurer vos fournisseurs de solutions de vulnérabilité à l'aide de l'Assistant de configuration.

Avant de commencer

Rôles requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou admin

Utilisez les sections suivantes pour compléter les instructions et les invites fournies dans l'Assistant de configuration pour les intégrations de solutions installées pour Gestion des solutions pour Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifiez que vous avez déjà installé Gestion des solutions pour vulnérabilités les solutions et les intégrations de solutions souhaitées avant de commencer. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.
- Vérifiez que vous disposez d'informations d'identification de compte tiers. Ils sont nécessaires pour modifier certaines intégrations de solutions.
- Reportez-vous à la section Installer l'application Gestion des solutions pour Réponse aux vulnérabilités pour plus d'informations avant de configurer les solutions installées.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions**.

   L'opération Microsoft Security Response Center Solution Integration nécessite une clé API et une URL de la Microsoft Security Response Center part de pour la configurer.

   Remarque : La saisie de la clé API est facultative pour MSRC. Pour obtenir la MSRC clé, vous devez disposer d'un ID Microsoft provenant d'un compte de messagerie live.com, outlook.com ou Microsoft.com, d'un numéro de téléphone enregistré auprès de Microsoft ou d'un identifiant Skype.

2. Entrez l'URL.
   L'URL dans l'Assistant de configuration pour MSRC est https://api.msrc.microsoft.com.
3. Cliquez sur **Terminer**.
4. **Facultatif :** Vous pouvez exécuter des importations à la demande en cliquant sur **Exécuter maintenant** sur la page de configuration après avoir entré vos informations d'identification.
5. Le Intégration de solution Red Hat est également disponible.
   Il ne nécessite pas de clé API.
6. Dans l'Assistant de configuration, à droite du Intégration de solution Red Hat, cliquez sur **Modifier**.
7. Vérifier l'URL dans l'Assistant de configuration pour RHSI est https://access.redhat.com/hydra/rest
8. **Facultatif :** Vous pouvez exécuter des importations sur demande en cliquant sur **Exécuter maintenant** sur la page de configuration.
9. Cliquez sur **Terminer,** puis sur **Marquer comme terminé** pour terminer la configuration.
   Une coche s'affiche dans l'assistant de configuration pour les intégrations de solutions lorsque vous avez terminé la configuration.

Configurer l'intégration de vulnérabilité MS TVM à l'aide de l'assistant de configuration

Configurez l'intégration avec l'application Réponse aux vulnérabilités Gestion des menaces et des vulnérabilités Microsoft (MS TVM) après l'avoir installée à l'aide de l'Assistant de configuration.

Avant de commencer

En plus des instructions et des invites fournies dans l'Assistant de configuration pour l'intégration à l'intégration Réponse aux vulnérabilités Microsoft Threat and Vulnerability Management, effectuez les actions suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifiez que vous avez déjà installé l'application avant de commencer. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.
- Consultez la section Préparation à l'intégration des vulnérabilités Microsoft Threat and Vulnerability Management pour plus d'informations avant de configurer l'intégration Microsoft Threat and Vulnerability Management pour Réponse aux vulnérabilités.
- Vérifiez que vous disposez des informations d'identification du compte MS TVM. Pour obtenir ces informations d'identification, reportez-vous à la section Configurer Azure pour l'intégration Microsoft MS TVM.

Rôles requis : administrateur système (admin) pour l'installation, administrateur de vulnérabilité (sn_vul.vulnerability_admin) ou sn_vul.admin (obsolète) et Configurer l'intégration (sn_vul_msft_tvm.configure_integration) pour la configuration

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.

   La vignette Microsoft Threat & Vulnerability Management s'affiche.

   MS TVM est une intégration multisources, ce qui signifie que vous pouvez avoir plusieurs déploiements de la même intégration tierce. Les paramètres de votre intégration tierce d'origine servent de modèle pour les paramètres de chaque nouvelle intégration.

   Remarque : Si vous supprimez l'intégration de vulnérabilité d'origine, vous devez sélectionner une autre intégration à utiliser comme modèle. Envisagez de désactiver l'intégration au lieu de la supprimer. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

   Les données de chaque intégration tierce sont identifiées de manière unique et disponibles dans une seule instance de Réponse aux vulnérabilités.

2. Pour configurer l'intégration Microsoft Threat and Vulnerability Management, cliquez sur **Modifier**.
3. Remplissez les champs du formulaire.

Formulaire Informations d'identification de compte

Champ	Description
Nom	Nom de l'instance.
Région TVM	Région proche de l'emplacement de votre serveur. Utilisez le serveur le plus proche de votre emplacement pour des performances optimales de l'API.
Type d'authentification	Méthode de vérification de l'identité. L'authentification utilisateur contrôle la visibilité de ressources spécifiques sur des utilisateurs spécifiques. MS TVM exporte les groupes d'appareils autorisés pour cet utilisateur. La valeur par défaut est Application.
ID de locataire	Identité du locataire de votre organisation.
ID client	Identité du client générée après l'enregistrement de MS TVM dans Microsoft Azure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom d'utilisateur	Utilisateur ayant accès au groupe d'appareils complet. Ce champ apparaît uniquement lorsque l'utilisateur est sélectionné à partir du type d'authentification.
Mot de passe	Mot de passe du nom d'utilisateur ayant accès au groupe complet d'appareils. Ce champ apparaît uniquement lorsque l'utilisateur est sélectionné à partir du type d'authentification.
Secret client	Clé secrète du client générée après l'enregistrement de l'application MS TVM. Ce champ apparaît uniquement lorsque Application est sélectionnée à partir du type d'authentification.

4. Pour enregistrer vos changements et passer au premier formulaire d'intégration, cliquez sur **Suivant**.
   Le formulaire Configuration de l'importation des vulnérabilités s'affiche.
5. Activez ou désactivez l'importation des vulnérabilités, déterminez la date de début initiale des vulnérabilités que vous souhaitez importer et planifiez le moment où l'importation des vulnérabilités MS TVM doit s'exécuter.
   Si vous souhaitez importer toutes les vulnérabilités, ne renseignez pas la date de démarrage initiale.
   a. Pour importer des données à la demande, cliquez sur **Importer les vulnérabilités maintenant**.
   b. Pour afficher l'enregistrement de l'intégration, cliquez sur **Paramètres avancés**.
6. Pour enregistrer vos changements et passer au premier formulaire d'intégration, cliquez sur **Suivant**.
   Le formulaire Configuration de l'importation des recommandations s'affiche.
7. Activez ou désactivez l'importation des recommandations et déterminez le calendrier d'exécution de l'importation des vulnérabilités MS TVM.
   a. Pour importer des données à la demande, cliquez sur **Importer les recommandations maintenant**.
   b. Pour afficher l'enregistrement de l'intégration, cliquez sur **Paramètres avancés**.
8. Pour enregistrer vos changements et passer au premier formulaire d'intégration, cliquez sur **Suivant**.
   Le formulaire Configuration de l'importation des machines s'affiche.
9. Activez ou désactivez l'importation des machines, déterminez la date de début initiale pour les machines que vous souhaitez importer et planifiez le moment où l'importation des machines MS TVM doit s'exécuter.
   Si vous souhaitez importer toutes les machines, ne renseignez pas la date de démarrage initiale.

   Remarque : Les balises machine sont importées par défaut et utilisées pour organiser et suivre les machines répertoriées dans l'environnement MS TVM.

   a. Pour afficher les règles de recherche d'éléments de configuration (CI) par défaut, cliquez sur **Règles de recherche de CI**. Les règles de recherche de CI définissent la manière dont les données machine de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans le ServiceNow AI Platform CMDB fichier . Vous pouvez ajouter des règles de recherche ou modifier les règles de recherche de CI par défaut sur cette page. Pour plus d'informations, consultez Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.
   b. Pour importer des données à la demande, cliquez sur **Importer des machines maintenant**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les ordinateurs dont l'état est intégré dans MS TVM sont récupérés par l'application ServiceNow.

c. Pour afficher l'enregistrement de l'intégration, cliquez sur **Paramètres avancés**.

10. Pour enregistrer vos changements et accéder au premier formulaire d'intégration, cliquez sur **Suivant**. Le formulaire Configuration de l'importation des vulnérabilités de la machine s'affiche.
11. Activez les intégrations suivantes et déterminez la date de début initiale pour les vulnérabilités que vous souhaitez importer.

Formulaire Configuration de l'importation des vulnérabilités de la machine

Intégration	Description
Importation Delta des vulnérabilités de la machine Microsoft TVM	Récupère les vulnérabilités qui ont été mises à jour pendant l'importation complète de la vulnérabilité, y compris les vulnérabilités nouvelles, corrigées et mises à jour. Vous ne pouvez importer des données delta que pour les 14 derniers jours.
Importation totale des vulnérabilités de la machine Microsoft TVM	Récupère toutes les vulnérabilités ouvertes. En raison du volume élevé d'importations de données, vous pouvez les planifier pour qu'elles s'exécutent chaque semaine.

Remarque :

Exécutez l'importation des machines avant l'intégration des vulnérabilités de la machine. Sinon, les VI ne sont pas créés pour les machines manquantes.

12. Pour enregistrer vos modifications et terminer la configuration dans l'Assistant de configuration, cliquez sur **Terminer**.

Que faire ensuite

Si vous souhaitez activer un regroupement d'éléments vulnérables dans l'environnement classique, accédez à > **Réponse aux vulnérabilités** > **Administration** > **Règles de la tâche de rattrapage** > **Recommandation Microsoft TVM**.

Dans le formulaire qui s'affiche, sélectionnez l'option **Actif** pour l'activer. Vous pouvez également sélectionner **Nouveau** pour créer une règle.

Pour plus d'informations, consultez Réponse aux vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage.

Configurer l'utilisation de l'assistant Qualys Vulnerability Integration de configuration

Après avoir installé l'application Qualys , configurez-la à l'aide de l'assistant de configuration.

Avant de commencer

Utilisez les sections suivantes pour compléter les instructions et les invites fournies dans l'assistant de configuration du Qualys Vulnerability Integration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifiez que vous avez déjà installé l'application avant de commencer. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.
- Pour plus d'informations, reportez-vous à la Qualys Vulnerability Integration section Préparation pour le Qualys Vulnerability Integration .
- Vérifiez que vous disposez d'informations d'identification de compte tiers. Ils sont nécessaires pour modifier certaines applications tierces.

Rôles requis : administrateur système (admin) pour l'installation, administrateur de vulnérabilité (sn_vul.vulnerability_admin) ou sn_vul.admin (déconseillé) pour la configuration.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
   Les intégrations installées s'affichent.
2. Cliquez sur **Modifier** à droite de la configuration Qualys Vulnerability Integration que vous souhaitez configurer.
3. Dans le formulaire Informations d'identification du compte, entrez vos Qualys Cloud Platform informations d'identification.
   Vos informations d'identification sont nécessaires pour le configurer.
4. Utilisez les remarques suivantes comme guide tout au long de la configuration.
   - Le lien **Paramètres avancés** vous dirige vers l'enregistrement d'intégration Qualys . Vous pouvez ajouter des paramètres pris en charge par le Qualys produit pour vos requêtes planifiées afin de vous aider à filtrer les données de vulnérabilité que vous importez. Consultez la section Définir des paramètres de filtre supplémentaires pour Qualys les importations pour plus d'informations.
   - Si vous avez effectué une mise à niveau à partir d'une version antérieure avec Réponse aux vulnérabilités une version que vous avez déjà configurée, cette version, avec ses paramètres de Qualys Vulnerability Integration configuration préservés, est toujours disponible.

     Sous Paramètres d'importation dans la configuration de détection d'hôte pour , il Qualys Vulnerability Integration existe une option permettant d'afficher les enregistrements de détection de vulnérabilité fixe Qualys . Si cette option est activée, elle vous permet de créer des éléments vulnérables à partir d'enregistrements de détection à l'état fixe (état=**Fixe**). Pour plus d'informations sur les détections d'éléments vulnérables, reportez-vous à la section Réponse aux vulnérabilités Détections d'éléments vulnérables à partir d'intégrations tierces.

     Vous pouvez activer la case à cocher **Rechercher par partition réseau** sur la page Configuration de la détection d'hôte pour inclure l'identificateur de partition réseau dans la recherche d'adresse IP. Consultez Mettre à jour les éléments de configuration avec l'identificateur de partition réseau pour le Qualys Vulnerability Integration pour plus d'informations.

     Toutes les balises d'hôte sont importées dans le cadre de l'intégration de la Qualys liste d'hôtes. Les balises d'hôte sont principalement utilisées pour le filtrage dans les règles de Réponse aux vulnérabilités tâche d'affectation et de rattrapage. Ils s'affichent dans le formulaire Élément détecté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L’intégration Qualys de la liste d’hôtes doit être exécutée avant de créer des règles de tâche d’affectation ou de rattrapage, afin Réponse aux vulnérabilités que toutes les balises puissent être présentes dans les règles et avant que les éléments vulnérables ne soient importés et regroupés.

Qualys **Les balises d’actif** sont stockées dans le module Balises d’hôte sous le Qualys Vulnerability Integration.

- Le prend Qualys Vulnerability Integration en charge multi-sources. Vous pouvez avoir plusieurs déploiements de la même intégration tierce. Pour ajouter une autre intégration, sur la page Intégrations de scanners, cliquez sur **Ajouter une intégration**.

  Les paramètres de votre intégration tierce d’origine servent de modèle pour les paramètres de chaque nouvelle intégration.

  Remarque : Si vous supprimez l'intégration de vulnérabilité d'origine, vous devez sélectionner une autre intégration à utiliser comme modèle. Envisagez de désactiver l’intégration au lieu de la supprimer. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

  Les données de chaque intégration tierce sont identifiées de manière unique et disponibles dans une seule instance de Réponse aux vulnérabilités.

- Vous pouvez exécuter des importations sur demande en cliquant sur **Exécuter maintenant** sur une page de configuration.

5. Cliquez sur **Terminer** pour terminer la configuration dans l’Assistant de configuration.

Configurer l’intégration de vulnérabilité Tenable à l’aide de l’assistant de configuration

Après avoir installé l’application Vulnerability Response integration with Tenable , configurez-la à l’aide de l’assistant de configuration.

Avant de commencer

Utilisez les sections suivantes pour compléter les instructions et les invites fournies dans l’assistant de configuration pour l’intégration Vulnerability Response integration with Tenable .

- Vérifiez que vous avez déjà installé l’application avant de commencer. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l’aide de l’assistant de configuration.
- Pour plus d’informations, reportez-vous à la Tenable pour Réponse aux vulnérabilités section Préparation à l’intégration de vulnérabilité Tenable .
- Vérifiez que vous disposez d’informations d’identification de compte tiers. Ils sont nécessaires pour modifier certaines applications tierces.

Rôles requis : Administrateur système (admin) pour l’installation, Administrateur de vulnérabilité (sn_vul.vulnerability_admin) ou sn_vul.admin (obsolète) et Configurer l’intégration (sn_vul_tenable.configure_integrations) pour la configuration.

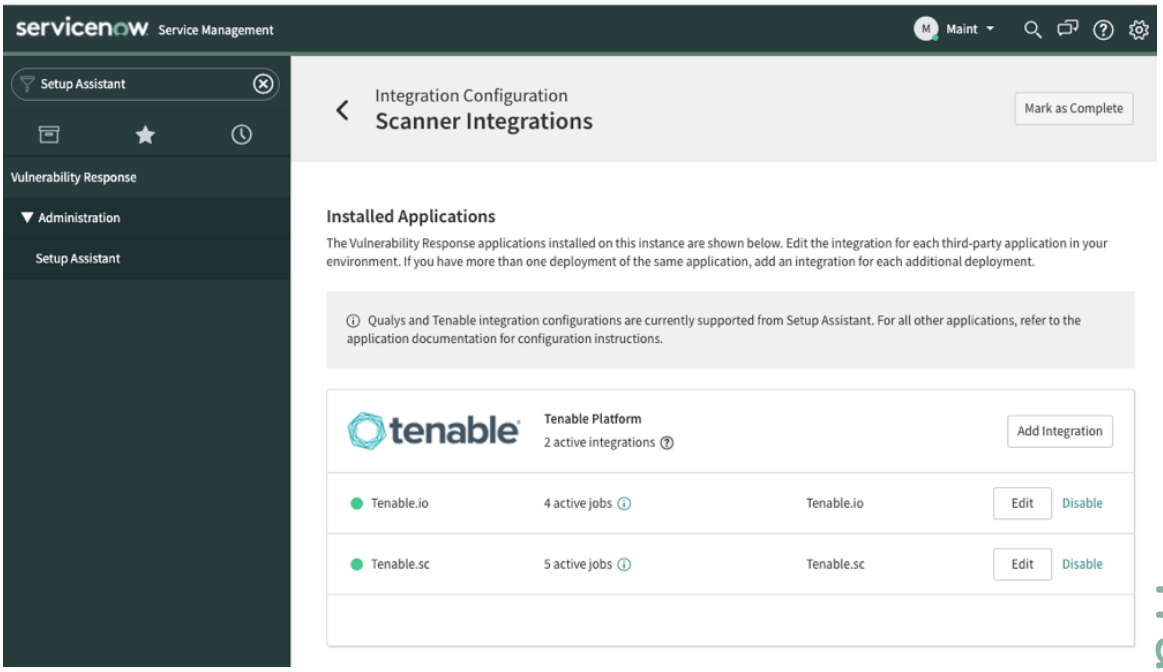
Procédure

1. S’il n’est pas affiché, accédez à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.

   Les , Tenable.sc et Tenable.cs intégrations Tenable.io s’affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Tenable est une intégration multisource, et vous pouvez avoir plusieurs déploiements de la même intégration tierce. Les paramètres de votre intégration tierce d'origine servent de modèle pour les paramètres de chaque nouvelle intégration.

Remarque : Si vous supprimez l'intégration de vulnérabilité d'origine, vous devez sélectionner une autre intégration à utiliser comme modèle. Envisagez de désactiver l'intégration au lieu de la supprimer. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

Les données de chaque intégration tierce sont identifiées de manière unique et disponibles dans une seule instance de Réponse aux vulnérabilités.

2. À droite de l'intégration Tenable que vous souhaitez configurer, sélectionnez **Modifier**.
3. Renseignez les champs du formulaire Informations d'identification de compte.

   - Tenable.io nécessite l'accès Administrateur avec un attribut d'autorisation supérieur ou égal à 64.

     Remarque : À partir de la version 3.8 de , l'accès Vulnerability Response integration with TenableTenable.io ne nécessite plus de privilèges d'administrateur. Un utilisateur de base avec un attribut d'autorisation égal à 16 peut également accéder au produit.

   - Tenable.sc nécessite l'accès d'analyste ou de gestionnaire de sécurité.
   - Tenable.cs nécessite un jeton donnant accès à la plateforme CS Tenable Générer un jeton.

   a. Sélectionnez votre produit Tenable.

   b. Entrez le nom de votre compte Tenable.

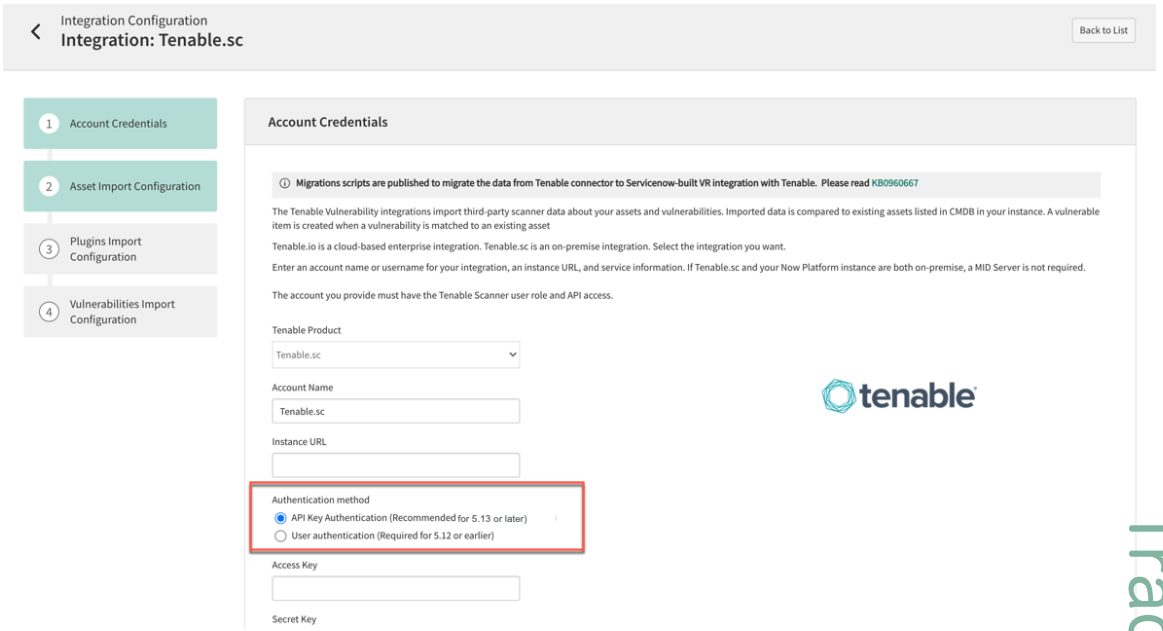
   c. Dans le champ URL de l'instance, saisissez l'URL de votre plateforme Tenable.

   d. Sélectionnez une méthode d'authentification (dans le cas de , passez à l'étape Tenable.cs f).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Selon votre version de Tenable.sc, deux options s'offrent à vous pour l'authentification :



i. À partir de la version 5.13 de , sélectionnez Authentification de Tenable.sc**clé API**. Saisissez vos clés d'accès et secrètes Tenable.

ii. Avant la version 5.13, l'authentification utilisateur est prise en charge par votre ServiceNow AI Platform® instance et est requise. Entrez votre nom d'utilisateur et votre ServiceNow AI Platform mot de passe.

Seule l'authentification de clé API est prise en charge pour Tenable.sc. Saisissez vos clés d'accès et secrètes Tenable.

e. **Facultatif :** Sélectionnez un MID Server

(Optional) Si votre instance et votre ServiceNow AI PlatformTenable.sc application ne se trouvent pas au même emplacement, choisissez un serveur MID configuré dans la liste. Pour plus d'informations, consultez Serveur MID .

- À partir des Réponse aux vulnérabilités versions 15.0 et 3.0 de , vous avez la possibilité d'activer le `Async_request` paramètre comme décrit dans Paramètres de récupération de données pour l'intégration de vulnérabilité Tenable.Tenable Vulnerability Integration Si vous souhaitez effectuer des appels synchrones, une configuration avec Tenable est nécessaire. Contactez le produit Tenable pour obtenir de l'aide. Ce paramètre, une fois activé, est applicable à toutes les intégrations de Tenable.sc et il y a un délai d'expiration de 30 secondes. Pour afficher les scripts correctifs, accédez à **Définition du système** > **Scripts correctifs**.

- (Optional) Pour les clients existants, un script correctif est disponible si vous utilisez des appels asynchrones.

Si votre instance et votre ServiceNow AI PlatformTenable.sc application sont toutes les deux sur site, bien que non requises, vous avez la possibilité de sélectionner un serveur MID configuré dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Que vous choisissiez d'utiliser un ou non Serveur MID , les intégrations expirent au bout de cinq minutes et un message s'affiche en l'absence de réponse du serveur.

En cas d'erreur de délai d'expiration, vérifiez dans l'Assistant de configuration que vous avez saisi les informations d'identification et l'URL correctes.

f. Entrez le jeton d'API.

Remarque : Si vous obtenez une erreur pour des informations d'identification non valides dans l'assistant de configuration, vérifiez que vous avez saisi les informations d'identification et l'URL correctes.

4. Sélectionnez **Suivant** pour enregistrer vos changements et passer au premier formulaire d'intégration. Dans le cas de et Tenable.sc, le formulaire Configuration de l'importation des Tenable.io actifs s'affiche. Dans le cas de , le formulaire Configuration de l'importation des Tenable.cs actifs de conteneur s'affiche.

Remarque : Le formulaire Configuration de l'importation des actifs de conteneur n'est visible que s'il Réponse aux vulnérabilités pour conteneurs est installé.

5. Sur ce formulaire, activez ou désactivez l'intégration d'importation d'actifs, déterminez la date de début initiale pour les actifs que vous souhaitez importer et planifiez le moment où l'importation d'actifs Tenable doit s'exécuter.

Pour Tenable.io

- L'intégration des actifs peut être utilisée avec les résultats de la conformité et l'intégration Tenable.io du remplissage des résultats de la conformité pour importer des données d'évaluation de configuration sécurisées concernant vos actifs dans l'application Conformité de la configuration .
- La version 12.2 de l'application Conformité de la configuration est requise sur votre instance si vous souhaitez importer et afficher ces données d'évaluation de configuration sécurisée.

  Consultez la rubrique Conformité de la configuration Données importées pour en savoir plus sur les données importées avec ces intégrations et sur l'endroit où elles sont publiées.
- Les Tenable.io intégrations Résultats de conformité et Remplissage des résultats de conformité ne sont pas activées par défaut. Si vous les activez, vous préférerez peut-être utiliser les paramètres de calendrier par défaut fournis. Consultez les étapes ci-dessous pour savoir comment localiser et activer les intégrations pour le Tenable Vulnerability Integration.
- Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Tenable.io produit à partir de votre instance. L'intégration Tenable.io du modèle et l'intégration des informations d'identification Tenable.io de numérisation doivent être activées avant de lancer de nouvelles analyses.

Par défaut, ces intégrations sont désactivées. Lorsque vous saisissez vos informations d'identification pour Tenable.io, toutes les Tenable.io intégrations sont automatiquement activées. Pour activer ou désactiver manuellement ces intégrations :

a. Accédez à la **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.

b. Dans la liste qui s'affiche, recherchez les enregistrements d'intégration Tenable.io souhaités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Ouvrez chaque enregistrement et cochez la case **Actif** pour activer l'intégration.

d. Sélectionnez **Mettre à jour** pour enregistrer vos changements.

e. Revenez à l'assistant de configuration pour poursuivre votre configuration pour le Tenable Vulnerability Integration avec Réponse aux vulnérabilités.

- Pour l'intégration Tenable.io , vous avez également la possibilité d'activer et de désactiver l'importation de balises d'actifs. Les balises d'actif sont importées par défaut et utilisées pour organiser et suivre les actifs répertoriés dans votre CMDB dans l'environnement Tenable.io .
- Pour les produits et Tenable.sc , si vous sélectionnez Activer la Tenable.io**recherche par partition réseau** sous Rechercher par partition réseau, vous pouvez créer des CI individuels à l'aide du moteur Identification et rapprochement (IRE) pour vos actifs qui ont la même adresse IP. Voir Mettre à jour les éléments de configuration avec l'identificateur de partition réseau pour le Tenable Vulnerability Integration et Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation pour plus d'informations.
- Pour Tenable.io et Tenable.sc en haut de l'écran à côté du lien d'importation de ressource, sélectionnez le lien des règles de recherche de CI pour afficher les règles de recherche **d'éléments** de configuration (CI) par défaut. Les règles de recherche de CI définissent la manière dont les données d'actifs de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans la ServiceNow AI Platform CMDB. Vous pouvez ajouter des règles de recherche ou modifier les règles de recherche de CI par défaut sur cette page. Pour plus d'informations, consultez Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.
- Sélectionnez **Importer des actifs maintenant** pour importer des données à la demande.
- Le lien **Paramètres avancés** vous dirige vers l'enregistrement d'intégration de l'actif. À partir de la version 3.3, vous pouvez ajouter des paramètres pris en charge par le Tenable.io produit pour vos requêtes planifiées afin de vous aider à filtrer les données de vulnérabilité que vous importez avec les Tenable.io Actifs et les intégrations de vulnérabilités fixes et ouvertes. Consultez la section Définir des paramètres de filtre supplémentaires pour Tenable.io les importations pour plus d'informations.

6. Sélectionnez **Suivant** pour enregistrer vos changements et passer au formulaire suivant.

> **Remarque :** Dans le cas de Tenable.io et Tenable.sc. Pour Tenable.cs le formulaire de configuration de l'importation des vulnérabilités de l'hôte s'affiche, continuez à partir de l'étape 9 pour une configuration CS Tenable plus approfondie.

Le formulaire Configuration de l'importation des modules d'extension s'affiche.

7. Dans le formulaire Configuration de l'importation des modules d'extension , activez ou désactivez l'importation des modules d'extension (entrées de vulnérabilité tierces) Déterminez la date de démarrage initiale pour les modules d'extension que vous souhaitez importer et planifiez le moment où l'importation des modules d'extension Tenable doit s'exécuter.

Si vous souhaitez importer l'ensemble des modules d'extension, vulnérabilités et actifs, laissez la date de début initiale vide.

- **Sélectionnez Importer les modules d'extension maintenant** pour importer des données à la demande.
- Le lien **Paramètres avancés** vous dirige vers l'enregistrement d'intégration des modules d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour l'importation des vulnérabilités, vous pouvez planifier et définir des niveaux de gravité pour Tenable.io les vulnérabilités que vous souhaitez ingérer. Déterminez une date afin que seules les vulnérabilités créées ou mises à jour à partir d'une date spécifique soient importées.
- Pour l'intégration Tenable.sc , vous pouvez déterminer un filtre de requête et une date afin que seules les vulnérabilités créées ou mises à jour à partir d'une date spécifique soient importées.

8. Sélectionnez **Suivant** pour enregistrer vos changements et passer au formulaire suivant.
   Le formulaire Configuration de l'importation des vulnérabilités s'affiche. Activez ou désactivez l'intégration et déterminez la date de début initiale pour les vulnérabilités que vous souhaitez importer.

   Pour le Tenable.io produit :

   - Importez uniquement les vulnérabilités et les VI associés qui correspondent aux conditions que vous choisissez avec le filtre Gravité.
   - Pour l'intégration des actifs, `Last Scan Time` est importée et mise à jour uniquement pour les Tenable.io actifs qui présentent des vulnérabilités.
   - Activez l'option **Vulnérabilités corrigées** pour afficher les VI des enregistrements de détection corrigés. Si ce marqueur est activé dans l'Assistant de configuration, de nouveaux VI sont créés pour les détections à l'état **Fixe** qui n'existent pas dans votre instance. Lorsqu'elle est activée, cette fonctionnalité peut avoir un impact négatif sur vos performances d'ingestion.
   - Le lien **Paramètres avancés** à côté de Filtres d'importation vous dirige vers l'enregistrement d'intégration des vulnérabilités.
   - Sélectionnez le lien **Importer les calendriers** en haut pour configurer la fréquence à laquelle les vulnérabilités sont ingérées et activer l'intégration.

   Pour le Tenable.sc produit :

   - Importez uniquement les vulnérabilités et les éléments vulnérables associés qui correspondent aux filtres de condition définis par une requête Tenable dans la plateforme Tenable. Voir la documentation Tenable pour plus d'informations sur les requêtes Tenable.

     Le filtre de requête Tenable que vous sélectionnez dans l'assistant de configuration s'applique également à l'intégration Tenable.sc des actifs. Seuls les actifs présentant les vulnérabilités qui correspondent aux conditions du filtre de requête sont importés.

   - Activez l'option **Vulnérabilités corrigées** pour afficher les VI des enregistrements de détection corrigés. Si ce marqueur est actif dans l'Assistant de configuration, de nouveaux VI sont créés pour les détections à l'état **Fixe** qui n'existent pas dans votre instance. Lorsqu'elle est active, cette fonctionnalité peut avoir un impact négatif sur vos performances d'ingestion.
   - Pour inclure l'identificateur de partition de réseau dans la recherche d'adresse IP, sélectionnez l'icône **Activer la recherche par partition de réseau** case à cocher dans le **Rechercher par partition réseau** section. Pour plus d'informations, consultez Mettre à jour les éléments de configuration avec l'identificateur de partition réseau pour le Tenable Vulnerability Integration.
   - Sélectionnez **Importer des calendriers** en haut pour configurer la fréquence à laquelle les vulnérabilités sont ingérées et activer l'intégration.
   - Le lien **Paramètres avancés** à côté de Filtres d'importation vous dirige vers l'enregistrement d'intégration des vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'intégration ServiceNow® Tenable.sc des informations d'identification d'analyse est activée (active) automatiquement à partir de l'assistant de configuration de votre instance lorsque vous configurez les Tenable.sc intégrations de vulnérabilités (Tenable.sc intégrations de vulnérabilités ouvertes et corrigées).

  Cette intégration importe et met à jour les Tenable.sc informations d'identification du scanner du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable. Accédez à la **Intégration de vulnérabilité Tenable** > **Intégrations** > **Intégration des informations d'identification de numérisation Tenable.sc** pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation.

9. Sélectionnez **Suivant** dans l'étape de configuration de l'importation des actifs de conteneur.
   Le formulaire Configuration de l'importation des vulnérabilités de l'hôte s'affiche. Activez ou désactivez l'intégration.
   - Importez uniquement les vulnérabilités et les VI associés qui correspondent aux conditions que vous choisissez avec le filtre Gravité.
   - Le lien Paramètres avancés à côté de Filtres d'importation vous dirige vers l'enregistrement d'intégration des vulnérabilités.
   - Sélectionnez le lien Importer les calendriers en haut pour configurer la fréquence à laquelle les vulnérabilités sont ingérées et activer l'intégration.
   - En haut de l'écran, à côté du lien Importer les calendriers, sélectionnez le lien Règles de recherche de CI pour afficher les règles de recherche d'éléments de configuration (CI) par défaut. Les règles de recherche de CI définissent la manière dont les données d'actifs de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans la ServiceNow AI Platform CMDB. Vous pouvez ajouter des règles de recherche ou modifier les règles de recherche de CI par défaut sur cette page. Pour plus d'informations, consultez Règles de recherche de CI pour l'identification des éléments de configuration à partir des intégrations de vulnérabilité tierces de Vulnerability Response.

10. **Remarque :** Cette étape concerne uniquement le Tenable.cs produit.

    Sélectionnez Suivant pour enregistrer vos changements et passer au formulaire suivant.
    - Importez uniquement les vulnérabilités de conteneurs et les CVI associées qui correspondent aux conditions que vous choisissez avec le filtre de gravité.
    - Le lien Paramètres avancés à côté de Filtres d'importation vous dirige vers l'enregistrement d'intégration des vulnérabilités.
    - Sélectionnez le lien Importer les calendriers en haut pour configurer la fréquence à laquelle les vulnérabilités sont ingérées et activer l'intégration.
    - La configuration de l'importation des vulnérabilités de conteneur n'est visible que si Container Vulnerability Response est installé.

    Le formulaire Configuration de l'importation des vulnérabilités du conteneur s'affiche. Activez ou désactivez l'intégration.

11. Sélectionnez **Terminer** pour enregistrer vos changements et terminer la configuration dans l'Assistant de configuration.

Que faire ensuite

(Facultatif) Accédez à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Calculateurs de vulnérabilités** > **Calculateur de risque par défaut** > **Règle de risque Tenable** pour activer la règle de risque Tenable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le formulaire Règle du calculateur de vulnérabilité qui s'affiche, cochez la case Actif pour l'activer.

La règle de risque Tenable est installée avec l'application dans le Vulnerability Response integration with Tenable cadre du calculateur de risque par défaut dans les calculateurs de vulnérabilité de Réponse aux vulnérabilités. L'évaluation de priorité de vulnérabilité (VPR) est un attribut du produit Tenable qui est importé et utilisé avec le nouveau calculateur de risque par défaut. Cette règle de risque est désactivée par défaut. En activant la règle du calculateur de risque Tenable, les valeurs VPR importées sont utilisées pour calculer le score de risque des éléments vulnérables. La distribution de poids par défaut pour ce calculateur de risque est la suivante : VPR = 70 %, Actif = 15 % et Criticité opérationnelle = 15 %. L'activation de cette règle du calculateur de risque Tenable peut avoir un impact sur vos performances d'ingestion de données.

Reportez-vous à la rubrique Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.

Configuration des fournisseurs de solutions de vulnérabilité

Configurez les fournisseurs de solutions de vulnérabilité en suivant la liste de vérification, puis en configurant les fournisseurs dans l'assistant de configuration.

Préparer la liste de vérification de l'intégration de solution

Utilisez l'assistant de configuration pour préparer l'implémentation d'une intégration d'intelligence de solution pour tous les fournisseurs qui prennent en charge le format de données du Cadre commun de génération de rapports de vulnérabilité (CVRF) ou du Cadre de travail commun de conseil de sécurité (CSAF).

Préparation de l'intégration de la solution CVRF (Common Vulnerability Reporting Framework)

Utilisez l'assistant de configuration pour préparer l'implémentation d'une intégration d'intelligence de solution pour tous les fournisseurs qui prennent en charge le format de données CVRF (Common Vulnerability Reporting Framework).

Avant de commencer

Pour intégrer les fournisseurs qui fournissent les solutions, assurez-vous d'effectuer les tâches dans la liste de vérification suivante. Vous pouvez imprimer la liste de vérification et vérifier que les éléments énumérés sont renseignés avant d'installer l'application.

Liste de vérification de la préparation de l'intégration

Tâche	Description
Applications dépendantes ☐	Vérifiez que les applications suivantes sont installées à partir de :ServiceNow Store • Gestion des solutions de vulnérabilité : Pour en savoir plus sur l'installation de Gestion des solutions pour vulnérabilités, reportez-vous à et Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configurationInstaller l'application Gestion des solutions pour Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
	• Vulnerability Response : pour plus d'informations sur l'installation et l'activation de l'application Réponse aux vulnérabilités , reportez-vous à la section Installer Réponse aux vulnérabilités. Cette intégration requiert la version 16.1 ou Réponse aux vulnérabilités ultérieure.
Informations d'identification de compte de tiers ☐	Vérifiez que vous disposez d'informations d'identification de compte tiers. Ils sont nécessaires pour modifier certaines intégrations de solutions.
Authentification du fournisseur ☐	Vérifiez que vous avez authentifié les fournisseurs pour l'importation de solutions à l'aide des API. Pour plus d'informations sur l'authentification des fournisseurs, reportez-vous à la section Configurer les alias de connexion et d'informations d'identification. Si vous ne souhaitez pas configurer un fournisseur basé sur une API, vous pouvez ignorer cette étape.
Personnalisation du flux et de l'action de flux ☐	Si vous souhaitez configurer un fournisseur basé sur une API autre que Cisco, vous devez personnaliser le flux et l'action de flux pour extraire une clé unique et une URL CVRF de la réponse d'un avertissement. **Remarque :** La publication de l'URL CVRF n'est pas standard pour tous les fournisseurs. Pour personnaliser le flux pour des fournisseurs autres que Cisco, reportez-vous à la section Configurer un fournisseur de Vulnerability Reporting Framework commun autre que Cisco. Vous pouvez ignorer cette étape s'ils ne veulent pas configurer des fournisseurs autres que Cisco. Par défaut, le flux pour Cisco a été livré avec l'application.
Rôles ☐	Vérifiez qu'un groupe d'administrateurs ou un utilisateur peut gérer l'intégration. S'il n'est pas affecté, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préparation de l'intégration de la solution Cadre de travail consultatif de sécurité commun (CSAF)

Utilisez l'assistant de configuration pour préparer l'implémentation d'une intégration d'intelligence de solution pour tous les fournisseurs qui prennent en charge le format de données CSAF (Common Security Advisory Framework).

Avant de commencer

Pour intégrer les fournisseurs qui fournissent les solutions, assurez-vous d'effectuer les tâches dans la liste de vérification suivante. Vous pouvez imprimer la liste de vérification et vérifier que les éléments énumérés sont renseignés avant d'installer l'application.

Liste de vérification de la préparation de l'intégration

Tâche	Description
Applications dépendantes ☐	Vérifiez que les applications suivantes sont installées à partir de :ServiceNow Store • Gestion des solutions de vulnérabilité : Pour en savoir plus sur l'installation de Gestion des solutions pour vulnérabilités, reportez-vous à et Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configurationInstaller l'application Gestion des solutions pour Réponse aux vulnérabilités. • Vulnerability Response : pour plus d'informations sur l'installation et l'activation de l'application Réponse aux vulnérabilités , reportez-vous à la section Installer Réponse aux vulnérabilités. Cette intégration requiert la version 16.1 ou Réponse aux vulnérabilités ultérieure.
Informations d'identification de compte de tiers ☐	Vérifiez que vous disposez d'informations d'identification de compte tiers. Ils sont nécessaires pour modifier certaines intégrations de solutions.
Authentification du fournisseur ☐	Vérifiez que vous avez authentifié les fournisseurs pour l'importation de solutions à l'aide des API. Pour plus d'informations sur l'authentification des fournisseurs, reportez-vous à la section Configurer les alias de connexion et d'informations d'identification pour le Cadre de travail consultatif de sécurité commun (CSAF). Si vous ne souhaitez pas configurer un fournisseur basé sur une API, vous pouvez ignorer cette étape.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
Personnalisation du flux et de l'action de flux ☐	Si vous souhaitez configurer un fournisseur basé sur une API autre que Red Hat, vous devez personnaliser le flux et l'action de flux pour extraire une clé unique et une URL CSAF de la réponse d'un avertissement. **Remarque :** La publication de l'URL CSAF n'est pas standard pour tous les fournisseurs. Pour personnaliser le flux pour les fournisseurs autres que , reportez-vous à Red Hat la section Configurer un fournisseur de cadre de travail consultatif de sécurité commun autre que Red Hat. Vous pouvez ignorer cette étape s'ils ne veulent pas configurer d'autres fournisseurs que Red Hat. Par défaut, le flux a Red Hat été livré avec l'application.
Rôles ☐	Vérifiez qu'un groupe d'administrateurs ou un utilisateur peut gérer l'intégration. S'il n'est pas affecté, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles.

Configurer les fournisseurs de solutions de vulnérabilité

Après avoir installé l'application Gestion des solutions de vulnérabilité, configurez les fournisseurs de solutions de vulnérabilité à l'aide de l'Assistant de configuration.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou administrateur.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration**.
2. Cliquez sur **Intégrations de solutions**.
3. Dans la section Solutions installées , extrayez les données à l'aide d'une URL, d'une API ou d'une importation.
   - Pour extraire des données à l'aide d'une URL ou d'une API, cliquez sur **Ajouter une intégration**.
   - Pour extraire des données en chargeant un fichier Cadre de travail commun de réponse aux vulnérabilités (CVRF) ou CSAF (Common Security Advisory **Framework**), cliquez sur Importer le fichier.

Que faire ensuite

Selon le format dans lequel vous souhaitez importer les données, vous pouvez effectuer l'une des tâches suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour CVRF :
  - Si vous souhaitez importer un fichier CVRF, reportez-vous à la section Importer les données courantes de l'infrastructure de génération de rapports sur les vulnérabilités via l'importation de fichiers.
  - Si vous souhaitez importer des données CVRF à l'aide des API, reportez-vous à la section Importer les données CVRF (Common Vulnerability Reporting Framework) via l'URL CVRF.
  - Si vous souhaitez importer des données CVRF par le biais de conseils, reportez-vous à la section Importer les données communes du cadre de travail de génération de rapports de vulnérabilité à partir d'avis.
- Pour CSAF :
  - Si vous souhaitez importer un fichier CSAF, consultez Importer les données communes du cadre de travail consultatif de sécurité via l'importation de fichier.
  - Si vous souhaitez importer des données CSAF à l'aide des API, consultez Importer des données CSAF (Security Advisory Framework) communes via l'URL CSAF.
  - Si vous souhaitez importer des données CSAF par le biais de conseils, consultez Importer des données communes du cadre de travail consultatif de sécurité à partir d'avis.
-

Cadre commun de génération de rapports sur les vulnérabilités (CVRF)

Le Cadre commun de génération de rapports de vulnérabilité (CVRF) offre un cadre de travail standardisé pour la création de la documentation des rapports de vulnérabilité. Il s'agit d'un langage XML qui simplifie le partage d'informations cruciales liées à la sécurité entre diverses parties prenantes au sein de plusieurs organisations. En utilisant le format CVRF, l'échange et le traitement de l'information peuvent être accélérés.

Importer les données courantes de l'infrastructure de génération de rapports sur les vulnérabilités via l'importation de fichiers

Importez un fichier CVRF pour afficher les données au format CVRF. L'importation est une activité ponctuelle.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou administrateur.

Pourquoi et quand exécuter cette tâche

Une fois importée, une entrée de file d'attente est créée avec une pièce jointe, qui est analysée lors du traitement de l'entrée. Les données sont ensuite renseignées dans les tables respectives. Avant d'analyser les données CVRF, un enregistrement de mappage de scanner est créé en fonction de la configuration. Ensuite, les données de mappage des scanners sont transformées en données de mappage des fournisseurs.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail de Vulnerability Response commun**.
2. Cliquez sur **Importer le fichier**.

   Remarque : Vous ne pouvez charger qu'un seul fichier XML à la fois avec une taille de fichier maximale de 1 Go.

3. Dans le champ **Nom** , saisissez un nom unique pour l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le planificateur est créé avec ce nom.

4. Dans le champ **Fournisseur** , entrez son nom.
   Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
5. Cliquez sur **Terminer**.

Résultats

Une file d'attente d'importation est créée. Cliquez sur le lien dans la barre d'informations pour afficher les entrées de file d'attente du fournisseur ainsi que la liste connexe. Vous pouvez également afficher l'état de la tâche.

Une fois les données importées au format CVRF, les données sont traitées de la manière suivante :

1. Lorsque la file d'attente est traitée, le fichier est analysé avec une source de données dédiée.
2. Une fois le traitement terminé, le journal des applications est mis à jour.
3. Une fois le fichier XML CVRF analysé, il remplit les tables suivantes dans l'application ServiceNow® Réponse aux vulnérabilités .
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Vous pouvez voir les informations détaillées relatives aux erreurs ou aux exceptions dans les journaux d'application.

Configurer les alias de connexion et d'informations d'identification

Configurez les alias de connexion et d'informations d'identification pour authentifier les fournisseurs. Dans l'analyse consultative, les fournisseurs tiers sont authentifiés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Procédure

1. Créez une authentification OAuth.
   Consultez Créer un point de terminaison pour permettre aux clients d'accéder à l'instance .
2. Créez un alias de connexion et d'informations d'identification.
   Voir Créer un alias de connexion et d'informations d'identification .
3. Créez une connexion.
   a. Cliquez sur le nom de l'alias de connexion et d'informations d'identification nouvellement créé.
   b. Sous l'onglet **Connexions** , cliquez sur **Nouveau**.
   c. Si le type d'authentification est OAuth, sélectionnez le profil de registre d'application créé à l'étape 1 en tant que **Profil de l'entité OAuth**.
   d. Créez un enregistrement dans Connexions à partir de la liste connexe de l'enregistrement.
   e. Dans le champ **Informations d'identification** , sélectionnez l'enregistrement d'informations d'identification créé à l'étape 3d.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Dans le champ **URL de connexion** , entrez l'URL du fournisseur.

g. Cliquez sur **Envoyer**.

Configurer un fournisseur de Vulnerability Reporting Framework commun autre que Cisco

Configurez un fournisseur CVRF (Common Vulnerability Reporting Framework) autre que Cisco avec la prise en charge de l'API.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Connexion et informations d'identification** > **Alias de connexion et d'informations d'identification**.
2. Créez un enregistrement avec le type d'authentification pris en charge par le fournisseur.
   Pour plus d'informations sur l'authentification d'un fournisseur, reportez-vous à la section Configurer les alias de connexion et d'informations d'identification.
3. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Concepteur de flux**.
4. Dupliquez le flux appelé « Analyse consultative ».

   Remarque :
   - Si l'une des actions doit être modifiée, copiez-la et utilisez-la dans le nouveau flux.
   - Mettre à jour la logique liée à la pagination selon le fournisseur

5. Si la logique de paramètre de plage de dates est différente de celle de Cisco, copiez l'action **Mettre à jour les paramètres de pagination** et apportez les modifications requises pour le fournisseur.
6. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Mappages des données d'enrichissement**.
7. Créez un enregistrement selon Cisco en modifiant la valeur de **la clé de propriété** selon le fournisseur.
   Cette logique permet de mapper les champs obligatoires d'une charge utile consultative à une ServiceNow table.
8. Mappez les balises API suivantes à partir de la charge utile de l'API.
   Ces balises doivent être mappées avec des détails à renseigner dans la table Mappage des données d'enrichissement. Par défaut, le mappage spécifique à Cisco est expédié.

   Remarque : Vous devez créer un enregistrement si vous devez configurer plusieurs fournisseurs qui publient des avis.

Balise de charge utile consultative	Colonne de la table sn_vul_cvrf_solution_integration	Description
URL de CVRF	cvrf_url	Nom de balise qui contient l'URL de CVRF.
ID consultatif (clé unique de réponse)	ID	Nom de balise qui contient un identificateur unique.
Dernière date modifiée	last_modified_date	Nom de balise qui contient la date de dernière mise à jour de l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Balise de charge utile consultative	Colonne de la table sn_vul_cvrf_solution_integration	Description
securityAdvisoryIntegrationSysId	intégration	Se réfère au sysId de la tâche planifiée d'intégration, qui crée les enregistrements de solution de vulnérabilité.

9. En fonction du format de réponse, modifiez la logique d'analyse en copiant l'action **Récupérer la liste** du flux d'analyse consultative.

Importer les données communes du cadre de travail de génération de rapports de vulnérabilité à partir d'avis

Importez les données CVRF à partir d'avis en configurant l'URL du fournisseur avec le type d'importation comme API.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche

Lorsque l'intégration s'exécute, les avis sont récupérés. L'URL CVRF et l'ID des avis sont extraits de la charge utile. Les appels d'API REST sont effectués pour chaque URL CVRF, et les données sont analysées et stockées dans la table sn_vul_solution.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail de Vulnerability Response commun**.
2. Cliquez sur **Ajouter une intégration**.
3. Remplissez les champs du formulaire.

Formulaire Avis sur les solutions d'importation

Champ	Description
Type d'importation	Option permettant de sélectionner le type d'importation. Sélectionnez **l'API**.
Nom	Nom unique pour l'intégration.
Fournisseur	Nom du fournisseur. **Remarque :** Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
Alias de connexion	Option permettant de sélectionner des informations d'identification authentifiées. **Remarque :** La table sys_alias stocke les informations d'identification et l'URL de base des conseils.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Planifier	Fréquence à laquelle les données doivent être mises à jour.
Jour	Jour de la semaine où vous souhaitez que les données soient mises à jour.
Heure	Moment de la semaine où vous souhaitez que les données soient mises à jour.
Configuration de l'API	
Flux	Option permettant de sélectionner le flux. Le flux est déclenché lorsque le planificateur est exécuté. Le flux prend en charge l'analyse des avis, extrait l'URL CVRF et stocke ces détails dans les tables de mise à jour. Vous pouvez copier le flux existant et le modifier si nécessaire. Par exemple, vous pouvez apporter des modifications liées à la pagination.
Action de flux	Option permettant de sélectionner l'action de flux. Les actions de flux prennent en charge la fonctionnalité de fenêtre glissante. Vous pouvez mettre à jour les actions de flux et ajouter le paramètre de requête directement à l'action en les faisant glisser.
Table de mappage	Option permettant de sélectionner la table de mappage. L'enregistrement de la table de mappage des données d'enrichissement est utilisé pour extraire l'URL CVRF et l'ID d'avis de la charge utile des avis.
Conseils à partir de la réponse	Option permettant d'entrer le nom de la balise à partir de la charge utile des avis à partir de laquelle la liste des avis peut être extraite.
Critère de filtre	
Paramètres de plage horaire	Option permettant de sélectionner la plage horaire de la demande et le format de date des appels d'API. Date/Date de fin Le paramètre de demande est le nom du paramètre utilisé pour la date de début et la date de fin pendant les appels d'API. Par exemple, StartDate, start_date, endDate, end_date.
Format de date	Option permettant d'entrer le format de date, par exemple,mm/jj/aaaa... Le format de date est le format dont l'API a besoin pour le filtrage. Les formats qui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ne sont pas pris en charge par GlideDate ne fonctionnent pas.
Plage initiale en jours	En les jours pour lesquels les données doivent être extraites lors de la première exécution du planificateur. Pour les exécutions suivantes, le mécanisme de la fenêtre coulissante est suivi. **Remarque :** Si vous ne souhaitez pas sélectionner de plage horaire, sélectionnez **Aucun paramètre**.
Mappages des analyses	
Source de l'analyse	Option permettant de sélectionner la source de l'entrée tierce (TPE).
Colonne de vulnérabilité	Option permettant de sélectionner le mot clé.
Mots clés	Option permettant d'entrer le mot clé pour rechercher la colonne de vulnérabilité sélectionnée.

4. Cliquez sur **Terminer**.

Importer les données CVRF (Common Vulnerability Reporting Framework) via l'URL CVRF

Importez des données CVRF en configurant l'URL du fournisseur dans l'Assistant de configuration.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche

Lorsque l'intégration s'exécute, les données sont extraites de l'URL qui est analysée. Les données sont ensuite stockées dans la table sn_vul_solution avec la source comme nom du fournisseur.

Remarque : Oracle publie directement l'URL CVRF pour fournir des solutions. Ainsi, si vous souhaitez configurer l'intégration pour l'importation de données Oracle, assurez-vous de disposer de l'URL CVRF pour Oracle et procédez comme suit.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail de Vulnerability Response commun**.
2. Cliquez sur **Ajouter une intégration**.
3. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire d'importation CVRF

Champ	Description
Type d'importation	Type d'importation. Sélectionnez **une URL**.
Nom	Nom unique pour l'intégration.
Fournisseur	Nom du fournisseur. **Remarque :** Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
URL	URL à partir de laquelle vous souhaitez extraire les données de la solution au format CVRF.
Planifier	Fréquence à laquelle les données doivent être mises à jour. **Remarque :** Si la balise d'état de CVRF indique « FINAL », le champ est automatiquement défini sur **Sur demande** pour éviter les exécutions inutiles.
Jour	Jour de la semaine où vous souhaitez que les données soient mises à jour.
Heure	Moment de la semaine où vous souhaitez que les données soient mises à jour.

4. Cliquez sur **Terminer**.

Dépannage de l'importation de données du cadre de travail de génération de rapports de vulnérabilité commun

Les actions de dépannage peuvent aider à résoudre les problèmes courants lors de l'importation de données CVRF dans l'application Vulnerability Response.

Problème	Action
La durée d'exécution de l'intégration est longue	Si l'intégration s'exécute pendant une période plus longue que prévu, procédez comme suit : 1. Accédez à la table sn_vul_ds_import_q_entry. 2. Regroupement par champ **État** . Vous pouvez voir les entrées dont l'état est Terminé, En cours ou En file d'attente.
Échec de l'intégration dans l'importation basée sur l'API	Si l'intégration échoue dans l'importation basée sur l'API, procédez comme suit : 1. Accédez à **Concepteur de flux**. 2. Ouvrez le flux qui a été sélectionné dans la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Problème	Action
	Remarque : Dans le cas de Cisco, ouvrez le flux Analyse des conseils. **3.** Cliquez sur **Exécutions**. **4.** Ouvrez la dernière exécution ou l'exécution qui doit être déboguée. **5.** Vérifiez le flux à chaque étape.
Échec de l'intégration dans l'importation basée sur l'API avec une erreur de délai d'expiration	Si l'intégration échoue dans une importation basée sur une API en raison d'un délai d'expiration dans le flux d'analyse de conseils, procédez comme suit : **1.** Augmentez le délai d'expiration en ouvrant sys_properties. LISTE. **2.** Dans la colonne Nom, recherchez `sn_vul.CVRFFlowTimeout (inMiliSeconds)`. **Remarque :** Le temps est en millisecondes. **3.** Ouvrez l'enregistrement et mettez à jour la valeur avec un nombre élevé. **4.** Enregistrez l'enregistrement et réexécutez l'intégration.
Échec de l'intégration avec l'erreur « Le mappage du scanner au fournisseur : la transformation des données de mappage est en cours »	Vérifiez si l'intégration échoue pendant l'importation basée sur l'URL ou l'API, avec l'erreur suivante : La transformation du mappage de scanner vers les données de mappage du fournisseur est en cours. Les données ne seront renseignées qu'une fois la transformation terminée. Essayez d'exécuter après un certain temps. Si vous rencontrez cette erreur, patientez un certain temps et exécutez à nouveau l'intégration.
La file d'attente d'importation n'est pas créée pendant l'importation du fichier	Lors de l'importation d'un fichier, la file d'attente d'importation n'est parfois pas créée. Cette défaillance signifie que la transformation des données de mappage des scanners en données de mappage des fournisseurs est en cours. L'entrée de file d'attente est créée une fois le processus terminé.

Cadre de travail consultatif de sécurité commun (CSAF)

Lorsqu'il est utilisé avec Gestion des solutions pour vulnérabilités, le Cadre de travail consultatif de sécurité commun (CSAF) active l'automatisation des notifications de sécurité via un format JSON lisible par machine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le CSAF vous permet de vous intégrer à n'importe quel fournisseur d'intelligence de solution en utilisant le cadre de travail de gestion des solutions pour importer les données d'intelligence. Les notifications de sécurité CSAF peuvent être de l'un des types suivants.

- Avis de sécurité
- Échange d'exploitabilité des vulnérabilités (VEX)
- Security Incident Response
- Avis d'information

Le CSAF ne prend en charge que les importations de fichiers, d'URL et d'API des avis de sécurité des fournisseurs.

Importer les données communes du cadre de travail consultatif de sécurité via l'importation de fichier

Importez un fichier CSAF pour afficher les données au format CSAF. L'importation est une activité ponctuelle.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche

Une fois importée, une entrée de file d'attente est créée avec une pièce jointe, qui est analysée lors du traitement de l'entrée. Les données sont ensuite renseignées dans les tables respectives. Avant d'analyser les données CSAF, un enregistrement de mappage de scanner est créé en fonction de la configuration. Ensuite, les données de mappage des scanners sont transformées en données de mappage des fournisseurs.

Le mappage d'analyse ne s'applique pas aux vulnérabilités basées sur la base de données de vulnérabilité nationale (NVD), qui sont des vulnérabilités avec une entrée de vulnérabilité commune (CVE) dans la base de données NVD.

Si vous n'avez qu'une seule solution de remplacement la plus élevée et qu'elle se déploie jusqu'aux éléments vulnérables, la solution préférée est renseignée. Lorsqu'il y a plusieurs solutions de fournisseurs incluses dans une entrée NVD, la solution préférée n'est pas renseignée, car il existe plus d'une solution de remplacement la plus élevée. Dans ce cas, vous devez sélectionner manuellement une solution. Pour les vulnérabilités tierces, la solution privilégiée n'est renseignée que si vous ajoutez le mappage d'analyse correspondant.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail consultatif de Security commun**.
2. Sélectionnez **Importer un fichier**.

   Remarque : Vous ne pouvez charger qu'un seul fichier JSON à la fois avec une taille de fichier maximale de 15 Mo.

3. Dans le champ **Nom** , saisissez un nom unique pour l'intégration.
   Le planificateur est créé avec ce nom.
4. Dans le champ **Fournisseur** , entrez son nom.
   Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
5. Sélectionnez **Finish** (Terminer).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Une file d'attente d'importation est créée. Sélectionnez le lien dans la barre d'informations pour afficher les entrées de file d'attente du fournisseur ainsi que la liste connexe. Vous pouvez également afficher l'état de la tâche.

Une fois les données importées au format CSAF, elles sont traitées de la manière suivante :

1. Lorsque la file d'attente est traitée, le fichier est analysé avec une source de données dédiée.
2. Une fois le traitement terminé, le journal des applications est mis à jour.
3. Une fois le fichier JSON CSAF analysé, il remplit les tables suivantes dans l'application ServiceNow® Réponse aux vulnérabilités .
   - sn_vul_solution
   - sn_vul_m2m_vulnerability_solution
   - sn_vul_nvd_entry
   - sn_vul_software
   - sn_vul_product_category

Vous pouvez voir les informations détaillées relatives aux erreurs ou aux exceptions dans les journaux d'application.

Configurer les alias de connexion et d'informations d'identification pour le Cadre de travail consultatif de sécurité commun (CSAF)

Configurez les alias de connexion et d'informations d'identification pour authentifier les fournisseurs. Dans l'analyse consultative, les fournisseurs tiers sont authentifiés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Procédure

1. Créez une authentification OAuth.
   Consultez Créer un point de terminaison pour permettre aux clients d'accéder à l'instance .
2. Créez un alias de connexion et d'informations d'identification.
   Voir Créer un alias de connexion et d'informations d'identification .
3. Créez une connexion.
   a. Sélectionnez le nom de l'alias de connexion et d'informations d'identification nouvellement créé.
   b. Sous l'onglet **Connexions** , sélectionnez **Nouveau**.
   c. Si le type d'authentification est OAuth, sélectionnez le profil de registre d'application créé à l'étape 1 en tant que **Profil de l'entité OAuth**.
   d. Créez un enregistrement dans Connexions à partir de la liste connexe de l'enregistrement.
   e. Dans le champ **Informations d'identification** , sélectionnez l'enregistrement d'informations d'identification créé à l'étape 3d.
   f. Dans le champ **URL de connexion** , entrez l'URL du fournisseur.
   g. Sélectionnez **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer un fournisseur de cadre de travail consultatif de sécurité commun autre que Red Hat

Configurez un fournisseur du Cadre de travail consultatif de sécurité commun (CSAF) autre qu'avec Red Hat la prise en charge de l'API.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Connexion et informations d'identification** > **Alias de connexion et d'informations d'identification**.
2. Créez un enregistrement avec le type d'authentification pris en charge par le fournisseur.
   Pour plus d'informations sur l'authentification d'un fournisseur, reportez-vous à la section Configurer les alias de connexion et d'informations d'identification pour le Cadre de travail consultatif de sécurité commun (CSAF).
3. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Concepteur de flux**.
4. Dupliquez le flux appelé « Analyse consultative ».

   Remarque :
   - Si l'une des actions doit être modifiée, copiez-la et utilisez-la dans le nouveau flux.
   - Examinez les paramètres page_index_key et page_size_key conformément à l'API du fournisseur.
   - Mettre à jour la logique liée à la pagination selon le fournisseur

5. Si la logique de paramètre de plage de dates est différente de Red Hat, copiez l'action **Mettre à jour les paramètres de pagination** et apportez les modifications nécessaires pour le fournisseur.
6. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Mappages des données d'enrichissement**.
7. Créez un enregistrement selon Red Hat en changeant la valeur de **la clé de propriété** selon le fournisseur.
   Cette logique permet de mapper les champs obligatoires d'une charge utile consultative à une ServiceNow table.
8. Mappez les balises API suivantes à partir de la charge utile de l'API.
   Ces balises doivent être mappées avec des détails à renseigner dans la table Mappage des données d'enrichissement. Par défaut, le Red Hat mappage spécifique est envoyé.

   Remarque : Vous devez créer un enregistrement si vous devez configurer plusieurs fournisseurs qui publient des avis.

Balise de charge utile consultative	Colonne de la table sn_vul_cvrf_solution_integration	Description
URL CSAF (URL de ressource pointant vers la charge utile CSAF)	cvrf_url	Nom de balise qui contient l'URL CSAF.
ID consultatif (clé unique de réponse)	ID	Nom de balise qui contient un identificateur unique.
Dernière date modifiée	last_modified_date	Nom de balise qui contient la date de dernière mise à jour de l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Balise de charge utile consultative	Colonne de la table sn_vul_cvrf_solution_integration	Description
CSAF (valeur statique)	advisory_format	Valeur au format consultatif pour les charges utiles CSAF. Notez qu'il s'agit d'une valeur statique applicable à toutes les intégrations CSAF.
securityAdvisoryIntegrationSysId	intégration	Se réfère au sysId de la tâche planifiée d'intégration, qui crée les enregistrements de solution de vulnérabilité.

9. En fonction du format de réponse, modifiez la logique d'analyse en copiant l'action **Récupérer la liste** du flux d'analyse consultative.

Importer des données communes du cadre de travail consultatif de sécurité à partir d'avis

Importez les données CSAF à partir d'avis en configurant l'URL du fournisseur avec le type d'importation comme API.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche

Lorsque l'intégration s'exécute, les avis sont récupérés. L'URL CSAF et l'ID des avis sont extraits de la charge utile. Les appels d'API REST sont effectués pour chaque URL CSAF, et les données sont analysées et stockées dans la table sn_vul_solution.

Le mappage d'analyse ne s'applique pas aux vulnérabilités basées sur la base de données de vulnérabilité nationale (NVD), qui sont des vulnérabilités avec une entrée de vulnérabilité commune (CVE) dans la base de données NVD.

Si vous n'avez qu'une seule solution de remplacement la plus élevée et qu'elle se déploie jusqu'aux éléments vulnérables, la solution préférée est renseignée. Lorsqu'il y a plusieurs solutions de fournisseurs incluses dans une entrée NVD, la solution préférée n'est pas renseignée, car il existe plus d'une solution de remplacement la plus élevée. Dans ce cas, vous devez sélectionner manuellement une solution. Pour les vulnérabilités tierces, la solution privilégiée n'est renseignée que si vous ajoutez le mappage d'analyse correspondant.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail consultatif de Security commun**.
2. Sélectionnez **Ajouter une intégration**.
3. Remplissez les champs du formulaire.

Formulaire Avis sur les solutions d'importation

Champ	Description
Type d'importation	Option permettant de sélectionner le type d'importation. Sélectionnez **l'API**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom unique pour l’intégration.
Fournisseur	Nom du fournisseur. **Remarque :** Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
Alias de connexion	Option permettant de sélectionner des informations d’identification authentifiées. **Remarque :** La table sys_alias stocke les informations d’identification et l’URL de base des conseils.
Planifier	Fréquence à laquelle les données doivent être mises à jour.
Jour	Jour de la semaine où vous souhaitez que les données soient mises à jour.
Heure	Moment de la semaine où vous souhaitez que les données soient mises à jour.
Configuration de l'API	
Flux	Option permettant de sélectionner le flux. Le flux est déclenché lorsque le planificateur est exécuté. Le flux se charge d’analyser les avis, extrait l’URL CSAF et stocke ces détails dans les tables de mise à jour. Vous pouvez copier le flux existant et le modifier si nécessaire. Par exemple, vous pouvez apporter des modifications liées à la pagination.
Action de flux	Option permettant de sélectionner l’action de flux. Les actions de flux prennent en charge la fonctionnalité de fenêtre glissante. Vous pouvez mettre à jour les actions de flux et ajouter le paramètre de requête directement à l’action en les faisant glisser.
Table de mappage	Option permettant de sélectionner la table de mappage. L’enregistrement de la table de mappage des données d’enrichissement est utilisé pour extraire l’URL CSAF et l’ID d’avis de la charge utile des avis.
Conseils à partir de la réponse	Option permettant d’entrer le nom de la balise à partir de la charge utile des avis à partir de laquelle la liste des avis peut être extraite.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Critère de filtre	
Paramètres de plage horaire	Option permettant de sélectionner la plage horaire de la demande et le format de date des appels d'API. Date/Date de fin Le paramètre de demande est le nom du paramètre utilisé pour la date de début et la date de fin pendant les appels d'API. Par exemple, StartDate, start_date, endDate, end_date.
Format de date	Option permettant d'entrer le format de date, par exemple,mm/jj/aaaa... Le format de date est le format dont l'API a besoin pour le filtrage. Les formats qui ne sont pas pris en charge par GlideDate ne fonctionnent pas.
Plage initiale en jours	En les jours pour lesquels les données doivent être extraites lors de la première exécution du planificateur. Pour les exécutions suivantes, le mécanisme de la fenêtre coulissante est suivi. **Remarque :** Si vous ne souhaitez pas sélectionner de plage horaire, sélectionnez **Aucun paramètre**.
Mappages des analyses	
Source de l'analyse	Option permettant de sélectionner la source de l'entrée tierce (TPE).
Colonne de vulnérabilité	Option permettant de sélectionner le mot clé.
Mots clés	Option permettant d'entrer le mot clé pour rechercher la colonne de vulnérabilité sélectionnée.

4. Sélectionnez **Finish** (Terminer).

Importer des données CSAF (Security Advisory Framework) communes via l'URL CSAF

Importez des données CSAF en configurant l'URL du fournisseur dans l'assistant de configuration.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin, sn_vul.admin (déconseillé) ou admin

Pourquoi et quand exécuter cette tâche
Lorsque l'intégration s'exécute, les données sont extraites de l'URL qui est analysée. Les données sont ensuite stockées dans la table sn_vul_solution avec la source comme nom du fournisseur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'URL peut être une charge utile CSAF directe, qui contient les détails consultatifs, ou une URL de flux ROLIE (Resource-Oriented Lightweight Information Exchange). Dans les deux cas, la charge utile est analysée en conséquence et les enregistrements de solution sont créés. Effectuez les étapes suivantes pour l'importation d'URL CSAF.

Vous pouvez également importer des solutions de vulnérabilité à partir d'agrégateurs CSAF ou de fournisseurs de confiance via une importation d'URL qui prend en charge le flux ROLIE. Ces solutions de vulnérabilité sont automatiquement mappées au fournisseur et aux éléments vulnérables (VIT) appropriés en fonction des vulnérabilités et expositions communes (CVE).

Le mappage d'analyse ne s'applique pas aux vulnérabilités basées sur la base de données de vulnérabilité nationale (NVD), qui sont des vulnérabilités avec une entrée de vulnérabilité commune (CVE) dans la base de données NVD.

Si vous n'avez qu'une seule solution de remplacement la plus élevée et qu'elle se déploie jusqu'aux éléments vulnérables, la solution préférée est renseignée. Lorsqu'il y a plusieurs solutions de fournisseurs incluses dans une entrée NVD, la solution préférée n'est pas renseignée, car il existe plus d'une solution de remplacement la plus élevée. Dans ce cas, vous devez sélectionner manuellement une solution. Pour les vulnérabilités tierces, la solution privilégiée n'est renseignée que si vous ajoutez le mappage d'analyse correspondant.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de solutions** > **Cadre de travail consultatif de Security commun**.
2. Sélectionnez **Ajouter une intégration**.
3. Remplissez les champs du formulaire.

Formulaire d'importation CSAF

Champ	Description
Type d'importation	Type d'importation. Sélectionnez **une URL**.
Nom	Nom unique pour l'intégration.
Fournisseur unique	Sélectionnez cette option si vous importez CSAF à partir d'un fournisseur.
Fournisseur	Nom du fournisseur. Ce champ **n'est** disponible que si vous sélectionnez Fournisseur unique. **Remarque :** Le champ **Source** des solutions est renseigné avec le nom du fournisseur.
Multi-fournisseur	Sélectionnez cette option si vous importez CSAF à partir de plusieurs fournisseurs.
Agrégateur	Un fournisseur de confiance dont vous pouvez importer la solution.
URL	URL à partir de laquelle vous souhaitez extraire les données de la solution au format CSAF.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Planifier	Fréquence à laquelle les données doivent être mises à jour. **Remarque :** Si la balise d'état de CSAF indique « FINAL », le champ est automatiquement défini sur **Sur demande** pour éviter les exécutions inutiles.
Jour	Jour de la semaine où vous souhaitez que les données soient mises à jour.
Heure	Moment de la semaine où vous souhaitez que les données soient mises à jour.
Mappages des analyses **Remarque :** La section Mappages de l'analyse est facultative pour CSAF.	
Source de l'analyse	Option permettant de sélectionner la source de l'entrée tierce (TPE).
Colonne de vulnérabilité	Option permettant de sélectionner le mot clé.
Mots clés	Option permettant d'entrer le mot clé pour rechercher la colonne de vulnérabilité sélectionnée.

4. Sélectionnez **Finish** (Terminer).

Dépannage de l'importation de données du cadre de travail consultatif de sécurité commun

Les actions de dépannage peuvent aider à résoudre les problèmes courants lors de l'importation de données CSAF dans l'application Vulnerability Response.

Problème	Action
La durée d'exécution de l'intégration est longue	Si l'intégration s'exécute pendant une période plus longue que prévu, procédez comme suit : 1. Accédez à la table sn_vul_ds_import_q_entry. 2. Regroupement par champ **État** . Vous pouvez voir les entrées dont l'état est Terminé, En cours ou En file d'attente.
Échec de l'intégration dans l'importation basée sur l'API	Si l'intégration échoue dans l'importation basée sur l'API, procédez comme suit : 1. Accédez à **Concepteur de flux**. 2. Ouvrez le flux qui a été sélectionné dans la configuration. **Remarque :** Dans le cas de Red Hat, ouvrez le flux Analyse consultative.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Problème	Action
	3. Sélectionnez Exécutions. **4.** Ouvrez la dernière exécution ou l'exécution qui doit être déboguée. **5.** Vérifiez le flux à chaque étape.
Échec de l'intégration dans l'importation basée sur l'API avec une erreur de délai d'expiration	Si l'intégration échoue dans une importation basée sur une API en raison d'un délai d'expiration dans le flux d'analyse de conseils, procédez comme suit : **1.** Augmentez le délai d'expiration en ouvrant sys_properties. LISTE. **2.** Dans la colonne Nom, recherchez sn_vul. CVRFFlowTimeout (inMiliSeconds). **Remarque :** Le temps est en millisecondes. **3.** Ouvrez l'enregistrement et mettez à jour la valeur avec un nombre élevé. **4.** Enregistrez l'enregistrement et réexécutez l'intégration.
Échec de l'intégration avec l'erreur « Le mappage du scanner au fournisseur : la transformation des données de mappage est en cours »	Vérifiez si l'intégration échoue pendant l'importation basée sur l'URL ou l'API, avec l'erreur suivante : La transformation du mappage de scanner vers les données de mappage du fournisseur est en cours. Les données ne seront renseignées qu'une fois la transformation terminée. Essayez d'exécuter après un certain temps. Si vous rencontrez cette erreur, patientez un certain temps et exécutez à nouveau l'intégration.
La file d'attente d'importation n'est pas créée pendant l'importation du fichier	Lors de l'importation d'un fichier, la file d'attente d'importation n'est parfois pas créée. Cette défaillance signifie que la transformation des données de mappage des scanners en données de mappage des fournisseurs est en cours. L'entrée de file d'attente est créée une fois le processus terminé.

Tâches d'installation et de configuration supplémentaires Réponse aux vulnérabilités

Pour vous aider dans le rattrapage, vous pouvez effectuer ces tâches de configuration administrative supplémentaires dans le cadre de votre configuration en dehors de la configuration de base. Vous effectuez ces tâches en dehors de l'assistant de configuration.

Vous pouvez utiliser les rapports par défaut fournis Réponse aux vulnérabilités avec pour surveiller votre posture de sécurité. Vous pouvez modifier ces rapports s'ils ne conviennent pas à votre environnement ou les utiliser comme modèles pour créer les vôtres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si l'application Analyse des performances pour Réponse aux vulnérabilités est installée, vous pouvez créer des rapports, des tableaux de bord réactifs, etc. Voir Introduction aux rapports pour plus d'informations.

Les notifications par e-mail augmentent la productivité et fluidifient le flux de travail.

Avec l'évaluation de l'exposition logicielle, recherchez l'éditeur, le nom du produit et le numéro de version dans Gestion des actifs logiciels (SAM Foundation) pour déterminer votre exposition aux logiciels vulnérables.

La visibilité sur les bibliothèques de vulnérabilités peut offrir une flexibilité pour les tâches de regroupement et de rattrapage.

Configurez Gestion des exceptions pour vous aider Lorsque votre organisation ne peut pas se conformer à une politique, une norme ou une directive de sécurité publiée, vous pouvez demander une exception.

Pour plus de tâches de configuration supplémentaires, consultez les rubriques qui suivent cette vue d'ensemble.

Tests de démarrage rapide pour Réponse aux vulnérabilités

Validez que Réponse aux vulnérabilités fonctionne toujours après avoir apporté un changement de configuration telle que l'application d'une mise à niveau ou le développement d'une application. Copiez et personnalisez ces tests de démarrage rapide à effectuer lorsque vous utilisez des données spécifiques à votre instance.

La propriété d'exécution de test est désactivée par défaut pour empêcher l'exécution de tests sur un système de production. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production. Pour Exécuter la suite de tests Framework de tests automatisés (ATF) pour Réponse aux vulnérabilités plus d'informations sur la configuration et l'exécution de la suite de tests pour Réponse aux vulnérabilités.

Les tests de démarrage rapide Réponse aux vulnérabilités nécessitent l'activation de l'application Réponse aux vulnérabilités (sn_vul) et le chargement des données de démonstration.

Tests Réponse aux vulnérabilités

Test	Description	Version
VR : créer une règle de cible de rattrapage	Créez une règle de cible de rattrapage.	Madrid
VR : créer une règle de groupe de vulnérabilité	Créer une règle de groupe de vulnérabilité.	Madrid
VR : créer un élément vulnérable via le formulaire	Déterminez si un utilisateur peut créer un élément vulnérable à partir du formulaire d'élément vulnérable.	Madrid
VR : cycle de vie du groupe de vulnérabilités	Déterminez si un utilisateur peut résoudre un groupe de vulnérabilités.	Madrid
VR : cycle de vie d'un élément vulnérable	Déterminez si un utilisateur peut faire évoluer un élément vulnérable	Madrid

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux vulnérabilités (suite)

Test	Description	Version
	tout au long de son cycle de vie, et déterminez si un élément vulnérable fermé peut être rouvert.	
VR : calculateur de déploiement	Déterminez si le calculateur de risque de déploiement peut fournir un score de risque global pour un groupe entier d'éléments vulnérables en utilisant les scores de tous les éléments vulnérables d'un groupe de vulnérabilité.	New York
VR : règles d'affectation de Réponse aux vulnérabilités	Déterminez si un exemple d'ensemble de règles d'affectation peut affecter automatiquement des éléments vulnérables à un groupe d'affectation pour la correction.	New York
VR : calculateurs de vulnérabilité	Testez les calculateurs de vulnérabilité.	New York
VR : recherche de CI - Qualys	Créez une nouvelle règle de recherche avec la méthode « field_matching » appelée « Rechercher par adaptateur réseau » pour Qualys. Déterminez si un élément de configuration est apparié avec succès dans la table Élément détecté par adaptateur réseau et adresse IP avec la nouvelle règle de recherche.	Orlando
VR : créer une demande de changement normal et urgent	Déterminez si l'utilisateur peut créer avec succès des demandes de changement normal et urgent depuis un groupe de vulnérabilité.	Orlando
VR : diviser un groupe de vulnérabilité	Déterminez si l'utilisateur peut diviser avec succès un groupe de vulnérabilité.	Orlando
VR : mettre à jour l'état d'un VG lorsqu'un CHG est annulé.	Déterminez si le champ État d'un groupe de vulnérabilité se modifie correctement lorsqu'une demande de changement associée au groupe de vulnérabilité est annulée.	Orlando
VR : mettre à jour l'état d'un VG lorsqu'un CHG passe à l'état Réviser.	Déterminez si le champ État d'un groupe de vulnérabilité se modifie correctement lorsqu'une demande de changement qui y est associée passe à l'état Réviser.	Orlando
VR : recherche de CI - Rapid7	Testez la recherche de CI à l'aide de la règle de recherche existante	Orlando

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux vulnérabilités (suite)

Test	Description	Version
	Intégration des vulnérabilités Rapid7, **adresse IP**.	
VR : recherche de CI - Qualys	Testez la recherche de CI en créant une règle de recherche pour Qualys Vulnerability Integration	Orlando
VR : workflow d'approbation des exceptions pour VI	Créez une demande d'exception et vérifiez que le processus d'approbation fonctionne.	Orlando
VR : workflow d'approbation des faux positifs pour VI	Créez une demande d'exception pour les faux positifs et vérifiez que le processus d'approbation fonctionne.	Orlando
VR : Réponse aux vulnérabilités des applications (AVR)	Déterminez si vos règles et calculateurs fonctionnent correctement. Vérifiez que les mises à jour fonctionnent.	Orlando
Règles de cibles de remédiation : test d'importation VI	Teste les règles de cibles de remédiation VR pendant l'importation.	Paris
VR : règle de classification	Exemple de règle de classification qui classifie automatiquement une vulnérabilité.	Tokyo

Information associée

Tests de démarrage rapide

Exécuter la suite de tests Framework de tests automatisés (ATF) pour Réponse aux vulnérabilités

Exécutez la suite de tests Framework de tests automatisés (ATF) après avoir installé ou mis à niveau l'application Réponse aux vulnérabilités .

Avant de commencer

Confirmez que l'installation a réussi et que votre instance fonctionne comme prévu.

La propriété d'exécution de test est désactivée par défaut pour empêcher l'exécution de tests sur un système de production. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production.

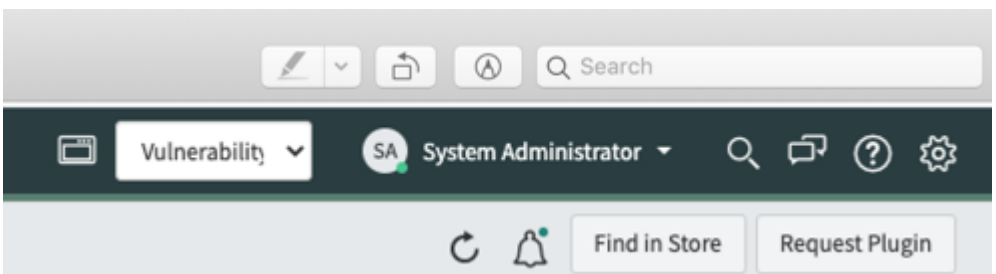
- Vérifiez que vous avez installé les données de démonstration lors de l'installation Réponse aux vulnérabilités de . Des données de démonstration sont nécessaires pour exécuter la suite de Réponse aux vulnérabilités tests.
- Pour activer le test, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Tous** > **Framework de tests automatisés (ATF)** > **Administration** > **Propriétés**.
2. Si elle n'est pas cochée, cochez la case **Activer l'exécution du test/de la suite de** tests.
3. Cliquez sur **Enregistrer**.
4. Si le champ d'application n'est pas défini sur **Vulnerability Response** dans l'en-tête, ou si le champ d'application n'est pas affiché dans l'en-tête, cliquez sur l'icône des paramètres en haut de la page dans la fenêtre du navigateur Icône Paramètres d'engrenage .
5. Dans la fenêtre Paramètres système, cliquez sur **Développeur**.
6. Si elle n'est pas sélectionnée, cliquez sur **Afficher le sélecteur d'application dans l'en-tête** et fermez la fenêtre.
7. Dans la liste qui s'affiche en regard de Administrateur système, cliquez sur **Réponse aux vulnérabilités** pour le champ.

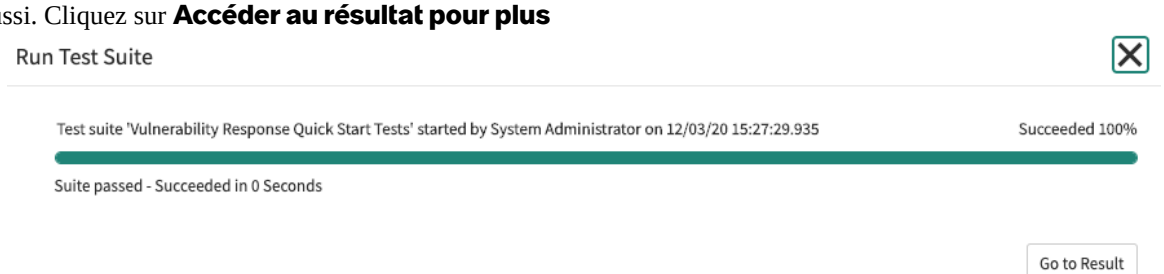
   Le champ s'affiche comme illustré dans l'image suivante.



Rôle requis : admin ou atf_test_admin

Procédure

1. Accédez à la **Tous** > **Framework de tests automatisés (ATF)** > **Suites**.
2. Dans la liste Suites de tests, localisez les **tests de démarrage rapide de Vulnerability Response**.
3. Sélectionnez-le pour ouvrir l'enregistrement.
4. Dans l'enregistrement ouvert, cochez la case **Actif** .
5. Cliquez sur **Mettre à jour**.
6. Si le bouton **Exécuter la suite de tests** ne s'affiche pas, actualisez votre écran, ouvrez à nouveau l'enregistrement et cliquez sur Exécuter la suite de **tests** pour démarrer le test.
   Après quelques instants, la boîte de dialogue Exécuter la suite de tests indique un test réussi. Cliquez sur **Accéder au résultat pour plus**



d'informations .

Que faire ensuite

Félicitations ! Vous pouvez poursuivre votre configuration de Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les tests automatisés et Réponse aux vulnérabilités les tests automatisés, les suites de tests et la création de tests automatisés, consultez Infrastructure de tests automatisés (ATF).

Installer Recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités

Installez Recommandations d'affectation de vulnérabilité pour réduire le temps que vous passez à identifier les propriétaires des résultats de vulnérabilité non affectés ou mal affectés. Cette application est disponible sous forme d'abonnement distinct dans le ServiceNow Store.

Avant de commencer

Avant d'exécuter la Recommandations d'affectation de vulnérabilité fonctionnalité dans Réponse aux vulnérabilités votre ServiceNow AI Platform® instance, vous devez d'abord télécharger et installer l'application Recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités . Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Pour plus d'informations, voir Activer une application ServiceNow Store.

Rôles requis : admin

Tâches de configuration	Action
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Accédez à la **Tous** > **Applications système** > **Toutes les applications** > **Installé dans votre instance**. Réponse aux vulnérabilités est affiché dans cette liste s'il est installé. Si l'application n'est pas installée et activée, reportez-vous à la section Installer Réponse aux vulnérabilités.
Vérifiez que l'application Intelligence prédictive est installée et activée.	Accédez à la **Applications système** > **Toutes les applications** > **Installé dans votre instance**. Intelligence prédictive est affiché dans cette liste s'il est installé. Si l'application n'est pas installée et activée, reportez-vous à la section Installer Intelligence prédictive .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Vérifiez que vous disposez des rôles requis suivants pour l'installation et la vérification des résultats attendus : • vulnerability_admin : nécessaire pour activer et configurer Recommandations d'affectation de vulnérabilité. Vous pouvez également l'utiliser pour afficher et sélectionner des recommandations

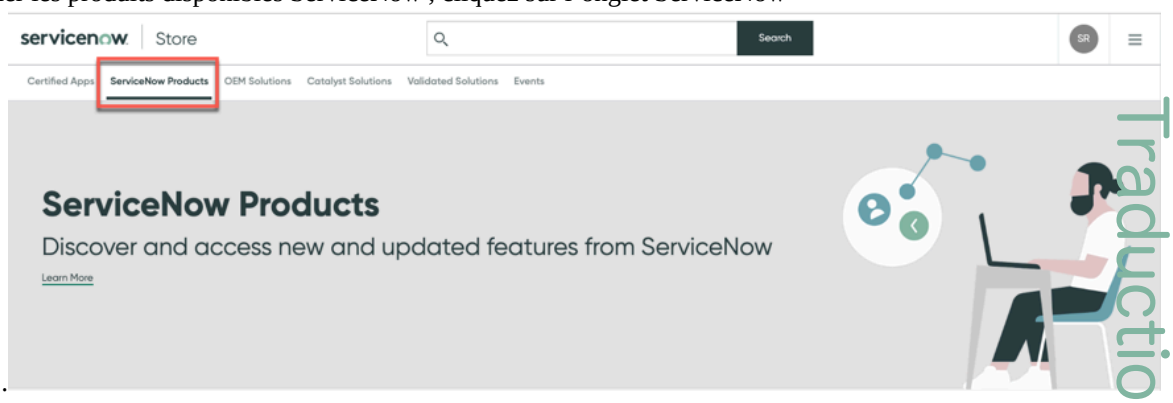
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Action
	d'affectation pour les éléments vulnérables et les tâches de rattrapage. • ServiceNow admin : nécessaire pour installer des applications.

Procédure

1. Accédez au ServiceNow Store.
2. Cliquez sur **Connexion** et saisissez vos informations d'identification HI.
3. Pour afficher les produits disponibles ServiceNow , cliquez sur l'onglet ServiceNow **Produits** .



4. Pour afficher toutes les applications associées auxquelles Recommandations d'affectation de vulnérabilité vous êtes autorisé, cliquez sur le Réponse aux vulnérabilités produit.

   La page répertorie toutes les applications auxquelles vous êtes éligible si vous vous abonnez. Pour en savoir plus sur une application, cliquez sur le lien correspondant à l'application.

5. Pour vérifier que vous avez le droit de Recommandations d'affectation de vulnérabilité, cliquez sur **Adhérer**.
6. Pour accepter les termes et conditions, à l'invite, cochez la case et cliquez sur **Accepter**.
   Un message s'affiche pour indiquer que vous êtes abonné à l'application.
7. Passez à l'étape 10 pour installer l'application sur votre ServiceNow AI Platform instance.
8. **Facultatif :** Si vous souhaitez gérer votre autorisation pour l'application sur d'autres ServiceNow AI Platform instances, cliquez sur **Gérer l'autorisation**Recommandations d'affectation de vulnérabilité.

   Remarque :

   Si le bouton **Gérer le droit** n'est pas affiché, cliquez sur l'application Recommandations d'affectation de vulnérabilité dans la Liste de produits pour l'afficher.

   a. Choisissez une option.

   b. Cliquez sur **OK** ou **sur Annuler** pour continuer.
   Vous pouvez activer les modules d'extension et installer l'application sur vos ServiceNow AI Platform instances.
9. Connectez-vous à l'instance ServiceNow AI Platform sur laquelle vous souhaitez installer l'application Recommandations d'affectation de vulnérabilité .
10. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Dans les applications répertoriées, localisez l'application Recommandations d'affectation de vulnérabilité (sn_vul_recom) et cliquez sur **Installer**.
    La boîte de dialogue d'installation de l'application s'affiche et toutes les dépendances installées s'affichent.
12. **Facultatif :** Si vous souhaitez des données de démonstration, cochez la case **Charger les données de démonstration** et cliquez sur **Installer**.

    Remarque : Si vous ne cochez pas la case **Charger les données de démonstration** , les données de démonstration ne sont pas disponibles pour une installation ultérieure à partir du gestionnaire d'applications. Pour plus d'informations sur l'installation ou la réinstallation des données de démonstration après l'installation initiale, consultez l'article Solution de contournement pour installer les données de démonstration si l'application est déjà installée [KB0722909] dans la base de Now Support connaissances.

    Cette installation peut prendre un certain temps. Un message s'affiche dans la boîte de dialogue Installer une fois l'application et ses dépendances installées.
13. Cliquez sur **Fermer**.
14. Pour configurer Recommandations d'affectation de vulnérabilité, reportez-vous à la section Configurer les recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités.

Configurer les recommandations d'affectation de vulnérabilité pour Réponse aux vulnérabilités

Activez cette option Recommandations d'affectation de vulnérabilité pour réduire le temps que vous consacrez à l'identification des propriétaires des résultats de vulnérabilité non affectés ou mal affectés.

Avant de commencer
Rôle requis : sn_vul.manage_assignment_recom_config

Pourquoi et quand exécuter cette tâche
Cette application n'est pas activée par défaut.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Recommandations d'affectation**.
2. Sélectionnez **Activer les recommandations d'affectation**.
   Le **champ de définition de la solution Intelligence prédictive** s'affiche. La valeur par défaut est **Affectation d'élément vulnérable**.
3. Cliquez sur **Enregistrer**.

Créer et former une définition de solution pour Réponse aux vulnérabilités

Créez et formez un modèle de définition de solution pour Réponse aux vulnérabilités à l'aide de Intelligence prédictive. Vous pouvez utiliser ce modèle pour prédire le groupe d'affectation d'un élément vulnérable (VI) ou d'une tâche de rattrapage (RT) en fonction des données existantes.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intelligence prédictive** > **Classification** > **Définitions des solutions**.
2. Dans le formulaire Définitions de classification, cliquez sur **Affectation d'élément vulnérable**. Il s'agit de la définition de la solution par défaut.

Remarque :

- La fréquence de formation par défaut est de 30 jours. Cela signifie que tous les 30 jours, le modèle se reforme automatiquement à l'aide de l'ensemble de données de VI qui correspond à la condition de filtre configurée.
- Les champs de la table Élément vulnérable peuvent être utilisés pour la formation. La définition de la solution par défaut s'entraîne sur deux champs **VI : Vulnérabilité.Résumé** et **Élément de configuration. Nom**. Vous pouvez personnaliser les champs utilisés pour la formation en fonction des champs que vous trouvez utiles pour prédire la propriété des vulnérabilités dans votre organisation.

3. Pour créer et former la solution de classification, consultez Créer et former une solution de classification .

Remarque : Vous pouvez également créer et former une solution de similarité ou de mise en grappe. Pour en savoir plus, consultez :

- Créez et formez une solution de similarité .
- Créez et formez une solution de mise en grappe .

4. Cliquez sur **Mettre à jour et reformer**.

Remarque : Pour configurer des paramètres avancés pour les solutions ML, consultez Configuration des paramètres avancés pour vos solutions ML .

Créer un Réponse aux vulnérabilités calculateur

Un calculateur de vulnérabilité est une formule prédéfinie permettant de calculer un champ cible lorsque certains critères sont remplis. Les calculateurs, qui calculent le **score** de risque de l'élément vulnérable, peuvent contenir **des règles de risque**.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Remarque : Vous pouvez constater une dégradation des performances lors de l'exécution de calculateurs de vulnérabilité contenant des scripts.

Organisez vos règles pour exécuter d'abord les règles les plus simples et exécutez uniquement des scripts sur les éléments qui ne peuvent pas être traités avec une condition et une valeur de modèle ou une règle de risque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Administration** > **Calculateurs de vulnérabilités**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Formulaire du calculateur de vulnérabilité

Champ	Description
Nom	Le nom du calculateur de vulnérabilité.
Table	Rempli automatiquement avec le nom de la table des éléments vulnérables.
Application	Rempli automatiquement avec Réponse aux vulnérabilités.
Champ cible	Champ à calculer.
Description	Description textuelle du calculateur.
Actif	Allumez ou désactivez la calculatrice.

4. Cliquez avec le bouton droit dans l'en-tête pour **enregistrer**.
   La section **Règles du calculateur de vulnérabilité** s'affiche.
5. Créez une règle pour le calculateur en cliquant sur **Nouveau**.

> **Remarque :** Pour le formulaire **Nouvelles règles de risque** (disponible uniquement lorsque le **champ cible** est **Score de risque**), reportez-vous à l'étape 10.

6. Renseignez les champs comme il convient.

Formulaire Règle du calculateur de vulnérabilité

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur de vulnérabilité. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Rempli automatiquement avec le parent de calculateur.
Actif	Par défaut, la case **Actif** est sélectionnée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Vue avancée	Lorsque cette option est sélectionnée, les conditions de script et les valeurs de script peuvent être sélectionnées à partir du **type de condition** et du **type de valeur**.

7. Renseignez les champs de l'onglet **Quand cette condition est remplie** , le cas échéant.

Quand cette condition est remplie pour l'onglet

Champ	Description
Nom	Nom de la règle du calculateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ordre	Ordre dans lequel exécuter le calculateur de vulnérabilité. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Rempli automatiquement avec le parent de calculateur.
Actif	Par défaut, la case **Actif** est sélectionnée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux éléments vulnérables créés dans le système.
Vue avancée	Lorsque cette option est sélectionnée, sélectionnez les conditions scriptées et les valeurs scriptées dans Type de **condition** et **Type de valeur**.
Type de condition	Disponible lorsque vous sélectionnez la **vue Avancée**. Les choix sont les suivants : ◦ Filtre : utilise des conditions de filtre. ◦ Groupe de filtres : voir Créer un nouveau groupe de filtres pour définir les critères du calculateur. ◦ Script : condition de script utilisée pour déterminer quand appliquer ce calculateur. **Remarque :** Avant d'écrire des scripts pour déterminer quand appliquer les calculateurs, revenez à la liste **des calculateurs de vulnérabilité** . Explorez les enregistrements du calculateur de vulnérabilité fournis avec le système de base.
Condition	Définit les conditions de filtre de base pour déterminer s'il faut utiliser le calculateur ou non. La sélection des types **de conditions de groupe de filtres** ou de **script** masque ce champ. La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.

8. Cliquez sur l'onglet **Définir ces valeurs** et renseignez les champs du formulaire comme il convient.

Onglet Définir ces champs

Champ	Description
Type de valeur	Disponible lorsque vous sélectionnez la **vue Avancée**. Les choix sont les suivants : ◦ Modèle : définissez les valeurs à définir sur chaque champ. ◦ Script : utilisé pour définir les valeurs de chaque champ.
Valeurs de script	Disponible si vous avez sélectionné le type de valeur **Script** . Définit les valeurs auxquelles appliquer les calculs.
Modèle	Sélectionnez les champs et les valeurs que vous souhaitez utiliser pour le calculateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La sélection du type de valeur **de script** masque ce champ.

9. Lorsque vous avez terminé toutes les entrées, cliquez sur **Soumettre**.

   Remarque : Lorsque vous modifiez un calculateur existant et que vous souhaitez mettre à jour tous les scores existants, vous pouvez utiliser le bouton **Réappliquer le calculateur** . Il passe en revue tous les éléments vulnérables (VI) actifs et, si ce calculateur est utilisé pour définir sa valeur, il recalcule la valeur de ces VI. Étant donné que la réapplication d'un calculateur peut prendre beaucoup de temps, une tâche planifiée le gère.

10. Pour le formulaire **Nouvelles règles de risque** , renseignez les champs comme il convient.

    Définissez chaque poids en fonction du pourcentage du résultat qui doit provenir de cette valeur. Pour toutes les données que votre scanner ne fournit pas, ou pour les données qui ne doivent pas faire partie du score de risque, définissez le poids sur zéro.

    Vous pouvez ajouter, supprimer ou mettre à jour les champs. Vous pouvez également configurer le pourcentage de pondération des valeurs de champ. Pour plus d'informations, consultez Définir les champs et les poids de la règle de risque pour les calculateurs de risque de Vulnerability Response.

    Lorsque vous mettez à jour les pondérations, les scénarios affichent les pondérations restantes, ainsi que les résultats du **score de risque** prévus.

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur de vulnérabilité. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Rempli automatiquement avec le parent de calculateur.
Actif	Par défaut, la case **Actif** est sélectionnée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Condition	Définit les conditions de filtre de base permettant de déterminer s'il faut utiliser le calculateur. La sélection des types **de conditions de groupe de filtres** ou de **script** masque ce champ.
Pondérations	
Gravité de la vulnérabilité	Pourcentage du résultat qui provient de la gravité.
Score EPSS de vulnérabilité	Probabilité d'exploitation de la vulnérabilité. Par défaut, le poids de ce critère est de zéro. Si vous souhaitez l'utiliser pour le calcul de votre score de risque, définissez une pondération appropriée par rapport à ce critère.
Existence de l'exploit	Pourcentage du résultat qui provient de l'existence d'un exploit. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.

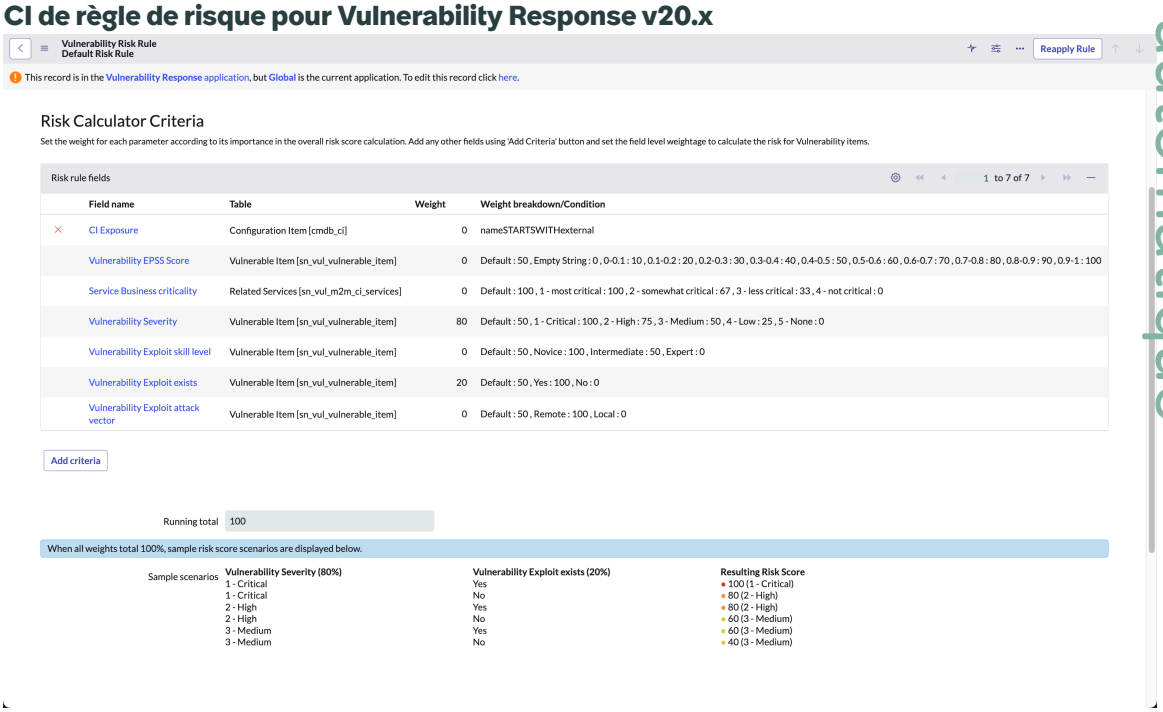
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Niveau de compétence de l'exploit	Pourcentage du résultat qui provient du niveau de compétence requis par l'exploit. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.
Vecteur d'attaque de l'exploit	Pourcentage du résultat qui provient de l'endroit où l'attaque est ciblée. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.
Criticité opérationnelle de service	Pourcentage du résultat qui provient de la criticité opérationnelle. Si vous n'avez pas lié vos CI aux services d'entreprise, définissez la pondération sur zéro.
Exposition CI	Pourcentage du résultat qui provient du fait que le CI est orienté vers Internet. Si le poids n'est pas nul, un filtre de condition apparaît pour définir quel CI est accessible sur Internet. Définissez le filtre pour sélectionner vos éléments de configuration orientés vers Internet. Vous pouvez prévisualiser les enregistrements qui correspondent à la condition.
Exécution totale	Pourcentages totaux calculés automatiquement. Lorsque cette valeur atteint 100, l'aperçu du scénario vous montre des exemples de scores de risque dans différents scénarios.
Scénarios de score de risque	Lorsque tous les poids totalisent 100 %, les scénarios de score de risque s'affichent, fournissant un aperçu du score de risque dans certains des scénarios possibles.

Vous pouvez ajouter ou supprimer des critères, et ajuster le poids de chaque critère à l'aide de la liste incorporée.

CI de règle de risque pour Vulnerability Response v20.x



11. Cliquez sur **Envoyer**.

Désactiver le calculateur de vulnérabilité par défaut s'il n'est pas utilisé

Si vous n'utilisez pas de calculateurs de vulnérabilité, désactivez le calculateur par défaut, en plus de tous les autres que vous avez définis. Les calculateurs de vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

s’exécutent chaque fois qu’un enregistrement d’élément vulnérable est créé ou mis à jour, et peuvent avoir un impact sur les performances d’importation initiales.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Calculateurs de vulnérabilités**.
2. Ouvrez le calculateur correspondant.
3. Décochez la case **Actif** pour désactiver le calculateur.
4. Cliquez sur **Mettre à jour**.

Créer, activer ou modifier des Réponse aux vulnérabilités règles de suppression automatique

Vous pouvez créer, activer ou modifier les règles de suppression d’élément de vulnérabilité (VI) et de suppression de tâche de rattrapage (RT). Utilisez la suppression automatique pour supprimer les enregistrements les plus anciens des tables de VI et RT.

Avant de commencer
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l’application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l’Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l’aide de l’assistant Réponse aux vulnérabilités de configuration. Pour plus d’informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôles requis :

- Administrateur : modifier les règles de suppression automatique
- sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) : afficher le module de suppression automatique

Pourquoi et quand exécuter cette tâche
Au fil du temps, une grande quantité d’enregistrements fermés sont susceptibles de s’accumuler dans les tables VI et VUL de votre instance. Beaucoup de ces dossiers peuvent avoir été fermés pendant plus de 365 jours, mais n’ont pas été supprimés. Utilisez des règles de suppression automatique pour supprimer un grand nombre de ces enregistrements plus anciens et fermés. La suppression de ces enregistrements réduit non seulement considérablement le nombre d’enregistrements dans les tables VI et VUL, mais leur suppression vous aide également à maintenir des performances élevées.

Bien que la suppression automatique cible par défaut les enregistrements fermés depuis 365 jours, la première exécution peut tenter de purger trop d’enregistrements en une seule transaction. En fonction de la taille de votre environnement, vous préférerez peut-être échelonner le processus de suppression pour limiter le champ d’application de la requête. Par exemple, vous pouvez commencer votre première exécution pour les enregistrements fermés de plus de 450 jours. Une fois cette exécution terminée, vous pouvez réduire par incréments plus petits (425, 400, 375) jusqu’à ce que vous ayez réduit le nombre d’enregistrements de plus de 365 jours.

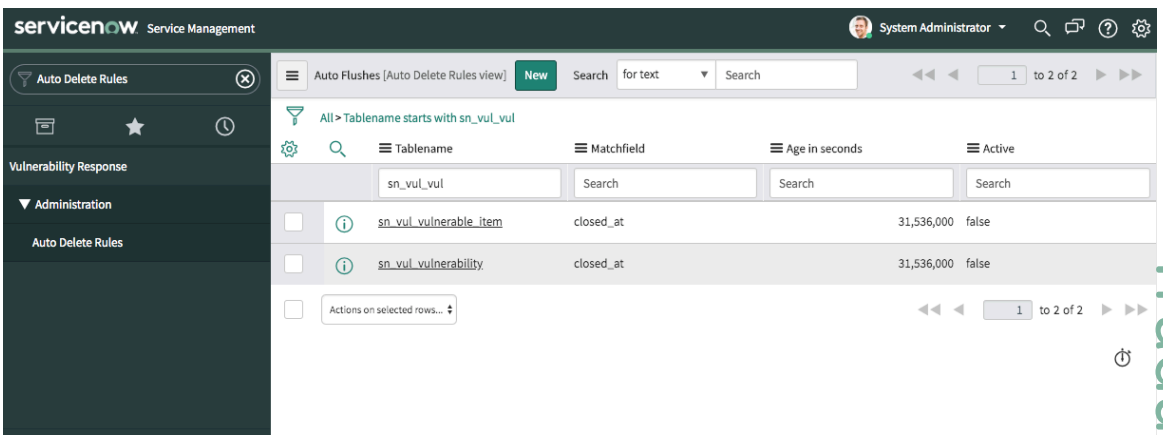
Deux règles fournies avec vous ServiceNow AI Platform® permettent de supprimer automatiquement les enregistrements fermés qui remplissent des conditions spécifiées, ainsi que tous les enregistrements qui s’y réfèrent. Une règle supprime les éléments vulnérables et l’autre règle supprime les tâches de rattrapage. Par défaut, ces règles

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de suppression automatique sont désactivées de sorte que vous devez les activer manuellement avant de supprimer tout enregistrement. Vous pouvez choisir les deux règles préconfigurées fournies avec votre instance ou créer la vôtre.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles de suppression automatique**.
   La vue de liste s'affiche.



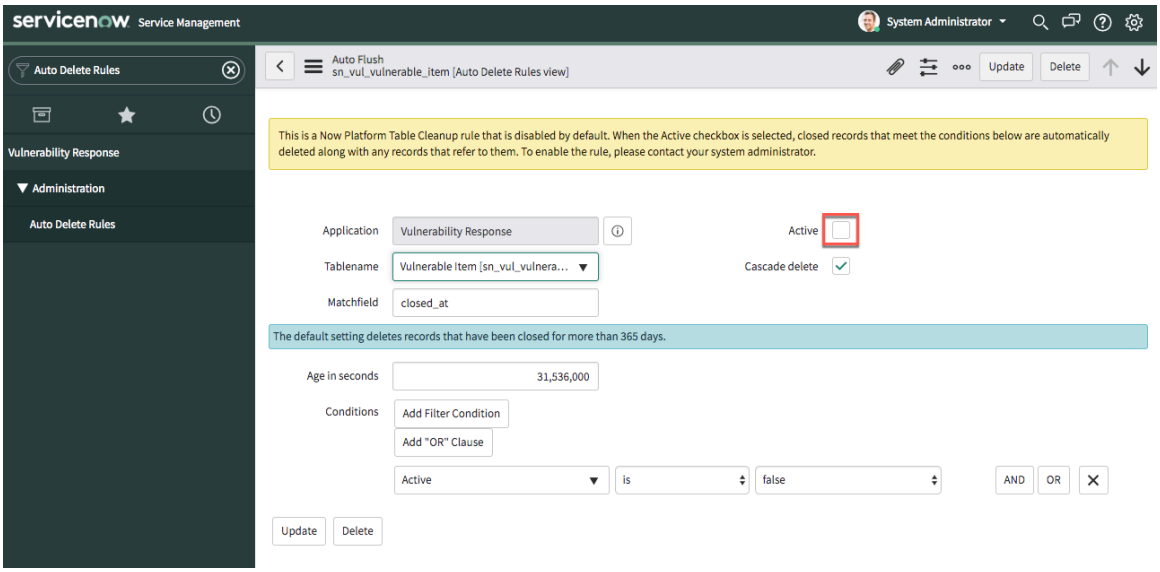
2. Pour modifier, sélectionnez la règle de suppression pour les éléments vulnérables (sn_vul_vulnerable_item) ou la règle pour les tâches de rattrapage (sn_vul_vulnerability).
3. Pour créer une règle, cliquez sur **Nouveau**.
4. Renseignez ou modifiez les champs du formulaire, selon vos besoins.

Champ	Description
Application	Nom de l'application dans laquelle les enregistrements sont supprimés. La valeur par défaut est Vulnerability Response.
Nom de table	Nom de la table pour laquelle la règle est appliquée.
Champ de correspondance	Champ dont le système surveille la durée.
Actif	Option permettant d'activer la règle. Une fois activé, l'enregistrement peut être supprimé.
Suppression en cascade	Option permettant de supprimer tous les enregistrements correspondants, ainsi que tous les enregistrements qui s'y réfèrent. Si cette option n'est pas sélectionnée, seuls les enregistrements correspondants sont supprimés, mais pas les enregistrements qui y font référence.
Âge en secondes	Âge de l'enregistrement de vulnérabilité à supprimer. Pour les règles VI et RT, l'âge est de 365 jours. Cet âge est affiché en secondes.
Conditions	Conditions de filtre définissant les enregistrements dans les tables VI et RT (VUL) auxquelles les règles s'appliquent.

5. Cochez la case **Actif** pour activer une règle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois la règle activée, la fonction horaire de la plateforme, **Effacement automatique**, supprime les enregistrements de la table pour laquelle la règle est activée.

Si votre environnement contient des millions, voire des dizaines de millions, d'enregistrements qui correspondent à vos critères de suppression, vous pouvez consulter ServiceNow l'assistance clientèle avant d'activer les règles de suppression automatique afin de vous aider à supprimer les enregistrements à l'aide d'un processus par étapes.

Ajouter des graphiques de signification de vulnérabilité à la page d'accueil de Vulnerability Response

Vous pouvez ajouter des graphiques de définition de l'importance de la vulnérabilité et d'autres visualisations à la vue d'ensemble.

Avant de commencer

- Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.
- Le module d'extension Analyse de vulnérabilité doit être activé.

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Vue d'ensemble**.
   Certains rapports sont ajoutés par défaut au tableau de bord. Pour en savoir plus sur ces rapports, reportez-vous à la section Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.
2. Près de l'en-tête du tableau de bord, cliquez sur l'icône de vue de carte **Ajouter du contenu** pour ouvrir la boîte de dialogue afin d'ajouter d'autres widgets.
3. Dans les listes de la boîte de dialogue **Ajouter des widgets** , sélectionnez **Rapports** pour afficher d'autres Réponse aux vulnérabilités rapports.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contenu	Options
Détails de la tâche de rattrapage	**Arborescence** > **Importance de la vulnérabilité** > **Importance de la vulnérabilité**
Rapport de score d'importance de la vulnérabilité	**Analyse des performances** > **Score** > **Services avec une importance de vulnérabilité**
Entrée vulnérable	**Rapports** > **Entrée vulnérable** > **Vulnérabilités par impact, score, semaine**
Tâche de remédiation	**Rapports** > **Tâche de remédiation** > **Tâches de remédiation par état de rattrapage**
Élément de tâche de rattrapage	**Rapports** > **Élément de tâche de rattrapage** > **Nouveaux éléments vulnérables**
Exécution de l'intégration de vulnérabilité	**Rapports** > **Exécution de l'intégration de vulnérabilité** > **Doublons Qualys, nouveaux VI, résultats, VI mis à jour, exécutions d'intégration Qualys au cours des 30 derniers jours**
Élément vulnérable	**Rapports** > **Élément vulnérable** > **Une liste complète de filtres d'éléments vulnérables, y compris les VI Qualys ouverts.**.

4. Cliquez sur l'emplacement de l'écran pour lequel vous souhaitez ajouter la jauge.
5. Fermez la zone **Ajouter du contenu** .

Définir les Réponse aux vulnérabilités notifications par e-mail

Configurez des notifications par e-mail pour partager des informations utiles sur les mises à jour et les activités importantes, telles que l'approbation et le rejet de demandes de faux positif. La création d'une notification par e-mail implique de spécifier quand l'envoyer, qui la reçoit et ce qu'elle contient.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Modèles d'e-mail**.
2. Sélectionnez **Nouveau**.

   Pour obtenir des instructions détaillées sur la création de notifications par e-mail, reportez-vous à la section Créer une notification par e-mail .

Résultats

Lorsqu'un destinataire clique sur les liens d'une notification par e-mail, les liens s'ouvrent dans le ou Espace de travail de remédiation IT en fonction de Espace de travail du gestionnaire de vulnérabilités son rôle.

- Des liens s'ouvrent Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs dotés des rôles sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Des liens s'ouvrent Espace de travail de remédiation IT pour les utilisateurs disposant du rôle sn_vul.remediation_owner.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si le destinataire ne possède aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Définir des Réponse aux vulnérabilités modèles d'e-mail

La création d'une notification par e-mail implique de spécifier quand l'envoyer, qui la reçoit et ce qu'elle contient.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Administration** > **Modèles d'e-mail**.
2. Sélectionnez **Nouveau**.

Pour obtenir des instructions détaillées sur la création de modèles d'e-mail, reportez-vous à la section Créer un message électronique avec un modèle .

Créer ou modifier des notifications de cible de rattrapage

Les administrateurs de vulnérabilité peuvent modifier la notification de cible de rattrapage ou en ajouter de nouvelles, en spécifiant quand envoyer la notification, qui reçoit la notification et quel contenu contient la notification.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Notifications**.
2. Sélectionnez l'enregistrement de notification de la cible de rattrapage ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Pour plus d'informations sur les champs de formulaire, consultez Créer une notification par e-mail .
4. Sélectionnez **Afficher l'aperçu** de la notification pour afficher le message.

Résultats

À partir de la version 21.0 de , lorsqu'un Réponse aux vulnérabilités destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités ou Espace de travail de remédiation IT en fonction de son rôle.

- Des liens s'ouvrent Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs dotés des rôles sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Des liens s'ouvrent dans le Espace de travail de remédiation IT pour les utilisateurs disposant des rôles, sn_vul.remediation_owner.

Si le destinataire ne possède aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Configurer l'évaluation de l'exposition à la vulnérabilité

Évaluez l'exposition zero-day (jour actuel) de vos actifs aux logiciels vulnérables avec l'application Vulnerability Exposure Assessment.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Vous pouvez effectuer l'évaluation de l'exposition à l'aide des vulnérabilités et expositions courantes (CVE) et du logiciel pour tirer parti des options supplémentaires de l'espace de travail Évaluation de la vulnérabilité. Pour plus d'informations, consultez Explorer l'espace de travail de l'évaluation de la vulnérabilité.

Rôle requis : admin

Compatibilité et configuration requise

L'application Réponse aux vulnérabilités est disponible sur le ServiceNow Store. L'application Gestion des actifs logiciels (SAM) Foundation [com.snc.asset_management] est installée avec l'application Réponse aux vulnérabilités . Pour vérifier que l'application SAM Foundation est installée sur votre instance, accédez à **Applications système** > **Toutes les applications disponibles** > **Tous** et recherchez com.snc.asset_management. Si l'application n'est pas installée, sélectionnez **Installer**. Pour plus d'informations sur les SAM Foundation, voir Module d'extension Software Asset Management Foundation .

Étant donné que l'application d'évaluation de l'exposition aux vulnérabilités nécessite l'accès aux données d'actif sur votre ServiceNow AI Platform® instance, les applications de gestion des actifs doivent avoir des données à référencer. La table Modèles de détection de logiciels [cmdb_sam_sw_discovery_model] et les installations de logiciels [cmdb_sam_sw_install] exigent des données.

L'application d'évaluation de l'exposition aux vulnérabilités fonctionne également avec les SAM Foundation applications SAM Pro ou SAM ProServiceNow AI Platform®. L'application SAM Pro ne fait pas partie du produit principal Réponse aux vulnérabilités de et ServiceNow Store nécessite un abonnement distinct.

Remarque : L'application SAM Pro n'est requise que pour la bibliothèque de contenu, qui peut produire de meilleurs résultats.

À partir de la version 23.0 de , si vous avez l'abonnement Réponse aux vulnérabilités Pro ou Enterprise, vous serez redirigé vers la page **Évaluation de l'exposition** dans les espaces de travail en fonction de votre rôle en cliquant sur le lien Évaluation de **l'exposition** dans le menu **Tout** :

Accès à la page d'évaluation de l'exposition dans les espaces de travail

Rôle	Espace de travail
Responsable des vulnérabilités	Espace de travail du gestionnaire de vulnérabilité
Gestionnaire d'événements [sn_vul_analyst.vul_event_manager] ou Réponse d'urgence [sn_vul_analyst.emergency_response]	Espace de travail de l'évaluation de la vulnérabilité

Pour éviter d'être redirigé vers les espaces de travail et de rester sur la page Évaluation de l'exposition classique, définissez le **type de lien** sur *Liste des enregistrements dans l'onglet Type de* lien de la page Module - Évaluation de l'exposition. Vous pouvez accéder à la page Module - Évaluation de l'exposition en sélectionnant l'icône **Modifier le module** en regard du lien Évaluation de **l'exposition** dans le menu **Tout** .

Avec le rôle d'écriture de vulnérabilité [sn_vulnerability_write], vous pouvez afficher le module d'évaluation de l'exposition et créer et modifier des enregistrements d'évaluation de l'exposition à la demande pour les logiciels vulnérables dans votre instance avec l'application Réponse aux vulnérabilités .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Évaluez votre exposition aux logiciels vulnérables

Configurer la gestion des exceptions pour Réponse aux vulnérabilités

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive publiée en matière de gestion des vulnérabilités ou de sécurité, vous pouvez demander une exception. La gestion des exceptions implique de demander, de réviser, d'approuver ou de rejeter des exceptions à un élément vulnérable (VI) ou à une tâche de rattrapage (RT) qui ne peuvent pas être corrigées conformément à la politique.

Avant de commencer

Limitez la durée d'une exception demandée et ajoutez un questionnaire à la demande d'exception ou de faux positif à l'aide du Réponse aux vulnérabilités module. Par défaut, une exception est demandée à l'aide du ServiceNow® Réponse aux vulnérabilités module. Vous pouvez également demander une exception à l'aide de l'intégration GRC : Gestion de la politique et de la conformité .

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.manage_exception_configuration

Pourquoi et quand exécuter cette tâche

Si Réponse aux vulnérabilités cette option est activée, vous pouvez limiter la durée pendant laquelle une exception peut être demandée. De même, si le GRC : Gestion de la politique et de la conformité module est installé, vous pouvez sélectionner GRC : Gestion de la politique et de la conformité sur l'écran de configuration. L'activation de cette option vous permet de demander une exception qui spécifie l'objectif de politique et de contrôle à partir de GRC.

Si vous ajoutez un questionnaire, il est envoyé à la personne qui émet la demande d'exception ou de faux positif. Vous pouvez utiliser le questionnaire par défaut ou en créer un en fonction de vos besoins.

Il est utile que l'approbateur d'exceptions comprenne la raison de la demande d'exception.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Configuration de gestion de l'exception, sélectionnez la façon dont vous souhaitez gérer une exception en sélectionnant une option dans la liste **Gérer les exceptions à l'aide** .
   Vous pouvez sélectionner soit Réponse aux vulnérabilités ou GRC : Gestion de la politique et de la conformité. Vous devez activer le module d'extension GRC à utiliser GRC : Gestion de la politique et de la conformité pour demander une exception. La modification de la configuration n'a pas d'impact sur les données existantes.
3. Si vous avez sélectionné l'option Réponse aux vulnérabilités , saisissez les informations suivantes :

Paramètres pour le formulaire de gestion des exceptions VR

Champ	Description
Durée	Période pour laquelle une exception peut être demandée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Unité	Unité de temps pour la période spécifiée.
Activer le questionnaire pour demander une exception	Option permettant d'ajouter un questionnaire à la demande d'exception en cours d'émission.
Questionnaire pour demander une exception	Affiche le questionnaire que vous avez sélectionné pour demander une exception. Le **questionnaire d'exceptions** s'affiche par défaut. **Remarque :** Ce champ s'affiche uniquement lorsque vous cochez la case **Activer le questionnaire pour demander une exception** .
Questionnaire pour le contrôle de compensation	Affiche le questionnaire auquel un propriétaire de rattrapage doit répondre pour les demandes de réduction des risques. À partir de la version 20.0 de , vous pouvez définir un questionnaire pour les demandes de réduction des Réponse aux vulnérabilités risques. Le **questionnaire pour le contrôle de compensation** est sélectionné par défaut. **Remarque :** Ce champ s'affiche uniquement lorsque vous cochez la case **Activer le questionnaire pour demander une exception** .
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Affiche le questionnaire que vous avez sélectionné pour marquer comme faux positif. Le questionnaire pour la demande de faux positif s'affiche par défaut. **Remarque :** Ce champ s'affiche uniquement si la case **Activer le questionnaire pour marquer comme faux positif** est cochée.

Si vous avez personnalisé le questionnaire existant et effectué une mise à niveau vers la version 20.0, ce questionnaire personnalisé s'affiche pour la demande de réduction des risques au lieu du **questionnaire de contrôle de compensation** par défaut.

4. Si vous avez sélectionné l'option GRC : Gestion de la politique et de la conformité , saisissez les informations suivantes :

Paramètres pour le formulaire de gestion des exceptions VR

Champ	Description
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Questionnaire pour marquer comme faux positif	Affiche le questionnaire que vous avez sélectionné pour marquer comme faux positif. Le questionnaire pour la demande de faux positif s'affiche par défaut.

5. Pour configurer des questionnaires basés sur des conditions de demandes d'exception et de faux positifs :

   a. Dans la section Configuration du questionnaire VR, sélectionnez **Nouveau**.

   b. Dans le formulaire Configuration du questionnaire - Nouvel enregistrement, renseignez les champs et sélectionnez **Soumettre**.
   Pour plus d'informations sur les champs du formulaire Configuration du questionnaire, reportez-vous à la section Champs de formulaire de configuration du questionnaire.
   Le questionnaire créé apparaît dans la section Configuration du questionnaire VR du formulaire Paramètres pour la gestion des exceptions VR.

   Par exemple, si vous souhaitez configurer un questionnaire pour les demandes de faux positif pour des éléments vulnérables critiques, sélectionnez la règle d'approbation **Faux positif pour les éléments vulnérables** , fournissez la condition en tant que `cote de risque est 1 - Critique` et sélectionnez le questionnaire souhaité dans le formulaire Configuration du questionnaire .

6. Sélectionnez **Enregistrer**.

Ajouter un approbateur d'exception

Ajoutez des utilisateurs aux groupes d'approbateurs afin de pouvoir demander une exception.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche

Jusqu'à Réponse aux vulnérabilités la version 14.0, une demande d'exclusion électroniquepour un élément vulnérable ou une tâche de rattrapage est approuvée à l'aide du workflow d'approbation à deux niveaux par défaut. La demande doit être approuvée par deux niveaux d'approbateurs.

Remarque : Jusqu'à Réponse aux vulnérabilités la version 14.0, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Toutefois, à partir de la version 15.0, si vous déployez l'application VR pour la première fois, le concepteur de Réponse aux vulnérabilités flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et les faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Groupes**.
2. Dans la colonne Nom, recherchez **Exception**, puis cliquez sur **Approbateur d'exception - Niveau 1**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la Réponse aux vulnérabilités version 12.8.1, vous pouvez utiliser les propriétés système fournies dans le système de base pour les approbations d'exception via workflow dans la table Propriétés système [sys_properties]. Ainsi, lorsqu'une demande d'exception ou de faux positif est émise via le workflow, elle est envoyée pour approbation aux ID de groupe définis dans la propriété système. Accédez à la **Tous** > **Propriétés système** et sélectionnez `sn_vul.exception_approver_L1`, `sn_vul.exception_approver_L2`ou `sn_vul.false_positive_approver_group` pour modifier la valeur de la propriété.

3. Dans le formulaire Approbateur d'exceptions de groupe - Niveau 1, cliquez sur la liste connexe Membres du groupe.
4. Cliquez sur **Nouveau** pour créer une liste.
5. Remplissez les champs du formulaire.

Formulaire d'utilisateur

Champ	Description
ID d'utilisateur	Identificateur unique pour l'utilisateur.
Prénom	Prénom de l'utilisateur.
Nom de famille	Nom de famille de l'utilisateur.
Titre	Fonction de l'utilisateur. Saisissez un titre ou une description de poste, ou sélectionnez-en un dans la liste.
Département	Département de l'utilisateur.
Mot de passe	Mot de passe affecté à l'utilisateur. Ce mot de passe peut être permanent ou temporaire.
Mot de passe à réinitialiser	Option permettant à l'utilisateur de réinitialiser le mot de passe pour garantir la sécurité.
Verrouillé	Option permettant de verrouiller l'utilisateur hors de l'instance et de mettre fin à toutes les sessions actives de l'utilisateur. Le système empêche les utilisateurs ayant le rôle admin de se verrouiller.
Actif	Option pour rendre cet utilisateur actif. Vous seul pouvez voir un utilisateur inactif dans les zones suivantes : ○ Listes d'utilisateurs ○ Liste de sélection sur les champs de référence (icône de loupe) ○ Liste de saisie semi-automatique qui s'affiche lorsque vous tapez dans un champ de référence
Accès au service Web uniquement	Option permettant de désigner cet utilisateur comme utilisateur non interactif.
Utilisateur d'intégration interne	Option permettant de désigner cet utilisateur comme utilisateur d'intégration interne.
E-mail	Adresse e-mail de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Langue	Langue préférée de l'utilisateur.
Intégration du calendrier	Calendrier utilisé pour gérer le calendrier de travail. Par exemple, Outlook.
Fuseau horaire	Fuseau horaire de l'emplacement de cet utilisateur.
Format de date	Format préféré de l'utilisateur pour les dates.
Tél. professionnel	Téléphone professionnel de l'utilisateur.
Tél. mobile	Téléphone mobile de l'utilisateur.
Photo	Photo que vous pouvez télécharger en cliquant sur **Cliquez pour ajouter...**.

6. Cliquez sur **Envoyer**.
7. Répétez les étapes 1 à 5 pour créer un approbateur d'exceptions - Niveau 2.
   L'approbateur doit accéder à **Réponse aux vulnérabilités** > **Mes approbations et approuver les demandes** .

> **Remarque :** Pour approuver une exception pour GRC : Gestion de la politique et de la conformité, reportez-vous à la configuration facultative de Policy and Compliance Management .

Configurer les règles d'approbation pour la gestion des exceptions

Réponse aux vulnérabilités À partir de la version 15.0, utilisez le concepteur de flux pour approuver les demandes d'exception pour la gestion des exceptions, les règles d'exception et la gestion des faux positifs. Si vous déployez Réponse aux vulnérabilités (VR) pour la première fois, Flow Designer est activé par défaut.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Si vous êtes un utilisateur VR existant, l'option par défaut est le workflow.
Si vous avez déployé Réponse aux vulnérabilités la version 15.0 ou ultérieure, la valeur de la propriété *sn_vul.flow_designer_activation* système est définie sur vrai. Cela signifie que Flow Designer est activé par défaut.

Si vous utilisez déjà une version Réponse aux vulnérabilités antérieure à la version 15.0, la valeur de cette propriété système est définie sur faux. Vous pouvez activer le concepteur de flux en changeant la valeur en vrai.

> **Remarque :** Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer. Pour une comparaison détaillée entre le workflow et Flow Designer, reportez-vous à la section Comparaison du workflow de gestion des exceptions et du concepteur de flux.

Pour utiliser Flow Designer, créez des règles à l'aide du module Règles d'approbation. À l'aide de ce module, vous pouvez configurer des règles d'approbation pour chacun des workflows de gestion des exceptions suivants.

- Demande d'exception pour les tâches de rattrapage
- Demande d'exception pour les éléments vulnérables
- Règle d'exception

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Faux positif pour les tâches de remédiation
- Faux positif pour les éléments vulnérables

Remarque : Vous pouvez également définir des conditions contenant plusieurs niveaux d'approbation dans une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant. Pour plus d'informations sur la configuration des niveaux d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.
2. Sur la page Règles d'approbation, sélectionnez le groupe pour lequel vous souhaitez définir la règle d'approbation.
3. Remplissez les champs du formulaire.

Formulaire Règle d'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Table	Table sur laquelle la règle est appliquée.
Application	La valeur par défaut est Réponse aux vulnérabilités.
Type de règle	Spécifie le type de règle. Par exemple, gestion des exceptions, faux positifs ou règle d'exception.
Actif	Activé par défaut, ce qui signifie que la règle d'approbation est utilisée.
Description	Brève description des règles d'approbation.
Expirationde l'approbation (jours) À partir de la version 21.0 de Réponse aux vulnérabilités	Date jusqu'à laquelle l'approbateur peut approuver la demande.
Notification de l'approbateur (jours) À partir de la version 21.0 de Réponse aux vulnérabilités	Date après laquelle l'approbateur est notifié pour effectuer des actions.

4. Sélectionnez **Mettre à jour**.
   Dans l'onglet Configurations d'approbation, deux niveaux d'approbateurs sont configurés par défaut. Vous pouvez sélectionner une règle pour définir les conditions en fonction de différents cas d'utilisation au sein d'une règle. Pour plus d'informations, consultez Créer des configurations pour une règle d'approbation.

Remarque : Dans chaque page de configuration, vous pouvez créer plusieurs niveaux d'approbation. Pour plus d'informations, consultez Créer des niveaux d'approbation pour la gestion des exceptions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example:
En fonction de différents cas d'utilisation, vous pouvez définir différents processus d'approbation pour les mêmes vulnérabilités trouvées dans différents éléments de configuration.

Créer des configurations pour une règle d'approbation

Définissez les conditions de filtrage des éléments vulnérables, des tâches de rattrapage ou des règles d'exception correspondants pour un niveau d'approbation.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Dans le module Configurations d'approbation, vous pouvez configurer plusieurs niveaux d'approbation pour différentes configurations. Définissez des règles basées sur des conditions, chaque règle contenant plusieurs niveaux d'approbation.

Remarque : Utilisez le module Règles d'approbation pour configurer les règles d'approbation pour les workflows de gestion des exceptions. Pour plus d'informations sur la configuration des règles d'approbation, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.
2. Sélectionnez une règle d'approbation et accédez à l'onglet **Configurations d'approbation** .
3. Sélectionnez une configuration.
4. Remplissez les champs du formulaire.

Formulaire de configuration de l'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Règle d'approbation	Contient les détails de la table et du type pour la règle d'approbation.
Ordre	Ordre d'exécution de diverses configurations au sein d'une règle. Par exemple, une configuration avec une entrée de commande de 100 est exécutée avant une configuration avec une entrée de commande de 200.
Actif	Activé par défaut, ce qui signifie que la configuration de l'approbation est utilisée.
Description	Brève description des niveaux de configuration de l'approbation.

5. Définissez une condition pour les éléments vulnérables ou les tâches de rattrapage de l'une des façons suivantes :

Champ	Description
Condition	Identifie les éléments vulnérables ou les tâches de rattrapage correspondants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Condition avancée	Script qui définit la condition des éléments vulnérables ou des tâches de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous cochez la case **Avancé** .

6. Sélectionnez **Mettre à jour**.

Vous pouvez définir des conditions contenant plusieurs niveaux d'approbation dans une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant. Pour plus d'informations sur la configuration des niveaux d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions.

Example:

Vous pouvez définir différents chemins d'approbation pour :

- Exemple 1 : Différents types de vulnérabilités ou d'éléments de configuration (accessibles sur Internet ou internes).
- Exemple 2 : demandes de report et de réduction des risques lorsqu'un propriétaire de rattrapage émet ces demandes simultanément pour des éléments vulnérables d'hôte (VIT) ou des tâches de rattrapage (VUL).

La colonne Approbation de changement contient les enregistrements d'approbation de changement de l'état du report. Lorsque vous définissez une condition dans la colonne Approbation de changement à l'aide du créateur de conditions, l'enregistrement de l'approbation de report est pris en compte, mais pas l'enregistrement de l'approbation de réduction des risques. Ainsi, pour définir la condition sur l'enregistrement d'approbation de changement d'état de réduction du risque, utilisez le champ **Condition avancée** .

Pour la règle d'approbation **Demande d'exception pour les éléments vulnérables** , la configuration **d'approbation Demande de cote de risque de moyen à faible** est fournie avec le système de base. Cette configuration est définie sur false par défaut. Vous pouvez utiliser cette configuration pour définir un chemin d'approbation pour les demandes de réduction des risques, de Moyen à Faible. Vous pouvez également mettre à jour le script dans cette configuration afin qu'il soit applicable pour divers changements de cote de risque dans les demandes de réduction des risques.

Demander une cote de risque de configuration moyenne à faible :

```
function evaluate() {
   var gr = new GlideRecord("sn_vul_change_approval");
   gr.addQuery("sys_id", approval);
   gr.addQuery("current_value", "3 - Medium");
   gr.addQuery("desired_value", "4 - Low");
   gr.query();
   if (gr.next()) {
      return true;
   }
   return false;
}
evaluate();
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définissez la configuration précédente sur vrai avec l'ordre le plus bas et définissez la **configuration par défaut : demande d'exception pour** la configuration VI sur vrai.

Résultat : lorsqu'un propriétaire de rattrapage émet simultanément des demandes de report et de réduction du risque à partir de l'espace de travail de remédiation informatique, les demandes d'approbation de report sont redirigées vers les approbateurs définis dans la **configuration par défaut : demande d'exception pour** VI et les demandes d'approbation de réduction du risque sont redirigées vers les approbateurs définis dans la **demande de cote de risque de moyenne à faible** .

Créer des niveaux d'approbation pour la gestion des exceptions

Définissez les niveaux d'utilisateurs et les groupes d'utilisateurs qui vont approuver les demandes d'exception.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.
2. Sélectionnez une règle d'approbation et accédez à l'onglet **Configurations d'approbation** .
3. Sélectionnez une configuration.
4. Dans la section Niveaux de l'approbateur, sélectionnez un niveau d'approbateur.
5. Remplissez les champs du formulaire.

Formulaire Niveau d'approbateur

Champ	Description
Nom	Nom du niveau d'approbation.
Approbation requise	Sélectionnez le nombre d'approbations requises pour le niveau sélectionné : ○ Un approbateur requis ○ Approbation de tous les utilisateurs requise
Actif	Activé par défaut, ce qui signifie que le niveau d'approbation est utilisé.
Ordre	Ordre d'exécution de diverses configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 s'exécute avant une configuration avec une entrée d'ordre de 200.
Règle d'approbation	Contient les détails de la table et du type pour la règle d'approbation.
Configuration de l'approbation	Contient les configurations d'approbation.
Affecter à l'aide de	Sélectionnez une option dans : ○ Utilisateur et groupe d'utilisateurs ○ Champ de la table des approbations ○ Script

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Groupes	Groupe au niveau de l'approbateur composé de plusieurs utilisateurs. L'utilisateur doit disposer de l'un des rôles suivants : ○ sn_vul.exception_approver : pour la gestion des exceptions et les règles d'exception ○ sn_vul.false_positive_approver : pour les faux positifs
Utilisateurs	Modifiez les utilisateurs répertoriés dans les groupes.

6. Pour enregistrer les changements, sélectionnez **Mettre à jour**.

Remarque : Avant la version 15.0, le processus de workflow était fonctionnel s'il n'y avait que des utilisateurs au niveau d'exception 1. Cependant, à partir de la version 15.0, il doit y avoir au moins un utilisateur dans chaque niveau.

Avant la version 15.0, dans le workflow, s'il n'y avait pas d'utilisateur dans le deuxième niveau, l'élément de vulnérabilité ou le groupe vulnérable était reporté. Toutefois, à partir de la version 15.0, s'il n'y a pas d'utilisateur dans le deuxième niveau, la demande d'approbation est automatiquement rejetée.

Example:
Il peut y avoir différents niveaux d'approbation des vulnérabilités pour les serveurs Linux et Windows.

Comparaison du workflow de gestion des exceptions et du concepteur de flux

Réponse aux vulnérabilités À partir de la version 15.0, si vous déployez Réponse aux vulnérabilités (VR) pour la première fois, le concepteur de flux pour l'approbation des demandes d'exception dans la gestion des exceptions est activé par défaut. Si vous êtes un utilisateur VR existant, l'option par défaut est le workflow.

Remarque : Réponse aux vulnérabilités À partir de la version 19.0, seul Concepteur de flux est pris en charge pour les nouveaux clients. Si vous êtes un utilisateur existant et que vous effectuez une mise à niveau vers Réponse aux vulnérabilités la version 19.0, le concepteur de flux et le workflow de gestion des exceptions sont pris en charge.

Comparaison entre Workflow et Flow Designer

Considérations	Workflow	Flow Designer
Version	Avant la version 15.0 de Réponse aux vulnérabilités.	À partir de la v15.0 de Réponse aux vulnérabilités.
Option par défaut	Option par défaut si vous êtes un utilisateur VR existant.	Option par défaut pour les nouveaux utilisateurs de VR à partir de la v15.0.
Définition du processus d'approbation	La gestion des exceptions inclut les demandes d'exception et de faux positifs ainsi que les règles d'exception.	Inclut la définition de différents niveaux et l'ajout d'approbateurs différents pour différents cas d'utilisation. Plus facile à mettre en œuvre que le workflow. La gestion

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparaison entre Workflow et Flow Designer (suite)

Considérations	Workflow	Flow Designer
		des exceptions inclut les demandes d'exception et de faux positifs ainsi que les règles d'exception.
Mise à niveau vers Flow Designer	Vous pouvez effectuer une mise à niveau vers Flow Designer à partir du workflow. Toutefois, les demandes existantes ne peuvent être approuvées qu'à l'aide du workflow.	Flow Designer est activé par défaut.
Propriété système `sn_vul.flow_designer_activation`	Si vous avez utilisé le workflow pour la gestion des exceptions avant la version 15.0, la propriété système est définie sur false. Pour activer Flow Designer, définissez cette propriété sur vrai. **Remarque :** Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer.	Si vous utilisez VR pour la première fois pour la version 15.0 ou ultérieure, la valeur de propriété système est définie sur vrai par défaut.
Module Règles d'approbation	Une fois la propriété système définie sur true, la tâche planifiée **Activer les règles d'approbation de module** s'exécute dans les 24 heures. Cette tâche planifiée active le module **Règles d'approbation** . Pour activer ce module instantanément, exécutez cette tâche manuellement.	Si vous avez déployé VR pour la première fois à partir de VR v15.0, ce module est disponible par défaut.
Niveaux d'approbation	Permet de définir uniquement deux niveaux d'approbateurs.	Fournit plusieurs options telles que la définition d'un nombre quelconque de configurations, de niveaux d'approbateurs et l'ajout dynamique d'approbateurs pour chaque règle.

Traduction automatique

Ajouter un approbateur faux positif

Seuls les utilisateurs ajoutés au groupe d'approbateurs de faux positifs peuvent approuver les faux positifs pour les éléments vulnérables (VI) et les tâches de rattrapage (VUL). L'octroi d'un faux positif est un processus d'approbation à un seul niveau.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

À partir de Vulnerability Response v15.0, si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et les faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tous** > > **Administration utilisateurs** > **Groupes**.
2. Dans la colonne **Nom** , recherchez **Faux positif** et cliquez sur l'option.
3. Dans le formulaire Groupe, accédez à **Membres du groupe** > **Nouveau** (ou **Modifier**).
4. Dans le formulaire Utilisateur, créez un enregistrement en saisissant les détails de l'utilisateur, puis cliquez sur **Soumettre**.
   Tous les rôles sont accordés à l'utilisateur. Les utilisateurs sélectionnés sont ajoutés à la liste Membres du groupe. Ces membres peuvent approuver les demandes de marquage de VI ou de tâches de rattrapage comme faux positifs. Une fois approuvé, l'état de l'enregistrement est mis à jour sur Fermé et il n'est rouvert qu'à la date spécifiée.

Configurer le questionnaire pour la réduction des risques

Réponse aux vulnérabilités À partir de la version 20.0, vous pouvez personnaliser le questionnaire de la demande de réduction des risques pour un ensemble d'éléments vulnérables filtrés ou de tâches de rattrapage.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Le **questionnaire pour les contrôles de compensation pour les éléments vulnérables** et le **questionnaire pour les contrôles de compensation pour** les règles d'approbation des groupes vulnérables sont envoyés avec le système de base.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Paramètres de gestion des exceptions VR, cochez la case Activer le questionnaire pour demander une exception.
3. Pour configurer des questionnaires basés sur des conditions pour les demandes de réduction des risques :

   a. Dans la section Configuration du questionnaire VR, sélectionnez **Nouveau**.

   b. Dans le formulaire Configuration du questionnaire : nouvel enregistrement, sélectionnez la règle d'approbation **Questionnaire pour les contrôles de compensation pour les groupes vulnérables** ou **Questionnaire pour les contrôles de compensation pour les éléments vulnérables** et fournissez la condition.

   c. Sélectionnez le questionnaire souhaité, puis sélectionnez **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les champs du formulaire Configuration du questionnaire, reportez-vous à la section Champs de formulaire de configuration du questionnaire.
Le questionnaire créé apparaît dans la section Configuration du questionnaire VR du formulaire Paramètres pour la gestion des exceptions VR.

4. Sélectionnez **Enregistrer** dans le formulaire Paramètres de gestion des exceptions VR.

Afficher les SLA de Vulnerability Response pour les tâches de remédiation

Pour vous assurer que les éléments vulnérables sont traités correctement, vous pouvez définir un accord sur les niveaux de service (SLA) pour Réponse aux vulnérabilités les tâches de rattrapage.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche
Les définitions de SLA de cette liste sont un sous-ensemble de la liste SLA de la plateforme, spécifique à Réponse aux vulnérabilités.

Pour obtenir des instructions, consultez Créer une définition de SLA .

Si vous suivez le temps nécessaire pour corriger les VI, vous préférerez peut-être utiliser Réponse aux vulnérabilités Règles de cibles de rattrapage. Les règles de cibles de rattrapage définissent les délais prévus pour le rattrapage des éléments vulnérables (VI) spécifiquement dans le contexte de Vulnerability Response, tandis que les SLA peuvent fournir un délai pour le rattrapage de la vulnérabilité elle-même.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Définitions de SLA**.
2. Cliquez sur une définition.
   Les SLA de tâche sont affichés dans les listes connexes des **tâches de rattrapage**.

Configurer WatchDog

Utilisez la page de configuration Watchdog pour créer de nouveaux chiens de garde ou mettre à jour les chiens de garde existants avec les conditions que vous voulez spécifier. Vous pouvez activer la notification pour chaque chien de garde et recevoir une notification lorsque les conditions sont remplies.

Avant de commencer
Rôle requis : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **WatchDog** > **Configuration**.
2. Sélectionnez l'organisme de surveillance que vous souhaitez implémenter.
3. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire d'intégration Watchdog

Champ	Description
Nom	Nom du chien de garde.
Actif	Cochez la case *true* pour activer le chien de garde.
Type de condition	Choisissez entre Filtre ou Script.
Condition avancée	Ce champ s'affiche uniquement lorsque le script est sélectionné à partir du type Condition.
Table	Sélectionnez la table pour exécuter la condition de surveillance.
Condition	Condition d'évaluation du chien de garde.
Notification	Case à cocher pour notifier les groupes ou les utilisateurs si la condition de chien de garde est remplie.
Utilisateurs	Liste des utilisateurs à informer si la condition de chien de garde est remplie.
Groupes	Groupe à informer si la condition de chien de garde est remplie.
Journal de surveillance	
Chien de garde	Référence à la table de surveillance.
Nombre	Nombre d'enregistrements qui répondent aux critères de surveillance.
Notes	Remarques supplémentaires pour les journaux de surveillance.

4. Sélectionnez **Mettre à jour**.

Configurer le nombre maximal de lignes dans la liste connexe

Contrôlez le nombre de lignes qui apparaissent dans les listes connexes pour réduire le temps de chargement et améliorer la lisibilité et les performances dans Vulnerability Response (VR), Configuration Compliance (CC), Cloud Vulnerability Response (CVR) et Application Vulnerability Response (AVR). Les listes connexes affichent les enregistrements associés, tels que les CI affectés, les résultats ou les tâches de rattrapage, afin que vous puissiez accéder rapidement aux détails pertinents sans quitter le formulaire.

Avant de commencer

Rôle requis : sn_vul_cmn.admin

Procédure

1. Accédez à la **Tous** > **sys_properties. LISTE**.
2. Recherchez et ouvrez la propriété : *sn_vul_cmn.related_list.set_max_row*
3. Dans le champ Valeur, entrez l'une des options suivantes :
   - Nombre entier positif : affiche ce nombre de lignes dans chaque liste connexe.
   - Nombre entier négatif : entrée ou valeur non valide ignorée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vide (aucune valeur) : affiche toutes les lignes.

Remarque : Afficher plus de 100 lignes affecte les performances.

4. Sélectionnez **Mettre à jour** pour appliquer les changements.

Résultats

Après avoir mis à jour la propriété système, les listes connexes suivantes reflètent la limite de lignes configurée :

Dans l'interface utilisateur classique

- CI affectés
- Conclusions de l'image
- Éléments en double potentiels
- Solutions potentielles
- Solutions privilégiées
- Tâches de remédiation
- Éléments vulnérables

Dans l'interface utilisateur de l'espace de travail

- Solutions potentielles
- CI affectés
- Applications affectées
- Images de Docker affectées

Tâches de configuration avancée Réponse aux vulnérabilités

Les tâches de configuration suivantes nécessitent un codage ou une expertise avancée ServiceNow et ne sont pas considérées comme faisant partie de la configuration de base.

Vous préférerez peut-être effectuer ces tâches uniquement si vous avez une expérience avancée du codage ou si vous avez une connaissance approfondie du ServiceNow AI Platform.

Créer des importations séparées par domaine pour une intégration

Si vous souhaitez que les données importées se trouvent dans un domaine spécifique, l'utilisateur affecté à l'exécution des intégrations doit appartenir à ce domaine.

Avant de commencer

Rôle requis :
import_admin et le rôle d'intégration Configurer pour votre intégration spécifique, par exemple, sn_vul.configure_r7_integration ou sn_vul_tenable.configure_integration.

Pourquoi et quand exécuter cette tâche

Cet ensemble de tâches nécessite du codage ou une expertise avancée ServiceNow .

Les files d'attente d'importation contiennent des pièces jointes de données traitées par les travaux planifiés (intégrations). Dans un environnement séparé par domaine, vous devez faire correspondre la tâche planifiée avec la file d'attente d'importation correcte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Créez un domaine.
2. Pour chaque domaine que vous créez, créez un utilisateur et affectez-le à ce domaine.

   Considérez cet utilisateur comme un espace réservé **run_as** pour le domaine dans votre intégration de vulnérabilité. C'est l'équivalent de la **VR. Utilisateur système** dans le domaine global. Cet utilisateur doit accéder aux sources de données, aux cartes de transformation et aux données de vulnérabilité.

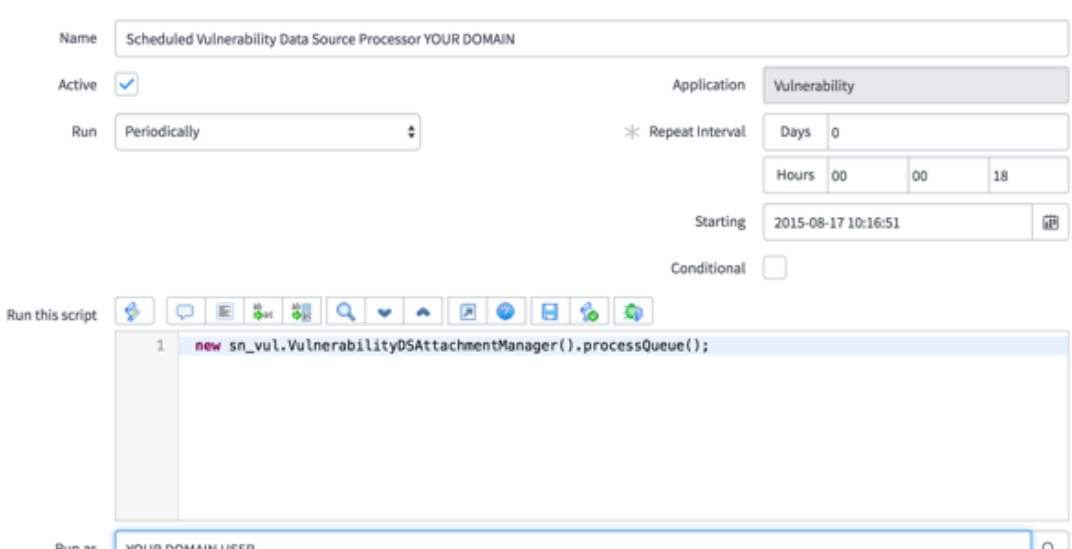
   Remarque : N'utilisez pas cet utilisateur à d'autres fins.

3. Créer une tâche planifiée dans chaque domaine.
   Pour plus d'informations sur les précautions et les paramètres supplémentaires, reportez-vous à la section Paramètres supplémentaires pour la séparation de domaine.

   a. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés**.

   b. Copiez le **processeur de source de données de vulnérabilité planifiée** dans le domaine.

   c. Pour identifier la tâche planifiée, ajoutez le domaine au nom.



   d. Dans le champ **Exécuter en tant que** , remplacez l'utilisateur **run_as** par l'utilisateur que vous avez créé à l'étape 2.

   À partir de la version 20.1 de Réponse aux vulnérabilités, les changements de script suivants sont fournis avec le système de base.

4. **Remarque :** Modifiez l'action d'interface utilisateur suivante afin que l'intégration s'exécute dans le domaine de l'utilisateur **run_as** .

   Modifiez l'action d'interface utilisateur **Exécuter maintenant** dans la tâche d'intégration de l'intégration de la **détection d'hôte Qualys** pour ajouter ce bloc de code en haut du fichier.

Traduction automatique

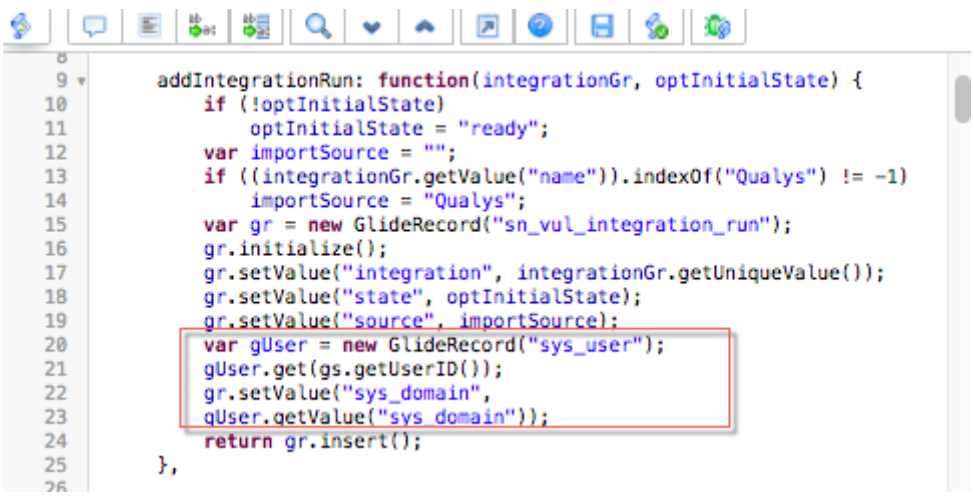
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

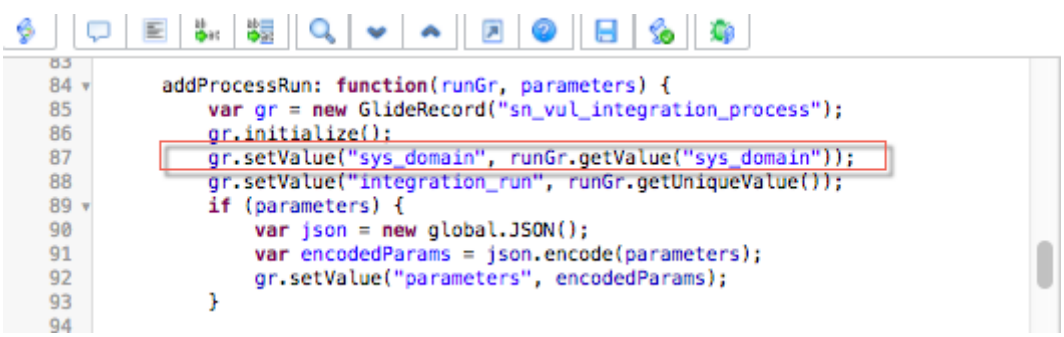
5. **Remarque :** Modifiez les includes de script suivants afin que l'intégration s'exécute dans le domaine de l'utilisateur **run_as** .

   Modifier la méthode d'include de script **VulnerabilityIntegrationUtils** , **addIntegrationRun** , pour ajouter le code en surbrillance



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Modifiez la méthode d'include de script **VulnerabilityIntegrationUtils** , **addProcessRun** pour ajouter le code en surbrillance dans l'image suivante.
   Code addProcessRun



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

7. Modifiez la méthode d'include de script **VulnerabilityIntegrationUtils** , **copyProcess** pour ajouter le code en surbrillance dans l'image suivante.
   copieTraiter le code

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Script

```
325
326     _copyProcess: function(intProcGr, isProcessErrored) {
327         var copy = new GlideRecord('sn_vul_integration_process');
328         copy.initialize();
329         copy.setValue('integration_run', intProcGr.getValue('integration_run'));
330         copy.setValue('parameters', intProcGr.getValue('parameters'));
331         copy.setValue('state', 'new');
332         copy.setValue('notes', '');
333         copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
334         if (isProcessErrored) {
335             copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
336             var nextRetryDueOn;
337             if (intProcGr.getValue('next_retry_due_on') != '')
338                 nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
339             else
340                 nextRetryDueOn = new GlideDateTime();
341
342             var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
343             var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
344             nextRetryDueOn.addSeconds(nextRetryDelay * 60);
345             if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
346                 copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
347         } else
348             copy.setValue('retries', intProcGr.retries + 1);
349
350         copy.insert();
351         return copy;
352     },
```

8. Modifiez la méthode d'include de script **DataSourceVulnReportRefreshProcessor_processFromDataSourceGroups** pour modifier ce code d'origine :
Code _processFromDataSourcesGroups d'origine

```
23
24     _processFromDataSourceGroups: function(payload, fileName) {
25         var gr = new GlideRecord("sn_vul_int_data_src");
26         gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27         gr.orderBy("ds_group_number");
28         gr.orderBy("last_used");
29         gr.query();
30         var lastGroup;
31         if (gr.getRowCount() == 0) {
32             throw new Error("There are no data sources to provide data to.");
33         }
34         while (gr.next()) {
35             var thisGroup = gr.getValue("ds_group_number");
36             if (lastGroup == thisGroup && lastGroup !== undefined) {
37                 continue;
38             } else {
39                 var ds = new GlideRecord("sys_data_source");
40                 if (!ds.get(gr.sys_data_source + ""))
41                     continue;
42
43                 var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                 mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                 gr.setValue("last_used", new GlideDateTime().getValue());
46                 gr.update();
47                 lastGroup = thisGroup;
48             }
```

À :

Code _processFromDataSourcesGroups modifié

```
43                 var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                 mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                 gr.setValue("last_used", new GlideDateTime().getValue());
46                 gr.update();
47                 lastGroup = thisGroup;
```

9. Modifiez la méthode d'include **de script VulnerabilityDSAttachmentManager** , **queueItem** pour ajouter les blocs de code en surbrillance suivants
élément de file d'attente

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.initialize();
    gr.setValue("status", "NEW");
    gr.setValue("data_source", dataSource);
    if (optIntegrationProcess)
        gr.setValue("integration_process", optIntegrationProcess);
    if(optDomain){
            gr.setValue("sys_domain", optDomain);
    }
    var sysId = gr.insert();
```

_getNext

```
_getNext: function() {
    // First go through the retries, if any
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    var sysDomainUser = gUser.getValue("sys_domain");
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "RETRY");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.orderBy("queued_on");
    gr.query();
    if (gr.next()) {
        return gr;
    }

    // Then handle the regular queued items
    gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "QUEUED");
    gr.orderBy("queued_on");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.query();
    if (gr.next()) {
        return gr;
    }
```

Fonction _processQueueEntry

```
_processQueueEntry: function(entry) {
    var schedGrId = this._getScheduledImportSet(entry.data_source);
    if (gs.nil(schedGrId)) {
        return;
    }

    var dataSourceGr = new GlideRecord("sys_data_source");
    if (!dataSourceGr.get(entry.data_source)) {
        gs.warn("Non existent data source - marking as complete");
        entry.setValue("status", "COMPLETE");
        entry.setValue("processing_notes", "Data source does not exist, could not process.");
        entry.update();
        return;
    }

    try {
        this._deleteDataSourceAttachments(entry.data_source);
        if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
            gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue
entry " + entry.sys_id);
            throw "Attachments not deleted";
        }
        var attachmentApi = new GlideSysAttachment();
        attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
        var schedGr = new GlideRecord("scheduled_import_set");
        schedGr.get(schedGrId);
        schedGr.setValue("data_source", entry.data_source);
        schedGr.setValue("run_as", gs.getUserID());
        schedGr.update();
```

À ce stade, vous êtes prêt pour les importations séparées par domaine.

Remarque : Si vous avez plusieurs déploiements d'une Réponse aux vulnérabilités intégration OU Réponse aux vulnérabilités des applications , répétez ce processus pour chaque déploiement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer et prendre en charge plusieurs domaines dans le cadre des tâches en arrière-plan

Les tâches en arrière-plan des produits Vulnerability Response sont conçues pour s'exécuter pendant de longues périodes afin d'exécuter plusieurs processus sur vos enregistrements. Les processeurs de tâches en arrière-plan sont fournis avec le système de base et s'exécutent via l'utilisateur système et créent des enregistrements dans le domaine global.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Administrateur de domaine** > **Domaines**.
2. Créez un domaine.

   Pour en savoir plus sur la création d'un domaine, reportez-vous à la section Créer un domaine .

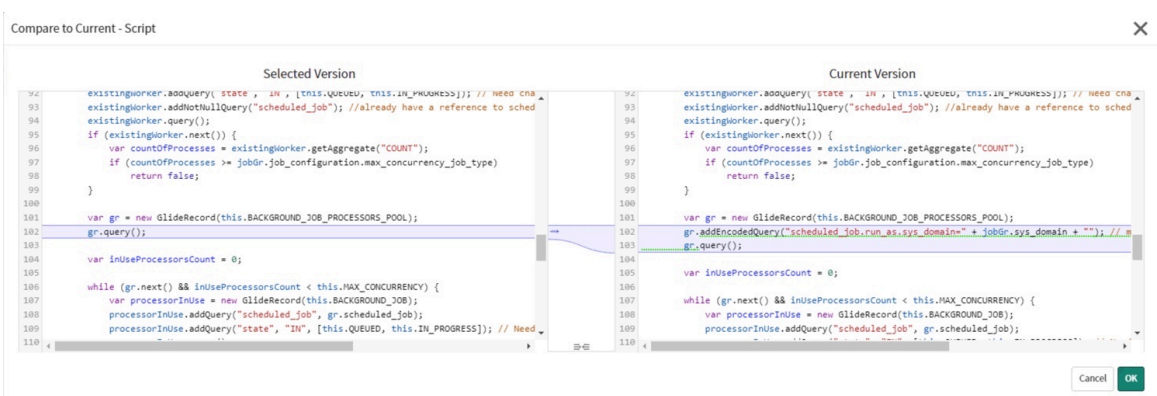
   Pour chaque domaine créé, créez un utilisateur et affectez-le au domaine. Supposons que cet utilisateur soit un espace réservé run_as pour le domaine. C'est l'équivalent de la réalité virtuelle. Utilisateur système dans le domaine global. Cet utilisateur doit accéder aux données de vulnérabilité.
3. Modifier l'run_as des travaux *`Scheduled Background Job Manager`* planifiés , et *`Close the parent background job`*.

   Si vous avez créé plusieurs domaines, dupliquez cette tâche et changez run_as'utilisateur en conséquence. Vous pouvez également conserver une copie des tâches précédentes avec l'utilisateur run_as du domaine global en mode inactif.

   Dix tâches de processeur (par exemple, *`Background job processor 10`*) sont fournies avec le système de base. Changez l'exécution à partir de ces tâches pour l'utilisateur séparé par domaine. Si plusieurs domaines sont présents, deux tâches par domaine suffisent, mais ces tâches peuvent également être dupliquées si nécessaire. Conservez deux tâches de processeur avec run_as utilisateur dans le domaine global.

   À partir de la version 20.0 de Réponse aux vulnérabilités, les changements de script suivants sont fournis avec le système de base.
4. Modifiez l'include *`BackgroundJobManager`* de script et ajoutez la ligne suivante, comme illustré dans l'image suivante.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" + jobGr.sys_domain + "");
```



Remarque : Déclenchez la réapplication sur demande de toutes les règles du domaine approprié.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une règle de recherche de CI de réponse aux vulnérabilités

Le module **Règles de recherche de CI** contient des règles qui sont utilisées pour trouver l'enregistrement correspondant aux informations sur l'hôte reçues lors des importations d'intégrations de vulnérabilités tierces. Les informations sur l'hôte correspondent aux éléments détectés, aux classes d'éléments de configuration sans correspondance et au fichier Base de données de gestion des configurations (CMDB).

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

La création de règles de recherche de CI nécessite une expertise et Réponse aux vulnérabilités une expertise avancéesServiceNow. Plutôt que de modifier l'une des règles de recherche existantes, envisagez de la copier et de modifier la copie. Lorsque vous êtes satisfait que la nouvelle règle fait ce que vous voulez, désactivez l'original.

Remarque : Une fois supprimées, les règles ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **CMDB** > **Règles de recherche de CI**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de règle de recherche de CI

Champ	Description
Nom	Nom de la règle.
Méthode de recherche	Méthode utilisée pour l'appariement. Les choix possibles sont les suivants : ○ **Script** : script prédéfini (adresse IP, nom DNS...) ou personnalisé. ○ **Correspondance de champ** : recherchez sur une table ou un champ dans la CMDB.
Type	Type utilisé avec la **méthode de recherche** de script.
Ordre	Ordre de priorité de la règle. Les règles avec l'ordre le plus bas sont évaluées en premier.
Actif	Cochez la case indiquant si la règle est active ou désactivée.
Source	Source utilisée comme entrée dans cette règle.
Champ source	Champ source utilisé comme entrée dans cette règle. Sélectionnez un champ, mais il est traité comme une valeur de chaîne.
Condition	Condition basée sur laquelle la règle de recherche de CI est appliquée. Cette condition dépend de l'attribut de l'analyseur tiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : L'attribut asset fait partie de la charge utile. Il est reçu du scanner tiers. Consultez la table Éléments détectés pour des exemples de charges utiles.
Script	Un exemple de script modifiable, basé sur le **type**, s'affiche. Implémentez le script personnalisé en fonction des commentaires inclus dans le modèle de la fonction par défaut. **Remarque :** La fonction de processus comporte trois paramètres : `rule`, `sourceValue`, et `sourcePayload`
Rechercher sur la table	Table à rechercher dans la CMDB. Utilisé avec **la méthode de recherche** de correspondance de champ.
Rechercher sur le champ	Champ qui contient des informations pouvant être utilisées pour localiser un CI. Utilisé avec la **méthode de recherche** de correspondance de champ. Ce champ peut se trouver sur l'enregistrement du CI ou sur un enregistrement connexe, tel qu'une carte réseau.

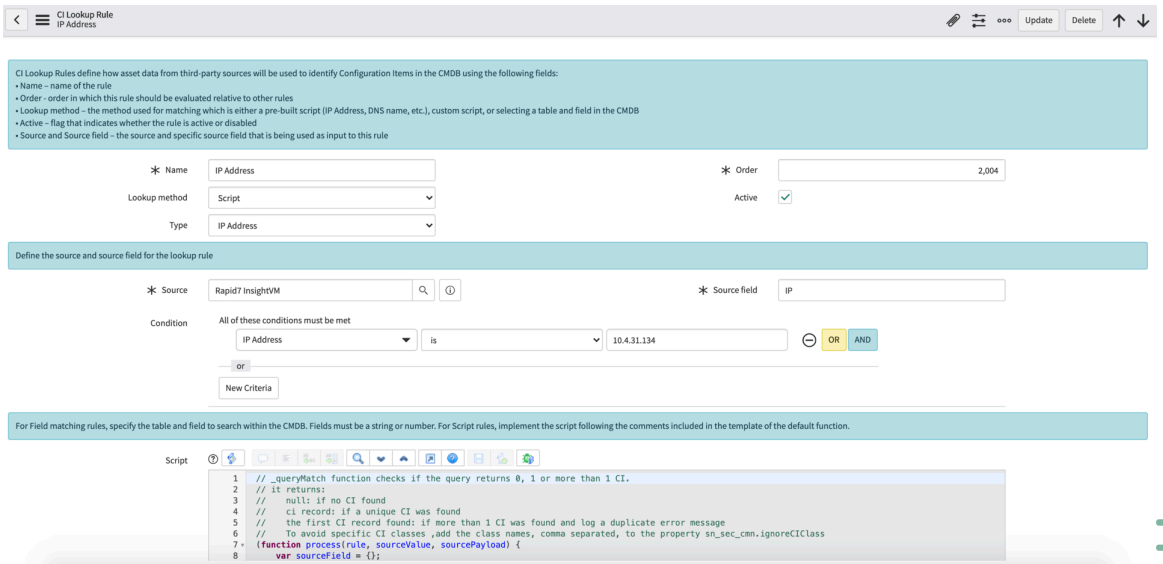
4. Cliquez sur **Envoyer**.

Pour plus d'informations sur l'implémentation des règles de recherche de CI, reportez-vous à la section Étapes pour empêcher les enregistrements dupliqués ou orphelins après l'exécution Réponse aux vulnérabilités de règles de recherche de CI.

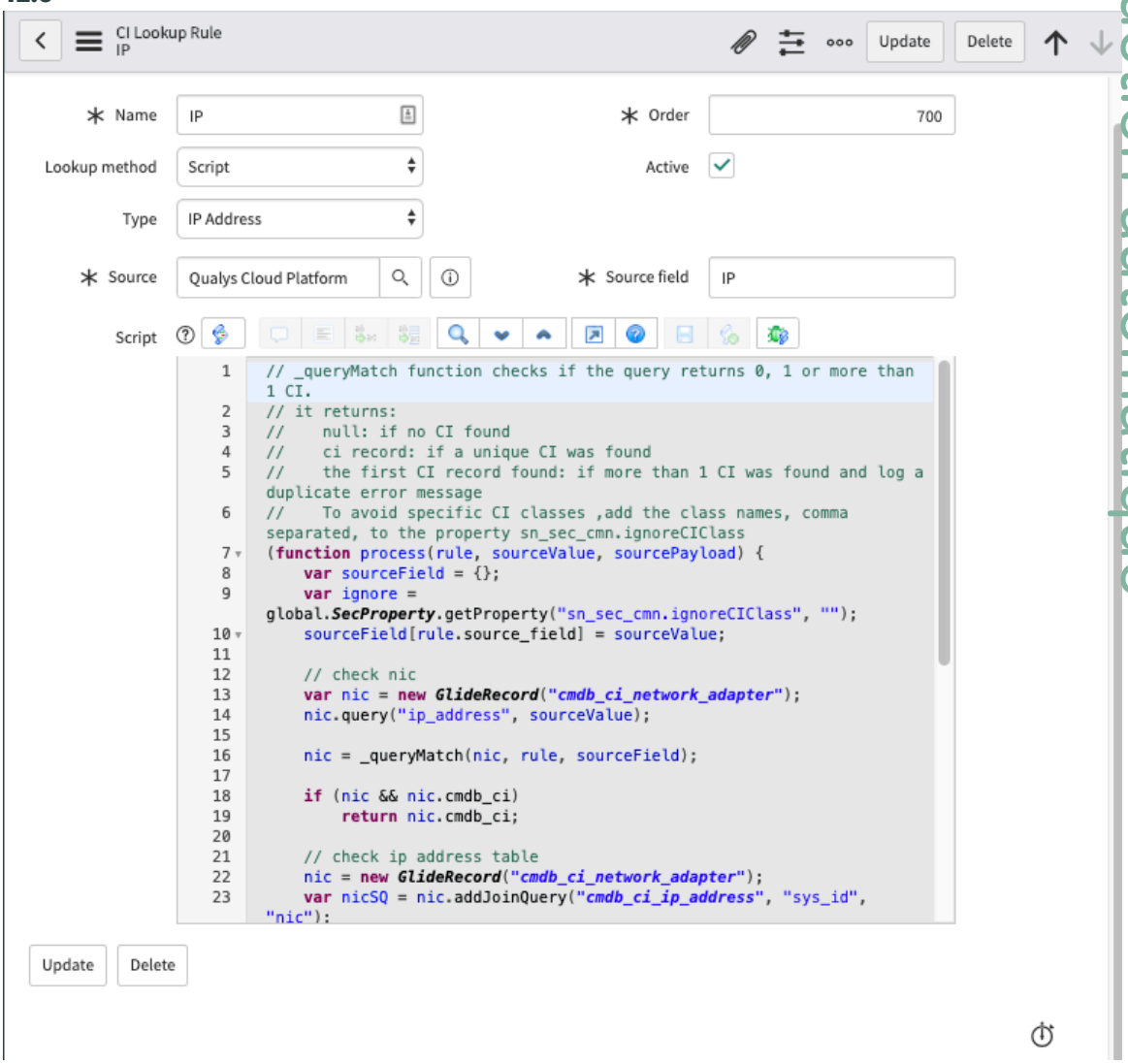
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de règle de recherche de CI à l'aide d'un créateur de conditions pour la version 12.0



Exemple d'une règle de recherche de CI utilisant un script antérieur à la version 12.0



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Réponse aux vulnérabilités Champs de formulaire d'élément vulnérable

Ignorer les classes CI

Pour ignorer certaines classes d'éléments de configuration (CI), par exemple l'équilibreur de charge [cmdb_ci_lb], lors de l'exécution des règles de recherche de CI, définissez la propriété système **ignoreCIClass** [*sn_sec_cmn.ignoreCIClass*].

Avant de commencer

Rôle requis : admin

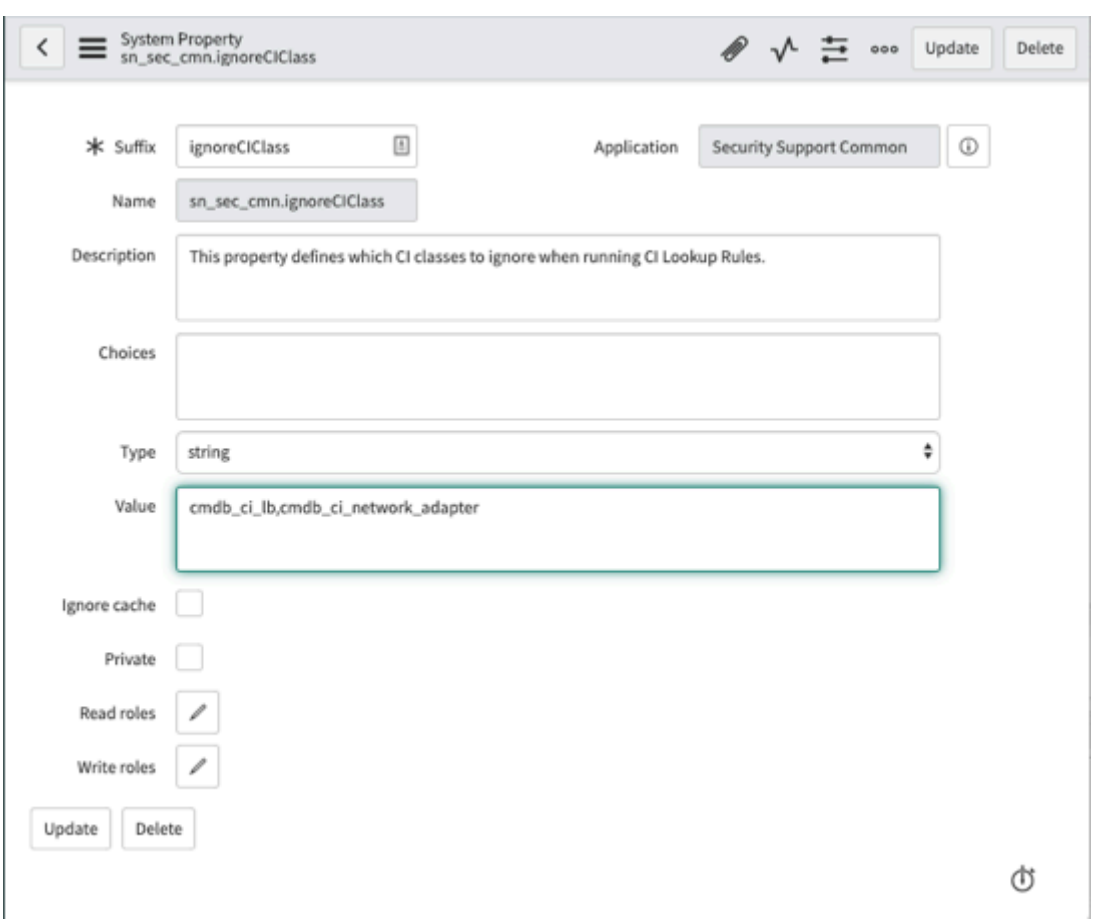
Remarque :

La propriété système **ignoreCIClass** est disponible à partir de Réponse aux vulnérabilités la version 9.0, cependant, la fonctionnalité de propriété n'est pas disponible lors de la mise à niveau à partir d'une version précédente.

Si vous avez effectué une mise à niveau à partir d'une Opérations de sécurité application antérieure à la version 9.0, reportez-vous à la KB0788209 pour obtenir des instructions sur l'activation de cette fonctionnalité.

Procédure

1. Entrez sys_properties.list dans la barre de navigation de gauche.
2. Cliquez sur **Entrée**.
3. Dans le menu **Rechercher** , sous **Nom** , saisissez sn_sec_cmn.ignoreCIClass.
4. Dans la zone **de texte Valeur** , entrez les classes CI à exclure dans une liste séparée par des virgules.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Mettre à jour**.
   Cette liste est utilisée par les règles de recherche de CI lors de la prochaine importation. Les éléments vulnérables créés pendant l'importation ne sont pas associés à un CI d'un type quelconque répertorié dans le champ **Valeur** de la propriété système sn_sec_cmn.ignoreCIClass .

Filtrer les CI désactivés

Filtrez les éléments de configuration (CI) désactivés lors de l'exécution des règles de recherche de CI. Pour filtrer les CI désactivés lors de l'exécution des règles de recherche de CI CMDB pour Opérations de sécurité, définissez la propriété système **filterOutDecommissionedCI** [**sn_sec_cmn.filterOutDecommissionedCI**] sur vrai.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La valeur par défaut de la propriété système est vrai. Cette propriété ne s'applique qu'aux règles de recherche de CI dans Réponse aux vulnérabilités et n'a pas d'impact sur la logique de recherche IRE.

Procédure

1. Entrez sys_properties.list dans la barre de navigation de gauche.
2. Sélectionnez **Entrée**.
3. Dans le menu **Rechercher** , sous **Nom** , saisissez sn_sec_cmn.filterOutDecommissionedCI pour filtrer les CI désactivés.
4. Dans la zone **de texte Valeur** , entrez la valeur vrai ou faux.
   La valeur par défaut est vrai.
5. Sélectionnez **Mettre à jour**.
   Cette valeur est utilisée par les règles de recherche de CI lors de l'importation suivante. La propriété système sn_sec_cmn.filterOutDecommissionedCI filtre les CI qui remplissent les conditions indiquées ci-dessous lors de l'exécution des règles de recherche.

```
_isCIDecommissioned: function(gr, filterDecommissionCi) {
      var install_status = false;
      var life_cycle_stage_status = false;
      // check for property
      if (filterDecommissionCi == "true") {
         if (gr.isValidField("install_status"))
            install_status = gr.install_status == 7;
         if (gr.isValidField("life_cycle_stage_status"))
            life_cycle_stage_status = gr.life_cycle_stage_status == "Retired";
      }
      return install_status || life_cycle_stage_status;
```

Promouvoir automatiquement les CI

Modifiez la chaîne JSON dans la propriété système **autoPromoteFields** [**sn_sec_cmn.autoPromoteFields**] afin que vos règles de recherche d'éléments de configuration (CI) promeuvent automatiquement tous les CI CMDB Security Operations auprès des entrées correspondantes de la table [cmdb_ci].

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Le type de propriété système est « chaîne » et nécessite la saisie d'une chaîne JSON. Cette propriété est activée par défaut et favorise les CI correspondants lors de l'exécution des règles de recherche de CI.

Les scripts de recherche personnalisés peuvent renvoyer des enregistrements de table enfants du script. Pour cette propriété, la *`_autoPromoteCI`* fonction prend *`CIIdentify Script Include`* le CI renvoyé par le script de recherche et parcourt automatiquement les relations pour arriver à l'entrée *`cmdb_ci`* et la renvoyer.

Pour remplacer la logique de promotion automatique, c'est-à-dire pour ajouter ou mettre à jour de nouvelles classes CI, ajoutez l'objet JSON dans le champ Valeur de la propriété système [**sn_sec_cmn.autoPromoteFields**].

Procédure

1. Entrez sys_properties.list dans la barre de navigation de gauche.
2. Sélectionnez **Entrée**.
3. Localisez la propriété système [**sn_sec_cmn.autoPromoteFields**] et sélectionnez l'enregistrement pour l'ouvrir.

   Chaîne par défaut :

   ```
   {
    "dscy_switchport":"cmdb_ci",
    "cmdb_ci_network_adapter":"cmdb_ci",
    "cmdb_ci_nic":"cmdb_ci",
    "cmdb_ci_ip_address":"nic"
   }
   ```

4. Dans la zone **de texte Valeur** , modifiez la chaîne à l'aide du format d'appariement par défaut.
5. Sélectionnez **Mettre à jour**.
   Cette valeur est utilisée par les règles de recherche de CI lors de l'importation suivante.

Configurer la clé de l'élément vulnérable

Configurez la granularité de la clé d'élément vulnérable (VIT) dans l'application Réponse aux vulnérabilités pour définir ce qui constitue un élément vulnérable (VIT) dans votre organisation.

Avant de commencer

Rôle requis : admin

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Termes clés :

Élément de configuration (CI)

Un actif existant répertorié sur votre CMDB.

Vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrement d'une vulnérabilité connue importée du National Institute of Standards and Technology (NIST), de la base de données de vulnérabilité nationale (NVD), de Common Vulnerabilities and Exposures (CWE) ou d'intégrations tierces avec Réponse aux vulnérabilités.

Élément vulnérable

Un élément vulnérable est créé lorsqu'une vulnérabilité importée correspond à un élément de configuration dans votre CMDB.

Détection

Une occurrence unique et distincte d'une vulnérabilité signalée par les scanners de vos intégrations tierces. Les détections sont importées et affichées à la fois sur les enregistrements de détection et les enregistrements d'éléments vulnérables de votre instance. Également appelée détection d'élément vulnérable.

Par défaut, un élément vulnérable est la combinaison unique d'un élément de configuration (CI), d'une vulnérabilité et d'une instance d'intégration. Pour créer des éléments vulnérables avec plus de granularité, ajoutez des ports ou des recommandations uniques (pour les vulnérabilités Microsoft TVM uniquement) à partir des détections d'éléments vulnérables. Cela vous aide à gérer le rattrapage des vulnérabilités au niveau que vous jugez le plus efficace pour votre organisation.

Si vous souhaitez créer des éléments vulnérables avec plus de granularité, configurez la clé de l'élément vulnérable de sorte qu'elle inclut le port ou la recommandation.

- Lorsque **Inclure le port** est activé, les éléments vulnérables sont créés par des ports uniques à partir des détections d'éléments vulnérables.
- Lorsque **l'option Inclure la recommandation** est activée, un élément vulnérable distinct est créé pour chaque recommandation associée à une vulnérabilité.

Remarque : L'option **Inclure la recommandation** s'affiche dans l'interface utilisateur uniquement si l'intégration Microsoft TVM est activée dans votre environnement.

À partir de Vulnerability Response V17.1, vous pouvez identifier et corriger les vulnérabilités Rapid7 en ajoutant la preuve comme clé de VI. Pour plus d'informations, consultez Ajout de preuve aux clés d'éléments vulnérables Rapid7.

Choisissez une option dans la table suivante pour activer l'option Inclure le port.

Trois scénarios pour activer l'option Inclure le port avec la clé de VI pour la première fois

Si...	Description
Une ou plusieurs des conditions suivantes sont vraies : • Vous effectuez une mise à niveau à partir d'une version antérieure à la version 10.0 qui ne prenait pas en charge la détection d'éléments Réponse aux vulnérabilités vulnérables. • Vous êtes un nouveau client et vous n'avez aucune donnée de Vulnerability Response (éléments vulnérables ou détections d'éléments vulnérables) dans votre ServiceNow AI Platform® instance.	Activez Inclure le port. Une fois Inclure le port activé, les détections importées créent des éléments vulnérables qui incluent des VI distingués par un port unique en commençant par l'importation suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trois scénarios pour activer l'option Inclure le port avec la clé de VI pour la première fois (suite)

Si...	Description
• Vous avez déjà supprimé tous vos enregistrements d'éléments vulnérables et les données connexes dans votre instance et vous êtes prêt à créer toutes vos données de Vulnerability Response en commençant par une nouvelle importation pour inclure les VI se distinguant par un port unique.	
Les deux conditions sont vraies : • Vous disposez de la version 10.0 ou ultérieure de et vous avez des données Vulnerability Response existantes (éléments vulnérables ou détections d'éléments Réponse aux vulnérabilités vulnérables) dans votre instance que vous souhaitez conserver. • Vous souhaitez commencer à créer de nouveaux éléments vulnérables pour inclure les VI qui se distinguent par un port unique.	Activez Inclure le port. Vos détections existantes et leurs éléments vulnérables associés sont conservés. Une fois Inclure le port activé, les nouvelles détections créent de nouveaux éléments vulnérables qui incluent les VI distingués par un port unique à partir de l'importation suivante.
Les deux conditions sont vraies : • Vous disposez de la version 10.0 ou ultérieure de Réponse aux vulnérabilités. • Vous disposez de données Vulnerability Response existantes (éléments vulnérables ou détections d'éléments vulnérables), mais vous ne souhaitez pas conserver vos données existantes, car vous préférez construire vos données de vulnérabilité à partir d'une nouvelle importation et vous souhaitez inclure des éléments vulnérables se distinguant par un port unique.	1. Supprimez tous vos enregistrements d'éléments vulnérables et les données connexes de votre instance. 2. Activez Inclure le port. Une fois Inclure le port activé, les nouvelles détections créent de nouveaux éléments vulnérables qui incluent les VI distingués par un port unique à partir de l'importation suivante.

Remarque :

Si l'option Inclure le port est activée, plusieurs éléments vulnérables peuvent être créés pour un élément de configuration. Par exemple, si une vulnérabilité existe pour deux ports sur un élément de configuration, les ports 80 et 443, deux VI uniques sont créés, un pour chaque port en commençant par l'importation suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Assurez-vous de vouloir créer des VI pour inclure des VI par ports uniques avant d'activer cette fonctionnalité. Une fois que vous activez la clé de VI pour inclure le port, vous devez d'abord supprimer vos données de réponse aux vulnérabilités avant de pouvoir désactiver l'inclusion du port et revenir à l'importation des données de vulnérabilité à l'aide de la granularité de clé de VI par défaut, c'est-à-dire lorsque les éléments vulnérables sont créés pour le port mais ne se distinguent pas par un port unique. Pour en savoir plus sur la suppression de vos données de vulnérabilité, reportez-vous à la section Supprimez tous vos enregistrements d'éléments vulnérables et les données connexes dans Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Configurer la fonctionnalité Gde l'élément vulnérable**.

   Le champ Dernière mise à jour affiche la date à laquelle la clé de VI a été configurée pour la dernière fois.

2. Cochez la case Include **Port (Inclure le port**) pour l'activer.

   Remarque : Si vous avez configuré l'intégration de Microsoft TVM, l'option **Inclure la recommandation** est également disponible. Cela permet de diviser les éléments vulnérables par recommandation unique à partir des données Microsoft TVM.

3. Sélectionnez **Enregistrer**.
   La boîte de dialogue de confirmation s'affiche.

   Si vous n'avez aucun enregistrement de détection d'éléments vulnérables dans votre instance, les détections d'éléments vulnérables et les éléments vulnérables sont créés par un port unique à partir de votre importation suivante.

   Si vous avez des détections d'éléments vulnérables et des éléments vulnérables existants dans votre instance, les détections existantes et les éléments vulnérables associés sont conservés. Les nouvelles détections créent de nouvelles vulnérabilités qui incluent des éléments vulnérables se distinguant par un port unique à partir de la prochaine importation.

Que faire ensuite

Vérifiez que les éléments vulnérables par port sont affichés dans les enregistrements de détection des éléments vulnérables et des éléments vulnérables. Pour plus d'informations, consultez Afficher les Réponse aux vulnérabilités données de détection des éléments vulnérables.

Ajout de preuve aux clés d'éléments vulnérables Rapid7

Ajoutez la preuve en tant que clé d'élément vulnérable (VI) pour les Rapid7 éléments vulnérables. L'inclusion de la preuve pour des vulnérabilités spécifiques permet à l'intégration Rapid7 du scanner de créer des VI pour chaque preuve reçue de Rapid7.

Une clé de VI est la combinaison de la vulnérabilité, de l'élément de configuration (CI) et de l'instance d'intégration. La division des détections en différents VI en fonction de la preuve crée plusieurs VI. Vous pouvez affecter les vulnérabilités aux propriétaires de rattrapage appropriés.

Par exemple, il peut y avoir deux détections avec la même vulnérabilité et le même CI, mais avec des preuves différentes, conduisant à la création d'un seul VI. À partir de la Réponse aux vulnérabilités version 17.1, vous pouvez identifier et corriger les vulnérabilités en ajoutant la preuve comme clé de VI.

Vous pouvez ajouter la preuve en tant que clé VI de la manière suivante :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Configurer la granularité VI** et sélectionnez l'option permettant d'inclure la preuve.

Cas d'utilisation : inclure la preuve dans la clé de VI pour les VI existants ou diviser les VI existants en fonction de la preuve de détection

Pour créer des VI basés sur des preuves, vous pouvez utiliser les vulnérabilités R7 log4j. Par exemple, vous pouvez utiliser l'une des multiples vulnérabilités R7 log4j telles que `R7-apache-log4j-core-cve-2021-44228`, `R7-amazon_linux-cve-2021-44228` ou `R7-amazon-linux-ami-2-cve-2021-44228`.

Si toutes les détections d'une VI ont la même preuve, alors le VI existant est mis à jour pour inclure « Preuve dans la clé de VI (external_id) ». S'il y a plusieurs détections avec des preuves différentes, le VI existant est fermé. Les détections sont réparties entre les nouveaux VI avec « Preuve dans la clé de VI (external_id) ».

Remarque :

Si vous fournissez l'ID de vulnérabilité, les VI existants sont divisés en fonction de la preuve. Les nouvelles vulnérabilités pour cet ID de vulnérabilité ont également une preuve comme l'une des clés de VI.

Supprimez tous vos enregistrements d'éléments vulnérables et les données connexes dans Réponse aux vulnérabilités

Supprimez définitivement toutes les données de Vulnerability Response (éléments vulnérables ou détections d'éléments vulnérables) ainsi que les données et enregistrements connexes de l'application Réponse aux vulnérabilités dans votre ServiceNow AI Platform® instance.

Avant de commencer

Supprimez de votre instance les enregistrements de détection d'éléments vulnérables, les éléments vulnérables, les groupes de vulnérabilité et tous les enregistrements connexes de l'application Réponse aux vulnérabilités . Utilisez ce processus pour nettoyer votre instance afin d'importer des données avec un nouveau départ à partir de vos intégrations tierces, ou comme condition préalable au retour de la configuration des clés de l'élément vulnérable (VI) à son paramètre par défaut. Pour plus d'informations sur la configuration de la clé de VI, reportez-vous à la section Configurer la clé de l'élément vulnérable.

Remarque : Cette action supprime tous les enregistrements d'éléments vulnérables et toutes les données connexes de votre instance. Une fois supprimées, ces données ne peuvent pas être récupérées. Vous devez également suspendre l'importation de données et désactiver vos intégrations tierces actives avec Réponse aux vulnérabilités.

La suppression de vos données d'élément vulnérable avec ce processus avant de modifier la configuration de la clé de VI est requise. La suppression de toutes les données garantit que tous vos éléments vulnérables et détections d'éléments vulnérables sont mappés et mis à jour avec les données les plus récentes à partir de la prochaine importation.

Vérifiez que les conditions suivantes s'appliquent avant de supprimer vos données :

- Vous avez installé la version 10.0 ou ultérieure Réponse aux vulnérabilités . Pour plus d'informations, consultez Réponse aux vulnérabilités Détections d'éléments vulnérables à partir d'intégrations tierces.
- Vous souhaitez désactiver l'option Inclure le port et rétablir le paramètre par défaut de la configuration des clés de VI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous avez des éléments vulnérables existants et des détections d'éléments vulnérables, mais vous ne voulez pas ou devez les mettre à jour et les conserver.
- Vous avez déterminé que vous souhaitez supprimer toutes les données de Vulnerability Response existantes et les enregistrements connexes pour nettoyer votre instance.

Rôle requis : sn_vul.vulnerability_admin

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Intégrations de vulnérabilité**.
2. Enregistrez toutes les intégrations actives affichées.

   Toutes les intégrations actives répertoriées avec les travaux planifiés sont désactivées avant la suppression de tous vos éléments vulnérables et des données connexes afin qu'aucune nouvelle donnée ne soit importée pendant la suppression des données. L'enregistrement de cette liste vous aide à activer vos intégrations une fois la suppression terminée.
3. Passez en revue l'article Comment supprimer des données de réponse aux vulnérabilités existantes pour la réimportation dans la base de connaissances HI.
4. Si un message d'avertissement vous empêche d'écrire dans la colonne Actif, procédez comme suit pour désactiver les intégrations actives.

   a. Dans la colonne Nom, cliquez sur un élément pour ouvrir l'enregistrement.

   b. Si vous ne pouvez pas modifier la case à cocher Actif, cliquez sur le lien **ici** pour modifier l'enregistrement.

   c. Cliquez sur la case **à cocher Actif** pour désactiver l'intégration et annuler la prochaine tâche planifiée.

   d. Cliquez sur **Mettre à jour** pour enregistrer vos modifications et revenir à la liste.

   e. Vérifiez que vous avez désactivé toutes les intégrations actives dans la liste Intégrations.
   Après avoir désactivé une intégration, elle n'est plus affichée dans la liste des intégrations actives. Pour répertorier les intégrations inactives et localiser toutes les intégrations que vous avez désactivées après avoir supprimé toutes vos données de vulnérabilité, saisissez `= faux` dans la colonne Actif.
5. Poursuivez les étapes de l'article de la base de connaissances pour supprimer vos données de vulnérabilité existantes.
6. Une fois que vous avez confirmé que toutes les données ont été supprimées avec succès, accédez à **Réponse aux vulnérabilités** > **Administration** > **Configurer la granularité VI**.
7. Sur le formulaire :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si vous avez supprimé des données parce que vous préférez créer vos données de vulnérabilité pour inclure le port à partir d'une nouvelle importation, activez Inclure le port et cliquez sur **Enregistrer**.
- Si vous avez supprimé des données parce que vous souhaitez rétablir les paramètres par défaut de la clé de VI, désactivez Inclure le port et cliquez sur **Enregistrer**.

Pour plus d'informations, consultez Configurer la clé de l'élément vulnérable.

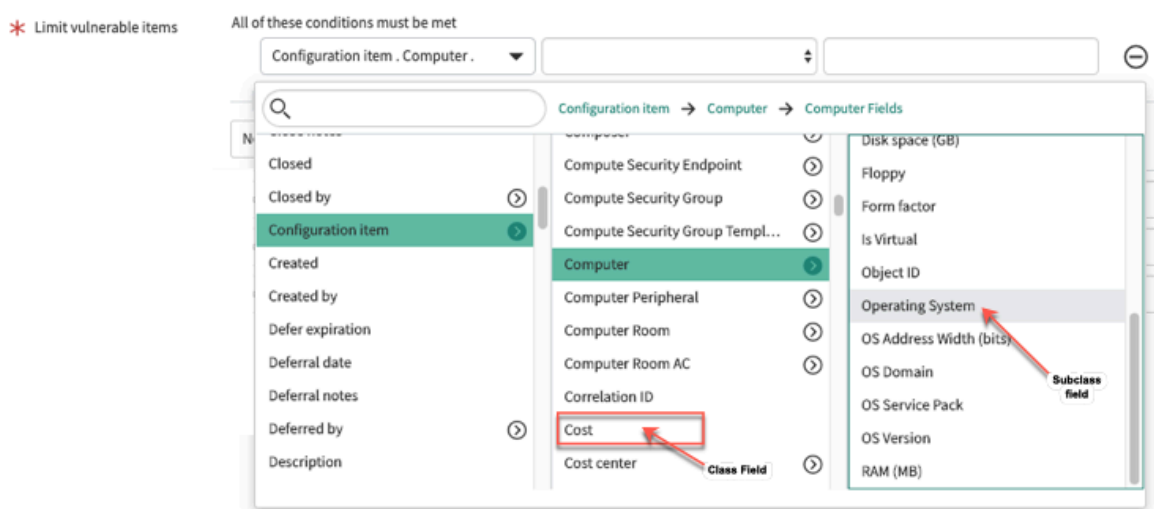
Filtrage au sein de Réponse aux vulnérabilités

Les règles, calculateurs et règles d'affectation de tâches de rattrapage utilisent des conditions lors de l'importation, créées à l'aide du **Créateur de conditions**. Les changements apportés à leurs critères peuvent affecter les performances, car chaque enregistrement est évalué à l'aide de ces filtres.

Les règles et calculateurs fournis avec le système de base sont optimisés pour les performances. L'édition ou la création de règles ou de calculateurs prend soin et peut nécessiter les deux ServiceNow et Réponse aux vulnérabilités une expertise.

Éviter le filtrage basé sur les champs de sous-classe

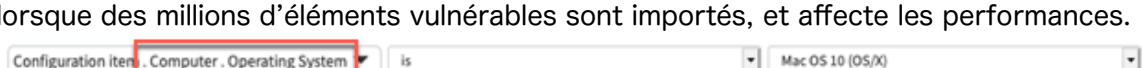
Certaines tables prennent en charge l'extension. La table CI CMDB [cmdb_ci] en est un exemple. Des tables comme cmdb_ci_hardware et cmdb_ci_computer étendre cette table. Si vous filtrez en fonction d'un champ qui ne figure pas dans la table parente, la construction et l'évaluation de ce filtre peuvent s'avérer coûteuses.



Par exemple, le filtrage sur **Élément de configuration** > **Coût** ne nuirait pas aux performances, car **le coût** est un champ de classe et non un champ de sous-classe de **l'élément de configuration**.



Élément de configuration > **Ordinateur**, cependant, est une sous-classe nécessitant une remontée pas à pas vers un autre champ, dans ce cas, **le système d'exploitation**. Ce processus peut prendre plusieurs millisecondes, ce qui s'additionne rapidement, lorsque des millions d'éléments vulnérables sont importés, et affecte les performances.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'utilisation de la condition [contient] s'apparente à une recherche par caractères génériques et peut avoir un impact sur les performances. L'utilisation de [est], dans la mesure du possible, est plus efficace.

Mappage de gravité pour Vulnerability Response

Vulnerability Response est fourni avec la base de données de vulnérabilité nationale (NVD) pour le mappage de gravité normalisé de ServiceNow. Les intégrations tierces ServiceNow fournissent des mappages de gravité lors de l'installation. Ces cartes peuvent être ajustées en modifiant les champs dans les cartes existantes.

Mappage de gravité de l'intégration des vulnérabilités Rapid7

Normalised_Severity

Calculez normalised_severity sur l'entrée tierce en utilisant la gravité provenant de **sn_vul_nvd_entry** table. Ceci est défini à l'aide des Règles métier pour rechercher la gravité normalisée sur **sn_vul_entry** table.

Source_severity

Les données de la table **severity_score** sont mappées à source_severity table pendant que **l'API d'intégration de vulnérabilité Rapid7** est en cours **d'exécution**.

Priorité

Ce champ est vide.

Mappage de gravité de l'intégration de vulnérabilité Qualys

Normalised_Severity

Calculez normalised_severity sur l'entrée tierce en utilisant la gravité provenant de **sn_vul_nvd_entry** table. Ceci est défini à l'aide des Règles métier pour rechercher la gravité normalisée sur **sn_vul_entry** table.

Source_severity

Les données du **SEVERITY_LEVEL** sont mappées à la table **source_severity** pendant **l'exécution de l'intégration de la base de connaissances Qualys** .

Priorité

Les données du champ Priorité sont obtenues à partir de la **table SEVERITY** et mappées à la table **Priorité** pendant que **l'intégration de la détection d'hôte Qualys** est en cours d'exécution à l'aide de la règle métier mappée aux données Qualys.

Remarque : Les règles métier s'exécutent en arrière-plan. Elles vérifient la priorité pour Qualys et mappe la priorité en conséquence. Ainsi, pour mapper les données Qualys, BR est responsable.

Mappage de gravité de l'intégration de vulnérabilité Tenable.io

Normalised_Severity

Calculez normalised_severity sur l'entrée tierce en utilisant la gravité provenant de **sn_vul_nvd_entry** table. Ceci est défini à l'aide des Règles métier pour rechercher la gravité normalisée sur **sn_vul_entry** table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Source_severity

Les données de **risk_factor** table sont mappées à **source_severity** table lorsque **l'intégration du module d'extension Tenable.io** est en cours d'exécution.

Priorité

Les données de **severity_id** sont mappées à **source_severity** pendant que **l'intégration des vulnérabilités ouvertes Tenable.io** est en cours d'exécution.

VPR

Les données du **score** sont mappées aux **Source_risk_score** pendant que **Tenable.io'intégration du module d'extension** est en cours d'exécution.

Les données de **Calculé à partir du score** sont mappées à **Source_risk_rating** pendant que **Tenable.io'intégration du module d'extension est en cours d'exécution** .

Mappage de gravité de l'intégration de vulnérabilité Tenable.sc

Normalised_Severity

Calculez **normalised_severity** sur l'entrée tierce en utilisant la gravité provenant de sn_vul_nvd_entry table. Ceci est défini à l'aide des Règles métier pour rechercher la gravité normalisée sur **sn_vul_entry** table.

Source_severity

Les données de la table **riskFactor** sont mappées à **source_severity** lorsque **l'intégration du module d'extension Tenable.io** est en cours d'exécution.

Priorité

Les données de **gravité** reçues en tant que **« sévérité » : { « id » : « 0 », « nom » : « Informations », « description » : « Informatif » }** sont mappées à **source_severity** pendant que **l'intégration des vulnérabilités ouvertes Tenable.io** est en cours d'exécution.

VPR

Les données de **vprScore** sont mappées à **Source_risk_score** pendant que **Tenable.io'intégration du module d'extension** est en cours d'exécution.

Les données de **Calculé à partir de vprScore** sont mappées à **Source_risk_rating** pendant que **Tenable.io'intégration du module d'extension** est en cours d'exécution.

Mappage de gravité TVM

Normalised_Severity

Calculez normalised_severity sur l'entrée tierce à l'aide de la valeur provenant de **sn_vul_nvd_entry** table. Ceci est défini à l'aide des Règles métier pour rechercher la gravité normalisée sur **sn_vul_entry** table.

Source_severity

Les données de la table de **gravité** sont mappées à **source_severity** pendant que **l'intégration de vulnérabilité Microsoft TVM (CVE)** est en cours d'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Priorité

Ce champ est vide.

Créer une carte de Réponse aux vulnérabilités gravité

Réponse aux vulnérabilités Le mappage de gravité transforme les champs de gravité sources tierces en champs reconnaissables dans Réponse aux vulnérabilités.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités est livré avec la base de données de vulnérabilité nationale (NVD) pour un ServiceNow mappage de gravité normalisé. ServiceNow Des intégrations tierces telles que Fournir Qualys Vulnerability Integration des mappages de gravité lors de l'installation. Ces cartes peuvent être ajustées en modifiant les champs dans les cartes existantes.

La création ou la modification d'une carte de gravité est destinée uniquement aux mappages tiers personnalisés ou non standard dans votre environnement.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Mappage de gravité normalisé**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Mappage de champs

Champ	Description
Source	Nom de la source pour le mappage de gravité.
Valeur de la source	Valeur de gravité source.
Valeur cible	Valeur de gravité cible. Les choix possibles sont les suivants : ○ 1 - Critique ○ 2 - Élevée ○ 3 : moyen ○ 4 - Faible ○ 5 : aucun

4. Répétez l'étape 3 pour chaque niveau de gravité de la source.
5. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir les classifications de service pour Réponse aux vulnérabilités la génération de rapports et les listes connexes

Mettez davantage l'accent sur la génération de rapports et les listes connexes en Réponse aux vulnérabilités définissant des classifications de services. En outre, la réduction du nombre de classifications de services demandées peut améliorer les performances de la collecte de Réponse aux vulnérabilités données.

Avant de commencer
Rôle requis : admin

Remarque :

La modification des propriétés système nécessite l'expertise des Réponse aux vulnérabilités deuxServiceNow.

Procédure

1. Entrez `sys_properties_list.do` dans la barre de navigation de gauche.
2. Cliquez sur **Entrée**.
3. Dans le menu **Rechercher** , sous **Nom** , saisissez `sn_vul.service_classifications`.
4. Ouvrez la propriété système *`sn_vul.service_classifications`* .
5. Dans la zone de texte **Valeur** , entrez la liste séparée par des virgules des classifications de service souhaitées.

   Remarque : Lorsque ce paramètre est vide, tous les services sont répertoriés.

   Exemples :

   Pour afficher les services d'entreprise, les services techniques et les services d'application et exclure les offres de service, les services partagés et les services non classifiés, définissez la valeur sur : **service d'entreprise, service technique, service d'application**.

   Pour afficher les services d'application, définissez la valeur sur : **Service d'application**.

6. Cliquez sur **Mettre à jour**.
   Les données de chaque liste connexe de rapports et d'éléments vulnérables sont filtrées par classification de service lors de la prochaine exécution de la tâche d'analyse des performances nocturne.

Auditez les champs sélectionnés dans la table des éléments vulnérables

Activez l'audit pour les champs que vous spécifiez dans la table Élément vulnérable [sn_vul_vulnerable_item]. Cette méthode d'audit est utile lorsque vous souhaitez auditer des champs que vous ne pouvez pas auditer par défaut.

Avant de commencer
Rôle requis : admin

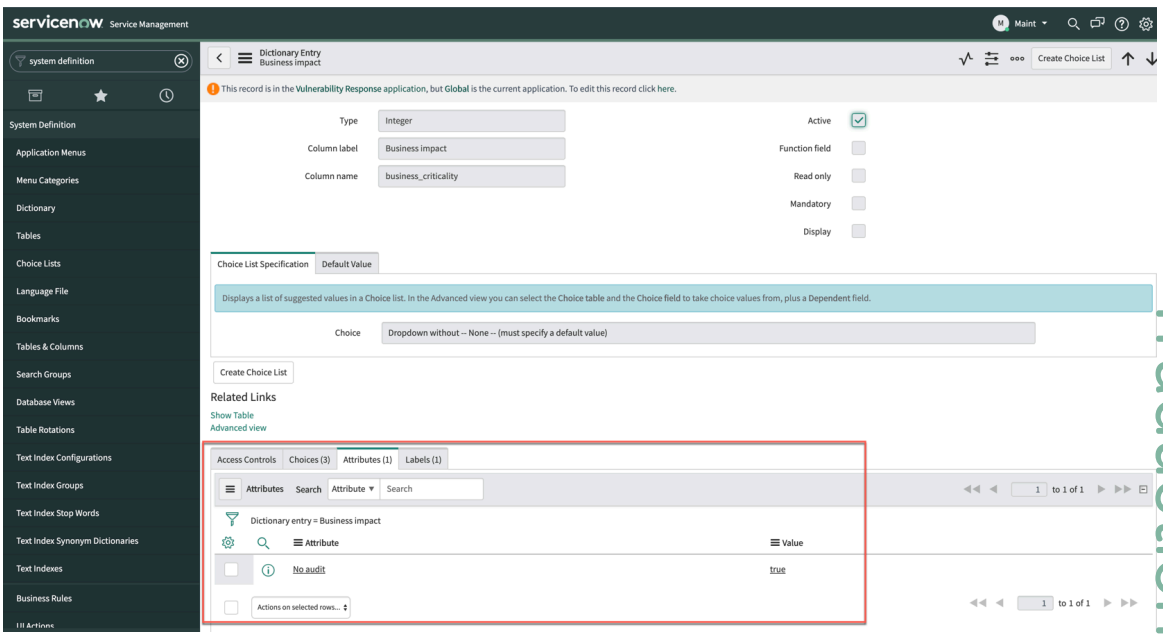
Pourquoi et quand exécuter cette tâche
La table sn_vul_vulnerable_item est auditable par défaut. Les champs dont l'attribut no_audit est défini sur vrai ne peuvent pas être audités. Pour plus d'informations sur l'audit des tables, consultez Activer l'audit pour une table .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Définition du système** > **Tables** et recherchez la table sn_vul_vulnerable_item.
   La liste des entrées de dictionnaire pour la table s'affiche.
2. Pour activer l'audit d'un champ, cliquez sur le nom de l'entrée.
   La page d'entrée du dictionnaire pour cette entrée s'affiche.



3. Accédez à la **Attributs** > **Pas d'audit**.
   La page Attribut du dictionnaire s'affiche.
4. Pour supprimer l'attribut no audit=true, cliquez sur **Supprimer**.
   L'audit de ce champ est activé.

Réponse aux vulnérabilités Configuration du cadre de travail de la tâche en arrière-plan

Définissez le cadre de travail de la tâche en arrière-plan dans votre ServiceNow AI Platform® instance. Ces changements de configuration peuvent vous aider à améliorer les performances en réduisant la quantité de ressources système utilisées pour exécuter vos tâches en arrière-plan.

Que pouvez-vous modifier dans le cadre de travail de la tâche en arrière-plan

Avec le module Configuration de la tâche en arrière-plan, vous disposez des options de paramétrage suivantes dans le cadre de travail :

- Vous pouvez définir le nombre de tâches en arrière-plan qui s'exécutent simultanément pour Réponse aux vulnérabilités des processus.
- Pour les tâches longues qui s'exécutent en arrière-plan et traitent de grandes quantités de données, vous pouvez créer des partitions pour traiter les données en blocs plus petits.
- Vous pouvez annuler une tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi configurer le cadre de travail de la tâche en arrière-plan

Les tâches en arrière-plan de votre ServiceNow AI Platform® sont conçues pour s'exécuter pendant de longues périodes afin d'exécuter plusieurs processus sur vos enregistrements dans Réponse aux vulnérabilités. Ces tâches étaient auparavant basées sur des règles métier qui s'exécutaient de manière asynchrone. Il n'existe aucune limite au nombre de ces tâches qui peuvent s'exécuter en arrière-plan dans votre instance afin que les grandes quantités d'enregistrements impactés par ces tâches puissent être traitées. Lorsque plusieurs tâches qui prennent beaucoup de temps s'exécutent simultanément en arrière-plan, les ressources système utilisées pour exécuter vos travaux planifiés sont affectées, ce qui peut avoir un impact négatif sur vos performances.

La configuration du cadre de travail des tâches en arrière-plan peut vous aider à améliorer vos performances en réduisant la quantité de ressources système utilisées pour exécuter vos tâches en arrière-plan.

Termes clés

Aptitude de la tâche

Décrit les tâches particulières. Par exemple, une tâche particulière peut inclure les capacités suivantes :

- La tâche peut être exécutée en parallèle avec une autre tâche du même type.
- La tâche peut être partitionnée.
- La tâche peut être annulée en cours d'exécution.

Concurrence

Fait référence à des tâches ou à des éléments de tâches qui s'exécutent en parallèle.

Partition

Les partitions sont des tâches qui peuvent être divisées afin qu'elles puissent être traitées en parallèle pour obtenir de meilleures performances. Fait généralement référence à des travaux avec de longues durées.

Configuration de la tâche

Fait référence aux paramètres d'une tâche planifiée particulière.

Tâche planifiée

Les travaux planifiés sont des éléments automatisés du travail qui peuvent être effectués à une heure spécifique ou selon un calendrier récurrent.

Ressources système

Désigne la quantité de ressources système dont vous avez besoin pour prendre en charge un nombre donné de travaux en arrière-plan et de travaux planifiés dans votre environnement.

Propriété système

Les propriétés système stockent des informations de configuration qui changent rarement ou jamais. Chaque fois que vous modifiez ou ajoutez une propriété système, le système vide le cache pour maintenir la synchronisation de tous les nœuds du cluster. Cette purge du cache a un impact sur les performances.

Business Rule

Une règle métier est un script de serveur qui s'exécute lorsqu'un enregistrement est affiché, inséré, mis à jour ou supprimé, ou lorsqu'une table est interrogée. Les règles métier accomplissent des tâches telles que le changement automatique des valeurs dans les champs de formulaire lorsque certaines conditions sont remplies, ou la création d'événements pour les notifications par e-mail et les actions des scripts.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation pour définir le cadre de travail de la tâche en arrière-plan

Par exemple, la tâche en arrière-plan qui applique les règles de cibles de rattrapage pour les enregistrements d'éléments vulnérables (VIT) et les enregistrements d'éléments vulnérables (AVIT) d'Application Vulnerability Response traite simultanément de grandes quantités d'enregistrements avec plusieurs tâches.

Selon la taille de l'importation et le nombre d'enregistrements dont vous disposez dans votre environnement, cette tâche peut utiliser une grande partie de vos ressources système disponibles et prendre beaucoup de temps. Les tâches de maintenance du système ou d'autres travaux planifiés peuvent être exécutés plus lentement.

Dans le module de configuration de la tâche en arrière-plan, les tâches sont répertoriées par nom et par ID de configuration unique. Sur ces enregistrements, vous pouvez définir le nombre de tâches que vous souhaitez exécuter simultanément pour une tâche en arrière-plan donnée. Vous pouvez également configurer la tâche pour traiter les partitions de données afin que les tâches s'effectuent plus rapidement et plus facilement et utilisent moins de ressources système. Vous pouvez également annuler une tâche si vous déterminez qu'elle est en cours d'exécution trop longue.

Module de configuration de la tâche en arrière-plan



Pour en savoir plus sur les étapes requises pour définir les configurations des tâches en arrière-plan, reportez-vous à la section Définir des configurations de tâche en arrière-plan dans Réponse aux vulnérabilités.

Définir des configurations de tâche en arrière-plan dans Réponse aux vulnérabilités

Définissez le nombre de tâches que vous souhaitez exécuter simultanément pour une tâche en arrière-plan donnée. Vous pouvez également configurer la tâche pour importer des partitions de données afin que les tâches s'effectuent plus rapidement et plus facilement et utilisent moins de ressources système. Vous pouvez également annuler une tâche si vous déterminez qu'elle est en cours d'exécution trop longue.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou gestionnaires des vulnérabilités avec le rôle granulaire sn_sec_cmn.manage_background_job

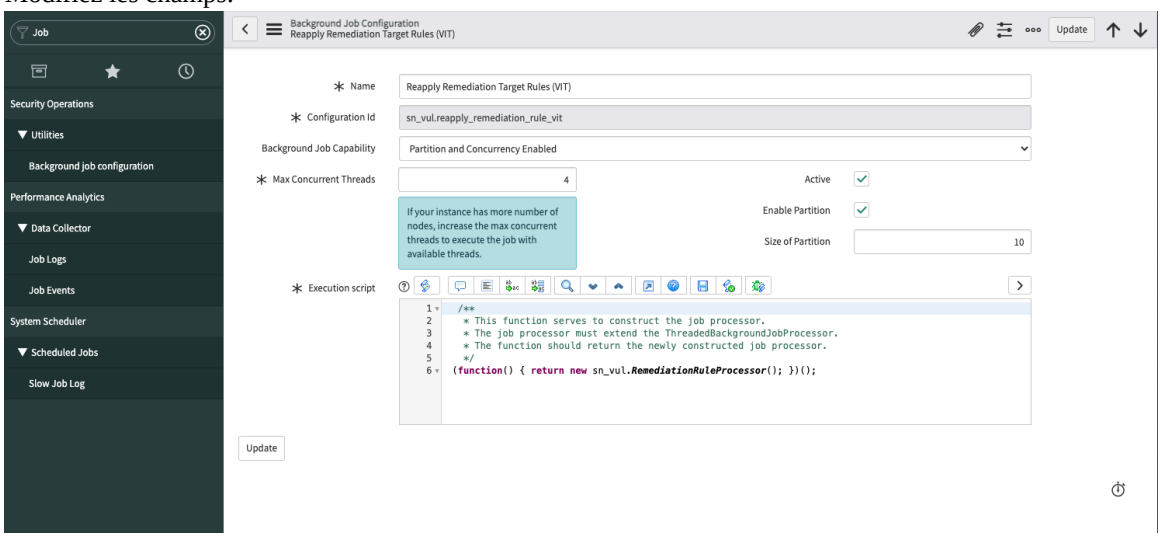
Consultez la section sous les étapes pour obtenir un exemple.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Configurations des tâches en arrière-plan**.
2. Dans la colonne Nom, cliquez sur un enregistrement pour l'ouvrir.
3. Modifiez les champs.



Champ	Description
Nom	Nom de la tâche.
ID de configuration	Lecture seule. ID unique utilisé pour identifier la tâche.
Aptitude de tâche en arrière-plan	Choisissez-en un. ○ Partition et concurrence activées : une tâche avec une longue durée d'exécution peut être divisée et la tâche peut être exécutée en parallèle avec une autre tâche du même type. ○ Concurrence activée : la tâche peut être exécutée en parallèle avec une autre tâche du même type. ○ Annulation activée : la tâche peut être annulée. ○ Concurrence et annulation activées : la tâche peut être exécutée en parallèle avec une autre tâche et être annulée. ○ Partition, concurrence et annulation activées : une tâche avec une longue durée d'exécution peut être divisée, la tâche peut être exécutée en parallèle avec une autre tâche du même type et la tâche peut être annulée. ○ Aucun La valeur affichée indique si une tâche prend en charge le partitionnement, la concurrence et l'annulation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nombre maximal de threads simultanés	ce champ n'est affiché que si la concur– rence est prise en charge. Entrez le nombre maximal de tâches que vous souhaitez que cette configuration exécute en parallèle. Le nombre de travaux planifiés pris en charge par votre instance est par défaut de 10. Vous pouvez réduire cette valeur si vous pensez utiliser ou si vous disposez de ressources système in– férieures pour exécuter vos tâches en ar– rière-plan.
Actif	Activer ou désactiver la tâche Si une tâche est désactivée, vous ne pou– vez pas créer de tâches de ce type. Toute tâche existante dans la file d'attente ne sera pas traitée.
Activer la partition	ce champ n'est affiché que si le partitionnement est pris en charge. Cette option vous permet de limiter et de définir le nombre d'éléments que cette tâche peut traiter à la fois. Le champ Taille de partition est également affiché. Si vous laissez ce champ désactivé, les tâches en arrière-plan qui prennent en charge le partitionnement traitent tous les éléments de votre instance avec cette tâche.
Taille de la partition	ce champ n'est affiché que si le partitionnement est pris en charge. La valeur par défaut est de 10 000 élé– ments. Entrez une valeur pour le nombre d'élé– ments par bloc de données que vous sou– haitez que cette tâche traite. Cette option est disponible pour les travaux qui traitent un grand nombre d'enregistrements tels que les éléments vulnérables, les tâches de rattrapage, les résultats des tests et les groupes de résultats des tests.
Script d'exécution	Affiche le processeur de tâches utilisé pour exécuter cette tâche. Une méthode par défaut est fournie pour les tâches qui prennent en charge le partitionnement.
Activer l'annulation	Ce champ n'est affiché que si l'annulation de tâche est prise en charge. Cette option est prise en charge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	pour les tâches qui traitent les éléments détectés et réappliquent des règles de CI.

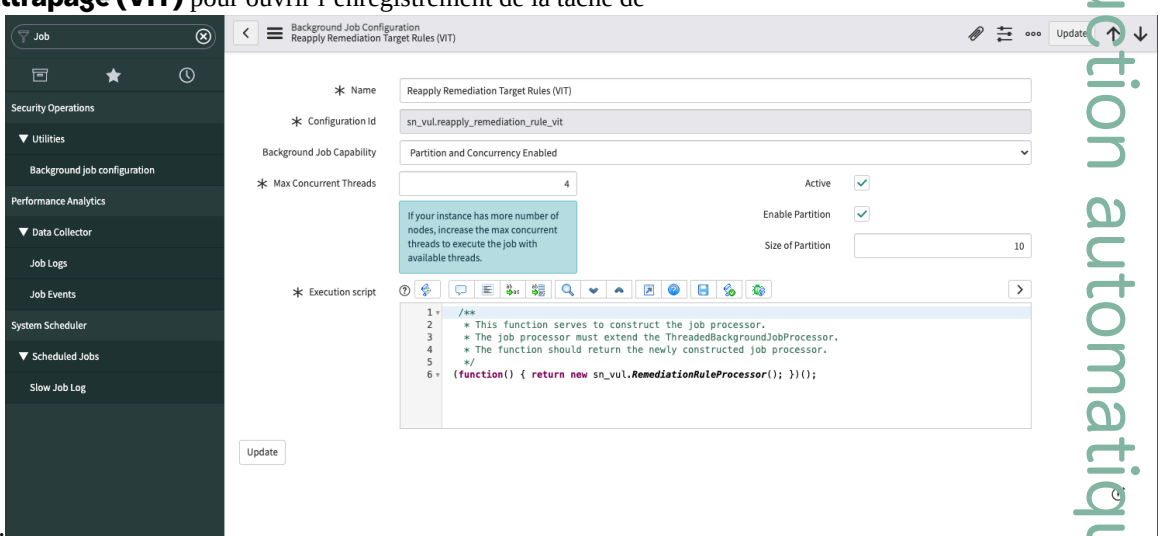
4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
   Consultez l'exemple suivant pour savoir comment vérifier les résultats de vos changements de configuration.

   Deux configurations de tâches de règles cibles de rattrapage sont incluses avec l'application, l'une pour les éléments vulnérables et l'autre pour les éléments vulnérables de l'application :

   - Réappliquer les règles de cibles de rattrapage (VIT)
   - Réappliquer les règles de cibles de rattrapage (AVIT)

   Supposons que vous modifiez vos règles de cibles de rattrapage et que vous souhaitez les réappliquer sans utiliser la plupart de vos ressources système de traitement disponibles. Pour vous aider à limiter les ressources de traitement, vous pouvez contrôler le nombre de tâches en arrière-plan que vous exécutez et le nombre d'éléments que vous traitez par tâche dans le module Configurations de tâches en arrière-plan.

5. Pour définir ces paramètres, accédez à **Security Operations** > **Configurations des tâches en arrière-plan** et cliquez sur **Réappliquer les règles de cibles de rattrapage (VIT)** pour ouvrir l'enregistrement de la tâche de configuration.

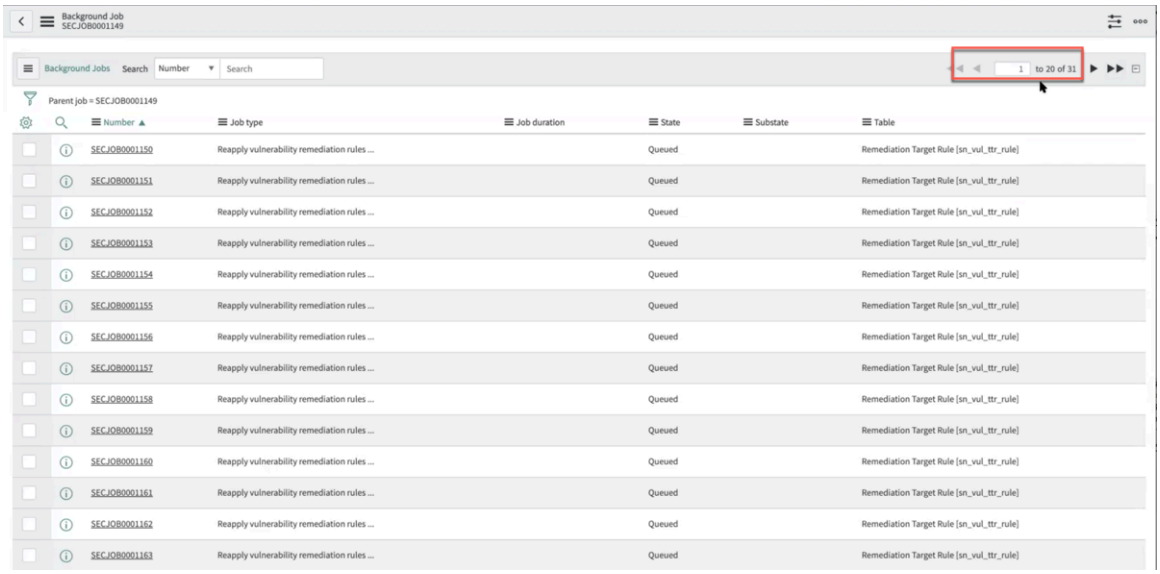


   Pour les besoins de l'exemple, disons que vous savez que vous avez un peu plus de 300 VI.

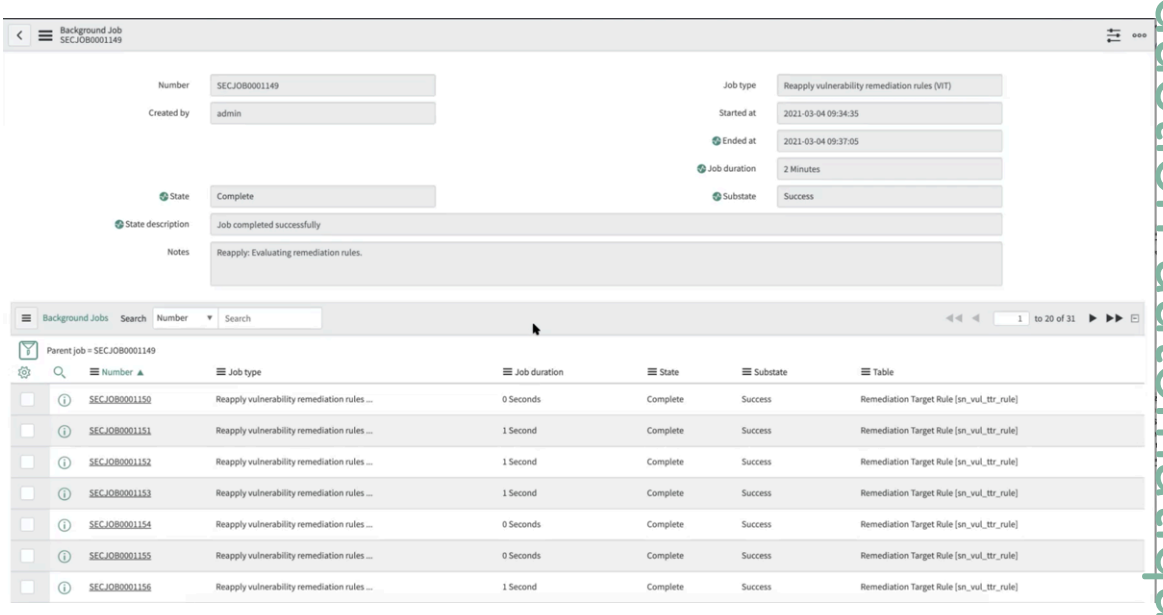
6. Sur l'enregistrement de la tâche de configuration ouverte, modifiez la valeur de taille de partition de **4** à **10**.
7. Accédez à la **Réponse aux vulnérabilités** > **Règles de cibles de remédiation**, localisez la règle de rattrapage de vulnérabilité réappliquée que vous avez modifiée, sélectionnez l'enregistrement dans la liste et cliquez sur **Appliquer les changements** pour réévaluer vos règles cibles pour vos VI existants.
   La tâche Réappliquer les règles de rattrapage des vulnérabilités (VIT) est en file d'attente.
8. Cliquez sur le lien **Afficher l'état** pour afficher l'enregistrement de la tâche en arrière-plan et vérifiez que les tâches sont en file d'attente, comme illustré dans l'image suivante.
   Pour cet exemple, 31 tâches sont créées pour traiter les règles cibles pour 307 VI (maximum de 10 éléments par tâche). Ces tâches sont des tâches enfants de la tâche d'arrière-plan principale. Les tâches enfants traitent les enregistrements séquentiellement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Lorsque toutes les tâches sont terminées avec succès, les champs sont mis à jour sur l'enregistrement de tâche en arrière-plan.



9. Accédez à vos éléments vulnérables et vérifiez qu'ils reflètent votre nouveau changement de règle.

Traitement parallèle avancé pour les tâches en arrière-plan dans Réponse aux vulnérabilités

Avec ce paramètre avancé, contrôlez le nombre total de travaux en arrière-plan traités en parallèle, quel que soit le type de travail.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou gestionnaires des vulnérabilités avec le rôle granulaire sn_sec_cmn.manage_background_job

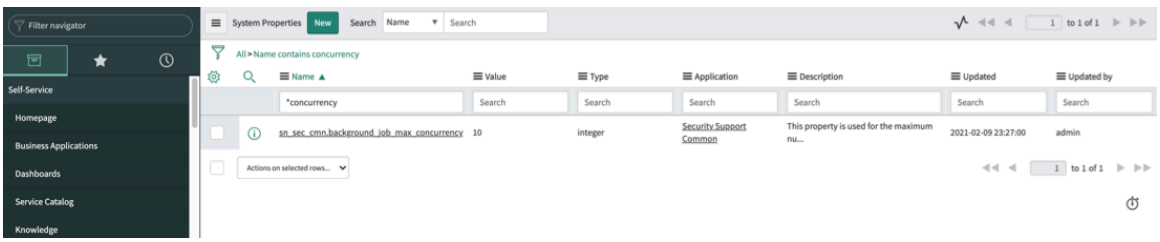
Remarque : Cette procédure nécessite des connaissances avancées en programmation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans le navigateur de filtre, saisissez **sys_properties.list** et localisez la propriété système *sn_sec_cmn.background_job_max_concurrency* .



2. Cliquez dessus pour ouvrir l'enregistrement.

   Par défaut, la *sn_sec_cmn.background_job_max_concurrency* propriété système exécute un maximum de 10 tâches en arrière-plan en parallèle.

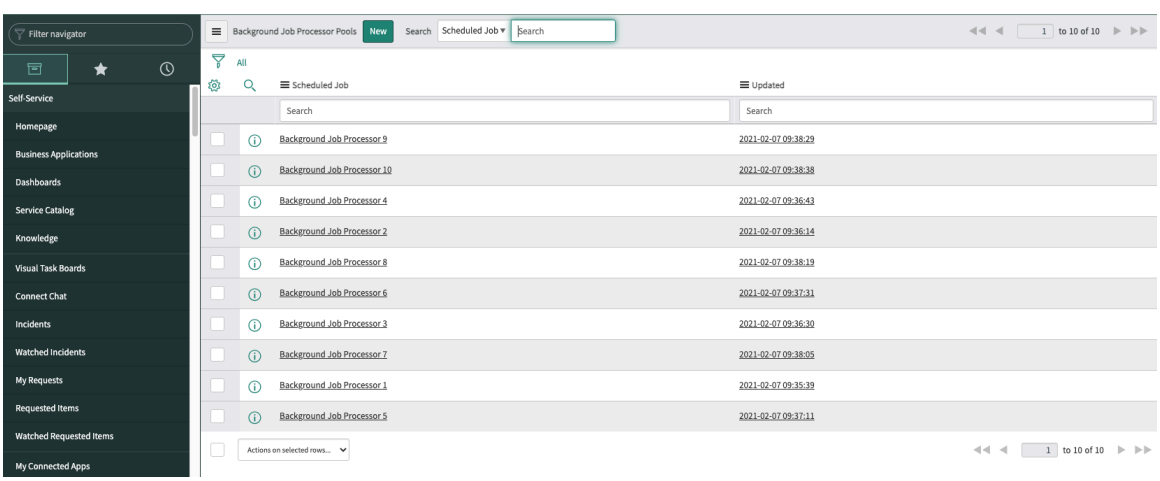
   Si votre instance comporte un faible nombre de nœuds, vous pouvez réduire cette valeur dans la propriété système. Par exemple, supposons que vous avez sept règles d'affectation sur votre liste de règles de groupe. Sur l'enregistrement de configuration de la tâche Réappliquer les règles d'affectation, trois tâches sont définies pour le nombre maximal de threads simultanés. Votre valeur de concurrence pour votre cadre de travail est de 10, mais votre système est une instance à nœud unique, de sorte que vous pouvez traiter simultanément deux tâches partitionnées à partir de votre tâche Réappliquer les règles d'affectation. Si vous définissez le nombre maximal de threads simultanés sur un enregistrement de tâche de règles d'affectation, tous les types de tâches Réappliquer les règles d'affectation seront traités séquentiellement.

   Inversement, si votre instance comporte plus de nœuds, vous pouvez augmenter cette valeur, mais vous devez également ajouter d'autres travaux planifiés pour effectuer ce changement.

   Pour augmenter le nombre de travaux planifiés, dupliquez un travail planifié autant de fois que nécessaire pour correspondre à la valeur dont vous avez augmenté votre propriété système. Par exemple, par défaut, il existe 10 travaux planifiés. Donc, si vous voulez 20 tâches, vous devez dupliquer une tâche 10 fois.

   Les dix travaux planifiés inclus dans le pour le ServiceNow AI Platform® traitement sont affichés dans la table sn_sec_cmn_background_job_processor_pool.

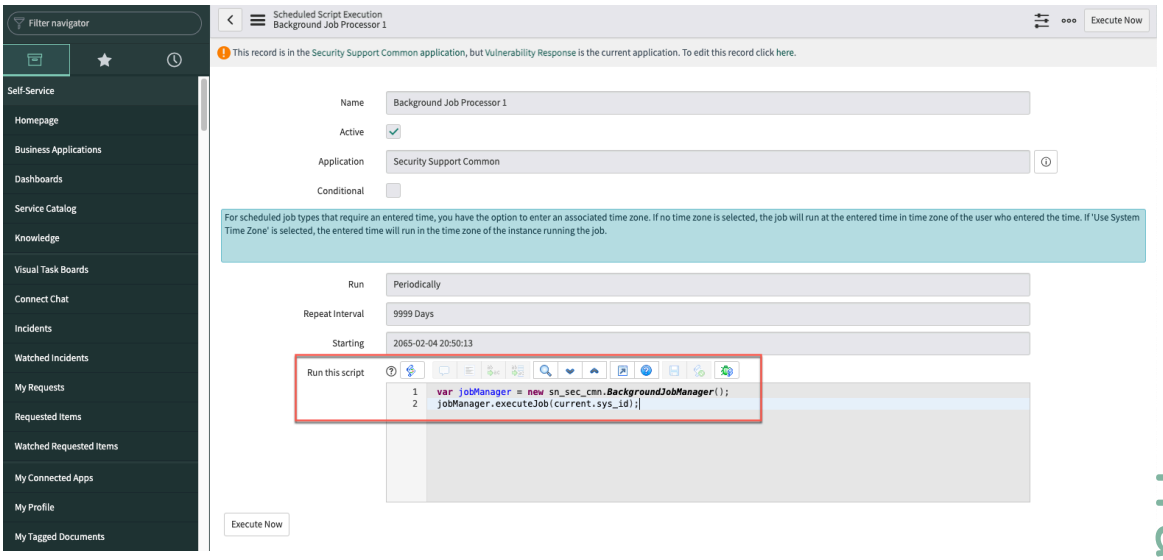
3. Dans le navigateur de filtre, saisissez **sn_sec_cmn_background_job_processor_pool.list**



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur une tâche pour la copier et la dupliquer autant de fois que nécessaire afin que le nombre de tâches corresponde à la valeur dont vous avez augmenté votre propriété système.



5. Une fois la tâche planifiée définie, ajoutez une référence en cliquant sur **Nouveau** dans la liste sn_sec_cmn_background_job_processor_pool de la tâche que vous avez copiée.

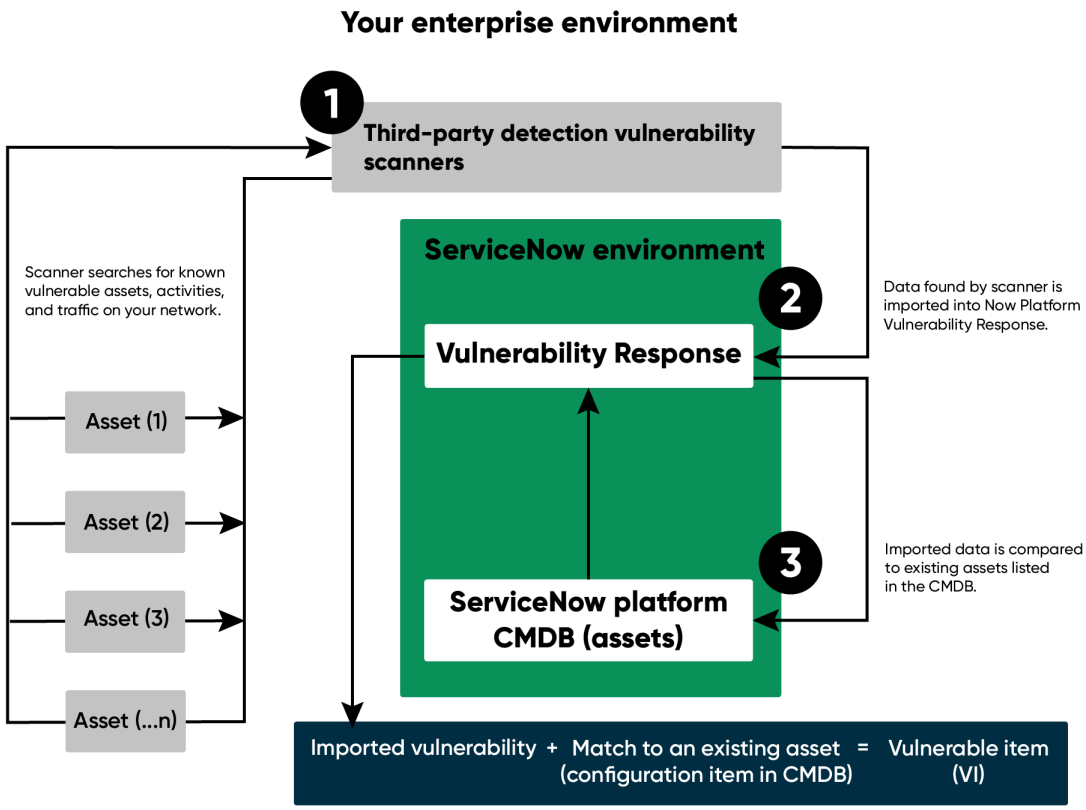
Intégrations de Réponse aux vulnérabilités

Réponse aux vulnérabilités inclut la prise en charge des intégrations tierces. Vous trouverez dans cette section quelques directives de base pour développer vos propres intégrations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations tierces



Les vulnérabilités importées de la base de données de vulnérabilité nationale (NVD) et les données de détection provenant d'analyseurs tiers sont rapprochées avec les actifs de votre CMDB. Lorsqu'une vulnérabilité importée correspond à un actif existant, un élément vulnérable est créé. Les éléments vulnérables sont automatiquement regroupés en tâches à corriger, notés en fonction du risque en fonction du contexte métier, classés par ordre de priorité et affectés aux équipes appropriées pour la correction.

Remarque :

Les intégrations tierces sont traitées séparément. Si plusieurs applications d'intégration tierces sont utilisées dans votre environnement, il n'y a pas de déduplication d'élément vulnérable (VI) entre les intégrations. Par exemple, la déduplication de VI entre Rapid7 et Qualys n'est pas disponible.

Cependant, des incohérences dans le nombre de détections entre un scanner tiers (par exemple, Qualys) et les VI de votre ServiceNow instance sont attendues, car nous dédupliquons les adresses IP, les ports, etc.

Pour plus d'informations sur les intégrations tierces prises en charge par Réponse aux vulnérabilités des applicationsIntégrer Réponse aux vulnérabilités des applications avec d'autres applications

- Intégration de CISA Known Exploit Vulnerability (KEV)
- Présentation de Microsoft Threat and Vulnerability Management Intégration des vulnérabilités
- Présentation de l'intégration de l'orchestration de correctifs HCL BigFix avec Réponse aux vulnérabilités
- Présentation de l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs à Microsoft SCCM

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Présentation des intégrations NVD
- Qualys Vulnerability Integration
- Présentation de Intégration des vulnérabilités Rapid7
- Shodan Exploit Integration
- Présentation de l'intégration de vulnérabilité Tenable
- Microsoft Security Response Center Solution Integration

  Le Microsoft Security Response Center Solution Integration est disponible avec Gestion des solutions pour vulnérabilités. Pour plus d'informations sur l'installation et la configuration de et de , reportez-vous à la Microsoft Security Response Center Solution IntegrationIntégration de solution Red Hat section Installer l'application Gestion des solutions pour Réponse aux vulnérabilités. Vous pouvez configurer, modifier, programmer et lancer sur demande le Microsoft Security Response Center Solution Integration et le Intégration de solution Red Hat à partir de l'assistant de configuration.

Remarques supplémentaires sur les intégrations

Si plusieurs déploiements sont pris en charge pour une intégration, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

- Vous pouvez installer, configurer, planifier et lancer sur demande de nombreuses applications d'intégration à partir de l'Assistant de configuration.
- Vous pouvez installer l'application à partir de l'assistant de configuration, mais la configuration n'est Intégration des vulnérabilités Rapid7 pas prise en charge pour cette intégration à partir de l'assistant de configuration. Consultez Installer Intégration des vulnérabilités Rapid7 pour plus d'informations.
- L'application Tenable pour Réponse aux vulnérabilités de Tenable est créée et gérée par Tenable. Voir leur documentation à l'adresse suivante : Tenable pour Réponse aux vulnérabilités.

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

À partir de VR v17.1, les noms d'état de processus d'intégration suivants ont été mis à jour :

Nom de l'État antérieur à la version 17.1	Nom de l'État V17.1 et suivants
Traitement	En cours de récupération
Attente terminée	En attente/en cours de traitement

Remarque : Vous pouvez afficher les pièces jointes qui sont téléchargées et traitées. Lorsque l'état de l'exécution de l'intégration est waitcomplete, il affiche le pourcentage d'intégration terminée.

Réponse aux vulnérabilités applications et CSDM tables

Réponse aux vulnérabilités des applications Les Réponse aux vulnérabilités intégrations et Nomenclature logicielle applications de vulnérabilité tierces gèrent les tables (y contribuent des données). CSDM Ces applications utilisent également des données provenant de CSDM tables générées par d'autres applications. Plusieurs ServiceNow produits bénéficient donc de ces Opérations de sécurité applications et y ajoutent de la valeur. Consultez Réponse aux vulnérabilités applications et CSDM tables pour plus d'informations.

Intégrations créées manuellement

Vous pouvez ajouter d'autres intégrations qui ne sont pas disponibles en tant qu'applications ServiceNow Store , selon vos besoins. Consultez Créer manuellement une intégration de vulnérabilité pour plus d'informations.

Présentation des intégrations NVD

Les intégrations NVD utilisent des données importées du produit National Vulnerability Database (NVD) du National Institute of Standards and Technology (NIST) pour vous aider à déterminer l'impact et la priorité des failles dans votre code. Exécutez cette intégration dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit d'analyse tiers.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Le NVD du NIST collecte à la fois des données CVE (Common Vulnerabilities and Exposures) et CPE (Common Platform Enumeration) et met ces données à la disposition du ServiceNow AI Platform®. Il s'intègre Réponse aux vulnérabilités facilement pour cartographier les vulnérabilités CVE et CPE, enrichissant ainsi les données de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Il existe un utilisateur d'exécution configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Une fois installée, l'intégration de l'API d'intégration de base de données de vulnérabilité nationale du NIST (CVE uniquement) est appelée automatiquement en tant que tâche planifiée et s'exécute quotidiennement. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Conseil : L'activation de ce module d'extension pour les instances de production peut nécessiter une licence distincte.

Versions disponibles

Version de mise en production	Notes de publication
Réponse aux vulnérabilités Intégration avec NVD v1.2	

Importation initiale des données de vulnérabilité avec les intégrations NVD et CWE

1. Effectuez une importation initiale des données CWE avec l'intégration complète CWE 2000.

   Consultez Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE. Vous effectuez des mises à jour CWE **sur demande** à partir de l'enregistrement d'intégration par défaut, et vous devez le configurer.

   Remarque : Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. Le jour par défaut pour la mise à jour NVD est le **lundi**, **chaque semaine**.

2. Vérifiez que l'intégration avec l'application NVD est installée et qu'une Réponse aux vulnérabilités importation de données initiale à partir de l'API (CVE uniquement) ou de l'API (CVE et CPE) est réussie.

   Pour les CPE, vérifiez qu'une importation de données initiale à partir de l'API : l'intégration de la base de données des vulnérabilités nationale du NIST (CPE uniquement) est réussie.

   L'activation de ce module d'extension pour les instances de production peut nécessiter une licence distincte. Une fois le module d'extension installé, l'API NIST National Vulnerability Database Integration (CVE uniquement) est activée par défaut. Il fonctionne quotidiennement. Consultez Installer l'intégration Réponse aux vulnérabilités avec la base de données de vulnérabilité nationale NIST pour plus d'informations.

3. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Consultez la documentation de votre intégration à l'adresse Intégrations de Réponse aux vulnérabilités pour plus d'informations sur les intégrations tierces.

Comprendre les données de vulnérabilité importées et les éléments vulnérables

Dans votre ServiceNow AI Platform instance, chaque vulnérabilité importée est représentée par une entrée de vulnérabilité dans les bibliothèques sources de produits d'analyse tiers

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

comme Qualys, par exemple. Les éléments vulnérables (VI) qui sont importés et mis à jour dans votre instance sont des références à des bibliothèques tierces, telles que la Qualys bibliothèque. Une bibliothèque tierce peut, à son tour, faire référence au NVD.

Par exemple, lorsque vous ingérez des données de vulnérabilité tierces à partir d'un produit comme Qualys, vous ingérez des VI qui font référence à un QID (Qualys identificateur). Dans le cas de Qualys, ce QID fait référence à son tour à un CVE de la bibliothèque NVD. Lorsque vous cliquez sur ce QID dans une tâche de rattrapage ou un enregistrement d'élément vulnérable dans l'application Réponse aux vulnérabilités , et que vous avez exécuté les intégrations NVD et CWE pour ingérer des données, vous visualisez des données de vulnérabilité enrichies actuelles qui vous permettent de voir les relations qui existent entre vos VI et CVE, CWE et CPE.

Avant d'exécuter un produit de scanner tiers comme Qualys celui qui a sa propre bibliothèque, vous devez d'abord installer et exécuter, au minimum, l'intégration NIST National Vulnerability Database Integration-API (CVE uniquement) (comprend également des détails liés à CISA), l'intégration CWE pour ingérer des données de vulnérabilité. Ces importations de données NVD et CWE enrichissent vos Réponse aux vulnérabilités données ou Réponse aux vulnérabilités des applications avant d'importer des données avec un produit tiers.

Pour plus d'informations sur la gestion des bibliothèques NVD, CWE et tierces et sur leur affichage, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces et Afficher les Réponse aux vulnérabilités bibliothèques de vulnérabilités.

Une fois que vous avez vérifié la réussite de l'importation NVD, pour enrichir davantage vos données de vulnérabilité, Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE.

Effectuez les importations NVD et CWE avant d'importer des données de vulnérabilité avec un produit tiers. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Consultez la documentation de votre intégration à l'adresse Intégrations de Réponse aux vulnérabilités pour plus d'informations sur les intégrations tierces.

Localisation des intégrations NVD

Pour afficher les intégrations NVD, accédez à **Vulnerability Response ou Application Vulnerability Response** > **Administration** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base.

Remarque : Seule l'intégration NIST National Vulnerability Database Integration : API (CVE uniquement) est active, par défaut.

Intégrations NVD

Intégration	Description
Intégration de la base de données des vulnérabilités nationale NIST - API (CVE uniquement)	Récupère uniquement les données de vulnérabilité NIST NIST NVD (CVE). Par défaut, cette intégration est automatiquement définie pour s'exécuter quotidiennement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations NVD (suite)

Intégration	Description
NIST National Vulnerability Database Integration-API (CPE uniquement)	Récupère les données CPE à partir de NVD NIST. Cette intégration est désactivée par défaut. Activez cette intégration si vous souhaitez capturer des données CPE qui incluent un format de nom formel, une méthode de vérification des noms par rapport à un système et un format de description pour lier du texte et des tests à un nom. Ces informations sont stockées dans un logiciel vulnérable. Cette intégration est définie pour s'exécuter quotidiennement et est inactive par défaut. Pour activer cette intégration, reportez-vous à la section Activer l'API de la base de données de vulnérabilité nationale NIST (CPE UNIQUEMENT).
Intégration de la base de données des vulnérabilités nationale NIST API (CPE non mappé)	Récupère les données CPE associées aux CVE récupérées à partir de NIST NVD. Cette intégration est désactivée par défaut. Activez cette intégration si vous souhaitez capturer des données CPE qui incluent un format de nom formel, une méthode de vérification des noms par rapport à un système et un format de description pour lier du texte et des tests à un nom. Ces informations sont stockées dans une liste connexe d'enregistrement d'entrée de vulnérabilité NVD. Cette intégration est définie pour s'exécuter sur demande et est inactive par défaut. Pour activer cette intégration, reportez-vous à la section Activer l'API de la base de données de vulnérabilité nationale NIST (CPE NON MAPPÉ).

Important : L'intégration « NIST National Vulnerability Database Integration-API (CVE and CPE) » est déconseillée.

Pour les états d'exécution de l'intégration, Afficher l'état de l'exécution de l'importation de l'intégration NVD (base de données de vulnérabilité nationale) reportez-vous à la section .

Préparation aux intégrations NVD

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Préparez-vous à l'intégration en effectuant ces tâches. Les intégrations NVD supposent que vous connaissez la base de données de vulnérabilité nationale (NVD) du NIST.

Rôle requis : admin

Remarque : Avant d'exécuter les intégrations NVD, apportez les changements de configuration nécessaires en fonction de vos besoins.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE

Lesimportations de données à partir de CWE enrichissent encore les données de vulnérabilité de votre instance. Utilisez les enregistrements CWE (Common Weakness Enumeration) téléchargés à partir de la base de données CWE comme référence pour décider si une vulnérabilité doit être remontée. Exécutez cette intégration dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit d'analyse tiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôles requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Remarque : Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. Le jour par défaut pour la mise à jour NVD est le **lundi**, **chaque semaine**.

Mettez à jour régulièrement les enregistrements des faiblesses courantes de la base de données Common Weakness Enumeration. Vous pouvez également mettre à jour le script par défaut ou écrire vos propres scripts, selon vos besoins.

Chaque enregistrement CWE comprend également un article de la base de connaissances associé qui décrit la faiblesse. Vous ne pouvez pas escalader une vulnérabilité à partir de la page Common Weakness Enumerations.

- Si vous disposez du rôle administrateur, vous pouvez ajouter des référentiels à la tâche planifiée.
- Si vous disposez de sn_vul.vulnerability_read, vous pouvez exécuter la tâche planifiée.
- Si vous disposez de sn_vul.vulnerability_write, vous pouvez modifier les détails de la tâche planifiée.

Pourquoi et quand exécuter cette tâche

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.
2. Sélectionnez la tâche planifiée **Intégration complète CWE 2000** .
3. Modifiez les champs selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire d'intégration de vulnérabilité

Champ	Description
Nom	Nom de la tâche planifiée.
Actif	Indique si la tâche planifiée est active. Si vous ne souhaitez pas que la tâche s'exécute pendant une période spécifique, vous pouvez configurer les paramètres que vous souhaitez utiliser et désactiver la tâche.
Exécuter	Fréquence à laquelle vous souhaitez que la tâche s'exécute. Les champs suivants sont affichés ou masqués en fonction de votre paramètre dans ce champ. **Remarque :** La mise à jour CWE est **Sur demande** par défaut. Définissez une période planifiée antérieure à vos mises à jour NVD. Les choix sont les suivants : ○ Quotidien : choisir une **heure** ○ Hebdomadaire : (choix le plus courant) Choisissez un **jour** et une**heure** ○ Mensuel : choisissez **le jour et l'heure** ○ Périodiquement : choisissez un intervalle de **répétition**, la date et l'heure de **début** ○ Une fois : choisissez une date et une heure de **début**
Jour	Le jour où vous souhaitez que la tâche planifiée s'exécute. Si vous avez sélectionné **Hebdomadaire** dans le champ **Exécuter** , ce champ affiche les jours de la semaine. Si vous avez sélectionné **Tous les mois** dans le champ **Exécuter** , ce champ affiche les jours du mois. **Remarque :** Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. Le jour par défaut pour la mise à jour NVD est le **lundi**, **chaque semaine**.
Heure	Heure à laquelle vous souhaitez que la tâche planifiée commence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Planifiez l'exécution de la mise à jour CWE avant la mise à jour de la base de données NVD. L'heure par défaut pour la mise à jour NVD est 01:00:00
Script d'intégration	Script permettant d'extraire les données des sources de données spécifiées dans la liste connexe **Sources de données** .
Intégration source	[Lecture seule]
Instance source	[Lecture seule]
Application	[Lecture seule] Nom de l'application pour laquelle vous exécutez la tâche planifiée.
Intervalle de répétition	Nombre de jours et d'heures avant que la tâche planifiée ne s'exécute à nouveau. Ce champ s'affiche lorsque **l'option Périodique** est sélectionnée dans la liste **Exécuter** .
En cours de démarrage	Date et heure de début des mises à jour périodiques. Ce champ s'affiche lorsque **l'option Périodique** est sélectionnée dans la liste **Exécuter** .
Conditionnel	Case à cocher permettant d'ajouter des paramètres conditionnels.
Condition	Conditions d'exécution de la tâche planifiée. Ce champ s'affiche lorsque la case **Conditionnel** est cochée.
Stratégie de processeur de rapport	Stratégie d'extraction des données et de traitement de la tâche planifiée. ○ Pour extraire les données des sources de données de la liste connexe **Sources de données** à l'aide du script indiqué dans le champ **Script d'intégration** , sélectionnez **Pièce jointe de source de données**. ○ Pour sélectionner un processeur personnalisé dans le champ de **script Processeur de rapport** , sélectionnez le **processeur de rapport personnalisé**.
Script de processeur de rapport	Script à exécuter lors de l'exécution de la tâche planifiée. Ce champ s'affiche lorsque **Processeur de rapport personnalisé** est sélectionné dans la liste **Stratégie de processeur de rapport** .
Script de l'instanciateur de processeur	Script permettant de créer le processeur de rapports. Ce champ s'affiche lorsque **Processeur de rapport personnalisé** est sélectionné dans la liste **Stratégie de processeur de rapport** .

Traduction automatique

4. Cliquez avec le bouton droit de la souris sur l'en-tête pour **enregistrer** vos modifications.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Pour exécuter immédiatement la tâche planifiée, cliquez **sur Exécuter maintenant**.
   Vous revenez à la vue Intégrations de vulnérabilité.
6. Pour observer la progression de l'importation, sélectionnez à nouveau la tâche planifiée **Intégration complète CWE 2000** et sélectionnez l'onglet **Exécutions d'intégration de vulnérabilité** .

   Voir Afficher les Réponse aux vulnérabilités bibliothèques de vulnérabilités pour voir les entrées importées.

Installer l'intégration Réponse aux vulnérabilités avec la base de données de vulnérabilité nationale NIST

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit NIST National Vulnerability Database (NVD) s'intègre correctement à Réponse aux vulnérabilités. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • S'il n'est pas déjà affecté, l'administrateur système [admin] installe l'application et affecte les utilisateurs au gestionnaire de vulnérabilité ou au groupe Gestionnaire de sécurité des applications dans Réponse aux vulnérabilitésRéponse aux vulnérabilités des applications. Pour plus d'informations sur les rôles de groupe dans Réponse aux vulnérabilités la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités. Pour en savoir plus sur les rôles de groupe dans la Réponse aux vulnérabilités des applications section Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	• Le gestionnaire de vulnérabilité ou le gestionnaire de sécurité des applications supervise la configuration et vérifie les résultats attendus.

Rôle requis : admin

Remarque : Avant d'exécuter les intégrations NVD, apportez les changements de configuration nécessaires en fonction de vos besoins.

Il existe un utilisateur d'exécution configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne changez pas cette valeur.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer les intégrations NVD.
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez l'application Vulnerability Response Integration with NVD.
4. Sélectionnez la vignette de l'application.
   Des informations détaillées sur l'application que vous installez s'affichent.

   Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

5. Sélectionnez **Demander une application** et saisissez vos Now Support informations d'identification de connexion.
6. Sélectionnez **Obtenir**.
7. Entrez le **nom et** la **raison d'être de l'instance**, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demande**.
   Vous recevrez un e-mail avec des instructions d'installation détaillées.
9. Accédez à la **Tous** > **Applications système** > **Applications** > **Tous**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Après l'installation initiale, pour les modifications, reportez-vous à Modification et activités d'intégration NVD facultatives.

Activer l'API de la base de données de vulnérabilité nationale NIST (CPE NON MAPPÉ)

Pour ingérer les données CPE (Common Platform Enumeration) pour les données CVE (Common Vulnerabilities and Exposures) extraites, vous pouvez effectuer une importation de données complète avec une tâche planifiée à la demande.

Avant de commencer

L'intégration NVD-API (Unmapped CPE) de la National Institute of Standards and Technology and Technology (National Vulnerability Database Integration) du NIST capture des données (CPE) qui comprennent un format de nom formel, une méthode de vérification des noms par rapport à un système et un format de description pour lier du texte et des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

tests à un nom. Ces informations sont stockées dans une liste connexe d'enregistrement d'entrée de vulnérabilité NVD.

Rôle requis : sn_vul.vulnerability_admin ou Gestionnaire App-Sec

Procédure

1. Accédez à la **Tous** > **Vulnerability Response ou Application Vulnerability Response** > **NVD** > **Intégrations**.
2. Sélectionnez l'intégration NIST National Vulnerability Database Integration-API (CPE non mappé).
3. Sélectionnez la case à cocher **Activé**.

   Remarque : L'intégration est préconfigurée pour s'exécuter sur demande. En activant l'intégration, elle s'exécutera automatiquement après l'intégration de l'API d'intégration NIST NVD (CVE uniquement). La modification de tout autre paramètre d'intégration nécessite à la fois ServiceNow une expertise et Réponse aux vulnérabilités et et peut entraîner des données incomplètes.

   a. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.

   b. Sélectionnez Intégration de la base de données des vulnérabilités nationale du NIST : intégration de l'API (CPE non mappé).

   c. Sélectionnez l'onglet **Détails de l'intégration** .
   Quelle que soit la valeur du champ **Importer depuis** , les CVE de tous les CVE récupérés sont récupérés.
4. Sélectionnez **Exécuter maintenant** pour effectuer une première exécution d'intégration de support complète.
   Une fois l'importation initiale terminée, les importations planifiées des données delta reprennent. Pour les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation de l'intégration NVD (base de données de vulnérabilité nationale).

Activer l'API de la base de données de vulnérabilité nationale NIST (CPE UNIQUEMENT)

Pour ingérer des données CPE (Common Platform Enumeration), vous pouvez effectuer une importation de données complète avec une tâche planifiée quotidienne.

Avant de commencer

L'intégration de la base de données de vulnérabilité nationale (NVD)-API (CPE uniquement) du National Institute of Standards and Technology (NIST) capture des données (CPE) qui incluent un format de nom formel, une méthode de vérification des noms par rapport à un système et un format de description pour lier du texte et des tests à un nom. Ces informations sont stockées dans une table de logiciels vulnérables.

Rôle requis : sn_vul.vulnerability_admin ou Gestionnaire App-Sec

Procédure

1. Accédez à la **Tous** > **Vulnerability Response ou Application Vulnerability Response** > **NVD** > **Intégrations**.
2. Sélectionnez l'intégration NIST National Vulnerability Database Integration-API (CPE uniquement).
3. Sélectionnez la case à cocher **Activé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'intégration est préconfigurée pour s'exécuter quotidiennement. La modification de tout autre paramètre d'intégration nécessite à la fois ServiceNow une expertise et peut entraîner des données incomplètes.
- L'activation de cette intégration active automatiquement les intégrations NIST National Vulnerability Database Integration-API (CVE uniquement) et NIST National Vulnerability Database Integration-API (CPE non mappé) et définit son champ Exécuter sur demande.
- En outre, une exécution réussie de l'intégration de la base de données des vulnérabilités nationale NIST (CPE UNIQUEMENT) déclenchera automatiquement l'API d'intégration de la base de données des vulnérabilités nationale du NIST (CVE UNIQUEMENT). Et la réussite de l'API d'intégration de la base de données de vulnérabilité nationale du NIST (CVE UNIQUEMENT) déclenchera automatiquement l'API d'intégration de la base de données de vulnérabilité nationale du NIST (CPE non mappé).

Remarque : Le champ Date d'importation de l'intégration de l'API (CPE uniquement) est vide par défaut. Laissez-le vide pour extraire les données des 357 derniers jours.

Pour récupérer les données historiques lors de votre importation initiale à partir de l'analyse NVD, définissez une date de début dans l'enregistrement d'intégration NIST National Vulnerability Database Integration- API (CPE uniquement).

a. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.

b. Sélectionnez NIST National Vulnerability Database Integration-API (CPE uniquement) Integration.

c. Sélectionnez l'onglet **Détails de l'intégration** .

d. Définissez la valeur du champ **Importer depuis** sur la date la plus ancienne que vous souhaitez récupérer.

Chaque importation réussie réinitialise cette date à la date et à l'heure du jour sélectionné.

4. Sélectionnez **Exécuter maintenant** pour effectuer une première exécution d'intégration de support complète.

   Une fois l'importation initiale terminée, les importations planifiées des données delta reprennent. Pour les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état de l'exécution de l'importation de l'intégration NVD (base de données de vulnérabilité nationale).

Modification et activités d'intégration NVD facultatives

Configurez des modifications facultatives spécifiques pour les intégrations NVD.

Remarque : La modification d'autres paramètres d'intégration NVD, autres que ceux répertoriés ici, nécessite une expertise avancée ServiceNow et Réponse aux vulnérabilités dépasse le cadre de la documentation du produit.

Effectuer une importation manuelle d'intégration NVD

Si votre importation initiale a échoué, ou si vous ne souhaitez pas attendre l'importation initiale planifiée, vous pouvez effectuer une importation de données complète indépendamment de la tâche planifiée quotidienne ou hebdomadaire.

Avant de commencer

Remarque : Les intégrations NIST National Vulnerability Database Integration-API (CPE uniquement) et NIST National Vulnerability Database Integration-API (CPE non mappé) sont inactives par défaut. Voir Activer l'API de la base de données de vulnérabilité nationale NIST (CPE UNIQUEMENT) et Activer l'API de la base de données de vulnérabilité nationale NIST (CPE NON MAPPÉ) pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tous** > **Vulnerability Response ou Application Vulnerability Response** > **Administration** > **Intégrations**.
2. Choisissez et intégrez, par exemple, l'intégration de l'API (CVE uniquement) NIST National Vulnerability Database Integration.
3. Sélectionnez **Exécuter maintenant**.

   Remarque : Si l'intégration NIST National Vulnerability Database Integration-API (CPE non mappé) est activée, les données CPE associées sont stockées dans la liste connexe Logiciel vulnérable de l'entrée de vulnérabilité NVD. Consultez Réponse aux vulnérabilités Champs du formulaire de vulnérabilité.

4. Pour les états d'exécution de l'intégration, Afficher l'état de l'exécution de l'importation de l'intégration NVD (base de données de vulnérabilité nationale) reportez-vous à la section .

Afficher l'état de l'exécution de l'importation de l'intégration NVD (base de données de vulnérabilité nationale)

Utilisez la liste connexe **Exécutions d'intégration de vulnérabilité** pour vérifier le succès de vos exécutions d'intégration, localiser les problèmes et éclairer vos décisions de correction.

Avant de commencer

Pour afficher l'état de l'exécution de l'importation de l'intégration NVD :

- Réponse aux vulnérabilités et l'intégration de Vulnerability Response avec l'application d'intégration NVD doivent être installés et configurés.
- Les importations d'intégration NVD doivent être en cours d'exécution. L'intégration NIST National Vulnerability Database Integration-API (CVE uniquement) s'exécute par défaut.

  Remarque : Les intégrations NIST National Vulnerability Database Integration-API (CPE uniquement) et NIST National Vulnerability Database Integration-API (Unmapped CPE) sont inactives par défaut. Voir Activer l'API de la base de données de vulnérabilité nationale NIST (CPE UNIQUEMENT) et Activer l'API de la base de données de vulnérabilité nationale NIST (CPE NON MAPPÉ) pour plus d'informations.

Rôle requis : sn_vul.vulnerability_admin ou Gestionnaire App-Sec

Pourquoi et quand exécuter cette tâche

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration.

Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite de temps d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

également de plus d'une heure. Le dernier enregistrement traité datant de plus d'une heure indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Si vous n'utilisez pas le tableau de l'état d'exécution de l'intégration NVD, Accédez à **Tous** > **Vulnerability Response ou Application Vulnerability Response** > **Administration** > **Intégrations**.
2. Sélectionnez un **lien** pour une intégration.
3. Sélectionnez la liste connexe **Exécutions d'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.

   Trouble?

   Les causes les plus courantes d'un échec d'exécution sont les suivantes :

   - Interruption du réseau.
   - Un problème dans le transfert des données entraînant des données corrompues pendant la transformation.

   Si l'une de ces conditions est réunie, sélectionnez **Exécuter maintenant** et réexécutez l'intégration.

Information associée

Réponse aux vulnérabilités Champs du formulaire de vulnérabilité

Ajouter des CVE à des entrées tierces

Les informations sur la vulnérabilité et l'exposition communes (CVE) peuvent être liées à une seule vulnérabilité tierce. Il est généralement ajouté lors de l'importation d'une intégration tierce, mais vous pouvez ajouter manuellement plusieurs CVE (vulnérabilités).

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

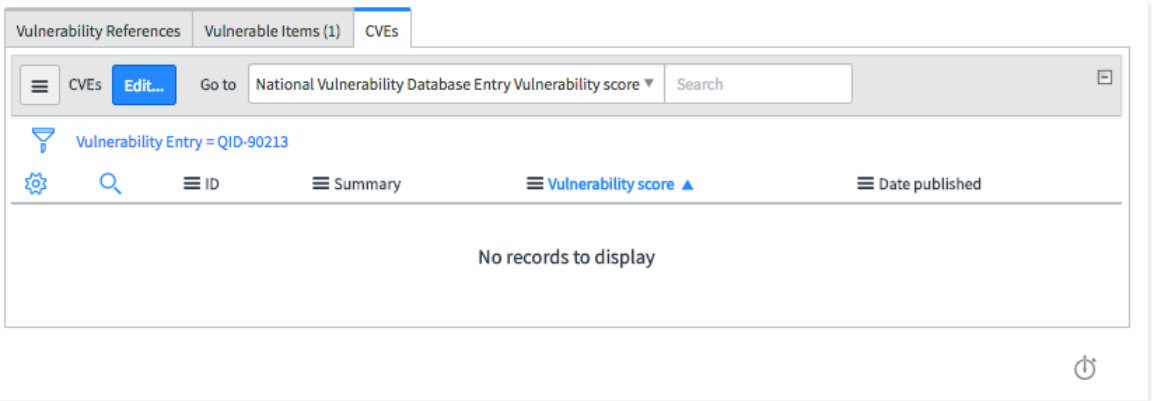
Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers**.
2. Ouvrez un enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur l'onglet de la liste connexe **CVE** .



4. Cliquez sur **Modifier**.
5. Choisissez les CVE à ajouter.

Remarque : Vous pouvez utiliser des filtres de condition pour affiner la collection CVE.

6. Cliquez sur **Enregistrer**.

Information associée

Réponse aux vulnérabilités Champs du formulaire de vulnérabilité

Afficher les Réponse aux vulnérabilités bibliothèques de vulnérabilités

Vous pouvez afficher les données de vulnérabilité importées à partir de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou de tiers pour décider s'il y a lieu d'escalader une tâche de rattrapage.

Avant de commencer

Rôle requis : sn_vul.remediation_owner

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Bibliothèques**.

Pour plus d'informations sur des champs spécifiques, reportez-vous à la section Réponse aux vulnérabilités Champs du formulaire de vulnérabilité.

Les bibliothèques suivantes sont disponibles :

Bibliothèques	Description
NVD	Liste des vulnérabilités trouvées par NVD et comprend des listes de vérification de sécurité, des failles logicielles liées à la sécurité, des erreurs de configuration, des noms de produits et des mesures d'impact, y compris les exploits.
CWE	Liste des types de faiblesses logicielles développés par la communauté. Chaque enregistrement CWE comprend également un article de la base de connaissances associé qui décrit la faiblesse. Vous ne pouvez

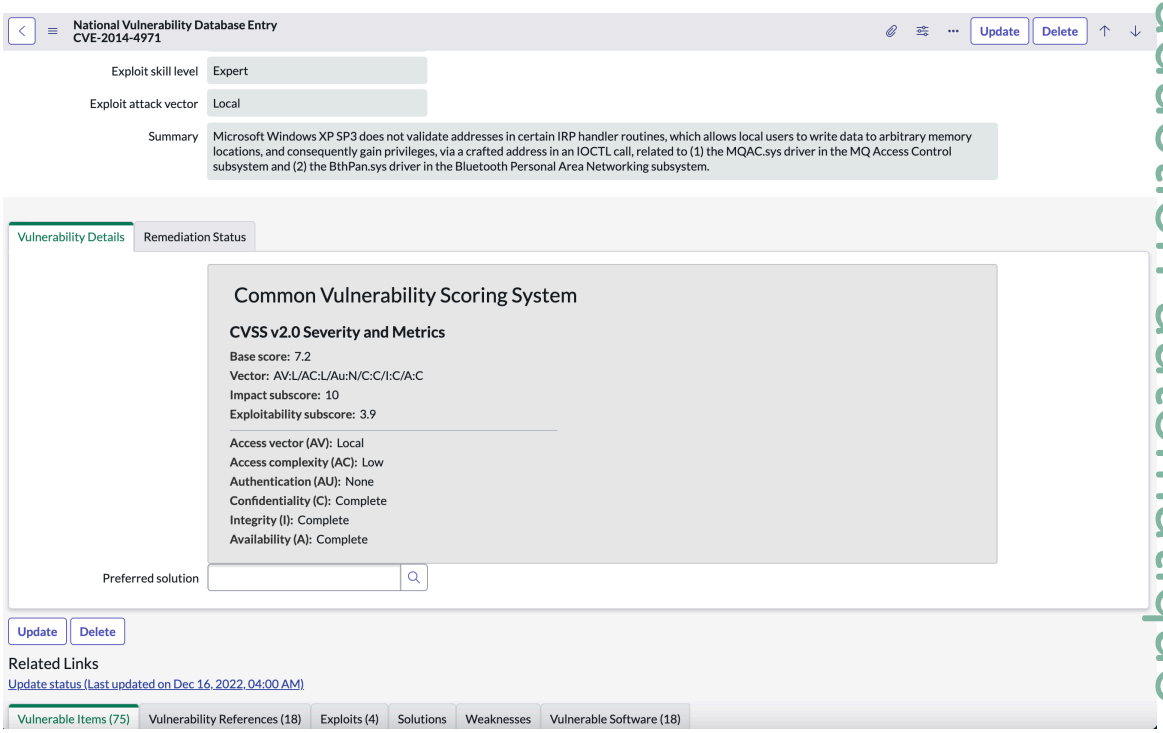
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bibliothèques	Description
	pas escalader une vulnérabilité à partir de l'écran Common Weakness Enumerations, à titre de référence uniquement.
Tiers	Liste des vulnérabilités tierces importées dans votre instance. Contient une liste des références, des éléments vulnérables, des exploits et des CVE connexes.

2. Choisissez une bibliothèque pour afficher les vulnérabilités.
3. Cliquez sur un lien dans la liste pour ouvrir un enregistrement.

   Un enregistrement CVE dans la bibliothèque National Vulnerabilities Database Entries De plus amples informations sont disponibles dans la **section Liens connexes**. Après une importation de données, vous pouvez sélectionner une vulnérabilité et explorer ses relations avec les éléments vulnérables, les exploits, les solutions possibles, les correctifs potentiels et toute référence aux articles de la base de connaissances dans la base de connaissances HI. S'il Gestion des solutions pour vulnérabilités est installé, vous pouvez afficher une solution préférée sur les enregistrements NVD si une solution est disponible.



Intégration de CISA Known Exploit Vulnerability (KEV)

L'intégration Réponse aux vulnérabilités au catalogue des vulnérabilités exploitées connues (KEV) de CISA ingère des données pour vous aider à hiérarchiser et à corriger efficacement ces vulnérabilités.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

CISA permet une remédiation urgente et prioritaire des vulnérabilités activement exploitées pour les agences gouvernementales et les entreprises.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À propos de CISA

La Cybersecurity & Infrastructure Security Agency (CISA) est une agence américaine de cybersécurité et de sécurité des infrastructures qui publie un rapport sur les vulnérabilités les plus exploitées. Il s'intègre Réponse aux vulnérabilités facilement pour cartographier les vulnérabilités courantes et les vulnérabilités CVE (Common Vulnerabilities), enrichissant ainsi les données de votre instance. Ces informations sont ensuite déployées dans la table Entrées de vulnérabilité tierces. La date d'échéance la plus proche est prise en compte pour le déploiement vers les éléments vulnérables.

Remarque : La case **à cocher CISA existe** pour les CVE récupérées par CISA.

Valeurs récupérées de l'intégration CISA :

- ID des CVE
- Date d'échéance
- Date d'ajout
- Fournisseur/Projet
- Produit
- Rançongiciel connu (à partir de la version 21.0 de , un nouveau champ **connu pour être utilisé dans les campagnes de**Réponse aux vulnérabilités rançongiciels est ingéré à partir du catalogue des vulnérabilités connues exploitées (KEV) de CISA. Cela est indiqué par le marquage du champ **Rançongiciel connu** sur la table de base de données Entrée de vulnérabilité nationale. Le marqueur est défini au niveau des vulnérabilités et expositions communes (CVE) et déployé jusqu'à l'entrée tierce (TPE).

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Travaux planifiés

L'intégration CISA est invoquée automatiquement en tant que tâche planifiée quotidienne. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Versions disponibles

Version de mise en production	Notes de publication
Réponse aux vulnérabilités v16.5, v18.0 Réponse aux vulnérabilités Intégration avec CISA v1.0, v1.2	

Affichage de l'intégration CISA

Pour afficher l'intégration CISA, accédez à **Réponse aux vulnérabilités** > **Administration** > **Intégrations** > **Intégration de vulnérabilité de l'exploit connu CISA**.

Les intégrations suivantes sont incluses dans le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Seule l'intégration CISA est active, par défaut.

Intégration CISA

Intégration	Description
Intégration de la Cybersecurity & Infrastructure Security Agency (CISA)	Récupère les données de vulnérabilité CISA (CVE) et enrichit les données de vulnérabilité existantes. Cette intégration est définie automatiquement pour s'exécuter quotidiennement.

Pour afficher les données dans les vulnérabilités tierces, reportez-vous à la section Afficher les Réponse aux vulnérabilités bibliothèques de vulnérabilités.

Préparation de l'intégration CISA

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Préparez-vous à l'intégration en effectuant ces tâches. L'intégration CISA Known Exploited Vulnerability suppose que vous connaissez la Cybersecurity & Infrastructure Security Agency (CISA).

Rôle requis : sn_vul.vulnerability_admin

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Remarque : Avant d'exécuter l'intégration CISA, apportez tout changement de configuration nécessaire en fonction de vos besoins.

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer l'application ServiceNow® Vulnerability Response Integration with CISA

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le conseiller en vulnérabilité exploitée connue de la Cybersecurity & Infrastructure Security Agency (CISA) s'intègre à Réponse aux vulnérabilités. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que l'application Réponse aux vulnérabilités Integration with NVD est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer l'intégration Réponse aux vulnérabilités avec la base de données de vulnérabilité nationale NIST reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte des utilisateurs au gestionnaire de vulnérabilités dans Réponse aux vulnérabilités. Pour plus d'informations sur les rôles de groupe dans Réponse aux vulnérabilités la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités. • Le gestionnaire de vulnérabilité supervise la configuration et vérifie les résultats attendus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : admin

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer le Vulnerability Response integration with CISA .
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez l'application Vulnerability Response integration with CISA .
4. Sélectionnez la vignette de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

5. Sélectionnez **Demander une application** et saisissez vos Now Support informations d'identification de connexion.
6. Sélectionnez **Obtenir**.
7. Entrez le **nom et** la **raison d'être de l'instance**, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demande**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Remarque : Aucune configuration n'est requise pour l'intégration CISA .

Présentation de l'intégration de l'EPSS (Exploit Prediction Scoring System)

Vue d'ensemble de l'intégration d'EPSS avec Réponse aux vulnérabilités.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Vue d'ensemble de l'intégration

L'intégration du système de notation de prédiction d'exploit (EPSS) importe les données EPSS relatives aux vulnérabilités et expositions courantes (CVE) à partir de First.org pour classer les vulnérabilités par ordre de priorité et corriger les vulnérabilités. Pour plus d'informations, reportez-vous à la section https://www.first.org . L'Exploit Prediction Scoring System (EPSS) est un effort basé sur les données pour estimer la probabilité (probabilité) qu'une vulnérabilité logicielle soit exploitée dans la nature. Le modèle EPSS produit un score de probabilité compris entre 0 et 1 (0 et 100 %). Plus le score est élevé, plus la probabilité qu'une vulnérabilité soit exploitée est élevée.

Les importations de données à partir de l'intégration EPSS enrichissent davantage les données NVD dans votre instance. Si les enregistrements NVD ne sont pas présents, cela créera un espace réservé dans la table CVE et ajoutera des détails EPSS dans la même

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

table. Exécutez cette intégration dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit d'analyse tiers.

Important : Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est VR. Système. Ne modifiez en aucun cas cette valeur.

Importation initiale de données avec l'intégration EPSS

1. Effectuez une importation initiale de données EPSS avec l'intégration First.org EPSS. Pour plus d'informations, consultez Configurer et exécuter une tâche planifiée pour mettre à jour les enregistrements CVE avec les données EPSS.

   Important : Vous effectuez des mises à jour de l'EPSS **tous les jours** à partir de l'enregistrement d'intégration par défaut, et vous devez le configurer si vous souhaitez qu'il s'exécute en tant que tâche planifiée.

2. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Pour plus d'informations, consultez Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.

   Important : Il est recommandé d'effectuer les intégrations NIST National Vulnerability Database Integration-API (CVE uniquement) avant EPSS.

Effectuez les importations EPSS avant d'importer des données de vulnérabilité avec un produit tiers. Les bibliothèques tierces sont mises à jour en tant que travaux planifiés. Consultez votre documentation d'intégration sur Intégrations Vulnerability Response pour plus d'informations sur les intégrations tierces.

Important : L'intégration suivante est incluse dans le système de base. L'intégration est active par défaut.

Après l'exécution initiale, les travaux planifiés du système de base exécutent automatiquement les intégrations dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Lors de l'activation de l'intégration de l'EPSS, les champs Score de l'EPSS, Centile de l'EPSS et Dernière modification de l'EPSS sont ajoutés à la table Entrées de vulnérabilité. Pour les CVE existants, ces champs sont mis à jour automatiquement une fois la tâche d'importation initiale terminée. Si de nouveaux CVE sont ajoutés à la table Entrées de vulnérabilité après l'achèvement de la tâche planifiée EPSS, les CVE nouvellement ajoutés indiqueront leur source en tant qu'EPSS. Les scores sont déployés sur les TPE existants à partir des CVE de la table NVD, à l'aide du système `Rollup EPSS score from NVD to TPEs calculator`de base. Vous pouvez également modifier le calculateur. Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs de cumul.

Information associée

Créer un Réponse aux vulnérabilités calculateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer et exécuter une tâche planifiée pour mettre à jour les enregistrements CVE avec les données EPSS

Personnalisez la tâche planifiée du système de base pour mettre à jour les enregistrements CVE avec les données EPSS.

Avant de commencer

Important : Vous devez télécharger et activer le module d'extension Vulnerability Response integration with CISA (com.snc.vulnerability.cisa) pour activer l'intégration de l'EPSS.

Voici la liste des nouveaux champs ajoutés dans la table NVD pour stocker les données de l'EPSS.

- Score de l'EPSS
- Centile de l'EPSS
- Dernière modification de l'EPSS

Remarque : Configurez la vue de liste ou la vue de formulaire selon les besoins pour afficher les champs récemment ajoutés.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Les importations de données à partir de l'intégration EPSS enrichissent davantage les données NVD dans votre instance. Si les enregistrements NVD ne sont pas présents, cela créera un espace réservé dans la table CVE et ajoutera des détails EPSS dans la même table. Exécutez cette intégration dans le cadre de votre configuration initiale de Vulnerability Response et publiez l'importation de données de vulnérabilité dans votre instance.

Remarque : Par défaut, l'intégration de l'EPSS First.org est à l'état **Actif** . La tâche planifiée du système de base est configurée, par défaut, pour s'exécuter quotidiennement.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.
2. Recherchez et sélectionnez First.org intégration de l'EPSS.
3. Modifiez les champs selon vos besoins.
4. Cliquez avec le bouton droit de la souris sur l'en-tête pour **enregistrer** vos modifications.
5. Sélectionnez **Exécuter maintenant** pour exécuter immédiatement la tâche planifiée.
   Vous revenez à la vue Intégrations de vulnérabilité.
6. Sélectionner **First.org EPSS** > **Onglet Exécutions d'intégration de vulnérabilité** pour afficher la progression de l'importation.
   Lors de l'achèvement réussi de la tâche planifiée, les scores de l'EPSS, le centile et l'horodatage du score de l'EPSS modifié sont mis à jour sur les CVE.

Que faire ensuite

- Consultez Ajouter une condition de score EPSS dans la règle métier du calculateur de risque.
- Voir Afficher les Réponse aux vulnérabilités bibliothèques de vulnérabilités pour voir les entrées importées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter une condition de score EPSS dans la règle métier du calculateur de risque

Modifier la règle métier pour ajouter une condition de score EPSS au calculateur de risque.

Avant de commencer

Remarque : La procédure suivante est requise pour que les mises à jour de l'EPSS sur les vulnérabilités soient déployées jusqu'aux éléments vulnérables.

Rôle requis : sn_vul.manage_risk_score_configuration

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Règle métier**.
2. Recherchez **Définir le marqueur Recalculer**.

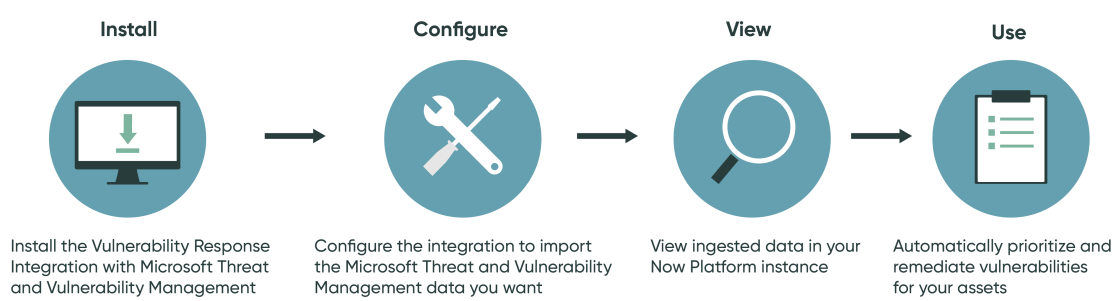
   Remarque : Il existe deux `Set recalculate flag` règles métier. Vous pouvez utiliser l'un ou l'autre.

3. Accédez à l'onglet **Quand exécuter** .
4. Sélectionnez **Ajouter une clause « OU »** et sélectionnez Score EPSS dans le **champ Choisir** et les changements dans le champ **Choisir un opérateur** .
5. Sélectionnez **Mettre à jour**.

Présentation de Microsoft Threat and Vulnerability Management Intégration des vulnérabilités

L'intégration Réponse aux vulnérabilités à l'application Gestion des menaces et des vulnérabilités Microsoft (MS TVM) utilise les données importées de MS TVM pour vous aider à hiérarchiser et à corriger les vulnérabilités de vos actifs. L'application est disponible avec un abonnement distinct du ServiceNow Store.

Vous pouvez utiliser l'intégration de MS TVM Vulnerability pour importer des données d'analyseurs tiers concernant vos actifs et vos vulnérabilités. Vous pouvez ensuite afficher les rapports sur les vulnérabilités et les éléments vulnérables sur les tableaux de Réponse aux vulnérabilités bord.



Versions disponibles

Version de mise en production	Notes de publication
Réponse aux vulnérabilités Intégration avec MS TVM v2.2	Pour plus d'informations sur les versions publiées de l'application Vulnerability

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Version de mise en production	Notes de publication
	Response, la compatibilité et les changements de schéma, consultez l'article Vulnerability Response Compatibility Matrix and Release Schema Changes [KB0856498] dans la base de connaissances HI .

Séparation de domaine et MS TVM

Importez les données d'intégration de vulnérabilité dans un domaine spécifié en affectant un utilisateur dans ce domaine pour exécuter les intégrations. Pour créer des importations séparées par domaine pour MS TVM Vulnerability Integration, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

Termes et fonctionnalités clés des intégrations

Éléments vulnérables et vulnérabilités

Un élément vulnérable est créé dans votre ServiceNow AI Platform instance lorsque :

- Une vulnérabilité importée à partir d'un scanner tiers est mise en correspondance avec un actif existant (élément de configuration) dans votre CMDB). Le produit MS TVM appelle ces correspondances des vulnérabilités.
- Une vulnérabilité importée à partir d'un scanner tiers ne correspond pas à un actif existant dans votre CMDB. Dans ce cas, un élément de configuration (CI) sans correspondance est également créé avec un élément vulnérable.

  Utilisez le moteur Identification et réconciliation (IRE) pour créer des CI dans deux nouvelles classes lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte. Dans le cas contraire, des CI sans correspondance sont créés dans les classes de CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation.

Entrées de vulnérabilité tierces

Les entrées de vulnérabilité tierces sont importées à partir d'analyseurs tiers tels que MS TVM et sont répertoriées dans la table Entrées de vulnérabilité tierces de votre ServiceNow AI Platform instance. En outre, les entrées de la base de données de vulnérabilité nationale (CVE) sont importées de MS TVM. Les informations d'exploitation associées à ces deux types d'entrées proviennent de MS TVM. Ces informations d'exploitation peuvent être utilisées pour le calcul du risque.

Remarque : Une vulnérabilité tierce n'est récupérée que pour les vulnérabilités auxquelles aucune CVE n'a été affectée. MS TVM peut ajouter un nom temporaire pour la vulnérabilité, par exemple, `TVM-XXXX-XXXX`. Ce nom est mis à jour après l'affectation d'un ID CVE.

Élément de configuration (CI)

Les CI sont les actifs existants répertoriés dans votre CMDB.

Élément découvert

Les éléments détectés sont les actifs ingérés à partir de l'importation de machine MS TVM qui correspondent aux CI existants dans votre CMDB.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si aucune correspondance n'est trouvée, un CI est créé dans la classe CI sans correspondance du CMDB. Activez le module d'extension Modèles de classe CI CMDB, le moteur Identification et rapprochement (IRE) crée des CI à l'aide de nouvelles classes. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation. Si le CI d'origine sans correspondance est reclassé, les enregistrements des éléments détectés sont mis à jour pour refléter cet état. Les éléments détectés vous donnent une visibilité sur la façon dont les actifs sont identifiés et mappés aux CI dans le CMDB.

Règles de recherche de CI

Lorsque les données sont importées à partir de MS TVM, Réponse aux vulnérabilités utilise automatiquement les données de la machine (actif) pour rechercher des correspondances dans le CMDB. Les règles de recherche de CI sont utilisées pour identifier les CI et les ajouter aux enregistrements de VI lors de la création de VI.

Instance

Une instance fait référence à plusieurs comptes de MS TVM. Chaque compte peut être une instance de l'application MS TVM.

Intégration

Une intégration est une tâche planifiée qui récupère des informations à partir d'une source tierce, telle que l'intégration des machines MS TVM.

Déploiement

Lorsqu'une intégration prend en charge le multisource, une seule existence d'intégration est considérée comme un déploiement de votre intégration. Un déploiement fait référence aux intégrations et aux produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de MS TVM dans votre environnement.

L'intégration MS TVM comprend également les fonctionnalités clés suivantes :

- Vous pouvez identifier les actifs dans votre environnement et mettre à jour les CI sur vos éléments détectés, éléments vulnérables et enregistrements de détection existants pour vous donner plus de détails sur vos vulnérabilités.
- Vous pouvez planifier le moment où vous souhaitez que les tâches s'exécutent pour toutes les intégrations MS TVM. Vous pouvez également exécuter des travaux planifiés sur demande.
- Vous pouvez regrouper les éléments vulnérables.
- Vous pouvez configurer des règles de recherche de CI pour définir comment les données d'actifs de sources tierces sont utilisées pour identifier les CI dans votre CMDB.

Rôles ServiceNow AI Platform requis

Les tâches d'intégration nécessitent les rôles suivants dans votre ServiceNow AI Platform instance.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'administrateur système utilise l'Assistant de configuration pour installer l'application MS TVM. S'il n'est pas affecté, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'assistant de configuration.

sn_vul.vulnerability_admin

Une fois affecté, l'administrateur de vulnérabilité termine la configuration des intégrations MS TVM dans l'assistant de configuration. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités et à ses enregistrements. L'administrateur de vulnérabilité configure toutes les applications et règles pour les Réponse aux vulnérabilités intégrations tierces installées.

sn_vul_msft_tvm.configure_integration

Ce rôle contient le rôle granulaire `sn_vul_msft_tvm.read_integration` . Les utilisateurs disposant de ce rôle peuvent configurer l'intégration de Vulnerability Response avec l'application Microsoft Threat and Vulnerability Management.

sn_vul_msft_tvm.read_integration

Les utilisateurs disposant de ce rôle ne peuvent afficher l'intégration de Vulnerability Response qu'avec les enregistrements de l'application Microsoft Threat and Vulnerability Management.

Groupe de réponse aux vulnérabilités

Par défaut, le groupe Réponse aux vulnérabilités est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Réponse aux vulnérabilités héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner.

Intégrations MS TVM

Le multisource est pris en charge pour toutes les intégrations MS TVM. Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'assistant de configuration dans Réponse aux vulnérabilités. Vous installez et configurez également l'intégration avec l'application MS TVM à partir de l'assistant Réponse aux vulnérabilités de configuration.

Pour afficher les intégrations MS TVM, accédez à **Intégration de vulnérabilité Microsoft TVM** > **Administration** > **Intégrations**. Réponse aux vulnérabilités fournit des intégrations avec les points de terminaison MS TVM pour importer les données en fonction des intervalles de temps planifiés. Les intégrations suivantes sont incluses dans le système de base.

Intégrations MS TVM

Séquence d'exécution	Planifier	Intégration	Description
1	Quotidien	Intégration des recommandations Microsoft TVM	Récupère une liste de toutes les recommandations de sécurité activables pour corriger les vulnérabilités.
2	Quotidien	Intégration de Microsoft TVM Vulnerability (CVE)	Récupère la liste des entrées de la base de données de vulnérabilité nationale et des entrées de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations MS TVM (suite)

Séquence d'exécution	Planifier	Intégration	Description
			vulnérabilité tierce, ainsi que les informations relatives à leur exploitation.
3	Quotidien	Intégration des machines Microsoft TVM	Récupère toutes les données d'actif (machine), y compris les balises machine, à partir de Microsoft TVM et les traite dans votre instance.
4	Hebdomadaire **Remarque :** Après l'installation, cette intégration est exécutée automatiquement après l'importation des machines.	Intégration des vulnérabilités des machines Microsoft TVM (importation complète)	Récupère toutes les vulnérabilités ouvertes sur tous les actifs.
5	Quotidien	Intégration des vulnérabilités des machines Microsoft TVM (importation Delta)	Récupère toutes les informations qui ont changé dans l'importation complète des vulnérabilités de l'organisation, y compris les vulnérabilités nouvelles, corrigées et mises à jour.

Les éléments vulnérables sont regroupés en tâches de rattrapage en fonction des règles de groupe que vous définissez et sont affectés au rattrapage en fonction de vos règles d'affectation. Pour plus d'informations, consultez Réponse aux vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage et Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Règles de recherche de CI

Lorsque les données sont importées à partir de MS TVM, Réponse aux vulnérabilités utilise automatiquement les données de la machine (actif) pour rechercher des correspondances dans le Base de données de gestion des configurations (CMDB). Les règles de recherche de CI sont utilisées pour identifier les CI et les ajouter aux enregistrements de VI lors de leur création. Pour en savoir plus sur le fonctionnement des règles de recherche de CI, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Remarque : Une fois que vous avez supprimé une règle, vous ne pouvez pas la récupérer. Au lieu de supprimer une règle existante, vous devez la désactiver.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les règles de recherche MS TVM suivantes sont fournies avec le système de base :

- MAC_ADDRESS
- FQDN
- IP

Remarque : Vous pouvez utiliser plusieurs valeurs pour la IP_ADDRESS et la MAC_ADDRESS d'un actif. Une règle de recherche de CI prend en compte toutes les valeurs pour la correspondance.

Éléments découverts

Vous pouvez voir les CI qui ont été détectés lors d'une importation à partir de l'intégration des machines MS TVM.

Remarque : Le filtre par défaut de cette liste est défini sur Sans correspondance. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour plus d'informations, consultez Éléments détectés.

Balises d'ordinateur

Les balises d'ordinateur, également appelées balises d'hôte, sont utilisées pour organiser et suivre les actifs de votre organisation. Vous attribuez des balises à vos machines.

Toutes les balises de machine sont importées dans le cadre de l'intégration des machines MS TVM. Les balises d'ordinateur sont généralement utilisées pour le filtrage dans les règles d'affectation et les règles de Réponse aux vulnérabilités tâche de rattrapage. Les balises sont affichées dans le formulaire Élément détecté.

Remarque : Exécutez l'intégration d'ordinateur MS TVM avant de créer Réponse aux vulnérabilités des règles de tâche d'affectation ou de rattrapage dans l'application Réponse aux vulnérabilités afin que toutes les balises soient disponibles pour ces règles avant que les éléments vulnérables ne soient importés et regroupés. Notez également les points suivants concernant les balises :

- Le stockage des balises n'est pas sensible à la casse. Si une balise Paris est créée, une balise PARIS ne peut pas être stockée dans la table Balise de machine. Paris et PARIS sont considérés comme la même balise machine par le système. La balise importée en premier est la balise qui est stockée et reconnue.
- L'utilisation de balises machine comme clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les clés de groupe sont des colonnes dans la table des tâches de rattrapage, tandis que les balises machine sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'ordinateur sont contrôlées par la propriété système globale sn_vul.import_host_tags. Cette propriété est définie sur vrai par défaut. La désactivation des balises les désactive dans toutes les ServiceNow AI Platform® instances.

Étapes suivantes

Une fois que vous avez téléchargé l'intégration avec Microsoft Threat and Vulnerability Management à partir de , l'installation et la ServiceNow® Store configuration sont prises en charge par l'Assistant Réponse aux vulnérabilités de configuration dans Réponse aux vulnérabilités. Pour plus d'informations, consultez Installez et configurez l'intégration Vulnerability Response avec l'application MS TVM à l'aide de l'assistant de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

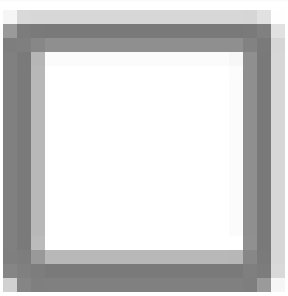
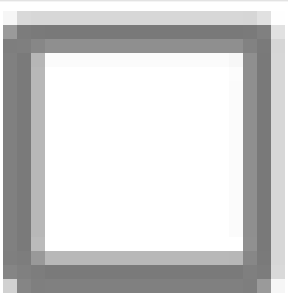
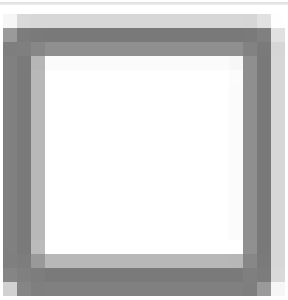
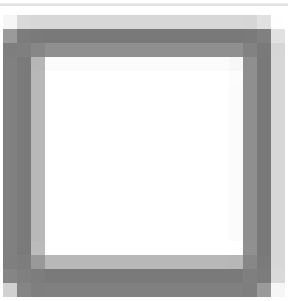
Préparation à l'intégration des vulnérabilités Microsoft Threat and Vulnerability Management

Vous pouvez préparer l'intégration de vulnérabilité ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) en effectuant des tâches de configuration.

Avant de commencer à utiliser une liste de vérification

Pour installer et configurer l'intégration avec l'application Réponse aux vulnérabilités MS TVM, vous pouvez imprimer la liste de vérification suivante et vérifier que les éléments énumérés sont renseignés avant d'installer l'application et d'importer les données de vulnérabilité dans votre ServiceNow AI Platform® instance.

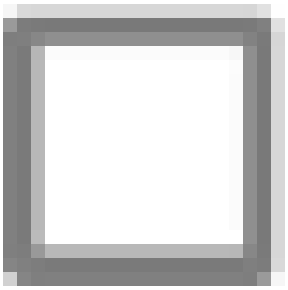
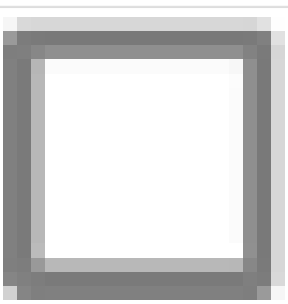
Liste de vérification de la préparation de l'intégration

Tâche	Description
	Vérifiez que vous disposez de l'un des ensembles d'informations suivants : • ClientSecret, ClientId et TenantId de votre compte MS TVM • Nom d'utilisateur, mot de passe, ClientId et TenantId de votre compte MS TVM. Pour obtenir ces informations, reportez-vous à la section Configurer Azure pour l'intégration Microsoft MS TVM.
	Si elle n'est pas déjà installée et activée, installez l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour plus d'informations sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration requiert la version 14.0 ou Réponse aux vulnérabilités ultérieure.
	Si vous n'avez pas encore l'application sur votre instance, obtenez des autorisations et téléchargez l'intégration avec l'application Réponse aux vulnérabilités MS TVM sur votre ServiceNow AI Platform® instance. Consultez .
	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance ou si vous avez besoin d'aide, contactez ServiceNow® l'assistance technique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

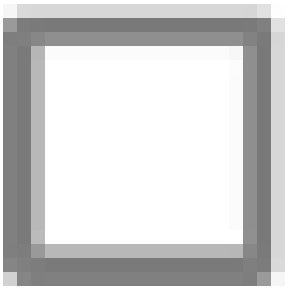
Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
	Vérifiez que vous disposez des groupes ou utilisateurs suivants pour gérer les intégrations et corriger les éléments vulnérables : **administrateur** Utilise l'assistant de configuration pour installer l'intégration de Vulnerability Response avec l'application MS TVM. S'il n'est pas affecté, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'assistant de configuration. **sn_vul.vulnerability_admin** Termine la configuration de l'intégration MS TVM. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Cet administrateur configure toutes les applications et règles VR et configure les intégrations tierces. **sn_vul_msft_tvm.configure_integration** Configure l'intégration de vulnérabilité MS TVM. Ce rôle contient le rôle granulaire sn_vul_msft_tvm.read_integration. **sn_vul_msft_tvm.read_integration** Affiche (lit) les enregistrements de l'intégration de vulnérabilité MS TVM. **Groupe de réponse aux vulnérabilités** Par défaut, le groupe Réponse aux vulnérabilités est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Réponse aux vulnérabilités héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance avant d'utiliser l'Assistant de configuration. Pour plus d'informations, consultez Créer un groupe d'utilisateurs . Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Réponse aux vulnérabilités . Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.
	Installez l'intégration Réponse aux vulnérabilités avec NVD et exécutez l'API d'intégration de la base de données des vulnérabilités nationale du NIST (CVE UNIQUEMENT).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
	Pour améliorer les performances de votre première importation, vous pouvez désactiver certaines fonctionnalités, règles ou tâches dans votre instance. • Désactivez les calculateurs de vulnérabilité si vous ne les utilisez pas. Ces calculateurs, ainsi que ceux que vous avez définis, s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour. Pour plus d'informations, consultez Désactiver le calculateur de vulnérabilité par défaut s'il n'est pas utilisé. • Lors de l'importation initiale des enregistrements, certaines règles métier liées aux notifications peuvent entraîner la génération de nombreuses notifications, ce qui peut avoir un impact sur les performances de l'ingestion.

Vous êtes prêt à Installez et configurez l'intégration Vulnerability Response avec l'application MS TVM à l'aide de l'assistant de configuration.

Configurer Azure pour l'intégration Microsoft MS TVM

Configurez votre compte dans le Microsoft portail Azure pour accéder à distance à l'API Microsoft Threat and Vulnerability Management (MS TVM). Vous avez besoin de ce compte pour pouvoir accéder au locataire MS TVM afin de recueillir des informations sur les machines, les vulnérabilités et les recommandations de sécurité.

Avant de commencer

Rôle requis : Microsoft administrateur du portail Azure.

Pourquoi et quand exécuter cette tâche

Effectuez les tâches de configuration suivantes dans votre Microsoft portail Azure avant d'installer l'application ServiceNow® pour cette intégration.

Pour vérifier que vous avez accès au contenu le plus récent, consultez le site web de la documentation Microsoft . Si vous n'avez pas créé d'ID d'application pour l'authentification OAuth 2.0 dans le Microsoft portail Azure, suivez les étapes de cette procédure.

Procédure

1. Connectez-vous au portail Azure à l'aide de vos informations d'identification d'administrateur du Microsoft portail Azure.
2. Dans le panneau de navigation de gauche du volet Accueil, cliquez sur **Azure Active Directory**.
3. Dans le volet Vue d'ensemble, cliquez sur **Inscriptions d'applications (aperçu).**
4. Dans le volet Inscriptions d'applications (aperçu), cliquez sur **Nouvelle inscription**.
   Le formulaire Enregistrer une application s'affiche.
5. Remplissez les champs du formulaire.

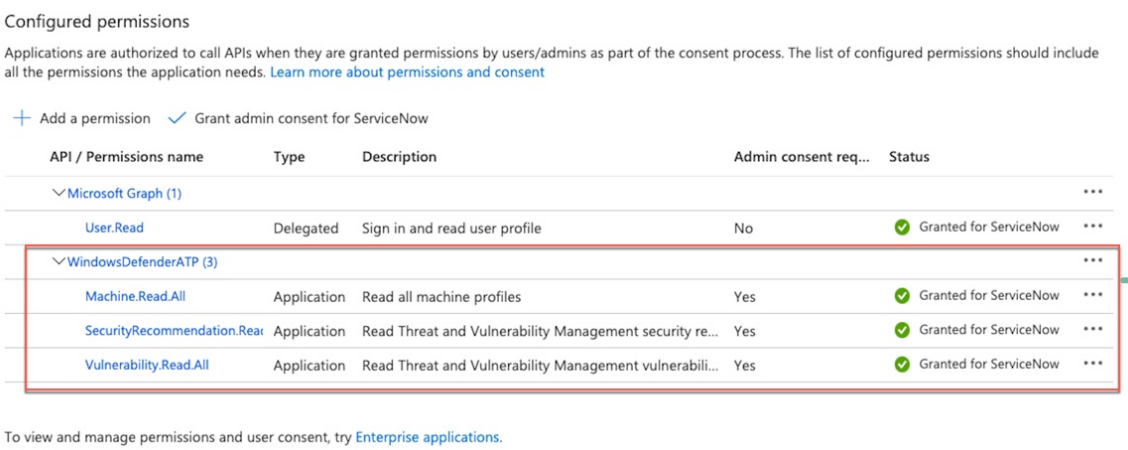
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrer un formulaire d'application

Champ	Description
Nom	Nom de l'application. Dans cet exemple, ServiceNow MS TVM Integration est saisi.
Types de compte pris en charge	Pour ce compte, dans Types de comptes pris en charge, cliquez sur **Comptes dans ce répertoire organisationnel uniquement (ServiceNow uniquement : locataire unique).**
URL de redirection (facultatif)	Si vous saisissez une valeur pour ce champ, elle n'est pas utilisée par l'intégration.

6. Cliquez sur **Inscrire**.
   L'ID (client) de l'application et l'ID du répertoire (locataire) sont créés. Saisissez ces valeurs sur la page de configuration dans les champs **ID client** et **ID de locataire** pendant l'étape de configuration de l'assistant de configuration de l'intégration ServiceNow VR-TVM. Cette étape a été décrite dans .Installez et configurez l'intégration Vulnerability Response avec l'application MS TVM à l'aide de l'assistant de configuration
7. Lorsque l'ID d'application (client) s'affiche dans le volet Intégration MS **TVM**, cliquez sur Afficher les autorisations de l'APIServiceNow.
8. Accédez à la **Demander des autorisations API** > **API utilisées par mon organisation**, puis cliquez sur **Windows Defender ATP**.
9. Dans le volet Intégration MS TVM ServiceNow - Autorisations API, cliquez sur **Ajouter une autorisation**.
10. Fournissez un accès en lecture aux machines, aux vulnérabilités et aux recommandations de



sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Cliquez sur **Accorder le consentement de l'administrateur pour <nom de votre organisation>**.

Remarque : Pour vous authentifier en tant qu'application à partir d'une ServiceNow instance, effectuez les actions suivantes :

a. Accédez à la **Intégration MS TVM ServiceNow** > **Certificats et secrets**, puis cliquez sur **Nouveau secret client**.

b. Remplissez les champs du formulaire.

Formulaire Secrets clients

Champ	Description
Description	Nom de l'application.
Date d'expiration	Date d'expiration.

c. Cliquez sur **Ajouter**.

Le champ **Valeur** est renseigné avec le nouveau secret client, qui est votre nouveau mot de passe.

Remarque : Vous aurez besoin de ce mot de passe lors de la configuration de l'intégration dans votre ServiceNow AI Platform instance. Pour plus d'informations, consultez Installez et configurez l'intégration Vulnerability Response avec l'application MS TVM à l'aide de l'assistant de configuration.

d. Enregistrez ce mot de passe dans un emplacement sécurisé. Une fois que vous avez quitté cette page, ce mot de passe n'est plus disponible.

Vous avez créé avec succès un ID d'application pour l'authentification dans le Microsoft portail Azure.

Que faire ensuite

Vous êtes prêt à configurer votre ServiceNow AI Platform® instance pour l'intégration.

Installez et configurez l'intégration Vulnerability Response avec l'application MS TVM à l'aide de l'assistant de configuration

Installez et configurez l'intégration Réponse aux vulnérabilités avec l'application Microsoft Threat and Vulnerability Management (MS TVM) afin de pouvoir utiliser les données importées de MS TVM pour classer par ordre de priorité et corriger les vulnérabilités de vos actifs.

Avant de commencer

Avant d'exécuter l'intégration ServiceNow® de vulnérabilité Microsoft Threat and Vulnerability Management, vous devez télécharger l'intégration de Vulnerability Response avec l'application Microsoft Threat and Vulnerability Management à partir de et ServiceNow Store l'installer et la configurer à l'aide de l'assistant d'installation de l'application Réponse aux vulnérabilités .

Avant d'installer l'application MS TVM, vérifiez que vous avez rempli tous les éléments de la liste de Préparation à l'intégration des vulnérabilités Microsoft Threat and Vulnerability Management vérification. Pour en savoir plus sur la configuration de votre Microsoft compte Azure, consultez Configurer Azure pour l'intégration Microsoft MS TVM.

Rôles requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- administrateur pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application Microsoft Threat and Vulnerability Management dans l'Assistant de configuration
- Administrateur de vulnérabilité (sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)) pour configurer l'application dans l'Assistant de configuration après son installation.

Pourquoi et quand exécuter cette tâche

Effectuez la procédure suivante avant d'installer et de configurer l'intégration MS TVM.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation de l'application d'intégration**.

   Après quelques instants, les applications disponibles pour installation sur votre instance s'affichent.

2. Localisez la vignette **Microsoft Threat and Vulnerability Management** , puis cliquez sur **Installer**.

   L'intégration Réponse aux vulnérabilités à l'application Microsoft Threat and Vulnerability Management que vous avez téléchargée à partir de ServiceNow Store est installée.

3. Suivez les instructions de l'assistant de configuration pour poursuivre l'installation.
   Pour plus d'informations sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.

Que faire ensuite

Une fois l'installation terminée dans l'Assistant de configuration, accédez à **Configuration de l'intégration** > **Intégrations de scanners** dans l'assistant de configuration pour poursuivre la configuration. Pour plus d'informations sur les invites fournies dans l'Assistant de configuration, reportez-vous à la section Configurer l'intégration de vulnérabilité MS TVM à l'aide de l'assistant de configuration.

Paramètres de récupération de données pour l'intégration Microsoft Threat and Vulnerability Management

Vous pouvez utiliser les paramètres de récupération de données pour vous aider à déterminer le type et le champ d'application des données que vous souhaitez importer de l'intégration de vulnérabilité ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) vers votre ServiceNow AI Platform® instance.

Les paramètres de récupération de données vous aident à contrôler les données que vous souhaitez importer. Vous pouvez définir les valeurs de ces filtres dans les instances d'intégration. Pour afficher les instances d'intégration, accédez à **Gestion des menaces et des vulnérabilités Microsoft Intégration des vulnérabilités** > **Instances d'intégration** et cliquez sur votre intégration MS TVM.

Sur la page Instance d'intégration, cliquez sur Paramètres **d'instance d'intégration** pour afficher une liste de paramètres, ou cliquez sur l'onglet **Intégrations de vulnérabilité** pour obtenir un calendrier, des détails REST, des détails d'intégration, des sources de données et des informations sur l'exécution de l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres et filtres de récupération de données pour les intégrations MS TVM dans votre ServiceNow AI Platform instance

Les paramètres suivants sont disponibles pour les intégrations MS TVM dans votre ServiceNow AI Platform instance. Ces paramètres de configuration et d'autres sont affichés sur la page Instance d'intégration de votre ServiceNow AI Platform instance. Vous préférez peut-être conserver ces paramètres dans leurs paramètres par défaut pour les premières exécutions d'intégration.

MS TVM.

vi_size_limit

Définit le nombre d'enregistrements d'éléments vulnérables à inclure dans l'ensemble des résultats de l'intégration des vulnérabilités de la machine MS TVM. Ce paramètre doit être au format int32. La valeur par défaut est 2 000.

vulnerabilities_size_limit

Définit le nombre d'enregistrements de vulnérabilité à inclure dans l'ensemble de résultats de l'intégration de vulnérabilité MS TVM (CVE). Ce paramètre doit être au format int32. La valeur par défaut est 2 000.

recommendations_size_limit

Définit le nombre d'enregistrements de vulnérabilité à inclure dans l'ensemble de résultats de l'intégration des recommandations MS TVM. Ce paramètre doit être au format int32. La valeur par défaut est 2 000.

asset_size_limit

Définit le nombre d'enregistrements de vulnérabilité à inclure dans l'ensemble de résultats de l'intégration des machines MS TVM. Ce paramètre doit être au format int32. La valeur par défaut est 2 000.

machine_filter

Filtre les machines provenant de MS TVM. Ce filtre est appliqué à l'intégration des machines MS TVM. La valeur par défaut consiste à importer des machines où onBoardingStatus est intégré.

Messages REST pour l'intégration des vulnérabilités Microsoft Threat and Vulnerability Management

Vous pouvez utiliser les messages REST pour l'intégration ServiceNow® des vulnérabilités Microsoft Threat and Vulnerability Management (MS TVM) afin de passer des appels à l'API MS TVM.

Jeton d'accès MS TVM

Vous pouvez également utiliser les messages REST du jeton d'accès MS TVM pour récupérer le jeton d'accès de l'API MS TVM afin de pouvoir authentifier les demandes d'API REST. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes d'authentification adressées à MS TVM.

Intégration MS TVM

Vous pouvez utiliser le message REST pour l'intégration MS TVM afin de récupérer des informations à partir de MS TVM. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes de récupération d'informations adressées à MS TVM. Les messages REST contiennent les méthodes REST suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Méthodes REST

Méthode REST	Description de la méthode
OBTENIR des vulnérabilités	Récupère les informations sur la vulnérabilité et les exploits à partir de MS TVM.
OBTENIR les vulnérabilités logicielles par ordinateur	Récupère toutes les vulnérabilités ouvertes.
OBTENIR des recommandations	Récupère la liste de toutes les recommandations de sécurité activables qui affectent l'organisation.
Obtenir des machines	Récupère la collection d'actifs.
GET changements de vulnérabilités logicielles par ordinateur	Récupère toutes les informations qui ont changé dans l'importation complète des vulnérabilités de l'organisation, y compris les vulnérabilités nouvelles, corrigées et mises à jour.

Transformation des données pour Microsoft Threat and Vulnerability Management Intégration des vulnérabilités

Une fois que vous avez identifié les données que vous souhaitez importer, les données sont récupérées à partir de l'application ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM), traitées via un ensemble de sources de données et transformées dans votre instance.

Lors de l'installation, les cartes de gravité normalisées sont installées dans le module Mappage de gravité normalisée. Ces cartes transforment les niveaux de gravité de vulnérabilité tiers importés Microsoft en niveaux de gravité standard pour le traitement dans votre instance. Pour plus d'informations sur la création de cartes de gravité, reportez-vous à la section Créer une carte de Réponse aux vulnérabilités gravité.

Importation des machines MS TVM

Les données des machines importées sont d'abord chargées dans la table d'importation des machines MS TVM [sn_vul_msft_tvm_machines_import].

La transformation des machines MS TVM est utilisée pour transformer les informations des machines importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation des machines MS TVM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez **Microsoft TVM Machines Transform**.

La table suivante répertorie les champs de carte de transformation par intégration.

Transformation des machines MS TVM Champs de carte

Champ source	Champ cible	Description
u_id	source_id	ID unique des actifs. Cet ID est mappé au source_id de l'enregistrement de l'élément détecté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Transformation des machines MS TVM Champs de carte (suite)

Champ source	Champ cible	Description
Adresse.mac u_ipaddresses	mac_address	Adresse MAC mappée à partir de l'API au champ d'adresse MAC de l'hôte de l'enregistrement cmdb_ci.
u_ipaddresses.adresse ipip	ip_address	Champ d'adresse IP mappé sur le champ d'adresse IP de l'enregistrement cmdb_ci.
u_lastseen	last_scan_date	Champ mappé au champ last_scan_date de l'enregistrement de l'élément détecté.
u_machinetags		Balises enregistrées dans sn_sec_cmn_host_tag. Le mappage des balises aux actifs est enregistré dans sn_sec_cmn_m2m_src_ci_tag.
u_osplatform	système d'exploitation	Champ mappé au champ du système d'exploitation sur l'enregistrement cmdb_ci.
u_computerdnsname	fqdn	Champ qui mappe le champ dnsname de l'API au champ FQDN sur l'enregistrement cmdb_ci.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Machines MS TVM Carte de transformation, synchronisation et finalité du script

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre (sn_vul_msft_tvm) pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour mettre à jour les valeurs dans l'hôte et vérifier si l'hôte existe. En fonction des résultats, ce script modifie les valeurs de la variable de portée (sn_vul_msft_tvm). Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre de CI créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

L'include de script MicrosoftTVMMachinesProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de l'intégration des machines Microsoft TVM et la transforme en CI. Tout changement apporté à cet include de script peut altérer la transformation des données des ordinateurs Microsoft TVM dans la table de CI et d'élément détecté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration des vulnérabilités MS TVM

Les données de vulnérabilités importées sont d'abord chargées dans la table d'importation Microsoft TVM CVE (Vulnerabilities) [sn_vul_msft_tvm_vulnerabilities_import].

Remarque : Les changements apportés à cette carte de transformation modifient la façon dont les données de l'importation de vulnérabilités MS TVM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez Microsoft **TVM Vulnerabilities Transform**.

La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation de vulnérabilités Microsoft TVM

Champ source	Champ cible	Description
u_id	id	Mappé à la colonne ID de l'enregistrement sn_vul_entry.
u_severity	source_severity	Mappe le champ Gravité à la gravité. La valeur par défaut est de 5.
u_publishedon	date_published	Mappe le champ u_publishedon à la date de publication.
u_publicexploit	public_exploit	Mappe le u_publicexploit fourni par le scanner à la colonne Exploitation publique dans la table Entrée de vulnérabilité.
u_cvssv3	v3_base_score	Mappe le score cvssv3 au score de base v3 dans l'enregistrement d'entrée de vulnérabilité.
u_description	résumé	Mappe la description au champ Résumé de l'enregistrement de l'entrée de vulnérabilité.
u_exploitinkit	malware_kit	Mappe le champ u_exploitinkit au kit malware dans la table Exploit.
u_exploittypes	type	Mappe le type d'exploit au type dans la table Exploit.
u_exploitverified	is_exploit_verified	Mappe le champ u_exploitverified à l'exploit vérifié dans la table Exploit.
u_exploituris	exploit_links	Mappe le champ u_exploituris aux liens d'exploits dans la table Exploit.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre (sn_vul_msft_tvm) pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour créer ou mettre à jour les valeurs dans la NVD ou la table d'entrée tierce. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir les valeurs des nouveaux éléments qui ont été créés et des éléments qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Importation des recommandations MS TVM

Les données de recommandation importées sont d'abord chargées dans la table Importation de recommandations MS TVM [sn_vul_msft_tvm_recom_import].

Remarque : Les changements apportés à cette carte de transformation modifient la façon dont les données de l'importation des recommandations MS TVM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez **Transformation de recommandation MS TVM**.

La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation de recommandation MS TVM

Champ source	Champ cible	Description
u_recommendedvendor	recommended_vendor	Mappe le champ u_recommendedvendor à la colonne Fournisseur.
u_weaknesses	Faiblesses	Mappe le champ u_weaknesses à la colonne Faiblesses.
u_exposedmachinescount	src_exposed_machines_cnt	Mappe le champ u_exposedmachinescount à la colonne Nombre d'ordinateurs exposés.
u_status	état	Mappe l'état au champ État de l'enregistrement de recommandation.
u_productname	product_name	Mappe le champ u_productname au nom du produit dans l'enregistrement de recommandation.
u_nonproductiv_impactedassets	non_prod_impacted_assets	Mappe le champ u_nonproductiv_impactedassets à la colonne Actifs impactés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation de recommandation MS TVM (suite)

Champ source	Champ cible	Description
		dans l'enregistrement de recommandation.
u_activealert	active_alert	Mappe le champ u_activealert à la colonne Alerte active dans l'enregistrement de recommandation.
u_recommendedversion	recommended_version	Mappe le champ u_recommendedversion à la colonne Version recommandée dans l'enregistrement de recommandation.
u_totalmachinecount	total_machine_count	Mappe le champ u_totalmachinecount à la colonne Nombre total d'ordinateurs dans l'enregistrement de recommandation.
u_exposureimpact	exposure_impact	Mappe le champ u_exposureimpact à la colonne Impact d'exposition dans l'enregistrement de recommandation.
u_recommendationname	recommendation_name	Mappe le champ u_recommendationname à la colonne Nom de la recommandation dans l'enregistrement de recommandation.
u_subcategory	sous-catégorie	Mappe le champ u_subcategory à la colonne Sous-catégorie dans l'enregistrement de recommandation.
u_id	source_id	Mappe l'ID de recommandation de MS TVM à la colonne ID source.
u_remediationtype	remediation_type	Mappe le champ u_remediationtype à la colonne Type de rattrapage dans l'enregistrement de recommandation.
u_relatedcomponent	related_component	Mappe le champ u_relatedcomponent à la colonne Composant connexe dans l'enregistrement de recommandation.
u_recommendedprogram	recommended_program	Mappe le champ u_recommendedprogram à la colonne Programme recommandé dans l'enregistrement de recommandation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation de recommandation MS TVM (suite)

Champ source	Champ cible	Description
u_recommendationcategory	recommendation_category	Mappe le champ u_recommendationcategory à la colonne Catégorie de recommandation dans l'enregistrement de recommandation.
u_publicexploit	public_exploit	Mappe le champ u_publicexploit à la colonne Exploitation publique dans l'enregistrement de recommandation.
u_vendor	vendor	Mappe le champ u_vendor à la colonne Fournisseur dans l'enregistrement de recommandation.
[Script]	integration_instance	Nom de l'instance à partir de laquelle la recommandation est importée.
[Script]	sys_domain	Domaine dans lequel cet enregistrement est importé.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Script de carte de transformation de recommandation MS TVM

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre (sn_vul_msft_tvm) pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour mettre à jour les valeurs dans les recommandations et vérifier si les recommandations existent. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir les valeurs des éléments créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Importation des vulnérabilités de la machine MS TVM

La carte de transformation des vulnérabilités des machines MS TVM est utilisée pour transformer les informations sur les vulnérabilités ouvertes et corrigées importées de MS TVM.

Remarque : Les changements apportés à cette carte de transformation modifient la façon dont les données de l'importation des vulnérabilités de la machine MS TVM sont traitées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour accéder aux cartes de transformation des vulnérabilités MS TVM ouvertes et corrigées, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez la **transformation des vulnérabilités de la machine MS TVM**.

La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation des vulnérabilités de machine MS TVM

Champ source	Champ cible	Description
u_id	detection_key	Mappe le champ u_id à la colonne Clé de détection dans la table de détection.
u_diskpaths	proof	Mappe le champ u_diskpaths à la colonne Preuve dans la table de détection.
u_registrypaths	proof	Mappe le champ u_registrypaths à la colonne Preuve dans la table de détection.
u_recommendedsecurityupdateid	preferred_solution	Mappe le champ u_recommendedsecurityupdateid à la colonne Solution préférée de la table des éléments vulnérables, si la solution existe avec le même ID dans la table des sn_vul_solution.
u_recommendationreference	recommandation	Mappe le champ u_recommendationreference à la colonne Recommandation de la table des éléments vulnérables.
u_cveid	vulnerability	Mappe le champ u_cveid à la colonne Vulnérabilité de la table des éléments vulnérables.
u_status	source_status	Mappe le champ u_status à la colonne État source dans la table de détection.
u_eventtimestamp	temporal_score	Mappe le champ u_eventtimestamp à la colonne Dernier trouvé dans la table des éléments vulnérables.
u_lastseentimestamp	last_seen	Mappe le champ u_lastseentimestamp à la colonne Dernier observé dans la table des éléments vulnérables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation des vulnérabilités de machine MS TVM (suite)

Champ source	Champ cible	Description
u_firstseentimestamp	first_seen	Mappe le champ u_firstseentimestamp à la colonne Premier vu dans la table des éléments vulnérables.
u_recommendedsecurityupdate	solution_summary	Mappe le champ u_recommendedsecurityupdate à la colonne Résumé de la solution dans la table des éléments vulnérables.
u_recommendedsecurityupdateurl	solution_summary	Mappe le champ u_recommendedsecurityupdateurl à la colonne Résumé de la solution dans la table des éléments vulnérables.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre (sn_vul_msft_tvm) pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour vérifier si l'entrée de vulnérabilité et les détections existent. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour mettre à jour le nombre de VI et de détections tels qu'importés de MS TVM. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Traduction automatique

Graphique de l'état d'exécution de l'intégration pour Microsoft Threat and Vulnerability Management Intégration des vulnérabilités

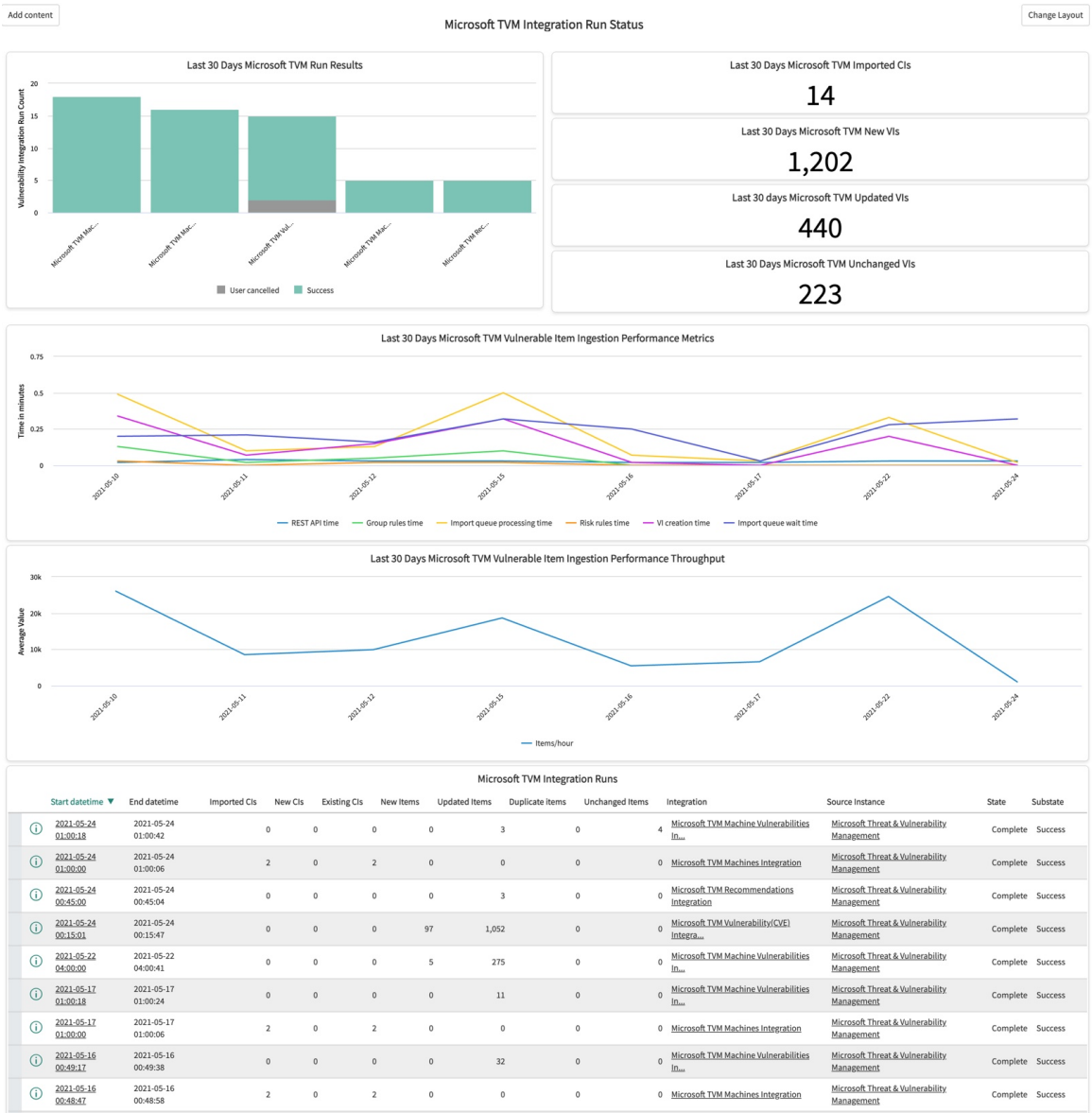
Vous pouvez utiliser le module État de l'exécution de l'intégration Microsoft Threat and Vulnerability Management (MS TVM) pour vous fournir une vue graphique de l'état des exécutions de l'intégration MS TVM.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Dans le graphique, vous pouvez pointer vers n'importe quelle partie du graphique pour afficher un résumé des données spécifiques à cette partie. Si vous cliquez sur une partie du graphique à barres, une liste s'ouvre pour fournir des informations plus détaillées.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Rapports du graphique d’état d’exécution de l’intégration MS TVM

Nom	Description
Résultats Microsoft TVM au cours des 30 derniers jours	Nombre d’exécutions d’intégration qui ont été effectuées pour chaque intégration. Ce rapport indique à la fois les exécutions réussies et échouées. Chaque exécution est affichée sous la forme d’une barre dans le graphique.
Nouveaux VI Microsoft TVM au cours des 30 derniers jours	Nombre de nouveaux éléments vulnérables importés au cours des 30 derniers jours.
VI Microsoft TVM mis à jour au cours des 30 derniers jours	Nombre d’éléments vulnérables mis à jour qui ont été importés au cours des 30 derniers jours.
VI Microsoft TVM inchangés au cours des 30 derniers jours	Nombre d’éléments vulnérables en double qui ont été importés au cours des 30 derniers jours.
Exécutions de l’intégration MS TVM	Enregistrements d’exécution d’intégration dans une liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
	Remarque : V16.1 : Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection dans la `sn_vul_detection` table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, une fois l'exécution de l'intégration terminée.
Mesures de performance d'ingestion d'élément vulnérables Microsoft TVM au cours des 30 derniers jours	Mesures des performances quotidiennes des éléments vulnérables comparées aux 30 derniers jours.
Rendement de performance d'ingestion d'élément vulnérables Microsoft TVM au cours des 30 derniers jours	Débit quotidien d'ingestion d'éléments vulnérables mesuré pour l'intégration de la détection d'hôte Microsoft TVM au cours des 30 derniers jours.
CI importés Microsoft TVM au cours des 30 derniers jours	Nombre de nouveaux éléments de configuration qui ont été importés au cours des 30 derniers jours.

Vérifier l'état d'exécution de l'importation de l'intégration Microsoft Threat and Vulnerability Management

Utilisez l'état d'exécution de l'importation Microsoft Threat and Vulnerability Management (MS TVM) pour vérifier le succès de vos exécutions d'intégration et localiser les problèmes.

Avant de commencer

Cette procédure fait les hypothèses suivantes :

- Vous avez Réponse aux vulnérabilités installé et configuré l'intégration de vulnérabilité MS TVM.
- Les importations d'intégration de vulnérabilité MS TVM sont planifiées et en cours d'exécution.

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dernier enregistrement traité pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Tous** > **Gestion des menaces et des vulnérabilités Microsoft** > **Intégrations**.
   a. Choisissez une intégration.
   b. Cliquez sur la liste connexe Exécutions d'intégration de vulnérabilité.
2. Vérifiez que l'état des importations est Terminé, avec le sous-état Réussite.
   Les causes les plus courantes d'un échec d'exécution sont les suivantes :
   - Interruption du réseau.
   - Décroissance des bits dans le transfert de données entraînant une altération des données pendant la transformation.
3. **Facultatif :** Si l'une de ces conditions a provoqué l'échec de l'exécution est présente, cliquez sur **Exécuter maintenant** et réexécutez l'intégration.

Fractionnez les détections Microsoft TVM en fonction de l'instance de vulnérabilité pour diviser les éléments vulnérables

ServiceNow® Vulnerability Response permet de séparer les détections des analyseurs Microsoft Threat and Vulnerability Management (MS TVM), ce qui permet de créer un élément vulnérable unique (VIT) pour chaque instance de vulnérabilité détectée. Cette répartition permet l'affectation de VIT à diverses équipes de remédiation, améliorant ainsi la gestion et le suivi des vulnérabilités.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La charge utile du scanner Microsoft Threat and Vulnerability Management (MS TVM) contient des données de détection, chaque chemin d'accès de la preuve étant utilisé pour diviser les détections. La balise diskpath dans la charge utile identifie l'emplacement de la vulnérabilité, ce qui facilite l'identification et la gestion précises des vulnérabilités en fonction de leurs chemins spécifiques.

Procédure

1. Dans la table Intégrations tierces [sn_sec_int_integration], définissez la valeur **Inclure la preuve dans** la clé du VI sur vrai pour Tenable.io et Tenable.sc.
2. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Configurer la granularité VI**.
3. Dans le formulaire Inclure le port, cochez la case Inclure le port et sélectionnez le lien **cliquer ici** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la liste Ajouter une preuve aux clés de VI, sélectionnez **Nouveau**.
5. Dans le formulaire Ajouter une preuve à la clé VI - Nouvel enregistrement, dans le champ **Vulnérabilité** , ajoutez l'équipe Microsoft Threat and Vulnerability Management (MS TVM) CVE pour laquelle vous souhaitez inclure la preuve et sélectionnez **Soumettre**.
   La vulnérabilité sélectionnée apparaît dans la liste Ajouter une preuve aux clés de VI.

Example: Fractionnement des détections à partir du scanner Microsoft Threat and Vulnerability Management (MS TVM)

La détection suivante du scanner Microsoft Threat and Vulnerability Management (MS TVM) affiche la preuve dans la balise diskpath.


```
          "id": "329f3283
fae116€796ff1b59c8dd56fef4067elf_mozilla_firefox_126.0.1.0_CVE-2024-7528",
          "deviceId":"329f3283fae116e796ff1b59c8dd56fef4067e1f",

          "rbacGroupId":
     "rbacGroupName": "Unassigned",
      "deviceName": "ip-0a1409fd.secops.com",
       "osPlatform": "WindowsServer2019",
        "oVersion": "10.0.17763.5936",
       "osArchitecture": "x64",
        "softwareVendor": "mozilla",
       "softwareName": "firefox",
       "softwareVersion": "126.0.1.0",

           "cveId"; "CVE-2024-7528",
          #vulnerabilitySeverityLevel": "High",
        #recommendedSecurityUpdate":; "mfsa2024-33",

        "recommendedSecurityUpdateId": null,

          "recommendedSecurityUpdateUrl": null,
           "diskPaths": ['c: llprogram files\lamazonllcfn-bootstraplilibcrypto-3.dll", "C: \lprogram
files\lamazon\lcfn-bootstrap\\libsst-3.dll,

         "registryPaths":
          1 "HKEY LOCAL, MACHINE\\SOFTWAREW\WOW6432Nodel
IMicrosoft|\Windows|1CurrentVersion\|Uninstalll\Mozilla Firefox 126.0.1 (x86 en-US)"


       #lastSeenTimestamp": "2024-08-28 19:36:07",

        "firstSeenTimestamp": "2024-08-06 20:32:34",

       "end0fSupportStatus": null,
         "end0fSupportDate": null,
      "exploitabilityLevel": "NoExploit",
         "recommendationReference": "va-_-mozilla-_-firefox",

        "cvssScore": 8.8,
```


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    "securityUpdateAvailable": true,
      "cveMitigationStatus": null
```

Présentation de l'intégration de l'orchestration de correctifs HCL BigFix avec Réponse aux vulnérabilités

Vous pouvez gérer les correctifs et les déploiements de correctifs pour les vulnérabilités critiques pour de grands groupes d'actifs avec l'intégration Réponse aux vulnérabilités d'orchestration de correctifs au produit HCL BigFix.

Orchestration de correctifs avec Réponse aux vulnérabilités

L'orchestration des correctifs utilise Réponse aux vulnérabilités des importations planifiées à partir d'intégrations de solutions tierces, de fournisseurs de correctifs et de scanners de vulnérabilité. Les données de détection des scanners font correspondre les ressources de votre environnement aux vulnérabilités et aux mises à jour de correctifs qui peuvent les corriger. Soumettez des demandes de correctifs pour approbation, planifiez des mises à jour de correctifs pour résoudre les éléments vulnérables et surveillez la progression du rattrapage à partir des enregistrements dans l'application Réponse aux vulnérabilités de votre ServiceNow AI Platform®.

Orchestration de correctifs Vulnerability Response avec HCL BigFix

Lorsque l'application Vulnerability Response Patch Orchestration avec HCL BigFix integration est utilisée avec , ServiceNow® Gestion des solutions pour vulnérabilités Patch Orchestration et Réponse aux vulnérabilités les applications, les gestionnaires de vulnérabilité et les analystes peuvent effectuer les tâches suivantes :

- Consultez plus de contexte et d'informations sur les types de correctifs et les solutions des fournisseurs (correctifs).
- Affichez et surveillez les données relatives aux vulnérabilités et aux solutions, ainsi que la progression du rattrapage des vulnérabilités à partir des enregistrements dans les espaces de Réponse aux vulnérabilités travail.

Les spécialistes informatiques et les propriétaires de rattrapage peuvent effectuer les tâches suivantes :

- Déployez les correctifs pris en charge par le produit BigFix pour leurs Windows ressources, CentOS, MAC, Oracle et d'autres ressources à intervalles réguliers et planifiés en dehors des heures de travail afin d'éviter les conflits de travail.
- Identifiez les actifs non corrigés présentant des vulnérabilités ou les actifs qui n'ont pas été mis à jour avec succès par des correctifs planifiés à partir des données de détection importées à partir d'analyses tierces.
- Planifiez les correctifs disponibles à partir de l'espace de travail de remédiation informatique ou de l'environnement classique pour les actifs vulnérables non corrigés à partir de la mise à jour du correctif, de la tâche de rattrapage et des enregistrements d'éléments détectés.

Termes clés dans les Réponse aux vulnérabilités applications et BigFix

Élément de configuration (CI)

Les CI sont les actifs existants répertoriés dans votre Base de données de gestion des configurations (CMDB). BigFix appelle les CI, les ordinateurs.

Groupes d'ordinateurs

Terminologie utilisée dans le produit BigFix qui fait référence à un groupe d'actifs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément vulnérable

Une vulnérabilité importée qui correspond à un actif existant dans votre CMDB.

Instance

Un compte rendu distinct de l'application BigFix. Chaque compte d'utilisateur peut être une instance de l'application BigFix. Ce terme fait également référence à une adresse Web unique et sécurisée pour une ServiceNow AI Platform instance.

Intégration

Une intégration est une tâche planifiée dans qui récupère des informations à ServiceNow AI Platform partir d'une source tierce, telle que l'intégration avec les machines BigFix.

Solution

Il existe deux types de solutions dans le cadre de cette intégration, potentielle et préférée. Une solution potentielle est une solution qui pourrait remédier à une vulnérabilité. Les vulnérabilités ont souvent de nombreuses solutions potentielles. #Une solution privilégiée correspond à la solution la plus efficace pour une vulnérabilité spécifique détectée.

Correctif

Mises à jour logicielles qui corrigent les vulnérabilités. Dans l'application BigFix, les correctifs sont appelés Fixlets. Par exemple, BigFix propose des fixlets pour Windows, CentOS, Oracle MAC et d'autres produits.

Correctif préféré

Les correctifs préférés sont des mises à jour logicielles destinées à corriger des vulnérabilités spécifiques. Une fois déployés, les correctifs sont mappés aux éléments vulnérables liés à des vulnérabilités spécifiques et les corrigent.

Tâche de rattrapage

Listes des éléments vulnérables dans l'application Réponse aux vulnérabilités des actions requises pour corriger les vulnérabilités.

Déploiement

Aux fins de cette intégration, le déploiement désigne l'application, le lancement ou la planification d'un correctif sur un ordinateur. BigFix appelle ces déploiements des actions. Vous pouvez déployer (créer des actions) pour les correctifs que vous avez téléchargés à partir de BigFix dans votre ServiceNow AI Platform. Accédez aux éléments détectés, aux correctifs ou aux tâches de rattrapage à partir d'enregistrements individuels dans Réponse aux vulnérabilités. Vous pouvez déployer des correctifs avec des travaux planifiés sur des machines individuelles ou sur des groupes d'ordinateurs.

Le déploiement dans peut ServiceNow AI Platform également faire référence à une intégration qui prend en charge le multisource. Une existence d'intégration unique est appelée un déploiement de votre intégration. Un déploiement fait référence aux intégrations et aux produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de l'intégration de vulnérabilité BigFix dans votre environnement.

Gestion des solutions de vulnérabilité et Vulnerability Response Patch Orchestration avec HCL Intégration BigFix

La gestion des solutions est assurée par l'application Gestion des solutions pour vulnérabilités , une ServiceNow AI Platform application qui met en corrélation vos résultats de vulnérabilité avec la répartition des solutions (correctifs) pour les corriger. Identifiez les correctifs logiciels tiers pour les produits et services, les mises à jour de configuration et les autres contrôles qui ont le plus d'impact sur votre organisation. En plus des informations sur les scanners tiers, les Gestion des solutions pour Réponse aux vulnérabilités applications , Réponse aux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilités et Vulnerability Response Patch Orchestration with HCL BigFix fonctionnent ensemble pour déployer les correctifs préférés de la solution, à la vulnérabilité, puis à l'élément vulnérable, afin de vous aider à corriger et à fermer les vulnérabilités de votre environnement.

, et Gestion des solutions pour Réponse aux vulnérabilités Vulnerability Response Patch Orchestration avec HCL BigFix Integration sont tous disponibles dans le ServiceNow® Store. Réponse aux vulnérabilités

Rôles ServiceNow AI Platform requis

Les tâches d'installation, de configuration et de rattrapage de l'intégration nécessitent les rôles suivants dans votre ServiceNow AI Platform instance.

administrateur

Les utilisateurs disposant de ce rôle obtiennent des autorisations pour les applications dans et ServiceNow Store les téléchargent vers les ServiceNow AI Platform instances.

sn_vul.vulnerability_admin

Les utilisateurs disposant de ce rôle activent les applications dans l'instance ServiceNow AI Platform et terminent la configuration de l'application Réponse aux vulnérabilités . Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Cet utilisateur administrateur configure l'ensemble des applications VR, des règles et des intégrations tierces.

sn_vul_bigfix.configure_integration

Les utilisateurs disposant de ce rôle configurent l'application BigFix Patch Orchestration Integration. Ce rôle contient le rôle granulaire sn_vul_bigfix.read_integration.

sn_vul_bigfix.read_integration

Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les enregistrements de l'application Réponse aux vulnérabilités BigFix Patch Orchestration Integration et les données d'orchestration de correctifs.

sn_vul_patch_orch.configure_patch

Les utilisateurs disposant de ce rôle peuvent configurer et appliquer des correctifs.

sn_vul_patch_orch.read_patch

Les utilisateurs disposant de ce rôle peuvent afficher (lecture seule) les informations sur les correctifs.

Approbateurs

Affectez des utilisations aux groupes d'approbateurs de niveau 1 et d'approbateur de niveau 2 si vous souhaitez que les demandes de correctifs soumises soient approuvées avant le déploiement.

Pour plus d'informations sur l'affectation de ces rôles à l'aide de l'assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour en savoir plus sur les Réponse aux vulnérabilités rôles de votre ServiceNow AI Platform, reportez-vous à la section Réponse aux vulnérabilités Profils et rôles granulaires.

Règles de recherche de CI

Lorsque des données sont importées depuis l'application BigFix, l'application Réponse aux vulnérabilités recherche automatiquement des correspondances dans les données de la Base de données de gestion des configurations (CMDB) machine utilisatrice (actif). Les règles de recherche de CI sont utilisées pour identifier les CI (actifs) et les ajouter automatiquement aux enregistrements d'éléments vulnérables (VI) lors de la création des VI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les règles de recherche de CI suivantes sont fournies avec le système de base et sont utilisées pour identifier les CI (actifs) et les ajouter à l'application Réponse aux vulnérabilités :

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

Vous pouvez utiliser plusieurs valeurs pour le IP_ADDRESS d'un actif. Une règle de recherche de CI prend en compte toutes les valeurs pour la correspondance. Pour en savoir plus sur le fonctionnement des règles de recherche de CI, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Serveur MID

L'intégration Réponse aux vulnérabilités Patch Orchestration with HCL BigFix est une intégration sur site. Elle nécessite un serveur MID autonome qui ne fait pas partie d'une grappe de serveurs MID. Le serveur MID est nécessaire pour exécuter des scripts sur des ordinateurs distants à partir de votre instance afin d'importer des données à partir du serveur BigFix. Les API pour cette intégration sont appelées à l'aide des MID Servers que vous configurez dans votre ServiceNow AI Platform instance. Consultez Préparer l'intégration de Patch Réponse aux vulnérabilités Orchestration avec HCL BigFix pour plus d'informations.

Intégrations et dépendances de l'intégration Réponse aux vulnérabilités de Patch Orchestration à HCL BigFix

Les applications de produits et dépendances suivantes sont requises pour Vulnerability Response Patch Orchestration avec HCL BigFix Integration. Ces applications sont disponibles dans le ServiceNow® Store.

Versions disponibles des applications et dépendances requises pour l'intégration de l'orchestration des correctifs

Pour afficher les données d'orchestration de correctifs et les mises à jour disponibles (correctifs) dans les espaces de travail de , les Réponse aux vulnérabilités applications suivantes sont requises. Toutes les applications répertoriées sont disponibles dans le ServiceNow® Store. Certaines applications nécessitent des abonnements distincts.

Pour plus d'informations sur la compatibilité des versions avec les applications et les versions de famille requises, consultez l'article KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes de la base de connaissances HI.

Application et version de mise en production
Réponse aux vulnérabilités
Gestion des solutions pour vulnérabilités
Application Vulnerability Response Patch Orchestration
Réponse aux vulnérabilités Orchestration de correctifs avec l'application HCL BigFix
Security Support Common
Orchestration du support de sécurité
Une application de scanner de vulnérabilité tierce prise en charge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités Tables de l'application Orchestration de correctifs

L'application Réponse aux vulnérabilités Patch Orchestration contient les tables suivantes :

Table	Description
Mise à jour du correctif [sn_vul_patch_orch_update]	Stocke des informations sur les correctifs disponibles sur des instances distinctes.
Mise à jour de l'appareil [sn_vul_patch_orch_m2m_src_ci_update]	Stocke les données relatives aux correctifs déployés, ainsi que l'état de déploiement, qui sont affichés sur les enregistrements d'éléments détectés.
Collecte [sn_vul_patch_orch_collection]	Stocke les données de collecte d'instances distinctes.
Ensemble d'appareils [sn_vul_patch_orch_m2m_src_ci_collection]	Stocke les données des collections sur les éléments découverts.
Déploiement de correctif [sn_vul_patch_orch_deployment]	Stocke des informations sur les correctifs déployés sur les collections et les CI.
Correctif potentiel [sn_vul_patch_orch_m2m_vuln_patch]	Stocke des données sur les correctifs et les vulnérabilités qui identifient les correctifs qui peuvent être utilisés pour résoudre une vulnérabilité.

Intégrations d'orchestration de correctifs Vulnerability Response avec HCL BigFix

Les intégrations développées par ServiceNow® l'ingénierie constituent le déploiement orchestré de la solution avec le produit BigFix. Les intégrations suivantes sont incluses dans l'application Réponse aux vulnérabilités Patch Orchestration Integration with HCL BigFix que vous téléchargez à partir du ServiceNow® Store.

Après avoir installé l'application d'intégration sur votre ServiceNow AI Platform instance, pour afficher ces intégrations, accédez à **Intégrations** > **Intégration d'orchestration de correctifs BigFix** > **Intégrations**. L'application Réponse aux vulnérabilités traite les données selon des intervalles de temps planifiés importés par ces intégrations avec les points de terminaison BigFix.

Intégration	Description
Intégration de collection BigFix	• Cette intégration est planifiée pour s'exécuter quotidiennement et s'exécute en premier dans l'exécution de l'intégration chaînée. • Récupère les ordinateurs et les groupes d'ordinateurs qui composent les groupes d'ordinateurs (éléments de configuration) à partir de l'application BigFix.
Intégration de fixlet BigFix	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de collecte BigFix. Vous pouvez également l'exécuter sur demande. • Récupère des informations sur tous les fixlets (correctifs) disponibles à partir du serveur BigFix.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
Intégration de fixlet d'appareil BigFix	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de fixlet BigFix. Vous pouvez également l'exécuter sur demande. • Récupère des informations sur les fixlets qui se trouvent actuellement sur les ordinateurs (actifs) à partir du serveur BigFix.
Intégration d'actions BigFix	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de fixlet de l'appareil BigFix. Vous pouvez également l'exécuter sur demande. • Récupère des informations sur les correctifs planifiés par l'équipe informatique dans le serveur BigFix.

Préparer l'intégration de Patch Réponse aux vulnérabilités Orchestration avec HCL BigFix

Préparez l'intégration en effectuant les tâches de configuration suivantes.

Avant de commencer

Rôles requis : admin pour l'installation des applications et l'affectation des rôles. D'autres rôles sont répertoriés dans le tableau suivant.

Pourquoi et quand exécuter cette tâche

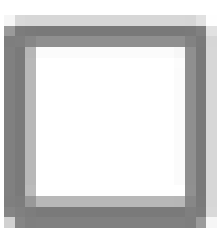
Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration.

Vous êtes prêt à Installer l'application Réponse aux vulnérabilités Patch Orchestration with HCL BigFix.

Procédure

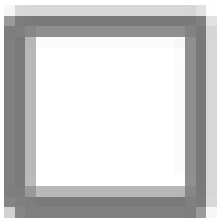
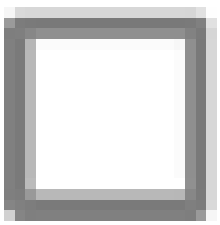
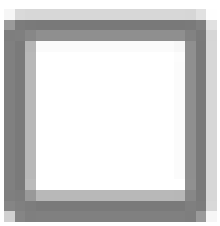
1. Pour une installation et une configuration fluides de l'application Réponse aux vulnérabilités Patch Orchestration with HCL BigFix, suivez la liste de vérification fournie.
2. Vous préférez peut-être imprimer la liste de vérification suivante et vérifier que les éléments énumérés sont renseignés avant d'installer l'application.

   Après l'installation et la configuration, importez les informations relatives aux vulnérabilités et aux correctifs dans votre ServiceNow AI Platform® instance.

Tâche	Description
	(Facultatif) Si elle n'est pas déjà installée et activée, vous préférerez peut-être installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour plus d'informations sur l'installation et l'activation de l'application, Installer Réponse aux vulnérabilités reportez-vous à la Réponse aux vulnérabilités section . Cette intégration nécessite la version 16.0 ou Réponse aux vulnérabilités ultérieure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Si ce n’est pas déjà fait, obtenez les autorisations et installez une application d’analyse tierce pour importer les données de vulnérabilité. Pour Intégrations de Réponse aux vulnérabilités plus d’informations sur les scanners tiers pris en charge par Réponse aux vulnérabilités. Consultez .
	Si ce n’est pas déjà fait, obtenez les autorisations et téléchargez l’application Vulnerability Response Patch Orchestration with HCL BigFix sur votre ServiceNow AI Platform® instance. Consultez .
	Obtenez les informations d’identification BigFix. Vérifiez que vous disposez des noms de compte, mots de passe et autres informations de service requis par vos produits BigFix afin d’y avoir accès.
	Vérifiez que vous disposez de groupes ou d’utilisateurs pour gérer les intégrations et corriger les éléments vulnérables. **administrateur** L’administrateur système obtient les autorisations, télécharge et installe l’application BigFix Patch Orchestration et les autres applications requises pour l’intégration. S’il n’est pas affecté, l’administrateur affecte l’administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d’autres rôles dans l’assistant de configuration dans Réponse aux vulnérabilités ou à partir du module Administration utilisateurs. **sn_vul.vulnerability_admin** Une fois affecté, l’administrateur de vulnérabilité termine la configuration des intégrations BigFix et des autres applications tierces. Ce rôle dispose d’un accès complet à l’application Réponse aux vulnérabilités (VR) et à ses enregistrements. Ce rôle configure toutes les applications de réalité virtuelle, les règles, les intégrations tierces, les applications Vulnerability Response Patch Orchestration et les applications Vulnerability Solution Management. **sn_vul_bigfix.configure_integration** Les utilisateurs disposant de ce rôle configurent l’application BigFix Patch Orchestration Integration. Ce rôle contient les rôles granulaires

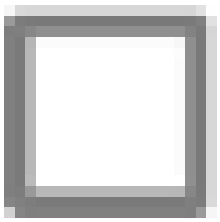
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	sn_vul_bigfix.read_integration et connection_admin qui permettent à l'utilisateur de se connecter à la console BigFix et de configurer les instances d'intégration dans votre ServiceNow AI Platform. **sn_vul_bigfix.read_integration** Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les enregistrements de l'application Réponse aux vulnérabilités BigFix Patch Orchestration Integration et les données d'orchestration de correctifs. **sn_vul_patch_orch.configure_patch** Les utilisateurs disposant de ce rôle peuvent configurer et appliquer des correctifs. Les correctifs demandés par cet utilisateur à partir des enregistrements d'élément vulnérable et de mise à jour de correctif sont envoyés pour approbation si Gestion des changements est actif et que des approbateurs sont affectés. **sn_vul_patch_orch.read_patch** Les utilisateurs disposant de ce rôle peuvent afficher (lecture seule) les informations sur les correctifs dans les enregistrements. Ce rôle est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail Rattrapage informatique et Responsable des vulnérabilités. **Approbateurs** Les groupes d'approbateurs affectés aux groupes d'approbateurs de niveau 1 et, éventuellement, d'approbateur 2 approuvent les demandes de correctifs soumises. Par défaut, les correctifs sont soumis au groupe des approbateurs de niveau 1 pour approbation avant le déploiement. Pour plus d'informations sur le processus d'approbation, reportez-vous à Orchestration de correctifs avec Réponse aux vulnérabilités. Pour plus d'informations sur la configuration des approbateurs et des groupes, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. L'administrateur système procède à l'affectation initiale des rôles aux utilisateurs et aux groupes pour l'intégration. Par défaut, le groupe Vulnerability Response est disponible. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires pour les rôles de spécialiste du rattrapage et d'analyste de vulnérabilité et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance. Voir Créer un groupe d'utilisateurs .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Vérifiez que vous avez activé toutes les fonctionnalités, règles, dépendances, modules d'extension ou tâches dans votre instance requis pour l'intégration. ○ Vulnerability Response Patch Orchestration avec HCL BigFix est une intégration locale qui nécessite l'utilisation d'un serveur MID autonome. Pour plus d'informations sur les serveurs MID dans votre instance, consultez Serveur MID . ○ Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous** et localisez le module d'extension. S'il n'est pas installé dans votre instance, installez-le et activez-le.

Que faire ensuite

Vous êtes maintenant prêt à Installer l'application Réponse aux vulnérabilités Patch Orchestration with HCL BigFix.

Installer l'application Réponse aux vulnérabilités Patch Orchestration with HCL BigFix

Téléchargez l'application Vulnerability Response Patch Orchestration avec HCL BigFix à partir du ServiceNow® Store.

Avant de commencer

Rôles requis : administrateur pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application. Administrateur de vulnérabilité (sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)) pour configurer Vulnerability Response Patch Orchestration avec HCL BigFix et d'autres applications après leur installation.

Pourquoi et quand exécuter cette tâche

Avant d'installer l'application, vérifiez que vous avez rempli tous les éléments de la liste de vérification dans Préparer l'intégration de Patch Réponse aux vulnérabilités Orchestration avec HCL BigFix.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Procédure

1. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.
2. Localisez l'application **Vulnerability Response Patch Orchestration avec HCL BigFix** et cliquez sur **Installer**.

   Cette action installe l'application que vous avez téléchargée à partir du ServiceNow Store.
3. Vous pouvez également installer des applications à partir de l'assistant de configuration.
   Pour plus d'informations sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Une fois l'installation terminée, accédez à **Tous** > **Intégration d'orchestration de correctifs BigFix** > **Configuration** pour poursuivre la configuration.

Configurer l'intégration de l'orchestration des Réponse aux vulnérabilités correctifs avec HCL BigFix

Après avoir installé l'application, configurez-la avec les informations de votre compte BigFix et validez vos informations d'identification.

Avant de commencer

Rôles requis : sn_vul.vulnerability_admin et sn_vul_bigfix.configure_integration

Procédure

1. Accédez à la **Intégration d'orchestration de correctifs BigFix** > **Configuration**.
2. Renseignez les champs avec vos informations et informations d'identification BigFix.

Champ	Description
Instance d'intégration	Le nom du compte d'instance BigFix que vous souhaitez utiliser, par exemple l'intégration de la gestion des correctifs BigFix.
Nom d'hôte	Saisissez l'URL de l'hôte BigFix.
Nom d'utilisateur	Saisissez le nom d'utilisateur de votre compte BigFix.
Mot de passe	Saisissez le mot de passe de votre compte BigFix.
Serveur MID	Entrez le nom du Serveur MID autonome dans la liste que vous voulez utiliser. Pour Préparer l'intégration de Patch Réponse aux vulnérabilités Orchestration avec HCL BigFix plus d'informations sur les serveurs MID et configurez les tâches dans votre ServiceNow AI Platform®.

3. Cliquez sur Enregistrer et tester les informations d'identification.
   L'état de votre connexion entre BigFix et votre ServiceNow AI Platform® instance est affiché dans le champ État de validation. Si vous ne voyez pas de test réussi, suivez les invites.
4. **Facultatif :** L'application Séparation de domaine est prise en charge pour cette intégration.
   Vous pouvez ajouter plusieurs configurations à votre instance. Pour ajouter des configurations supplémentaires :
   a. Accédez à la **Intégration d'orchestration de correctifs BigFix Instances d'intégration**.
   b. Vérifiez que le périmètre de l'application, Vulnerability Response Patch Orchestration with HCL BigFix, s'affiche dans le champ Périmètre de l'application.
   c. Cliquez sur **Nouveau**.
   d. Remplissez le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom de l'instance d'intégration.
Application	Orchestration de correctifs Vulnerability Response avec HCL BigFix
Intégration	[Lecture seule] La gestion des correctifs BigFix est la gestion par défaut.
Actif	La valeur par défaut est activée (sélectionnée). Si elle est décochée, l'instance n'est pas active.

e. Cliquez sur **Envoyer**.
Votre nouvelle instance d'intégration s'affiche dans la liste Instances d'intégration.

f. Répétez les étapes 1 à 3 pour configurer votre instance d'intégration et tester vos informations d'identification.

5. Configurez les approbations pour les demandes de correctifs.
Par défaut, une propriété système [**sn_vul_patch_orch.patch_approval_required**] est activée de sorte que, lorsque des déploiements de correctifs sont planifiés, ils sont soumis pour revue et approbation aux utilisateurs affectés au groupe d'approbation de mise à jour de correctif de niveau 1 - correctif.

Si vous souhaitez que les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch planifient des correctifs sans approbation, vous pouvez désactiver la propriété [**sn_vul_patch_orch.patch_approval_required**]. Vous préférez peut-être laisser les approbations activées afin que les correctifs planifiés n'entrent pas en conflit avec les heures de travail normales.

Remarque : Si vous désactivez la propriété système d'approbation, tout utilisateur disposant du rôle sn_vul_patch_orch.configure_patch peut planifier et déployer des correctifs sans examen ni approbation.

En tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin, désactivez la propriété système :

a. Accédez à la **liste.propriétés.système**.

b. Recherchez **sn_vul_patch_orch.patch_approval_required** et cliquez dessus pour ouvrir l'enregistrement.

c. Dans le champ Valeur, tapez `faux`.

d. Cliquez sur **Mettre à jour**.

6. Si vous ne désactivez pas cette propriété, vous devez affecter des approbateurs pour les demandes de correctifs.
En tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin, procédez comme suit.

a. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.

b. Si la règle **d'approbation d'approbation de mise à jour de correctif de déploiement** ne s'affiche pas dans la liste, cliquez sur **Tout** à droite de l'icône de filtre verte en haut à gauche de l'écran pour afficher toute la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. À partir de la liste, cliquez sur **Déployer l'approbation de mise à jour de correctif**.

d. Sur l'enregistrement, avec l'onglet Configuration de l'approbation sélectionné, cliquez sur **Approbation de la mise à jour du correctif de configuration par défaut**.

e. Sur l'enregistrement, cliquez sur **Niveau 1 : approbation de la mise à jour du correctif**.

f. Ajouter des utilisateurs à ce groupe.

Les utilisateurs affectés à ce groupe approuvent les demandes de correctifs soumises par les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch. Naviguez vers **Mes approbations** pour afficher et traiter les demandes.

7. Cliquez sur**Mettre à jour** pour enregistrer vos modifications.

8. **Facultatif :** Vous pouvez configurer des approbations à plusieurs niveaux de sorte que plusieurs approbations soient requises avant le déploiement des demandes de correctifs planifiées.

a. Une fois l'enregistrement d'approbation de mise à jour de correctif de configuration par défaut affiché, cliquez sur **Nouveau**.

b. Renseignez les champs.

Champ	Description
Nom	Nom du niveau d'approbation, par exemple, **Niveau 2 : approbation de mise à jour du correctif**.
Actif	Activé par défaut, ce qui signifie que le niveau d'approbation est utilisé.
Approbation requise	Sélectionnez le nombre d'approbations requises pour le niveau sélectionné : ▪ Un approbateur requis ▪ Approbation de tous les utilisateurs requise
Ordre	Ordre d'exécution de diverses configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 s'exécute avant une configuration avec une entrée d'ordre de 200.
Rôle	Sélectionnez un rôle pour le groupe dans la liste.
Règle d'approbation	Contient les détails de la table et du type pour la règle d'approbation.
Configuration de l'approbation	Contient les configurations d'approbation.
Affecter à l'aide de	Sélectionnez une option :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ Utilisateur et groupe d'utilisateurs ▪ Champ de la table des approbations ▪ Script
Groupes	Groupe au niveau de l'approbateur composé de plusieurs utilisateurs. L'utilisateur doit disposer de l'un des rôles suivants que vous spécifiez.
Utilisateurs	Modifiez les utilisateurs répertoriés dans les groupes.

c. Cliquez sur **Soumettre** pour enregistrer vos modifications.

Affichage des données de correctifs pour l'intégration d'orchestration Réponse aux vulnérabilités de correctifs à HCL BigFix

Les données de correctifs et les données de déploiement de correctifs, ainsi que les informations de vulnérabilité et l'état de rattrapage de vos vulnérabilités, sont affichées sur les enregistrements de votre instance.

Afficher les données des correctifs dans les espaces de Réponse aux vulnérabilités travail

Rôles requis :

- Rôle sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs
- sn_vul_patch_orch.read_patch pour afficher (lecture seule) les informations sur les correctifs dans les enregistrements. Ce rôle est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst qui sont requis pour les espaces de travail du rattrapage informatique et du gestionnaire de vulnérabilité

Dans l'espace de travail de remédiation informatique, vous pouvez afficher les correctifs :

- Dans la vue Accueil, où vous pouvez cliquer sur les tableaux de résultats pour afficher les enregistrements de solutions préférées sur les éléments vulnérables, de CI vulnérables et de correctifs préférés sur les éléments vulnérables.
- Dans la vue de liste, où vous pouvez afficher tous les enregistrements de mise à jour de correctif (VPU) à partir des liens de correctifs et les éléments vulnérables (VIT) qui vous sont affectés et qui ont des correctifs.

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- À partir de la mise à jour du correctif (VPU)
- Tâche de rattrapage (RT)
- Enregistrements d'éléments détectés (SDI)

Dans l'espace de travail Responsable des vulnérabilités, vous pouvez afficher les correctifs :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- À partir de la vue Accueil sur les rubriques de visualisation, où vous pouvez afficher les correctifs préférés et potentiels, les dates planifiées des correctifs et, si le correctif a été téléchargé, le tout dans l'onglet **Éléments vulnérables** .
- Dans la vue de listes sur les efforts de rattrapage, où vous pouvez afficher les données de correctifs sur les enregistrements de VI à partir de l'onglet**Éléments vulnérables** .

Dans la vue d'environnement classique, accédez à **Tous** > **Réponse aux vulnérabilités** > **Correctifs**.

Correctif : mettre à jour les enregistrements dans les espaces de travail VR et dans la vue de l'environnement classique

Les données de correctif et les données et l'état de déploiement de correctif s'affichent sur les enregistrements de votre instance. Les enregistrements de correctifs sont inclus dans le cadre de la fonctionnalité d'orchestration des correctifs de cette intégration avec Réponse aux vulnérabilités. Affichez les enregistrements Patch (VPU) dans Réponse aux vulnérabilités les espaces de travail à partir de la vue de liste de l'espace de travail de remédiation informatique. Les enregistrements de mise à jour de correctif dans la vue classique et Réponse aux vulnérabilités dans les espaces de travail incluent les données suivantes :

- Données et informations de solutions de vulnérabilité provenant des fournisseurs de correctifs importées par l'application Gestion des solutions de vulnérabilité.
- État du rattrapage à la source qui inclut le nombre total d'appareils présentant une vulnérabilité donnée pouvant être corrigée par un correctif et tous les appareils pour lesquels des mises à jour sont manquantes.
- État du rattrapage qui inclut le % de VI rattrapés et le total des VI qui ont un correctif comme correctif préféré.
- Appareils associés, éléments vulnérables, déploiements de correctifs et demandes de correctifs sur les liens connexes des enregistrements dans la vue de classe. Ces données sont affichées sur les onglets des enregistrements dans les espaces de Réponse aux vulnérabilités travail.
- Demandes de correctifs que les propriétaires de rattrapage ont soumises pour approbation.

Déploiement d'état sur les enregistrements d'éléments vulnérables

Pour plus d'informations sur le déploiement de l'état vers les enregistrements, reportez-vous à la section Données de correctif et déploiement d'état pour l'orchestration de correctifs dans Réponse aux vulnérabilités.

Enregistrements qui recupèrent les nombres de VI actifs

Pour éviter de déployer tous les correctifs sur toutes les vulnérabilités, la tâche planifiée ne récupère que les changements apportés au nombre de VI actifs. Ces changements de nombre et les données connexes sont déployés dans les enregistrements suivants dans Réponse aux vulnérabilités:

- VIT
- RT
- Solution de vulnérabilité
- Mise à jour du correctif

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des données pour les correctifs sans solutions

Pour plus d'informations sur l'affichage des patchs sans solutions, reportez-vous à la section Afficher les correctifs sans solutions dans Réponse aux vulnérabilités.

Données du correctif avec Réponse aux vulnérabilités

Les tableaux de bord Gestion de la vulnérabilité (PA) et CISO sont inclus dans un abonnement à l'application Analyse des performancesRéponse aux vulnérabilités . Si vous avez un abonnement pour Analyse des performances, mais qu'aucune intégration d'orchestration de correctifs n'est installée, l'onglet Rattrapage s'affiche sur le tableau de bord du CISO, mais il n'est pas renseigné avec des données.

Pour le tableau de bord Gestion de la vulnérabilité (PA), accédez à **Tous** > **Réponse aux vulnérabilités** > **Vue d'ensemble**. Cliquez sur l'onglet **Rattrapage** et faites défiler vers le bas de la page pour afficher les données des mises à jour de correctifs : correctifs planifiés et non planifiés, correctifs manquant leur date cible et nombres hebdomadaires.

Pour le tableau de bord CISO, accédez à **Tous** > **Réponse aux vulnérabilités** > **Tableau de bord des CISO**. Avec l'onglet Vue d'ensemble sélectionné, faites défiler vers le bas de la page pour afficher les données de couverture des correctifs : criticité, correctifs planifiés et non planifiés et correctifs manquants dans leur date cible.

Pour en savoir plus sur les tableaux de Réponse aux vulnérabilités bord, reportez-vous à Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités, Orchestration de correctifs avec les Réponse aux vulnérabilités espaces de travail et Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord.

Planifier des correctifs avec l'intégration d'orchestration Réponse aux vulnérabilités de correctifs HCL BigFix

Planifiez des correctifs à partir des enregistrements de tâche de mise à jour de correctif et de rattrapage dans l'application de votre Réponse aux vulnérabilitésServiceNow AI Platform instance.

Avant de commencer

À partir de la version 16.1, vous pouvez planifier des correctifs à partir des espaces de Réponse aux vulnérabilités travail ou de l'environnement classique.

Rôles requis :

- Rôle sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs
- sn_vul_patch_orch.read_patch pour afficher (lecture seule) les informations sur les correctifs dans les enregistrements. Ce rôle est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst qui sont requis pour les espaces de travail du rattrapage informatique et du gestionnaire de vulnérabilité

Procédure

1. Dans les espaces de travail de vulnérabilité Réponse aux vulnérabilités , en tant qu'utilisateur disposant du rôle sn_vul.remediation_owner, accédez à **Tous** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
2. Sur la page d'accueil, cliquez sur **Patch préféré sur les VI.**
   La liste des enregistrements de mises à jour de correctifs pour les éléments vulnérables avec les correctifs préférés qui vous sont affectés s'affiche.
3. Localisez un enregistrement que vous souhaitez ouvrir et cliquez pour l'ouvrir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sinon, dans la vue de liste de l'espace de travail, cliquez sur **Correctifs** > **Tous** et localiser un enregistrement de mise à jour de correctif.
   L'enregistrement de la mise à jour du correctif s'affiche. Vous préférez peut-être examiner les données avant de planifier un correctif, car d'autres correctifs peuvent déjà être planifiés.
5. Reportez-vous au tableau suivant pour connaître les données affichées et ce que vous pouvez faire.

Tâche	Description
Cliquer sur un lien d'éléments connexes	○ Vue d'ensemble : affichez des détails tels que le numéro d'enregistrement de la mise à jour du correctif, les ID de l'article et du bulletin, la date de publication et la catégorie de la mise à jour, le nom du site du correctif, la cote de risque, le score de risque, la description, la solution (le cas échéant) et l'état du rattrapage. ○ Appareils associés : liste des éléments de configuration impactés affectés par le correctif et l'état. ○ Éléments vulnérables : la liste des éléments vulnérables associés à la vulnérabilité et au correctif. ○ Déploiements de correctifs : les noms et les informations relatifs aux déploiements de ce correctif sur des actifs ou des groupes d'actifs pour ce correctif. ○ Demandes de correctifs : une liste des demandes de correctifs déjà soumises pour ce correctif. Cela s'affiche.
Cliquez sur un lien pour ouvrir un enregistrement	Dans les listes affichées sur les enregistrements ouverts à partir des liens d'éléments connexes, affichez plus de détails, y compris les messages sur les cibles manquées. Une fois ouverts, les enregistrements restent ouverts sous forme d'onglets jusqu'à ce que vous les fermiez.
Planifier le correctif	Lorsque vous êtes prêt à planifier un correctif ou à soumettre une demande, cliquez sur **Planifier un correctif**. Dans la boîte de dialogue qui s'affiche, renseignez les champs. Pour en savoir plus, reportez-vous aux étapes ci-dessous.
Ajouter une note de travail ou joindre un fichier	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'éclair) et entrez une note de travail. Cliquez sur l'icône pour activer/désactiver le panneau. Vous pouvez également charger un fichier.

6. Cliquez sur **Planifier le correctif**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Renseignez les champs de la boîte de dialogue.

Champ	Description
Sélectionner la cible	
Ressources	Choisissez-en un dans la liste pour continuer. Le groupe d'ordinateurs est affiché par défaut. ○ Groupe d'ordinateurs : sélectionnez cette option si vous souhaitez choisir une collection (un groupe d'actifs) pour ce correctif. Les groupes sont constitués des éléments de configuration importés depuis l'application BigFix. ○ Liste d'ordinateurs : sélectionnez cette option si vous souhaitez choisir des ordinateurs individuels (actifs) pour ce correctif. Vous pouvez voir des données sur le fabricant, l'emplacement, la classe, la date de la dernière mise à jour et le calendrier de maintenance dans la boîte de dialogue qui s'affiche. Cliquez sur **Suivant** pour continuer.
Groupe d'ordinateurs ou liste d'ordinateurs	En fonction de votre sélection pour Actifs, l'un des champs s'affiche. Choisissez dans les listes.
Planifier	
Nom du déploiement	Entrez un nom pour ce déploiement de correctif. Ce nom vous permet de suivre vos mises à jour.
Type de déploiement	Choisissez une option dans la liste.
Heure de date limite	Définissez la valeur de l'heure limite. Cette valeur est l'heure à laquelle le correctif est disponible pour la dernière fois pour le déploiement.
Temps disponible	Définissez la valeur correspondant à l'heure à laquelle le correctif devient disponible.
Temps disponible basé sur	Sélectionnez un fuseau horaire dans la liste sur lequel votre fenêtre de temps de déploiement sera basée.
Autoriser le redémarrage	Désactivé par défaut. Activez (sélectionnez) cette option pour demander aux machines du groupe de redémarrer automatiquement une fois le correctif terminé.
Description	Ajoutez plus de texte pour à propos du correctif. Ces informations sont affichées dans le champ Description des enregistrements de mise à jour de correctifs.

8. Cliquez sur **Déployer**.
La demande de correctif est envoyée à pour révision. Vous pouvez afficher l'état de toutes vos demandes soumises à partir de **Demandes d'exception** > **Mes demandes** dans la vue de liste.

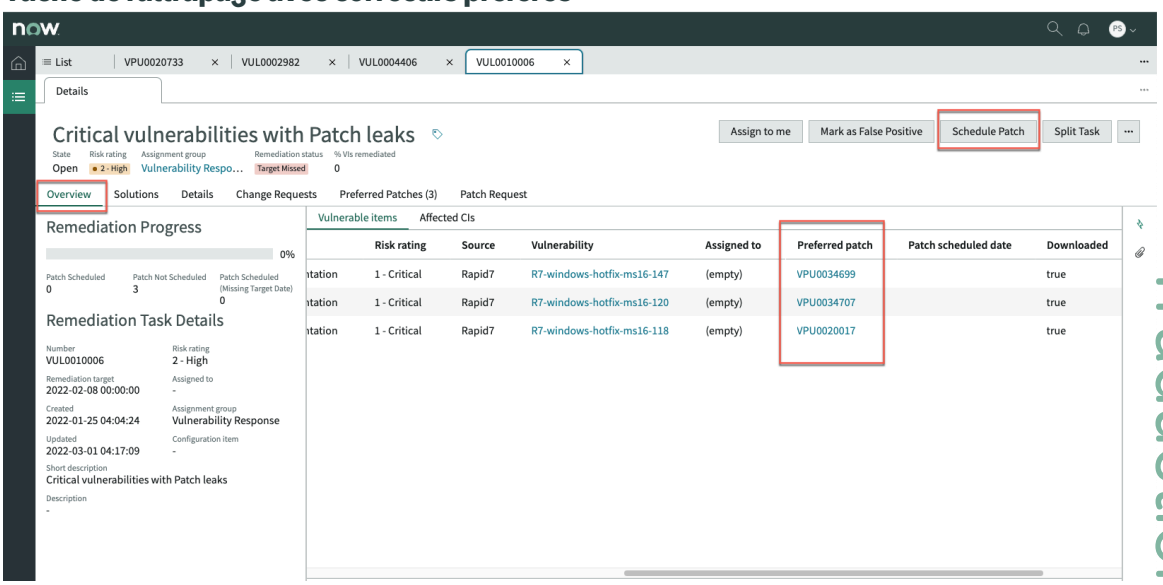
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Vous pouvez également planifier des correctifs à partir des tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe.

   Remarque : L'option permettant de planifier un correctif à partir d'un enregistrement de tâche de rattrapage n'est disponible que si des correctifs sont mappés aux VI (associés à) dans la tâche. Ces correctifs s'affichent dans la colonne Correctif préféré si vous faites défiler vers la droite d'un enregistrement de tâche de rattrapage avec l'onglet Vue d'ensemble sélectionné.

Tâche de rattrapage avec correctifs préférés



10. Cliquez sur **Planifier le correctif** dans l'enregistrement RT et suivez les étapes répertoriées ci-dessus pour le planifier dans la boîte de dialogue.

11. Vous pouvez planifier des correctifs pour les étapes répertoriées précédemment dans l'environnement classique.
    Pour localiser ces enregistrements, procédez comme suit.

    a. Dans l'environnement classique, accédez à **Réponse aux vulnérabilités** > **Correctifs** > **Tous**.

    b. Dans la liste qui s'affiche, localisez un enregistrement de mise à jour de correctif.

    c. Pour les tâches de rattrapage, accédez à **Réponse aux vulnérabilités** > **Tâches de remédiation** et localiser un enregistrement.
    Suivez l'état du rattrapage dans l'onglet État du rattrapage. Au bas de l'enregistrement, les données du correctif sont affichées sur les liens connexes.

    d. Cliquez sur Planifier le correctif et remplissez les champs.

Champ	Description
Nom du déploiement	Entrez un nom pour ce déploiement de correctif. Ce nom vous permet de suivre vos mises à jour.
Mise à jour de correctif	Choisissez-en un parmi les correctifs disponibles sur la liste.
Ressources	Sélectionner un élément :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ Groupe d'ordinateurs : sélectionnez cette option si vous souhaitez choisir une collection (un groupe d'actifs) pour ce correctif. Les groupes sont constitués des éléments de configuration importés depuis l'application BigFix. ▪ Liste d'ordinateurs : sélectionnez cette option si vous souhaitez choisir des ordinateurs individuels (actifs) pour ce correctif. Vous pouvez voir des données sur le fabricant, l'emplacement, la classe, la date de la dernière mise à jour et le calendrier de maintenance dans la boîte de dialogue qui s'affiche.
Heure de début et heure de fin	Entrez les heures de début et de fin de la fenêtre horaire. Entrez la date à laquelle vous souhaitez que le correctif commence son déploiement et le dernier jour d'installation du correctif.

Messages REST pour l'intégration d'orchestration de correctifs Vulnerability Response avec HCL BigFix

Les messages REST de l'orchestration Réponse aux vulnérabilités des correctifs avec HCL BigFix sont utilisés pour effectuer des appels vers l'API BigFix.

Connexion BigFix

Vous pouvez également utiliser les messages REST pour la connexion BigFix afin de pouvoir authentifier les demandes d'API REST. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes d'authentification adressées à BigFix.

Nom de paramètre	Valeur	Description
sourceType	cumulatif	Indique la source à partir de laquelle l'intégration extrait les données. Utilisé par le code. Il n'est pas recommandé d'apporter des modifications.
triDIR	Desc	Indique le sens de tri des données extraites de l'intégration. Il n'est pas recommandé d'apporter des modifications.
Champ de tri	severity	Indique le champ sur lequel le tri des données est basé. Il n'est pas recommandé d'apporter des modifications.
type	vulnérabilité	Indique le type de données à extraire de l'intégration pour l'intégration des actifs. Il n'est

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
		pas recommandé d'apporter des modifications.

Intégration BigFix

Vous pouvez utiliser le message REST pour l'intégration BigFix afin de récupérer des informations à partir de BigFix. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes de récupération d'informations adressées à BigFix. Les messages REST contiennent les méthodes REST suivantes.

Méthodes REST

Méthode REST	Description
GET Extraire les données	Récupère les informations de BigFix concernant l'un des éléments suivants en fonction de la requête fournie : • Ordinateur/groupes d'ordinateurs • Fixlets • Fixlets pertinents sur les ordinateurs • Actions

Nom de paramètre	Valeur	Description
URL	Valeurs dynamiques basées sur l'utilisateur	Indique le point de terminaison de la console BigFix

Correctif de déploiement BigFix

Vous pouvez utiliser le message REST de l'intégration BigFix pour planifier des correctifs de votre ServiceNow AI Platform® vers BigFix. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes de récupération d'informations adressées à BigFix. Les messages REST contiennent les méthodes REST suivantes.

Méthode REST	Description
PUBLIER le déploiement du correctif	Planifie le correctif sur la console BigFix sur un ou plusieurs ordinateurs.

Nom de paramètre	Valeur	Description
URL	Valeurs dynamiques basées sur l'utilisateur	Indique le point de terminaison de la console BigFix.
Titre	Valeurs dynamiques basées sur l'utilisateur	Titre du déploiement.
settings_tag	Paramètres nommés par balise XML avec valeurs	Indique les paramètres qui ont des paramètres différents et qui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
		sont envoyés à BigFix lors de la planification du correctif.
computer_tag	Balise XML Ordinateurs avec valeurs	Indique la liste des ordinateurs sur lesquels le correctif va être planifié.
site_name	Valeur de la mise à jour du correctif	Nom du site où le fixlet est présent.
fixlet_id	Valeur de la mise à jour du correctif	ID du fixlet.

Transformation des données pour l'intégration d'orchestration de correctifs à HCL BigFix

Les données sont récupérées à partir de l'orchestration des correctifs avec l'intégration Réponse aux vulnérabilités HCL BigFix, traitées via un ensemble de sources de données et transformées dans votre ServiceNow AI Platform® instance.

Importation de collection BigFix

Les données des actifs importés (ordinateurs et groupes d'ordinateurs) sont chargées dans la table d'importation de collection BigFix [sn_vul_bigfix_collection_import]. L'outil d'importation d'ordinateur BigFix et de groupes d'ordinateurs (carte de transformation ?) est utilisé pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de collection BigFix sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et localisez BigFix Computer et Computer Groups Import TM. La table suivante répertorie les champs de carte de transformation par intégration.

Importation d'ordinateurs BigFix et de groupes d'ordinateurs Carte de transformation minutage de script

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_bigfix] pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour créer et mettre à jour des CI en fonction des règles de recherche de CI et des collections, ainsi que des relations entre elles. En fonction des résultats, ce script modifie les valeurs de la variable de périmètre [sn_vul_bigfix]. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre de CI créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation de fixlet BigFix

Les données des fixlets importés sont chargées dans la table d'importation de fixlets BigFix [sn_vul_bigfix_patch_update_import].

BigFix Fixlet Import TM est utilisé pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de fixlet BigFix sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et localisez BigFix Fixlet Import TM.

La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation d'importation de fixlet BigFix

Champ source	Champ cible	Description
u_id	article_id	ID unique d'un fixlet dans un site.
u_id	source_id	ID unique d'un fixlet dans un site.
U_site_name	Sn_vul_bigfix_site_name	Nom du site dans BigFix sur lequel le Fixlet s'appuie.
U_display_name	Titre	Titre du fixlet.
[Script]	Bulletin_id	ID source de la solution.
[Script]	Sn_vul_solution	Solution basée sur l'ID source.
U_source	bulletin_source	Fournisseur source de la solution.
[Script]	Date_release	Date de mise en production du fixlet.
U_category	Update_category	Catégorie du fixlet.
[Script]	Is_highest_supersedence	Booléen pour savoir si le fixlet est le remplacement le plus élevé ou non.
[Script]	Is_downloaded	Booléen indiquant si le fixlet est téléchargé ou non.
[Script]	Integration_instance	Nom de l'instance à partir de laquelle le fixlet est importé.
U_source_severity	Source_severity	Gravité du fixlet.
U_applicable_count	Num_total	Nombre total d'appareils avec des fixlets manquants.
[Script]	Last_modified	Date de la dernière modification du fixlet.

Importation de fixlet BigFix Minutage de script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_bigfix] pour le processus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation de fixlet BigFix Minutage de script de carte de transformation (suite)

Script	Description
	d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour mettre à jour les valeurs de la variable de périmètre [sn_vul_bigfix]. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre de fixlets créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Importation de fixlet d'appareil BigFix

Les données des fixlets pertinents importés sur les ordinateurs sont chargées dans la table d'importation de fixlets d'appareils BigFix [sn_vul_bigfix_device_patch_import].

BigFix Device Fixlet TM est utilisé pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de fixlet d'appareil BigFix sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et localisez le BigFix Device Fixlet TM.

La table suivante répertorie les champs de carte de transformation par intégration.

Fixlet de l'appareil BigFix Carte de transformation Minutage de script

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_bigfix] pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour créer et mettre à jour des CI en fonction des règles et collections de recherche de CI, ainsi que des relations entre elles. En fonction des résultats, ce script modifie les valeurs de la variable de périmètre [sn_vul_bigfix]. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre de CI créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation d'actions BigFix

Les données des actions importées sont chargées dans la table d'importation d'actions BigFix [sn_vul_bigfix_deployment_import].

La BigFix Actions Import TM est utilisée pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation d'actions BigFix sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et localisez BigFix Fixlet Import TM.

La table suivante répertorie les champs de carte de transformation par intégration.

Actions BigFix Importer les champs de carte de transformation

Champ source	Champ cible	Description
u_id	source_id	ID unique d'une action.
U_name	nom	Nom de l'action
[Script]	Sn_vul_bigfix_discovered_item	Référence de l'élément détecté sur lequel le correctif est déployé
U_status	état	Statut de l'action
[Script]	Sn_vul_patch_orch_update	Référence du correctif
U_apply_count	Count_success	Nombre de réussites de l'action.
U_retry_count	retry	Nombre de nouvelles tentatives de l'action.
[Script]	Deployment_time	Heure de début de l'action.
[Script]	date limite	Heure de fin de l'action.
[Script]	Source_created	Heure de création de l'action.
[Script]	Integration_instance	Nom de l'instance à partir de laquelle l'action est importée.

Actions BigFix Importer une carte de transformation Minutage de script

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_bigfix] pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour mettre à jour les valeurs de la variable de périmètre [sn_vul_bigfix]. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'actions créées, mises à jour et ignorées. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de workflow pour l'intégration de Vulnerability Response Patch Orchestration à HCL BigFix

Exemple du fonctionnement de l'orchestration des correctifs avec le produit HCL BigFix.

Avant de commencer

Imaginons, par exemple, que l'ensemble de votre environnement soit corrigé une fois toutes les trois semaines. La fenêtre d'application de correctif la plus récente s'est terminée il y a une semaine, mais vous souhaitez appliquer un correctif pour corriger une vulnérabilité critique récemment connue. En raison de la nature critique de cette vulnérabilité, vous ne pouvez pas attendre deux semaines de plus pour le prochain correctif planifié.

Rôles requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour l'espace de travail du gestionnaire de vulnérabilités.
- sn_vul.remediation_owner pour afficher l'espace de travail du propriétaire de rattrapage informatique.
- Rôle sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs.
- sn_vul_patch_orch.read_patch pour afficher (lecture seule) les informations sur les correctifs dans les enregistrements. Ce rôle est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail Rattrapage informatique et Responsable des vulnérabilités.

Pourquoi et quand exécuter cette tâche

En tant que responsable ou analyste des vulnérabilités travaillant dans Vulnerability Manager Workspace, vous pouvez envisager de créer des rubriques de visualisation ou de modifier des rubriques de surveillance existantes pour vous aider à capturer les VI importés présentant des vulnérabilités critiques. Avec l'intégration de l'orchestration des correctifs, vous pouvez également voir les correctifs que vous souhaitez utiliser pour corriger et suivre ces vulnérabilités. Le tableau suivant répertorie quelques exemples avec les conditions que vous pouvez définir pour les rubriques de surveillance pour l'orchestration des correctifs. Utilisez ces exemples pour vous aider à déterminer les paramètres les plus adaptés à votre environnement. Voir Créer une rubrique de surveillance dans le Espace de travail du gestionnaire de vulnérabilités pour plus d'informations sur la configuration de la rubrique de la montre.

Exemples de rubriques de surveillance pour l'orchestration des correctifs dans l'espace de travail du gestionnaire de vulnérabilité

Nom de la rubrique de surveillance	Description
Vulnérabilités critiques avec fuites de correctifs	La cote de risque est 1 : critique ET La raison pour laquelle le correctif n'est pas planifié
Vulnérabilités critiques avec correctifs planifiés (SLA manquant)	Motif : correctif planifié (date cible manquante)
Vulnérabilités critiques avec correctifs planifiés	La cote de risque est 1 : critique ET La date planifiée du correctif n'est pas vide ET

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemples de rubriques de surveillance pour l'orchestration des correctifs dans l'espace de travail du gestionnaire de vulnérabilité (suite)

Nom de la rubrique de surveillance	Description
	Motif pour lequel le correctif est planifié

- En tant que gestionnaire de vulnérabilité ou analyste, après avoir créé les rubriques de surveillance et les efforts de rattrapage, vous générez des tâches de rattrapage. À partir des enregistrements de VI et des tâches de rattrapage, vous pouvez explorer l'onglet Détections et localiser les enregistrements d'éléments détectés qui présentent la vulnérabilité que vous suivez, ainsi que les actifs importés par le produit BigFix.
- En tant qu'analyste ou administrateur de vulnérabilités, vous pouvez surveiller les données des correctifs associées à la vulnérabilité. Vous pouvez également déployer un ou plusieurs correctifs sur un actif spécifique (élément de configuration) à partir d'un enregistrement d'élément détecté.

En tant que spécialiste de la remédiation informatique, vous disposez d'options pour traiter la vulnérabilité avec un déploiement de correctif.

- Vous pouvez planifier le correctif à partir d'un enregistrement de mise à jour de correctif (VPU#).
- Si des solutions préférées sont mappées aux éléments vulnérables (VI) et qu'elles vous sont affectées ou sont affectées à vous ou à vos groupes, vous pouvez planifier les correctifs à partir d'une tâche de rattrapage qui comporte ces éléments vulnérables.

Procédure

1. En tant que spécialiste de la remédiation informatique, dans l'espace de travail de remédiation informatique, cliquez sur la vue Accueil.
2. Dans la vue d'accueil, cliquez sur le tableau de résultats **des tâches de rattrapage affectées** pour afficher les enregistrements.

   Pour les besoins de cet exemple, vous pouvez vérifier le champ Description brève de la tâche de rattrapage (VUL#) pour tout texte relatif à votre vulnérabilité critique. Imaginons, par exemple, que vous sachiez que votre gestionnaire de vulnérabilité a créé une rubrique de surveillance appelée Vulnérabilités critiques avec fuites de correctifs pour attraper les VI (VIT#) avec cette vulnérabilité critique.

   Une fois l'enregistrement ouvert, vous pouvez également examiner les éléments vulnérables et les correctifs préférés, et voir si vous ou un membre de votre groupe avez déjà soumis des demandes de correctifs pour approbation.
3. Si vous disposez de suffisamment d'informations, vous préférerez peut-être soumettre une demande de correctif maintenant à partir de cette tâche de rattrapage.

   Remarque : Si les éléments vulnérables associés à l'enregistrement ne possèdent pas de correctifs mappés, le bouton **Planifier le correctif** n'est pas disponible sur l'enregistrement.
4. Cliquez sur **Planifier le correctif** et remplissez les champs dans la boîte de dialogue. Pour plus d'informations sur la planification d'un patch, reportez-vous à la section Planifier des correctifs avec l'intégration d'orchestration Réponse aux vulnérabilités de correctifs HCL BigFix.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. À partir de la vue de liste de l'espace de travail de remédiation informatique, vous pouvez également cliquer sur les liens Tâches de remédiation, Éléments vulnérables, Solutions et Correctifs pour afficher ces enregistrements.

   Dans le cas de cet exemple, au lieu d'un nom de rubrique de visualisation, vous connaissez peut-être l'ID de l'article ou l'ID du bulletin et le titre du patch. Si tel est le cas, vous voudrez peut-être vérifier si l'un des VI avec cette vulnérabilité vous est affecté ou à vos groupes. À partir des enregistrements de mise à jour de correctifs, vous pouvez soumettre des demandes de correctifs. À partir des enregistrements de VI, vous pouvez rechercher des correctifs potentiels et ouvrir la tâche de rattrapage associée si vous souhaitez soumettre une demande de correctif.

6. Si vous n'avez pas accès aux espaces de travail ou si vous préférez afficher les données et planifier des correctifs à partir de l'environnement classique, procédez comme suit.

   a. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Correctifs** > **Tous**.

   b. Localisez l'enregistrement de mise à jour de correctif souhaité.
   Vous préférez peut-être filtrer les enregistrements avec des scores de risque critique .

   c. Examinez les champs des VI associés et % des VI rattrapés dans l'onglet État du rattrapage.
   Si les VI disposent de correctifs, le bouton **Planifier le correctif** s'affiche dans le coin supérieur droit de l'enregistrement.

   d. Si vous décidez de soumettre une demande, cliquez sur **Planifier le correctif**.
   Pour plus d'informations sur la planification d'un patch, reportez-vous à la section Planifier des correctifs avec l'intégration d'orchestration Réponse aux vulnérabilités de correctifs HCL BigFix.

   e. Vous pouvez également dire que vous ne disposez pas des informations relatives à l'ID du correctif, mais que vous pouvez consulter le champ Description brève des tâches de rattrapage affectées à votre groupe pour tout texte relatif à votre vulnérabilité critique.

   f. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**.

   g. Recherchez l'enregistrement souhaité et cliquez dessus pour l'ouvrir.
   Dans l'enregistrement ouvert, passez en revue l'onglet État du rattrapage pour les VI et % des VI rattrapés. Cliquez sur les liens connexes pour les enregistrements de VI, les solutions préférées, les correctifs préférés et les demandes de correctifs.

   > **Remarque :** Si les éléments vulnérables associés à l'enregistrement ne possèdent pas de correctifs mappés, le bouton **Planifier le correctif** n'est pas disponible sur l'enregistrement.

   h. Cliquez sur **Planifier un correctif** dans l'enregistrement si vous souhaitez soumettre une demande de correctif.

Présentation de l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs à Microsoft SCCM

Gérez les correctifs et les déploiements de correctifs pour les vulnérabilités critiques sur vos actifs grâce à l'intégration Réponse aux vulnérabilitésMicrosoft au produit System Center Configuration Manager (SCCM).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Orchestration de correctifs avec Réponse aux vulnérabilités

L'orchestration des correctifs utilise Réponse aux vulnérabilités des importations planifiées à partir d'intégrations de solutions tierces, de fournisseurs de correctifs et de scanners de vulnérabilité. Les données de détection des scanners font correspondre les ressources de votre environnement aux vulnérabilités et aux mises à jour de correctifs qui peuvent les corriger. Vous soumettez des demandes de correctifs pour approbation, planifiez des mises à jour de correctifs pour résoudre les éléments vulnérables et surveillez la progression du rattrapage à partir de votre ServiceNow AI Platform® instance.

Réponse aux vulnérabilités orchestration de correctifs avec Microsoft SCCM

Lorsque l'orchestration de correctifs Vulnerability Response avec l'application Microsoft SCCM est utilisée avec l'orchestration de ServiceNow® Gestion des solutions pour vulnérabilités correctifs et Réponse aux vulnérabilités les applications, les gestionnaires de vulnérabilités et les analystes peuvent effectuer les tâches suivantes :

- Consultez plus de contexte et d'informations sur les types de correctifs et les solutions des fournisseurs (correctifs).
- Affichez et surveillez les données relatives aux vulnérabilités et aux solutions, ainsi que la progression du rattrapage des vulnérabilités à partir des enregistrements dans les espaces de Réponse aux vulnérabilités travail.

Les spécialistes informatiques et les propriétaires de rattrapage peuvent effectuer les tâches suivantes :

- Déployez les correctifs pris en charge par le Microsoft produit SCCM pour leurs Windows, CentOS, MacOS, Oracle et d'autres ressources à intervalles réguliers et planifiés en dehors des heures de travail afin d'éviter les conflits de travail.
- Identifiez les actifs non corrigés présentant des vulnérabilités ou les actifs qui n'ont pas été mis à jour avec succès par des correctifs planifiés à partir des données de détection importées à partir d'analyses tierces.
- Planifiez les correctifs disponibles à partir de l'espace de travail de remédiation informatique ou de l'interface utilisateur classique pour les actifs vulnérables non corrigés à partir de la mise à jour du correctif, de la tâche de rattrapage et des enregistrements d'éléments détectés.

Termes clés dans les Réponse aux vulnérabilitésMicrosoft applications et SCCM

Élément de configuration (CI)

Les CI sont les actifs existants répertoriés dans votre Base de données de gestion des configurations (CMDB). Microsoft SCCM appelle les CI, les appareils.

Collections et collections d'appareils

Terminologie utilisée dans le Microsoft produit SCCM qui fait référence à un groupe d'actifs.

Élément vulnérable

Une vulnérabilité importée qui correspond à un actif existant dans votre CMDB.

Instance

Un compte rendu distinct de l'application Microsoft SCCM. Chaque compte utilisateur peut être une instance de l'application Microsoft SCCM. Ce terme fait également référence à une adresse Web unique et sécurisée pour une ServiceNow AI Platform instance.

Intégration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une intégration est une tâche planifiée dans qui ServiceNow AI Platform récupère des informations d'une source tierce, telle que l'intégration avec les Microsoft machines SCCM.

Solution

Il existe deux types de solutions dans le cadre de cette intégration, potentielle et préférée. Une solution potentielle est une solution qui pourrait remédier à une vulnérabilité. Les vulnérabilités ont souvent de nombreuses solutions potentielles. #Une solution privilégiée correspond à la solution la plus efficace pour une vulnérabilité spécifique détectée.

Correctifs

Mises à jour logicielles qui corrigent les vulnérabilités. Dans l'application Microsoft SCCM, les correctifs sont appelés correctifs. Par exemple, Microsoft SCCM dispose de correctifs pour Windows, CentOS, Oracle MAC et d'autres produits.

Correctif préféré

Les correctifs préférés sont des mises à jour logicielles destinées à corriger des vulnérabilités spécifiques. Une fois déployés, les correctifs sont mappés aux éléments vulnérables liés à des vulnérabilités spécifiques et les corrigent.

Tâche de rattrapage ou, avant la version 15.0 de , groupes de Réponse aux vulnérabilités vulnérabilité

Listes des éléments vulnérables dans l'application Réponse aux vulnérabilités des actions requises pour corriger les vulnérabilités.

Déploiement

Aux fins de cette intégration, le déploiement désigne l'application, le lancement ou la planification d'un correctif sur un ordinateur. Vous pouvez déployer les correctifs que vous avez téléchargés à partir de Microsoft SCCM dans votre ServiceNow AI Platform en accédant aux éléments détectés, aux correctifs ou aux tâches de rattrapage à partir d'enregistrements individuels dans Réponse aux vulnérabilités. Vous pouvez déployer des correctifs avec des travaux planifiés sur des machines individuelles ou sur des groupes d'ordinateurs.

Le déploiement dans peut ServiceNow AI Platform également faire référence à une intégration qui prend en charge le multisource. Une existence d'intégration unique est appelée un déploiement de votre intégration. Un déploiement fait référence aux intégrations et aux produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de l'intégration Microsoft de vulnérabilité SCCM dans votre environnement.

Gestion des solutions pour vulnérabilités et l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs à Microsoft SCCM

L'application Gestion des solutions pour vulnérabilités est une ServiceNow AI Platform application qui met en corrélation vos résultats de vulnérabilité avec la répartition des solutions (correctifs) qui les corrigent. Identifiez les correctifs logiciels tiers pour les produits et services, les mises à jour de configuration et les autres contrôles qui ont le plus d'impact sur votre organisation. En plus des informations sur les scanners tiers, , Gestion des solutions pour Réponse aux vulnérabilitésRéponse aux vulnérabilités et Vulnerability Response Patch Orchestration avec Microsoft applications SCCM fonctionnent ensemble pour déployer les correctifs préférés de la solution à la vulnérabilité et à l'élément vulnérable, afin de vous aider à corriger et à fermer les vulnérabilités de votre environnement. Les Gestion des solutions pour Réponse aux vulnérabilités applications d'intégration SCCM , Réponse aux vulnérabilités, et Patch Réponse aux vulnérabilités Orchestration Microsoft sont toutes disponibles dans le ServiceNow® Store.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles ServiceNow AI Platform requis

Les tâches d'installation, de configuration et de rattrapage de l'intégration nécessitent les rôles suivants dans votre ServiceNow AI Platform instance.

administrateur

Les utilisateurs disposant de ce rôle obtiennent des autorisations pour les applications dans et ServiceNow Store les téléchargent vers les ServiceNow AI Platform instances.

sn_vul.vulnerability_admin

Les utilisateurs ayant ce rôle activent les applications dans l'instance ServiceNow AI Platform et terminent la configuration de l'application Réponse aux vulnérabilités . Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Cet utilisateur administrateur configure l'ensemble des applications VR, des règles et des intégrations tierces.

sn_vul_sccm.configure_integration

Les utilisateurs possédant ce rôle configurent l'application d'intégration Microsoft SCCM Patch Orchestration. Ce rôle contient le rôle granulaire sn_vul_sccm.read_integration.

sn_vul_sccm.read_integration

Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les enregistrements de l'application Réponse aux vulnérabilités SCCM Patch Orchestration Integration et les données d'orchestration Microsoft de correctifs.

sn_vul_patch_orch.configure_patch

Les utilisateurs disposant de ce rôle peuvent configurer et appliquer des correctifs.

sn_vul_patch_orch.read_patch

Les utilisateurs disposant de ce rôle peuvent afficher (lecture seule) les informations sur les correctifs.

Approbateurs

Affectez des utilisations aux groupes d'approbateurs de niveau 1 et d'approbateur de niveau 2 si vous souhaitez que les demandes de correctifs soumises soient approuvées avant le déploiement.

Pour plus d'informations sur l'affectation de ces rôles à l'aide de l'assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

Règles de recherche de CI

Lorsque des données sont importées à partir de l'application Microsoft SCCM, celle-ci Réponse aux vulnérabilités recherche automatiquement des correspondances dans les données d'ID Base de données de gestion des configurations (CMDB) de ressource utilisée. Les règles de recherche de CI sont utilisées pour identifier les CI (actifs) et les ajouter automatiquement aux enregistrements d'éléments vulnérables (VI) lors de la création des VI. Les règles de recherche de CI suivantes sont fournies avec le système de base et sont utilisées pour identifier les CI (actifs) et les ajouter aux éléments détectés.

Cette règle de recherche s'appuie sur les données apportées par Service Graph Connector avec SCCM. Vous devez installer et exécuter l'intégration CMDB avant d'exécuter les intégrations SCCM. Si vous avez plusieurs installations du serveur SCCM, vous pouvez configurer l'alias de connexion de Connecteur du graphe de services sur la page de configuration de l'orchestration du correctif SCCM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Serveur MID

Vulnerability Response Patch Orchestration avec Microsoft SCCM est une intégration sur site. Elle nécessite un serveur MID autonome Windows qui ne fait pas partie d'une grappe de serveurs MID. Le serveur MID est nécessaire pour exécuter des scripts sur des ordinateurs distants à partir de votre instance afin d'importer des données à partir du serveur SCCM. Les API pour cette intégration sont appelées à l'aide des MID Servers que vous configurez dans votre ServiceNow AI Platform instance. Préparer l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs avec Microsoft SCCM

Intégrations et dépendances de Vulnerability Response Patch Orchestration avec l'application Microsoft SCCM

Les applications de produits et dépendances suivantes sont requises pour Vulnerability Response Patch Orchestration avec Microsoft System Center Configuration Manager (SCCM). Ces applications sont disponibles dans le ServiceNow® Store

Versions disponibles des applications et dépendances requises pour l'intégration de l'orchestration des correctifs

Pour afficher les données d'orchestration des correctifs et les mises à jour disponibles (correctifs) dans les espaces de travail et l'interface utilisateur classique dans Réponse aux vulnérabilités, les applications suivantes sont requises. Toutes les applications répertoriées sont disponibles dans le ServiceNow® Store. Certaines applications nécessitent des abonnements distincts.

Pour plus d'informations sur la compatibilité des versions avec les applications et les versions de famille requises, consultez l'article KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes de la base de connaissances HI.

Application et version de mise en production
Réponse aux vulnérabilités
Gestion des solutions pour vulnérabilités
Application Vulnerability Response Patch Orchestration
Vulnerability Response Patch Orchestration avec l'application Microsoft SCCM
Security Support Common
Orchestration du support de sécurité
Connecteur du graphe de services avec SCCM

Réponse aux vulnérabilités Tables de l'application Patch Orchestration

L'application Réponse aux vulnérabilités Patch Orchestration contient les tables suivantes :

Table	Description
Mise à jour du correctif [sn_vul_patch_orch_update]	Stocke des informations sur les correctifs disponibles sur des instances distinctes.
Mise à jour de l'appareil [sn_vul_patch_orch_m2m_src_ci_update]	Stocke les données relatives aux correctifs déployés, ainsi que l'état de déploiement, qui sont affichés sur les enregistrements d'éléments détectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Collecte [sn_vul_patch_orch_collection]	Stocke les données de collecte d'instances distinctes.
Ensemble d'appareils [sn_vul_patch_orch_m2m_src_ci_collection]	Stocke les données des collections sur les éléments découverts.
Déploiement de correctif [sn_vul_patch_orch_deployment]	Stocke des informations sur les correctifs déployés sur les collections et les CI.
Correctif potentiel [sn_vul_patch_orch_m2m_vuln_patch]	Stocke des données sur les correctifs et les vulnérabilités qui identifient les correctifs qui peuvent être utilisés pour résoudre une vulnérabilité.

Vulnerability Response Patch Orchestration avec Microsoft intégrations SCCM

Les intégrations développées par ServiceNow® l'ingénierie constituent le déploiement orchestré de la solution avec le Microsoft produit SCCM. Les intégrations suivantes sont incluses dans l'application d'intégration Microsoft SCCM Patch Orchestration que vous téléchargez à partir du ServiceNow® Store.

Après avoir installé l'application d'intégration sur votre ServiceNow AI Platform instance, pour afficher ces intégrations, accédez à **Intégrations** > **Intégration d'orchestration du correctif SCCM** > **Intégrations**. L'application Réponse aux vulnérabilités traite les données selon les intervalles de temps planifiés importés par ces intégrations avec Microsoft les points de terminaison SCCM.

Intégration	Description
Microsoft Intégration de la collection SCCM	• Cette intégration est planifiée pour s'exécuter quotidiennement et s'exécute en premier dans l'exécution de l'intégration chaînée. • Récupère les collections d'appareils à partir des collections SCCM.
Microsoft Intégration de la collection des appareils SCCM	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de la collection SCCM. Vous pouvez également l'exécuter sur demande. • Cette intégration récupère les appareils sous chaque collection. Cette intégration crée des enregistrements dans la table Éléments détectés et dans la table Collection d'appareils.
Microsoft Intégration de la mise à jour du correctif SCCM	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de la collection d'appareils SCCM. Vous pouvez également l'exécuter sur demande. • Récupère des informations à partir du serveur SCCM sur les correctifs installés ou manquants sur les appareils (actifs).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
Microsoft Intégration des déploiements SCCM	• Lorsqu'elle est planifiée, cette intégration est déclenchée par l'achèvement de l'intégration de la mise à jour des correctifs. Vous pouvez également l'exécuter sur demande. • Récupère les informations sur les correctifs planifiés par l'équipe informatique sur le serveur SCCM.

Préparer l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs avec Microsoft SCCM

Préparez l'intégration en effectuant les tâches de configuration suivantes.

Avant de commencer

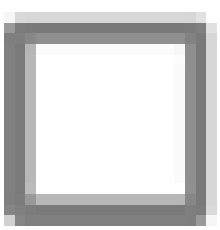
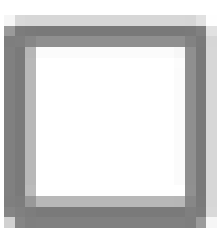
Rôles requis : admin pour l'installation des applications et l'affectation des rôles. D'autres rôles sont répertoriés dans le tableau suivant.

Pourquoi et quand exécuter cette tâche

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration.

Procédure

1. Pour une installation et une configuration fluides de l'application Vulnerability Response Patch Orchestration avec Microsoft SCCM, suivez la liste de vérification ci-dessous.
2. Vous préférez peut-être imprimer la liste de vérification suivante et vérifier que les éléments énumérés sont renseignés avant d'installer l'application et d'importer les informations relatives à la vulnérabilité et aux correctifs dans votre ServiceNow AI Platform® instance.

Tâche	Description
	(Facultatif) Si elle n'est pas déjà installée et activée, vous préférerez peut-être installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour plus d'informations sur l'installation et l'activation de l'application, Installer Réponse aux vulnérabilités reportez-vous à la Réponse aux vulnérabilités section . Cette intégration requiert la version 16.1 ou Réponse aux vulnérabilités ultérieure.
	Si ce n'est pas déjà fait, obtenez les autorisations et installez une application d'analyse tierce pour importer les données de vulnérabilité. Pour Intégrations de Réponse aux vulnérabilités plus d'informations sur les scanners tiers pris en charge par Réponse aux vulnérabilités. Consultez .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
☐	Si ce n’est pas déjà fait, obtenez les autorisations et téléchargez l’application Vulnerability Response Patch Orchestration avec Microsoft SCCM sur votre ServiceNow AI Platform® instance. Consultez .
☐	Obtenez Microsoft les informations d’identification SCCM. Vérifiez que vous disposez des noms de compte, mots de passe et autres informations de service requis par vos Microsoft produits afin d’y avoir accès.
☐	Vérifiez que vous disposez de groupes ou d’utilisateurs pour gérer les intégrations et corriger les éléments vulnérables. **administrateur** L’administrateur système obtient les autorisations, télécharge et installe l’application Microsoft SCCM Patch Orchestration et les autres applications requises pour l’intégration. S’il n’est pas affecté, l’administrateur affecte l’administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d’autres rôles dans l’assistant de configuration dans Réponse aux vulnérabilités ou à partir du module Administration utilisateurs. **sn_vul.vulnerability_admin** Une fois affecté, l’administrateur de vulnérabilité termine la configuration des intégrations SCCM et des Microsoft autres applications tierces. Ce rôle dispose d’un accès complet à l’application Réponse aux vulnérabilités (VR) et à ses enregistrements. Ce rôle configure toutes les applications de réalité virtuelle, les règles, les intégrations tierces, Réponse aux vulnérabilités l’orchestration des correctifs et les applications de gestion des solutions de vulnérabilité. **sn_vul_sccm.configure_integration** Les utilisateurs possédant ce rôle configurent l’application d’intégration Microsoft SCCM Patch Orchestration. Ce rôle contient les rôles granulaires sn_vul_sccm.read_integration et connection_admin qui permettent à l’utilisateur de se connecter à la console SCCM et de configurer les instances d’intégration dans votre ServiceNow AI Platform. **sn_vul_sccm.read_integration**

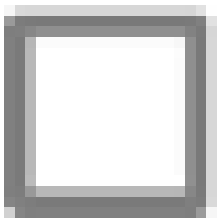
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Les utilisateurs disposant de ce rôle peuvent afficher (en lecture seule) les enregistrements de l'application Réponse aux vulnérabilités SCCM Patch Orchestration Integration et les données d'orchestration Microsoft de correctifs. **sn_vul_patch_orch.configure_patch** Les utilisateurs disposant de ce rôle peuvent configurer et appliquer des correctifs. Les correctifs demandés par cet utilisateur à partir des enregistrements d'élément vulnérable et de mise à jour de correctif sont envoyés pour approbation si Gestion des changements est actif et que des approbateurs sont affectés. **sn_vul_patch_orch.read_patch** Les utilisateurs disposant de ce rôle peuvent afficher (lecture seule) les informations sur les correctifs dans les enregistrements. Ce rôle est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail Rattrapage informatique et Responsable des vulnérabilités. **Approbateurs** Les groupes d'approbateurs affectés aux groupes d'approbateurs de niveau 1 et, éventuellement, d'approbateur 2 approuvent les demandes de correctifs soumises. Par défaut, les correctifs sont soumis au groupe d'approbateurs de niveau 1 pour approbation avant le déploiement. Pour plus d'informations sur le processus d'approbation, reportez-vous à Configurer Vulnerability Response Patch Orchestration avec Microsoft l'intégration SCCM. Pour plus d'informations sur la configuration des approbateurs et des groupes, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. L'administrateur système procède à l'affectation initiale des rôles aux utilisateurs et aux groupes pour l'intégration. Par défaut, le Réponse aux vulnérabilités groupe est disponible. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires pour les rôles de spécialiste du rattrapage et d'analyste de vulnérabilité et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance. Voir Créer un groupe d'utilisateurs .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Vérifiez que vous avez activé toutes les fonctionnalités, règles, dépendances, modules d'extension ou tâches dans votre instance requis pour l'intégration. ○ Vulnerability Response Patch Orchestration avec Microsoft SCCM est une intégration sur site qui nécessite l'utilisation d'un serveur MID autonome Windows . Pour plus d'informations sur les serveurs MID dans votre instance, consultez Serveur MID . ○ Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous** et localisez le module d'extension. S'il n'est pas installé dans votre instance, installez-le et activez-le.

Installer l'orchestration de correctifs avec Microsoft l'application Réponse aux vulnérabilités SCCM

Téléchargez l'application à partir ServiceNow Store du .

Avant de commencer

Avant d'installer l'application, vérifiez que vous avez rempli tous les éléments de la liste de vérification dans Préparer l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs avec Microsoft SCCM.

Rôles requis : administrateur pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application. Administrateur de vulnérabilité (sn_vul.vulnerability_admin ou sn_vul.admin (obsolète) pour configurer l'orchestration Microsoft de correctifsRéponse aux vulnérabilités, SCCM et d'autres applications après leur installation.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de sous-production ou de développement, il n'est pas nécessaire d'obtenir l'autorisation, passez à Activer une ServiceNow Store application.

Procédure

1. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.
2. Localisez l'application **Vulnerability Response Patch Orchestration avec Microsoft SCCM** et cliquez sur **Installer**.

   Cette action installe l'application que vous avez téléchargée à partir du ServiceNow Store.
3. Vous pouvez également installer des applications à partir de l'assistant de configuration.
   Pour plus d'informations sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.

Que faire ensuite

Une fois l'installation terminée, accédez à **Tous** > **Intégration d'orchestration de correctifs SCCM Microsoft** > **Configuration** pour poursuivre la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Vulnerability Response Patch Orchestration avec Microsoft l'intégration SCCM

Une fois l'application installée, configurez-la avec les informations de votre compte et validez vos informations d'identification.

Avant de commencer

Rôles requis : sn_vul.vulnerability_admin et sn_vul_sccm.configure_integration

Procédure

1. Accédez à la **Tous** > **Intégration d'orchestration de correctifs SCCM Microsoft** > **Configuration**.
2. Renseignez les champs avec vos informations SCCM et vos Microsoft informations d'identification.

Champ	Description
Instance d'intégration	Le nom du compte d'instance SCCM que vous souhaitez utiliser, par exemple, intégration de la Microsoftgestion des correctifs Microsoft SCCM.
Nom d'hôte	Entrez l'URL de l'hôte Microsoft SCCM.
Nom d'utilisateur	Entrez le nom d'utilisateur de votre Microsoft compte SCCM.
Mot de passe	Saisissez le mot de passe de votre Microsoft compte SCCM.
Serveur MID	Entrez le nom du Serveur MID autonome dans la liste que vous voulez utiliser. Pour Préparer l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs avec Microsoft SCCM plus d'informations sur les serveurs MID et configurez les tâches dans votre ServiceNow AI Platform®.

3. Cliquez sur Enregistrer et tester les informations d'identification.
   L'état de votre connexion entre Microsoft SCCM et votre ServiceNow AI Platform® instance est affiché dans le champ État de validation. Si vous ne voyez pas de test réussi, suivez les invites.
4. **Facultatif :** L'application Séparation de domaine est prise en charge pour cette intégration.
   Vous pouvez ajouter plusieurs configurations à votre instance. Pour ajouter des configurations supplémentaires :
   a. Accédez à la **Tous** > **Intégration d'orchestration de correctifs SCCM Microsoft Instances d'intégration**.
   b. Vérifiez que le périmètre de l'application, Vulnerability Response Patch Orchestration with Microsoft SCCM, s'affiche dans le champ Périmètre de l'application.
   c. Cliquez sur **Nouveau**.
   d. Remplissez le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom de l'instance d'intégration.
Application	Orchestration de correctifs Vulnerability Response avec Microsoft SCCM
Intégration	[Lecture seule] Microsoft La gestion des correctifs SCCM est la gestion par défaut.
Actif	Activé par défaut. Si elle est décochée, l'instance n'est pas active.

e. Cliquez sur **Envoyer**.
Votre nouvelle instance d'intégration s'affiche dans la liste Instances d'intégration.

f. Répétez les étapes 1 à 3 pour configurer votre instance d'intégration et tester vos informations d'identification.

5. Configurez les approbations pour les demandes de correctifs.
Par défaut, une propriété système [**sn_vul_patch_orch.patch_approval_required**] est activée de sorte que, lorsque des déploiements de correctifs sont planifiés, ils sont soumis pour revue et approbation aux utilisateurs affectés au groupe d'approbation de mise à jour de correctif de niveau 1 - correctif.

Si vous souhaitez que les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch planifient des correctifs sans approbation, vous pouvez désactiver la propriété [**sn_vul_patch_orch.patch_approval_required**]. Vous préférez peut-être laisser les approbations activées afin que les correctifs planifiés n'entrent pas en conflit avec les heures de travail normales.

Remarque : Si vous désactivez la propriété système d'approbation, tout utilisateur disposant du rôle sn_vul_patch_orch.configure_patch peut planifier et déployer des correctifs sans examen ni approbation.

En tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin, désactivez la propriété système :

a. Accédez à la **Tous** > **liste.propriétés.système**.

b. Recherchez **sn_vul_patch_orch.patch_approval_required** et cliquez dessus pour ouvrir l'enregistrement.

c. Dans le champ Valeur, tapez `faux`.

d. Cliquez sur **Mettre à jour**.

6. Si vous ne désactivez pas cette propriété, vous devez affecter des approbateurs pour les demandes de correctifs.
En tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin, procédez comme suit.

a. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'approbation**.

b. Si la règle **d'approbation d'approbation de mise à jour de correctif de déploiement** ne s'affiche pas dans la liste, cliquez sur **Tout** à droite de l'icône de filtre verte en haut à gauche de l'écran pour afficher toute la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. À partir de la liste, cliquez sur **Déployer l'approbation de mise à jour de correctif**.

d. Sur l'enregistrement, avec l'onglet Configuration de l'approbation sélectionné, cliquez sur **Approbation de la mise à jour du correctif de configuration par défaut**.

e. Sur l'enregistrement, cliquez sur **Niveau 1 : approbation de la mise à jour du correctif**.

f. Ajouter des utilisateurs à ce groupe.

Les utilisateurs affectés à ce groupe approuvent les demandes de correctifs soumises par les utilisateurs disposant du rôle sn_vul_patch_orch.configure_patch. Naviguez vers **Mes approbations** pour afficher et traiter les demandes.

7. Cliquez sur**Mettre à jour** pour enregistrer vos modifications.

8. **Facultatif :** Vous pouvez configurer des approbations à plusieurs niveaux de sorte que plusieurs approbations soient requises avant le déploiement des demandes de correctifs planifiées.

a. Une fois l'enregistrement d'approbation de mise à jour de correctif de configuration par défaut affiché, cliquez sur **Nouveau**.

b. Renseignez les champs.

Champ	Description
Nom	Nom du niveau d'approbation, par exemple, **Niveau 2 : approbation de mise à jour du correctif**.
Actif	Activé par défaut, ce qui signifie que le niveau d'approbation est utilisé.
Approbation requise	Sélectionnez le nombre d'approbations requises pour le niveau sélectionné : ▪ Un approbateur requis ▪ Approbation de tous les utilisateurs requise
Ordre	Ordre d'exécution de diverses configurations au sein d'une règle. Par exemple, une configuration avec une entrée d'ordre de 100 s'exécute avant une configuration avec une entrée d'ordre de 200.
Rôle	Sélectionnez un rôle pour le groupe dans la liste.
Règle d'approbation	Contient les détails de la table et du type pour la règle d'approbation.
Configuration de l'approbation	Contient les configurations d'approbation.
Affecter à l'aide de	Sélectionnez une option :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ Utilisateur et groupe d'utilisateurs ▪ Champ de la table des approbations ▪ Script
Groupes	Groupe au niveau de l'approbateur composé de plusieurs utilisateurs. L'utilisateur doit disposer de l'un des rôles suivants que vous spécifiez.
Utilisateurs	Modifiez les utilisateurs répertoriés dans les groupes.

c. Cliquez sur **Soumettre** pour enregistrer vos modifications.

Affichage des données de correctif et du déploiement de données de correctif pour l'intégration de Patch Réponse aux vulnérabilités Orchestration à Microsoft SCCM

Les données de correctifs et de déploiement de correctifs, ainsi que les informations de vulnérabilité et l'état de rattrapage de vos vulnérabilités sont affichées sur les enregistrements de votre instance.

Afficher les données des correctifs dans les espaces de Réponse aux vulnérabilités travail

Rôles requis :

- Rôle sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs
- sn_vul_patch_orch.read_patch pour afficher (lecture seule) les informations sur les correctifs dans les enregistrements. Ce rôle est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst qui sont requis pour les espaces de travail du rattrapage informatique et du gestionnaire de vulnérabilité

Dans l'espace de travail de remédiation informatique, vous pouvez afficher les correctifs :

- Dans la vue Accueil, où vous pouvez cliquer sur les tableaux de résultats pour afficher les enregistrements de solutions préférées sur les éléments vulnérables, de CI vulnérables et de correctifs préférés sur les éléments vulnérables.
- Dans la vue de liste, où vous pouvez afficher tous les enregistrements de mise à jour de correctif (VPU) à partir des liens de correctifs et les éléments vulnérables (VIT) qui vous sont affectés et qui ont des correctifs.

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- À partir de la mise à jour du correctif (VPU)
- Tâche de rattrapage (RT)
- Enregistrements d'éléments détectés (SDI)

Dans l'espace de travail Responsable des vulnérabilités, vous pouvez afficher les correctifs :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- À partir de la vue Accueil sur les rubriques de visualisation, où vous pouvez afficher les correctifs préférés et potentiels, les dates planifiées des correctifs et, si le correctif a été téléchargé, le tout dans l'onglet **Éléments vulnérables** .
- Dans la vue de listes sur les efforts de rattrapage, où vous pouvez afficher les données de correctifs sur les enregistrements de VI à partir de l'onglet**Éléments vulnérables** .

Dans la vue d'environnement classique, accédez à **Tous** > **Réponse aux vulnérabilités** > **Correctifs**.

Correctif : mettre à jour les enregistrements dans les espaces de travail VR et dans la vue de l'environnement classique

Les données de correctif et les données et l'état de déploiement de correctif s'affichent sur les enregistrements de votre instance. Les enregistrements de correctifs sont inclus dans le cadre de la fonctionnalité d'orchestration des correctifs de cette intégration avec Réponse aux vulnérabilités. Affichez les enregistrements Patch (VPU) dans Réponse aux vulnérabilités les espaces de travail à partir de la vue de liste de l'espace de travail de remédiation informatique. Les enregistrements de mise à jour de correctif dans l'environnement classique et Réponse aux vulnérabilités dans les espaces de travail incluent les données suivantes :

- Données et informations de solutions de vulnérabilité provenant des fournisseurs de correctifs importées par l'application Gestion des solutions de vulnérabilité.
- État du rattrapage à la source qui inclut le nombre total d'appareils présentant une vulnérabilité donnée qui peut être corrigée par un correctif. En outre, il inclut également tous les appareils pour lesquels des mises à jour sont manquantes.
- État du rattrapage qui inclut le % de VI rattrapés et le total des VI qui ont un correctif comme correctif préféré.
- Appareils associés, éléments vulnérables, déploiements de correctifs et demandes de correctifs sur les liens connexes des enregistrements dans la vue de classe. Ces données sont affichées sur les onglets des enregistrements dans les espaces de Réponse aux vulnérabilités travail.
- Demandes de correctifs que les propriétaires de rattrapage ont soumises pour approbation.

Déploiement d'état sur les enregistrements d'éléments vulnérables

Pour plus d'informations sur le déploiement de l'état vers les enregistrements, reportez-vous à la section Données de correctif et déploiement d'état pour l'orchestration de correctifs dans Réponse aux vulnérabilités.

Enregistrements qui recupèrent les nombres de VI actifs

Pour éviter de déployer tous les correctifs sur toutes les vulnérabilités, la tâche planifiée ne récupère que les changements apportés au nombre de VI actifs. Ces changements de nombre et les données connexes sont déployés dans les enregistrements suivants dans Réponse aux vulnérabilités:

- VIT
- RT
- Solution de vulnérabilité
- Mise à jour du correctif

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des données pour les correctifs sans solutions

Pour plus d'informations sur l'affichage des patchs sans solutions, reportez-vous à la section Afficher les correctifs sans solutions dans Réponse aux vulnérabilités.

Données du correctif avec Réponse aux vulnérabilités

Les tableaux de bord Gestion de la vulnérabilité (PA) et CISO sont inclus dans un abonnement à l'application Analyse des performancesRéponse aux vulnérabilités . Si vous avez un abonnement pour Analyse des performances, mais qu'aucune intégration d'orchestration de correctifs n'est installée, l'onglet Rattrapage s'affiche sur le tableau de bord du CISO, mais il n'est pas renseigné avec des données.

Pour le tableau de bord Gestion de la vulnérabilité (PA), accédez à **Tous** > **Réponse aux vulnérabilités** > **Vue d'ensemble**. Cliquez sur l'onglet **Rattrapage** et faites défiler vers le bas de la page pour afficher les données des mises à jour de correctifs : correctifs planifiés et non planifiés, correctifs manquant leur date cible et nombres hebdomadaires.

Pour le tableau de bord CISO, accédez à **Tous** > **Réponse aux vulnérabilités** > **Tableau de bord des CISO**. Avec l'onglet Vue d'ensemble sélectionné, faites défiler vers le bas de la page pour afficher les données de couverture des correctifs : criticité, correctifs planifiés et non planifiés et correctifs manquants dans leur date cible.

Pour en savoir plus sur les tableaux de Réponse aux vulnérabilités bord, reportez-vous à Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités, Orchestration de correctifs avec les Réponse aux vulnérabilités espaces de travail et Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord.

Planifier des correctifs avec l'intégration Microsoft SCCM avec Réponse aux vulnérabilités

Planifiez des correctifs à partir des enregistrements de tâche de mise à jour de correctif et de rattrapage dans l'application de votre Réponse aux vulnérabilitésServiceNow AI Platform instance.

Avant de commencer
À partir de la version 16.1, vous pouvez planifier des correctifs à partir des espaces de Réponse aux vulnérabilités travail ou de l'environnement classique.

Rôles requis :

- Rôle sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs
- sn_vul_patch_orch.read_patch pour afficher (lecture seule) les informations sur les correctifs dans les enregistrements. Ce rôle est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst qui sont requis pour les espaces de travail du rattrapage informatique et du gestionnaire de vulnérabilité

Procédure

1. Dans les espaces de travail de vulnérabilité Réponse aux vulnérabilités , en tant qu'utilisateur disposant du rôle sn_vul.remediation_owner, accédez à **Tous** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
2. Sur la page d'accueil, cliquez sur **Patch préféré sur les VI.**
   La liste des enregistrements de mises à jour de correctifs pour les éléments vulnérables avec les correctifs préférés qui vous sont affectés s'affiche.
3. Localisez un enregistrement que vous souhaitez ouvrir et cliquez pour l'ouvrir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sinon, dans la vue de liste de l'espace de travail, cliquez sur **Correctifs** > **Tous** et localiser un enregistrement de mise à jour de correctif.
   L'enregistrement de la mise à jour du correctif s'affiche. Vous préférez peut-être examiner les données avant de planifier un correctif, car d'autres correctifs peuvent déjà être planifiés.
5. Reportez-vous au tableau suivant concernant les données affichées dans l'espace de travail de remédiation informatique et ce que vous pouvez faire.

Tâche	Description
Cliquer sur un lien d'éléments connexes	○ Vue d'ensemble : affichez des détails tels que le numéro d'enregistrement de la mise à jour du correctif, les ID de l'article et du bulletin, la date de publication et la catégorie de la mise à jour, le nom du site du correctif, la cote de risque, le score de risque, la description, la solution (le cas échéant) et l'état du rattrapage. ○ Appareils associés : liste des éléments de configuration impactés affectés par le correctif et l'état. ○ Éléments vulnérables : la liste des éléments vulnérables associés à la vulnérabilité et au correctif. ○ Déploiements de correctifs : les noms et les informations relatifs aux déploiements de ce correctif sur des actifs ou des groupes d'actifs pour ce correctif. ○ Demandes de correctifs : une liste des demandes de correctifs déjà soumises pour ce correctif.
Cliquez sur un lien pour ouvrir un enregistrement	Dans les listes affichées sur les enregistrements ouverts à partir des liens d'éléments connexes, affichez plus de détails, y compris les messages sur les cibles manquées. Une fois ouverts, les enregistrements restent ouverts sous forme d'onglets jusqu'à ce que vous les fermiez.
Planifier le correctif	Lorsque vous êtes prêt à planifier un correctif ou à soumettre une demande, cliquez sur **Planifier un correctif**. Dans la boîte de dialogue qui s'affiche, renseignez les champs. Pour en savoir plus, reportez-vous aux étapes ci-dessous.
Ajouter une note de travail ou joindre un fichier	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'éclair) et entrez une note de travail. Cliquez sur l'icône pour activer/désactiver le panneau. Vous pouvez également charger un fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Planifier le correctif**.
7. Renseignez les champs de la boîte de dialogue.

Champ	Description
Étape 1 : Sélectionner la cible	
Collection	Choisissez une collection (groupe d'actifs) dans la liste pour continuer. Il s'agit des collections importées de SCCM.
Étape 2 : Planifier	
Nom du déploiement	Entrez un nom pour ce déploiement de correctif. Ce nom vous permet de suivre vos mises à jour.
Type de déploiement	Choisissez une option dans la liste. ○ Requis : ce correctif est une mise à jour requise. ○ Disponible : ce correctif n'est pas obligatoire, mais disponible pour le déploiement.
Heure de date limite	Fixez la date limite. Cette valeur indique le dernier jour d'installation du correctif.
Temps disponible	Définissez la valeur du moment où le correctif devient disponible pour le déploiement.
Temps disponible basé sur	Sélectionnez un fuseau horaire dans la liste sur lequel votre fenêtre de temps de déploiement sera basée.
Autoriser le redémarrage	Désactivé par défaut. Activez (sélectionnez) cette option pour demander aux machines du groupe de redémarrer automatiquement une fois le correctif terminé.
Description	Ajoutez plus de texte pour à propos du correctif. Ces informations sont affichées dans le champ Description de l'enregistrement de mise à jour du correctif.

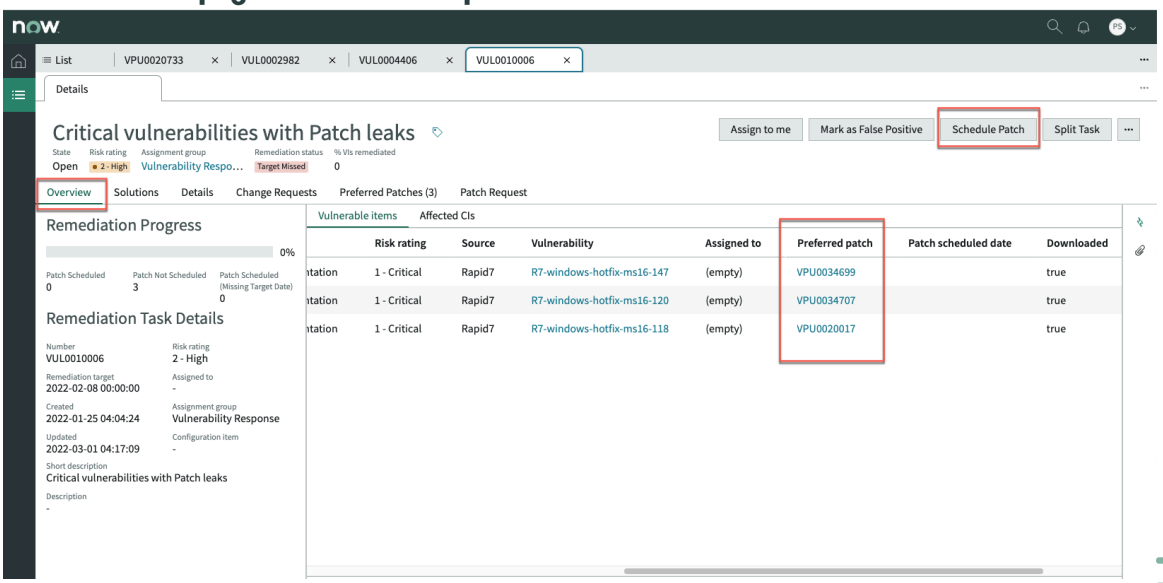
8. Cliquez sur **Déployer**.
   La demande de correctif est envoyée à pour révision. Vous pouvez afficher l'état de toutes vos demandes soumises à partir de **Demandes d'exception** > **Mes demandes** dans la vue de liste.
9. Vous pouvez également planifier des correctifs à partir des tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe.

> **Remarque :** L'option permettant de planifier un correctif à partir d'un enregistrement de tâche de rattrapage n'est disponible que si des correctifs sont mappés aux VI (associés à) dans la tâche. Ces correctifs s'affichent dans la colonne Correctif préféré si vous faites défiler vers la droite d'un enregistrement de tâche de rattrapage avec l'onglet Vue d'ensemble sélectionné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de rattrapage avec correctifs préférés



10. Cliquez sur **Planifier le correctif** dans l'enregistrement RT et suivez les étapes répertoriées ci-dessus pour le planifier dans la boîte de dialogue.

11. **Facultatif :** Vous pouvez planifier des correctifs pour les étapes précédemment dans l'environnement classique.
    Pour localiser ces enregistrements, procédez comme suit.

    a. Dans l'environnement classique, accédez à **Tous** > **Réponse aux vulnérabilités** > **Correctifs** > **Tous**.

    b. Dans la liste qui s'affiche, localisez un enregistrement de mise à jour de correctif.

    c. Pour les tâches de rattrapage, accédez à **Réponse aux vulnérabilités** > **Tâches de remédiation** et localiser un enregistrement.
    Suivez l'état du rattrapage dans l'onglet État du rattrapage. Au bas de l'enregistrement, les données du correctif sont affichées sur les liens connexes.

    d. Cliquez sur **Planifier le correctif** et remplissez les champs.

Champ	Description
Nom du déploiement	Entrez un nom pour ce déploiement de correctif. Ce nom vous permet de suivre vos mises à jour.
Description	Ajoutez plus de texte pour à propos du correctif. Ces informations sont affichées dans le champ Description de l'enregistrement de mise à jour du correctif.
Type de déploiement	Choisissez une option dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ Requis : ce correctif est une mise à jour requise. ▪ Disponible : ce correctif n'est pas obligatoire, mais disponible pour le déploiement.
Collection	Choisissez une collection (groupe d'actifs) dans la liste pour continuer. Ces groupes correspondent aux collections d'actifs importées à partir de SCCM.
Temps disponible basé sur	Sélectionnez un fuseau horaire dans la liste sur lequel votre fenêtre de temps de déploiement sera basée.
Temps disponible	Définissez la valeur du moment où le correctif devient disponible pour le déploiement.
Date limite	Fixez la date limite. Cette valeur indique le dernier jour d'installation du correctif.

e. Cliquez sur **Déployer**.

Messages REST pour l'orchestration Réponse aux vulnérabilités du correctif avec Microsoft SCCM

L'orchestration de correctifs Vulnerability Response avec Microsoft SCCM utilise les classes WMI (Windows Management Instrumentation) SCCM pour effectuer des appels à l'API du serveur SCCM.

Vue d'ensemble des messages REST

Le fournisseur de SMS fournit à l'API un accès d'interopérabilité via HTTPS, appelé service d'administration. Le service d'administration est une API REST (Representational State Transfer) basée sur le protocole Open Data (OData) v4.

Pour plus d'informations sur le service d'administration utilisé avec cette intégration, consultez Qu'est-ce que le service d'administration dans le gestionnaire de configuration .

Étant donné que l'authentification nécessaire utilise le protocole NTLM de Windows New Technology LAN Manager, les appels aux API sont effectués via le serveur MID à l'aide de scripts PowerShell.

Microsoft Intégration SCCM

Vous pouvez utiliser le message REST pour l'intégration Microsoft SCCM afin de récupérer des informations à partir de Microsoft SCCM. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes d'informations adressées à Microsoft SCCM. Les messages REST contiennent les méthodes REST suivantes.

Noms de classes WMI :

- SMS_Collection
- SMS_DeploymentSummary

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
URL	Valeurs dynamiques basées sur l'utilisateur	Indique le point de terminaison de la console SCCM

Microsoft Déployer le correctif SCCM

Vous pouvez utiliser le message REST pour l'intégration de Microsoft SCCM afin de planifier des correctifs de votre ServiceNow AI Platform® vers le Microsoft SCCM. Les modifications apportées à la méthode d'enregistrement du message REST ont un impact sur les demandes d'informations adressées à SCCM. Les messages REST contiennent les méthodes REST suivantes.

Méthode REST	Description
PUBLIER le déploiement du correctif	Programme le correctif sur la console SCCM sur un ou plusieurs ordinateurs.

Nom de paramètre	Valeur	Description
URL	Valeurs dynamiques basées sur l'utilisateur	Indique le point de terminaison de la console SCCM.
Titre	Valeurs dynamiques basées sur l'utilisateur	Titre du déploiement.
settings_tag	Paramètres nommés par balise XML avec valeurs	Indique les paramètres qui ont des paramètres différents et qui sont envoyés à SCCM lors de la planification du correctif.
computer_tag	Balise XML Ordinateurs avec valeurs	Indique la liste des ordinateurs sur lesquels le correctif va être planifié.
site_name	Valeur de la mise à jour du correctif	Nom du site où le correctif est présent.
Patch_id	Valeur de la mise à jour du correctif	ID du correctif.

Transformation des données pour l'orchestration de correctifs avec Microsoft l'intégration SCCM

Les données sont extraites de l'orchestration des correctifs avec Microsoft intégration SCCM, traitées via un ensemble de sources de données et transformées dans votre ServiceNow AI Platform® instance.

Importation de collection SCCM

Les données des collections importées sont chargées dans la table d'importation de collection SCCM [sn_vul_sccm_collection_import]. Les collections SCCM (carte de transformation) sont utilisées pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de la collection SCCM sont traitées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour accéder à cette carte de transformation, accédez à **Tous** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de la collection SCCM. La table suivante répertorie les champs de carte de transformation par intégration.

Champ source	Champ cible	Description
u_collectionid	source_id	ID unique de la collection.
u_name	nom	Nom de la collection.
u_membercount	device_count	Nombre d'appareils dans cette collection.
[script]	integration_instance	Nom de l'instance à partir de laquelle le correctif est importé.

Collection SCCM Importer une carte de transformation Minutage de script

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour mettre à jour les valeurs de la variable de périmètre [sn_vul_sccm]. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Importation de la mise à jour du correctif SCCM

Les données des correctifs importés sont chargées dans la table d'importation de mise à jour de correctif SCCM [sn_vul_sccm_patch_update_import].

La transformation de mise à jour du correctif SCCM est utilisée pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de la mise à jour du correctif SCCM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Tous** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de mise à jour du correctif SCCM.

La table suivante répertorie les champs de carte de transformation par intégration.

Mise à jour du correctif SCCM Importer les champs de carte de transformation

Champ source	Champ cible	Description
[Script]	URL	URL du correctif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise à jour du correctif SCCM Importer les champs de carte de transformation (suite)

Champ source	Champ cible	Description
u_nummissing	num_missing	Nombre d'appareils manquants pour ce correctif.
[Script]	date_release	Date de publication du correctif.
u_bulletinid	bulletin_id	ID du bulletin pour le correctif.
u_numtotal	num_total	Nombre total d'appareils.
u_localizeddescription	description	Description du correctif.
[Script]	is_highest_supersedence	Est le patch avec la plus haute sursance.
u_numnotapplicable	num_not_applicable	Nombre d'appareils non applicables pour ce correctif.
u_iscontentprovisioned	is_downloaded	Si le correctif est téléchargé sur le serveur SCCM.
u_numunknown	num_unknown	Nombre total d'appareils inconnus.
u_articleid	article_id	ID d'article du correctif.
u_localizeddisplayname	Titre	Titre du patch.
u_ci_id	source_id	ID unique du correctif dans SCCM.
u_numpresent	num_present	Nombre d'appareils sur lesquels le correctif est installé.
[Script]	integration_instance	Nom de l'instance à partir de laquelle le correctif est importé.
[Script]	sn_vul_solution	Solution basée sur l'ID source.
[Script]	last_modified	Date de la dernière modification du correctif.
u_severity	source_severity	Gravité du correctif.

Mise à jour du correctif SCCM Importer la carte de transformation Minutage de script

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour mettre à jour les valeurs de la variable de périmètre [sn_vul_sccm]. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation de la mise à jour du correctif de l'appareil SCCM

Les données des correctifs pertinents importés sur les appareils sont chargées dans la table d'importation de mises à jour de correctifs de l'appareil SCCM [sn_vul_sccm_device_patch_import].

La transformation de la mise à jour du correctif de l'appareil SCCM est utilisée pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de la mise à jour des correctifs de l'appareil SCCM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Tous** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de mise à jour du correctif de l'appareil SCCM.

La table suivante répertorie les champs de carte de transformation par intégration.

Mise à jour du correctif de l'appareil SCCM Minutage du script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour créer et mettre à jour des CI en fonction des règles de recherche de CI et des correctifs, ainsi que de la relation entre eux. En fonction des résultats, ce script modifie les valeurs de la variable de périmètre [sn_vul_sccm]. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Importation de la collection des appareils SCCM

Les données des ensembles d'appareils importés sont chargées dans la table d'importation d'ensemble d'appareils SCCM [sn_vul_sccm_device_collection_import].

La transformation d'importation de collection d'appareils SCCM est utilisée pour transformer les informations importées.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de la collection d'appareils SCCM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Tous** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de la collection d'appareils SCCM.

La table suivante répertorie les champs de carte de transformation par intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Collection d'appareils Importer le script de carte de transformation Minutage

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour créer et mettre à jour les CI en fonction des règles de recherche de CI et des collections, ainsi que de la relation entre eux. En fonction des résultats, ce script modifie les valeurs de la variable de périmètre [sn_vul_sccm]. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Collection d'appareils SCCM Importer les champs de carte de transformation

Champ source	Champ cible	Description
u_id	source_id	ID unique d'une action.
U_name	nom	Nom de l'action
[Script]	Sn_vul_sccm_discovered_item	Référence de l'élément détecté sur lequel le correctif est déployé
U_status	état	Statut de l'action
[Script]	Sn_vul_patch_orch_update	Référence du correctif
U_apply_count	Count_success	Nombre de réussites de l'action.
U_retry_count	retry	Nombre de nouvelles tentatives de l'action.
[Script]	Deployment_time	Heure de début de l'action.
[Script]	date limite	Heure de fin de l'action.
[Script]	Source_created	Heure de création de l'action.
[Script]	Integration_instance	Nom de l'instance à partir de laquelle l'action est importée.

Importation du déploiement SCCM

Les données des déploiements importés sont chargées dans la table d'importation de déploiement SCCM [sn_vul_sccm_deployment_import].

La transformation d'importation de déploiement SCCM est utilisée pour transformer les informations importées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données de l'importation de déploiement SCCM sont traitées.

Pour accéder à cette carte de transformation, accédez à **Tous** > **Ensembles de données à importations système** > **Cartes de transformation** et localisez la transformation de déploiement SCCM.

Déploiement SCCM Champs de carte de transformation

Champ source	Champ cible	Description
u_id	source_id	ID unique d'un déploiement.
u_name	nom	Nom du déploiement.
[Script]	date limite	Heure limite du déploiement.
u_numberinprogress	count_progress	Nombre d'appareils en cours pour le déploiement.
[Script]	deployment_time	Heure de début du déploiement.
[Script]	integration_instance	Nom de l'instance à partir de laquelle le déploiement est importé.
[Script]	source_created	Heure de création du déploiement.
[Script]	sn_vul_patch_orch_update	Référence du correctif
[Script]	sn_vul_patch_orch_collection	Référence de l'élément détecté sur lequel le correctif est déployé.
u_softwarename	nom	Nom du déploiement.
u_numberother	count_other	Autre nombre d'appareils pour le déploiement.
u_numberunknown	count_unknown	Nombre d'états inconnu des appareils pour le déploiement.
u_deploymentid	source_id	Identificateur unique du déploiement.
u_numbersuccess	count_success	Nombre d'appareils réussis pour le déploiement.
u_numbererrors	count_error	Nombre d'erreurs d'appareils pour le déploiement.
u_numbertargeted	count_total	Nombre total d'appareils pour le déploiement.

Importation du déploiement SCCM Minutage de script de carte de transformation

Script	Description
OnStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour initialiser les valeurs de la variable de périmètre [sn_vul_sccm] pour le processus d'intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Script utilisé pour mettre à jour les valeurs de la variable de périmètre [sn_vul_sccm].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation du déploiement SCCM Minutage de script de carte de transformation (suite)

Script	Description
	Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Script utilisé pour définir le nombre d'éléments créés, mis à jour et ignorés. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Exemple de workflow pour l'intégration Réponse aux vulnérabilités de Patch Orchestration à Microsoft SCCM

Exemple de fonctionnement de l'orchestration des correctifs avec Microsoft SCCM.

Avant de commencer

Imaginons, par exemple, que l'ensemble de votre environnement soit corrigé une fois toutes les trois semaines. La fenêtre d'application de correctif la plus récente s'est terminée il y a une semaine, mais vous souhaitez appliquer un correctif pour corriger une vulnérabilité critique récemment connue. En raison de la nature critique de cette vulnérabilité, vous ne pouvez pas attendre deux semaines de plus pour le prochain correctif planifié.

Rôles requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour l'espace de travail du gestionnaire de vulnérabilités.
- sn_vul.remediation_owner pour afficher l'espace de travail du propriétaire de rattrapage informatique.
- Rôle sn_vul_patch_orch.configure_patch pour configurer et planifier les correctifs.
- sn_vul_patch_orch.read_patch pour afficher (lecture seule) les informations sur les correctifs dans les enregistrements. Ce rôle est hérité avec les rôles sn_vul.remediation_owner et sn_vuln.vulnerability_analyst requis pour les espaces de travail Rattrapage informatique et Responsable des vulnérabilités.

Pourquoi et quand exécuter cette tâche

En tant que responsable ou analyste des vulnérabilités travaillant dans Vulnerability Manager Workspace, vous pouvez envisager de créer des rubriques de visualisation ou de modifier des rubriques de surveillance existantes pour vous aider à capturer les VI importés présentant des vulnérabilités critiques. Avec l'intégration de l'orchestration des correctifs, vous pouvez également voir les correctifs que vous souhaitez utiliser pour corriger et suivre ces vulnérabilités. Le tableau suivant répertorie quelques exemples avec les conditions que vous pouvez définir pour les rubriques de surveillance pour l'orchestration des correctifs. Utilisez ces exemples pour vous aider à déterminer les paramètres les plus adaptés à votre environnement. Voir Créer une rubrique de surveillance dans le Espace de travail du gestionnaire de vulnérabilités pour plus d'informations sur la configuration de la rubrique de la montre.

Exemples de rubriques de surveillance pour l'orchestration des correctifs dans l'espace de travail du gestionnaire de vulnérabilité

Nom de la rubrique de surveillance	Description
Vulnérabilités critiques avec fuites de correctifs	La cote de risque est 1 : critique ET

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemples de rubriques de surveillance pour l'orchestration des correctifs dans l'espace de travail du gestionnaire de vulnérabilité (suite)

Nom de la rubrique de surveillance	Description
	La raison pour laquelle le correctif n'est pas planifié
Vulnérabilités critiques avec correctifs planifiés (SLA manquant)	Motif : correctif planifié (date cible manquante)
Vulnérabilités critiques avec correctifs planifiés	La cote de risque est 1 : critique ET La date planifiée du correctif n'est pas vide ET Motif pour lequel le correctif est planifié

- En tant que gestionnaire de vulnérabilité ou analyste, après avoir créé les rubriques de surveillance et les efforts de rattrapage, vous générez des tâches de rattrapage. À partir des enregistrements de VI et des tâches de rattrapage, vous pouvez explorer l'onglet Détections et localiser les enregistrements d'éléments détectés qui présentent la vulnérabilité que vous suivez, ainsi que les actifs importés par le produit SCCM.
- En tant qu'analyste ou administrateur de vulnérabilités, vous pouvez surveiller les données des correctifs associées à la vulnérabilité. Vous pouvez également déployer un ou plusieurs correctifs sur un actif spécifique (élément de configuration) à partir d'un enregistrement d'élément détecté.

En tant que spécialiste de la remédiation informatique, vous disposez d'options pour traiter la vulnérabilité avec un déploiement de correctif.

- Vous pouvez planifier le correctif à partir d'un enregistrement de mise à jour de correctif (VPU#).
- Si des solutions préférées sont mappées aux éléments vulnérables (VI) et qu'elles vous sont affectées ou sont affectées à vous ou à vos groupes, vous pouvez planifier les correctifs à partir d'une tâche de rattrapage qui comporte ces éléments vulnérables.

Procédure

1. En tant que spécialiste de la remédiation informatique, dans l'espace de travail de remédiation informatique, cliquez sur la vue Accueil.
2. Dans la vue d'accueil, cliquez sur le tableau de résultats **des tâches de rattrapage affectées** pour afficher les enregistrements.

   Pour les besoins de cet exemple, vous pouvez vérifier le champ Description brève de la tâche de rattrapage (VUL#) pour tout texte relatif à votre vulnérabilité critique. Imaginons, par exemple, que vous sachiez que votre gestionnaire de vulnérabilité a créé une rubrique de surveillance appelée Vulnérabilités critiques avec fuites de correctifs pour attraper les VI (VIT#) avec cette vulnérabilité critique.

   Une fois l'enregistrement ouvert, vous pouvez également examiner les éléments vulnérables et les correctifs préférés, et voir si vous ou un membre de votre groupe avez déjà soumis des demandes de correctifs pour approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Si vous disposez de suffisamment d'informations, vous préférerez peut-être soumettre une demande de correctif maintenant à partir de cette tâche de rattrapage.

   Remarque : Si les éléments vulnérables associés à l'enregistrement ne possèdent pas de correctifs mappés, le bouton **Planifier le correctif** n'est pas disponible sur l'enregistrement.

4. Cliquez sur **Planifier le correctif** et remplissez les champs dans la boîte de dialogue.
   Pour plus d'informations sur la planification d'un patch, reportez-vous à la section Planifier des correctifs avec l'intégration Microsoft SCCM avec Réponse aux vulnérabilités.

5. À partir de la vue de liste de l'espace de travail de remédiation informatique, vous pouvez également cliquer sur les liens Tâches de remédiation, Éléments vulnérables, Solutions et Correctifs pour afficher ces enregistrements.
   Dans le cas de cet exemple, au lieu d'un nom de rubrique de visualisation, vous connaissez peut-être l'ID de l'article ou l'ID du bulletin et le titre du patch. Si tel est le cas, vous voudrez peut-être vérifier si l'un des VI avec cette vulnérabilité vous est affecté ou à vos groupes. À partir des enregistrements de mise à jour de correctifs, vous pouvez soumettre des demandes de correctifs. À partir des enregistrements de VI, vous pouvez rechercher des correctifs potentiels et ouvrir la tâche de rattrapage associée si vous souhaitez soumettre une demande de correctif.

6. Si vous n'avez pas accès aux espaces de travail ou si vous préférez afficher les données et planifier des correctifs à partir de l'environnement classique, procédez comme suit.

   a. Accédez à la **Réponse aux vulnérabilités** > **Correctifs** > **Tous**.

   b. Localisez l'enregistrement de mise à jour de correctif souhaité.
      Vous préférez peut-être filtrer les enregistrements avec des scores de risque critique .

   c. Examinez les champs des VI associés et % des VI rattrapés dans l'onglet État du rattrapage.
      Si les VI disposent de correctifs, le bouton **Planifier le correctif** s'affiche dans le coin supérieur droit de l'enregistrement.

   d. Si vous décidez de soumettre une demande, cliquez sur **Planifier le correctif**.
      Pour plus d'informations sur la planification d'un patch, reportez-vous à la section Planifier des correctifs avec l'intégration Microsoft SCCM avec Réponse aux vulnérabilités.

   e. Vous pouvez également dire que vous ne disposez pas des informations relatives à l'ID du correctif, mais que vous pouvez consulter le champ Description brève des tâches de rattrapage affectées à votre groupe pour tout texte relatif à votre vulnérabilité critique.

   f. Accédez à la **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**.

   g. Recherchez l'enregistrement souhaité et cliquez dessus pour l'ouvrir.
      Dans l'enregistrement ouvert, passez en revue l'onglet État du rattrapage pour les VI et % des VI rattrapés. Cliquez sur les liens connexes pour les enregistrements de VI, les solutions préférées, les correctifs préférés et les demandes de correctifs.

      Remarque : Si les éléments vulnérables associés à l'enregistrement ne possèdent pas de correctifs mappés, le bouton **Planifier le correctif** n'est pas disponible sur l'enregistrement.

   h. Cliquez sur **Planifier un correctif** dans l'enregistrement si vous souhaitez soumettre une demande de correctif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Présentation de Qualys Vulnerability Integration

Les Qualys capteurs du produit collectent les données et les envoient automatiquement à l'application Qualys , qui analyse et corrèle en permanence les informations. Il s'intègre Réponse aux vulnérabilités facilement à la Qualys Vulnerability Integration cartographie des vulnérabilités avec les CI et les services d'entreprise afin de déterminer l'impact et la priorité des menaces potentiellement malveillantes.

Configurer votre Qualys Vulnerability Integration utilisation **Vulnérabilité** > **Administration** > **Assistant de configuration** pour rendre la récupération de données plus flexible et évolutive.

Si vous avez plusieurs déploiements de l'application Qualys Cloud Platform , vous pouvez ajouter une intégration pour chaque déploiement. Les actifs, identifiés par plusieurs déploiements tiers et leurs vulnérabilités, sont consolidés et rapprochés avec votre CMDB. Cette consolidation se produit même lorsque les processus d'analyse se chevauchent entre les multiples déploiements. Les données provenant de chaque déploiement sont identifiées et disponibles dans une instance unique de Réponse aux vulnérabilités. Qualys Vulnerability Integration Les enregistrements de la base de connaissances sont normalisés dans tous les déploiements, ce qui garantit que les instances de la même vulnérabilité dans tous les déploiements sont traitées comme la même vulnérabilité.

Remarque : Vous ne pouvez pas supprimer l'intégration de vulnérabilité d'origine, mais vous pouvez la désactiver. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Remarque : Bien que les créations d'intégrations pour la liste des dispositifs soient créées, le groupe d'actifs Qualys Vulnerability Integration , la liste de recherche dynamique et la liste de recherche statique, elles ne sont pas nécessaires pour un fonctionnement normal.

Versions disponibles

Version de mise en production pour Zurich	Notes de publication
Qualys Vulnerability Integration v12.7, v12.8	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Composants installés

Pour obtenir la liste actuelle des rôles, des tâches d'intégration et des tables installés avec l'intégration, ainsi qu'un lien vers les instructions d'affichage de ce qui est actuellement installé dans votre instance, reportez-vous à la section Composants installés avec le Qualys Vulnerability Integration.

Intégrations principale et de support

Qualys Les intégrations principales et de support enrichissent les données de vulnérabilité de votre instance en récupérant les données de Qualys Vulnerability Integration. Une série

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de travaux planifiés appelle automatiquement les intégrations. Vous pouvez également les exécuter manuellement. Les travaux planifiés simplifient le cycle de vie du rattrapage de la vulnérabilité en maintenant l'instance synchronisée avec d'autres systèmes de gestion de la vulnérabilité. Les intégrations principale et de prise en charge peuvent être modifiées.

Les Qualys intégrations sont exécutées en tant que travaux planifiés. Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Cette valeur ne doit pas être modifiée.

Remarque : Si vous ne définissez pas un utilisateur run-as valide, plusieurs pièces jointes de récupération de données, souvent en double, sont jointes sur les enregistrements de source de données, à chaque fois que l'intégration s'exécute. Plusieurs pièces jointes sur la source de données augmentent le temps de traitement, ce qui entraîne des résultats de transformation incohérents.

Pendant l'importation, les enregistrements CVE, qui ne sont pas déjà présents, sont créés en tant qu'enregistrements NVD et référencés dans des entrées tierces par Qualys défaut.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Intégrations principales

Une intégration primaire est un point d'entrée pour l'interaction avec l'API Qualys Cloud PlatformQualys invoquée dans un calendrier.

Affichez les intégrations primaires en accédant à **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.

Intégrations prises en charge

Une intégration de support est un processus qui n'est pas destiné à s'exécuter selon une planification ni sans invocation par une intégration principale.

Affichez les intégrations prises en charge en accédant à **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations prises en charge**.

Connecteur du graphe de services pour Qualys

À partir de la version 2.2, Connecteur du graphe de services pour Qualys est disponible à partir du ServiceNow® Store. Consultez Connecteur du graphe de services pour Qualys pour plus d'informations.

Les données des champs de source de Qualys données sont importées avec l'API Global Asset et l'API Asset Management and Tagging.

API d'actif global :

- Une licence CSAM est requise.
- Les informations sur les actifs comprennent des détails tels que la catégorie de matériel et la catégorie de système d'exploitation.

API de gestion des actifs et de balisage :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Une licence CSAM n’est pas nécessaire
- Les informations sur les actifs n’incluent pas les détails sur la catégorie de matériel et la catégorie de système d’exploitation.

Pour plus d'informations, voir API Connecteur du graphe de services pour Qualys

.

Créer des CI à l’aide du moteur Identification et réconciliation (IRE)

Vous pouvez utiliser le moteur Identification et réconciliation pour créer de nouveaux CI lorsqu’un CI existant ne peut pas être mis en correspondance avec un hôte importé à partir d’un scanner tiers. Activez le module d’extension Modèles de classe CI CMDB pour créer des CI à l’aide des nouvelles classes, sinon des CI sans correspondance sont créés dans les classes CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l’utilisation du moteur Identification et réconciliation. Pour plus d’informations sur la configuration de la catégorisation des ressources cloud sans correspondance dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

Listes de recherches

Les listes de recherche sont utilisées pour Qualys créer des groupes personnalisés de vulnérabilités. Vous pouvez les enregistrer et les utiliser pour la création de tickets et pour personnaliser les analyses et les rapports de vulnérabilité. Le module Listes de recherches vous permet de télécharger de manière planifiée les données de listes de recherches de Qualys vers votre instance.

Les listes de recherches sont extraites à l’aide des cartes de transformation de données d’importation de Qualysliste de recherches dynamiques et/ou d’importation de liste de recherches statiques . Dans chacune de ces transformations, vous pouvez définir des calendriers pour l’exécution de l’importation.

Profils d'option

Les profils d’option sont disponibles avec Qualys les paramètres d’analyse. Un profil d’option est requis lorsque vous lancez une analyse à partir de votre ServiceNow AI Platform.

Les profils d’option sont importés du produit par l’intégration de la Qualys liste des profils d’option. Vous préférez peut-être exécuter l’intégration de la liste des profils d’options après une importation à partir des intégrations des listes de recherche, de la Qualys liste de recherche dynamique et Qualys des intégrations de la liste de recherches statiques afin de voir quelles listes de recherche sont associées aux profils d’option.

Groupes d'actifs

Les groupes d’actifs sont configurés dans la Qualys plateforme. Les groupes d’actifs identifient les dispositifs de scanner utilisés pour analyser les adresses IP correspondantes lorsqu’une analyse est lancée à partir du ServiceNow AI Platform.

Les groupes de ressources auxquels des dispositifs sont associés sont extraits par l’intégration de la liste des groupes de Qualys ressources.

Lancez l’intégration de la liste des dispositifs après avoir importé des groupes d’actifs pour remplir les champs Nom du dispositif et État du dispositif sur les enregistrements Applications Qualys par défaut de votre ServiceNow AI Platform.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Balises d'hôtes

Toutes les balises d'hôte sont importées dans le cadre de l'intégration de la Qualys liste d'hôtes. Les balises d'hôte sont principalement utilisées pour le filtrage dans les règles de Réponse aux vulnérabilités tâche d'affectation et de rattrapage. Ils s'affichent dans le formulaire Élément détecté.

Remarque : L'intégration Qualys de la liste d'hôtes doit être exécutée avant de créer des règles de tâche d'affectation ou de rattrapage, afin Réponse aux vulnérabilités que toutes les balises puissent être présentes dans les règles et avant que les éléments vulnérables ne soient importés et regroupés.

- Le stockage des balises n'est pas sensible à la casse. Si une balise **San Diego** est créée, une balise **SAN DIEGO** ne peut pas être stockée dans la table des balises d'hôte. 'San Diego' et 'SAN DIEGO' sont considérés comme le même tag d'hôte. Quelle que soit la balise importée en premier, elle gagne.
- L'utilisation de balises d'hôte comme clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises d'hôte sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'hôte sont contrôlées par la propriété système globale **sn_vul.import_host_tags**. Cette propriété est définie sur vrai par défaut. La désactivation des balises les désactive dans toutes les instances.

Les balises d'hôte (également appelées balises d'actif) sont utilisées pour organiser et suivre les actifs de votre organisation. Vous pouvez affecter des balises à vos ressources hôtes. Ensuite, lors du lancement des analyses, vous pouvez sélectionner les balises associées aux hôtes que vous souhaitez analyser. Le module Balises d'hôte vous permet de télécharger de manière planifiée les données de balises d'hôte depuis Qualys votre instance.

Réouverture des éléments vulnérables résolus non fermés par les analyses

Les éléments vulnérables définis sur « Résolu » dans votre ServiceNow AI Platform instance, mais non transitionnés vers « Fermé/Corrigé » par les exécutions d'intégration tierces sont rouverts s'ils sont détectés lors des nouvelles analyses.

En ce Qualys qui concerne les détections, si le scanner continue de trouver des VI qui ont été définis sur « Résolu », mais qui ne sont pas passés à « Fermé/Corrigé » par les analyses suivantes, ces VI repassent à « Ouvert » lorsque la dernière date trouvée est postérieure à la date de résolution.

Limites de la récupération de données

Par défaut, il n'existe aucune restriction sur la façon dont les données sont récupérées à partir de Qualys. De nombreux enregistrements peuvent être liés à des vulnérabilités de faible gravité qu'un client n'est pas disposé à corriger à l'aide de son processus de réponse aux vulnérabilités. La mise à jour des paramètres de message/méthode REST correspondants peut modifier ce comportement.

Le message/la méthode REST responsable de cette mise à jour est **Qualys Host Detection – Standard/POST**. Pour mettre à jour les valeurs, ajoutez un nouveau paramètre de requête HTTP à la méthode POST avec les valeurs suivantes :

- Nom : gravités
- Valeur : 3-5 (ou toute autre sévérité appropriée souhaitée)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Information associée

Qualys Messages REST

Préparation pour le Qualys Vulnerability Integration

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Il est essentiel que vous prépariez l'intégration en effectuant ces procédures. Cela Qualys Vulnerability Integration suppose que vous connaissez et exécutez des analyses Qualys Cloud Platform dans votre environnement.

Remarque : Apportez tous les changements de configuration nécessaires en fonction de vos besoins avant d'exécuter les intégrations.

Prérequis importants

Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service client et assistance.

Utilisez le filtrage pour limiter le nombre d'éléments pour l'importation initiale et échelonnez votre déploiement en ajustant les filtres dans les importations suivantes.

Les Qualys scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Analyser de nouveau** n'est pas disponible.

Mesures à prendre

- Déterminez une date de début initiale pour les intégrations **d'importation de la liste de détection d'hôte** .

  Envisagez de définir le champ **Heure de début** sur quelques heures ou quelques jours dans le passé. Idéalement, choisissez la date de la dernière analyse Qualys. La date de début peut inclure les vulnérabilités détectées avant d'utiliser la solution de gestion de la vulnérabilité. Définissez l'heure de début la plus proche utilisée au début de votre cycle d'analyse. Donc, s'il faut une semaine avant que tous les hôtes ne soient analysés, définissez cette valeur sur une semaine avant cette heure.

- Ajoutez des utilisateurs aux rôles administrateur, sn_vuln.admin et sn_vul_qualys.admin. Pour plus d'informations, consultez Affecter un rôle à un utilisateur .

- Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

- Si vous n'utilisez pas de calculateurs de vulnérabilité, Désactiver le calculateur de vulnérabilité par défaut s'il n'est pas utilisé, en plus de tous les autres que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérable est créé ou mis à jour, et peuvent avoir un impact sur les performances d'importation initiales.

- Lors de l'importation initiale d'enregistrements, certaines règles métier liées aux notifications peuvent entraîner la génération de nombreuses notifications, ce qui a un impact sur les performances. Avant votre importation initiale, désactivez les règles métier.
- Si vous souhaitez utiliser un scanner différent de celui par défaut de Qualys, consultez Configurer les dispositifs de scanner.
- Préparez l'URL du serveur Qualys et les informations d'identification de l'authentification. Les informations d'identification doivent fournir les autorisations adéquates pour récupérer les informations de connaissance, d'analyse et de détection pour un abonnement Qualys.
- Si vous prévoyez d'utiliser des balises d'hôte dans Réponse aux vulnérabilités les règles de tâche d'affectation ou de rattrapage, assurez-vous que l'intégration de la liste d'hôtes Qualys a été exécutée avant de créer des règles.

Installer Qualys Vulnerability Integration

Avant d'exécuter dans Qualys Vulnerability Integration votre instance, vous devez installer et configurer l'application Qualys Vulnerability Integration . Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Rôle requis : admin pour télécharger et installer l'application

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Obtenez les autorisations pour l'application Qualys Vulnerability Integration et téléchargez-la sur votre ServiceNow AI Platform® instance.	Si l'application n'est pas déjà téléchargée sur votre instance, reportez-vous à la section .
Préparez l'intégration.	Consultez Préparation pour le Qualys Vulnerability Integration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.

   Après quelques instants, les applications disponibles pour installation sur votre instance s'affichent.

2. Localisez la Qualys Vulnerability Integration tuile et cliquez sur **Installer**.
3. Suivez les instructions de l'assistant de configuration.
   Pour plus d'informations sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.
4. Accédez à **Configuration de l'intégration>Intégrations des scanners dans l'assistant** de configuration pour poursuivre la configuration.
   Pour plus d'informations sur le complément des invites fournies dans l'Assistant de configuration, reportez-vous à la section Configurer l'utilisation de l'assistant Qualys Vulnerability Integration de configuration.

Que faire ensuite

Activez les scanners, car ils sont inactifs par défaut dans l'application Réponse aux vulnérabilités . Pour plus d'informations sur l'activation des Qualys scanners, reportez-vous à la section Activer les Qualys scanners.

Activer les Qualys scanners

Vous devez activer les scanners après l'installation de car Qualys Vulnerability Integration ils sont désactivés par défaut dans l'application Réponse aux vulnérabilités .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Analyser de nouveau** n'est pas disponible.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Localisez le produit de scanner que vous souhaitez activer et sélectionnez l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher **Activé**.
4. Sélectionnez **Mettre à jour**.
5. Le produit que vous avez activé s'affiche dans le champ **Source** sur un élément vulnérable et des enregistrements de tâche de rattrapage après l'importation suivante, et **Ré-analyser** est disponible en tant qu'action d'interface utilisateur.

Mettre à jour les éléments de configuration avec l'identificateur de partition réseau pour le Qualys Vulnerability Integration

Créez des éléments de configuration (CI) uniques pour les actifs de votre environnement qui partagent des adresses IP. Identifiez les actifs distincts dans votre environnement et mettez automatiquement à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous fournir plus de détails sur vos vulnérabilités.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Par défaut, dans l'application, une façon d'identifier Réponse aux vulnérabilités vos actifs est l'adresse IP. Dans certains cas, les actifs peuvent partager des adresses IP, mais elles sont stockées sous la forme d'un seul CI dans votre CMDB.

Par exemple, comme indiqué dans les tables suivantes, plusieurs actifs (CI) de votre environnement peuvent partager des adresses IP, mais ont des ID de réseau et de référentiel uniques. Toutefois, par défaut, ces actifs sont généralement identifiés et stockés sous la forme d'un seul CI (CI 1) lors de la recherche d'adresse IP.

Recherche d'adresses IP et création de CI par défaut

Source	Adresse IP	NETWORK_ID	Élément de configuration
Qualys Vulnerability Integration: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	Adresse IP	REPOSITORY_ID	Élément de configuration
Qualys Vulnerability Integration: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Vous pouvez créer des CI individuels pour des actifs qui ont la même adresse IP afin de les identifier comme des actifs distincts. À partir d'une importation de données récente, vous pouvez mettre à jour vos CI existants avec plus de granularité qui inclut l'identificateur de partition de réseau [network_partition_identifier] en exécutant la tâche planifiée, *`Update existing discovered items with network partition identifier`*.

Cette tâche planifiée est désactivée par défaut. Activez cette fonctionnalité pour les intégrations Actifs et Vulnérabilités immobilisées et ouvertes dans Qualys Vulnerability Integration l'assistant de configuration afin d'afficher cet identificateur sur vos enregistrements.

Lorsqu'elle est activée, cette tâche planifiée ajoute l'identificateur de partition de réseau [network_partition_identifier] aux enregistrements de CI existants à partir des données importées. Les CI existants créés par l'IRE sont également mis à jour. La tâche planifiée crée également des CI qui incluent l'identificateur de partition de réseau à partir de l'importation suivante. Vous pouvez également lancer la tâche à la demande pour mettre à jour vos données existantes.

À partir des Réponse aux vulnérabilités versions 14.0 et 12.1 de Vulnerability Qualys Vulnerability Integration Integration, les modèles de classe CI CMDB (1.0.21.) sont pris en charge. Les modèles de classes ont l'identificateur de partition de réseau [network_partition_identifier] dans les règles d'identification IRE (Identification et rapprochement).

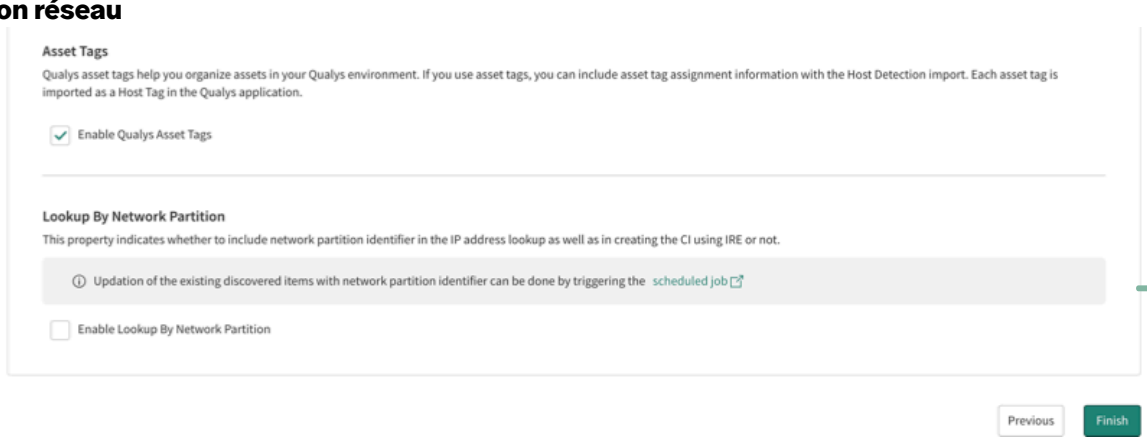
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Exécuter les travaux planifiés sur demande.	Mettez à jour vos éléments détectés existants. Les CI de vos données existantes Qualys Vulnerability Integration sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau. Les éléments détectés, les éléments vulnérables et les enregistrements de détection sont tous mis à jour avec les nouveaux CI.
Attendez les importations de données fraîches à partir des intégrations avec les travaux planifiés suivants.	Créez des CI pour chaque nouvel actif à l'aide de l'identificateur de partition de réseau en commençant par la tâche planifiée suivante. Les enregistrements de CI, d'éléments vulnérables et de détection sont tous mis à jour pour inclure la nouvelle granularité. De nouveaux CI sont créés lorsqu'aucune correspondance exacte n'est trouvée.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
2. Choisissez Qualys Vulnerability Integration.
3. **Modifiez** l'intégration requise.
4. Choisir **Configuration de la détection de l'hôte**.
5. Choisir **Activer la recherche par partition de réseau** case à cocher dans le **Rechercher par partition réseau**



section.

6. Cliquez sur **Terminer**.

Les identificateurs de partition de réseau NETWORK_ID et REPOSITORY _ID inclus dans la recherche d'adresses IP et la création de CI

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
Qualys Vulnerability Integration: intégrations	123.12.12.141	03712	CI 1	CI 1

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
des actifs et des vulnérabilités immobilisées et ouvertes				
	123.12.12.141	03713	CI 1	CI 2

Source	Adresse IP	REPOSITORY_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
Qualys : intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Les règles de recherche d'identification de CI d'adresse IP et d'adresse IP incomplète incluent automatiquement l'attribut d'identificateur de partition de réseau pour une importation de données à partir des intégrations Actifs et Vulnérabilités fixes et ouvertes pour Qualys Vulnerability Integration.

Après avoir activé le travail planifié et enregistré les enregistrements, vous pouvez également mettre à jour vos éléments détectés existants avec des CI qui incluent l'identificateur de partition de réseau en lançant des travaux planifiés à la demande. Les CI de vos enregistrements d'élément détecté, d'élément vulnérable et de détection existants sont automatiquement mis à jour.

Modifications facultatives de Qualys

Configurez les modifications facultatives et rationalisez certaines données spécifiquement pour l'intégration Qualys.

Vous pouvez réinitialiser cette date de début dans l'Assistant de configuration ou à partir de l'intégration principale, ou modifier les règles métier pour les désactiver lors d'une importation initiale.

Désactiver les règles métier liées aux notifications avant l'importation initiale de l'enregistrement

Lors de l'importation initiale d'enregistrements, certaines règles métier liées aux notifications peuvent générer de nombreuses notifications, ce qui a un impact sur les performances. Ces règles métier doivent être modifiées pour les désactiver au cours de l'importation.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la**Tous** > **Définition du système** > **Règles métier**.
2. **Rechercher les notifications de CI affectés**.
3. Ouvrez la règle métier et insérez cette condition : `current.sys_class_name != « sn_vul_vulnerable_item ».`
4. Cliquez sur **Mettre à jour**.
5. Répétez cette procédure pour les règles métier suivantes :
   - Notifications des centres de coûts affectés
   - Notifications des groupes affectés
   - Notifications des emplacements affectés

Remarque : Une fois l'importation de l'enregistrement initial terminée, vous avez la possibilité de réactiver ces règles métier. Cependant, envisagez de les laisser désactivés. Elles peuvent générer un grand nombre de notifications et avoir un impact sur les performances de votre instance.

Activer l'intégration du Qualys score QVS

À l'aide de l'intégration du Qualys score QVS, vous pouvez remplir automatiquement les scores QVS pour CVE afin de vous aider à évaluer le risque de vulnérabilité plus précisément dans le sn_vul_nvd_entry. LIST.

Avant de commencer

Rôle requis : sn_vul_cmn.admin

Procédure

1. Accédez à la **Tous** > **Intégrations de Qualys** > **Intégration du score Qualys QVS**.
2. Cochez la case **Actif** pour activer l'intégration.

Remarque : Cette fonctionnalité est désactivée par défaut.

Résultats

Lorsque l'intégration s'exécute, elle recherche Qualys les derniers scores QVS des CVE mis à jour au cours des 15 derniers jours et renseigne la colonne**Score de vulnérabilité Qualys** dans le [sn_vul_nvd_entry. LIST].

Remarque : Si le score QVS est vide, les CVE n'ont pas été mises à jour au cours des 15 derniers jours.

Modifier une date de début initiale

Lors de l'installation à l'aide de l'Assistant de configuration, vous définissez une date de démarrage initiale pour les intégrations Qualys. Vous pouvez réinitialiser cette date de début dans l'assistant de configuration ou à partir de l'intégration principale, comme indiqué ci-dessous.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
2. Cliquez sur **Intégration de la détection d'hôte Qualys**.
3. Cliquez sur **Détails de l'intégration**.
4. Définissez le champ **Heure de début** sur une valeur dans le passé, de sorte que toutes les vulnérabilités analysées et détectées depuis cette heure soient détectées.

   Si vous avez configuré Qualys à l'aide de l'Assistant de configuration, le champ **Heure de début** est prérempli, initialement jusqu'à trois mois avant la date d'aujourd'hui, puis jusqu'à la date d'aujourd'hui.

   Remarque : Envisagez de définir la valeur sur un mois maximum dans le passé. Cela empêche une grande quantité de données de dépasser les limites de débit de l'API Qualys et de déclencher des délais d'exécution.

5. Cliquez sur **Envoyer** ou **Mettre à jour**.
6. **Facultatif :** Cliquez sur **Exécuter maintenant** pour l'exécuter immédiatement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurations et modifications avancées Qualys

Configurez des modifications facultatives avancées et rationalisez certaines des données spécifiquement pour l'intégration Qualys . La plupart de ces modifications nécessitent un codage ou une expertise avancée ServiceNowQualys Cloud Platform .

Pour plus de conseils sur Qualys les importations, consultez l'article de la base de connaissances Conseils de réglage des performances pour les tâches d'importation Qualys dans la base de connaissances HI.

Modifier les valeurs de mappage de priorité et d'état de Qualys vers ServiceNow

Modifiez les valeurs de mappage pour la priorité et l'état de vos besoins.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Il s'agit d'une option de personnalisation avancée.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Règles métier**.
2. Recherchez **les valeurs de carte Qualys** et ouvrez-la.
3. Cliquez sur l'onglet **Avancé** .
4. Modifiez selon vos besoins.
   Les modifications les plus courantes incluent l'ajout de nouvelles valeurs d'état ou la révision de la criticité ou de la priorité.
5. Cliquez sur **Mettre à jour**.

Restreindre la possibilité d'écrire dans un enregistrement en fonction d'un groupe d'affectation

Vous pouvez restreindre les droits d'écriture/de lecture sur les enregistrements en fonction de l'appartenance à un groupe affecté. Modifiez les conditions et le script en fonction des besoins spécifiques.

Avant de commencer

Rôle requis : security_admin (rôle élevé de l'administrateur)

Remarque : Cette action est effectuée dans le périmètre de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Contrôle d'accès (ACL)**.
2. Recherchez les ACL qui commencent par sn_vul.
3. Choisissez un enregistrement de contrôle d'accès, par exemple, sn_vul_vulnerable_item, **Opération écriture**.
4. Cochez la case **Avancé** de l'enregistrement, si nécessaire, pour afficher les entrées **de rôle** .
5. Modifiez le script du **rôle** en fonction de vos besoins.
   Exemple de modification de l'accès par groupe.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Cliquez sur **Mettre à jour**.

Configurer les dispositifs de scanner

Si vous lancez des analyses à partir de votre ServiceNow AI Platform® et non directement à partir de Qualys, vous pouvez configurer des analyses pour les plages d'adresses IP.

Avant de commencer

Les données proviennent de l'intégration basée sur Qualys les groupes d'actifs Qualys et leurs dispositifs par défaut connexes (scanners).

Si aucun dispositif n'est configuré pour les plages d'adresses IP ciblées, le dispositif défini par défaut pour l'instance d'intégration est utilisé pour l'analyse.

Rôle requis : sn_vul_qualys.admin

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Dispositifs de scanner**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom du dispositif	Vous êtes invité à remplir ce champ lorsque vous créez un enregistrement manuellement. Entrez le nom du Qualys dispositif de scanner à utiliser pour invoquer des analyses afin de faire correspondre les éléments de configuration. Utilisez la valeur Externe lorsque vous souhaitez lancer l'analyse avec un scanner externe.
ID du dispositif	Entrez l'identificateur Qualys du dispositif de scanner à utiliser pour appeler des analyses afin de faire correspondre les éléments de configuration. Vous êtes invité à remplir ce champ lorsque vous créez un enregistrement manuellement. Utilisez la valeur 0 lorsque vous souhaitez lancer l'analyse avec un scanner externe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
États des dispositifs	Affiche le dernier état du dispositif de scanner sur les données retournées par l'intégration Qualys . Pour les enregistrements créés manuellement, l'état n'est mis à jour que si un **ID de dispositif** valide est spécifié.
ID du groupe de ressources	Affiche l'identificateur du groupe de Qualys ressources qui a créé cet enregistrement. Ce champ affiche une valeur uniquement pour les enregistrements créés par l'intégration Qualys .
Nom du groupe de ressources	Affiche le nom du groupe de Qualys ressources qui a créé cet enregistrement. Ce champ affiche une valeur uniquement pour les enregistrements créés par l'intégration Qualys .
Ordre	Entrez une valeur à utiliser pour déterminer la priorité d'analyse. Pour les dispositifs dont les critères sont contradictoires, la priorité est accordée à un dispositif dont la valeur d'ordre est inférieure.
Créé manuellement	Indique si cet enregistrement a été créé manuellement par l'utilisateur.
Utiliser un groupe de filtres	Cochez cette case pour spécifier un groupe de filtres afin de trouver des éléments de configuration correspondants pour l'analyse.
Groupe de filtres	Sélectionnez le groupe de filtres que vous souhaitez utiliser pour trouver des éléments de configuration correspondants pour l'analyse. Ce champ s'affiche uniquement si vous avez sélectionné **Utiliser un groupe de filtres**.
IP	Liste séparée par des virgules d'adresses IP ou de plages d'adresses IP que cette appliance doit utiliser lors de l'appel d'analyses.
Instance d'intégration	Instance Qualys d'intégration associée à ce dispositif.
Profil d'option	Sélectionnez le profil d'option que vous souhaitez utiliser pour les analyses afin de faire correspondre les éléments de configuration.

3. Cliquez sur **Mettre à jour**.

Configurer et gérer Qualys les scanners et analyses de vulnérabilité

Qualys Des analyses de vulnérabilité peuvent être effectuées pour détecter les vulnérabilités logicielles qui affectent vos CI. Vous pouvez lancer des analyses à partir d'un enregistrement d'élément vulnérable ou en créant un enregistrement d'analyse directement pour les éléments de configuration (CI) et les adresses IP.

Si vous analysez Qualys les éléments vulnérables directement à partir de l'écran des éléments vulnérables, vous avez également la possibilité d'analyser plusieurs éléments vulnérables en même temps.

Si Réponse aux incidents de sécurité cette option est activée, vous pouvez également lancer une analyse à partir du catalogue des incidents de sécurité, d'un enregistrement d'incident de sécurité ou d'une demande d'analyse de sécurité.

Les analyses soumises à partir d'éléments vulnérables, d'incidents Catalogue des incidents de sécurité de sécurité ou de demandes d'analyse Qualys de sécurité sont effectuées par l'analyseur par défautQualys.

Vous pouvez sélectionner le profil d'option que vous souhaitez utiliser pour les analyses afin de faire correspondre les éléments de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les profils d'option contiennent Qualys des paramètres d'analyse.
- Un profil d'option est requis lorsque vous lancez une Qualys analyse à partir de votre ServiceNow AI Platform®.

Configurer l'analyse IP initiée par Qualys ServiceNow

Le Qualys scanner inclus avec le système de base fournit une intégration de base de référence pour lancer des analyses basées sur les adresses IP.

Avant de commencer
Vous pouvez sélectionner le profil d'option que vous souhaitez utiliser pour les analyses afin de faire correspondre les éléments de configuration.

- Les profils d'option contiennent Qualys des paramètres d'analyse.
- Un profil d'option est requis lorsque vous lancez une analyse Qualys à partir de votre ServiceNow AI Platform®.

Rôle requis : sn_vul_qualys.admin

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Ouvrez l'enregistrement Qualys .
3. Cochez les cases**Actif** et **Par défaut** .

   Sélectionner **Actif** est nécessaire pour utiliser le Qualys scanner afin d'analyser Qualys automatiquement les VI. Vous n'avez pas non plus besoin de sélectionner **Par défaut** pour qu'il s'exécute automatiquement.

   Avant la version 12.0, **Actif** est requis pour utiliser le scanner. Si Par **défaut** est également sélectionné, le scanner est automatiquement utilisé sans avoir à être sélectionné pendant la numérisation.
4. Pour le champ Intégration source, cliquez sur l'icône de recherche et sélectionnez l'option **pour Qualys**, par exemple, **Qualys Cloud Platform**.
5. Cliquez sur **Mettre à jour**.
6. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
7. Ouvrez **l'intégration de la liste des groupes de ressources Qualys**.
   a. Sélectionnez la case à cocher **Activé**.
   b. Cliquez sur **Exécuter maintenant**.
8. Suivez ces étapes pour remplir vos dispositifs de scanner.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous préférez peut-être exécuter l'intégration de la liste des profils d'options après une importation à partir des intégrations des listes de recherche, de la liste de recherches dynamiques Qualys et des intégrations de listes de recherches statiques Qualys, afin de voir quelles listes de recherches sont associées aux profils d'options.

a. Ouvrez l'intégration de la **liste des profils des options Qualys**.

b. Sélectionnez la case à cocher **Activé**.

c. Cliquez sur **Exécuter maintenant**.

d. Suivez les étapes répertoriées dans Configurer les dispositifs de scanner pour configurer vos dispositifs de scanner.
Revenez ici une fois ces étapes terminées pour poursuivre la configuration.

e. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.

f. Ouvrez **l'intégration de la liste des dispositifs Qualys**.

g. Sélectionnez la case à cocher **Activé**.

h. Cliquez sur **Exécuter maintenant**.
Vos Qualys dispositifs de scanner sont maintenant correctement renseignés.

Information associée

Présentation de Qualys Vulnerability Integration

Analyser plusieurs Qualys vulnérabilités ou éléments vulnérables

Vous pouvez analyser simultanément plusieurs Qualys vulnérabilités ou éléments vulnérables qui contiennent au moins un élément de configuration (CI) affecté ou une adresse IP renseignée sur le formulaire.

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Effectuez l'une des actions suivantes :
   - Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
   - Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tous les éléments vulnérables**.
2. Cochez les cases en regard des enregistrements que vous souhaitez analyser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur la liste **Actions sur les lignes sélectionnées** , puis cliquez sur **Analyser à nouveau pour rechercher les éléments vulnérables**.
   Un message s'affiche avec un lien vers l'analyse et les notes de travail sont mises à jour.
4. Cliquez sur le lien pour afficher la progression ou les résultats de l'analyse.

Configurer l'analyse Qualys automatique pour les tâches de rattrapage résolues

Vous pouvez planifier l'analyse qui s'exécute automatiquement pour mettre à jour vos Qualys éléments vulnérables.

Avant de commencer
Une fois qu'une tâche de rattrapage est passée à **l'état Résolu**, une analyse est lancée automatiquement pour mettre à jour l'état des éléments vulnérables associés.

- L'analyse est désactivée par défaut.
- Activez l'analyse avec le paramètre **d'instance** d'intégration scan_on_resolved dans l'enregistrement **Qualys** situé à **Tous** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration** > **Qualys**. Pour plus d'informations, reportez-vous aux étapes suivantes.
- Cette analyse est spécifique à l'instance. Si vous avez plusieurs instances et que vous souhaitez activer ou désactiver cette analyse, vous devez désactiver le paramètre **scan_on_resolved** dans l'instance d'intégration Paramètres de chaque instance que vous souhaitez modifier.
- Lorsque l'analyse est activée, vous pouvez la lancer à la demande ou vous pouvez la programmer pour qu'elle s'exécute uniquement dans une fenêtre de temps spécifiée. Reportez-vous à la section Configurer Qualys les nouvelles analyses pour qu'elles s'exécutent uniquement dans les intervalles planifiés Comment définir les heures de début et de fin de la fenêtre horaire.

Rôle requis : sn_vul_qualys.admin

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Instances d'intégration**.
2. Sélectionnez **Qualys** pour ouvrir l'enregistrement.
   Les paramètres d'instance d'intégration de Qualys sont affichés dans un onglet.
3. Pour activer l'analyse automatique, localisez le *`scan_on_resolved`* paramètre.
4. Dans la colonne Valeur de la propriété, saisissez `vrai`.
5. Cliquez sur **Mettre à jour**.

Configurer Qualys les nouvelles analyses pour qu'elles s'exécutent uniquement dans les intervalles planifiés

Pour l'intégration Qualys de vulnérabilité, définissez les paramètres d'heure de début et de fin de l'analyse afin que les nouvelles analyses s'exécutent, ou ne soient disponibles, que pendant les heures souhaitées.

Avant de commencer
Cette configuration s'applique à la fois aux nouvelles analyses planifiées et aux nouvelles analyses que vous lancez manuellement dans le Qualys produit à partir de votre ServiceNow AI Platform® instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La définition des paramètres d'heure de début et de fin de l'analyse pour les instances d'intégration vous permet de spécifier des fenêtres de temps lorsque de nouvelles analyses dans le Qualys produit sont disponibles. Par exemple, vous préférerez peut-être spécifier que les nouvelles analyses ne sont disponibles que pendant les heures creuses, par exemple, de minuit à 10 heures.

Ce paramètre est spécifique à l'instance. Si vous avez plusieurs instances, vous devez configurer les valeurs scan_start_time et scan_end_time dans les paramètres d'instance d'intégration de chaque instance que vous souhaitez modifier.

Rôle requis : sn_vul_qualys.admin

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration** > **Qualys**.
2. Cliquez sur **Qualys** pour ouvrir l'enregistrement.
   Les paramètres d'instance d'intégration s'affichent Qualys .
3. Pour le paramètre scan_start_time, dans la colonne Valeur, entrez l'heure dans le fuseau horaire UTC au format 24 heures (00:00 à 24:00) pour l'heure de début de la fenêtre dans laquelle vous souhaitez que les nouvelles analyses soient disponibles.
4. Pour la scan_end_time, dans la colonne Valeur, entrez les heures au même format (00:00 à 24:00) pour l'heure de fin de la fenêtre disponible.
   Par exemple, si vous entrez une heure de début de 00:00 pour le paramètre scan_start_time et une scan_end_time de 10:00 le matin même, les analyses planifiées ou lancées manuellement en dehors de la fenêtre horaire de minuit à 10 heures sont mises en file d'attente et lancées à l'heure de début de la fenêtre horaire du jour suivant, 00:00.

   Dans le même exemple, si un propriétaire de rattrapage lance manuellement une nouvelle analyse à 11h00, la nouvelle analyse n'est pas immédiatement lancée, car elle se trouve en dehors des heures d'analyse configurées disponibles. La demande d'analyse reste en file d'attente jusqu'au début de la fenêtre horaire du jour suivant, dans cet exemple (00:00).
5. Cliquez sur **Mettre à jour** pour enregistrer vos paramètres.

Qualys Limites des taux d'analyse de vulnérabilité

Vous pouvez définir la fréquence à laquelle différents types d'analyses sont effectués pour limiter le nombre de demandes envoyées à un scanner externe. Une fois que vous avez défini des limites de débit, vous pouvez les appliquer aux Qualys scanners.

Définir les Qualys limites de taux d'analyse

Vous pouvez définir le taux auquel différents types d'analyses sont effectués pour équilibrer la charge dans votre file d'attente d'analyse. Les conditions définies dans la limite des taux déterminent si les limites des taux sont appliquées aux entrées mises en file d'attente.

Avant de commencer

Rôle requis : sn_vul.admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Définitions de limite d'évaluation**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définition de limite de taux

Champ	Description
Nom	Fournissez un nom descriptif qui identifie les conditions que l'entrée de file d'attente doit remplir. Par exemple, analyses par minute
Conditions de la file d'attente	Entrez les conditions utilisées pour déterminer si une entrée d'analyse en file d'attente est soumise à cette limite de taux. Les conditions ne doivent pas être spécifiques à un scanner particulier.
Script d'évaluation	Écrivez un script avec la logique pour évaluer l'entrée en file d'attente. Il est important que le script retourne vrai/faux pour définir si l'entrée est traitée. Basez également le script d'évaluation sur l'entrée en file d'attente évaluée.

4. Cliquez sur **Envoyer**.

Appliquer des limites de taux d'analyse aux Qualys scanners

Après avoir défini des limites de taux d'analyse à l'aide de définitions de **limites de taux**, vous pouvez appliquer des limites de taux à des scanners spécifiques Qualys .

Avant de commencer

Rôle requis : sn.vul_admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Limites de taux des scanners**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Limite de taux du scanner

Champ	Description
Scanner	Sélectionnez le scanner auquel vous souhaitez appliquer une limite de taux.
Limite du taux	Sélectionnez la limite de débit que vous souhaitez appliquer à ce scanner.
Seuil	Entrez le seuil auquel vous souhaitez soumettre le scanner sélectionné pour la limite de taux sélectionnée. Par exemple, si le scanner autorise 4 balayages par minute et que la limite de débit est définie comme requêtes par minute, le seuil sera 4.

4. Cliquez sur **Envoyer**.

Afficher la file d'attente de l'analyse de vulnérabilité Qualys

Les demandes d'analyse de vulnérabilité soumises à l'intégration de l'analyse des vulnérabilités sont mises en Qualys file d'attente afin de ne pas surcharger les ressources système. Vous pouvez afficher l'état des demandes mises en file d'attente, selon vos besoins.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Dans la liste des analyses en file d'attente, chaque analyse comprend un nom d'analyse généré automatiquement qui identifie le CI qui a été analysé.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **File d'attente de l'analyse**.
   Toutes les Qualys demandes d'analyse qui ont été soumises sont affichées dans une liste. La colonne **État** affiche l'état actuel de chaque entrée mise en file d'attente. Un état **Terminé** indique que l'analyse a quitté la file d'attente. Cela n'indique pas nécessairement que le traitement de l'analyse est terminé. Lorsque les analyses sont terminées ou en cas d'échec, la colonne **Traitement** affiche le texte des notes de travail approprié.

   Remarque : Si une valeur de hachage a été soumise pour analyse et que le scanner ne parvient pas à trouver un résultat, **l'état** indique **Terminé** et la note de travail dans la colonne **Traitement** indique **Inconnu**.

2. Une fois le traitement d'une analyse terminé, cliquez sur un enregistrement en file d'attente pour afficher les détails de la demande d'analyse.

Activer le filtre du système de base pour les importations de détection confirmées

Activez un filtre par défaut à l'aide des paramètres d'intégration pour importer uniquement les détections confirmées à partir de Qualys Cloud Platform.

Avant de commencer

Rôle requis : sn_vul_qualys.admin, sn_vul.vr_import_admin

Pourquoi et quand exécuter cette tâche

Un paramètre d'instance d'intégration système de base « include_only_confirmed » est disponible pour importer une liste filtrée de détections à partir de .Qualys Cloud Platform Par défaut, ce paramètre est défini sur *FAUX* et toutes les détections, qu'elles soient potentielles, confirmées ou informatives, sont importées.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Instances d'intégration**.
2. Ouvrez Qualys Cloud Platform Integration à partir de la liste Instances d'intégration.
3. Dans la liste Paramètres de l'instance d'intégration, ouvrez le paramètre '*include_only_confirmed*'.
4. Mettez à jour la valeur par défaut sur *Vrai*.
5. Cliquez sur **Mettre à jour**.
   Vous avez activé le filtre pour importer les détections confirmées à partir de l'intégration Qualys Cloud Platform .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Par défaut, seules les détections confirmées de l'intégration Qualys Cloud Platform sont importées lors de l'exécution de la prochaine importation de vulnérabilité Qualys. Toutes les autres détections, notamment informatives et potentielles, sont ignorées et ne sont pas importées. Pour plus d'informations, consultez Afficher les données de détection d'éléments vulnérables de Vulnerability Response.

Lancer une nouvelle analyse pour le Qualys Vulnerability Integration

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans le Qualys produit à partir de votre ServiceNow AI Platform commande à la demande.

Avant de commencer
Vous pouvez lancer de nouvelles analyses à partir des espaces de travail Réponse aux vulnérabilités. Pour plus d'informations, consultez Analyser de nouveau les enregistrements et les tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT.

Pour les nouvelles analyses dans l'environnement classique, consultez les sections suivantes pour savoir comment lancer de nouvelles analyses.

Configuration requise pour les nouvelles analyses dans le Qualys produit initiées à partir de votre ServiceNow AI Platform:

Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Qualys produit à partir de votre ServiceNow AI Platform® instance.

Pour réduire les frais généraux et le volume liés aux analyses complètes planifiées, les propriétaires de rattrapages, les spécialistes informatiques, les analystes de vulnérabilité ou les gestionnaires de vulnérabilité peuvent lancer de nouvelles analyses ciblées à la demande pour détecter des vulnérabilités spécifiques sur les actifs (éléments de configuration) de leurs environnements. Vous pouvez lancer de nouvelles analyses dans le produit à partir d'enregistrements Qualys d'élément vulnérable (VI), de tâches de rattrapage (RT), d'entrée tierce (TPE) ou d'éléments découverts à partir de votre ServiceNow AI Platform instance.

Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, correctifs et autres actions ont correctement corrigé des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Cas d'utilisation:

Par exemple, supposons que l'ensemble de votre environnement soit analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été terminée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines pour la prochaine analyse planifiée afin de vérifier qu'elle a été corrigée. Pour vérifier que votre correctif a corrigé avec succès une vulnérabilité critique découverte lors d'une analyse précédente, vous pouvez lancer une nouvelle analyse ciblée à partir de votre ServiceNow AI Platform pour rechercher Qualys les éléments vulnérables.

Vous pouvez lancer de nouvelles analyses pour les VI qui ont Qualys comme source des états autres que Fermé. Consultez Analyser de nouveau les enregistrements et les tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT.

Vérifiez que vous avez effectué la configuration suivante requise pour les nouvelles analyses. Pour en savoir plus, consultez les étapes commençant par la section Configurer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

et gérer Qualys les scanners et analyses de vulnérabilité répertoriées dans les sections précédentes.

Rôle requis : sn_vul_manually_initiate_rescan

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Vous ne pouvez lancer de nouvelles analyses que pour les VI ayant Qualys comme source. Vérifier Qualys s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le générateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue de liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône**Personnaliser la liste** (icône Engrenage) et utilisez la zone de liste double pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**, **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers**ou aux **éléments détectés** pour la tâche de rattrapage, l'entrée tierce ou les enregistrements d'éléments détectés, respectivement, que vous souhaitez utiliser pour la nouvelle analyse.

   Selon votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

   - Sur un enregistrement de VI unique, l'élément vulnérable doit provenir du Qualys produit et se trouver dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent avoir Qualys comme source et dans un état autre que **Fermé**.
   - Sur un enregistrement RT, la tâche de rattrapage peut être dans n'importe quel état autre que **Fermé**, et tous les VI associés doivent avoir Qualys comme source.
   - Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé dans un état autre que **Fermé** avec Qualys comme source.
   - Sur un enregistrement d'élément détecté, l'élément de configuration a au moins un VI associé comme Qualys source dans un état autre que **Fermé**.

4. Dans l'angle supérieur droit de l'enregistrement que vous avez choisi, cliquez sur **Analyser à nouveau**. Dans la boîte de dialogue qui s'affiche, choisissez-en une pour continuer.

Option	Description
Cochez la case **Spécifier les profils d'option** .	Dans la liste, choisissez le profil d'option du Qualys scanner que vous souhaitez utiliser pour la nouvelle numérisation. Il s'agit des appliances (scanners) que vous avez configurées et répertoriées dans **Intégration de vulnérabilité Qualys** > **Dispositifs de scanner**.
Décochez la case **Spécifier les profils d'option** (non cochée).	Le Qualys profil d'option du scanner que vous avez défini comme scanner par défaut dans la liste Dispositifs de scanner est utilisé pour l'analyse. Pour plus d'informations sur la configuration des scanners par défaut que vous lancez à partir de votre ServiceNow AI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Platform, Configurez les dispositifs de scanner répertoriés dans la section précédente pour plus d'informations.

5. Cliquez sur **Demander une analyse**.

   Un message s'affiche pour indiquer que votre analyse est en cours de traitement. L'état de toutes les nouvelles analyses peut être trouvé à tout moment dans les listes associées à l'analyse sur les enregistrements VI, RT, TPE et d'éléments découverts que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

   Votre instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée.

   Une fois la nouvelle analyse terminée, l'intégration de la détection d'hôte Qualys est automatiquement lancée pour mettre à jour vos éléments vulnérables. En fonction du nombre d'éléments vulnérables dont vous disposez, vos détections, éléments vulnérables et éléments de tâche sont mis à jour après l'achèvement de l'analyse de l'intégration de détection Qualys d'hôte. Accédez à ces enregistrements pour afficher les mises à jour une fois l'intégration de la détection d'hôte terminée.

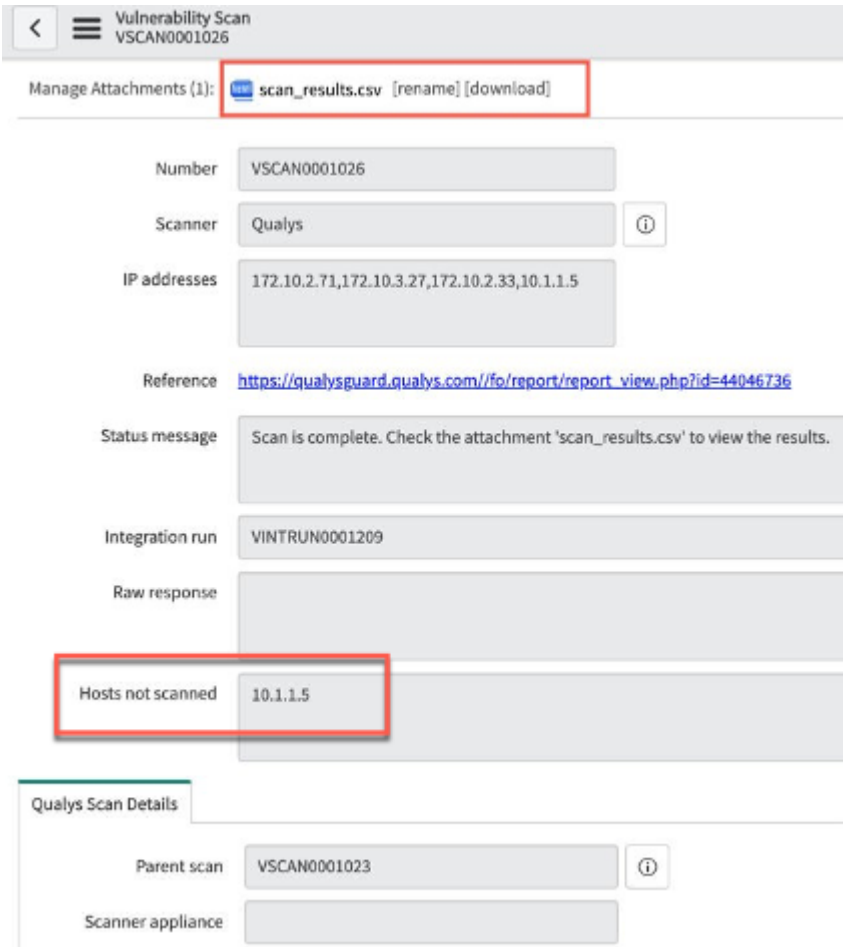
   Cette analyse est spécifique à l'instance et peut être désactivée. Pour en savoir plus sur les Qualys intégrations et sur leur présentation, reportez-vous à la section Présentation de Qualys Vulnerability Integration.

Que faire ensuite

Vous pouvez afficher une pièce jointe .csv sur l'enregistrement de numérisation pour voir les détails des nouvelles analyses.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Comme le montre l'image précédente, lors de la nouvelle analyse, si les hôtes (éléments de configuration) de votre environnement ne sont pas accessibles, les détections et les éléments vulnérables associés à ces actifs ne sont pas mis à jour lorsque la nouvelle analyse est terminée. Pour vous aider à comprendre pourquoi ils ne sont pas inclus, une fois la nouvelle analyse terminée, les adresses IP des actifs de ces CI sont répertoriées dans les enregistrements de vulnérabilité dans le champ Hôtes non analysés.

Qualys Métadonnées pour les vulnérabilités

L'intégration Qualys de la détection d'hôte est améliorée pour inclure d'autres champs à partir de Qualys. Ces champs aident à filtrer les vulnérabilités non exploitables Linux . Cette amélioration améliore l'intégration au niveau de la détection et au niveau de l'élément vulnérable (EV).

Importer des métadonnées supplémentaires à partir de Qualys

Importez des métadonnées supplémentaires pour les éléments de vulnérabilité (VI) afin de filtrer les vulnérabilités en fonction de l'impact sur un noyau ou un service.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.
2. Sous Configuration de l'intégration, cliquez sur **Intégrations de scanners**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sous Application installée, cliquez sur **Modifier** pour l'application Qualys .
4. Cliquez sur **Configuration de la détection d'hôte**.
5. Accédez à la **Importer des métadonnées supplémentaires pour les détections**.
6. Pour importer des métadonnées supplémentaires à partir de Qualys, cochez manuellement l'une des cases suivantes dont vous avez besoin.
   - **Métadonnées du noyau** : identifie les vulnérabilités trouvées sur les noyaux Linux en cours d'exécution ou non.

     Si la valeur des métadonnées renvoyées est **Non**, cela signifie que la vulnérabilité n'est pas exploitable en raison d'un noyau non exécuté. Pour plus d'informations sur les valeurs récupérées, reportez-vous à la section Qualys Valeurs de métadonnées pour les vulnérabilités.
   - **Métadonnées de service** : identifie les vulnérabilités trouvées sur les ports ou services en cours d'exécution ou non.
   - **Métadonnées de configuration exploitables** : identifie les vulnérabilités qui peuvent être exploitables ou non en raison de la configuration actuelle de l'hôte.

   Remarque : Par défaut, ces cases ne sont pas cochées.
7. Exécutez l'intégration de détection d'hôte Qualys avec une date de rétroactivité.
   Pour plus d'informations sur la définition de la date de début, reportez-vous à la section Modifications facultatives de Qualys.

Résultats
Les métadonnées ont été importées.

Que faire ensuite
Pour afficher les métadonnées importées, saisissez `sn_vul_detection.list` dans la navigation de filtre. La liste des détections d'éléments vulnérables s'affiche. Pour plus d'informations sur les valeurs affichées dans les colonnes nouvellement ajoutées, reportez-vous à .Qualys Valeurs de métadonnées pour les vulnérabilités

Qualys Valeurs de métadonnées pour les vulnérabilités

Lorsque les métadonnées de noyau, les métadonnées de service et les métadonnées de configuration sont importées, certaines valeurs sont également récupérées. Les valeurs **0**, **1** et **Non disponible** sont traitées dans le back-end et converties respectivement en **Non**, **Oui** et **Vide** .

Ces valeurs sont renseignées dans les colonnes suivantes de la liste Éléments de vulnérabilité détectés et Éléments de vulnérabilité :

- Affecte l'exécution de la colonne de service
- Affecte la colonne de configuration exploitable
- Affecte l'exécution des colonnes du noyau

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Ces colonnes ne sont pas visibles par défaut. Pour en savoir plus sur la configuration de la mise en page du formulaire, voir Configurer la mise en page du formulaire
- Pour les détections plus anciennes, les valeurs de ces colonnes peuvent être vides. Pour mettre à jour les données, exécutez une intégration de détection d'hôte Qualys antidatée. Pour plus d'informations sur la définition de la date de début, reportez-vous à la section Modifications facultatives de Qualys.

Le tableau suivant indique les valeurs récupérées et leur importance.

Valeurs de champ récupérées et leur signification

Champ	Valeur	Importance
AFFECT_RUNNING_KERNEL	0	La vulnérabilité se trouve sur un noyau qui n'est pas en cours d'exécution. La vulnérabilité n'est pas exploitable.
AFFECT_RUNNING_KERNEL	1	La vulnérabilité se trouve sur un noyau en cours d'exécution. La vulnérabilité est exploitable.
AFFECT_RUNNING_KERNEL	Non disponible	La vulnérabilité n'est pas une vulnérabilité liée au noyau.
AFFECT_RUNNING_SERVICE	1	La vulnérabilité se trouve sur les ports ou les services non exécutés. La vulnérabilité n'est pas exploitable.
AFFECT_RUNNING_SERVICE	0	La vulnérabilité se trouve sur les ports ou les services en cours d'exécution. La vulnérabilité est exploitable.
AFFECT_RUNNING_SERVICE	Non disponible	La vulnérabilité n'est pas une vulnérabilité connexe.
AFFECT_EXPLOITABLE_CONFIG	1	La vulnérabilité n'est pas exploitable en raison de la configuration de l'hôte.
AFFECT_EXPLOITABLE_CONFIG	0	La vulnérabilité est exploitable en raison de la configuration de l'hôte.
AFFECT_EXPLOITABLE_CONFIG	Non disponible	La vulnérabilité n'est pas une vulnérabilité connexe.

Traduction automatique

Définir des paramètres de filtre supplémentaires pour Qualys les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec Qualys Vulnerability Integration le pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec les intégrations prises en charge Qualys .

Avant de commencer

Cas d'utilisation : en tant que responsable ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que des détails spécifiques de la vulnérabilité. Par exemple, supposons que vous souhaitiez afficher les vulnérabilités importées qui sont filtrées par des adresses IP ou des plages d'adresses IP spécifiques. Vous souhaitez également importer uniquement les machines qui sont dans votre champ d'application, par exemple, uniquement les machines de votre réseau d'entreprise qui ne sont pas des périphériques externes.

Pour vous aider à collecter ces données, vous pouvez ajouter Qualys des paramètres pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

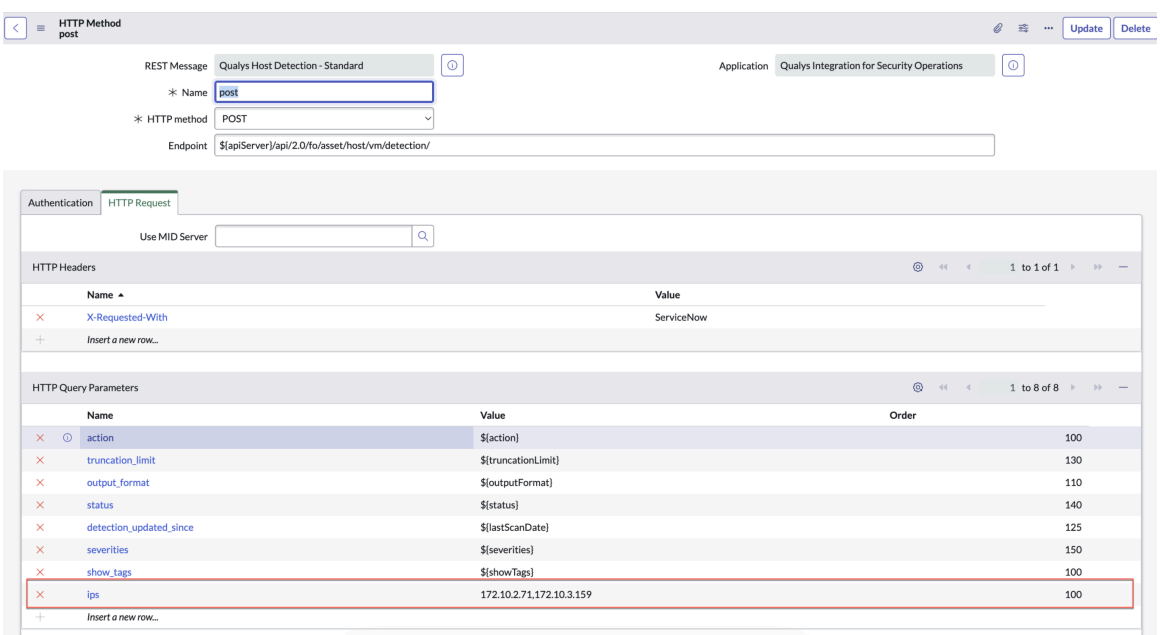
Sans ajouter d'appels d'API ou de codage supplémentaires, cette fonctionnalité vous permet de personnaliser vos informations de requête HTTP avec Qualys les paramètres de votre ServiceNow AI Platform. Vous modifiez ou ajoutez ces valeurs à votre enregistrement de méthode HTTP sous la méthode REST pour les intégrations prises en charge Qualys de la Qualys Vulnerability Integration.

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Recherchez les paramètres pris en charge par le Qualys produit sur le site développeur que vous souhaitez utiliser pour votre filtrage.
   Les paramètres et les Qualys valeurs que vous saisissez à partir du produit ne sont pris en charge qu'au niveau de l'instance d'intégration dans votre ServiceNow AI Platform. Toutes les Qualys intégrations prennent en charge le filtrage à l'aide de paramètres de requête.
2. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
3. Sur la Qualys page de liste Intégrations, cliquez sur l'enregistrement de l'intégration pour laquelle vous souhaitez ouvrir l'enregistrement.
4. Une fois l'onglet Qualys Détails REST sélectionné, recherchez et cliquez sur l'icône d'informations (I) pour la méthode REST, puis sur **Ouvrir l'enregistrement** pour ouvrir l'enregistrement de la méthode HTTP.
5. Sélectionnez l'onglet **de demande HTTP** .
6. Dans les paramètres de requête HTTP du corps de la demande, ajoutez les valeurs que vous avez obtenues sur le Qualys site développeur.

   Dans l'image suivante, à titre d'exemple, le paramètre qui ingère uniquement certaines adresses *ips={value}* /plages IP a été ajouté. Dans ce cas, la **valeur** est une ou plusieurs adresses IP/plages que vous spécifiez. Les entrées multiples sont séparées par des virgules, 172.10.2.71, 172.10.3.159, et une plage est spécifiée par un trait d'union, 10.10.10.1-10.10.10.100. Consultez le site du Qualys développeur pour plus d'informations.



   Si vous souhaitez entrer plusieurs paramètres, consultez la documentation pour plus d'informations sur la Qualys façon de séparer chaque valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous devez connaître vos exigences en matière d'API. Vous devrez peut-être ajouter ces propriétés API aux paramètres de requête ou au contenu du corps.

Quelques autres paramètres que vous pourriez trouver utiles sur le Qualys site du développeur :

- `ag_ids` - ID de listes de groupes d'actifs à récupérer. Ce paramètre garantit que seules les machines sous votre champ d'application sont introduites.
- `qids` - Ce paramètre limite les résultats à certaines vulnérabilités seulement (QID dans la table Third-Party Entry). Ce paramètre empêche d'inonder votre système d'enregistrements d'informations.

7. Cliquez sur **Mettre à jour**.

Résolution des problèmes d'intégration de vulnérabilité Qualys

Certains problèmes couramment rencontrés, ainsi que des solutions de contournement sont abordés.

Les pièces jointes n'apparaissant pas après l'importation

Si les pièces jointes n'apparaissent pas comme prévu pour les sources de données ou sur un incident de sécurité après les importations d'intégrations tierces, vérifiez vos restrictions IP.

Les restrictions d'accès IP peuvent empêcher les pièces jointes d'être vues, sauf si vous êtes connecté à partir d'une adresse IP sécurisée. Étant donné qu'une nouvelle pièce jointe est ajoutée à chaque importation, cela peut entraîner des doublons que vous devez supprimer.

Par exemple, lorsque vous exécutez une intégration d'importation d'hôte tierce, si vous ne voyez aucune pièce jointe sur vos sources de données, vérifiez vos restrictions IP et ajoutez des utilisateurs à la liste sûre avant l'importation.

Modifier les cartes de transformation

Les cartes de transformation sont fournies avec des configurations de base et sont généralement suffisantes. Vous pouvez modifier les mappages de transformation en fonction des besoins de votre organisation.

Avant de commencer

Rôle requis : sn_vul_qualys.admin + import_admin

Procédure

1. Accédez à la **Tous** > **Ensembles de données à importations système** > **Administration** > **Cartes de transformation** pour afficher les messages REST.
2. Filtrez la liste résultante par application et limitez la liste à l'application **Qualys Vulnerability Integration** .
3. Modifiez les cartes de transformation selon les besoins du client.

Pour plus d'informations sur les données fournies par l'API Qualys, consultez la documentation de l'API Qualys .

Vérifier la taille de la propriété de la pièce jointe XML

Vérifie que la propriété de pièce jointe XML est suffisante pour les fichiers volumineux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Importer/exporter**.
2. Faites défiler vers le bas jusqu'à **Propriétés d'importation** > **Format XML** en bas de la page.



3. Si nécessaire, remplacez la valeur par 250 et cliquez sur **Enregistrer**.

Information associée

Propriétés système disponibles

Limites de la récupération de données

Par défaut, il n'existe aucune restriction sur la façon dont les données sont récupérées à partir de Qualys. De nombreux enregistrements peuvent être liés à des vulnérabilités de faible gravité qu'un client n'est pas disposé à corriger à l'aide de son processus de réponse aux vulnérabilités. La mise à jour des paramètres de message/méthode REST correspondants peut modifier ce comportement.

Le message/la méthode REST responsable de cette mise à jour est **Qualys Host Detection – Standard/POST**. Pour mettre à jour les valeurs, ajoutez un nouveau paramètre de requête HTTP à la méthode POST avec les valeurs suivantes :

- Nom : gravités
- Valeur : 3-5 (ou toute autre sévérité appropriée souhaitée)

Résolution d'un échec d'intégration à la base de connaissances Qualys

Résolvez Qualys l'échec de l'intégration de la base de connaissances en réduisant la taille de la pièce jointe de Qualys la charge utile reçue à la limite spécifiée.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Assurez-vous que la taille de la pièce jointe de la charge utile se trouve dans la limite spécifiée.
   a. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration**.
   b. Sélectionnez l'onglet **Paramètres d'instance d'intégration** .
   c. Sélectionnez **max_delta_days** et modifiez la valeur par défaut sur 3.
2. Si l'intégration échoue toujours, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Intégrations principales**.

b. Sélectionnez **la base de connaissances Qualys**.

c. Sélectionnez l'onglet **Détails de l'intégration** .

d. Dans le champ **Heure de début** , sélectionnez la date actuelle pour ignorer l'exécution de l'exécution pour ce jour.

e. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration**.

f. Sélectionnez l'onglet **Paramètres d'instance d'intégration** .

g. Sélectionnez **kb_backfill_full_import** et remplacez la valeur par défaut par true.

Résultats
L'exécution de l'intégration du remplissage de la base de connaissances Qualys met à jour toutes les entrées tierces (TPE) dans le système. Alors que l'intégration de la détection d'hôte Qualys crée une entrée d'espace réservé, l'intégration du remplissage de la base de connaissances Qualys la met à jour.

Qualys Vulnerability Integration Rapports

La Qualys Cloud Platform vue d'ensemble est une vue exécutive de l'activité de vulnérabilité. En fournissant des tendances, des rapports et des détails sur des données spécifiques, un administrateur ou un analyste peut rapidement identifier les zones de préoccupation. Les graphiques sont renseignés avec les données après la récupération des éléments vulnérables et des données de la Qualys base de connaissances.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à surveiller la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en affichant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Consultez Réponse aux vulnérabilités Espaces de travail et Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Versions antérieures de Réponse aux vulnérabilités

Les analystes de vulnérabilité peuvent également utiliser les tableaux de bord par défaut de l'environnement classique pour surveiller les données de vulnérabilité. Consultez Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités pour plus d'informations.

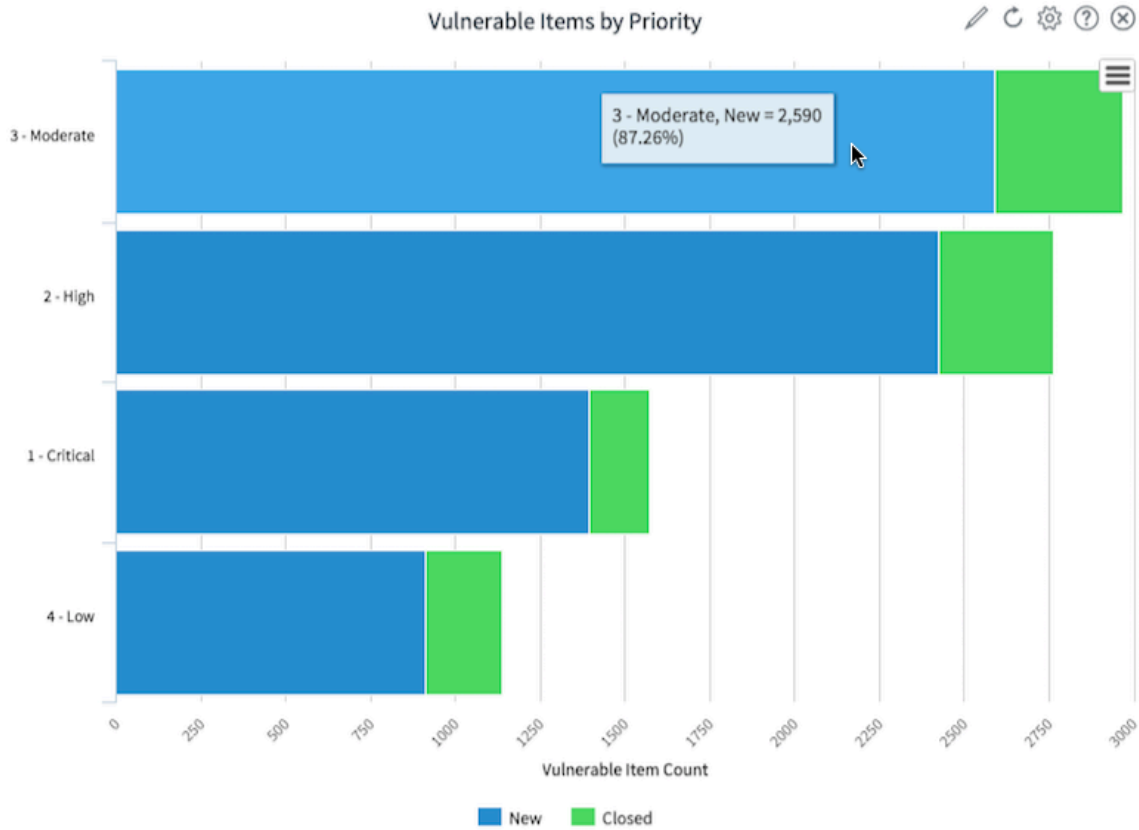
Remarque : L'utilisation de l'intégration de vulnérabilité suppose que le réglage, les tests et le Qualys Cloud Platform déploiement ont eu lieu dans votre instance. Ces fonctions sont des domaines qui dépassent le cadre de la documentation produit. Pour obtenir de l'aide, contactez Service client et assistance.

Dans chaque graphique, vous pouvez pointer vers n'importe quelle partie d'un graphique (barre, secteur, point de données, etc.) pour afficher des données générales spécifiques à cette partie. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de Qualys Vulnerability Integration graphique



Les rapports suivants sont disponibles sur la page d'accueil Qualys Cloud Platform .

Qualys Vulnerability Integration Rapports Vue d'ensemble

Nom	Visuel	Description
CI synchronisés avec Qualys	À barres	Affiche le nombre d'éléments vulnérables ouverts enregistrés pour chaque CI, du plus important au moins élevé.
Ouvrir les éléments vulnérables Qualys	À barres	Affiche le nombre d'éléments vulnérables ouverts associés à des vulnérabilités (enregistrements CVE), du plus important au moins élevé.
Total des éléments vulnérables Qualys	À barres	Affiche le nombre d'éléments vulnérables ignorés dont l'expiration est prévue dans les 7 jours.
Éléments vulnérables par priorité	Graphique de tendance	Affiche le nombre d'entrées de vulnérabilité enregistrées chaque semaine.
Prévalence QID	À barres	Affiche le nombre d'éléments vulnérables enregistrés pour chaque modèle, du plus au moins important.
Ouvrir les éléments vulnérables Qualys	Liste	Affiche le nombre d'éléments vulnérables enregistrés pour chaque éditeur, du plus important au moins élevé.

Qualys Graphique de l'état d'exécution de l'intégration

Le Qualys module État de l'exécution de l'intégration est une vue graphique de l'état des exécutions de l'intégration Qualys .

Pour afficher l'état des exécutions d'intégration, accédez à **Intégration de vulnérabilité Qualys** > **État de l'exécution de l'intégration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

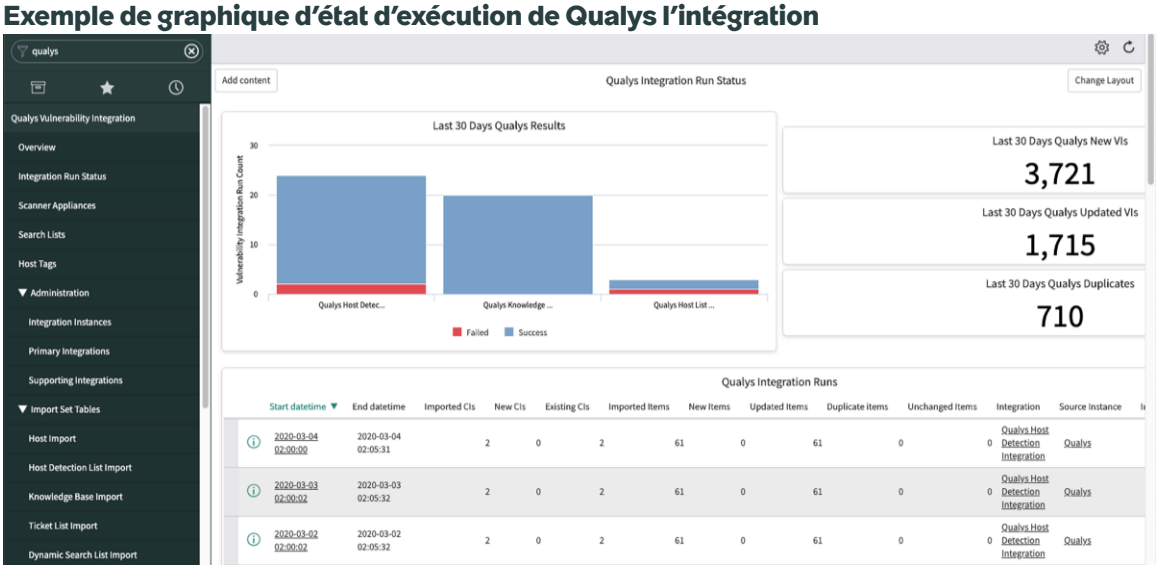
Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Dans le graphique, pointez sur n'importe quelle partie (barre, secteur, point de données, etc.) pour afficher des données générales spécifiques à cette partie. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

L'état Qualys de l'exécution de l'intégration affiche l'état d'exécution de l'intégration de vulnérabilité au cours des 30 derniers jours. Le nombre de VI mis à jour Qualys [qualys] indique le nombre de détections uniques dans le même actif. L'élément vulnérable est ensuite mis à jour avec la nouvelle détection.

Remarque : Le nombre d'exécutions de l'intégration de vulnérabilité n'est affiché que pour les intégrations, qui sont définies sur l'état actif. Accédez à la **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales** et définissez l'état sur actif.

Exemple de graphique d'état d'exécution de Qualys l'intégration



- Les valeurs de la colonne Éléments importés représentent le nombre total d'enregistrements créés à partir d'une exécution d'intégration.
- La colonne Nouveaux éléments affiche le nombre d'enregistrements créés à partir d'une exécution d'intégration.
- La colonne Éléments en double n'est plus renseignée. Vous préférez peut-être supprimer cette colonne de l'affichage.
- La colonne Éléments mis à jour affiche le nombre de fois que les enregistrements sont mis à jour au cours d'une exécution d'intégration. Cette valeur n'est pas le nombre d'enregistrements uniques qui sont mis à jour. Si, par exemple, un enregistrement est mis à jour deux fois pendant l'exécution de l'intégration, il est compté deux fois et s'affiche sous la forme de 2 éléments mis à jour.
- La colonne Éléments inchangés affiche les enregistrements trouvés pendant l'exécution de l'intégration qui existent déjà dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'intégration s'exécute sans résultat pour les quatre valeurs suivantes : **Nouveaux CI**, **CI existants**, **Nouveaux éléments** et **Éléments mis à jour** sont filtrés hors de la liste des **exécutions d'intégration Qualys** .

Qualys Rapports des graphiques d'état d'exécution de l'intégration

Nom	Description
Résultats des 30 derniers jours Qualys	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Exécuter dans un visuel de barre.
Nouveaux VI au cours des 30 derniers jours Qualys	Nombre de nouveaux enregistrements importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour au cours des 30 derniers jours Qualys	Nombre d'enregistrements mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Doublons des 30 derniers jours Qualys	Nombre d'enregistrements en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Qualys Exécutions des intégrations	Les enregistrements d'exécution de l'intégration dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection dans la `sn_vul_detection` table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, une fois l'exécution de l'intégration terminée.
Mesures de performance d'ingestion d'élément vulnérables au cours des 30 derniers jours Qualys	Mesures des performances quotidiennes des éléments vulnérables comparées aux 30 derniers jours.
Rendement de performance d'ingestion d'élément vulnérable au cours des 30 derniers jours Qualys	Débit quotidien d'ingestion d'éléments vulnérables mesuré pour l'intégration de la détection d'hôte Qualys au cours des 30 derniers jours.

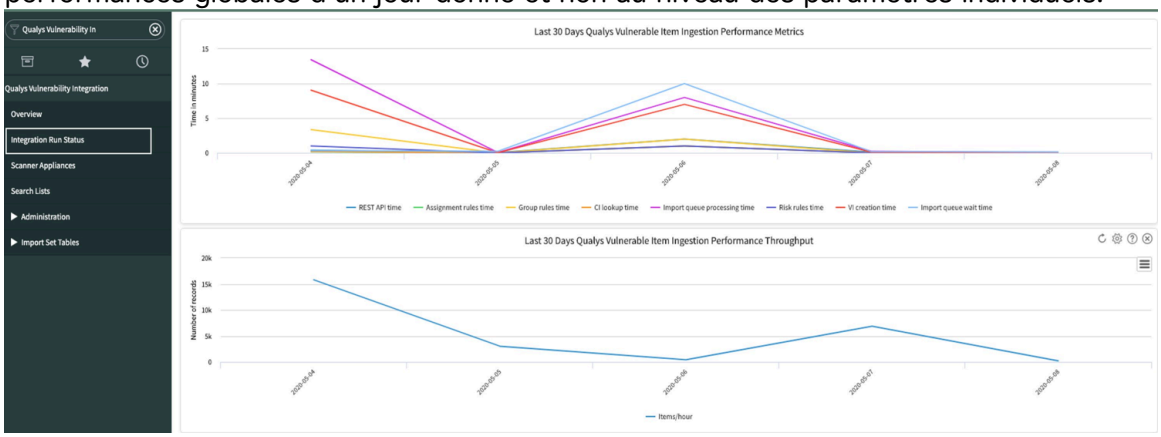
Plusieurs facteurs peuvent avoir un impact sur les performances de l'exécution de l'intégration, comme la quantité de données et le temps nécessaire pour traiter ces données. Deux graphiques comparent les mesures des performances :

- Qualys Mesures de performance d'ingestion d'élément vulnérable : comparez les mesures de performances quotidiennes pour les règles d'affectation, les règles de groupe, les règles de risque, le temps d'attente de la file d'attente, le temps de traitement de la file d'attente et d'autres statistiques relatives aux éléments vulnérables au cours des 30 derniers jours, afin d'identifier la cause de tout écart de performance. La performance est calculée en fonction du temps nécessaire pour chaque activité. Ces paramètres sont calculés et associés au niveau de l'exécution de l'intégration. Chaque paramètre est codé par couleur pour faciliter l'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Qualys Débit de performance d'ingestion d'élément vulnérable : comparez le débit quotidien d'ingestion d'éléments vulnérables pour l'intégration de la détection d'hôte Qualys . Le débit est mesuré en éléments par heure. Ce rapport montre les performances globales d'un jour donné et non au niveau des paramètres individuels.



Transformation des données Qualys

Les données récupérées à partir de Qualys sont traitées via un ensemble de sources de données et de transformations.

La plupart des transformations sont effectuées à l'aide de Qualys Vulnerability Integration scripts de transformation. Ces scripts sont destinés à un usage interne, la suppression n'est pas recommandée. Les modifications nécessitent un codage ou une expertise avancée ServiceNowQualys Vulnerability Integration . Les cartes restantes sont répertoriées dans cette section et utilisent des cartes de terrain.

Remarque : Lors de l'installation, des cartes de gravité normalisées, qui transforment les niveaux de gravité importés Qualys Cloud Platform en niveaux de gravité standard, sont installées dans le module Mappage de Réponse aux vulnérabilités gravité normaliséeServiceNow. Consultez Créer une carte de Réponse aux vulnérabilités gravité pour plus d'informations.

Importation de liste de recherches dynamiques

La carte de transformation de liste de recherches dynamiques Qualys est utilisée pour transformer et importer des listes de recherches dynamiques Qualys. Les changements apportés à cette transformation modifient la façon dont les listes de recherches dynamiques sont traitées et insérées dans le système.

Pour accéder à cette carte de transformation, accédez à **Intégration de vulnérabilité Qualys** > **Tables de jeux d'importation** > **Importation de liste de recherches dynamiques**.

La table affiche les champs en cours de transformation.

Champs de carte de transformation de liste de recherche dynamique Qualys

Champ source	Champ cible	Description
u_id	id	Utilisé comme identificateur pour la liste de recherches dynamiques Qualys.
[Script]	list_type	Type de liste de recherche. L'option Dynamique correspond à la valeur par défaut pour la transformation de la liste de recherches dynamiques.
u_title	Titre	Nom dans Qualys de cette liste de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En plus des mappages de champs, il existe également un script de transformation qui est exécuté pendant le processus de transformation.

La table suivante indique quand ce script s'exécute et à quoi il sert.

Liste de recherche dynamique Qualys : carte de transformation, script, minutage et objectif

Lorsque le script est exécuté	Objectif du script
onAfter (une fois qu'un jeu d'importation a terminé la transformation).	Crée les relations entre les listes de recherches et leurs vulnérabilités associées. Réservée à une utilisation interne. Il n'est pas recommandé de modifier ou de supprimer.

Importation de liste de recherches statiques

La carte de transformation de liste de recherches statiques Qualys est utilisée pour transformer et importer des listes de recherches statiques Qualys. Les changements apportés à cette transformation modifient la façon dont les listes de recherches statiques sont traitées et insérées dans le système.

Pour accéder à cette carte de transformation, accédez à **Intégration de vulnérabilité Qualys** > **Tables de jeux d'importation** > **Importation de liste de recherches statiques**.

La table affiche les champs en cours de transformation.

Champs de carte de transformation de liste de recherches statiques Qualys

Champ source	Champ cible	Description
u_id	id	Utilisé comme identificateur pour la liste de recherches statiques Qualys.
u_title	Titre	Nom dans Qualys de cette liste de recherche.
[Script]	list_type	Type de liste de recherche. Statique est la valeur par défaut pour la transformation de la liste de recherches statiques.

En plus des mappages de champs, il existe également un script de transformation qui est exécuté pendant le processus de transformation.

La table suivante indique quand ce script s'exécute et à quoi il sert.

Liste de recherche statique Qualys : carte de transformation, script, minutage et objectif

Lorsque le script est exécuté	Objectif du script
onAfter (une fois qu'un jeu d'importation a terminé la transformation).	Crée les relations entre les listes de recherches et leurs vulnérabilités associées. Réservée à une utilisation interne. Il n'est pas recommandé de modifier ou de supprimer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importation d'un groupe de ressources

La carte de transformation du dispositif du groupe d'actifs Qualys est utilisée pour transformer les données du groupe d'actifs Qualys afin de créer des enregistrements de dispositif de scanner. Les changements apportés à cette transformation modifient la façon dont les dispositifs de scanner sont créés et modifiés.

Pour accéder à cette carte de transformation, accédez à **Intégration de vulnérabilité Qualys** > **Tables de jeux d'importation** > **Importation d'un groupe de ressources**.

La table affiche les champs en cours de transformation.

Champs de carte de transformation des groupes de ressources Qualys

Champ source	Champ cible	Description
u_id	id	Utilisé comme identificateur pour le groupe d'actifs Qualys.
[Script]	Manuelle	Valeur scriptée pour déterminer comment l'enregistrement cible a été créé. Lorsqu'il est créé via des transformations, ce champ est toujours faux.
[Script]	ip	Adresses IP associées au groupe d'actifs en cours de transformation.
u_default_appliance_id	appliance_id	Identificateur d'équipement Qualys pour le dispositif par défaut dans ce groupe d'actifs.
u_title	asset_group_name	Nom du groupe de ressources Qualys.

En plus des mappages de champs, il existe également un script de transformation qui est exécuté pendant le processus de transformation.

La table suivante indique quand ce script s'exécute et à quoi il sert.

Script de carte de transformation du groupe d'actifs Qualys, minutage et objectif

Lorsque le script est exécuté	Objectif du script
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Le script qui contraint le groupe d'actifs importe uniquement aux groupes d'actifs disposant d'un dispositif par défaut et d'un ensemble d'adresses IP mappées. Réservée à une utilisation interne. Il n'est pas recommandé de modifier ou de supprimer.

Importation du dispositif

La carte de transformation du dispositif Qualys est utilisée pour transformer les données du dispositif Qualys en enregistrements de dispositif. Elle permet de mettre à jour les enregistrements du dispositif qui devaient initialement être créés à partir de l'importation du groupe de ressources. Les changements apportés à cette transformation modifient la façon dont les enregistrements du dispositif sont mis à jour avec les détails du dispositif.

Pour accéder à cette carte de transformation, accédez à **Intégration de vulnérabilité Qualys** > **Tables de jeux d'importation** > **Importation du dispositif**.

La table affiche les champs en cours de transformation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation du dispositif Qualys

Champ source	Champ cible	Description
u_name	appliance_name	Nom du dispositif de scanner Qualys.
u_status	appliance_status	Le dernier état signalé du dispositif de scanner Qualys.
u_id	appliance_id	L'identificateur du dispositif Qualys.

En plus des mappages de champs, il existe également un script de transformation qui est exécuté pendant le processus de transformation.

La table suivante indique quand ce script s'exécute et à quoi il sert.

Synchronisation et objectif du script de carte de transformation du dispositif Qualys

Lorsque le script est exécuté	Objectif du script
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Utilisé pour mettre à jour les noms et les états des dispositifs pour l'ID donné. Réservée à une utilisation interne. Il n'est pas recommandé de modifier ou de supprimer.

Qualys Messages REST

Les messages REST Qualys sont utilisés pour effectuer des appels vers l'API Qualys.

À partir de la version 12.9.2 de , vous avez la possibilité de Qualys choisir entre l'authentification de base ou OAuth. La méthode d'authentification dans le cloud Qualys de paramètre d'instance est préconfigurée pour l'authentification de base. Si vous préférez utiliser OAuth, vous devez modifier le paramètre d'instance d'intégration, puis configurer le message REST directement pour OAuth.

Message REST de détection d'hôte Qualys

Le message REST de la détection d'hôte Qualys effectue l'appel initial de l'API de détection de liste d'hôtes pour l'intégration de la détection d'hôte Qualys.

Paramètres de message REST de détection d'hôte Qualys

Nom de paramètre	Valeur	Description
action	liste	Indique le type d'opération demandée. Paramètre requis. Aucun changement n'est nécessaire.
output_format	XML	Définit le format du rapport renvoyé par Qualys. Les différents scripts et transformations supposent du langage XML, il n'est donc pas recommandé de modifier la valeur.
detection_processed_after	${lastScanDate}	Affiche uniquement les détections dont l'état de détection a changé après une date et une heure données. Pour les détections

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de message REST de détection d'hôte Qualys (suite)

Nom de paramètre	Valeur	Description
		qui n'ont jamais changé, la date est appliquée à la dernière date de détection.
truncation_limit	500	Nombre d'hôtes à partir desquels récupérer les données, en fonction de la demande. Ce paramètre est utilisé à des fins de pagination. La valeur par défaut est 500, mais vous pouvez utiliser des valeurs plus grandes ou plus petites. Ne définissez pas à moins de 100 car cela augmente considérablement la charge du système. Les valeurs plus petites nécessitent plus d'appels à l'API Qualys et les valeurs plus grandes entraînent des ensembles de résultats à traiter plus volumineux et des délais potentiels de récupération/traitement des données.
état	Nouveau, Fixe, Actif, Rouvert	États de détection à récupérer à partir de Qualys. La valeur par défaut récupère tous les états. Pour les extractions de données volumineuses (souvent l'extraction initiale des données), il peut être avantageux d'exclure les statuts fixes de cette liste. Il est important d'inclure l'état Corrigé lors de la mise à jour des vulnérabilités déjà présentes dans le système.

Message REST de pagination de détection d'hôte Qualys

Le message REST Pagination de détection d'hôte gère les demandes de pagination vers l'API de détection d'hôte.

Lorsque la détection d'hôte primaire s'exécute, si l'API Qualys fournit une URL pour extraire la page de données suivante, ce message REST récupère ces données supplémentaires. Ces données sont utilisées par le gestionnaire de pagination de détection d'hôte.

Pagination de détection d'hôte REST est un message REST spécialisé et n'a pas vocation à être modifié.

Base de connaissances Qualys (remplissage) Message REST

Le message REST de la base de connaissances Qualys (remplir) récupère les données de la base de connaissances Qualys en fonction de l'horodatage de la dernière modification des données de vulnérabilité pour l'intégration de la base de connaissances Qualys.

Les modifications apportées à l'enregistrement de la méthode de message REST ont un impact sur la demande de récupération des informations de la base de connaissances effectuée à Qualys.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La table suivante répertorie les paramètres de demande envoyés.

Base de connaissances Qualys (remplissage) Paramètres des messages REST

Paramètre	Valeur	Description
action	liste	Indique le type d'opération demandé. Paramètre requis. Il n'est pas recommandé d'apporter des changements.
Détails	Tous	Indique le niveau de détail affiché pour les vulnérabilités récupérées. Vous pouvez modifier en toute sécurité si nécessaire.
ids	${qids}	Spécifie les QID à récupérer à partir de Qualys. Référencé dans le code. Aucune modification n'est recommandée.

Message REST de la base de connaissances Qualys (basé sur la date)

Le message REST de la base de connaissances Qualys (basé sur la date) est utilisé pour récupérer les données de la base de connaissances Qualys en fonction de l'horodatage de la dernière modification des données de vulnérabilité. Ce message est utilisé par l'intégration de la base de connaissances Qualys.

Les modifications apportées à l'enregistrement de la méthode de message REST ont un impact sur la demande de récupération des informations de la base de connaissances effectuée à Qualys.

La table suivante répertorie les paramètres de demande envoyés.

Base de connaissances Qualys (basé sur la date) Paramètres du message REST

Champ source	Champ cible	Description
action	liste	Indique le type d'opération demandée. Paramètre requis. Il n'est pas recommandé d'apporter des changements.
Détails	Tous	Indique le niveau de détail affiché pour les vulnérabilités récupérées. Vous pouvez modifier en toute sécurité si nécessaire.
last_modified_after	${dateStart}	Indique quand commencer à récupérer les données historiques. Utilisé par le code pour déterminer l'heure de début et pour faciliter la pagination. Il n'est pas recommandé de modifier ou de supprimer.
last_modifiedbefore	${dateEnd}	Indique quand terminer la récupération des données historiques. Utilisé par le code pour déterminer l'heure de fin et pour faciliter la pagination.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Base de connaissances Qualys (basé sur la date) Paramètres du message REST (suite)

Champ source	Champ cible	Description
		Il n'est pas recommandé de modifier ou de supprimer.

Tickets Qualys Message REST

Le message REST des tickets Qualys récupère les informations des tickets Qualys pour l'intégration des tickets Qualys. Les changements apportés à l'enregistrement de la méthode de message REST ont un impact sur les demandes de récupération des informations de ticket adressées à Qualys.

La table affiche les paramètres de demande envoyés.

Paramètres du message REST des tickets Qualys

Nom de paramètre	Valeur	Description
modified_since_datetime	${lastRunDatetime}	Indique la date de dernière exécution de l'intégration et la date après laquelle extraire les données. Utilisé par le code. Il n'est pas recommandé d'apporter des changements.
since_ticket_number	${lastTicketNumber}	Indique le dernier ticket récupéré à partir de Qualys. Utilisé pour la pagination. Il n'est pas recommandé d'apporter des changements.
show_vuln_details	1	Indique si les détails de la vulnérabilité ont été récupérés.

Diviser les détections Qualys en fonction de l'instance de vulnérabilité

Vulnerability Response vous permet de séparer les détections des scanners Qualys, créant ainsi un élément vulnérable (VIT) unique pour chaque instance de vulnérabilité détectée. Cela permet une affectation plus précise aux équipes de remédiation et améliore la gestion et le suivi des vulnérabilités.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La charge utile du scanner Qualys inclut des données de détection avec des détails de preuve. Chaque chemin d'accès de la preuve est utilisé pour identifier et diviser les instances de vulnérabilité. La balise de sortie dans la charge utile indique l'emplacement de la vulnérabilité, ce qui permet une séparation et une gestion précises des détections.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Activer le fractionnement de détection
   a. Accédez à la table Intégration tierce [sn_sec_int_integration].
   b. Ouvrez l'enregistrement pour *`Qualys Cloud Platform`*.
   c. Définissez *`Include proof VI key`* sur *true*.
   d. Enregistrez l'enregistrement.
2. **Facultatif :** Exclure des QID spécifiques du fractionnement de détection
   a. Ouvrez la propriété système [sn_vul_qualys.skip_split_detection_ids].
   b. Dans le champ **Valeur** , saisissez une liste séparée par des virgules de QID que vous souhaitez exclure du fractionnement.

      Remarque : Par défaut, les QID suivants sont exclus de la division en raison du volume de leurs résultats : QID-989920, QID-993308, QID-5001711, QID-5001632.

   c. Enregistrez la propriété.
3. S'assurer que les QID sont répertoriés pour la division
   a. Accédez à la table Liste de vulnérabilité de clé de preuve [sn_vul_proof_key_vulnerability_list].
   b. Vérifiez que les QID que vous souhaitez diviser sont répertoriés.

Résultats

Après l'intégration de la *`détection d'hôte Qualys`*, les détections sont divisées en fonction des preuves, créant des éléments vulnérables (VIT) individuels pour chaque instance de vulnérabilité. Vous pouvez vérifier les résultats dans la table Détections d'éléments de vulnérabilité [sn_vul_detection_list], où chaque détection apparaît sous la forme d'un enregistrement distinct.

Composants installés avec le Qualys Vulnerability Integration

Les rôles, tâches d'intégration et tables suivants sont installés avec le Qualys Vulnerability Integration.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Afficher les listes filtrées des composants installés avec une application

Filtrez la table Fichiers d'applications afin de n'afficher que les rôles, les travaux planifiés et les tables installés avec une application. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés dans l'instance et dans la table de métadonnées. Suivez ces étapes pour afficher les listes filtrées à partir de la table Fichiers d'applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application. Par exemple : **Application** > **est** > **Réponse aux vulnérabilités**.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, sélectionnez **ET,** puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
sn_vul_qualys.read	Dispose d'un Qualys Vulnerability Integration accès en lecture aux enregistrements.	
sn_vul_qualys.utilisateur	Utilisateur pour Qualys Vulnerability Integration. Peut lire et écrire des enregistrements	sn_vul_qualys.read
sn_vul_qualys.admin	Administrateur pourQualys Vulnerability Integration. Par exemple, vous pouvez modifier les dates de début d'intégration et définir des paramètres de configuration avancés.	• sn_vul_qualys.utilisateur • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Peut configurer le Qualys Vulnerability Integration	sn_vul_qualys.admin

Tâches d'intégration installées

Tâche d'intégration	Description
Qualys Intégration de liste de recherches statiques	Synchronise les listes de recherches pour trouver les Qualys entrées vulnérables. Récupère uniquement les enregistrements de type liste statique.
Qualys Intégration complète de la détection d'hôte	Récupère les données d'hôte et de Qualys vulnérabilité et les traite dans votre instance. Il coordonne les appels de messages REST à l'API de détection d'hôte. Le résultat de cette intégration est constitué d'éléments vulnérables. Cette intégration importe tous les états de la vulnérabilité : Nouveau, Corrigé, Actif et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche d'intégration	Description
	Rouvert. Par défaut, cette intégration est inactive et s'exécute chaque semaine. **Remarque :** Une fois cette intégration activée, la tâche globale quotidienne importe uniquement les états Nouveau, Corrigé et Rouvert.
Qualys Intégration de la liste d'hôtes	Récupère les données d'analyse de l'hôte authentifiées et non authentifiées et les balises hôte une Qualys fois par semaine et les stocke dans le module Éléments détectés de votre instance. Permet d'identifier les actifs qui n'ont pas été analysés récemment.
Qualys Intégration de la détection d'hôte	Récupère les données d'hôte et de Qualys vulnérabilité et les traite dans votre instance. Il coordonne les appels de messages REST à l'API de détection de liste d'hôtes. Les résultats de cette intégration sont des éléments vulnérables. Qualys Les balises d'hôte sont importées dans cette intégration.
Qualys Intégration des tickets	Récupère les Qualys tickets et les ajoute à votre instance. Il coordonne les appels de messages REST à l'API de liste de tickets. Il y a souvent moins de tickets que les détections d'hôte, car Qualys les paramètres peuvent limiter les détections qui entraînent un ticket.
Qualys Intégration de la liste des profils d'options	Récupère les profils d'option du Qualys produit. Les profils d'option incluent les paramètres d'analyse requis lorsque vous lancez des analyses à partir de votre ServiceNow AI Platform instance.
Qualys Intégration de la liste des dispositifs	Récupère les informations sur le dispositif de scanner à partir de Qualys.
Qualys Intégration de groupes d'actifs	Récupère les informations sur le groupe d'actifs à partir de Qualys. Les groupes d'actifs sont utilisés pour identifier les dispositifs de scanner à utiliser pour analyser les éléments de configuration correspondants.
Qualys Base de connaissances (remplissage)	Récupère les entrées de la base de Qualys connaissances. Exécution planifiée après l'intégration de la détection d'hôte Qualys . Met à jour votre instance avec tous les QID qui ont été référencés dans l'intégration de la détection

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche d'intégration	Description
	d'hôte, mais qui n'existaient pas dans le système.
Qualys Base de connaissances	Récupère les entrées de la base de Qualys connaissances. Les données récupérées sont basées sur la date à laquelle les vulnérabilités ont été mises à jour par Qualys et depuis la dernière exécution de l'intégration. Ces données sont utiles pour renseigner les données historiques dans votre instance et pour s'assurer que les Qualys identificateurs (QID) sont à jour.
Qualys Intégration de la liste de recherches dynamiques	Synchronise les listes de recherches pour rechercher des Qualys entrées vulnérables et récupère les enregistrements de type liste dynamique.
Fixation des détections pour la clé mise à jour pour Qualys	Combinaison hachée de champs qui permet d'identifier et de lier une détection à un Qualys élément vulnérable.
Qualys Mettre à jour les éléments détectés existants avec l'identificateur de partition de réseau	Met à jour vos éléments détectés existants. Les CI de vos données d'intégration de vulnérabilité existantes Qualys sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau.

Tables installées

Table	Description
Vulnérabilité de la liste de recherches sn_vul_qualys_m2m_search_list_vul	Stocke le mappage entre la Qualys liste de recherches et une vulnérabilité.
Qualys Scanner de vulnérabilité sn_vul_qualys_scanner	Table qui étend les scanners de vulnérabilité pour stocker des informations de scanner pour la Qualys fonctionnalité de nouvelle analyse.
Qualys Listes de recherches sn_vul_qualys_search_list	Stocke les listes de recherches récupérées par l'intégration de la Qualys liste de recherche.
Qualys Importation du dispositif sn_vul_qualys_appliance_imp	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de réponse est traitée directement avec le script onComplete.
Qualys CI sn_vul_qualys_ci	Table non utilisée
Pagination de détection d'hôte sn_vul_qualys_host_detection_pagination	Table non utilisée
Qualys Exécution de l'intégration	Table non utilisée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
sn_vul_qualys_integration_run	
Qualys Intégration sn_vul_qualys_integration	Table étendant l'intégration de vulnérabilité et stockant toutes les intégrations qui correspondent à Qualys.
Qualys Importation de liste de recherches statiques sn_vul_qualys_static_search_list_imp	Table étendant la ligne de jeu d'importation. Les cartes de champs sont utilisées pour transformer les données en table cible, Qualys listes de recherche.
Qualys Base de connaissances sn_vul_qualys_knowledge_base	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de réponse est traitée directement avec le script onComplete.
Qualys Liste des tickets sn_vul_qualys_ticket_list_imp	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de réponse est traitée directement avec le script onComplete.
Qualys Profil d'option sn_vul_qualys_option_profile	Table stockant les profils d'option récupérés à partir de Qualys. Table utilisée avec la nouvelle analyse.
Qualys Importation de liste de recherches dynamiques sn_vul_qualys_dynamic_search_list_imp	Table étendant la ligne de jeu d'importation. Les cartes de champs sont utilisées pour transformer les données en table cible, Qualys listes de recherche.
Qualys Réexécuter le jeu d'importation sn_vul_qualys_import_rerun	Table non utilisée
Qualys Importation du profil d'option sn_vul_qualys_option_profile_import	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de réponse est traitée directement avec le script onComplete.

Présentation de Intégration des vulnérabilités Rapid7

Utilise ServiceNow® Intégration des vulnérabilités Rapid7 les données importées de l'entrepôt Rapid7 de données ou des Rapid7 InsightVM produits pour vous aider à déterminer l'impact et la priorité des menaces potentiellement malveillantes.

Rapid7 Nexpose Les capteurs collectent les données et les envoient automatiquement à l'entrepôt de données (sur site) ou Rapid7 InsightVM aux produits (basés sur le Rapid7 cloud), qui analysent et corrélent les informations en permanence. Il s'intègre ServiceNow® Réponse aux vulnérabilités facilement pour mapper les vulnérabilités aux CI et aux services. Enrichit Intégration des vulnérabilités Rapid7 les données de vulnérabilité sur votre instance.

Rapid7 Les intégrations sont des points d'entrée qui interagissent avec l'entrepôt Rapid7 de données ou Rapid7 InsightVM les produits, appelés en tant que travaux planifiés. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités. Les travaux planifiés sont exécutés automatiquement et dans l'ordre spécifié. Vous pouvez également exécuter manuellement des travaux planifiés individuels.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Si vous utilisez à la fois Rapid7 l'entrepôt de données et Rapid7 InsightVM comme sources de vos données, vous courez le risque de dupliquer les enregistrements de vulnérabilité.

Remarque : Lors de la migration du type d'intégration **Entrepôt de données** vers le type **InsightVM** , vous pouvez dédupliquer vos enregistrements d'entrepôt de données existants. Consultez Dédupliquer les enregistrements de l'entrepôt de Intégration des vulnérabilités Rapid7 données pour plus d'informations.

Si vous avez plusieurs déploiements de l'intégration Rapid7 InsightVM de vulnérabilité, vous pouvez ajouter une intégration pour chaque déploiement. Les actifs, identifiés par plusieurs déploiements tiers et leurs vulnérabilités, sont consolidés et rapprochés avec votre CMDB. Cette consolidation se produit même lorsque les processus d'analyse se chevauchent entre les multiples déploiements. Les données provenant de chaque déploiement sont identifiées et disponibles dans une instance unique de Réponse aux vulnérabilités.

Remarque : Vous ne pouvez pas supprimer l'intégration de vulnérabilité d'origine, mais vous pouvez la désactiver. Les intégrations créées à partir de modèles désactivés sont désactivées par défaut.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Versions disponibles

Version de mise en production pour Zurich	Notes de publication
Intégration des vulnérabilités Rapid7 v13.6, 13.7	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Rôles

Rapid7 Les tâches d'intégration de vulnérabilité impliquent les rôles suivants.

- sn_vul_r7.admin : autorisation de lecture, d'écriture et de suppression d'enregistrements.
- sn_vul_r7.user : autorisation de lecture et d'écriture d'enregistrements.
- sn_vul_r7.read : autorisation de lecture des enregistrements.

Intégrations de Intégration des vulnérabilités Rapid7

Pour afficher le Intégration des vulnérabilités Rapid7, accédez à **Rapid7** > **Administration** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapid7 Intégrations d'entrepôts de données

Intégration	Description
Intégration des vulnérabilités Rapid7	Récupère les données de vulnérabilité et Rapid7 Nexpose les traite dans votre instance.
Rapid7 Intégration de la liste des actifs	Récupère les données d'analyse une fois par semaine à partir de l'entrepôt de Rapid7 Nexpose données et les stocke dans le module Éléments détectés de votre instance. Permet d'identifier les actifs qui n'ont pas été analysés récemment à l'aide de la date de **la dernière analyse** . Affichez l'heure de la dernière analyse dans la liste des éléments **détectés** dans Réponse aux vulnérabilités.
Rapid7 Intégration de catégorie	Récupère les informations de catégorie à partir de Rapid7 Nexpose. Les catégories fournissent une classification de haut niveau des vulnérabilités.
Rapid7 Intégration d'exploit	Récupère les informations sur l'exploit à partir de Rapid7 Nexpose.
Rapid7 Intégration de kit malware	Récupère les informations du kit malware à partir de Rapid7 Nexpose.
Rapid7 Intégration de référence	Récupère les références à des documents de référence externes tels que les CVE ou les références de vulnérabilité spécifiques au fournisseur.
Rapid7 Intégration de solution	Récupère les données de solution à partir de Rapid7 Nexpose, qui fournit des solutions recommandées à des vulnérabilités spécifiques.
Rapid7 Intégration de solution de remplacement	Récupère des informations sur les solutions qui sont remplacées par d'autres.
Rapid7 Intégration de solution prérequise	Récupère des informations sur les solutions qui sont des prérequis pour d'autres solutions. Lorsque cette intégration s'exécute, elle récupère le mappage des solutions et des solutions prérequises à partir de l'entrepôt Rapid7 de données. **Remarque :** Cette intégration fonctionne uniquement si le module d'extension Gestion des solutions pour vulnérabilités est activé.
Rapid7 Intégration de la carte de solution de vulnérabilité	Récupère le mappage pour associer des solutions à des vulnérabilités.
Rapid7 Intégration d'élément vulnérable	Récupère les données d'éléments Rapid7 Nexpose vulnérables et les traite dans votre instance. Les résultats de cette intégration sont des éléments vulnérables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapid7 Intégrations d'entrepôts de données (suite)

Intégration	Description
Rapid7 Intégration de résolution de l'élément vulnérable	Récupère des informations sur les éléments vulnérables marqués comme fermés dans Rapid7 Nexpose et ferme les éléments vulnérables correspondants dans Réponse aux vulnérabilités.
Rapid7 Intégration de site	Récupère les données du site à partir de Rapid7 Nexpose. Un site est une collection d'actifs qui sont ciblés pour une analyse.
Rapid7 Intégration de la liste des actifs	Récupère les balises d'hôte et les données d'analyse une fois par semaine à partir de l'entrepôt Rapid7 de données et les stocke dans le module Éléments détectés de votre instance. Permet d'identifier les actifs qui n'ont pas été analysés récemment à l'aide de la date de **la dernière analyse** . Afficher l'heure de la dernière analyse dans la liste des éléments **détectés** dans Réponse aux vulnérabilités
Rapid7 Intégration complète des éléments vulnérables	Importe toutes les détections Rapid7 pour tous les éléments de configuration analysés depuis la dernière exécution réussie de l'intégration. En fonction des données importées les plus récentes, les éléments vulnérables qui n'ont pas été trouvés récemment lors des analyses passent automatiquement à l'état « Fermé » lorsque le module Fermer automatiquement les éléments vulnérables périmés est activé.

Intégrations de Rapid7 InsightVM

Intégration	Description
Rapid7 Intégration d'éléments vulnérables : API	Récupère les données des éléments vulnérables d'InsightVM Rapid7 et les traite dans votre instance.
Intégration des vulnérabilités Rapid7 : API	Récupère les données de référence, de catégorie, d'exploit, de kit malware et de vulnérabilité d'InsightVM Rapid7 et les traite dans votre instance.
Rapid7 Intégration de la liste des actifs : API	Récupère les balises d'hôte et les données d'analyse une fois par semaine à partir de Rapid7 InsightVM et les stocke dans le module Éléments détectés de votre instance. Permet d'identifier les actifs qui n'ont pas été analysés récemment à l'aide de la date de **la dernière analyse** . Affichez l'heure de la dernière analyse dans la liste des éléments **détectés** dans Réponse aux vulnérabilités.
Rapid7 Intégration complète des éléments vulnérables : API	Importe toutes les détections Rapid7 pour tous les éléments de configuration analysés depuis la dernière exécution réussie de l'intégration. En fonction des données importées les plus récentes, les éléments vulnérables qui n'ont pas été trouvés récemment lors des analyses passent automatiquement à l'état « Fermé » lorsque le module Fermer automatiquement les éléments vulnérables périmés est activé.
Rapid7 Intégration de site	Récupère les données du site à partir du Rapid7 InsightVM produit. Cette intégration est définie pour s'exécuter chaque semaine à 00:00:00.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pendant l'importation, les enregistrements CVE qui ne sont pas déjà présents sont créés en tant qu'enregistrements NVD et référencés dans des entrées tierces par Rapid7 défaut. L'intégration du modèle ne Rapid7 peut pas être supprimée. Désactivez-le à la place.

Connecteur du graphe de services pour Rapid7

À partir de la version 2.0, Service Graph Connector for Rapid7 est disponible à partir du ServiceNow® Store. Consultez Connecteur du graphe de services pour Rapid7 pour plus d'informations.

Règles de recherche de CI

Les règles de recherche de CI déterminent comment remplir le champ **Élément de configuration** dans un enregistrement d'élément vulnérable.

Pour en savoir plus sur le fonctionnement des règles de recherche de CI, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Pour créer ou modifier des règles de recherche, reportez-vous à la section Créer une règle de recherche de CI de réponse aux vulnérabilités.

Remarque : Une fois supprimées, les règles ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Éléments détectés

Ce module répertorie les éléments de configuration détectés lors de l'importation à partir des intégrations d'éléments Rapid7 vulnérables (entrepôt de données ou API InsightVM) et de l'intégration de la Rapid7 liste des actifs : API. L'API Rapid7 d'intégration de la liste des actifs importe tous les actifs Rapid7 analysés pour détecter des vulnérabilités depuis la dernière exécution de l'intégration. L'intégration Rapid7 de la liste des actifs de l'entrepôt de données est incluse.

Remarque : Le filtre par défaut de cette liste est défini sur **Sans correspondance**. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Reportez-vous Éléments détectés à pour Réponse aux vulnérabilités en savoir plus sur le module Éléments détectés.

Balises d'hôtes

Les balises d'hôte sont importées dans le cadre de l'intégration de la liste des actifs - intégration de l'API Rapid7 pour Rapid7 InsightVM. Ils sont principalement utilisés pour le filtrage dans les Réponse aux vulnérabilités règles de tâche d'affectation et de rattrapage dans Rapid7 InsightVM. Ils s'affichent dans le formulaire Élément détecté.

Balises d'hôtes

Remarque : L'intégration Rapid7 de la liste des actifs : l'intégration de l'API doit être exécutée avant de créer des règles de tâche d'affectation ou de rattrapage, afin Réponse aux vulnérabilités que toutes les balises puissent être présentes dans les règles et avant que les éléments vulnérables ne soient importés et regroupés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le stockage des balises n'est pas sensible à la casse. Si une balise **San Diego** est créée, une balise **SAN DIEGO** ne peut pas être stockée dans la table des balises d'hôte. « San Diego » et « SAN DIEGO » sont considérés comme le même tag d'hôte. Quelle que soit la balise importée en premier, elle gagne.
- L'utilisation de balises d'hôte comme clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises d'hôte sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'hôte sont contrôlées par la propriété système globale **sn_vul.import_host_tags**. Cette propriété est définie sur vrai par défaut. La désactivation des balises les désactive dans toutes les instances.

Sites

Un site est une collection d'actifs ciblés pour une analyse. Un site se compose d'actifs cibles, d'un modèle d'analyse, d'un ou de plusieurs moteurs d'analyse et d'autres paramètres liés à l'analyse tels que les calendriers ou les alertes. Les sites sont gérés par Rapid7 des applications.

Intégration des vulnérabilités Rapid7 Le filtrage de site pendant la configuration vous permet de classer et de demander des ressources par site pendant l'importation. Voir Filtrage par Rapid7 sites pour plus d'informations sur le filtrage des importations.

L'entrepôt Rapid7 de données et Rapid7 InsightVM les intégrations de sites importent des sites en tant que tâche planifiée hebdomadaire.

Pour afficher les sites importés dans une liste, accédez à **Rapid7** > **Sites**.

Réouverture des éléments vulnérables résolus non fermés par les analyses

Les éléments vulnérables définis sur « Résolu » dans votre ServiceNow AI Platform instance, mais pas transitionnés vers « Fermé/Corrigé » par les exécutions d'intégration suivantes sont rouverts s'ils sont détectés lors des nouvelles analyses.

Pour Rapid7 les détections, une option est maintenant disponible sur la page de configuration Rapid7 de votre instance pour rouvrir les VI résolus par âge. S'ils sont activés, les VI sont définis sur « Résolu », mais ne sont pas transitionnés vers « Fermé/Corrigé » lors des analyses suivantes qui retournent à « Ouvert » après le nombre de jours que vous entrez.

Créer des CI à l'aide du moteur Identification et réconciliation (IRE)

Vous pouvez utiliser le moteur Identification et réconciliation pour créer de nouveaux CI lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte importé à partir d'un scanner tiers. Activez le module d'extension Modèles de classe CI CMDB pour créer des CI à l'aide des nouvelles classes, sinon des CI sans correspondance sont créés dans les classes CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation. Pour plus d'informations sur la configuration de la catégorisation des ressources cloud sans correspondance dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyser de nouveau les éléments vulnérables

Lancez de nouvelles analyses dans la Rapid7 plateforme pour vérifier que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Consultez Lancer une nouvelle analyse pour l'intégration de vulnérabilité Rapid7.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Rapid7 Gestion des solutions

Si vous avez activé le module d'extension Gestion des solutions pour vulnérabilités , les solutions pour l'entrepôt Rapid7 de Rapid7 données et Rapid7 InsightVM la table Solutions en matière de vulnérabilité [sn_vul_solution]. Toutefois, si vous n'avez pas activé le module d'extension Gestion des solutions pour vulnérabilités , il Intégration des vulnérabilités Rapid7 fonctionne tel quel et importe les solutions dans la table personnalisée [sn_vul_r7_solution]. Pour plus d'informations, consultez Rapid7 Gestion des solutions.

Préparation pour le Intégration des vulnérabilités Rapid7

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Préparez-vous à l'intégration en effectuant ces tâches. Cela Intégration des vulnérabilités Rapid7 suppose que vous connaissez et Rapid7 exécutez des analyses d'entrepôt de données ou Rapid7 InsightVM de produits dans votre environnement.

Rôle requis : admin

Les Rapid7 scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Analyser de nouveau** n'est pas disponible.

Avant de télécharger l'application Intégration des vulnérabilités Rapid7 à partir de et de ServiceNow® Store l'installer sur votre instance, consultez les informations suivantes sur les types d'intégration et les informations de configuration :

Il existe deux types d'intégrations incluses dans le Intégration des vulnérabilités Rapid7 qui est disponible dans :ServiceNow® Store

- Rapid7 InsightVM
- Rapid7 entrepôt de données

Type d'entrepôt Rapid7 de données :

- L'URL de votre serveur d'entrepôt de données et vos Rapid7 informations d'identification d'authentification sont requises
- Nécessite un serveur MID
- Utilise un pilote PostgresSQL pour exécuter des requêtes sur l'entrepôt de données
- Ne prend pas en charge plusieurs instances

Le Rapid7 InsightVM type d'intégration :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Est basé sur le cloud et utilise une API REST. Cette intégration nécessite une clé API dans votre Rapid7 compte Insight.
- Prend en charge plusieurs instances.

Consultez Configurer l'intégration de l'entrepôt de Rapid7 données (entrepôt de données) et Configurer pour l'intégration Rapid7 InsightVM pour en savoir plus sur les exigences de configuration de ces types d'intégration.

Configurer l'intégration de l'entrepôt de Rapid7 données

L'intégration Rapid7 de l'entrepôt de données est l'un des types d'intégration inclus dans le Intégration des vulnérabilités Rapid7 Intégration des vulnérabilités Rapid7.

Avant de commencer

Avant d'exécuter l'intégration de l'entrepôt de Rapid7 données, procédez comme suit :

- Obtenez le Rapid7 module complémentaire Entrepôt de données. Consultez le Rapid7 site Web et la documentation pour acquérir et installer ce module complémentaire.
- Obtenez le pilote PostgresSQL le plus récent. Accédez à https://jdbc.postgresql.org/ et téléchargez le dernier pilote.
- Un Serveur MID pour exécuter des requêtes sur l'entrepôt de données. Voir Serveur MID pour plus d'informations sur la configuration d'un Serveur MID.

  Notez le nom de l'entrepôt de données. Le Rapid7 type d'intégration d'entrepôt de données prend uniquement en charge les serveurs MID autonomes. Les serveurs MID en grappe ne sont pas pris en charge.

- Obtenez l'URL de votre serveur d'entrepôt de données et vos Rapid7 informations d'identification d'authentification et rendez-les accessibles.

Rôle requis : l'administrateur système [admin] télécharge et installe l'application. Le sn_vul.vulnerability_admin ou sn_vul.admin supervise la configuration et vérifie les résultats attendus.

Procédure

1. Connectez-vous à l'instance ServiceNow AI Platform sur laquelle vous souhaitez installer l'application Intégration des vulnérabilités Rapid7 .
2. Installez le fichier JAR PostgreSQL que vous avez téléchargé dans les tâches de configuration répertoriées précédemment.

   a. Dans votre ServiceNow AI Platform instance, accédez à **Tous** > **Serveur MID** > **Fichiers JAR**.

   b. Cliquez sur **Nouveau**.

   c. Entrez le nom du pilote PostgresSQL que vous avez téléchargé précédemment.

      Vous pouvez également saisir les informations **Version**, **Source** et **Description** . Laissez la case **à cocher Actif** cochée.

   d. Joignez le fichier JAR téléchargé à l'aide de l'icône de dans l'en-tête.

   e. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez terminé la configuration de l'intégration de l'entrepôt Rapid7 de données. Si vous n'avez pas passé en revue les exigences de l'intégration Rapid7 InsightVM , avant d'installer le Intégration des vulnérabilités Rapid7, reportez-vous à la section Configurer pour l'intégration Rapid7 InsightVM et Préparation pour le Intégration des vulnérabilités Rapid7.

Pour connaître la procédure à suivre pour obtenir des autorisations, télécharger et installer le , reportez-vous à la Intégration des vulnérabilités Rapid7 section Installer Intégration des vulnérabilités Rapid7.

Configurer pour l'intégration Rapid7 InsightVM

L'intégration Rapid7 InsightVM est l'un des types d'intégration inclus dans le Intégration des vulnérabilités Rapid7 Intégration des vulnérabilités Rapid7.

Avant de commencer

Avant d'exécuter l'intégration Rapid7 InsightVM , effectuez les tâches de configuration suivantes.

Rôle requis : l'administrateur système [admin] télécharge et installe l'application. Le sn_vul.vulnerability_admin ou sn_vul.admin supervise la configuration et vérifie les résultats attendus.

Procédure

1. Pour le type d'intégration Rapid7 InsightVM , préparez votre région et votre clé API.
   Contactez Rapid7 pour obtenir la région et la clé API appropriées.
   Vous avez terminé la configuration de l'intégration Rapid7 InsightVM . Si vous n'avez pas passé en revue les exigences relatives à l'intégration de l'entrepôt Rapid7 de Intégration des vulnérabilités Rapid7 données, reportez-vous à la section Configurer l'intégration de l'entrepôt de Rapid7 données et Préparation pour le Intégration des vulnérabilités Rapid7.
2. Pour connaître la procédure à suivre pour obtenir des autorisations, télécharger et installer le , reportez-vous à la Intégration des vulnérabilités Rapid7 section Installer Intégration des vulnérabilités Rapid7.

Installer Intégration des vulnérabilités Rapid7

Une fois que vous avez configuré les étapes de l'intégration afin qu'elle s'intègre Réponse aux vulnérabilités correctement à , obtenez les autorisations, téléchargez et installez l'application sur votre ServiceNow AI Platform® instance.

Avant de commencer

Rôle requis : admin pour le téléchargement et l'installation, sn_vuln.admin supervise la configuration et vérifie les résultats attendus.

1. Voir Préparation pour le Intégration des vulnérabilités Rapid7, Configurer l'intégration de l'entrepôt de Rapid7 données et Configurer pour l'intégration Rapid7 InsightVM pour plus d'informations sur les types d'intégration et les exigences de configuration pour le Intégration des vulnérabilités Rapid7.
2. Effectuez la liste de vérification de configuration suivante avant le téléchargement et l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.
3. Une fois l'application activée, procédez comme suit pour configurer le Intégration des vulnérabilités Rapid7.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow AI Platform pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus. Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités. • L'administrateur système [admin] installe l'application. S'il n'est pas déjà affecté, l'administrateur attribue le rôle d'administrateur de vulnérabilité [sn_vul.vulnerability_admin ou sn_vul.admin]. • L'administrateur de vulnérabilité supervise la configuration et vérifie les résultats attendus. Le Rapid7 rôle administrateur est hérité lorsqu'un rôle administrateur vous est affecté dans l'application Réponse aux vulnérabilités (VR).
Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables que vous prévoyez d'importer.	Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service client et assistance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
Configurer le filtrage	Utilisez le filtrage pour limiter le nombre d'éléments pour l'importation initiale et échelonnez votre déploiement en ajustant les filtres dans les importations suivantes.
Désactiver les calculateurs de vulnérabilité	Si vous n'utilisez pas de calculateurs de vulnérabilité, Désactiver le calculateur de vulnérabilité par défaut s'il n'est pas utilisé, en plus de tous les autres que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour, et peuvent avoir un impact sur les performances d'importation initiales.
Conserver la valeur par défaut pour l'utilisateur Exécuter en tant que	Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.
Utilisation de balises d'hôte	Si vous prévoyez d'utiliser des balises d'hôte dans Réponse aux vulnérabilités les règles de tâche d'affectation ou de rattrapage, exécutez l'intégration de la liste des actifs Rapid7 avant de créer des règles.
Dédupliquer les enregistrements de données existants	Lors de la migration du type d'intégration **Entrepôt de données** vers le type **InsightVM** , vous pouvez dédupliquer vos enregistrements d'entrepôt de données existants. Consultez Dédupliquer les enregistrements de l'entrepôt de Intégration des vulnérabilités Rapid7 données pour plus d'informations.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer l'application Intégration des vulnérabilités Rapid7 .
2. Accédez à et ServiceNow Store connectez-vous.
3. Dans , ServiceNow Store recherchez l'application Intégration des vulnérabilités Rapid7 .

   Remarque : Dans , ServiceNow Store l'application est appelée Rapid7 Integration for Security Operations Cette application nécessite un abonnement.

4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous recevrez un e-mail contenant des instructions d'installation détaillées.

9. Dans votre ServiceNow AI Platform instance, accédez à **Applications système** > **Toutes les applications** > **Tous**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Dans la boîte de dialogue Installer, votre état de dépendance s'affiche. Si vous avez besoin d'une application dépendante, l'application dont vous avez besoin s'affiche. Suivez les invites de la boîte de dialogue pour installer l'application Intégration des vulnérabilités Rapid7 sur votre instance.

> **Remarque :** L'administrateur de vulnérabilité peut maintenant terminer la configuration de l'application. Consultez Configurez la Intégration des vulnérabilités Rapid7..

Configurez la Intégration des vulnérabilités Rapid7.

Configurez le Intégration des vulnérabilités Rapid7 une fois l'application installée et activée sur votre ServiceNow AI Platform®.

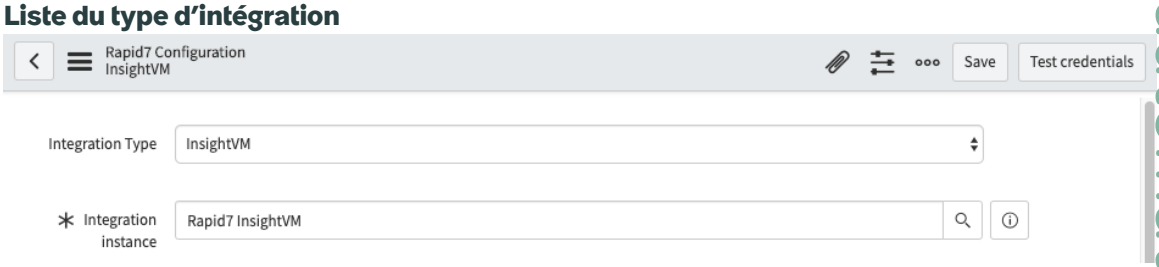
Avant de commencer

Rôle requis : l'administrateur [admin] télécharge et installe l'application. Le sn_vul.vulnerability_admin ou sn_vul.admin supervise la configuration et vérifie les résultats attendus.

Procédure

1. Une fois l'application activée (installée), accédez à **Rapid7 Vulnerability Integration** > **Administration** > **Configuration**.
2. Sélectionnez un type d'intégration dans la liste.

Liste du type d'intégration



3. Sélectionnez une instance d'intégration.
   L'instance d'intégration par défaut Rapid7 InsightVM est sélectionnée par défaut. Si c'est le type d'intégration que vous souhaitez, procédez comme suit. Si vous souhaitez configurer le type d'intégration de l'entrepôt de données, passez à l'étape Rapid7 4.

   a. Une fois l'onglet **Configuration de l'intégration** sélectionné sur le formulaire qui s'affiche, renseignez les champs suivants :

Onglet Configuration de l'intégration pour le type d'intégration InsightVM

Champ	Description
Région InsightVM	URL du serveur que vous avez acquise à partir du Rapid7 site.
Clé API	La clé API que vous avez acquise à partir de votre Rapid7 compte Insight.
État de validation	Lecture seule : état du processus de validation des informations d'identification.

   b. Vérifiez la réussite de la configuration en cliquant sur **Tester les informations d'identification**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si un message d’erreur s’affiche pendant la configuration, saisissez à nouveau vos données.

c. Après un test réussi, cliquez sur **Enregistrer**.

d. Cliquez sur l’onglet **Configuration de l’importation** .

Renseignez les champs du formulaire qui s’affiche.

Onglet Configuration de l’importation pour InsightVM

Champ	Description
Score CVSS min.	Score CVSS d’élément vulnérable minimal utilisé pour filtrer les éléments vulnérables pendant l’importation.
Score CVSS max.	Score CVSS d’élément vulnérable maximal utilisé pour filtrer les éléments vulnérables pendant l’importation.
Filtre de site	Limite les données aux Rapid7 InsightVM sites choisis dans la liste Sites. Consultez Filtrage par Rapid7 sites. Vous pouvez choisir plus d’un site. La valeur par défaut (vide) affiche tous les sites. Pour préremplir la liste Sites, exécutez l’API Intégration de site Rapid7 avant de définir ce champ. Pour plus d’informations sur l’utilisation du filtrage de site, reportez-vous à la section Filtrage par Rapid7 sites.
Créer automatiquement une entrée CVE	La propriété système permettant de créer une entrée CVE est active (vrai) par défaut. Les espaces réservés CVE sont créés automatiquement avec l’ingestion de connaissances Rapid7 si l’ID CVE n’existe pas. Si vous souhaitez que cette fonctionnalité soit inactive, désactivez la propriété [sn_vul_r7.create_cve_for_vulnerabilities] à partir de la liste Propriétés système.
Réouverture résolue par âge	Lorsque cette option est sélectionnée, les éléments vulnérables sont automatiquement rouverts lorsque le nombre de jours pendant lesquels ils ont été résolus mais non fermés correspond à la valeur affichée dans le champ **Réouverture résolue après** .

e. Cliquez sur **Enregistrer**.

Pour plusieurs déploiements de type Rapid7 InsightVM intégration :

f. Dans le champ **Instance d’intégration** , ouvrez dans la liste de recherche et sélectionnez une instance d’intégration existante ou cliquez sur **Nouveau** dans le menu contextuel.

g. Pour **Nouveau**, saisissez un **nom** pour l’instance d’intégration et cliquez sur **Soumettre**.
Le type d’intégration apparaît dans le formulaire de Rapid7 configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez supprimer n'importe quelle instance d'intégration, à l'exception de l'instance par défaut. La suppression d'une instance supprime les éléments suivants (à l'exception des VI) :

- Intégrations
- Paramètres d'instance
- Exécutions des intégrations
- Processus d'intégration
- La colonne d'instance sur le VI est marquée comme vide

h. Vérifiez la réussite de la configuration en cliquant sur **Tester les informations d'identification**.

i. Après un test réussi, cliquez sur **Enregistrer**.

4. Dans le champ Type d'intégration, développez la liste et cliquez sur **Entrepôt de données**.

a. Sélectionnez l'onglet **Configuration de l'intégration** .

Renseignez les champs du formulaire qui s'affiche.

Onglet Configuration de l'intégration pour le type d'intégration Entrepôt de données

Champ	Description
Nom d'identification JDBC	Nom de vos informations d'identification d'entrepôt de données.
Nom d'utilisateur	Nom d'utilisateur de l'entrepôt de données Rapid7.
Mot de passe	Mot de passe de l'entrepôt de données Rapid7.
État de validation	Lecture seule : état du processus de validation des informations d'identification.
Détail de validation	Lecture seule : entrepôt de données uniquement. Affiche des informations supplémentaires sur le contrôle de validation après avoir cliqué sur Tester les informations d'identification au moins une fois. Cela peut être utile pour déboguer votre configuration (par exemple, valider si votre serveur MID est mal configuré ou si vous avez simplement des informations d'identification incorrectes.
Serveur de base de données DNS/ IP	Adresse DNS ou IP de votre entrepôt de données.
Port de la base de données	Port à utiliser pour l'intégration de votre entrepôt de données.
Nom de base de données	Nom de votre entrepôt de données.
Décalage du retard de données (en jours)	Le décalage du retard de données tient compte du délai entre les données en temps réel dans le Rapid7 Nexpose scanner et les données dans l'entrepôt de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Serveur MID	Serveur MID à utiliser. Seuls les MID Servers autonomes sont pris en charge. Les serveurs MID en grappe ne sont pas pris en charge.
Délai d'expiration du serveur MID (min)	Nombre de minutes à attendre la réponse du serveur MID avant expiration de l'exécution de l'intégration.

b. Vérifiez la réussite de la configuration en cliquant sur **Tester les informations d'identification**.

c. Après un test réussi, cliquez sur **Enregistrer**.

d. Cliquez sur l'onglet **Configuration de l'importation** .

Renseignez les champs du formulaire qui s'affiche.

Onglet Configuration de l'importation pour l'entrepôt de données

Champ	Description
Avant la version 12.0 : case à cocher Créer une entrée CVE	Lorsque cette option est cochée, les espaces réservés pour les CVE, qui ne sont pas déjà présents, sont créés en tant qu'enregistrements NVD et référencés dans l'entrée tierce pour Rapid7. Lorsque cette option n'est pas cochée, ces CVE sont ignorées.
Score CVSS min.	Score CVSS d'élément vulnérable minimal utilisé pour filtrer les éléments vulnérables pendant l'importation.
Score CVSS max.	Score CVSS d'élément vulnérable maximal utilisé pour filtrer les éléments vulnérables pendant l'importation.
Filtre de site	Limite les données d'intégration de sites importées aux sites choisis. Vous pouvez en choisir plusieurs. **Remarque :** Étant donné que le paramètre par défaut consiste à importer des données à partir de tous les sites, vous n'avez pas besoin d'utiliser le filtre si vous voulez tous les sites. Cela ralentit la demande.
Réouverture résolue par âge	Lorsque cette option est sélectionnée, les éléments vulnérables sont automatiquement rouverts lorsque le nombre de jours pendant lesquels ils ont été résolus mais non fermés correspond à la valeur affichée dans le champ **Réouverture résolue après** .

5. Cliquez sur **Enregistrer**.

6. Facultatif : Si vous souhaitez définir une date de début dans les Rapid7 enregistrements Intégration de vulnérabilité - API et Intégration d'élément vulnérable - Intégration Rapid7 - Intégration API pour récupérer les données historiques lors de votre importation initiale à partir de l'analyse Rapid7 , procédez comme suit. Vous pouvez utiliser ces données pour vous aider avec Fermeture des détections obsolètes dans Réponse aux vulnérabilités.

a. Accédez à la **Rapid7 Vulnerability Integration** > **Administration** > **Intégrations**.
La Rapid7 liste des intégrations s'affiche.

b. Cliquez sur l'un des enregistrements d'intégration pour l'ouvrir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(Optional) En haut du formulaire, cliquez sur le lien **ici** pour modifier l'enregistrement.

Le champ **Date d'importation depuis** les Rapid7 intégrations est vide par défaut, à l'exception de l'API et de l'API Rapid7 d'intégration des éléments vulnérables Rapid7. Pour ces intégrations, ces champs sont définis sur 1998-12-31 ou 1999-01-01.

Pour récupérer les données historiques lors de votre importation initiale à partir de l'analyse Rapid7 , définissez une date de début dans les enregistrements d'intégration appropriés. Ce processus fonctionne pour toute Rapid7 intégration, à l'exception des éléments suivants :

- Les Rapid7 intégrations Exploit et Malware Kit n'affichent pas le champ **Importer depuis** , car elles n'effectuent pas de mises à jour delta et n'utilisent donc pas ce champ.
- L'intégration Rapid7 de la liste des actifs ignore le champ, car son intention est de récupérer toutes les données.
- Pour l'exécution initiale de l'API Rapid7 InsightVM d'intégration complète des éléments vulnérables lorsque le module Fermer automatiquement les éléments vulnérables périmés est activé et que le champ **Importer depuis** est laissé vide.

  Lorsque vous activez la fonctionnalité de fermeture automatique, une exécution réussie à partir de l'intégration complète des éléments vulnérables Rapid7 ou de l'API d'intégration complète des éléments vulnérables Rapid7 est requise. Ces intégrations sont désactivées par défaut.

  Lorsque vous activez l'API Rapid7 InsightVM d'intégration complète des éléments vulnérables, si vous laissez le champ **Importer depuis** vide sur la page de configuration de l'intégration, la valeur du champ « **jours plus tôt** » du formulaire Fermer automatiquement les éléments vulnérables périmés est également utilisée pour la date d'importation **depuis** lors de la première exécution de l'intégration. La valeur par défaut pour Fermer automatiquement les éléments vulnérables périmés est de (90 jours).

  Par exemple, si le champ **jours plus tôt** du formulaire Fermer automatiquement les éléments vulnérables périmés est 90 et que le champ **Importer depuis** de la page Intégration complète des éléments vulnérables Rapid7 - Configuration de l'API est vide, la première exécution de l'intégration importe les données des 90 derniers jours.

  Cette relation entre les champs **Importer depuis** et **jours plus tôt** s'applique uniquement à la première exécution de l'intégration. Après cela, la modification du champ **jours plus tôt** sur le formulaire Fermer automatiquement les éléments vulnérables périmés n'affecte pas le champ **Importer depuis** de la page Intégration complète des éléments vulnérables Rapid7 - Configuration de l'API. Le champ est modifié à l'heure de début de la première exécution afin que les exécutions d'intégration suivantes importent uniquement les informations delta

  Le champ **Importer depuis** est modifiable et vous pouvez saisir les valeurs que vous voulez pour chacune des intégrations.

7. Accédez à la **Tous** > **sn_sec_int_impl.liste** > **Rapid7 InsightVM**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Le paramètre **d'instance** d'intégration import_startime_buffer_comprehensive définit un délai tampon de 24 heures avant l'heure spécifiée dans le champ **Importer depuis** afin que les actifs analysés à partir de ce délai tampon soient récupérés pendant l'exécution de l'intégration **complète des éléments vulnérables Rapid7 -** intégration de l'API.
Vous pouvez modifier ce temps tampon en fonction de vos besoins.

b. **Facultatif :** Définissez le paramètre **close_stale_detections** sur *vrai* pour fermer les détections périmées qui ne proviennent plus de l'API Rapid7 pour les actifs qui sont analysés et récupérés via l'API Rapid7 via **l'intégration complète des éléments vulnérables (API) Rapid7**.

Vous avez terminé avec succès les étapes d'installation, d'installation et de configuration pour le Intégration des vulnérabilités Rapid7. Vous êtes maintenant prêt à examiner et à vérifier les données importées.

Que faire ensuite

Les Rapid7 scanners et Qualys sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Analyser de nouveau** n'est pas disponible.

Pour activer ces scanners, en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin :

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Recherchez le produit de scanner que vous souhaitez activer et cliquez sur l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher Activé.
4. Cliquez sur **Mettre à jour**.

   Le produit que vous avez activé s'affiche dans le champ Source sur les enregistrements d'élément vulnérable et de tâche de rattrapage après la prochaine importation, et **Analyser à nouveau** est disponible en tant qu'action d'interface utilisateur.

Si votre environnement nécessite des importations séparées par domaine, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

Pour créer ou affiner vos règles de recherche avant l'importation, reportez-vous à la section Créer une règle de recherche de CI de réponse aux vulnérabilités.

Filtrage par Rapid7 sites

Filtrez par site pour Rapid7 InsightVM les types d'intégration ainsi que Rapid7 Nexpose pour les types d'intégration d'entrepôt de données.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Remarque : L'utilisation du filtrage de site peut avoir un impact sur les performances. Pour plus d'informations sur les performances et d'autres considérations avant d'utiliser le filtrage de site, consultez KB0789221 .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

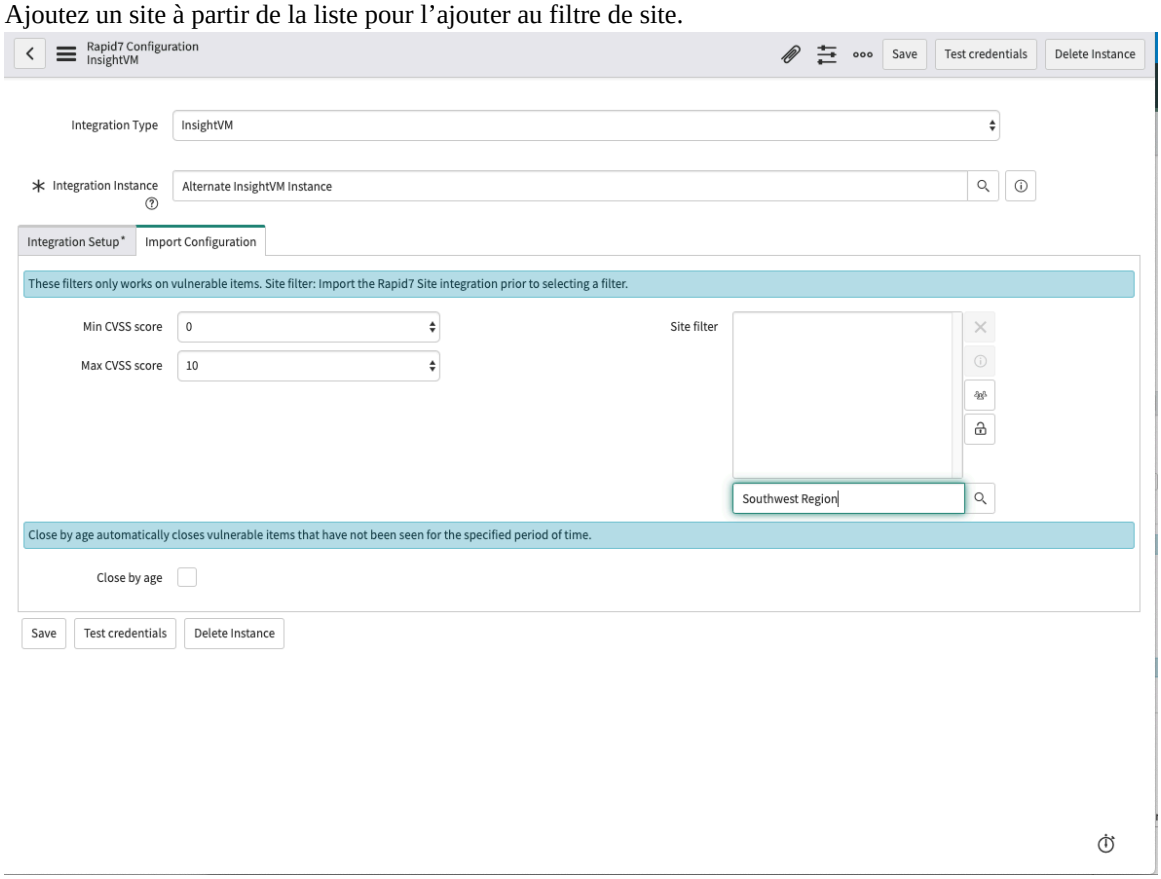
Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tous** > **Rapid7 Vulnerability Integration** > **Configuration**.
2. Sélectionnez une instance d'intégration.
3. Cliquez sur l'onglet **Configuration de l'importation** .

> **Remarque :** Si vous voulez tous les sites, laissez le champ de filtre de site vide. Aucun filtre de site n'équivaut à ajouter tous les sites.
>
> Les sites sont spécifiques à l'instance d'intégration. La liste de recherche pour le filtrage de site affiche les deux sites et les Rapid7 InsightVMRapid7 Nexpose sites d'instance d'intégration d'entrepôt de données. Assurez-vous que le site que vous choisissez correspond à l'instance d'intégration que vous avez sélectionnée. Par exemple, si vous choisissez un site d'entrepôt de données, ce site ne fonctionnera pas par erreur pour le filtrage de site par Rapid7 InsightVM.

4. Cliquez sur la liste de recherche pour afficher les enregistrements de site de l'instance d'intégration actuelle.
5. Ajoutez un site à partir de la liste pour l'ajouter au filtre de site.



6. Répétez la sélection pour ajouter d'autres sites.
7. Cliquez sur **Enregistrer**.
   Ces sites sont utilisés pour filtrer par site lors de la prochaine importation. Voir Ajoutez SITE à vos balises de site Rapid7 InsightVM pour plus d'informations sur l'ajout du préfixe SITE aux données de votre site.

Ajoutez SITE à vos balises de site Rapid7 InsightVM

Ajoutez le préfixe, SITE, à vos Rapid7 InsightVM balises de site pour les mettre en évidence parmi votre liste de balises.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Remarque : Si nécessaire, changez votre champ d'application pour l'intégration Rapid7 pour Security Operations.

Procédure

1. Dans la zone de navigation de gauche, tapez : *`sys_properties.list`*.
2. Sous **Nom**, recherchez : *`sn_vul_r7.prefix_site_to_rapid7_tags`*.
3. Ouvrir *`sn_vul_r7.prefix_site_to_rapid7_tags`*.
4. Changer la **valeur** en **vrai**.
5. Cliquez sur **Mettre à jour**.
   Les balises de site nouvelles et existantes sont préfixées lors de l'importation suivante de Rapid7 InsightVM.

Intégration des vulnérabilités Rapid7 Graphique d'état d'exécution

Rapid7 Nexpose Les capteurs collectent les données et les envoient automatiquement aux produits OR Rapid7 NexposeRapid7 InsightVM , qui analysent et corrèlent en permanence les informations.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à surveiller la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en affichant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Consultez Réponse aux vulnérabilités Espaces de travail et Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Intégration des vulnérabilités Rapid7 fonctionne facilement avec pour Réponse aux vulnérabilités mapper les vulnérabilités aux CI et aux services d'entreprise afin de déterminer l'impact et la priorité des menaces potentiellement malveillantes. Le Intégration des vulnérabilités Rapid7 module État d'exécution est une vue graphique de l'état des Intégration des vulnérabilités Rapid7 exécutions.

Pour afficher ces données dans la vue héritée, accédez à **Tous** > **Toutes les intégrations de vulnérabilité Rapid7** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions précédentes de Réponse aux vulnérabilités

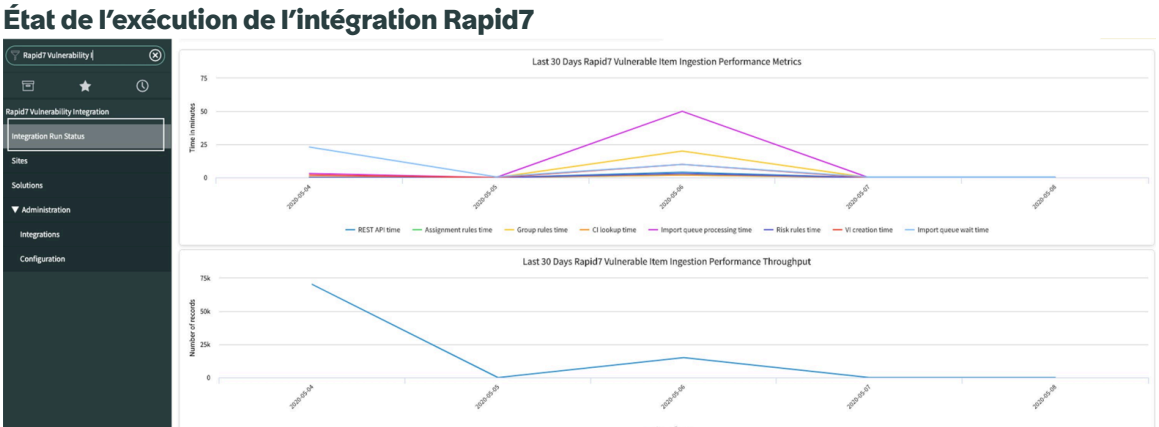
Dans le graphique, pointez sur n'importe quelle partie (barre, secteur, point de données, etc.) pour afficher des données générales spécifiques à cette partie. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Plusieurs facteurs peuvent avoir un impact sur les performances de l'exécution de l'intégration, comme la quantité de données et le temps nécessaire pour traiter ces données. Deux nouveaux graphiques ont été ajoutés pour comparer les mesures de performance :

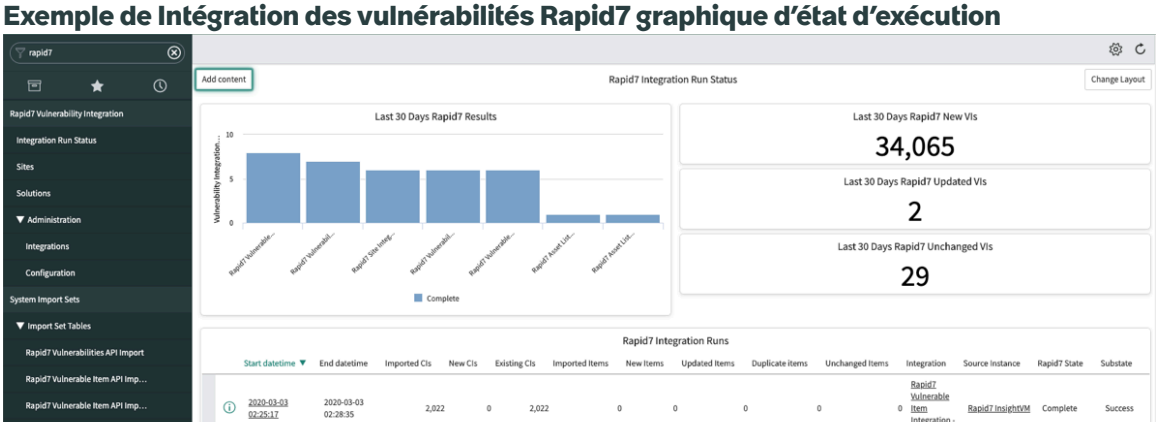
- Rapid7 Mesures de performance d'ingestion d'élément vulnérable : comparez les mesures de performances quotidiennes pour les règles d'affectation, les règles de groupe, les règles de risque, le temps d'attente de la file d'attente, le temps de traitement de la file d'attente et d'autres statistiques relatives aux éléments vulnérables au cours des 30 derniers jours, afin d'identifier la cause de tout écart de performance.
- Rapid7 Débit de performance d'ingestion d'élément vulnérable : comparez le débit quotidien d'ingestion d'éléments vulnérables pour l'API d'intégration Rapid7 des éléments vulnérables. Le débit est mesuré en éléments par heure.

Remarque : Dans Rapid7, ces graphiques ne sont pris en charge que pour l'intégration de l'ordinateur virtuel Insight.

État de l'exécution de l'intégration Rapid7



Exemple de Intégration des vulnérabilités Rapid7 graphique d'état d'exécution



- La valeur de la colonne Éléments importés représente le nombre total d'éléments vulnérables créés à partir d'une exécution d'intégration.
- La colonne Nouveaux éléments affiche le nombre d'éléments vulnérables créés à partir d'une exécution d'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La colonne Éléments en double n'est plus renseignée. Vous préférez peut-être supprimer cette colonne de l'affichage.
- La colonne Éléments mis à jour affiche le nombre de fois où les éléments vulnérables sont mis à jour au cours d'une exécution de l'intégration. Cette valeur n'est pas le nombre d'éléments vulnérables uniques qui sont mis à jour. Si, par exemple, un élément vulnérable est mis à jour deux fois pendant l'exécution de l'intégration, il est compté deux fois et affiché sous la forme de 2 éléments mis à jour.
- La colonne Éléments inchangés affiche les éléments vulnérables trouvés pendant l'exécution de l'intégration qui existent déjà dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Remarque : L'intégration s'exécute sans résultat pour les quatre valeurs suivantes : **Nouveaux CI**, **CI existants**, **Nouveaux éléments** et **Éléments mis à jour** sont exclus de la liste **des exécutions d'intégration Rapid7** .

Intégration des vulnérabilités Rapid7 Rapports des graphiques d'état d'exécution

Nom	Description
Résultats des 30 derniers jours Rapid7	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Exécuter dans un visuel de barre.
Nouveaux VI au cours des 30 derniers jours Rapid7	Nombre de nouveaux éléments vulnérables importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour au cours des 30 derniers jours Rapid7	Nombre d'éléments vulnérables mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Doublons des 30 derniers jours Rapid7	Nombre d'éléments vulnérables en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Rapid7 Exécutions des intégrations	Les enregistrements d'exécution de l'intégration dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection dans la `sn_vul_detection` table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, une fois l'exécution de l'intégration terminée.
Mesures de performance d'ingestion d'élément vulnérables au cours des 30 derniers jours Rapid7	Mesures des performances quotidiennes des éléments vulnérables comparées aux 30 derniers jours.
Rendement de performance d'ingestion d'élément vulnérable au cours des 30 derniers jours Rapid7	Débit quotidien d'ingestion d'éléments vulnérables pour l'API Rapid7 Vulnerable Item Integration mesuré au cours des 30 derniers jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher le tableau de bord de l'état des exécutions d'importation Intégration des vulnérabilités Rapid7

Utilisez le Rapid7 tableau de bord de l'état d'exécution de l'importation de vulnérabilités pour vérifier le succès de vos exécutions d'intégration, localiser les problèmes et prendre des décisions éclairées en matière de correction.

Avant de commencer

Rôles requis : sn_vuln.admin

Pourquoi et quand exécuter cette tâche

Cette procédure fait les hypothèses suivantes.

- Vous avez Réponse aux vulnérabilités et le Intégration des vulnérabilités Rapid7 installé et configuré.
- Intégration des vulnérabilités Rapid7 Les importations sont planifiées et en cours d'exécution.
- Rapid7 Les graphiques d'état d'exécution de l'intégration sont en cours d'utilisation.

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 19.0 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à cœur) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Rapid7** > **État de l'exécution de l'intégration**.

   À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

   Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

2. Si vous n'utilisez pas le graphique de l'état d'exécution de l'intégration Rapid7 , accédez à **Rapid7** > **Intégrations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Choisissez une intégration.

b. Cliquez sur la liste connexe **Exécutions d'intégration de vulnérabilité** .

3. Vérifiez que toutes les importations ont réussi.

Trouble?

Les causes les plus courantes d'un échec d'exécution :

- Interruption du réseau
- Décroissance des bits dans le transfert de données entraînant des données corrompues pendant la transformation

Pour toutes ces conditions, cliquez sur **Exécuter maintenant** et réexécutez l'intégration.

Dédupliquer les enregistrements de l'entrepôt de Intégration des vulnérabilités Rapid7 données

Lors de la migration vers le type d'intégration **InsightVM** à partir du type d'intégration **Entrepôt de données** , vous pouvez dédupliquer les éléments vulnérables de l'entrepôt de données existants tant qu'ils appartiennent aux mêmes données sources que vos Rapid7 InsightVM données.

Avant de commencer

Rôle requis : sn_vul_r7.admin, sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Cette déduplication fonctionne uniquement lors de la migration de l'entrepôt Rapid7 Nexpose de données vers l'intégration Rapid7 InsightVM des éléments vulnérables.

Procédure

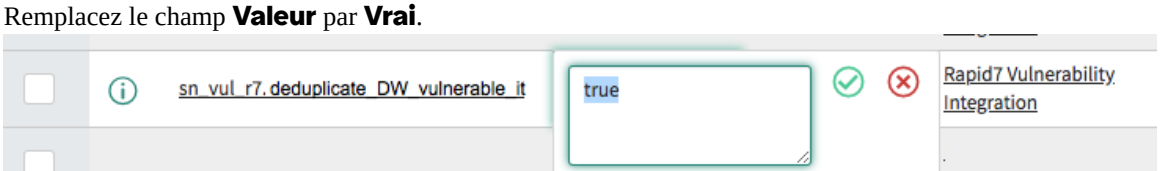
1. Accédez à la **Tous** > **Rapide 7** > **Intégrations**.

2. Définissez tous les paramètres de colonnes **actives** sur toutes les Rapid7 Nexpose intégrations d'entrepôt de données sur **Faux**, ce qui désactive les intégrations.

3. Entrez sys_properties.list dans le panneau de navigation de gauche.

4. Recherchez le **nom** : sn_vul_r7.deduplicate_DW_vulnerable_item.

5. Remplacez le champ **Valeur** par **Vrai**.



6. Cliquez sur l'icône de coche verte .
Lors de la prochaine Rapid7 InsightVM importation d'intégration d'élément vulnérable, toute correspondance avec les enregistrements d'entrepôt de données existants empêche la création d'un élément vulnérable en double.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lancer une nouvelle analyse pour l'intégration de vulnérabilité Rapid7

Lancez de nouvelles analyses dans la Rapid7 plateforme pour vérifier que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés.

Avant de commencer

Remarque : Les nouvelles analyses pour Rapid7 les éléments vulnérables de l'entrepôt de données ne sont pas prises en charge.

Vous pouvez lancer de nouvelles analyses à partir des espaces de travail Réponse aux vulnérabilités. Pour plus d'informations, consultez Analyser de nouveau les enregistrements et les tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT.

Rôles requis : Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Pourquoi et quand exécuter cette tâche

Pour les nouvelles analyses dans l'environnement classique, reportez-vous aux sections suivantes.

Les nouvelles analyses sont prises en charge. Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables importés depuis Rapid7 InsightVM les intégrations de votre ServiceNow AI Platform® instance.

Remarque : Le Rapid7 scanner est désactivé par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont Rapid7 l'application comme source, le bouton Analyser de nouveau n'est pas disponible.

Pour réduire les frais généraux et le volume liés aux analyses complètes planifiées, les propriétaires de rattrapages, les spécialistes informatiques, les analystes de vulnérabilité ou les gestionnaires de vulnérabilité peuvent lancer de nouvelles analyses ciblées à la demande pour détecter des vulnérabilités spécifiques sur les actifs (éléments de configuration) de leurs environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de rattrapage (RT), d'entrée tierce (TPE) ou d'éléments découverts à partir de votre ServiceNow AI Platform® instance.

Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, correctifs et autres actions ont correctement corrigé des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Par exemple, l'ensemble de votre environnement est analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été terminée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines pour la prochaine analyse planifiée afin de vérifier qu'elle a été corrigée. Pour vérifier que votre correctif a corrigé avec succès une vulnérabilité critique découverte lors d'une analyse précédente, vous pouvez lancer une nouvelle analyse ciblée à partir de votre ServiceNow AI Platform pour rechercher Rapid7 les éléments vulnérables. Vous pouvez afficher les résultats mis à jour sur vos éléments vulnérables avec la prochaine importation planifiée de Vulnérabilité et Intégrations d'éléments Rapid7 InsightVM vulnérables.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

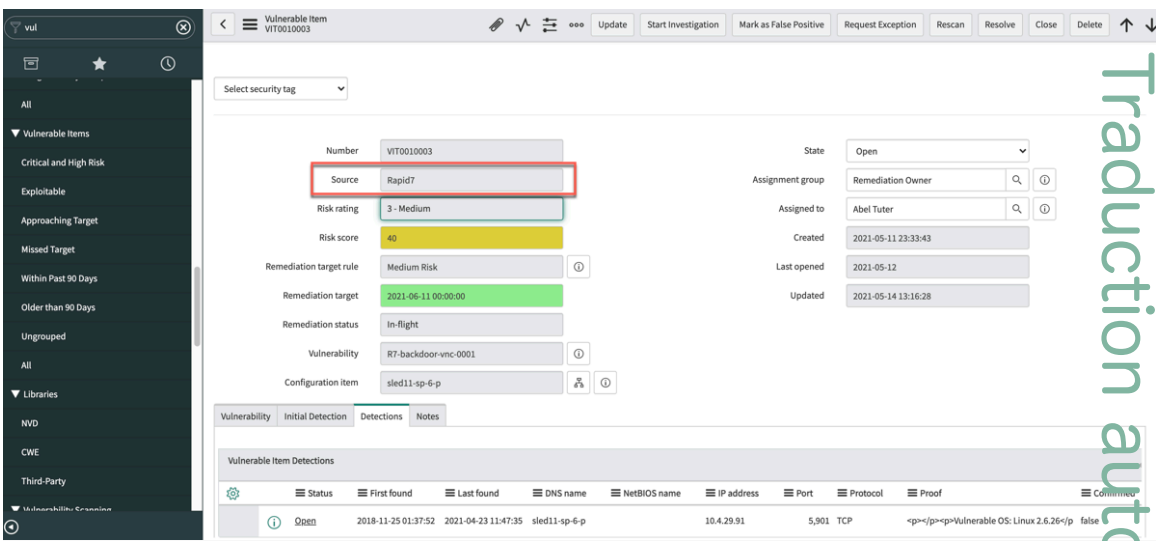
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lancez de nouvelles analyses pour les VI ayant Rapid7 comme source. Vérifier Rapid7 s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le générateur de conditions pour regrouper les VI par source. Ou, si la colonne **Source** n'est pas affichée dans la vue de liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône d'engrenage et déplacez la **source** de **Disponible** à **Sélectionnée**.

Lorsque vous lancez de nouvelles analyses, évitez de déclencher simultanément des analyses pour un ID source à partir de plusieurs sources. La dernière demande d'analyse générera une erreur.

Par exemple, si vous lancez une nouvelle analyse d'un élément vulnérable à partir d'un enregistrement de VI et que vous demandez également une autre analyse à partir d'un enregistrement de tâche de rattrapage qui contient ce même élément vulnérable, il est probable que la deuxième demande échoue.



3. Vous pouvez également accéder à **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **tiers** pour la tâche de rattrapage ou les enregistrements d'entrée tierce, respectivement, que vous souhaitez utiliser pour la nouvelle analyse.

   Selon votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

   - Sur un enregistrement de VI unique, l'élément vulnérable doit provenir du Rapid7 produit et se trouver dans un état autre que Fermé. Pour plusieurs enregistrements de VI, tous les VI que vous sélectionnez dans la vue de liste doivent provenir du Rapid7 produit et dans un état autre que Fermé.
   - Sur un enregistrement de tâche de rattrapage, la tâche de rattrapage peut être dans n'importe quel état autre que Fermé et tous les VI associés doivent provenir du Rapid7 produit.
   - Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du Rapid7 produit dans un état autre que Fermé.
   - Sur un enregistrement d'élément détecté, l'élément vulnérable doit provenir du Rapid7 produit et se trouver dans un état autre que **Fermé**.

4. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour les vues de listes, sélectionnez les éléments vulnérables de la liste que vous souhaitez analyser à nouveau et, dans la liste **Action sur les lignes sélectionnées** , sélectionnez **Analyser à nouveau**.

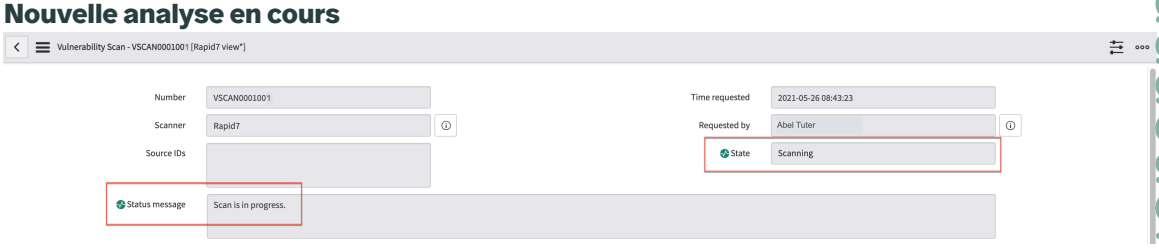
5. Dans la fenêtre contextuelle qui s'affiche, confirmez la nouvelle analyse.
   Un message s'affiche indiquant que votre analyse est en cours de traitement (**mise en file d'attente**). Dans le message, cliquez sur le lien **Afficher les détails** pour vérifier l'état de la nouvelle analyse (analyse enfant) et affichez toutes les autres nouvelles analyses lancées à partir de l'enregistrement. L'état de toutes les nouvelles analyses se trouve à tout moment dans la liste connexe Analyses au bas des enregistrements de VI, de tâche de rattrapage, de TPE et d'éléments détectés que vous utilisez pour lancer les nouvelles analyses.

   Lorsque l'analyse est en cours, le champ État passe à **Analyse** et le champ Message d'état affiche **L'analyse est en cours**.

   Remarque : Chaque nouvelle analyse prend en charge 500 actifs par analyse. Si votre demande comporte plus de 500 actifs, davantage d'analyses enfants sont demandées.

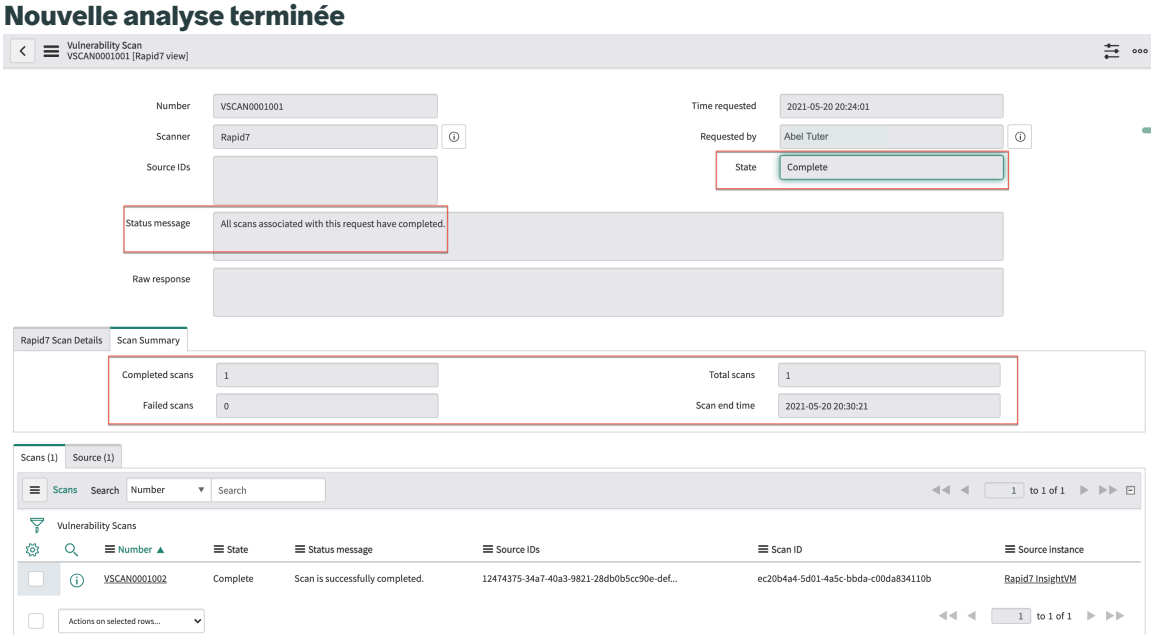
   Votre ServiceNow AI Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité.

Nouvelle analyse en cours



   Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform® votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée. Tous les VI qui sont passés ou passeront à l'état Fermé/Corrigé sont importés lors de la prochaine importation planifiée des Rapid7 intégrations.

Nouvelle analyse terminée



   Vous pouvez également lancer une nouvelle analyse sur demande pour une vulnérabilité spécifique sur un actif spécifique. Vous pouvez afficher les résultats de ces analyses

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

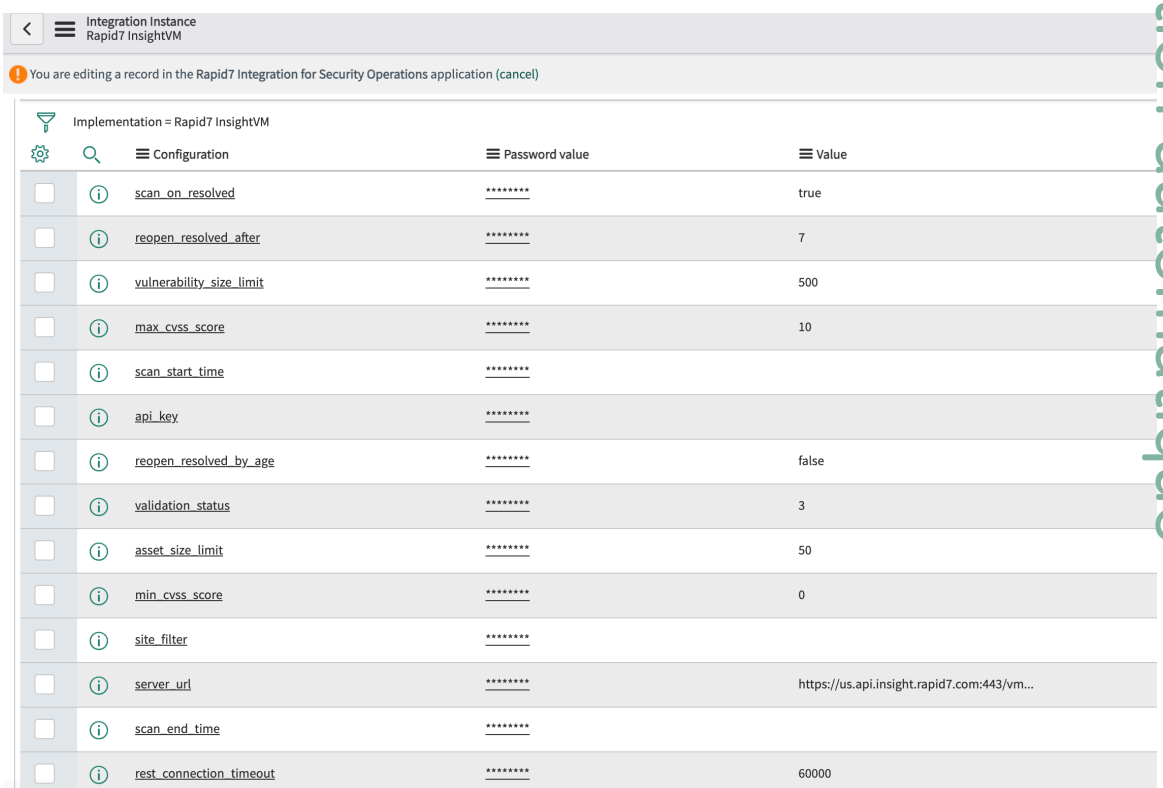
une fois l'analyse terminée sur le VI actualisé, la tâche de rattrapage, le TPE et les enregistrements d'éléments détectés à partir desquels vous avez lancé l'analyse.

La valeur du champ État sur les enregistrements d'analyse de vulnérabilité est importée de Rapid7. Lorsque l'analyse est terminée avec succès, l'état est défini sur Terminé. Si l'analyse ne se termine pas correctement, une valeur d'erreur s'affiche.

Analyses automatiques et analyses planifiées

En tant que gestionnaire ou analyste des vulnérabilités, vous pouvez spécifier et planifier le moment où de nouvelles analyses sont lancées pour les VI et les RT. Vous pouvez également activer les analyses automatiques pour les VI et les tâches de rattrapage qui sont définies pour être résolues.

6. Pour modifier les paramètres d'intégration sur l'instance d'intégration, accédez à **Rapid7 Vulnerability Integration** > **Administration** > **Configuration**.
7. Dans l'enregistrement de configuration Rapid7, s'il n'est pas sélectionné, dans la liste **Type d'intégration**, sélectionnez **Rapid7 InsightVM.**
8. À droite du champ **Instance d'intégration** , cliquez sur l'icône d'informations, puis sur **Enregistrement ouvert**.
9. Sur l'enregistrement Rapid7 InsightVM de l'instance d'intégration, localisez les paramètres de planification des analyses et modifiez-les si nécessaire.



scan_on_resolved Indique si l'analyse est lancée lorsqu'une vulnérabilité est résolue. La valeur par défaut est **faux** (désactivé).

Si ce paramètre est défini sur vrai, chaque fois qu'un VI ou un RT est défini sur Résolu, le workflow pour réanalyser le VI et la tâche de rattrapage respectifs est déclenché automatiquement.

scan_start_time

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définissez l'heure de début de l'analyse au **format HH :mm** (format 24 heures) dans le fuseau horaire UTC pour l'heure de début de la fenêtre dans laquelle vous souhaitez que les nouvelles analyses soient disponibles.

La valeur par défaut est 00:00.

scan_end_time

Définissez l'heure de fin de l'analyse au **format HH :mm** (format 24 heures) dans le fuseau horaire UTC pour l'heure de fin de la fenêtre d'analyse disponible.

La valeur par défaut est 23:59.

Si une analyse est lancée dans la fenêtre de temps prévue, elle se lance instantanément. Si l'analyse est lancée en dehors de la fenêtre, elle est mise en file d'attente pour la fenêtre planifiée suivante.

Par exemple, si vous entrez une heure de début de 00h00 pour le *scan_start_time* paramètre et une *scan_end_time* heure de 10h00 le matin même, les analyses planifiées ou lancées manuellement en dehors de la fenêtre horaire de minuit à 10h sont mises en file d'attente et lancées à l'heure de début de la fenêtre horaire du jour suivant 00:00.

Dans le même exemple, si vous lancez manuellement une nouvelle analyse à 11h00, la nouvelle analyse n'est pas immédiatement lancée, car elle se trouve en dehors des heures d'analyse configurées disponibles. La demande d'analyse reste en file d'attente jusqu'au début de la fenêtre horaire du jour suivant, dans cet exemple 00:00.

Définir des paramètres de filtre supplémentaires pour Rapid7 InsightVM les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec le Intégration Rapid7 pour Opérations de sécurité pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec le Rapid7 InsightVM produit.

Avant de commencer

Cas d'utilisation : en tant que gestionnaire ou analyste de vulnérabilités, vous pouvez filtrer les données de vos requêtes afin de pouvoir examiner uniquement des détails de vulnérabilité spécifiques. Par exemple, vous pouvez afficher uniquement les vulnérabilités importées qui sont critiques et graves.

Pour vous aider à collecter ces données, vous ajoutez Rapid7 des paramètres pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, à partir de la version 13.4, la fonctionnalité vous permet de personnaliser vos informations de requête HTTP avec Rapid7 InsightVM les paramètres de votre ServiceNow AI Platform. Les intégrations suivantes Rapid7 InsightVM prennent en charge le filtrage en ajoutant du contenu JSON dans le corps de la demande :

- Rapid7 InsightVM Élément vulnérable API d'intégration
- Rapid7 InsightVM API d'intégration de vulnérabilité
- Rapid7 InsightVM

Vous devez savoir comment utiliser JSON les chaînes pour cette fonctionnalité.

Rôle requis : sn_vul.vulnerability_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Recherchez les paramètres pris en charge par le Rapid7 InsightVM produit sur le site développeur Rapid7 que vous souhaitez utiliser pour votre filtrage.

   Vous pouvez créer les paramètres du corps de la demande en vous reportant à la Rapid7 documentation. Les paramètres et les valeurs que vous saisissez à partir du Rapid7 InsightVM produit ne sont pris en charge qu'au niveau de l'instance d'intégration.

2. Accédez à la **Tous** > **Rapid7 Vulnerability Integration** > **Administration** > **Intégrations**.
3. Sur la page de liste Intégrations Rapid7, cliquez sur l'enregistrement de l'intégration pour laquelle Rapid7 InsightVM vous souhaitez l'ouvrir.
4. À droite de la page, cliquez sur l'icône d'informations (I) pour le message REST, puis sur **Ouvrir l'enregistrement**.
5. Avec l'onglet Demande HTTP sélectionné, sous Méthodes HTTP, dans la colonne Nom, cliquez sur un élément pour ouvrir ses paramètres de requête HTTP.
6. Sous Enregistrement de méthode HTTP, sous Paramètres de requête HTTP, dans le champ Contenu, entrez les valeurs de paramètres que vous avez trouvées sur le site développeur Rapid7 .

   Dans l'image suivante, la chaîne de gravité est ajoutée.



   Si vous souhaitez entrer plusieurs paramètres, consultez la documentation pour plus d'informations sur la Rapid7 façon de séparer chaque valeur.

7. Cliquez sur **Mettre à jour**.

Présentation de l'intégration de Shodan Exploit

L'application ServiceNow® Shodan Exploit Integration utilise les Shodan données importées du moteur de recherche pour vous aider à déterminer l'impact et la priorité des exploits potentiellement malveillants.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Shodan Exploit Integration

Le Shodan moteur de recherche collecte les données d'exploitation et l'API Shodan met cette base de données à la disposition du ServiceNow AI Platform®. Il s'intègre facilement à l'application ServiceNow® Réponse aux vulnérabilités pour mapper les exploits aux vulnérabilités tierces, enrichissant ainsi les données d'exploitation de votre instance.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Chaque jour, les travaux planifiés appellent automatiquement les intégrations dans l'ordre dans lequel elles sont répertoriées. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Versions disponibles

Version de mise en production pour Zurich	Notes de publication
Intégration d'exploit Shodan v10.6, 10.7	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Rôles

Shodan Les tâches d'intégration d'exploits impliquent les rôles suivants.

- sn_vul_shodan.admin : les utilisateurs disposant de ce rôle peuvent lire, écrire et supprimer des enregistrements.
- sn_vul_shodan.user : les utilisateurs disposant de ce rôle peuvent lire et écrire des enregistrements.
- sn_vul_shodan.read : les utilisateurs disposant de ce rôle peuvent lire les enregistrements.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Intégrations d'exploits Shodan

Pour afficher les intégrations d'exploits Shodan , accédez à **Tous** > **Shodan Exploit Integration** > **Intégrations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les intégrations suivantes sont incluses dans le système de base. Ces intégrations sont actives par défaut.

Intégrations d'exploits Shodan

Intégration	Description
Intégration Shodan ExploitDB	Récupère les données ExploitDB à partir de vos données de Shodan vulnérabilité tierces et les enrichit. Cette intégration devrait s'exécuter quotidiennement à 03:15:00.
Intégration de Shodan Metasploit	Récupère les informations Metasploit à partir de vos données de Shodan vulnérabilité tierces et les enrichit. Cette intégration est définie pour s'exécuter quotidiennement à 01:15:00.

Pour modifier l'heure de début par défaut des importations d'intégration planifiées, reportez-vous à la section Définir le Shodan temps d'importation de l'intégration de l'exploit.

Pour afficher les données d'exploitation dans les vulnérabilités tierces, reportez-vous à la section Afficher les Réponse aux vulnérabilités bibliothèques de vulnérabilités.

La modification d'autres paramètres d'Exploit Integration nécessite une Shodan expertise avancée ServiceNow et Réponse aux vulnérabilités dépasse le cadre de la documentation du produit.

Préparation à l'intégration de l'exploit Shodan

Une intégration réussie Shodan d'Exploit nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Préparez-vous à l'intégration en effectuant ces tâches. L'intégration de l'exploit Shodan suppose que vous connaissez le moteur de recherche et l'API Shodan .

Avant de commencer

L'intégration d'exploit Shodan nécessite une clé API. Inscrivez-vous sur le Shodan site Web pour un abonnement gratuit afin d'acquérir cette clé.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration, apportez les changements de configuration nécessaires en fonction de vos besoins.

- Si vous n'avez pas importé les données de la base de données de vulnérabilité NIST (NVD) dans Réponse aux vulnérabilités, faites-le avant d'installer l'intégration d'exploit Shodan . L'importation des données NVD garantit que vos données CVE (Common Vulnerability and Exposure) remplissent automatiquement les enregistrements d'exploits.

  Sans les données NVD, un espace réservé est créé dans l'enregistrement de l'exploit et n'est pas saisi avant la prochaine mise à jour NVD. Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.

- Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installez et configurez le Intégration d'exploit Shodan pour Opérations de sécurité

Avant de pouvoir exécuter dans Intégration d'exploit Shodan votre instance, téléchargez-la et installez-la à partir du ServiceNow Store. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que vous disposez des autorisations valides ServiceNow pour l'application Réponse aux vulnérabilités et l'application Intégration d'exploit ShodanOpérations de sécurité .	Pour vérifier les autorisations, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Pour plus d'informations sur l'obtention d'autorisations pour une Opérations de sécurité application à partir de , reportez-vous à la ServiceNow Store section Obtenir une autorisation pour un produit ou une Opérations de sécurité application.
(Facultatif) Si elle n'est pas déjà installée et activée, vous préférerez peut-être installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce.	Pour plus d'informations sur l'installation et l'activation de l'application, Installer Réponse aux vulnérabilités reportez-vous à la Réponse aux vulnérabilités section .
Munissez-vous de la clé API d'intégration des Shodan exploits à portée de main.	Consultez Préparation à l'intégration de l'exploit Shodan.

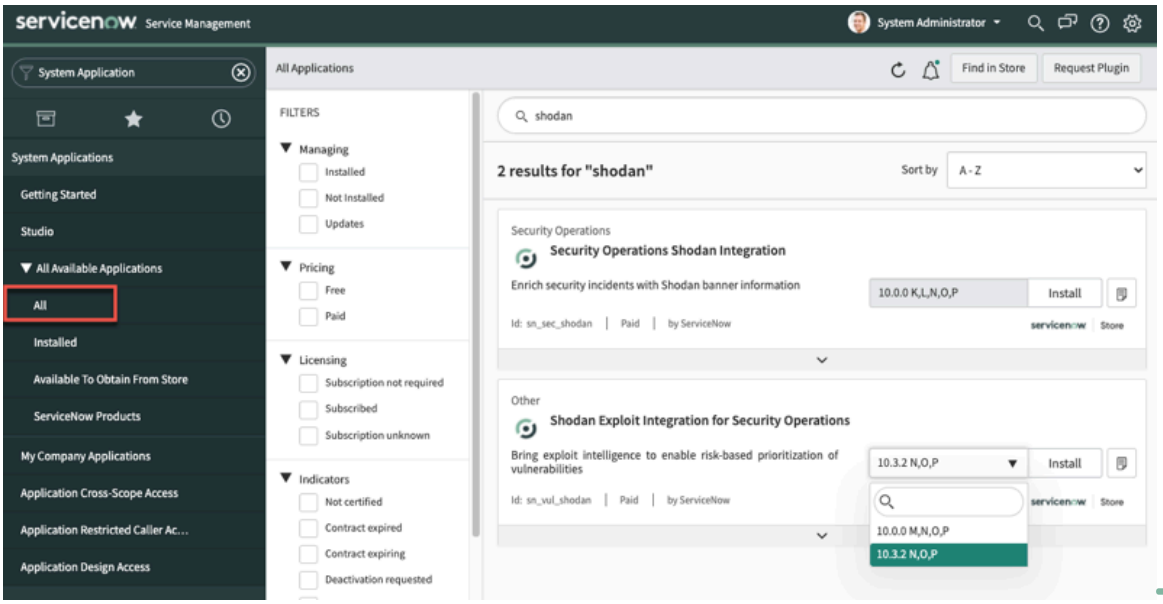
Rôle requis : admin

Procédure

1. Connectez-vous à l'instance ServiceNow AI Platform sur laquelle vous souhaitez installer l'application Intégration d'exploit Shodan .
2. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous**.
3. Localisez l'application Intégration d'exploit ShodanOpérations de sécurité , sélectionnez la version souhaitée, puis cliquez sur **Installer**.

Traduction automatique

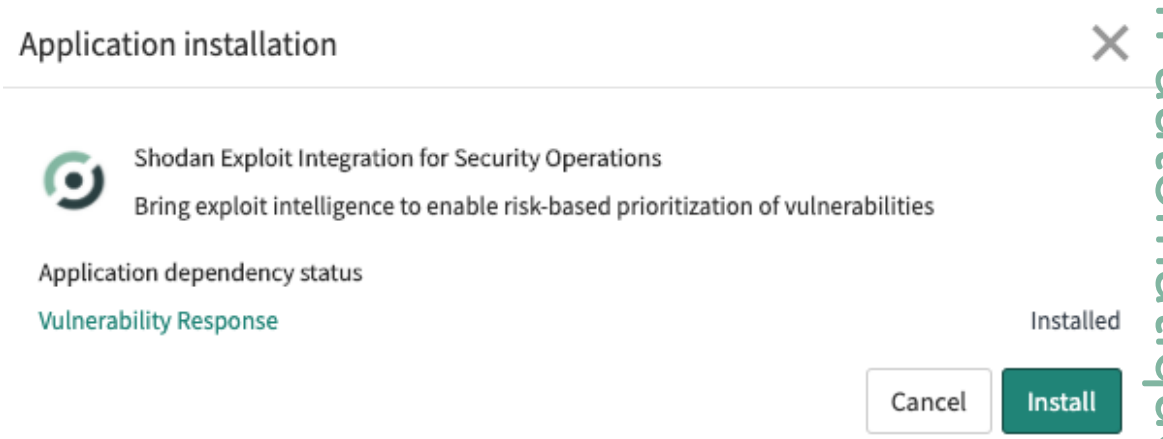
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Si vous avez droit à une mise à jour pour cette application, le bouton **Mettre à jour** s'affiche.

La boîte de dialogue d'installation de l'application affiche l'état de dépendance de l'application. Toutes les dépendances requises qui ne sont pas déjà installées sont automatiquement installées avec l'application.

4. Dans la boîte de dialogue, cliquez sur **Installer**.

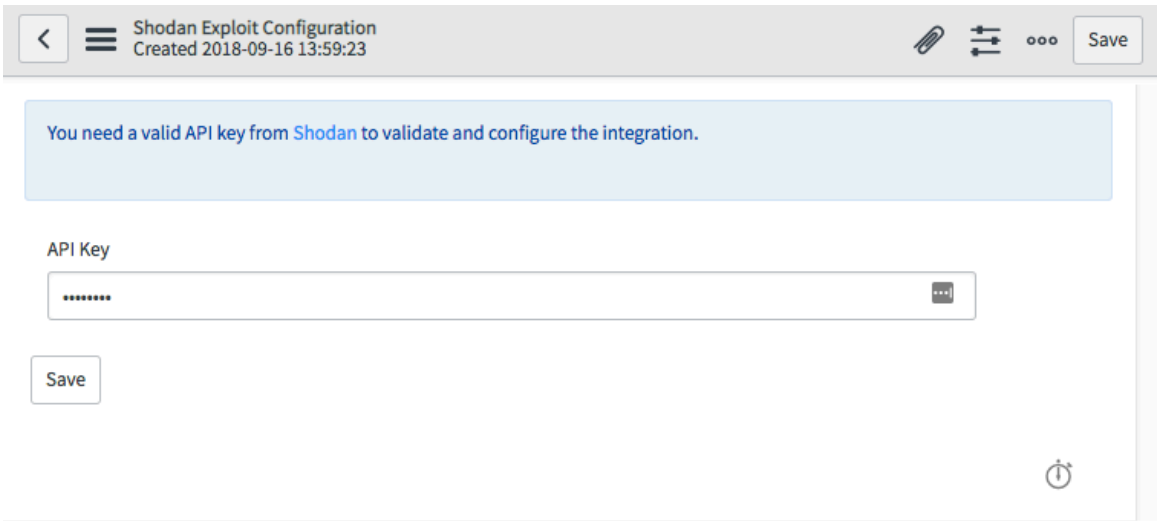


La boîte de dialogue Installer indique que l'installation est terminée.

5. Fermez la boîte de dialogue Installer.
6. Accédez à la **Shodan Exploit Integration** > **Configuration**.
7. Saisissez votre Shodan clé API.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Cliquez sur **Enregistrer**.
   Votre Intégration d'exploit Shodan configuration est terminée.

Définir le Shodan temps d'importation de l'intégration de l'exploit

Pour vous faciliter la tâche, vous pouvez réinitialiser l'heure de début des intégrations d'exploits Shodan .

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Après l'importation initiale, Shodan les intégrations d'exploits apportent des données delta, sauf si une importation complète est demandée. Consultez la section Effectuer une importation manuelle Shodan d'exploits pour plus d'informations sur les importations complètes.

Procédure

1. Accédez à la **Tous** > **Shodan Exploit Integration** > **Intégrations**.
2. Choisissez une intégration.
3. Cliquez sur le lien pour modifier l'enregistrement.
4. Définissez les nouvelles options **Exécution** et **Heure** .
   L'heure est calculée en heures en heure locale. L'heure par défaut pour les importations d'exploits Shodan est 03:15:00.
5. Cliquez sur **Mettre à jour**.
   La nouvelle heure est utilisée pour la prochaine importation planifiée.

Effectuer une importation manuelle Shodan d'exploits

Si votre importation initiale a échoué, ou si vous ne souhaitez pas attendre l'importation initiale planifiée, vous pouvez effectuer une importation de données complète indépendamment de la tâche planifiée quotidienne.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Shodan Exploit Integration** > **Intégrations**.
2. Choisissez une intégration.
3. Cochez la case **Importation complète des données** .
4. Cliquez sur **Exécuter maintenant**.
   Une fois l'importation terminée, la case est décochée et les importations delta reprennent.

Afficher l'état de l'exécution de l'importation d'intégration d'exploit Shodan

Utilisez la liste connexe Exécutions d'intégration de vulnérabilité pour vérifier le succès de vos exécutions d'intégration, localiser les problèmes et éclairer vos décisions de correction.

Avant de commencer

Pour afficher l'état de l'exécution de l'importation Shodan :

- L'application Réponse aux vulnérabilités et l'intégration de l'exploit Shodan doivent être installées et configurées.
- Les importations d'intégration Shodan d'exploits doivent être planifiées et en cours d'exécution.

Rôle requis : sn_vuln.admin

Pourquoi et quand exécuter cette tâche

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Shodan Exploit Integration** > **Intégrations**.
2. Sélectionnez une intégration.
3. Cliquez sur la liste connexe **Exécutions d'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.

Trouble?

Les causes les plus courantes d'un échec d'exécution sont les suivantes :

- Interruption du réseau
- Décroissance des bits dans le transfert de données entraînant des données corrompues pendant la transformation

Si vous rencontrez l'une de ces conditions, cochez la case **Importation complète des données** , cliquez sur **Exécuter maintenant** et réexécutez l'intégration.

Présentation de l'intégration de vulnérabilité Tenable

L'application Vulnerability Response integration with Tenable développée par ServiceNow l'ingénierie pour l'intégration de vulnérabilité Tenable utilise les données importées de , Tenable.ioTenable.sc et Tenable.cs les produits pour vous aider à classer par ordre de priorité et à corriger les vulnérabilités de vos actifs. L'application est disponible avec un abonnement distinct du ServiceNow® Store.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

L'intégration Tenable Vulnerability utilise trois intégrations Tenable, Tenable.io et , Tenable.sc pour Tenable.cs importer des données d'analyseurs tiers concernant vos actifs et vos vulnérabilités. L'application Vulnerability Response integration with Tenable prend en charge le produit à partir de la version 5.13 et Tenable.cs le produit à partir de la Tenable.sc version 5.0.1.

- Tenable.io est une intégration d'entreprise basée sur le cloud.
- Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le Tenable.sc produit et votre ServiceNow AI Platform instance se trouvent dans le même environnement.
- Si le Tenable.sc produit et votre ServiceNow AI Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID.
- Tenable.cs est une intégration d'entreprise basée sur le cloud.

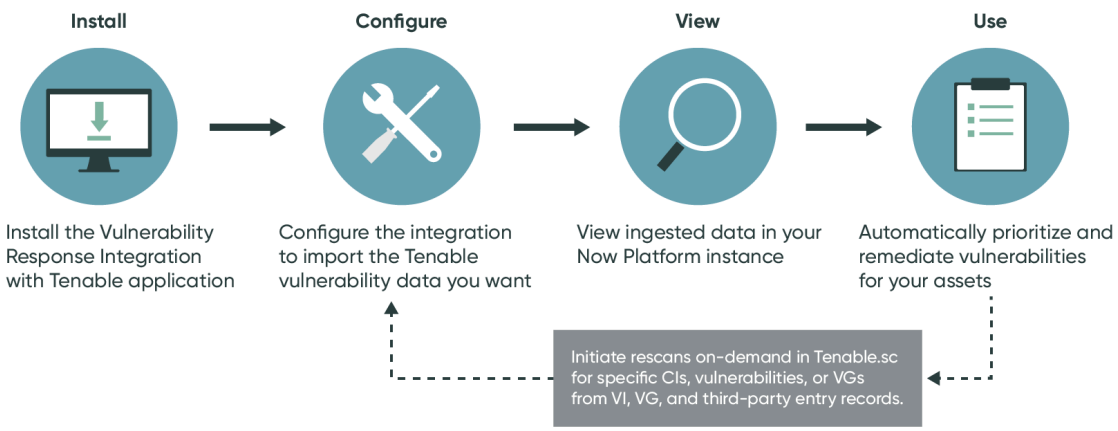
L'application Vulnerability Response integration with Tenable est disponible sur le ServiceNow Store avec un abonnement séparé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour obtenir la liste et la description des intégrations dans , consultez Tenable.sc Intégrations avec l'application Réponse aux vulnérabilitésTenable.io Intégrations avec les Réponse aux vulnérabilités applications et Conformité de la configuration et Tenable Vulnerability Integration.

Intégration de vulnérabilité Tenable



Versions disponibles pour Zurich

Version de mise en production	Notes de publication
Vulnerability Response integration with Tenable v3.13.1, v4.1, v5.0.1	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Termes et fonctionnalités clés des intégrations

Éléments vulnérables et vulnérabilités

Un élément vulnérable est créé dans votre ServiceNow AI Platform instance lorsque :

- Une vulnérabilité importée à partir d'un scanner tiers est mise en correspondance avec un actif existant (un élément de configuration dans votre CMDB). Le produit Tenable appelle ces **correspondances des vulnérabilités**.
- Une vulnérabilité importée à partir d'un scanner tiers ne correspond pas à un actif existant dans votre CMDB. Dans ce cas, un CI sans correspondance est également créé avec un élément vulnérable.

  Pour les CI sans correspondance, vous pouvez également utiliser le moteur IRE (Identification et rapprochement) pour créer des CI dans deux nouvelles classes lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte. Dans le cas contraire, des CI sans correspondance sont créés dans les classes de CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation.

Entrées de vulnérabilité tierces et modules d'extension

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les entrées de vulnérabilité tierces sont importées à partir d'analyseurs tiers et répertoriées dans la table Entrées de vulnérabilité tierces de votre ServiceNow AI Platform instance. À partir de la version 24.0 de Réponse aux vulnérabilités, la colonne Logiciels de la table Entrées de vulnérabilité tierces renseigne les énumérations de plateforme communes (CPE) associées à une entrée tierce. Les entrées de vulnérabilité tierces de Tenable sont ingérées et mises en correspondance avec les actifs existants répertoriés Réponse aux vulnérabilités dans votre CMDB. Tenable fait référence aux entrées de vulnérabilité tierces sous forme de **modules d'extension.**

Élément de configuration (CI)

Les éléments de configuration sont les actifs existants répertoriés dans votre CMDB.

Élément découvert

Les actifs ingérés à partir de l'importation d'actifs Tenable correspondent aux éléments de configuration existants dans votre CMDB. Les actifs importés sont mis à jour.

Si aucune correspondance n'est trouvée, un CI est créé dans la classe CI sans correspondance du CMDB. Si le module d'extension Modèles de classe CI CMDB est activé, le moteur Identification et rapprochement (IRE) crée des CI à l'aide de nouvelles classes. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation. Si le CI d'origine sans correspondance est reclassé, les enregistrements d'éléments détectés sont mis à jour pour refléter l'état. Les éléments détectés vous donnent une visibilité sur la façon dont les actifs sont identifiés et mappés aux CI dans le CMDB.

Règles de recherche de CI

Lorsque les données sont importées à partir d'une intégration tierce, Vulnerability Response utilise automatiquement les données de l'hôte (actif) pour rechercher des correspondances dans la Base de données de gestion des configurations (CMDB). Les règles de recherche de CI sont utilisées pour identifier les CI et les ajouter aux enregistrements de VI lorsque des VIT sont créés pour vous aider dans la correction.

Analyse de nouveau et analyse de rattrapage

Vous pouvez lancer une commande de nouvelle analyse ciblée sur un élément de configuration, une tâche de rattrapage ou une entrée tierce directement à partir des enregistrements d'entrée d'élément vulnérable, de tâche de rattrapage et de vulnérabilité tierce dans votre ServiceNow AI Platform instance. Tenable appelle cette nouvelle analyse une analyse de **correction**.

Fermer automatiquement les anciens VI

Avec le module Fermer automatiquement les éléments vulnérables périmés dans votre ServiceNow AI Platform, vous pouvez nettoyer les éléments vulnérables plus anciens et périmés (EV) qui n'ont pas été trouvés récemment par vos intégrations tierces. Le déplacement de ces VI vers **Fermé** vous aide à réduire le nombre d'éléments vulnérables actifs et de tâches de rattrapage, et à rapprocher les actifs dans votre CMDB. Vous pouvez utiliser toutes les intégrations avec Vulnerability Response integration with Tenable pour fermer automatiquement les VI périmés.

Instance

Ce terme fait référence à une occurrence distincte de votre ServiceNow AI Platform® application.

Intégration

Une intégration est une référence spécifique à un produit à une intégration, telle que l'intégration Tenable.io des actifs ou l'intégration des modules d'extension Tenable.sc . Il s'agit des intégrations distinctes qui appartiennent à des produits Tenable spécifiques dans l'intégration de vulnérabilité Tenable de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Instance d'intégration

Ce terme fait référence aux intégrations Tenable distinctes répertoriées par leurs Tenable.io et Tenable.sc produits.

Déploiement

Lorsqu'une intégration prend en charge le multisource, une existence d'intégration unique et distincte est appelée un déploiement de votre intégration. Le terme est utilisé pour désigner la ou les intégrations et les produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de diverses intégrations de Tenable.io produits dans Tenable.sc votre environnement.

Les Tenable.io intégrations , Tenable.sc, et incluent Tenable.cs également les fonctionnalités clés suivantes :

- Les résultats de l'évaluation de la configuration, c'est-à-dire les résultats des tests ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources faisant autorité peuvent être importés dans l'application Conformité de la configuration avec le Tenable.io produit. Consultez Tenable.io Intégrations avec les Réponse aux vulnérabilités applications et Conformité de la configuration et Explorer Conformité de la configuration pour plus d'informations sur le fonctionnement de cette intégration avec l'application Conformité de la configuration .
- À partir de la version 2.1 de , Tenable Vulnerability Integration créez des éléments de configuration (CI) uniques qui incluent différents identificateurs de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. Identifiez les actifs distincts dans votre environnement et mettez à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous donner plus de détails sur vos vulnérabilités.
- Vous pouvez planifier le moment où vous souhaitez que les tâches s'exécutent pour toutes les Tenable.io intégrations et Tenable.scTenable.cs . Vous pouvez également exécuter des travaux planifiés manuellement à la demande.
- Pour les importations d'actifs avec Tenable.io, vous pouvez activer les balises d'actifs pour organiser et suivre les actifs répertoriés dans CMDB votre Tenable.io environnement.
- Les Tenable.io intégrations de , Tenable.sc et Tenable.cs vous permettent de configurer des règles de recherche de CI pour définir la façon dont les données d'actifs de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans votre ServiceNow AI Platform CMDB.
- Les Tenable.io intégrations de , Tenable.sc et Tenable.cs vous permettent de définir des filtres d'importation sur l'importation des vulnérabilités afin d'importer uniquement les vulnérabilités de Tenable que vous souhaitez. Pour Tenable.io, vous avez la possibilité d'importer les vulnérabilités **corrigées** de Tenable avec l'importation des vulnérabilités.
- Pour Tenable.sc, vous avez la possibilité de lancer de nouvelles analyses sur demande directement à partir d'un élément vulnérable, d'une tâche de rattrapage et d'enregistrements d'entrée tiers dans votre ServiceNow AI Platform instance. Si les VI sont passés à **l'état Fermé/Corrigé,** mais ne sont pas encore mis à jour dans votre instance, vous pouvez vérifier que les vulnérabilités sur des éléments de configuration spécifiques ont été corrigées. Consultez Lancer une nouvelle analyse pour l'intégration Tenable.sc.

Les sections suivantes répertorient plus de détails sur les intégrations Tenable.

Rôles ServiceNow AI Platform requis

Les tâches d'intégration nécessitent les rôles suivants dans votre ServiceNow AI Platform instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

administrateur

L’administrateur système utilise l’assistant de configuration pour installer l’application Vulnerability Response integration with Tenable . S’il n’est pas affecté, l’administrateur affecte l’administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d’autres rôles dans l’assistant de configuration.

sn_vul.vulnerability_admin

Une fois affecté, l’administrateur de vulnérabilité termine la configuration des intégrations Tenable dans l’assistant de configuration. Ce rôle dispose d’un accès complet à l’application Réponse aux vulnérabilités (VR) et à ses enregistrements. L’administrateur de vulnérabilité configure toutes les applications et règles de réalité virtuelle pour les intégrations tierces installées.

sn_vul_tenable.configure_integration

Ce rôle contient le rôle granulaire sn_vul_tenable.read_integration et les utilisateurs disposant de ce rôle peuvent configurer l’application Vulnerability Response integration with Tenable .

sn_vul_tenable.read_integration

Les utilisateurs disposant de ces rôles peuvent afficher (lire) mais pas modifier les enregistrements de l’application Vulnerability Response integration with Tenable .

Groupe de réponse aux vulnérabilités

Par défaut, le groupe Réponse aux vulnérabilités est disponible dans l’Assistant de configuration. Les utilisateurs affectés au groupe Réponse aux vulnérabilités héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner.

Éléments vulnérables

Les éléments vulnérables sont regroupés en tâches de rattrapage en fonction des règles de tâche de rattrapage et affectés au rattrapage en fonction de vos règles d’affectation. Pour plus d'informations, consultez Réponse aux vulnérabilités Vue d’ensemble des tâches de rattrapage et des règles de tâche de rattrapage et Réponse aux vulnérabilités Vue d’ensemble des règles d’affectation.

Règles de recherche d’éléments de configuration (CI)

Les règles de recherche de CI identifient les CI et déterminent quand les ajouter à un élément vulnérable. Pour en savoir plus sur le fonctionnement des règles de recherche de CI, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d’intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Remarque : Une fois supprimées, les règles ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lors de leur création.

Les règles de recherche suivantes Tenable.io sont fournies avec le système de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nom d'hôte
- DNS
- IP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les Tenable.io règles de recherche de CI classent par ordre de priorité et renseignent les valeurs d'interface réseau non vides (FDQN, IPV4 et MacAddress) par rapport aux valeurs FDQN, IPV4 et MacAddress normales d'un élément détecté. Lorsque ces valeurs d'interface réseau sont vides, les valeurs FDQN, IPV4 et MacAddress normales sont renseignées pour un élément détecté.

Les règles de recherche suivantes Tenable.sc sont fournies avec le système de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Remarque : Plusieurs valeurs pour ip_address, mac_address, FQDN et network_interfaces sont utilisées pour un actif. Toutes les valeurs sont prises en compte dans les règles de recherche de CI pour la mise en correspondance. Toutes les valeurs sont utilisées pour créer plusieurs cartes réseau à l'aide d'IRE.

L'ID Tenable.cs de ressource cloud de règle de recherche est fourni avec le système de base.

Pour plus d'informations sur la configuration de la catégorisation des ressources cloud sans correspondance dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

Nouvelles propriétés à ignorer Adresses IP

Dans Tenable.io, deux propriétés sont disponibles si vous souhaitez ignorer plusieurs adresses IP ou plusieurs adresses Mac dans le cadre de vos règles de recherche de CI :

ignoreIPAddress

Une liste d'adresses IP à ignorer pour la recherche et la création de CI.

ignoreMacAddress

Une liste d'adresses MAC à ignorer pour la recherche ou la création de CI.

Éléments découverts

Ce module répertorie les éléments de configuration détectés lors de l'importation à partir des intégrations d'éléments vulnérables Tenable et des intégrations d'actifs Tenable.

Remarque : Le filtre par défaut de cette liste est défini sur Sans correspondance. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour en savoir plus sur le module Éléments détectés, reportez-vous à la section Éléments détectés.

Étiquette d'actifs

Les balises d'actif (également appelées balises d'hôte) sont utilisées pour organiser et suivre les actifs de votre organisation. Vous pouvez affecter des balises à vos actifs. Ensuite, lors du lancement des analyses, vous pouvez sélectionner des balises associées aux ressources que vous souhaitez analyser. Le module Balises d'actifs vous permet de télécharger de manière planifiée des données de balises d'actifs vers Tenable.io votre instance. Les données d'actif qui incluent des balises d'actif sont extraites des cartes de transformation de l'intégration de Tenable.io Asset Transform et transformées à l'aide de Tenable.io ces derniers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Toutes les balises d'actifs sont importées dans le cadre de l'intégration Tenable.io des actifs. Les balises d'actif sont utilisées pour le filtrage dans les règles d'affectation et les Réponse aux vulnérabilités règles de tâche de rattrapage. Les balises sont affichées dans le formulaire Élément détecté.

Remarque : Exécutez l'intégration Tenable.io des actifs avant de créer Réponse aux vulnérabilités des règles d'affectation ou des règles de tâche de rattrapage dans l'application Réponse aux vulnérabilités afin que toutes les balises soient disponibles pour ces règles avant que les éléments vulnérables ne soient importés et regroupés. Notez également les points suivants concernant les balises :

- Le stockage des balises n'est pas sensible à la casse. Par exemple, si vous créez une balise pour décrire les actifs de votre emplacement à San Diego et que vous créez la balise `San Diego` , vous ne pouvez pas également créer une balise `SAN DIEGO` et la stocker dans la table Balise d'actif. `San Diego` et `SAN DIEGO` sont considérés comme le même actif par le système. La balise importée en premier est la balise qui est stockée et reconnue à l'avenir.
- L'utilisation de balises d'actifs comme clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises d'actif sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'actif sont contrôlées par la propriété système globale sn_vul.import_asset_tags. Cette propriété est définie sur `vrai` par défaut. La désactivation des balises les désactive dans toutes les ServiceNow AI Platform® instances.

Filtres de récupération de données

Les paramètres de récupération de données vous aident à déterminer précisément le type et l'étendue des données que vous souhaitez importer de l'application Tenable vers votre ServiceNow AI Platform® instance. Pour obtenir la liste des paramètres les plus couramment utilisés, reportez-vous à la section Paramètres de récupération de données pour l'intégration de vulnérabilité Tenable.

Évaluation de la priorité de vulnérabilité (VPR)

L'évaluation de priorité de vulnérabilité (VPR) est un attribut du produit Tenable qui est importé et utilisé avec un nouveau calculateur de risque par défaut dans Réponse aux vulnérabilités. La règle de risque Tenable est installée avec l'application dans le Vulnerability Response integration with Tenable cadre du calculateur de risque par défaut dans les calculateurs de vulnérabilité de Réponse aux vulnérabilités.

Cette règle de risque est inactive par défaut.

En activant la règle du calculateur de risque Tenable, les valeurs VPR importées sont utilisées pour calculer le score de risque des éléments vulnérables. La distribution de poids par défaut pour ce calculateur de risque est la suivante : VPR = 70 %, Actif = 15 % et Criticité opérationnelle = 15 %. L'activation de cette règle du calculateur de risque Tenable peut avoir un impact sur vos performances d'ingestion de données. Pour plus d'informations sur Réponse aux vulnérabilités les calculateurs et la règle du calculateur de risque Tenable, reportez-vous à la section Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.

Installation et configuration

Après avoir téléchargé le Vulnerability Response integration with Tenable , l'installation et la ServiceNow® Store configuration sont prises en charge par l'assistant de configuration dans Réponse aux vulnérabilités. Consultez Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.io Intégrations avec les Réponse aux vulnérabilités applications et Conformité de la configuration

Les Tenable.io intégrations dans l'application Vulnerability Response integration with Tenable sont disponibles dans les Réponse aux vulnérabilités applications et Conformité de la configuration .

Liste des Tenable.io intégrations

Le multisource est pris en charge pour toutes les Tenable.io intégrations et Tenable.sc . Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'assistant de configuration dans Réponse aux vulnérabilités. Vous installez et configurez également l'application à partir de l'Assistant Vulnerability Response integration with Tenable de configuration.

Tenable.io est une intégration d'entreprise basée sur le cloud. Consultez le tableau suivant pour connaître les noms et les descriptions des intégrations prises en charge pour le Tenable.io produit.

L'intégration Tenable.io des résultats de conformité et l'intégration du Tenable.io remplissage des résultats de conformité sont inactives par défaut.

Pour les activer :

1. Accédez à la **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
2. Dans la liste des intégrations Tenable, cliquez sur un nom d'intégration pour ouvrir l'enregistrement et cochez la case **Actif** pour l'activer. Vous préférez peut-être laisser les paramètres de calendrier dans leurs valeurs par défaut pour que ces intégrations démarrent.

Intégrations de Tenable.io

Intégration	Description
Tenable.io Intégration des actifs	• Récupère toutes les données d'actif, y compris les balises d'actif Tenable.io , à partir du produit et les traite dans votre instance. • À partir de la version 3.0, si l'intégration des résultats de la Tenable.io conformité est activée, vous pouvez importer des données d'évaluation de configuration sécurisée avec les données d'actif importées. Ces données peuvent vous aider à identifier et à répondre aux vulnérabilités liées à la configuration de vos actifs. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de messages REST à l'API d'actif. • Cette intégration génère des éléments détectés. • Les données sont importées en blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	table supprime automatiquement les données stockées de cette table après 30 jours. • À partir de la version v2.2, `Last Scan Time` est importé et mis à jour uniquement pour les actifs qui présentent des vulnérabilités.
Tenable.io Intégration des résultats de la conformité	• À partir de la version 3.0, les données d'évaluation de la configuration sécurisée importées à partir de l'intégration des résultats de la conformité, ainsi que les données importées de l'intégration des actifs peuvent vous aider à identifier les vulnérabilités liées à la configuration sur vos actifs et à y répondre. • Si cette option est activée, elle récupère les données d'évaluation de la configuration sécurisée de haut niveau et les traite dans votre ServiceNow AI Platform instance. Les données importées comprennent les résultats des tests ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources faisant autorité. • Les données d'évaluation des actifs manquants ou des actifs sans ID d'actif ne sont pas importées. • Si un résultat de test est importé et que son actif correspondant ne peut pas être mis en correspondance dans votre instance, le résultat du test est ignoré et l'ID de l'actif manquant est stocké dans un enregistrement temporaire dans la table [sn_vul_tenable_missing_asset]. • La valeur totale des actifs ignorés (manquants) est répertoriée dans le champ **CI ignorés** de l'onglet **Configuration** de l'enregistrement d'exécution de l'intégration pour cette intégration.
Tenable.io Intégration du remplissage des résultats de la conformité	• Lorsqu'elle est activée, cette intégration s'exécute automatiquement une fois que l'intégration des actifs est terminée avec succès dans le cadre d'une exécution d'intégration chaînée. Cette intégration met en correspondance les données d'évaluation de la configuration avec les actifs manquants répertoriés dans la table [sn_vul_tenable_missing_asset]. • Importe jusqu'à 200 ID d'actifs pour tous les actifs manquants découverts ou présents dans l'instance une fois l'importation de l'intégration des actifs terminée. • Supprime les enregistrements temporaires de la table [sn_vul_tenable_missing_asset] lorsque les actifs peuvent être mis en correspondance avec les données d'évaluation de la configuration correspondantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
Tenable.io Intégration des informations d'identification de numérisation	• Cette intégration récupère les informations d'identification de numérisation configurées dans Tenable.io. • Coordonne les appels de messages REST à l'API d'informations d'identification. • La sortie de cette intégration est les informations d'identification de numérisation renseignées dans la table [sn_vul_tenable_scan_credential]. • Les informations d'identification importées sont utilisées pour accéder au scanner lorsque des demandes d'analyse sont lancées à partir de .ServiceNow AI Platform • Cette intégration est planifiée pour s'exécuter chaque semaine.
Tenable.io Intégration de modèles	Un enregistrement de modèle est envoyé lors de la Tenable.io nouvelle analyse. Cette intégration récupère les informations d'identification disponibles Tenable.io à utiliser pour les nouvelles analyses. Les informations d'identification sont spécifiques à l'instance et un enregistrement de modèle unique est importé et stocké temporairement en toute sécurité sur la table [sn_vul_tenable_io_template].
Tenable.io Intégration de module d'extension	• Récupère les données du module d'extension à partir du Tenable.io produit. Les données récupérées sont basées sur la date à laquelle les modules d'extension ont été mis à jour pour la dernière fois par une exécution d'intégration Tenable.io . • Cette importation garantit que les Tenable.io identificateurs (dix ID) sont à jour. • Coordonne les appels de messages REST à l'API du module d'extension. • Le résultat de cette intégration est les vulnérabilités tierces.
Tenable.io Intégration des vulnérabilités corrigées	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.io produit et les traite dans votre instance. Les éléments vulnérables sont créés pour les enregistrements de détection avec les états **Ouvert** et **Rouvert** , car ces enregistrements requièrent une correction. Les éléments vulnérables existants sont mis à jour par Vulnerability Response si les détections sont **corrigées**, mais les éléments vulnérables ne sont pas créés pour les détections **fixes** par défaut, car Tenable considère que les vulnérabilités **corrigées** sont **atténuées**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	• Lorsque le marqueur **Créer des périodes vulnérables pour les détections de vulnérabilité fixes** est activé dans l'Assistant de configuration, de nouveaux VI sont créés à l'état **Fixe** afin que vous ayez une visibilité sur les détections qui les ont créés. Étant donné que les VI sont créés pour des détections **fixes** qui n'existent pas déjà dans votre instance, cela peut avoir un impact négatif sur vos performances d'importation. Vous préférez peut-être laisser cette fonctionnalité désactivée afin que les détections **fixes** ne fassent qu'actualiser les états des éléments vulnérables existants. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de messages REST à l'API de vulnérabilités. • La sortie de cette intégration est Éléments vulnérables (VI) **fermés/corrigés** . Il crée également des actifs et des entrées tierces s'ils n'existent pas. • Les données sont importées en blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. Cette exécution de l'intégration est planifiée. Il s'agit d'une intégration chaînée, ce qui signifie qu'une fois l'exécution terminée avec succès, l'intégration des vulnérabilités ouvertes décrite ci-dessous est déclenchée. À partir de Tenable v3.3, vous pouvez afficher les informations suivantes pour les exécutions d'intégration de vulnérabilité : • **Blocs au total :** Nombre total de blocs générés par Tenable • **Blocs disponibles :** Nombre de blocs disponibles au téléchargement pour ServiceNow
Tenable.io Intégration des vulnérabilités ouvertes	• Cette intégration est déclenchée une fois que l'intégration Tenable.io des vulnérabilités corrigées est terminée. • Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.io produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	• Coordonne les appels de messages REST à l'API de vulnérabilités. • La sortie de cette intégration est Éléments vulnérables (VI) **nouveaux/rouverts** . Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas. Tenable considère les vulnérabilités actives **cumulatives** (actuelles). • Les données sont importées en blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. À partir de Tenable v3.3, vous pouvez afficher les informations suivantes pour les exécutions d'intégration de vulnérabilité : • **Blocs au total :** Nombre total de blocs générés par Tenable • **Blocs disponibles :** Nombre de blocs disponibles au téléchargement pour ServiceNow
Tenable.io/scan Intégration des métadonnées	Cette intégration récupère les métadonnées à partir du point de terminaison /scans. Il extrait les informations d'analyse en fonction des last_schedule_id des données d'actif existantes dans Tenable.io. L'intégration du point de terminaison /scans à partir de Tenable.io implique les étapes d'implémentation suivantes : • **Création de table** : une nouvelle table personnalisée, **sn_vul_tenable_scan**, est créée pour stocker les métadonnées d'analyse récupérées à partir du Tenable.io point de terminaison /scans. Il s'agit notamment de détails tels que l'ID d'analyse, le nom, l'état, l'heure de début, l'heure de fin et le type d'analyse. • **Association de données** : un champ de référence est établi entre les éléments découverts (éléments de configuration ou vulnérabilités) et le dernier enregistrement d'analyse correspondant dans la table **sn_vul_tenable_scan** . Ce couplage vous permet de : ◦ Affichez les informations d'analyse les plus récentes associées à chaque élément découvert. ◦ Améliorez le contexte pour les décisions de triage et de rattrapage des vulnérabilités. ◦ Améliorez la vérifiabilité et les capacités de génération de rapports en conservant un enregistrement historique des activités d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.sc Intégrations avec l'application Réponse aux vulnérabilités

Les Tenable.sc intégrations dans l'application Vulnerability Response integration with Tenable .

Réponse aux vulnérabilités À partir de la version 20.0, si un actif est analysé par un agent, la colonne « L'agent existe » dans la liste des éléments détectés affiche la valeur comme « vrai ». Cela indique que l'analyse est authentique.

Liste des Tenable.sc intégrations

Le multisource est pris en charge pour toutes les Tenable.io intégrations et Tenable.sc . Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'application à partir de l'Assistant Vulnerability Response integration with Tenable de configuration.

- Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le Tenable.sc produit et votre ServiceNow AI Platform instance se trouvent dans le même environnement.
- Si le Tenable.sc produit et votre ServiceNow AI Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID.

Intégrations de Tenable.sc

Intégration	Description
Tenable.sc Intégration des actifs	Pour éviter de créer des éléments détectés en double avec des données d'actifs importées, l'intégration des actifs du Tenable.sc produit comprend deux intégrations. **L'intégration Tenable.sc des actifs ouverts** Cette intégration importe des données de vulnérabilité sur vos actifs que Tenable considère comme **cumulatives** (actuelles) ou **ouvertes**. Les éléments vulnérables (VI) qui sont créés dans votre instance avec ces données d'actif importées sont considérés comme ouverts, c'est-à-dire à l'état **Ouvert** . Ces éléments vulnérables nécessitent une enquête et peuvent nécessiter une correction. **L'intégration Tenable.sc des actifs immobilisés** Cette intégration importe les données de vulnérabilité de vos actifs que Tenable considère comme **atténuées** (n'étant plus vulnérables) ou **corrigées**. Les éléments vulnérables de ces actifs passent de l'état **Ouvert** à l'état **Fermé/Fixe** dans votre instance, car les résultats des analyses montrent qu'ils ne sont plus vulnérables. • Récupère toutes les données d'actif du Tenable.sc produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent une adresse IP. • Coordonne les appels de messages REST à l'API Assets.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	• Cette intégration génère des éléments détectés. • Le filtre de requête Tenable que vous sélectionnez dans l'assistant de configuration s'applique également à l'intégration Tenable.sc des actifs. Seuls les actifs présentant les vulnérabilités qui correspondent aux conditions du filtre de requête sont importés.
Tenable.sc Intégration de module d'extension	• Récupère les données du module d'extension à partir du Tenable.sc produit. Les données récupérées sont basées sur la date à laquelle les modules d'extension ont été mis à jour pour la dernière fois par une exécution d'intégration Tenable.sc . • Cette importation garantit que les Tenable.sc identificateurs (dix ID) sont à jour et que seules les vulnérabilités actives sont importées. • Coordonne les appels de messages REST à l'API des modules d'extension. • Le résultat de cette intégration est les vulnérabilités tierces.
Tenable.sc Intégration des vulnérabilités corrigées	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.sc produit et les traite dans votre instance. Les éléments vulnérables sont créés pour les enregistrements de détection avec les états **Ouvert** et **Rouvert** , car ces enregistrements requièrent une correction. Les éléments vulnérables existants sont mis à jour par Vulnerability Response si les détections sont **corrigées**, mais les éléments vulnérables ne sont pas créés pour les détections **fixes** par défaut, car Tenable considère que les vulnérabilités **corrigéessont atténuées**. • Lorsque le marqueur **Créer des moments vulnérables pour les détections de vulnérabilité fixes** est activé dans l'Assistant de configuration, il crée des VI à l'état **Fixe** afin que vous ayez une visibilité sur les détections qui les ont créées. Comme des VI sont créés pour des détections **fixes** qui n'existent pas dans votre instance, cela peut avoir un impact négatif sur vos performances d'importation. Vous préférez peut-être laisser cette fonctionnalité désactivée afin que les détections **fixes** ne fassent qu'actualiser les états des éléments vulnérables existants. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent une adresse IP. • Coordonne les appels de messages REST à l'API de vulnérabilités. La sortie de cette intégration est Éléments vulnérables (VI) **fermés/corrigés** . Il crée également des actifs et des entrées tierces s'ils n'existent pas. Cette exécution d'intégration est une exécution planifiée. Il s'agit d'une intégration chaînée, ce qui signifie qu'une fois l'exécution terminée avec succès, l'intégration Tenable.sc des vulnérabilités ouvertes décrite ci-dessous est déclenchée. **Remarque :** Par défaut, les ID de famille 0 et 39 sont exclus de cette intégration.
Tenable.sc Intégration des vulnérabilités ouvertes	• Cette intégration est déclenchée lors de la réussite de l'intégration Tenable.sc des vulnérabilités corrigées. • Récupère les données de vulnérabilité en fonction des filtres de requête sélectionnés dans le Tenable.sc produit et les traite dans votre instance. • Crée les éléments vulnérables correspondants pour les vulnérabilités actives. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent une adresse IP. • Coordonne les appels de messages REST à l'API de vulnérabilités. • Le résultat de cette intégration est **Mettre à jour/Créer de nouveaux** éléments vulnérables (VI) s'ils n'existent pas. Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas. **Remarque :** Par défaut, les ID de famille 0 et 39 sont exclus de cette intégration.
Tenable.sc Intégration des informations d'identification de numérisation	• Cette intégration récupère les informations d'identification de numérisation configurées dans Tenable.sc. • Coordonne les appels de messages REST à l'API d'informations d'identification. • La sortie de cette intégration est les informations d'identification de numérisation renseignées dans la table [sn_vul_tenable_scan_credential].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	• Les informations d'identification importées sont utilisées pour accéder au scanner lorsque des demandes d'analyse sont lancées à partir de .ServiceNow AI Platform • Cette intégration est planifiée pour s'exécuter chaque semaine.
Tenable.sc Intégration des vulnérabilités de remplissage	• Cette intégration de remplissage importe toutes les vulnérabilités ouvertes et corrigées qui auraient pu être manquées lors d'une importation. • Cette intégration importe les vulnérabilités ouvertes et corrigées des sept derniers jours pour mettre à jour vos détections et vos éléments vulnérables. • Cette intégration peut avoir un impact sur vos performances. • Cette intégration est désactivée par défaut. • Pour mettre à jour vos données de vulnérabilité et éviter d'éventuels problèmes de performances, vous pouvez planifier l'exécution des intégrations Tenable.sc Vulnérabilités corrigées et Vulnérabilités ouvertes lorsqu'aucune autre analyse n'est en cours d'exécution. • Le résultat de cette intégration est : ○ Éléments vulnérables (VI) **fermés/corrigés**. Il crée également des actifs et des entrées tierces s'ils n'existent pas. ○ **pour mettre à jour/créer de nouveaux** éléments vulnérables (VI) s'ils n'existent pas. Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas.

Authentification utilisateur et Tenable.sc

L'authentification utilisateur est prise en charge par votre instance et la ServiceNow AI Platform®Tenable.sc version 5.13 du produit. L'authentification utilisateur est requise si vous utilisez la version 5.12 et antérieure du Tenable.sc produit.

Lorsque vous sélectionnez l'authentification utilisateur pour les intégrations, les jetons peuvent expirer et être remplacés pendant l'exécution de l'intégration Tenable.sc . Dans la colonne Notes de l'enregistrement d'exécution de l'intégration de vulnérabilité (VIN), le message suivant s'affiche pour un processus lorsqu'un jeton expire, Erreur : la validation du jeton a échoué. Aucune action n'est requise si ce message s'affiche. Les jetons expirés sont automatiquement actualisés en arrière-plan et le message n'indique pas de pause ou d'erreur dans le processus d'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Intégrations avec l'application Réponse aux vulnérabilités AND Réponse aux vulnérabilités pour conteneurs

Les Tenable.cs intégrations dans l'application Vulnerability Response integration with Tenable sont disponibles dans Vulnerability Response et Réponse aux vulnérabilités pour conteneurs les applications.

À partir de la version 20.0 Réponse aux vulnérabilités, si un actif est analysé par un agent, la colonne « L'agent existe » dans la liste des éléments détectés affiche « vrai », indiquant que l'analyse est authentique.

Liste des Tenable.cs intégrations

Le multisource est pris en charge pour toutes les Tenable.io intégrations , Tenable.sc et .Tenable.cs Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'application à partir de l'Assistant Vulnerability Response integration with Tenable de configuration.

Tenable.cs est une intégration d'entreprise basée sur le cloud. Consultez le tableau suivant pour connaître les noms et les descriptions des intégrations prises en charge pour le Tenable.cs produit.

Intégrations de Tenable.cs

Intégration	Description
Tenable.cs Intégration des actifs de conteneur dans le cloud	• Récupère toutes les données d'actif du conteneur à partir du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants. Coordonne les appels de messages REST à l'API d'actif. La sortie de cette intégration est les images de conteneur détectées, les images Docker et les référentiels de conteneur.
Tenable.cs Intégration ouverte des vulnérabilités du conteneur dans le cloud	Lorsqu'elle est activée, cette intégration s'exécute automatiquement une fois que l'intégration des actifs du conteneur est terminée avec succès dans le cadre d'une exécution d'intégration chaînée. • Récupère les données de vulnérabilité du conteneur en fonction des filtres de gravité du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants. • Coordonne les appels de messages REST à l'API de vulnérabilités. La sortie de cette intégration est Éléments vulnérables de conteneur (CVI) nouveaux/réouverts. S'ils n'existent pas, il crée également des images de conteneurs découverts, des images Docker, des référentiels de conteneurs, des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.cs (suite)

Intégration	Description
	résultats d'image, des entrées tierces et des vulnérabilités et expositions courantes (CVE).
Tenable.cs Correction des vulnérabilités du conteneur dans le cloud : intégration	Cette intégration est déclenchée lors de la réussite de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud ouverts. • Récupère les données de vulnérabilité du conteneur en fonction des filtres de gravité du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants • Coordonne les appels de messages REST à l'API de vulnérabilités. Le résultat de cette intégration est Éléments vulnérables de conteneur (CVI) nouveaux/rouverts. S'ils n'existent pas, il crée également des images de conteneur de détection, des images Docker, des référentiels de conteneur, des résultats d'image, des entrées tierces et des CVE. Les résultats d'image sont créés à l'état Fermé.
Tenable.cs Intégration ouverte des vulnérabilités de l'hôte dans le cloud	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants. • Coordonne les appels de messages REST à l'API de vulnérabilités. La sortie de cette intégration est Éléments vulnérables (VI) nouveaux/rouverts. S'ils n'existent pas, il crée également des éléments de configuration, des entrées tierces et des CVE. Les détections de vulnérabilité sont créées à l'état ouvert.
Tenable.cs Intégration des vulnérabilités de l'hôte dans le cloud corrigées	Cette intégration est déclenchée lors de la réussite de l'intégration des vulnérabilités de l'hôte dans le Tenable.cs cloud ouvert. • Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants. • Coordonne les appels de messages REST à l'API de vulnérabilités. Le résultat de cette intégration est Fermer les éléments vulnérables (VI). S'ils n'existent pas, il crée également des éléments de configuration, des entrées tierces et des CVE. Les détections de vulnérabilité sont créées à l'état Fermé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification utilisateur et Tenable.sc

L'authentification utilisateur est prise en charge par votre instance et la ServiceNow AI Platform®Tenable.sc version 5.13 du produit. L'authentification utilisateur est requise si vous utilisez la version 5.12 et antérieure du Tenable.sc produit.

Lorsque vous sélectionnez l'authentification utilisateur pour les intégrations, les jetons peuvent expirer et être remplacés pendant l'exécution de l'intégration Tenable.sc . Dans la colonne Notes de l'enregistrement d'exécution de l'intégration de vulnérabilité (VIN), le message suivant s'affiche pour un processus lorsqu'un jeton expire, Erreur : la validation du jeton a échoué. Si ce message s'affiche, aucune action n'est requise. Les jetons expirés sont automatiquement actualisés en arrière-plan et le message n'indique pas de pause ou d'erreur dans le processus d'intégration.

Préparation à l'intégration de vulnérabilité Tenable

Préparez l'intégration de Tenable ServiceNow® Vulnerability en effectuant les tâches de configuration suivantes.

Avant de commencer

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Pour une installation et une configuration fluides de l'application Vulnerability Response integration with Tenable , vous pouvez imprimer la liste de vérification suivante et vérifier que les éléments énumérés sont renseignés avant d'installer l'application et d'importer les données de vulnérabilité dans votre ServiceNow AI Platform® instance.

Remarque : Si vous avez importé des données avec l'intégration créée par Tenable et que vous souhaitez commencer à utiliser l'intégration ServiceNow® de réponse aux vulnérabilités avec Tenable, consultez les

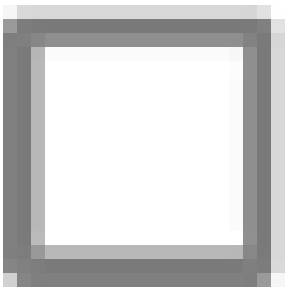
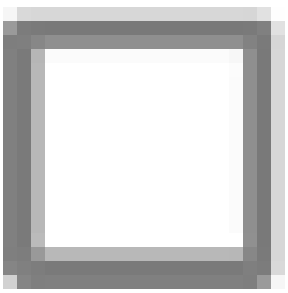
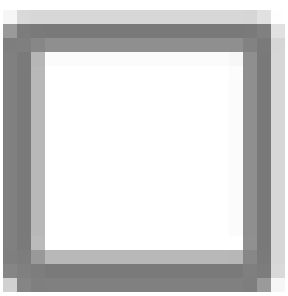
Pour obtenir des informations à jour sur le nettoyage des données et la migration de l'intégration créée par Tenable vers l'intégration créée par ServiceNow, consultez les directives de migration de l'intégration Tenable Vulnerability Response vers l'article Intégration ServiceNow Vulnerability Response avec Tenable [KB0960667].

Rôle requis : administrateur pour télécharger et installer l'application.

Tâche	Description
	(Facultatif) Si elle n'est pas déjà installée et activée, vous préférerez peut-être installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour plus d'informations sur l'installation et l'activation de l'application, Installer Réponse aux vulnérabilités reportez-vous à la Réponse aux vulnérabilités section . Cette intégration requiert la version 12.1 ou ultérieure Réponse aux vulnérabilités .

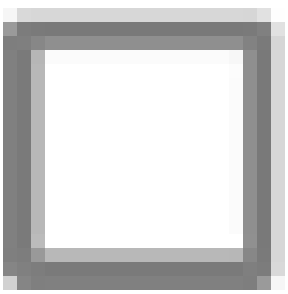
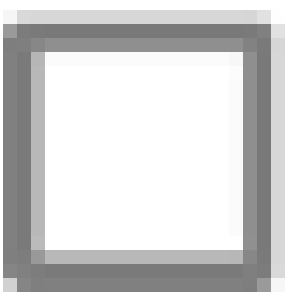
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Si vous ne l'avez pas déjà sur votre instance, obtenez des autorisations et téléchargez l'application Vulnerability Response integration with Tenable sur votre ServiceNow AI Platform® instance. L'application Vulnerability Response integration with Tenable prend en charge le produit à partir de la version 5.13 et Tenable.cs le produit à partir de la Tenable.sc version 5.0.1. .
	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, ou si vous avez besoin d'aide, contactez ServiceNow® l'assistance technique.
	Vérifiez que vous disposez de groupes ou d'utilisateurs pour gérer les intégrations et corriger les éléments vulnérables. **administrateur** L'administrateur système utilise l'assistant de configuration pour installer l'application Vulnerability Response integration with Tenable . S'il n'est pas affecté, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'assistant de configuration. **sn_vul.vulnerability_admin** Une fois affecté, l'administrateur de vulnérabilité termine la configuration des intégrations Tenable. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Configure toutes les applications et règles VR et configure les intégrations tierces. **sn_vul_tenable.configure_integration** Peut configurer l'intégration de vulnérabilité Tenable. Ce rôle contient le rôle granulaire sn_vul_tenable.read_integration. **sn_vul_tenable.read_integration** Peut afficher (lire) les enregistrements de l'intégration de vulnérabilité Tenable. **Groupe de réponse aux vulnérabilités** Par défaut, le groupe Réponse aux vulnérabilités est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Réponse aux vulnérabilités héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner. L'administrateur système effectue l'affectation initiale des rôles aux utilisateurs et aux groupes dans l'assistant de configuration pour l'intégration. Par défaut, le groupe Vulnerability Response

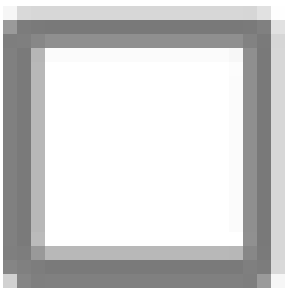
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	est disponible. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance avant d'utiliser l'Assistant de configuration. Voir Créer un groupe d'utilisateurs . Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.
	Pour améliorer les performances de votre première importation, vous pouvez désactiver certaines fonctionnalités, règles ou travaux dans votre instance. • Désactivez les calculateurs de vulnérabilité si vous ne les utilisez pas. Ces calculateurs, ainsi que ceux que vous avez définis, s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour. Voir Désactiver les calculateurs de vulnérabilité. • Lors de l'importation initiale d'enregistrements, certaines règles métier liées aux notifications peuvent entraîner la génération de nombreuses notifications, ce qui a un impact sur les performances. Avant votre importation initiale, vous préférerez peut-être désactiver les règles métier liées aux notifications, comme décrit dans .Importer des modifications pour l'intégration de vulnérabilité Tenable
	Vérifiez que vous avez activé toutes les fonctionnalités, règles, dépendances, modules d'extension ou tâches dans votre instance requis pour l'intégration. • Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le Vulnerability Response integration with Tenable produit et votre ServiceNow AI Platform instance se trouvent dans le même environnement. Si le Tenable.sc produit et votre ServiceNow AI Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID. Pour plus d'informations sur les serveurs MID dans votre instance, consultez Serveur MID . • Vérifiez que le module d'extension Centre d'intégration est installé et activé. Ce module d'extension permet aux composants du système de base d'appeler des systèmes externes à l'aide

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	d'API d'intégration et active les étapes de protocole telles que REST. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous** et localisez le module d'extension. S'il n'est pas installé dans votre instance, installez-le et activez-le.
	Obtenir les informations d'identification Tenable. Vérifiez que vous disposez des noms de compte, mots de passe et autres informations de service requis par vos produits Tenable afin d'y avoir accès. Tenable.io nécessite l'accès Administrateur avec un attribut d'autorisation supérieur ou égal à 64. Tenable.sc nécessite l'accès d'analyste ou de gestionnaire de sécurité. **Remarque :** À partir de la version 3.8 de , l'accès Vulnerability Response integration with TenableTenable.io ne nécessite plus de privilèges d'administrateur. Un utilisateur de base avec un attribut d'autorisation égal à 16 peut également accéder au produit.

Vous êtes prêt à Installer l'application à l'aide de l'assistant Vulnerability Response integration with Tenable de configuration.

Installer l'application à l'aide de l'assistant Vulnerability Response integration with Tenable de configuration

Avant d'exécuter l'intégration ServiceNow® de vulnérabilité Tenable, vous devez télécharger l'application Vulnerability Response integration with Tenable à partir de et ServiceNow Store l'installer et la configurer à l'aide de l'assistant de configuration de l'application Réponse aux vulnérabilités .

Avant de commencer

Avant d'installer l'application Tenable, vérifiez que vous avez rempli tous les éléments de la liste de vérification dans Préparation à l'intégration de vulnérabilité Tenable.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Rôles requis : administrateur pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application Tenable dans l'assistant de configuration. Administrateur de vulnérabilité (sn_vul.vulnerability_admin ou sn_vul.admin (obsolète) pour configurer l'application dans l'Assistant de configuration après son installation.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation de l'application d'intégration**.

   Après quelques instants, les applications disponibles pour installation sur votre instance s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Localisez la tuile **Tenable (Tenable Platform)** et cliquez sur **Installer**.

   Cette action installe l'application Vulnerability Response integration with Tenable que vous avez téléchargée à partir du ServiceNow Store.

3. Suivez les instructions fournies dans l'assistant de configuration pour poursuivre l'installation.

4. Pour plus d'informations sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.

Que faire ensuite

Une fois l'installation terminée dans l'Assistant de configuration, accédez à **Configuration de l'intégration>Intégrations des scanners dans l'Assistant** de configuration pour poursuivre la configuration. Si vous souhaitez obtenir plus d'informations pour compléter les invites fournies dans l'Assistant de configuration, reportez-vous à la section Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration.

Paramètres de récupération de données pour l'intégration de vulnérabilité Tenable

Les paramètres de récupération de données suivants vous aident à déterminer spécifiquement le type et l'étendue des données que vous souhaitez importer de l'intégration ServiceNow® de vulnérabilité Tenable vers votre ServiceNow AI Platform® instance.

Les paramètres décrits dans les sections suivantes vous aident à contrôler les données que vous souhaitez importer. En outre, vous pouvez définir les valeurs de ces filtres dans les instances d'intégration. Pour afficher les instances d'intégration, accédez à **Intégration de vulnérabilité Tenable** > **Instances d'intégration** et sélectionnez votre intégration, Tenable.io, Tenable.sc ou Tenable.cs.

Sur la page Instance d'intégration qui s'affiche, sélectionnez les paramètres d'instance d'intégration pour afficher une liste de paramètres, ou les onglets Intégrations de vulnérabilité pour un calendrier, les détails REST, les détails de l'intégration, les sources de données et les informations sur l'exécution de l'intégration.

Paramètres et filtres de gravité et de récupération communs pour Tenable.io et Tenable.scTenable.cs dans votre ServiceNow AI Platform instance

Les paramètres suivants sont disponibles pour les Tenable.io intégrations , Tenable.sc et dans Tenable.cs votre ServiceNow AI Platform instance. Ces paramètres de configuration et d'autres sont affichés sur la page Instance d'intégration de votre ServiceNow AI Platform instance. Vous préférez peut-être laisser ces paramètres par défaut pour les premières exécutions d'intégration.

Tenable.io

insert_fixed

Si vous activez le marqueur **insert_fixed** dans l'assistant de configuration pour l'intégration d'importation des vulnérabilités, de nouveaux éléments vulnérables sont créés pour les détections à l'état **Fixe** qui n'existent pas dans votre instance.

severity_critical

Ce filtre est activé par défaut (vrai) pour recevoir les Tenable.io vulnérabilités de gravité critique à partir des intégrations de vulnérabilités ouvertes et Tenable.io de vulnérabilités corrigées.

severity_high

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de gravité élevée à partir des intégrations de Tenable.io vulnérabilités ouvertes et Tenable.io de vulnérabilités corrigées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

severity_medium

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité moyenne à partir des intégrations de Tenable.io vulnérabilités ouvertes et Tenable.io de vulnérabilités corrigées.

severity_info

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité au niveau des informations à partir des Tenable.io intégrations Vulnérabilités ouvertes et Tenable.io Vulnérabilités corrigées.

severity_low

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité faible provenant des intégrations de Tenable.io vulnérabilités ouvertes et Tenable.io de vulnérabilités corrigées.

taille

Ce paramètre définit le nombre d'enregistrements de module d'extension à inclure dans le jeu de résultats de l'intégration des modules d'extension Tenable.io . Doit être au format int32. La valeur par défaut est 1 000. La taille maximale est de 10 000.

num_assets

Le nombre maximal de vulnérabilités par bloc exporté à partir des intégrations de vulnérabilités corrigées et Tenable.io de Tenable.io vulnérabilités ouvertes. La valeur par défaut est 50.

chunk_size

Spécifie le nombre d'actifs par bloc exporté par l'intégration Tenable.io des actifs. La valeur par défaut est 1 000.

Tenable.sc

async_request

Ce paramètre est désactivé par défaut (faux). Activez ou désactivez ce paramètre pour effectuer des appels d'API asynchrones ou synchrones avec Tenable.sc respectivement. Pour les appels synchrones, s'il y a un délai d'expiration de 30 secondes, contactez le support du produit Tenable pour régler la boîte. Ce paramètre, une fois activé, est applicable à toutes les intégrations de Tenable.sc. Pour les clients existants utilisant des appels asynchrones, un script correctif est disponible, qui ajoute un nouveau paramètre async_request aux instances d'intégration existantes Tenable.sc . Pour afficher les scripts correctifs, accédez à **Définition du système** > **Scripts correctifs**.

insert_fixed

Si vous activez le marqueur **insert_fixed** dans l'assistant de configuration pour l'intégration d'importation des vulnérabilités, de nouveaux éléments vulnérables sont créés pour les détections à l'état **Fixe** qui n'existent pas dans votre instance.

décalage

Spécifie le nombre d'actifs, de modules d'extension et de vulnérabilités importés en une seule exécution d'intégration.

Filtres de requête

Les filtres de requête sont configurés à partir de la console Tenable. Ces filtres de requête ont des ID qui peuvent être sélectionnés à partir de l'Assistant de configuration ou de la page Instances d'intégration de votre ServiceNow AI Platform instance. Ces filtres sont appliqués lors de la récupération des données à partir des Tenable.sc intégrations.

Tenable.cs

compute_severity_critical

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce filtre est activé par défaut (vrai) pour recevoir les vulnérabilités de gravité critique de l'intégration des vulnérabilités de l'hôte dans le cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte dans le Tenable.cs cloud corrigé.

compute_severity_high

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de gravité élevée provenant de l'intégration des vulnérabilités de l'hôte cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte Tenable.cs cloud fixe.

compute_severity_medium

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité moyenne provenant de l'intégration des vulnérabilités de l'hôte cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte Tenable.cs cloud corrigé.

compute_severity_info

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité de niveau d'informations provenant de l'intégration des vulnérabilités de l'hôte cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte Tenable.cs cloud corrigé.

compute_severity_low

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de faible gravité provenant de l'intégration des vulnérabilités de l'hôte cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte Tenable.cs cloud fixe.

container_severity_critical

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de conteneur de gravité critique à partir de l'intégration des vulnérabilités des conteneurs dans le cloud ouverts et Tenable.cs de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

container_severity_high

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de conteneur de gravité élevée à partir de l'intégration des vulnérabilités des conteneurs dans le cloud ouverts et Tenable.cs de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

container_severity_medium

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de conteneur de gravité moyenne à partir de l'intégration des vulnérabilités des conteneurs dans le cloud ouverte et Tenable.cs de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

container_severity_info

Ce filtre est inactif par défaut (faux). Activer ce filtre pour recevoir des vulnérabilités de gravité de niveau d'informations Vulnérabilités du conteneur Vulnérabilités de l'intégration des vulnérabilités des conteneurs dans le cloud ouvert et Tenable.cs intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

container_severity_low

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de conteneur de gravité faible à partir de l'intégration des vulnérabilités des conteneurs dans le cloud ouverte et Tenable.cs de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

asset_page_limit

Ce paramètre définit le nombre d'enregistrements d'actifs de conteneur à inclure dans l'ensemble de résultats de Cloud Tenable.cs Container Assets Integration. La valeur par défaut est 1 000. La taille maximale est de 1 000.

vuln_page_limit

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce paramètre définit le nombre d'enregistrements de vulnérabilités à inclure dans l'ensemble de résultats de l'intégration des vulnérabilités de l'hôte cloud ouvert, Tenable.cs de l'intégration Tenable.cs des vulnérabilités de l'hôte cloud fixe, de l'intégration des vulnérabilités du conteneur cloud ouvert et Tenable.cs de l'intégration Tenable.cs des vulnérabilités du conteneur cloud fixe. La valeur par défaut est 1 000. La taille maximale est de 10 000.

Messages REST pour l'intégration de vulnérabilité Tenable

Les ServiceNow® messages REST de l'intégration de vulnérabilité Tenable sont utilisés pour effectuer des appels à l'API Tenable.

Tenable.io Message REST sur les actifs

Le Tenable.io message REST Actifs récupère les informations sur les actifs pour l'intégration Tenable.io des actifs. Les changements apportés à l'enregistrement de la méthode de message REST ont un impact sur les demandes de Tenable.io récupération des informations sur les actifs. La tâche d'exportation des actifs est soumise avec les filtres suivants :

- « is_deleted » : faux
- « is_licensed » : vrai

Tenable.io Message REST des modules d'extension

Le Tenable.io message REST Modules d'extension récupère les informations sur le module d'extension pour l'intégration du module d'extension Tenable.io . Les changements apportés à l'enregistrement de la méthode de message REST ont un impact sur les demandes de récupération des informations des modules d'extension Tenable.io .

Tenable.io Message REST de vulnérabilités

Le Tenable.io message REST sur les vulnérabilités récupère les informations sur les vulnérabilités ouvertes et fermées à partir de l'intégration Tenable.io des vulnérabilités. Les changements apportés à l'enregistrement de la méthode de message REST ont un impact sur les demandes de Tenable.io récupération des informations sur les vulnérabilités.

Tenable.sc requêtes du message REST

Le message REST Tenable.sc requêtes récupère les informations du filtre de requête pour l'intégration des actifs Tenable.sc et l'intégration des vulnérabilités Tenable.sc où le filtre de requête est configuré.

Tenable.sc Message REST des modules d'extension

Le Tenable.sc message REST du module d'extension récupère les informations sur le module d'extension pour l'intégration des modules d'extension Tenable.sc . Les changements apportés au message REST Obtenir l'enregistrement de méthode des modules d'extension ont un impact sur les demandes effectuées pour récupérer les informations des modules d'extension Tenable.sc .

Nom de paramètre	Valeur	Description
type	actif	Indique la source à partir de laquelle Tenable extrait les données. Utilisé par le code. Il n'est pas recommandé d'apporter des changements.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
champs	id, description, cvssVector,cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso, solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	Indique la liste des champs importés de Tenable.

Tenable.sc Message REST de vulnérabilités

Le Tenable.sc message REST de vulnérabilités récupère les informations sur les vulnérabilités à partir de l'intégration Tenable.sc . Les modifications apportées au message REST La méthode Extraire les vulnérabilités ou Extraire les vulnérabilités corrigées ou, à partir des versions 14.0 Réponse aux vulnérabilités et 2.2 de l'intégration de vulnérabilité Tenable, Extraire l'enregistrement des vulnérabilités de remplissage a un impact sur les demandes effectuées Tenable.sc pour récupérer les informations sur les vulnérabilités.

Tenable.sc Message REST des informations d'identification de numérisation

Tenable.sc Message REST de la politique

Le Tenable.sc message POST REST de la politique ajoute une politique pour les modules d'extension demandés. La politique générée est utilisée dans les Tenable.sc demandes d'analyse.

Tenable.sc Analyser le message REST

Le message REST POST de l'analyse Tenable.sc ajoute une analyse qui dépend de l'accès et de l'autorisation définis dans le corps de la demande du message REST. Elle utilise la politique, l'ID du module d'extension et la ou les adresses IP dans le corps de la demande pour la demande d'analyse.

Tenable.sc Message REST du résultat de l'analyse

Le Tenable.sc message REST GET de résultat d'analyse fournit les détails de l'analyse générée à l'aide du message REST d'analyse. Elle utilise scanResultId dans la réponse des messages REST d'analyse et récupère les détails de l'analyse déclenchée.

Tenable.sc Informations d'identification de numérisation

Le Tenable.sc message REST des informations d'identification de numérisation récupère les informations d'identification à partir de Tenable.sc. Les modifications apportées à l'enregistrement de la méthode « Importer » du message REST ont un impact sur les demandes de Tenable.sc récupération des informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
champs	ID, nom, description, type	Indique la liste des champs importés à partir de Tenable.sc
filtre	utilisable	Indique que l'intégration extrait uniquement les informations d'identification utilisables de Tenable.sc Il n'est pas recommandé de modifier l'un ou l'autre des paramètres.

Tenable.cs Message REST GraphQL : le Tenable.cs message REST GraphQL récupère les informations sur l'actif du conteneur, l'hôte et les informations de vulnérabilité du conteneur pour Tenable.cs l'intégration. Les modifications apportées au message REST Extraire les actifs du conteneur, Extraire les vulnérabilités du conteneur, Extraire les vulnérabilités de calcul Impact de l'enregistrement Tenable.cs de la méthode Impact des demandes effectuées pour récupérer les informations sur les actifs et les vulnérabilités.

Transformation des données pour l'intégration de vulnérabilité Tenable

Une fois que vous avez identifié les données à importer, elles sont récupérées à partir du produit Tenable et traitées via un ensemble de sources de données et transformées dans votre instance.

Lors de l'installation, les cartes de gravité normalisées sont installées dans le module Mappage de gravité normalisée. Ces cartes transforment les niveaux de gravité Tenable importés en niveaux de gravité standard pour le traitement dans votre instance. Pour plus d'informations sur la création de cartes de gravité, consultez Créer une carte de gravité de Vulnerability Response dans la Réponse aux vulnérabilités documentation.

Importation d'actif Tenable.io

Les données d'actif importées sont d'abord chargées dans la table d'importation d'actif Tenable.io [sn_vul_tenable_io_asset_import].

La carte de transformation de l'intégration des actifs Tenable.io est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données de l'importation d'actif Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez Tenable.io transformation d'actif.

La table suivante répertorie les champs de carte de transformation par intégration.

Tenable.io Champs de carte de transformation d'actif

Champ source	Champ cible	Description
u_id	source_id	Tenable fournit un ID unique pour les actifs et les mappe à l'enregistrement de l'élément détecté et est utilisé pour la recherche de CI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.io Champs de carte de transformation d'actif (suite)

Champ source	Champ cible	Description
u_ipv4s	ip_address	Mappe la première valeur IP au champ ip_address de l'enregistrement de l'élément détecté.
u_mac_addresses	mac_address	Mappe la première valeur mac_address au champ d'adresse mac de l'enregistrement d'élément détecté.
u_fqdns	fqdn	Mappe la première valeur FQDN au champ FQDN de l'enregistrement d'élément détecté.
u_netbios_names	Netbios	Mappe la première valeur NetBIOS au champ NetBIOS de l'enregistrement d'élément détecté.
u_operating_systems	système d'exploitation	Mappe la première valeur du système d'exploitation au champ du système d'exploitation de l'enregistrement de l'élément détecté.
(Avant les versions 14.0 Réponse aux vulnérabilités et 2.2 de l'intégration de vulnérabilité Tenable u_last_scan_time	last_scan_date	Mappé au champ last_scan_date de l'enregistrement de l'élément détecté.
u_last_authenticated_scan_date	last_auth_scan_date	Mappé au champ last_auth_scan_date de l'enregistrement de l'élément détecté.
[script]	nom	Mappe le nom d'hôte à l'aide de la logique du script.
u_tags		Les balises sont enregistrées dans sn_sec_cmn_host_tag. Le mappage des balises aux actifs est enregistré dans sn_sec_cmn_m2m_src_ci_tag.

Traduction automatique

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Tenable.io Transformation de l'actif : script, synchronisation et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Initialise les valeurs du import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque le script est exécuté	Objectif
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Met à jour les valeurs dans l'hôte et vérifie si l'hôte existe. En fonction des résultats, modifie les valeurs d'un import_set. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Définit les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Intégration des modules d'extension Tenable.io

La carte de transformation des modules d'extension Tenable.io est utilisée pour transformer les modules d'extension importés à partir de Tenable.io.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données reçues des modules d'extension Tenable sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la transformation du module d'extension Tenable.io.

La charge utile des modules d'extension tenable.io contient tous les champs de la colonne u_attributes de la table sn_vul_tenable_io_plugin_import. Le champ d'attributs est analysé et mappé aux enregistrements de la table d'entrée tierce, tels que répertoriés dans la table suivante.

Champ source	Champ cible	Description
id	id	Mappe l'ID à partir de la source et y ajoute le préfixe TEN. Par exemple, si l'ID reçu est 12345, l'ID dans la table cible est TEN-12345.
Description	résumé	Mappe la description du module d'extension à la colonne de résumé.
[script]	source	La source de l'entrée tierce importée (TPE) est Tenable.io.
[script]	source_instance	Référence au déploiement Tenable qui importe cet enregistrement.
famille	catégorie	Mappe la famille de module d'extension à la colonne de catégorie
plugin_modification_date	last_modified	Mappe le plugin_modification_date au champ de la dernière modification.
plugin_publication_date	date_published	Mappe le plugin_publication_date à la date de publication.
has_patch	remediation_type	Mappe le type de rattrapage à partir de has_patch valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
synopsis	menace	Mappe les informations sur cette vulnérabilité.
cvss_base__score	score	Mappe le score de base du système de notation des vulnérabilités courantes (CVSS) à la colonne de score dans la table d'entrée tierce.
solution	solution	Mappe la solution fournie par le scanner à la colonne de solution dans la table d'entrée tierce.
exploit_available	exploit	Mappe le exploit_available fourni par le scanner à la colonne Exploit dans la table d'entrée tierce.
vpr.score	source_risk_score	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9–10 – Critique • 7–9 – Élevé • 4 à 7 – Moyen • 0–4 : faible
vpr.drivers.age_of_vuln	age_of_vuln	Mappe l'âge de la vulnérabilité du scanner à la colonne age_of_vuln dans la table d'entrée tierce.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
vpr.drivers.product_coverage	product_coverage	Mappe la couverture du produit du scanner à product_coverage dans la table d'entrée tierce.
vpr.drivers.threat_sources_last28	threat_sources	Mappe les sources de menace au cours des 28 derniers jours, du scanner au threat_sources dans la table tierce.
vpr.drivers.threat_intensity_last28	threat_intensity	Mappe l'intensité de menace au cours des 28 derniers jours du scanner à la threat_intensity dans la table d'entrée tierce.
vpr.drivers.threat_recency	threat_recency	Mappe les informations sur la récence des menaces du scanner à la threat_recency dans la table d'entrée tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mappe le score d'impact cvss3 à v3_impact_subscore colonne de la table d'entrée tierce.
cvss_temporal_score	cvss_temporal_score	Mappe le score temporel pour CVSS v2.
cvss_v3_temporal_score	v3_temporal_score	Mappe le score temporel pour CVSS v3.
risk_factor	source_severity	Mappe à la gravité de la source dans la table d'entrée tierce.
nom	nom	Mappe le nom du module d'extension au nom dans la table d'entrée tierce.
stig_severity	stig_severity	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
plugin_type	check_type	Mappe le type de module d'extension à check_type dans la table d'entrée tierce.
unsupported_by_vendor	unsupported_by_vendor	Mappe le champ unsupported_by_vendor à la colonne unsupported_by_vendor.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction du exploit_available et de l'v3_attack_vector des colonnes.

En plus des champs directs, d'autres informations sont ajoutées en tant que listes connexes aux entrées tierces.

Champ source	Description
cve	Insère les données liées à CVE dans la table de référence (sn_vul_nvd_entry). Si les mêmes vulnérabilités et expositions courantes (CVE) dans la table d'entrée NVD (sn_vul_nvd_entry) sont trouvées, elles associent la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
offre	La liste des transactions de bogues est ajoutée à titre de référence.
see_also	La liste des URL est ajoutée en tant que référence.
xrefs	La liste de X-REF est ajoutée à titre de référence.
[script]	Liste des exploits pour ce module d'extension et mappage des insertions pour le cadre de travail de l'exploit et le module d'extension applicables à sn_vul_m2m_framework_vul.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Initialise les valeurs du import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Met à jour les valeurs de l'entrée tierce et vérifie si l'entrée tierce existe. En fonction des résultats, modifie les valeurs d'une entrée tierce. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Définit les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

L'include de script TenableIOPluginsImportProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de l'intégration des modules d'extension de Tenable.io et la transforme en ServiceNow AI Platform entrées de vulnérabilité tierces. Tout changement apporté à cet include de script peut altérer la transformation des données des modules d'extension de Tenable.io dans la table d'entrée tierce.

Tenable.io l'importation des vulnérabilités

La carte de transformation d'élément vulnérable Tenable.io est utilisée pour transformer les informations sur les vulnérabilités ouvertes et corrigées importées à partir de Tenable.io.

Remarque : Les changements apportés à cette carte de transformation modifient la façon dont les données de l'importation des vulnérabilités de Tenable sont traitées.

La même carte de transformation est utilisée pour l'intégration des vulnérabilités corrigées Tenable.io et l'intégration des vulnérabilités ouvertes Tenable.io. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la carte de transformation de l'élément vulnérable Tenable.io.

Champ source	Champ cible	Description
u_asset.uuid	id	L'UUID est mappé au champ d'ID de l'enregistrement cmdb_ci.
u_asset.ipv4	ip_address	Le champ ipv4 est mappé au champ d'adresse IP de l'enregistrement cmdb_ci.
u_asset.last_authenticated_results	last_auth_scan_date	La date de la dernière analyse authentifiée est mappée à la date de la dernière analyse d'authentification de l'enregistrement cmdb_ci.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_asset.mac_addess	mac_address	L'adresse Mac est mappée au champ adresse MAC de l'hôte de l'enregistrement cmdb_ci.
nom_bios u_asset.net	Netbios	NetBIOS est mappé au champ NetBIOS de cmdb_ci enregistrement.
u._plugin.cvss3_base_score	v3_base_score	Le score de base CVSS v3 est mappé au score de base v3 de l'enregistrement d'entrée tierce.
u._plugin.cvss3_score_temporal	v3_temporal_score	Le score temporel CVSS v3 est mappé au score temporel v3 dans l'enregistrement d'entrée tierce.
u._plugin.cvss_score_base	score	Le score de base CVSS est mappé au champ de score de l'enregistrement d'entrée du tiers.
u._plugin.cvss_temporal_score	temporal_score	Le score temporel est mappé au score temporel dans l'enregistrement d'entrée tierce.
u_plugin.description	résumé	La description est mappée au champ Résumé de l'enregistrement d'entrée tierce.
u_plugin.famille	catégorie	Mappe la famille de modules d'extension à la colonne catégorie de l'enregistrement d'entrée tiers.
u_plugin.modification_date	last_modified	La date de la dernière modification est mappée à la date de la dernière modification du module d'extension dans l'enregistrement d'entrée tierce.
u_plugin.publication_date	date_published	La date de publication est mappée au champ de date de publication de l'enregistrement d'entrée tierce.
u_plugin.facteur_risque	source_severity	Le facteur de risque est mappé au champ source_severity de l'enregistrement d'entrée tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_plugin.solution	solution	La solution est mappée au champ de solution de l'enregistrement d'entrée tierce.
u_plugin.synopsis	menace	Synopsis est mappé au champ Menace de l'enregistrement d'entrée tierce.
u_severity_id	Priorité	La priorité est mappée à l'ID de gravité de la charge utile. La valeur par défaut est de 5.
u_plugin.exploit_available	exploit	Mappe le exploit_available fourni par le scanner à la colonne Exploit dans la table d'entrée tierce.
vpr.score	source_risk_score	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9–10 – Critique • 7–9 – Élevé • 4 à 7 – Moyen • 0–4 : faible
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	Mappe l'âge de vulnérabilité du scanner à age_of_vuln dans la table d'entrée tierce.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mappe la couverture du produit du scanner à product_coverage dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	Mappe les sources de menace au cours des 28 derniers jours à partir du scanner pour threat_sources dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	Mappe l'intensité de menace au cours des 28 derniers jours du scanner à la threat_intensity dans la table d'entrée tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_plugin.vpr.drivers.threat_recency	threat_recency	Mappe les informations sur la récence des menaces du scanner aux threat_recency dans la table d'entrée tierce.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mappe le score d'impact CVSS3 v3 à v3_impact_subscore colonne de la table d'entrée tierce.
u_plugin.type	check_type	Mappe le type de module d'extension à check_type dans la table d'entrée tierce.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Mappe le champ unsupported_by_vendor dans le module d'extension à la colonne unsupported_by_vendor.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction du exploit_available et de l'v3_attack_vector des colonnes.
u_plugin.family_id	Family_id	Mappe l'ID de famille du module d'extension à family_id colonne dans la table d'entrée tierce.
port	port	Le port est mappé au champ port de l'enregistrement d'élément vulnérable.
protocol	protocol	Le protocole est mappé au champ Protocole de l'enregistrement d'élément vulnérable.
u_first_found	first_found	Le premier trouvé est mappé au champ premier trouvé de l'enregistrement d'élément vulnérable.
u_last_found	last_found	Dernier trouvé est mappé au champ Dernier trouvé de l'enregistrement d'élément vulnérable.
u_state	État	L'état est mappé au champ État dans l'enregistrement d'élément vulnérable
[script]	source	La source de l'intégration est renseignée. Les éléments vulnérables créés à partir

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		de cette intégration ont Tenable.io comme source.
[script]	integration_instance	Le integration_instance est le nom de l'instance à partir de laquelle l'élément vulnérable est importé.
u_plugin.nom	nom	Mappe le nom du module d'extension au nom dans la table d'entrée tierce.
u_plugin.stig_severity	stig_severity	Mappe la gravité stig du module d'extension à la colonne de gravité stig dans la table d'entrée tierce

En plus des champs directs, d'autres informations sont ajoutées en tant que listes connexes aux entrées tierces.

Champ source	Description
cve	Insère les données liées à CVE dans la table de référence (sn_vul_nvd_entry). Si le même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvé, il associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
offre	La liste des transactions de bogues est ajoutée à titre de référence.
see_also	La liste des URL est ajoutée en tant que référence.
xrefs	La liste de X-REF est ajoutée à titre de référence.
[script]	La liste des exploits pour ce module d'extension et insère le mappage pour le cadre de travail de l'exploit et le module d'extension applicables à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	TTriggers Processeurs de vulnérabilités IO Tenable qui importe les données de Tenable.io à l'aide du jeu d'importation et charge chaque enregistrement dans la table CI CMDB, la table Éléments vulnérables et la table Vulnérabilité tierce. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Vérifie si l'entrée et les détections tierces existent. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. n'est pasCe script est

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque le script est exécuté	Objectif
	destiné à un usage interne. Il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Met à jour le nombre de CI, de VIT et de détections tels qu'importés à partir de Tenable.io. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Importation d'actif Tenable.sc

Les données d'actif importées à partir de Tenable.sc sont d'abord chargées dans la table d'importation d'actif Tenable.sc (sn_vul_tenable_sc_asset_import). La carte de transformation de l'intégration des actifs Tenable.sc est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données de l'importation d'actif Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la transformation de l'actif Tenable.sc.

Champ source	Champ cible	Description
u_uuid	id	L'uuid n'est pas renseigné à partir de l'API Tenable, c'est pourquoi l'attribut « u_uniqueness » est utilisé pour créer un champ uuid unique pour les actifs et le mapper à l'enregistrement cmdb_ci.
u_ip	ip_address	Mappe le champ IP de l'API au champ ip_address d'un enregistrement cmdb_ci.
u_macaddress	mac_address	Mappe le champ d'adresse mac de l'API au champ d'adresse de l'enregistrement cmdb_ci.
u_dnsname	fqdn	Mappe le champ dnsname de l'API au champ FQDN sur l'enregistrement cmdb_ci.
u_netbiosname	Netbios	Mappe le champ netbios de l'API au champ netbios sur l'enregistrement cmdb_ci.
u_oscpe	système d'exploitation	Les informations sur le système d'exploitation sont extraites de l'attribut oscpe dans la charge utile et les mappent au champ du système d'exploitation de l'enregistrement cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mappe le champ lastauthrun de l'API au champ last_auth_scan_date de l'enregistrement de l'élément détecté.
u_lastauthrun et u_lastunauthrun	last_scan_date	Le lastauthrun est extrait de l'API Tenable ou lastunauthrun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		Le champ last_scan_date de l'enregistrement d'élément détecté est renseigné en fonction de la valeur qui apparaît dans la charge utile.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Initialise les valeurs du import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Met à jour les valeurs dans l'hôte et vérifie si l'hôte existe. En fonction des résultats, modifie les valeurs d'un import_set. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Définit les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.sc l'importation des modules d'extension

Les données de modules d'extension importées à partir de Tenable.sc sont d'abord chargées dans la table d'importation de modules d'extension Tenable.sc (sn_vul_tenable_sc_plugin_import). La carte de transformation du module d'extension Tenable.sc est utilisée pour transformer les informations des modules d'extension qui ont été importées. Les changements apportés à cette transformation modifient la façon dont les données provenant de l'importation du module d'extension Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez Tenable.sc carte de transformation du module d'extension.

Champ source	Champ cible	Description
u_id	id	Mappe l'ID à partir de la source et ajoute le préfixe TEN. Par exemple, si l'ID reçu est 12345, l'ID dans la table cible est TEN-12345.
u_description	résumé	Mappe la description du module d'extension à la colonne de résumé.
[script]	source	Le TPE importé à partir de cette intégration a Tenable.sc comme source.
[script]	source_instance	Référence au déploiement Tenable qui importe cet enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_family	catégorie	Mappe le champ nom dans l'objet de famille du module d'extension à la colonne catégorie.
u_plugin_modification_date	last_modified	Mappe le plugin_modification_date au champ de la dernière modification.
u_plugin_publication_date	date_published	Mappe le plugin_publication_date à la date de publication.
u_has_patch	Remediation_type	Mappe le type de rattrapage à partir de has_patch valeur.
u_synopsis	menace	Mappe les informations sur cette vulnérabilité.
u_cvss_base_score	score	Mappe le score de base CVSS à la colonne de score dans la table d'entrée tierce.
u_solution	solution	Mappe la solution fournie par le scanner à la colonne de solution dans la table d'entrée tierce.
u_cvss_temporal_score	cvss_temporal_score	Mappe le score temporel pour CVSS v2.
u_cvss_v3_temporal_score	v3_temporal_score	Mappe le score temporel pour CVSS v3.
u_risk_factor	Gravité de la source	Mappe à la gravité de la source dans la table d'entrée tierce.
u_cvss_v3_base_score	v3_base_score	Mappe le score de base CVSS dans la table d'entrée tierce.
u_exploit_available	exploit	Mappe l'exploitAvailable fourni par le scanner à la colonne exploit dans la table d'entrée tierce.
u_vpr_score	source_risk_score	Mappe le score VPR du scanner au score de risque source dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9–10 – Critique • 7–9 – Élevé • 4 à 7 – Moyen • 0–4 : faible
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mappe l'âge de la vulnérabilité du scanner à age_of_vuln dans la table d'entrée tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_vpr_context[id=product_coverage]	product_coverage	Mappe la couverture du produit du scanner à product_coverage dans la table d'entrée tierce.
u_vpr_context[id="threat_sources_last_28"]	threat_sources	Mappe les sources de menace au cours des 28 derniers jours, du scanner au threat_sources dans la table tierce.
u_vpr_context[id="threat_intensity_last_28"]	threat_intensity	Mappe l'intensité de menace au cours des 28 derniers jours du scanner à la threat_intensity dans la table d'entrée tierce.
u_vpr_context[id="threat_recency"]	threat_recency	Mappe les informations sur la récence des menaces du scanner à threat_recency dans la table d'entrée de tiers.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mappe le score d'impact CVSS v3 du scanner à v3_impact_subscore dans la table d'entrée tierce.
u_name	nom	Mappe le nom du module d'extension à la colonne nom dans la table d'entrée tierce.
u_stig_severity	stig_severity	Mappe le champ stig_severity dans le module d'extension à stig_severity dans la table d'entrée tierce.
u_check_type	check_type	Mappe le type de vérification à check_type dans la table d'entrée tierce.
u_family.id	family_id	Mappe le module d'extension family_id à family_id dans la table d'entrée tierce.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction du exploit_available et de l'v3_attack_vector des colonnes.

En plus des champs directs, d'autres informations sont ajoutées en tant que listes connexes aux entrées tierces.

Champ source	Description
u_cpe	La liste des CPE est ajoutée à titre de référence.
u_see_also	La liste des URL est ajoutée en tant que référence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
u_exploit_frameworks	Liste des exploits pour ce module d'extension et mappage des insertions pour le cadre de travail de l'exploit et le module d'extension applicables à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Cette transformation permet d'initialiser les valeurs dans le import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Fonction utilisée pour mettre à jour les valeurs de l'entrée tierce et vérifier si l'entrée tierce existe. En fonction des résultats, modifie les valeurs d'une entrée tierce. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des modules d'extension créés et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

L'include de script TenableSCPluginsImportProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de l'intégration des modules d'extension Tenable.sc et la transforme en ServiceNow entrées de vulnérabilité tierces. Toute modification apportée à cet include de script peut altérer la transformation des données des modules d'extension de Tenable.sc dans la table d'entrée tierce.

Tenable.sc l'importation des vulnérabilités

La carte de transformation des vulnérabilités ouvertes Tenable.sc est utilisée pour transformer les données importées à partir de l'intégration des vulnérabilités ouvertes Tenable.sc, et la carte de transformation des vulnérabilités Tenable.sc et corrigées est utilisée pour transformer les données importées à partir de l'intégration des vulnérabilités corrigées Tenable.sc.

Remarque : Les changements apportés à ces cartes de transformation modifient la façon dont les données de l'importation de vulnérabilités Tenable corrigées/ouvertes sont traitées.

Pour accéder aux Tenable.sc cartes de transformation des vulnérabilités ouvertes et corrigées, accédez à **Intégration de vulnérabilité Tenable** > **Administration** > **Instances d'intégration** > **Tenable.sc l'intégration des vulnérabilités corrigées/ouvertes** > **Sources de données** > **Tenable.sc vulnérabilités ouvertes/corrigées** > **Les transformations**.

Champ source	Champ cible	Description
u_pluginID	ID	Utilisé comme identificateur du module d'extension. Ce champ est mappé à l'ID du

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		module d'extension dans l'enregistrement d'entrée tierce.
u_riskfactor	source_severity	Ce champ est mappé à source_severity dans l'enregistrement d'entrée tierce.
u_severity	Priorité	Le champ de priorité est mappé avec la gravité. La valeur par défaut est de 5.
u_hasbeenmitigated	État	A été atténué est mappé au champ d'état de l'enregistrement de vulnérabilité. Pour l'intégration des vulnérabilités corrigées, tous les VI sont à l'état « Fermé ».
u_ip	ip_address	L'adresse IP est mappée au champ IP de l'hôte de cmdb_ci table.
u_port	port	Le port est mappé au champ port de l'enregistrement d'élément vulnérable.
u_protocol	protocol	Le protocole est mappé au champ de port de l'enregistrement d'élément vulnérable.
u_firstSeen	first_found	La première valeur vue est mappée au premier champ trouvé de l'enregistrement de VI.
u_lastSeen	last_found	La dernière valeur vue est mappée au champ dernier trouvé de l'enregistrement de VI.
u_exploitAvailable	exploit	ExploitAvailable est mappé au champ d'exploit dans l'enregistrement d'entrée tierce.
u_synopsis	menace	Synopsis est mappé au champ Menace dans l'enregistrement d'entrée tierce.
u_description	résumé	La description est mappée au champ Résumé de l'enregistrement d'entrée tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_solution	solution	La solution est mappée au champ Solution dans l'enregistrement d'entrée tierce.
u_basescore	score	BaseScore est mappé au champ de score dans l'enregistrement d'entrée tierce.
u_temporalScore	temporal_score	Le score temporel est mappé au score temporel dans l'enregistrement d'entrée tierce.
u_cvssv3basescore	v3_base_score	Cvssv3basescore est mappé au score de base v3 dans l'enregistrement d'entrée tierce.
u_cvsstemporalscore	v3_temporal_score	Le score temporel Cvssv3 est mappé au score temporel v3 dans l'enregistrement d'entrée tierce.
u_pluginpubdate	date_published	La date de publication du module d'extension est mappée à la date de publication du module d'extension dans l'enregistrement d'entrée tiers.
u_pluginmoddate	last_modified	La date de la dernière modification est mappée à la date de la dernière modification du module d'extension dans l'enregistrement d'entrée tierce.
u_dnsname	fqdn	DnsName est mappé au champ FQDN de l'enregistrement cmdb_ci.
u_macaddress	mac_address	MacAddress est mappé au champ mac_address de l'enregistrement cmdb_ci.
u_netbiosName	Netbios	NetbiosName est mappé au champ NETBIOS de l'enregistrement cmdb_ci.
u_ip	ip	L'adresse IP est mappée au champ IP de cmdb_ci enregistrement.
hostUniqueness	uuid	L'unicité de l'hôte n'est mappée à aucun champ,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		mais est utilisée pour déterminer l'uuid de l'hôte.
u_family	catégorie	Mappe le champ nom de l'objet famille du module d'extension à la colonne catégorie de l'enregistrement d'entrée tierce.
u_plugintext	proof	Le texte du module d'extension est mappé à la preuve dans l'enregistrement TPE.
[script]	source	La source de l'intégration est renseignée. Les éléments vulnérables créés à partir de cette intégration ont Tenable.sc comme source.
[script}	integration_instance	Le integration_instance est le nom de l'instance à partir de laquelle l'élément vulnérable est importé.
u_vpr_score	source_risk_score	Mappe le score VPR du scanner au score de risque source dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 à 7 – Moyen • 0–4 : faible
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mappe l'âge de la vulnérabilité du scanner à age_of_vuln dans la table d'entrée tierce.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_vpr_context[id=product_coverage]	product_coverage	Mappe la couverture du produit du scanner à product_coverage dans la table d'entrée tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_vpr_context[id="threat_sources_last_28]	threat_sources	Mappe les sources de menace au cours des 28 derniers jours, du scanner aux threat_sources dans la table tierce.
u_vpr_context[id="threat_intensity_last_28]	threat_intensity	Mappe l'intensité de menace au cours des 28 derniers jours du scanner à la threat_intensity dans la table d'entrée tierce.
u_vpr_context[id="threat_recency"]	threat_recency	Mappe les informations sur la récence des menaces du scanner à threat_recency dans la table d'entrée de tiers.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mappe le score d'impact CVSS v3 du scanner à v3_impact_subscore dans la table d'entrée tierce.
u_pluginname	nom	Mappe le nom du module d'extension à la colonne de nom dans la table d'entrée tierce.
u_stigseverity	stig_severity	Mappe le champ stig_severity dans le module d'extension à stig_severity dans la table d'entrée tierce.
u_checktype	check_type	Mappe le type de vérification à check_type dans la table d'entrée tierce.
u_family.id	family_id	Mappe le module d'extension family.id à family_id dans la table d'entrée tierce.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table third_party_entry est renseignée en fonction de la exploit_available et de la v3_attack_vector des colonnes.

Champ source	Description
u_cve	Insère les données liées à CVE dans la table de référence (sn_vul_nvd_entry). Si le même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvé,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
	il associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
u_bid	La liste des transactions de bogues est ajoutée à titre de référence.
u_cpe	La liste des CPE est ajoutée à titre de référence.
u_seealso	La liste des URL est ajoutée en tant que référence.
u_xrefs	La liste des X-REF est ajoutée à titre de référence.
u_exploitframeworks	La liste des exploits pour ce module d'extension et insère le mappage pour le cadre de travail de l'exploit et le module d'extension applicables à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Cette transformation permet d'initialiser les valeurs dans le import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Fonction utilisée pour mettre à jour les valeurs de la vulnérabilité et vérifier si la vulnérabilité existe. En fonction des résultats, modifie les valeurs d'une table d'éléments vulnérables. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux VI créés et des VI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.cs Importation d'actif de conteneur

Les données d'actif importées sont d'abord chargées dans la table d'importation d'actif Tenable.cs de conteneur [sn_vul_tenable_cs_container_asset_import].

La Tenable.cs carte de transformation d'actif de conteneur est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données de l'importation d'actif de Tenable.cs conteneur sont traitées. Pour accéder à cette carte de transformation, accédez à Jeux d'importation système > Cartes de transformation. Recherchez la transformation de Tenable.cs l'actif de conteneur.

Les tables suivantes répertorient les champs de carte de transformation par intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation d'actif de conteneur

Champ source	Champ cible	Description
u_digest	Image_id	Tenable fournit une synthèse unique pour les actifs du conteneur et est mappé à l'image du conteneur détecté et à l'enregistrement de l'image Docker. Il est utilisé pour la recherche de CI.
u_digest	Image_digest	Tenable fournit une synthèse unique pour les actifs du conteneur et est mappé à l'image du conteneur détecté et à l'enregistrement de l'image Docker. Il est utilisé pour la recherche de CI.
u_name	nom	Mappé au champ de nom de l'enregistrement d'image Docker.
u_repositoryuri	nom	Mappé à l'enregistrement du référentiel du conteneur
u_repositoryuri	réf.	Mappe à l'enregistrement d'image du conteneur détecté.
u_virtualmachines	host_list	Mappe à l'enregistrement d'image du conteneur détecté
u_labels	Image_labels	Mappe la première valeur du système d'exploitation au champ de système d'exploitation de l'enregistrement de l'élément détecté.
u_clusters	image_cluster	Mappe à l'enregistrement d'image du conteneur détecté
u_imagetags	balises	Mappe à l'enregistrement d'image du conteneur détecté
u_cloudprovider	cloud_providers	Mappe à l'enregistrement d'image du conteneur détecté
u_accountid	cloud_account_ids	Mappe à l'enregistrement d'image du conteneur détecté
u_region	cloud_regions	Mappe à l'enregistrement d'image du conteneur détecté
u_operatingsystem	système d'exploitation	Mappe à l'enregistrement d'image du conteneur détecté
u_scantime	last_scan_date	Mappe à l'enregistrement d'image du conteneur détecté

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Actif conteneur, carte de transformation, script, minutage et objectif

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Cette transformation permet d'initialiser les valeurs dans le import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Fonction utilisée pour mettre à jour les valeurs de l'hôte et vérifier si l'hôte existe. En fonction des résultats, modifie les valeurs d'un import_set. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.cs Importation de vulnérabilité du conteneur

Les données de vulnérabilité du conteneur importées sont d'abord chargées dans la table d'importation de vulnérabilité du Tenable.cs conteneur [sn_vul_tenable_cs_container_vuln_import].

La Tenable.cs carte de transformation de vulnérabilité du conteneur est utilisée pour transformer les informations de vulnérabilité du conteneur importé. Les changements apportés à cette transformation modifient la façon dont les données de l'importation Tenable.cs de vulnérabilité de conteneur sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Tenable.cs Recherchez Transformation de vulnérabilité de conteneur.

Les tableaux suivants répertorient les champs de carte de transformation par intégration.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur

Champ source	Champ cible	Description
[script]	Image_id	La synthèse est extraite du champ Resource.Id de l'API et mappée au champ de image_id'image du conteneur détecté et de l'enregistrement de l'image Docker.
[script]	Image_digest	La synthèse est extraite du champ Resource.Id de l'API et mappée au champ de image_digest'image du conteneur découvert et de l'enregistrement de l'image Docker.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
[script]	nom	Les informations du référentiel sont extraites du champ de nom et mappées à l'image Docker et à l'enregistrement du référentiel du conteneur.
[script]	réf.	Les informations du référentiel sont extraites du champ de nom et mappées pour détecter l'enregistrement d'image du conteneur.
u_resource. Étiquettes	Image_labels	Mappe à l'enregistrement d'image du conteneur détecté
u_resource. Fournisseur de cloud	cloud_providers	Mappe à l'enregistrement d'image du conteneur détecté
u_resource. AccountId	cloud_account_ids	Mappe à l'enregistrement d'image du conteneur détecté
u_resource. Région	cloud_regions	Mappe à l'enregistrement d'image du conteneur détecté
u_vulnerability. ID	id	Mappe l'ID à partir de la source et ajoute le préfixe TEN-. Par exemple, si l'ID reçu est 12345, l'ID dans la table d'entrée tierce est TEN-12345.
u_vulnerability. Description Id	ID résumé	Mappe à l'enregistrement d'entrée du tiers. ou un enregistrement CVE.
u_vulnerability. Sévérité	v4_base_severity	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Score VPR	source_risk_score	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Gravité VPR	source_severity	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Vecteur d'attaque	v4_attack_vector	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Maturité de l'exploit	v4_exploit_maturity	Mappe à l'enregistrement d'entrée du tiers.
[script]	source	La source pour le TPE importé est Tenable.cs.
u_vulnerability. Id	nom	Mappé à l'enregistrement des références de vulnérabilité
u_vulnerability. Liens	URL	Mappé à l'enregistrement des références de vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
	vulnerability	Référence de TPE ou CVE dans l'enregistrement des références de vulnérabilité
u_software. Nom	nom	Mappé à l'enregistrement du package d'images du conteneur
u_software. Version	version	Mappé à l'enregistrement du package d'images du conteneur
u_software. Type	package_type	Mappé à l'enregistrement du package d'images du conteneur
u_softwarepaths	chemin d'accès	Mappé à l'enregistrement du package d'images du conteneur
u_resolved	état	Mappé à l'enregistrement de résultat d'image du conteneur
u_firstscantime	first_found	Mappé à l'enregistrement de résultat d'image du conteneur
u_resource. Analyser l'heure	last_found	Mappé à l'enregistrement de résultat d'image du conteneur
u_vulnerability. Description	proof	Mappé à l'enregistrement de résultat d'image du conteneur
u_resolved	État	Mappé à l'enregistrement de l'élément vulnérable du conteneur
u_firstscantime	first_found	Mappé à l'enregistrement de l'élément vulnérable du conteneur
u_resource. Analyser l'heure	last_found	Mappé à l'enregistrement de l'élément vulnérable du conteneur
[script]	source	La source de l'enregistrement d'élément vulnérable de conteneur est Tenable.cs.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Tenable.cs Vulnérabilité du conteneur : synchronisation et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Déclenche les vulnérabilités du conteneur TenableCS Processeur qui importe les données à partir de l'utilisation du Tenable.cs jeu d'importation et charge chaque enregistrement dans la table CI CMDB, la table Élément vulnérable, la table Entrée de vulnérabilité tierce, la table Référence de vulnérabilité, le package d'images de conteneur, le résultat d'image de conteneur et l'élément vulnérable

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Vulnérabilité du conteneur : synchronisation et objectif du script de carte de transformation (suite)

Lorsque le script est exécuté	Objectif
	de conteneur. Il n'est pas recommandé de modifier ou de supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation)	Vérifie si les conclusions d'entrée et d'image tierces existent. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation)	Met à jour le nombre de CI, de VIT et de conclusions tels qu'importés à partir de Tenable.cs. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.cs Importation de la vulnérabilité de calcul

Les données de vulnérabilité de l'hôte importées sont d'abord chargées dans la table d'importation de Tenable.cs vulnérabilité de calcul [sn_vul_tenable_cs_compute_vuln_import].

La Tenable.cs carte de transformation Vulnérabilité de calcul est utilisée pour transformer les informations de vulnérabilité de l'hôte importé. Les changements apportés à cette transformation modifient la façon dont les données de l'importation Tenable.cs de vulnérabilité de calcul sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Ensembles de données à importations système**. Tenable.cs Recherchez Transformation de vulnérabilité de calcul.

La table suivante répertorie les champs de carte de transformation par intégration.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur

Champ source	Champ cible	Description
u_resource. Id	object_id	Mappé à l'enregistrement CI CMDB.
u_resource. Nom	nom	Mappé à l'enregistrement CI CMDB.
	asset_category	Le cloud est mappé en tant que catégorie d'actif dans l'enregistrement de l'élément détecté.
U_resource. Fournisseur de cloud	cloud_service_provider	Mappé à l'enregistrement de l'élément détecté
u_resource. Région	cloud_region	Mappé à l'enregistrement de l'élément détecté
u_resource. ID de compte	cloud_account	Mappé à l'enregistrement de l'élément détecté
u_resource. CloudProvider	cloud_resource_type	Mappé à l'enregistrement de l'élément détecté

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
u_resource. Id	resource_id	Mappé à l'enregistrement de l'élément détecté
u_resource. Nom	resource_name	Mappé à l'enregistrement de l'élément détecté
u_vulnerability. Id	id	Mappe l'ID à partir de la source et ajoute le préfixe TEN-. Par exemple, si l'ID reçu est 12345, l'ID dans la table d'entrée tierce est TEN-12345. Mappe également l'ID aux CVE.
u_vulnerability. Description	résumé	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Sévérité	v4_base_severity	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Score VPR	source_risk_score	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Gravité VPR	source_severity	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Vecteur d'attaque	v4_attack_vector	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Maturité de l'exploit	v4_exploit_maturity	Mappe à l'enregistrement d'entrée du tiers.
[script]	source	La source du TPE importé est Tenable.cs.
u_vulnerability. Id	nom	Mappé à l'enregistrement des références de vulnérabilité
u_vulnerability. Liens	URL	Mappé à l'enregistrement des références de vulnérabilité
	vulnerability	Référence de TPE ou CVE dans l'enregistrement des références de vulnérabilité
u_resolved	état	Mappé à l'enregistrement de détection d'éléments vulnérables
u_firstscantime	first_found	Mappé à l'enregistrement de détection d'éléments vulnérables
u_resource. Analyser l'heure	last_found	Mappé à l'enregistrement de détection d'éléments vulnérables
u_softwarepaths	proof	Mappé à l'enregistrement de détection d'éléments vulnérables

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
u_softwareresolutionversions	solution_summary	Mappé à l'enregistrement de détection d'éléments vulnérables
u_resolved	État	Mappé à l'enregistrement d'élément vulnérable
u_firstscantime	first_found	Mappé à l'enregistrement d'élément vulnérable
u_resource. Analyser l'heure	last_found	Mappé à l'enregistrement d'élément vulnérable
[script]	source	La source de l'enregistrement d'élément vulnérable est Tenable.cs.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Tenable.cs Vulnérabilité de calcul, synchronisation et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Déclenche le processeur de vulnérabilités de calcul Tenable CS qui importe les données à l'aide du Tenable.cs jeu d'importation et charge chaque enregistrement dans la table CI CMDB, la table Éléments vulnérables et la table Vulnérabilité tierce. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Vérifie si l'entrée et les détections tierces existent. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Met à jour le nombre de CI, de VIT et de détections tels qu'importés à partir de Tenable.cs. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur

Champ source	Champ cible	Description
u_digest	Image_id	Une synthèse unique fournie par Tenable pour les actifs du conteneur. Il est mappé à l'image du conteneur découvert et à l'enregistrement de l'image Docker et est utilisé pour la recherche de CI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
u_name	nom	Mappé au champ de nom de l'enregistrement d'image Docker.

Définir des paramètres de filtre supplémentaires pour Tenable.io les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec le Tenable Vulnerability Integration pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec le Tenable.io produit.

Avant de commencer

Cas d'utilisation : en tant que responsable ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que des détails spécifiques de la vulnérabilité. Par exemple, supposons que vous souhaitiez afficher les vulnérabilités importées qui sont filtrées par `cidr_range`, `num_assets`, `indexed_at`et `plugin_family`. Ou supposons que vous souhaitiez exécuter une Tenable.io intégration de telle sorte qu'une exécution importe uniquement les vulnérabilités critiques toutes les quatre heures et qu'une autre s'exécute toutes les 24 heures pour extraire toutes les autres vulnérabilités non critiques.

Pour vous aider à collecter ces données, vous pouvez ajouter des paramètres pris en charge par Tenable pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, cette fonctionnalité vous permet de personnaliser vos informations de requête HTTP avec les paramètres Tenable dans votre ServiceNow AI Platform. Les intégrations suivantes Tenable.io prennent en charge le filtrage en fournissant du contenu JSON dans le corps de la demande :

- Intégration des actifs
- Intégration de vulnérabilité corrigée
- Intégration des vulnérabilités ouvertes

Vous devez savoir comment utiliser JSON les chaînes pour cette fonctionnalité.

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Recherchez les paramètres pris en charge par le Tenable.io produit sur le site développeur que vous souhaitez utiliser pour votre filtrage.

   Les paramètres et les valeurs que vous saisissez à partir du Tenable.io produit ne sont pris en charge qu'au niveau de l'instance d'intégration.

2. Accédez à la **Tous** > **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
3. Sur la page de liste Intégrations Tenable, cliquez sur l'enregistrement de l'intégration Tenable.io que vous souhaitez ouvrir.
4. Une fois l'onglet Méthodes REST Tenable sélectionné, cliquez sur l'icône d'informations (I) de la méthode REST, puis sur **Ouvrir l'enregistrement**.
5. Sélectionnez l'onglet **de demande HTTP** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Pour modifier l'enregistrement, en haut de la page, cliquez sur le lien dans Pour modifier l'enregistrement, cliquez **ici**.
7. Dans le champ Contenu de l'enregistrement Méthode REST, saisissez le contenu JSON que vous souhaitez inclure dans le corps de la demande.

   Par exemple, vous pouvez définir le paramètre de gravité pour les vulnérabilités importées comme, `{"filters": {"severity": ["critical"]}}` pour l'intégration Tenable.io des actifs afin qu'elle importe uniquement les vulnérabilités critiques (score CVSS de 10,0).

   Si vous souhaitez entrer plusieurs paramètres, consultez la documentation pour plus d'informations sur la Tenable.io façon de séparer chaque valeur.
8. Cliquez sur **Mettre à jour**.

Génération de rapports sur l'intégration de vulnérabilité Tenable

Affichez les rapports sur les vulnérabilités et les éléments vulnérables sur les tableaux de Réponse aux vulnérabilités bord.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à surveiller la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en affichant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Consultez Réponse aux vulnérabilités Espaces de travail et Exploration de l'Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Versions précédentes de Réponse aux vulnérabilités

Le tableau de bord de vue d'ensemble de Réponse aux vulnérabilités (Gestion de la vulnérabilité) fournit une vue d'ensemble des vulnérabilités et des éléments vulnérables, ce qui aide l'administrateur des vulnérabilités à identifier rapidement les zones de préoccupation. Le tableau de bord de rattrapage de Vulnerability Response (Vulnerability Remediation) permet à un spécialiste du rattrapage de se concentrer sur les tâches de rattrapage et les éléments vulnérables qu'il possède.

Consultez Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités pour plus d'informations.

Rôle requis : propriétaire du rattrapage.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher le tableau de bord, accédez à **Réponse aux vulnérabilités** > **Aperçu du rattrapage**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Graphique de l'état d'exécution de l'intégration pour l'intégration de vulnérabilité Tenable

Le module État de l'exécution de l'intégration Tenable vous fournit une vue graphique de l'état des exécutions de l'intégration Tenable.

Dans le graphique, pointez sur n'importe quelle partie du graphique pour afficher un résumé des données spécifiques à cette partie. Si vous cliquez sur une partie du graphique à barres, une liste s'ouvre pour fournir des informations plus détaillées.

Rôle requis : administrateur de vulnérabilité.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

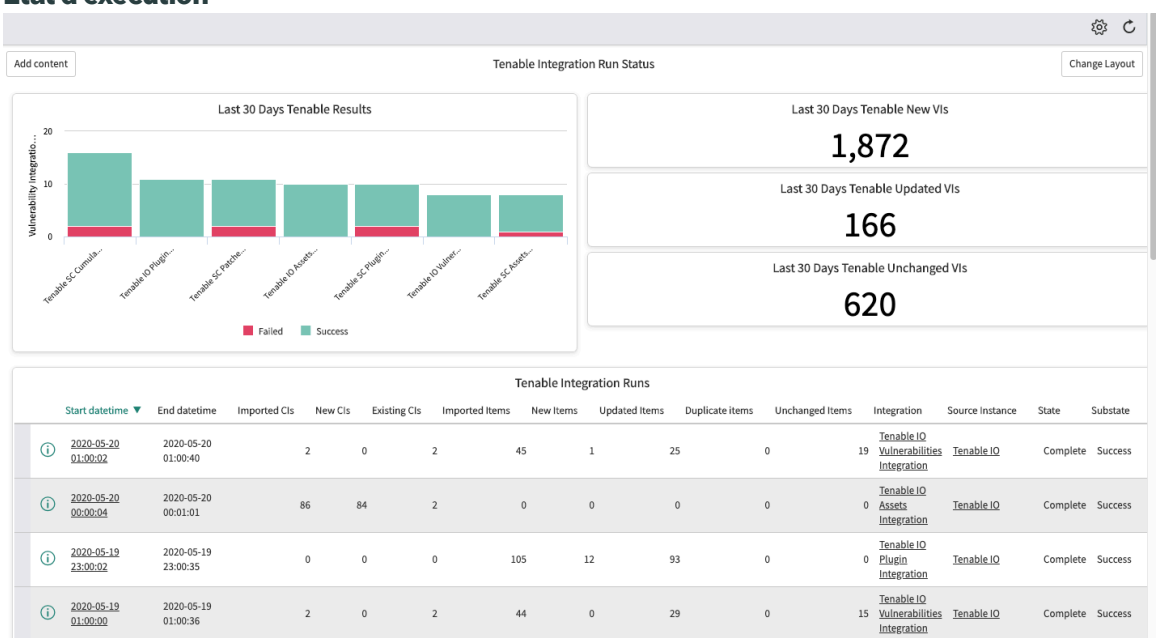
Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher les données, accédez à **Tous** > **Intégration de vulnérabilité Tenable** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

État d'exécution



Rapports des graphiques d'état d'exécution de l'intégration Tenable

Nom	Description
Résultats Tenable au cours des 30 derniers jours	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Chaque exécution s'affichait sous la forme d'une barre dans le graphique.

Traduction automatique

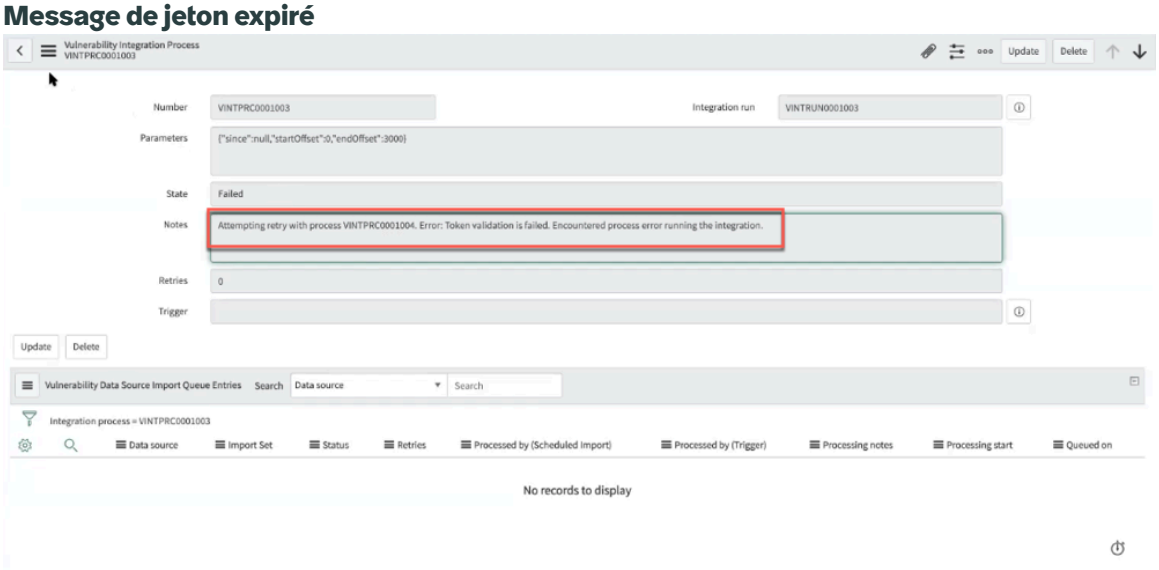
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
Nouveaux VI Tenable au cours des 30 derniers jours	Nombre de nouveaux éléments vulnérables importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour Tenable au cours des 30 derniers jours	Nombre d'éléments vulnérables mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI non modifiés Tenable au cours des 30 derniers jours	Nombre d'éléments vulnérables en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Exécutions d'intégration Tenable	Les enregistrements d'exécution de l'intégration dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection dans la `sn_vul_detection` table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, une fois l'exécution de l'intégration terminée.

Expiration de la validation du jeton

Si l'exécution d'une intégration de Tenable.sc échoue pour une raison quelconque, le jeton d'authentification de Tenable.sc expire automatiquement et un message s'affiche dans l'enregistrement du processus d'intégration de vulnérabilité.

Message de jeton expiré



Un nouveau jeton est automatiquement généré pour le processus d'intégration suivant. Tous les processus d'intégration, ayant échoué ou réussi, sont affichés dans l'onglet Processus d'intégration de vulnérabilité de l'enregistrement du processus d'intégration de vulnérabilité.

Lancer une nouvelle analyse pour l'intégration Tenable.sc

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans la plateforme Tenable. Vous pouvez lancer une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

nouvelle analyse sur demande des éléments vulnérables pour le Tenable.sc produit à partir de votre ServiceNow AI Platform® instance.

Avant de commencer

Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Remarque : Tenable.sc ne prend pas en charge le lancement de RECAN sur les machines basées sur agent.

Vérifiez que votre scanner est activé avant de commencer. Accédez à la **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.

Pourquoi et quand exécuter cette tâche

Pour lancer une nouvelle analyse à partir des espaces de travail, reportez-vous à la section Analyser Tenable.io de nouveau et Tenable.sc les éléments vulnérables à partir des espaces de Réponse aux vulnérabilités travail.

Suivez les étapes énumérées ci-dessous pour lancer une nouvelle analyse dans l'environnement classique.

Pour réduire les frais généraux et le volume liés aux analyses complètes planifiées, les propriétaires de rattrapages, les spécialistes informatiques, les analystes de vulnérabilité ou les gestionnaires de vulnérabilité peuvent lancer de nouvelles analyses ciblées à la demande pour détecter des vulnérabilités spécifiques sur les actifs (éléments de configuration) de leurs environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de rattrapage (RT), d'entrée tierce (TPE) ou d'éléments découverts à partir de votre ServiceNow AI Platform instance.

Les nouvelles analyses permettent à vos propriétaires de rattrapage et à vos analystes de vulnérabilité de vérifier que vos activités de rattrapage, correctifs et autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Par exemple, l'ensemble de votre environnement est analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été terminée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines pour la prochaine analyse planifiée afin de vérifier qu'elle a été corrigée. Pour vérifier que votre correctif a corrigé avec succès une vulnérabilité critique découverte lors d'une analyse précédente, vous pouvez lancer une nouvelle analyse ciblée à partir de votre ServiceNow AI Platform pour rechercher Tenable.sc les éléments vulnérables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous demandez une nouvelle analyse à partir de votre ServiceNow AI Platform® instance, la sélection des informations d'identification Vulnerability Response integration with Tenable est facultative. L'intégration ServiceNow® Tenable.sc des informations d'identification de numérisation importe et met à jour les informations d'identification Tenable.sc du scanner du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable.

Notez que ces données importées n'incluent pas les mots de passe Tenable ni d'autres informations sensibles sur le compte Tenable. L'intégration ServiceNow® Tenable.sc des informations d'identification d'analyse est activée (active) automatiquement à partir de l'assistant de configuration de votre instance lorsque vous configurez les Tenable.sc intégrations de vulnérabilités (Tenable.sc intégrations de vulnérabilités ouvertes et corrigées).

Notez les informations suivantes concernant les informations d'identification que vous importez afin que vos utilisateurs puissent les consulter selon les besoins de votre ServiceNow AI Platform instance :

- Les informations d'identification créées avec le rôle d'utilisateur administrateur sont disponibles pour les Tenable.sc utilisateurs de toutes vos organisations.
- Les informations d'identification créées avec le rôle d'utilisateurs de l'organisation Tenable.sc ne sont disponibles que pour les utilisateurs de cette organisation. Ces informations d'identification ne sont pas importées dans le ServiceNow AI Platform pour les utilisateurs extérieurs à l'organisation du créateur, sauf si elles sont partagées avec le compte de l'utilisateur utilisé pour se connecter à l'instance.

Consultez le site web de la Tenable.sc documentation pour plus d'informations.

Pour plus d'informations sur la configuration de l'application, reportez-vous à la Tenable.sc section Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration . Pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation, accédez à **Tous** > **Intégration de vulnérabilité Tenable** > **Intégrations** > **Intégration des informations d'identification de numérisation Tenable.sc**.

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Vous ne pouvez lancer de nouvelles analyses que pour les VI ayant Tenable.sc comme source. Vérifier Tenable.sc s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le générateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue de liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône **Personnaliser la liste** (icône Engrenage) et utilisez la zone de liste double pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** pour la tâche de rattrapage ou les enregistrements d'entrée tierce, respectivement, que vous souhaitez utiliser pour la nouvelle analyse.

   Selon votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

   - Sur un enregistrement de VI unique, l'élément vulnérable doit provenir du Tenable.sc produit et se trouver dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent provenir du produit Tenable.sc et dans un état autre que **Fermé**.
   - Sur un enregistrement RT, la tâche de rattrapage peut être dans n'importe quel état autre que **Fermé**, et tous les VI associés doivent provenir du Tenable.sc produit.
   - Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du Tenable.sc produit dans un état autre que **Fermé**.

4. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**.
   Vous êtes invité à choisir les informations d'identification du scanner pour accéder au scanner. Il s'agit des informations d'identification importées par l'intégration des informations d'identification Tenable.sc de numérisation.
5. Dans la boîte de dialogue, sélectionnez les filtres et les types d'informations d'identification souhaités.
6. Cliquez sur **Demander une analyse**.

   Un message s'affiche pour indiquer que votre analyse est en cours de traitement. L'état de toutes les nouvelles analyses peut être trouvé à tout moment dans les listes associées à l'analyse sur les enregistrements VI, RT, TPE que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

   Le champ État de l'enregistrement d'analyse parent est marqué comme terminé une fois que toutes les analyses enfants ont été terminées avec succès. Les analyses enfants

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

importent des données. L'enregistrement d'analyse parent est un conteneur pour les analyses enfants.

Votre ServiceNow AI Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform® votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée. Tous les éléments vulnérables qui sont passés ou passeront à l'état **Fermé/Corrigé** sont importés lors de la prochaine importation planifiée de l'intégration des vulnérabilités corrigées Tenable.sc.

Lancer une nouvelle analyse pour l'intégration Tenable.io

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans la plateforme Tenable. Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Tenable.io produit à partir de votre ServiceNow AI Platform® instance.

Avant de commencer

Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Vérifiez que votre scanner est activé avant de commencer. Accédez à la **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.

Pourquoi et quand exécuter cette tâche

- Consultez et Analyser de nouveau les enregistrements et les tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et pour Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT lancer une nouvelle analyse dans les espaces de travail Réponse aux vulnérabilités.
- Suivez les étapes énumérées ci-dessous pour lancer une nouvelle analyse dans l'environnement classique.

Remarque : Tenable.io ne prend pas en charge le lancement de RECAN sur les machines basées sur agent.

Pour réduire les frais généraux et le volume liés aux analyses complètes planifiées, en tant que propriétaire de rattrapage, informaticien, analyste de vulnérabilité ou gestionnaire de vulnérabilité, vous pouvez lancer de nouvelles analyses ciblées à la demande. Vous pouvez rechercher des vulnérabilités spécifiques sur les actifs (éléments de configuration) de vos environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de rattrapage (VUL), d'entrée tierce (TPE) ou d'éléments découverts (SDI) à partir de votre ServiceNow AI Platform instance. Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, correctifs et autres actions ont correctement corrigé des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous demandez une nouvelle analyse à partir de votre ServiceNow AI Platform® instance, la sélection des informations d'identification Vulnerability Response integration with Tenable est facultative. L'intégration ServiceNow® Tenable.io des informations d'identification de numérisation importe et met à jour les informations d'identification Tenable.io du scanner du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable.

Notez que ces données importées n'incluent pas les mots de passe Tenable ni d'autres informations sensibles sur le compte Tenable.

Les informations suivantes décrivent les informations d'identification que vous importez afin que vos utilisateurs puissent les afficher selon les besoins à partir de votre ServiceNow AI Platform instance :

- Les informations d'identification créées avec le rôle d'utilisateur administrateur sont disponibles pour les Tenable.io utilisateurs de toutes vos organisations.
- Les informations d'identification créées avec le rôle d'utilisateurs de l'organisation Tenable.io ne sont disponibles que pour les utilisateurs de cette organisation. Ces informations d'identification ne sont pas importées dans le ServiceNow AI Platform pour les utilisateurs extérieurs à l'organisation du créateur, sauf si elles sont partagées avec le compte de l'utilisateur utilisé pour se connecter à l'instance.

  Consultez le site web de la Tenable.io documentation pour plus d'informations.

- L'intégration Tenable.io du modèle et l'intégration des informations d'identification Tenable.io de numérisation doivent être activées avant de lancer de nouvelles analyses. Pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation, accédez à **Intégration de vulnérabilité Tenable** > **Intégrations** > **Intégration des informations d'identification Tenable.io Scan**.

  Par défaut, les intégrations de modèle et d'informations d'identification d'analyse sont désactivées. Lorsque vous saisissez vos informations d'identification pour Tenable.io, toutes les Tenable.io intégrations sont automatiquement activées. Pour activer ou désactiver manuellement ces intégrations :

  1. Accédez à la **Tous** > **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
  2. Dans la liste qui s'affiche, recherchez les enregistrements d'intégration Tenable.io souhaités.
  3. Ouvrez chaque enregistrement et cochez la case **Actif** pour activer l'intégration.
  4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
  5. Revenez à l'assistant de configuration pour poursuivre votre configuration pour le Tenable Vulnerability Integration avec Réponse aux vulnérabilités.

Pour plus d'informations sur la configuration des produits andTenable.sc, reportez-vous Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration à la Tenable.io section .

Supposons que l'ensemble de votre environnement soit analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été terminée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines pour la prochaine analyse planifiée afin de vérifier qu'elle a été corrigée. Pour vérifier que votre correctif a corrigé avec succès une vulnérabilité critique découverte lors d'une analyse précédente,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vous pouvez lancer une nouvelle analyse ciblée à partir de votre ServiceNow AI Platform pour rechercher Tenable.io les éléments vulnérables.

Vous pouvez afficher les résultats mis à jour sur les enregistrements à partir desquels vous avez lancé les analyses après la prochaine importation planifiée de l'intégration des vulnérabilités corrigées.

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Si vous utilisez le Tenable.io scanner, vous ne pouvez lancer de nouvelles analyses que pour les éléments vulnérables ayant Tenable.io comme source. Vérifier Tenable.io s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le générateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue de liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône **Personnaliser la liste** (icône Engrenage) et utilisez la zone de liste double pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** pour les enregistrements que vous souhaitez utiliser pour la nouvelle analyse.

   Selon votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

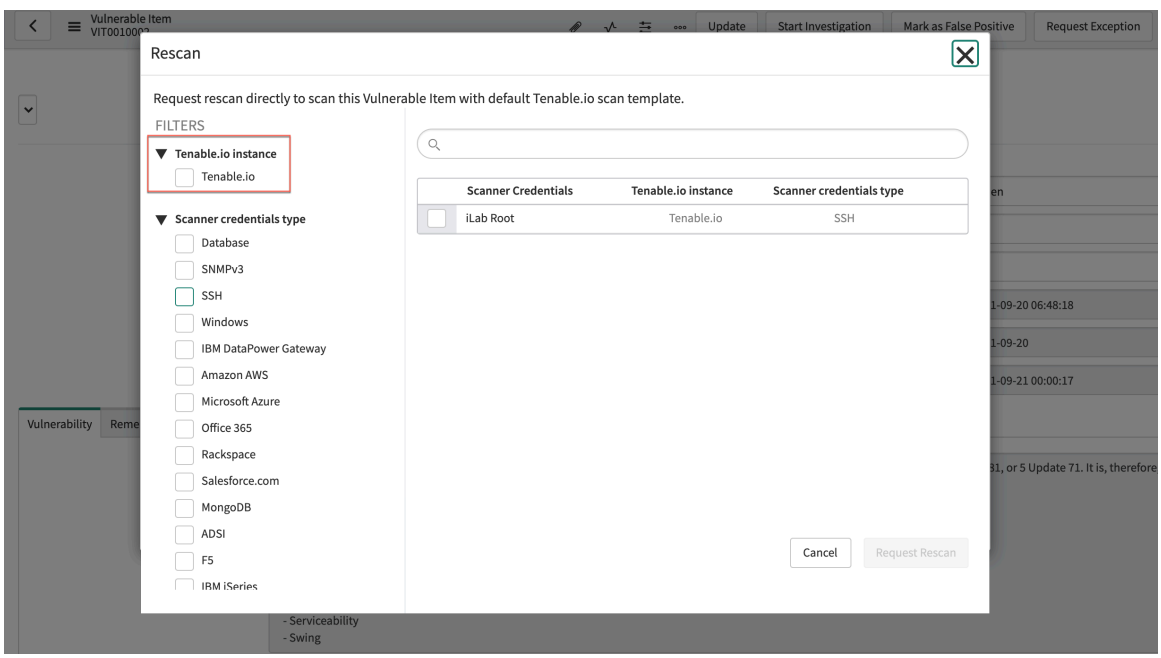
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sur un enregistrement de VI unique, le VI doit être dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent provenir du Tenable.io produit et dans un état autre que **Fermé**.
- Pour les enregistrements de tâche de rattrapage, seules les tâches de rattrapage dans un état autre que **Fermé** sont prises en charge. Tous les VI associés doivent être dans un état autre que **Fermé** et être utilisés Tenable.io comme source.
- Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du Tenable.io produit dans un état autre que **Fermé**.
- Sur les enregistrements d'éléments détectés, l'enregistrement doit avoir au moins un enregistrement de VI associé du Tenable.io produit dans un état autre que **Fermé**.
- Dans la liste Éléments vulnérables, vous pouvez sélectionner des éléments vulnérables individuels que vous souhaitez analyser à nouveau. Utilisez le menu Actions sur les lignes sélectionnées en bas à gauche de l'écran pour lancer la nouvelle analyse. Vous êtes invité à saisir vos informations d'identification.

4. Dans l'angle supérieur droit d'un enregistrement, cliquez sur **Analyser à nouveau**.
   Vous êtes invité à choisir l'instance ou les instances pour la nouvelle analyse et les informations d'identification du scanner que vous souhaitez utiliser pour accéder au scanner. Les informations d'identification affichées sont celles importées par l'intégration des informations d'identification Tenable.io de numérisation.
5. Dans la boîte de dialogue, sélectionnez l'instance et/ou les instances et les types d'informations d'identification que vous souhaitez utiliser.

   Dans l'image suivante, une instance d'intégration, Tenable.io s'affiche. Si vous avez plusieurs Tenable.io instances, elles sont toutes affichées dans la section Tenable.io du formulaire.



Champ	Description
Instance Tenable.io	Choisissez une Tenable.io instance d'intégration à partir de laquelle vous souhaitez lancer la nouvelle analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Toutes vos instances d'intégration pour Tenable.io s'affichent. Si un élément vulnérable existe dans plusieurs instances d'intégration, vous pouvez utiliser ce filtre pour limiter ou développer les instances que vous souhaitez analyser. **Remarque :** Si vous choisissez d'analyser à nouveau les éléments vulnérables à partir d'un enregistrement de tâche de rattrapage pour une seule instance d'intégration, seuls les éléments vulnérables actifs associés à cette tâche de rattrapage, pour cette instance, à l'aide des informations d'identification que vous sélectionnez sont analysés.
Filtre de type d'informations d'identification du scanner	Utilisez ce filtre pour afficher les informations d'identification par type.
Volet avec les informations d'identification du scanner, Tenable.io instance, type d'informations d'identification du scanner	Il s'agit des informations d'identification de scanner disponibles importées à partir des Tenable.io produits. Choisissez une ou plusieurs informations d'identification à utiliser pour l'analyse.

6. Cliquez sur **Demander une nouvelle analyse**.

Un message s'affiche pour indiquer que votre analyse est en cours de traitement et qu'un enregistrement d'analyse parent est créé. L'état de toutes les analyses enfants peut être trouvé à tout moment dans les listes connexes d'analyse sur les enregistrements du VI, de la tâche de rattrapage, du TPE et du SDI que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

Le champ État de l'enregistrement d'analyse parent est marqué comme terminé une fois que toutes les analyses enfants ont été terminées avec succès. Les analyses enfants importent des données. Chaque analyse prend en charge une combinaison unique d'instance d'intégration, de TPE, d'adresse IP et d'ID de réseau. Vous pouvez voir plusieurs analyses enfants sur un enregistrement d'analyse parent. Par exemple, le nombre maximum d'adresses IP qu'une analyse enfant peut prendre en charge est de 1 000. S'il existe 1 002 adresses IP pour un élément vulnérable, deux analyses enfants sont créées et répertoriées dans la liste connexe Analyses pour prendre en charge la demande. L'enregistrement d'analyse parent est un conteneur pour les analyses enfants et son état reflète l'état des analyses enfants.

Votre ServiceNow AI Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform® votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée. Tous les VI qui sont passés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ou passeront à **l'état Fermé/Corrigé** sont importés avec la prochaine importation planifiée de l'intégration Tenable.io des vulnérabilités corrigées.

Pour les analyses qui présentent une erreur, vous pouvez vérifier les analyses enfants sur l'enregistrement d'analyse parent. Affichez l'erreur dans la charge utile de la réponse de l'analyse enfant.

Vous pouvez afficher les résultats mis à jour sur les enregistrements à partir desquels vous avez lancé les analyses après la prochaine importation planifiée de l'intégration des vulnérabilités corrigées.

Mettre à jour les éléments de configuration avec l'identificateur de partition réseau pour le Tenable Vulnerability Integration

Créez des éléments de configuration (CI) uniques pour les actifs de votre environnement qui partagent des adresses IP. Identifiez les actifs distincts dans votre environnement et mettez automatiquement à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous fournir plus de détails sur vos vulnérabilités.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Par défaut dans l'application Réponse aux vulnérabilités , une façon d'identifier vos actifs est l'adresse IP. Dans certains cas, les actifs peuvent partager des adresses IP, mais elles sont stockées sous la forme d'un seul CI dans votre CMDB.

Par exemple, comme indiqué dans les tables suivantes, plusieurs actifs (CI) de votre environnement peuvent partager des adresses IP, mais ont des ID de réseau et de référentiel uniques. Toutefois, par défaut, ces actifs sont généralement identifiés et stockés sous la forme d'un seul CI (CI 1) lors de la recherche d'adresse IP.

Recherche d'adresses IP et création de CI par défaut

Source	Adresse IP	Network_id	Élément de configuration
Tenable.io: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	Adresse IP	Repository_id	Élément de configuration
Tenable.sc: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Vous pouvez créer des CI individuels pour des actifs qui ont la même adresse IP afin de les identifier comme des actifs distincts. À partir d'une importation de données récente, vous pouvez mettre à jour vos CI existants avec plus de granularité qui inclut l'identificateur de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

partition de réseau [network_partition_identifier] en exécutant la tâche planifiée, *Update existing discovered items with network partition identifier*.

Cette tâche planifiée est désactivée par défaut. Activez cette fonctionnalité pour les intégrations Actifs et Vulnérabilités immobilisées et ouvertes pour les produits dans Tenable.sc l'assistant de configuration afin d'afficher Tenable.io cet identificateur sur vos enregistrements.

Lorsqu'elle est activée, cette tâche planifiée ajoute l'identificateur de partition de réseau [network_partition_identifier] aux enregistrements de CI existants à partir des données importées. Les CI existants créés par l'IRE sont également mis à jour. La tâche planifiée crée également des CI qui incluent l'identificateur de partition de réseau à partir de l'importation suivante. Vous pouvez également lancer la tâche à la demande pour mettre à jour vos données existantes.

Lorsque vous effectuez une mise à niveau à partir des Réponse aux vulnérabilités versions 14.0 et 2.2 de l'intégration de vulnérabilité Tenable, les modèles de classe CI CMDB (1.0.21) sont pris en charge. Les modèles de classes ont l'identificateur de partition de réseau [network_partition_identifier] dans les règles d'identification IRE (Identification et rapprochement).

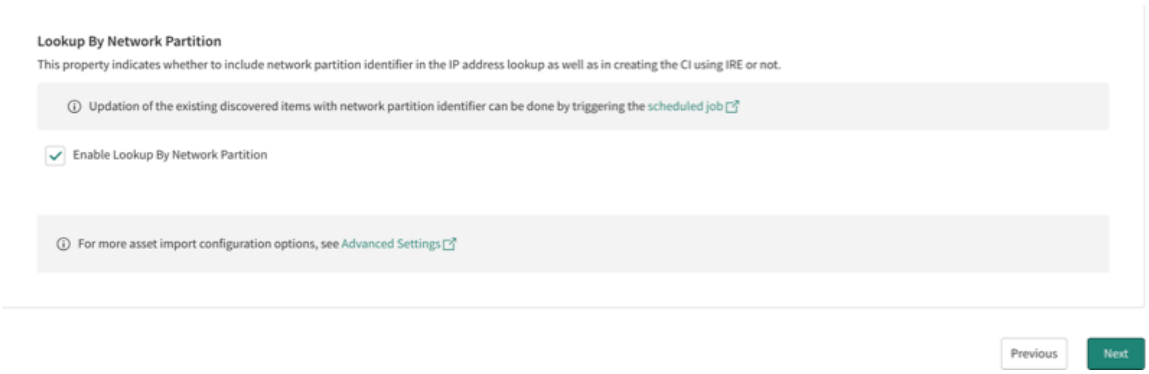
Option	Description
Exécuter les travaux planifiés sur demande.	Mettez à jour vos éléments détectés existants. Les CI de vos données Tenable existantes sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau. Les éléments détectés, les éléments vulnérables et les enregistrements de détection sont tous mis à jour avec les nouveaux CI.
Attendez les importations de données fraîches à partir des intégrations avec les travaux planifiés suivants.	Créez des CI pour chaque nouvel actif à l'aide de l'identificateur de partition de réseau en commençant par la tâche planifiée suivante. Les enregistrements de CI, d'éléments vulnérables et de détection sont tous mis à jour pour inclure la nouvelle granularité. De nouveaux CI sont créés lorsqu'aucune correspondance exacte n'est trouvée.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
2. Sélectionnez Tenable.io des intégrations ou Tenable.sc des intégrations.
3. **Modifiez** l'intégration requise.
4. Sélectionner **Configuration de l'importation d'actifs**.
5. Sélectionner **Activer la recherche par partition de réseau** case à cocher dans le **Activer la recherche par partition de réseau** section.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Suivant**.

Les identificateurs de partition de réseau NETWORK_ID et les _ID REPOSITORY sont inclus et mettent à jour les CI existants ou créent des CI avec la tâche planifiée suivante.

Attribut d'identificateur de partition de réseau inclus dans la recherche d'adresses IP et la création de CI

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
Tenable.io: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	Adresse IP	REPOSITORY_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
Tenable.sc: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Avec la prochaine tâche planifiée, les règles de recherche d'identification d'adresse IP et d'adresse IP incomplète incluent automatiquement l'attribut d'identificateur de partition de réseau pour une importation de données à partir des intégrations Actifs et Vulnérabilités fixes et ouvertes pour les et les Tenable.ioTenable.sc produits.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que vous avez activé la propriété système et enregistré les enregistrements, vous pouvez également mettre à jour vos éléments détectés existants avec des CI qui incluent l'identificateur de partition de réseau en lançant les travaux planifiés à la demande.

Importer des modifications pour l'intégration de vulnérabilité Tenable

Configurez des modifications facultatives et rationalisez certaines des données spécifiquement pour l'intégration d'importation des vulnérabilités Tenable dans l'intégration ServiceNow® des vulnérabilités Tenable.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Cet ensemble de tâches nécessite du codage et des connaissances avancées sur le ServiceNow AI Platform.

Suivez ces étapes pour créer des importations séparées par domaine pour les intégrations de vulnérabilités Tenable. L'exemple suivant concerne l'intégration des vulnérabilités ouvertes Tenable.io, mais ce contenu s'applique aux autres intégrations Tenable.

Procédure

1. Créez un domaine.
2. Pour chaque domaine que vous créez, créez un utilisateur et affectez-le à ce domaine.

   Considérez cet utilisateur comme un espace réservé run_as pour le domaine dans Tenable.io.

3. Intégration des vulnérabilités ouvertes.
   L'utilisateur est l'équivalent du VR. Utilisateur système dans le domaine global et doit avoir les rôles suivants : sn_vul.tenable_configure_integration, import_admin et sn_vul.vulnerability_write. Cet utilisateur doit avoir accès aux sources de données, aux cartes de transformation et aux données de vulnérabilité.

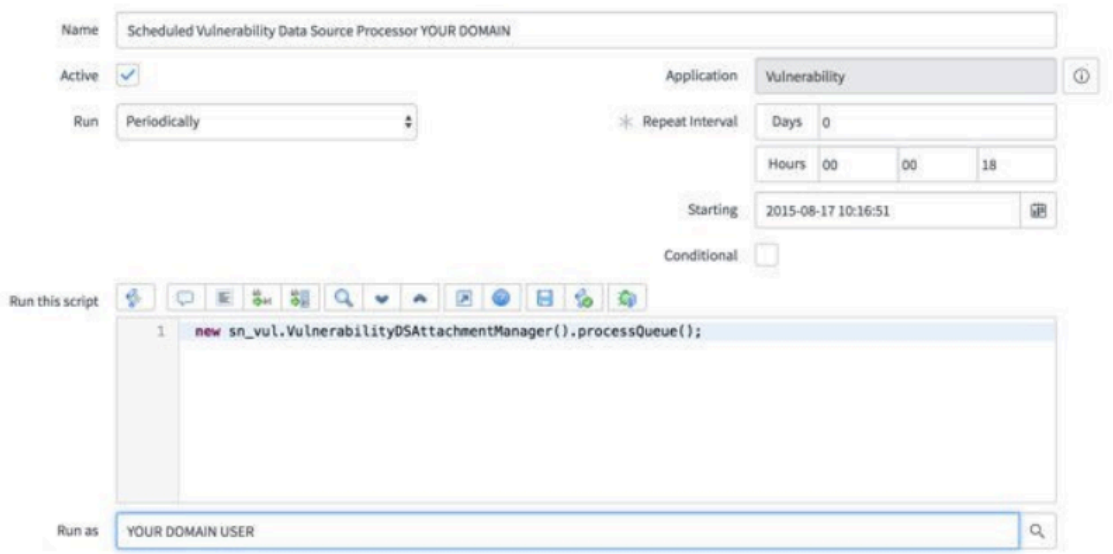
   Remarque : Considérez cet utilisateur comme spécifique à ce rôle. L'utilisateur ne doit pas avoir d'autre but

4. Dans chaque domaine, créez une tâche planifiée en copiant le processeur de source de données de vulnérabilité planifiée trouvé sous **Définition du système** > **Travaux planifiés**.
5. Ajoutez le domaine au nom pour identifier la tâche planifiée.
6. Remplacez l'utilisateur run_as par l'utilisateur que vous avez créé à l'étape précédente.

   Remarque : Modifiez l'action d'interface utilisateur suivante afin que l'intégration s'exécute dans le domaine de l'utilisateur run_as.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Modifiez l'action d'interface utilisateur Exécuter maintenant dans l'intégration des vulnérabilités ouvertes Tenable.io pour ajouter ce bloc de code en haut du fichier.

```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
```

Remarque : Modifiez les includes de script suivants afin que l'intégration s'exécute dans le domaine de l'utilisateur run_as.

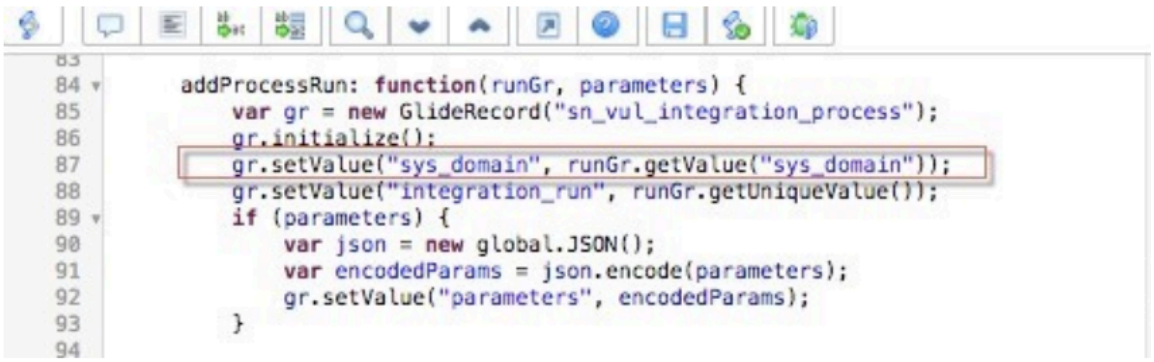
8. Modifiez la méthode d'include de script VulnerabilityIntegrationUtils, addIntegrationRun, pour ajouter le code en surbrillance.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Modifiez la méthode d'include de script VulnerabilityIntegrationUtils, addProcessRun, pour ajouter le code en surbrillance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Modifiez la méthode d'include de script DataSourceVulnReportRefreshProcessor _processFromDataSourceGroups pour modifier ce code d'origine : Code _processFromDataSourcesGroups original en code _processFromDataSourcesGroups modifié.
11. Modifiez la méthode d'include de script VulnerabilityDSAttachmentManager, queueItem pour ajouter les blocs de code en surbrillance suivants, queueItem, _getNext _processQueueEntry fonction.

Vous êtes prêt pour les importations de détections d'hôtes séparés par domaine.

Désactiver les calculateurs avant l'importation

Suivez ces étapes pour désactiver le calculateur par défaut s'il n'est pas utilisé. Si vous n'utilisez pas de calculateurs de vulnérabilité, il est préférable de désactiver les calculateurs par défaut en plus de ceux que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est consulté et peuvent avoir un impact sur les performances de l'instance.

Rôle requis : sn_vul.vulnerability_admin.

12. Accédez à la **Tous** > **Vulnérabilité** > **Administration** > **Calculateurs de vulnérabilités**.
13. Ouvrez le groupe Impact de vulnérabilité.
14. Ouvrez le calculateur de score et d'impact basé sur le service.
15. Désélectionnez le champ Actif pour désactiver le calculateur.
16. Cliquez sur Mettre à jour.

Vous avez désactivé le calculateur par défaut.

Désactiver les règles métier basées sur la notification avant l'importation initiale

Procédez comme suit pour désactiver les règles métier liées aux notifications avant l'importation initiale de l'enregistrement. Lors de l'importation initiale d'enregistrements, certaines règles métier liées aux notifications peuvent générer de nombreuses notifications, ce qui a un impact sur les performances. Ces règles métier doivent être modifiées pour les désactiver au cours de l'importation.

Le rôle requis est sn_vul.vulnerability_admin.

17. Accédez à la **Tous** > **Définition du système** > **Règles métier**.
18. Rechercher les notifications de CI affectés.
19. Ouvrez la règle métier et insérez la condition suivante : `current.sys_class_name != "sn_vul_vulnerable_item"`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

20. Cliquez sur **Mettre à jour**.
21. Répétez cette procédure pour les règles métier suivantes :
    - Notifications des centres de coûts affectés
    - Notifications des groupes affectés
    - Notifications des emplacements affectés

    Remarque : Une fois l'importation de l'enregistrement initial terminée, vous avez la possibilité de réactiver ces règles métier. Cependant, envisagez de les laisser désactivés. Elles peuvent générer un grand nombre de notifications et avoir un impact sur les performances de votre instance.

    Modifier une date de début initiale

    Procédez comme suit pour modifier une date de début initiale. Lors de l'installation à l'aide de l'Assistant de configuration, vous définissez une date de début initiale pour les intégrations Tenable. Vous pouvez réinitialiser cette date de début dans l'Assistant de configuration ou à partir de l'intégration principale, comme indiqué dans les étapes suivantes.

22. Accédez à la **Tous** > **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
23. Cliquez sur n'importe quelle intégration.
24. Cliquez sur Détails de l'intégration.
25. Définissez le champ Heure de début sur une valeur dans le passé, de sorte que toutes les vulnérabilités analysées et détectées depuis cette heure soient détectées.

    Si vous avez configuré Tenable à l'aide de l'assistant de configuration, le champ Heure de début est pré-rempli, initialement jusqu'à trois mois avant la date d'aujourd'hui, puis jusqu'à la date d'aujourd'hui. Remarque : Envisagez de définir la valeur sur un maximum d'un mois dans le passé. Cela empêche une grande quantité de données de dépasser les limites de débit de l'API de Tenable et de déclencher des délais d'exécution.

26. Cliquez sur **Envoyer** ou **Mettre à jour**.
27. **Facultatif :** Cliquez sur **Exécuter maintenant** pour l'exécuter immédiatement.

Fractionner les détections Tenable en fonction de l'instance de vulnérabilité pour diviser les éléments vulnérables

ServiceNow® Vulnerability Response permet de séparer les détections des scanners Tenable, ce qui permet de créer un élément vulnérable unique (VIT) pour chaque instance de vulnérabilité détectée. Cette répartition permet l'affectation de VIT à diverses équipes de remédiation, améliorant ainsi la gestion et le suivi des vulnérabilités.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La charge utile du scanner Tenable contient des données de détection, chaque chemin d'accès de la preuve étant utilisé pour diviser les détections. La balise de sortie dans la charge utile identifie l'emplacement de la vulnérabilité, ce qui facilite l'identification et la gestion précises des vulnérabilités en fonction de leurs chemins spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans la table Intégrations tierces [sn_sec_int_integration], définissez la valeur de la colonne **Inclure la preuve dans la clé du VI** sur vrai pour Tenable.io, Tenable.sc et .Tenable.cs
2. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Configurer la granularité VI**.
3. Pour Tenable.cs le produit, accédez à la table **Configuration de clé de détection** [sn_vul_detection_key_config], sélectionnez Tenable.cs Enregistrer et mettre à jour,
4. Dans le formulaire Inclure le port, cochez la case **Inclure le port** et sélectionnez le lien **cliquer ici** (s'applique uniquement aux Tenable.io et Tenable.sc).
5. Dans la liste Ajouter une preuve aux clés de VI, sélectionnez **Nouveau**.
6. Dans le formulaire Ajouter une preuve à la clé de VI- Nouvel enregistrement, dans le champ **Vulnérabilité** , ajoutez l'ID Tenable pour lequel vous souhaitez inclure la preuve.

   Remarque : Vous pouvez diviser les détections en fonction des informations de chemin d'accès ou en combinant les détails de chemin d'accès et de version. Pour plus de détails, reportez-vous à la section « Fractionnement des détections à partir des scanners Tenable » sur cette page.

7. Dans le champ **Expression régulière pour diviser les VIT Tenable** :
   - Divisez la détection en fonction du chemin d'accès uniquement en saisissant Chemin d'accès\s+ :\s+([A\n]+).
   - Divisez la détection en fonction du chemin d'accès et des versions installées et corrigées en saisissant Chemin\s+ :\s+([A\n]+)\n\s+Installed\s+version\s+ :\s+([A \n]+)\n\s+Fixe\s+version\s+ :\s+([A\n]+).
8. Sélectionnez **Soumettre**.

Example: Fractionnement des détections à partir des scanners Tenable

La détection suivante à partir d'un scanner Tenable montre la preuve dans la balise de sortie qui inclut à la fois des informations sur le chemin et la version.

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
                     "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
                    "tracked": true


                "output": "In                              C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                                    Path
                "plugin":
                      "bid":
                            123456


                     "checks_for_default_account": false,
                    "checks_for malware": false,

                      "coe":
                     "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"


                      "cvSs3_base_score": 7.8,
                     "cvss3 temporal score": 7.0,

                     "cvss3_temporal_vector": {
                           "exploitability": "Proof-of-Concept",
                           "remediation level": "Official Fix",
                            "report_confidence": "Confirmed",
                            "raw": "E: P/RL:0/RC: C"
```


Présentation de l'intégration Atlassian Jira avec Réponse aux vulnérabilités

L'intégration Atlassian Jira vous Réponse aux vulnérabilités permet de tirer parti de différents outils de suivi des problèmes et de gestion agile pour suivre les efforts de résolution des vulnérabilités.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Vue d'ensemble

ServiceNow® Réponse aux vulnérabilités est intégré Atlassian Jira à pour créer des problèmes correspondant aux vulnérabilités et a synchronisé l'entité du problème et Jira l'entité de l'élément de vulnérabilité de Réponse aux vulnérabilités façon bidirectionnelle pour refléter les dernières mises à jour. Les gestionnaires de vulnérabilité exigent que les éléments de vulnérabilité présents dans ServiceNow Réponse aux vulnérabilités soient créés et affectés aux utilisateurs de rattrapage (développeurs dans le cas de Réponse aux vulnérabilités des applications) dans leur système d'enregistrement préféré et outil de gestion des problèmes tels que Atlassian Jira. Toute progression effectuée sur les vulnérabilités dans l'outil de gestion des problèmes doit être mise à jour dans ServiceNow Réponse aux vulnérabilités pour que les gestionnaires des vulnérabilités puissent la voir. En outre, toutes les mises à jour effectuées par les gestionnaires de vulnérabilité pour Réponse aux vulnérabilités les éléments de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilité doivent également être transmises à l'outil de gestion des problèmes pour que les utilisateurs de la correction puissent en rendre la visibilité.

Versions disponibles

Version de mise en production	Notes de publication
Réponse aux vulnérabilités	Notes de version de Vulnerability Response Integration
Vulnerability Response et Configuration Compliance pour le conteneur	Notes de version de Container Vulnerability Response
Spoke Jira	Notes de version du spoke Jira

Jira Intégrations de vulnérabilité

Pour afficher l'intégration de Jira vulnérabilité, accédez à **Tous** > **Agile Management pour VR** > **Configurer les outils Agile** .

Les intégrations suivantes sont incluses dans le système de base. Ces intégrations ne sont pas toutes actives par défaut.

Après l'exécution initiale, chaque jour, des travaux planifiés sont enchaînés pour exécuter les intégrations automatiquement dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Préparation de l'intégration Jira Réponse aux vulnérabilités

Une intégration réussie Jira de Vulnerability nécessite la planification et l'exécution de tâches de pré-intégration. Préparez-vous à l'intégration en effectuant ces tâches. L'intégration Jira Réponse aux vulnérabilités suppose que vous connaissez le produit et l'API Jira .

Composants installés avec Agile Integration et Réponse aux vulnérabilitésJira Integration for Vulnerability Response

Plusieurs types de composants sont installés avec l'activation des modules d'extension Agile Integration for Vulnerability Response et Jira Integration for Vulnerability Response, notamment les tables et les rôles d'utilisateur.

Rôles installés

Titre du rôle [name]	Description
Administrateur de l'outil Agile [sn_vul_agile.agile_tool_admin]	Vous permet de créer une règle de configuration pour Agile Management afin de créer ou de mettre à jour des problèmes. Créez des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles installés (suite)

Titre du rôle [name]	Description
	configurations de règles pour Agile Management.
Administrateur JIRA [sn_vul_jira.admin]	Vous permet de sélectionner l'outil Agile pour créer des problèmes pour la table d'entité sélectionnée.

Tables installées

Table	Description
Configuration de l'outil Agile [sn_vul_agile_tool_rule_config]	Contient des règles de configuration pour créer des problèmes sur la plateforme Agile.
Mappage de champs de l'outil Agile [sn_vul_agile_tool_field_mapping]	Contient le mappage de champs de la règle de configuration.
Mappage de l'état de l'outil Agile [sn_vul_agile_tool_state_mapping]	Contient le mappage d'état de l'état du problème Jira avec l'état de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur, de la tâche de rattrapage de l'application et de la tâche de rattrapage du conteneur.
Manifeste de l'outil Agile [sn_vul_agile_tool_manifest]	Contient la charge utile pour la création de problème.
Ressource de données de l'outil Agile [sn_vul_agile_tool_data_resource]	Contient les informations sur le problème Jira créé.
Administrateur JIRA [sn_vul_jira.admin]	Vous permet de sélectionner l'outil Agile pour créer des problèmes pour la table d'entité sélectionnée.

Traduction automatique

Installer l'intégration de Vulnerability Response avec Jira

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit s'intègre Jira correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Rôle requis : admin.

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que l'application Vulnerability Response est installée et activée.	• L'intégration Jira pour Vulnerability Response nécessite l'application Vulnerability Response. • Pour obtenir la version la plus récente de Jira Integration for Vulnerability Response, vérifiez que la version la plus récente de Vulnerability Response est installée. Consultez KB0856498 les changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response . • Si l'application n'est pas installée et activée, consultez Installer Vulnerability Response .
Vérifiez que le module d'extension du concentrateur d'intégration est installé.	• Le spoke Jira nécessite le concentrateur d'intégration. • Consultez KB1112383 pour l'installation du concentrateur d'intégration. • Pour plus d'informations, consultez Calendriers juridiques - Vue d'ensemble du Centre d'intégration .
Vérifiez que la dernière version est Jira Rayon installée.	Consultez KB0792632 pour l'installation du spoke Jira.
Vérifiez que l'intégration de Vulnerability Response avec Agile Management est installée.	Vulnerability Response Integration with Atlassian Jira nécessite cette intégration.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer l'intégration Jira Réponse aux vulnérabilités .
2. Accédez au ServiceNow Store.
3. Dans , recherchez l'intégration avec Jira l'application.ServiceNow StoreRéponse aux vulnérabilités
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre application est automatiquement installée sur votre instance.

Configurer les règles dans la configuration de l'outil Agile

Jira Les problèmes sont créés sur la plateforme si les enregistrements créés dans l'élément vulnérable d'application Jira , l'élément vulnérable de conteneur, la tâche de rattrapage d'application et la tâche de rattrapage de conteneur correspondent aux règles créées dans la configuration de l'outil Agile.

Avant de commencer

Rôles requis : sn_vul.app_read_all, sn_vul_container.read_all, sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin.

Procédure

1. Accédez à la **Tous** > **Agile Management pour VR** > **Configurer les outils Agile**.
2. Pour créer une règle de configuration dans la configuration de l'outil Agile, sélectionnez **Nouveau**.
3. Remplissez les champs du formulaire.

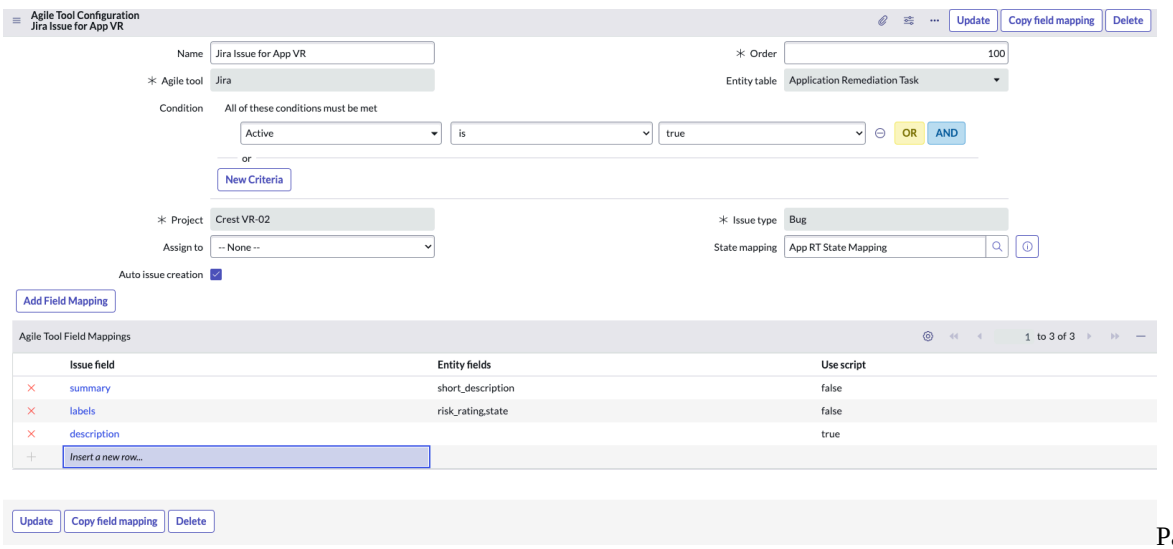
Formulaire de configuration de l'outil Agile

Champ	Description
Nom	Nom de la configuration de l'outil Agile.
Ordre	Ordre de la configuration de l'outil Agile.
Outil Agile	L'outil agile pour créer des problèmes sur une plateforme Agile spécifique.
Table d'entité	Table sur laquelle la règle de configuration doit être appliquée.
Condition	Condition de filtre sur la table d'entité sélectionnée pour créer des problèmes sur la plateforme Agile.
Création automatique de problème	La règle de configuration sera interrogée lorsqu'un nouvel enregistrement est créé dans la table d'entité sélectionnée, uniquement si la case est cochée. **Remarque :** L'utilisateur doit utiliser l'action de la liste pour créer des problèmes pour les enregistrements d'entité existants.
Projet	Le projet dans lequel le problème Jira sera créé.
Type de problème	Type de problème à créer dans un projet particulier.
Affecter à	Le délégataire auquel le problème doit être affecté lors de la création du problème. Pour conserver les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	problèmes créés comme non affectés, sélectionnez « Aucun ».
Mappage de l'état	Les mappages d’état existants à partir de la table Mappage de l’état de l’outil Agile ou créez un nouveau mappage d’état entre l’état du problème dans la plateforme Agile et les états de la table d’entité ServiceNow .



Par défaut, lorsque l’application est installée, la tâche de rattrapage d’application et la tâche de rattrapage de conteneur s’affichent dans le champ Table d’entité du formulaire de configuration de l’outil Agile.

4. Pour ajouter l’élément vulnérable d’application et l’élément vulnérable de conteneur dans la liste de choix de la table d’entités, accédez aux **propriétés système** > **sn_vul_agile.tablesToShow** et ajoutez tout dans le champ Valeur.

Formulaire de propriété système

Champ	Description
Choix	Valeurs séparées par des virgules pour une liste de choix.
Valeur	Définissez la valeur souhaitée pour la propriété. Toutes les valeurs de propriété sont stockées sous forme de chaînes. Lors de la récupération des propriétés via la méthode gs.getProperty(), traitez les résultats comme des chaînes. Par exemple, une propriété true|false renvoie 'true' ou 'false' (chaînes), et non l’équivalent booléen.

5. Sélectionnez l’enregistrement de mappage d’état existant ou créez un nouveau mappage d’état dans Mappage d’état de l’outil Agile.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Mappage de l’état de l’outil Agile

Champ	Description
Nom	Insérez le nom unique du mappage d’état.
Outil Agile	Sélectionnez l’outil agile.
Table d'entité	Sélectionnez la table source sur laquelle le mappage d’état sera créé.
Projet	Sélectionnez le projet dans lequel l’état sera mappé.
État de l'entité ServiceNow	Sélectionnez l’état que vous souhaitez mapper avec l’état de l’outil agile.
État de l'outil Agile	Sélectionnez l’état que vous souhaitez mapper à partir des états des éléments de vulnérabilité.

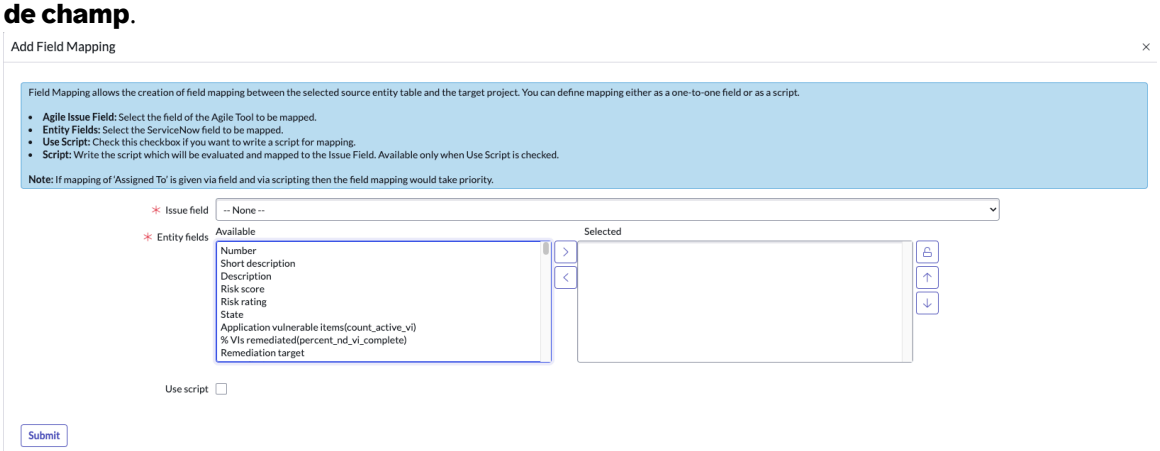
6. Cliquez sur **Enregistrer et extraire les projets** pour récupérer les projets dans le champ Projet Règle de configuration et valider les informations d’identification de l’outil Agile.

   Conseil : Vous pouvez définir la propriété système **projectsPageSize** pour extraire un certain nombre de projets par page.

7. Accédez à **Propriétés système> sn_vul_jira.projectsPageSize** et ajoutez le nombre de projets à extraire par page dans le champ Valeur de Jira Cloud.
8. Sélectionnez le projet, le type de problème et Affecter à dans la règle de configuration une fois les projets récupérés.

   Le mappage de champs par défaut est renseigné dans la liste incorporée des mappages de champs d’outils Agile. Par défaut, les champs Résumé et Description des problèmes sont mappés.

9. Pour mapper d’autres champs de problème avec les ServiceNow champs, cliquez sur Ajouter un **mappage de champ**.



Remarque :

- Vous devez mapper uniquement les champs de type Chaîne et Choix.
- Assurez-vous que tous les champs de problèmes obligatoires de l'outil Agile sont correctement mappés avec le champ d'entité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Mappage de l'état de l'outil Agile

Champ	Description
Champ du problème	Contient les champs de problème du projet actuellement sélectionné et le type de problème dans la règle de configuration.
Champs d'entité	Contient les champs de la table d'entité sélectionnée dans la règle de configuration.
Utiliser le script	Sélectionnez cette option pour utiliser le script de mappage des champs de problème avec les champs d'entité.
Script	Script pour mapper le champ Problème avec les champs d'entité.

10. Cliquez sur **Soumettre** dans la fenêtre modale Glide pour soumettre l'enregistrement du mappage de champs dans la table Mappages de champs de l'outil Agile.

    Remarque : Si vous ne mappez pas les champs obligatoires, aucun problème ne sera créé pour cette règle de configuration.

    Les champs obligatoires sont affichés en haut du formulaire Configuration de l'outil Agile.
    Tous les mappages de champs pour une règle de configuration particulière sont affichés dans la liste incorporée de la table Mappage de champs de l'outil Agile dans la table Configuration de l'outil Agile.

11. Cliquez avec le bouton droit de la souris sur l'en-tête pour enregistrer vos modifications.
    L'enregistrement enregistré est visible dans la table Configuration de l'outil Agile. Si un enregistrement est créé dans l'élément vulnérable d'application, l'élément vulnérable de conteneur, la tâche de rattrapage d'application et la tâche de rattrapage de conteneur correspond à une règle de configuration, le problème sera créé pour l'enregistrement en fonction du mappage dans la règle de configuration.

12. Accédez à **Propriétés système> sn_vul_jira.cloudBulkSize** et définissez le nombre de problèmes à créer par lot dans le champ Valeur.

    Remarque : Le nombre maximal de problèmes pouvant être créés par lot dans Jira Cloud est de 50).

    Vous pouvez définir la taille du lot pour créer des problèmes sur le serveur Jira.

13. Accédez aux **propriétés système> sn_vul_jira.onPremBulkIssue** et définissez le nombre de problèmes à créer par lot dans le champ **Valeur** .
    Vous pouvez également définir le nombre d'erreurs dans le champ Valeur de la propriété système pour traiter les enregistrements de la table manifeste afin de créer des problèmes Jira jusqu'à un nombre d'erreurs spécifique.

14. Accédez aux **propriétés système** > **sn_vul_agile. ManifestErrorCount** et définir le nombre maximal de fois où le manifeste avec erreur doit être traité.

Créer manuellement un problème Agile à l'aide de l'action de liste

Lorsqu'une action de liste : Créer un problème Jira est déclenchée, les enregistrements qui correspondent aux critères de configuration de la règle doivent être pris en compte pour « Créer un problème Jira » et ces enregistrements doivent être ingérés dans la table sn_vul_agile_tool_manifest avec le mappage sélectionné dans la règle de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all, sn_vul_container.read_all.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste** > **Tâches de rattrapage/Éléments vulnérables de l'application/Éléments vulnérables du conteneur**.
2. Sélectionnez plusieurs enregistrements pour créer des problèmes Jira, puis cliquez sur **Créer un problème Jira**.
   Les enregistrements sélectionnés doivent prendre en compte le mappage de champs et le mappage d'état de l'outil Agile associé.
   Les enregistrements sélectionnés qui satisfont à la condition de règle de configuration doivent être éligibles à la création de problèmes Jira et ajoutés à la `sn_vul_agile_tool_manifest` table.

Créer manuellement un problème Agile à l'aide de l'action de formulaire

Créez manuellement un problème Agile à l'aide de l'action de formulaire. Si l'enregistrement est mis en correspondance avec une condition de règle de configuration, une fenêtre contextuelle sera remplie avec les valeurs sélectionnées dans la règle de configuration. Si elle ne correspond à aucun critère, l'utilisateur sera autorisé à sélectionner des valeurs pour les champs prédéfinis.

Avant de commencer

Assurez-vous que tous les champs de problèmes obligatoires de l'outil Agile sont correctement mappés avec le champ d'entité.

Rôles requis : sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all sn_vul_container.read_all.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste** > **Tâches de rattrapage/Éléments vulnérables de l'application/Éléments vulnérables du conteneur**.
2. Sélectionnez n'importe quel enregistrement pour créer manuellement un problème Agile.
3. Sélectionnez **Créer un problème Agile**.
4. Insérez les détails valides pour les champs mentionnés.

   Si l'enregistrement satisfait à la condition d'une règle de configuration, les champs ci-dessous doivent être renseignés avec la valeur configurée et l'utilisateur peut modifier les valeurs de champ.

Champ	Description
Projet	Sélectionnez le projet dans lequel le problème Jira sera créé.
Type de problème	Sélectionnez le type de problème à créer dans un projet particulier.
Affecter à	Sélectionnez le délégataire auquel le problème doit être affecté lors de la création du problème.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mappage de champs	Sélectionnez les champs de type de problème de l'outil Agile et insérez les valeurs directes pour le champ sélectionné.

5. Sélectionnez **Créer un problème Agile** pour soumettre l'enregistrement.
   Après avoir soumis l'enregistrement, l'entrée d'enregistrement est créée dans sn_vul_agile_tool_manifest table.

Synchroniser manuellement l'état Jira du problème

Mettez à jour l'état de l'enregistrement unique en cliquant sur le bouton **Synchroniser l'état Agile** du menu contextuel du formulaire et mettez à jour les états de plusieurs enregistrements en cliquant sur l'action de liste **. Synchroniser l'état Agile** de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur et de la table Tâche de rattrapage dans l'espace de travail du gestionnaire de vulnérabilité.

Avant de commencer

Rôles requis : sn_vul_agile.agile_tool_admin ou sn_vul_jira.admin, sn_vul.app_read_all sn_vul_container.read_all.

Pourquoi et quand exécuter cette tâche

L'état est synchronisé depuis l'outil Agile si l'état de ServiceNow l'entité est fermé ServiceNow dans ou si une entité est rouverte (c.-à-d. si l'état est Ouvert). Tous les autres états seront reflétés de l'outil Agile vers ServiceNow. L'utilisateur ne sera pas autorisé à synchroniser l'état des enregistrements dont la règle configurée associée n'a pas de mappage d'état ni les problèmes directement créés à partir de l'action de formulaire.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste** > **Tâches de rattrapage/Éléments vulnérables de l'application/Éléments vulnérables du conteneur**.
2. Sélectionnez plusieurs enregistrements pour créer des problèmes Jira, puis cliquez sur **Synchroniser l'état Agile**.
   Les états des enregistrements pour lesquels des problèmes sont déjà créés sont mis à jour si l'enregistrement n'est pas à l'état Fermé et si le mappage d'état existe pour les enregistrements sélectionnés dans la règle de configuration.
3. Ouvrez un enregistrement et **l'état de synchronisation Agile** est visible dans le menu contextuel du formulaire si les conditions suivantes sont remplies.
   - Un problème a été créé pour l'enregistrement et l'enregistrement n'est pas à l'état Fermé
   - Le mappage d'état existe pour l'enregistrement
4. Cliquez sur **Synchroniser l'état Agile** pour synchroniser l'état Agile avec l'état mappé.
   Vous pouvez définir la propriété système pour définir la taille du lot pour l'extraction de l'état du problème à partir de Jira.
5. Accédez à la **Propriété système > sn_vul_jira.bulkIssueStatusSize**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour le serveur Jira, le nombre maximum de problèmes à renvoyer (par défaut est 50). La valeur maximale autorisée est dictée par la propriété Jira « jira.search.views.default.max ». Si vous spécifiez une valeur supérieure à ce nombre, vos résultats de recherche seront tronqués.
- Si le problème est créé à partir d'une action de formulaire ou si la règle configurée n'a pas de mappage d'état, ces enregistrements ne sont pas pris en compte pour la synchronisation de l'état.

Configurer le planificateur pour créer automatiquement des problèmes

Configurez le planificateur pour qu'il s'exécute et crée automatiquement les Jira problèmes pour les enregistrements qui ont été créés dans la table sn_vul_agile_tool_manifest.

Avant de commencer
Rôle requis : admin ou schedule_admin.

Pourquoi et quand exécuter cette tâche
Tous les enregistrements de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur, de la tâche de rattrapage de l'application et du rattrapage du conteneur créés dans la table sn_vul_agile_manifest seront pris en compte pour Jira la création du problème.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés** > **Créer des problèmes Jira**.
2. Vous pouvez modifier les champs Exécution, Fuseau horaire et Heure dans le script planifié.

Formulaire Exécution de script planifiée

Champ	Description
Exécuter	Intervalle de temps à utiliser pour l'exécution de la tâche planifiée : ○ Quotidien : s'exécute quotidiennement, à une heure donnée. ○ Hebdomadaire : s'exécute toutes les semaines, à une heure et un jour donnés. ○ Mensuel : s'exécute mensuellement, à une heure et un jour désignés du mois. ○ Périodiquement : s'exécute sur un intervalle de répétition désigné. ○ Once (Une fois) : s'exécute pour une seule occurrence. ○ Sur demande : s'exécute immédiatement sur demande. ○ Calendrier d'entreprise : début de l'entrée : s'exécute aux dates d'entrée de début du calendrier d'entreprise que vous sélectionnez dans le champ. Une tâche planifiée s'exécute pour la date de début de chaque entrée d'entreprise que vous avez définie pour le calendrier d'entreprise. Par exemple, si le calendrier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'entreprise représente une année fiscale et que la date de début de chaque entrée est un mois fiscal, alors la tâche planifiée s'exécute le premier jour de chaque mois. ○ Calendrier d’entreprise : fin de l’entrée : s’exécute pour la date de fin du calendrier d’entreprise que vous sélectionnez dans le champ. Cette sélection s'exécute de la même façon que Calendrier d'entreprise : début de l'entrée, mais en fonction des dates de fin des entrées du calendrier d'entreprise associées. **Remarque :** Lorsque vous sélectionnez Calendrier d'entreprise : début de l'entrée ou Calendrier d'entreprise : fin de l'entrée, vous pouvez appliquer un facteur de décalage pour planifier la tâche à exécuter avant ou après la période du calendrier d'entreprise sélectionné. Pour en savoir plus, consultez les champs Type de décalage et Décalage. Pour en savoir plus sur la création et l’utilisation de calendriers d’entreprise et sur la définition d’entrées de calendrier d’entreprise, reportez-vous aux rubriques Créer un calendrier d’entreprise et Définir des entrées de calendrier d’entreprise .
Jour	Jour où la tâche planifiée doit s'exécuter. ○ Si le champ Exécution est défini sur Hebdomadaire, sélectionnez le jour de la semaine. Choisissez mercredi, par exemple. ○ Si le champ Exécution est défini sur Mensuel, sélectionnez le jour du mois. Par exemple, sélectionnez 25 pour le 25e jour du mois. Ce champ n'apparaît que si vous sélectionnez Mensuel ou Hebdomadaire dans le champ Exécution.
Intervalle de répétition	Durée de l'intervalle de répétition pour chaque exécution de tâche planifiée. Entrez la durée en nombre de jours, d'heures ou de minutes. Par exemple :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Pour exécuter la tâche prévue tous les quatre jours, saisissez 04 dans le champ Jours. ○ Pour l'exécuter toutes les 26 heures, entrez 26 dans le champ Heures. ○ Si elle doit se répéter à un intervalle de 13 heures 30 minutes et 25 secondes, saisissez 13 dans le champ Heures, puis 30 et 25 dans les deux champs non libellés suivants.
Heure	Heure de la journée à laquelle la tâche planifiée doit s'exécuter, indiquée en heures, minutes et secondes dans un format de 24 heures. La sélection que vous effectuez dans le champ Fuseau horaire détermine le fuseau horaire de cette entrée.
Fuseau horaire	Fuseau horaire à utiliser avec l'entrée du champ Heure lorsque vous spécifiez l'heure à laquelle la tâche planifiée doit être exécutée. Sélectionnez une entrée de fuseau horaire : ○ **Aucun** : utilisez le fuseau horaire par défaut pour l'utilisateur connecté qui crée la tâche planifiée. Par exemple, la tâche planifiée s'exécute à 16 h 45, heure US/Pacific, s'il s'agit du fuseau horaire affecté à l'utilisateur et que vous entrez 16:45 dans le champ Heure. ○ **Utiliser le fuseau horaire du système** : utilisez le fuseau horaire du système par défaut spécifié pour l'instance dans laquelle il s'exécute. Par exemple, la tâche prévue s'exécute à 22 h 15, heure de Londres, si Europe/London est le fuseau horaire du système par défaut pour l'instance, et que vous entrez 22:15 dans le champ Heure. ○ Fuseau horaire actuel. ○ Par exemple, la tâche planifiée s'exécute à 13 h 30 dans le fuseau horaire de l'Est des États-Unis si vous sélectionnez États-Unis/Est et saisissez 13 h 30 dans le champ Heure.
run_as	Par défaut, run_ en tant que valeur de champ doit être vide. L'utilisateur peut définir la valeur en tant que valeur de l'utilisateur de domaine pour créer un problème pour un domaine spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer le planificateur pour mettre à jour automatiquement les problèmes

Configurez le planificateur pour qu'il mette à jour automatiquement les Jira problèmes pour les enregistrements qui ont été ajoutés dans la table sn_vul_agile_tool_manifest.

Avant de commencer
Rôle requis : admin ou schedule_admin.

Pourquoi et quand exécuter cette tâche
Tous les enregistrements de l'élément vulnérable de l'application, de l'élément vulnérable du conteneur, de la tâche de rattrapage de l'application et du rattrapage du conteneur créés dans la table sn_vul_agile_manifest sont pris en compte pour Jira la mise à jour du problème. Si l'enregistrement est fermé et que des commentaires sont ajoutés, ces valeurs doivent également être mises à jour pour le problème associé Jira .

Remarque :

- La tâche planifiée « Mettre à jour les problèmes » ne met pas à jour l'état Jira si le workflow pour le projet de problème Agile choisi empêche tout utilisateur de modifier directement l'état à partir d'un autre état.
- Si vous fermez un enregistrement d'entité avec des commentaires supplémentaires, seul le dernier commentaire est pris en compte au moment de la mise à jour. Pour la prochaine mise à jour, tous les commentaires sont ajoutés à l'enregistrement associé Jira.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés** > **Mettre à jour les problèmes Jira**.
2. Vous pouvez modifier les champs **Exécution**, **Fuseau horaire** et **Heure** dans le script planifié.

Formulaire Exécution de script planifiée

Champ	Description
Exécuter	Intervalle de temps à utiliser pour l'exécution de la tâche planifiée : ○ Quotidien : s'exécute quotidiennement à l'heure désignée. ○ Hebdomadaire : S'exécute toutes les semaines, à une heure et un jour précis. ○ Mensuel : s'exécute tous les mois, à une heure et un jour du mois désignés. ○ Périodiquement : s'exécute selon l'intervalle de répétition désigné. ○ Une fois : s'exécute pour une seule occurrence uniquement. ○ Sur demande : s'exécute immédiatement sur demande. ○ Calendrier d'entreprise : début de l'entrée : s'exécute aux dates d'entrée de début du calendrier d'entreprise que

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	vous sélectionnez dans le champ. Une tâche planifiée s'exécute pour la date de début de chaque entrée d'entreprise que vous avez définie pour le calendrier d'entreprise. Par exemple, si le calendrier d'entreprise représente une année fiscale et que la date de début de chaque entrée est un mois fiscal, alors la tâche planifiée s'exécute le premier jour de chaque mois. ○ Calendrier d'entreprise : fin de l'entrée : s'exécute pour la date de fin du calendrier d'entreprise que vous sélectionnez dans le champ. Cette sélection s'exécute de la même façon que Calendrier d'entreprise : début de l'entrée, mais en fonction des dates de fin des entrées du calendrier d'entreprise associées. **Remarque :** Lorsque vous sélectionnez Calendrier d'entreprise : début de l'entrée ou Calendrier d'entreprise : fin de l'entrée, vous pouvez appliquer un facteur de décalage pour planifier la tâche à exécuter avant ou après la période du calendrier d'entreprise sélectionné. Pour en savoir plus, consultez les champs Type de décalage et Décalage. Pour en savoir plus sur la création et l'utilisation de calendriers d'entreprise et sur la définition d'entrées de calendrier d'entreprise, reportez-vous aux rubriques et Créer un calendrier d'entreprise Définir des entrées de calendrier d'entreprise .
Jour	Jour où la tâche planifiée doit s'exécuter. ○ Si le champ Exécution est défini sur Hebdomadaire, sélectionnez le jour de la semaine. Choisissez mercredi, par exemple. ○ Si le champ Exécution est défini sur Mensuel, sélectionnez le jour du mois. Par exemple, sélectionnez 25 pour le 25e jour du mois. Ce champ n'apparaît que si vous sélectionnez Mensuel ou Hebdomadaire dans le champ Exécution.
Intervalle de répétition	Durée de l'intervalle de répétition pour chaque exécution de tâche planifiée. Entrez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	la durée en nombre de jours, d'heures ou de minutes. Par exemple : ○ Pour exécuter la tâche prévue tous les quatre jours, saisissez 04 dans le champ Jours. ○ Pour l'exécuter toutes les 26 heures, entrez 26 dans le champ Heures. ○ Si elle doit se répéter à un intervalle de 13 heures 30 minutes et 25 secondes, saisissez 13 dans le champ Heures, puis 30 et 25 dans les deux champs non libellés suivants.
Heure	Heure de la journée à laquelle la tâche planifiée doit s'exécuter, indiquée en heures, minutes et secondes dans un format de 24 heures. La sélection que vous effectuez dans le champ Fuseau horaire détermine le fuseau horaire de cette entrée.
Fuseau horaire	Fuseau horaire à utiliser avec l'entrée du champ Heure lorsque vous spécifiez l'heure à laquelle la tâche planifiée doit être exécutée. Sélectionnez une entrée de fuseau horaire : ○ Aucun : utilisez le fuseau horaire par défaut pour l'utilisateur connecté qui crée la tâche planifiée. Par exemple, la tâche planifiée s'exécute à 16h45. Heure des États-Unis/Pacifique s'il s'agit du fuseau horaire affecté à l'utilisateur et si vous saisissez 16:45 dans le champ Heure. ○ Utiliser le fuseau horaire du système : utilisez le fuseau horaire du système par défaut spécifié pour l'instance dans laquelle il s'exécute. Par exemple, la tâche planifiée s'exécute à 22h15, heure de Londres, si Europe/Londres est le fuseau horaire système par défaut pour l'instance, et vous saisissez 22h15 dans le champ Heure. ○ Fuseau horaire actuel. ○ Par exemple, la tâche planifiée s'exécute à 13h30 dans le fuseau horaire de l'Est des États-Unis si vous sélectionnez US/Est et entrez 13h30 dans le champ Heure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
run_as	Par défaut, la valeur **du champ run_ en tant que** est vide. Vous pouvez définir la valeur sur un utilisateur de domaine pour créer un problème pour un domaine spécifique.

Configurer le planificateur pour synchroniser automatiquement l'état JiraServiceNow® sur

Configurez le planificateur pour synchroniser l'état des problèmes avec l'élément de vulnérabilité de l'application, les éléments de vulnérabilité du Jira conteneur et les tâches dans la table sn_vul_agile_manifest.

Avant de commencer

Rôle requis : schedule_admin ou admin

Pourquoi et quand exécuter cette tâche

Le planificateur s'exécute automatiquement en fonction de la planification configurée. L'état des enregistrements créés dans la table Élément vulnérable d'application, Élément vulnérable de conteneur, Tâche de rattrapage d'application et Tâche de rattrapage de conteneur qui ont des problèmes créés dans Jira est mis à jour en fonction de l'état actuel du problème dans la Jira plateforme en fonction du mappage d'état dans la règle de configuration.

Tous les enregistrements d'élément vulnérable d'application, d'élément vulnérable de conteneur, de tâche de rattrapage d'application et de rattrapage de conteneur créés dans la table sn_vul_agile_manifest seront pris en compte pour Jira la création du problème.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés** > **État de la synchronisation**.
2. Vous pouvez modifier les champs Exécution, Fuseau horaire et Heure dans le script planifié.

Formulaire Exécution de script planifiée

Champ	Description
Exécuter	Intervalle de temps à utiliser pour l'exécution de la tâche planifiée : ○ Quotidien : s'exécute quotidiennement à l'heure désignée. ○ Hebdomadaire : S'exécute toutes les semaines, à une heure et un jour précis. ○ Mensuel : s'exécute tous les mois, à une heure et un jour du mois désignés. ○ Périodiquement : s'exécute selon l'intervalle de répétition désigné. ○ Une fois : s'exécute pour une seule occurrence uniquement. ○ Sur demande : s'exécute immédiatement sur demande. ○ Calendrier d'entreprise : début de l'entrée : s'exécute aux dates d'entrée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	de début du calendrier d’entreprise que vous sélectionnez dans le champ. Une tâche planifiée s’exécute pour la date de début de chaque entrée d’entreprise que vous avez définie pour le calendrier d’entreprise. Par exemple, si le calendrier d'entreprise représente une année fiscale et que la date de début de chaque entrée est un mois fiscal, alors la tâche planifiée s'exécute le premier jour de chaque mois. ○ Calendrier d’entreprise : fin de l’entrée : s’exécute pour la date de fin du calendrier d’entreprise que vous sélectionnez dans le champ. Cette sélection s'exécute de la même façon que Calendrier d'entreprise : début de l'entrée, mais en fonction des dates de fin des entrées du calendrier d'entreprise associées. **Remarque :** Lorsque vous sélectionnez Calendrier d'entreprise : début de l'entrée ou Calendrier d'entreprise : fin de l'entrée, vous pouvez appliquer un facteur de décalage pour planifier la tâche à exécuter avant ou après la période du calendrier d'entreprise sélectionné. Pour en savoir plus, consultez les champs Type de décalage et Décalage. Pour en savoir plus sur la création et l’utilisation de calendriers d’entreprise et sur la définition d’entrées de calendrier d’entreprise, reportez-vous aux rubriques Créer un calendrier d’entreprise et Définir des entrées de calendrier d’entreprise .
Jour	Jour où la tâche planifiée doit s'exécuter. ○ Si le champ Exécution est défini sur Hebdomadaire, sélectionnez le jour de la semaine. Choisissez mercredi, par exemple. ○ Si le champ Exécution est défini sur Mensuel, sélectionnez le jour du mois. Par exemple, sélectionnez 25 pour le 25e jour du mois. Ce champ n'apparaît que si vous sélectionnez Mensuel ou Hebdomadaire dans le champ Exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Intervalle de répétition	Durée de l'intervalle de répétition pour chaque exécution de tâche planifiée. Entrez la durée en nombre de jours, d'heures ou de minutes. Par exemple : ○ Pour exécuter la tâche prévue tous les quatre jours, saisissez 04 dans le champ Jours. ○ Pour l'exécuter toutes les 26 heures, entrez 26 dans le champ Heures. ○ Si elle doit se répéter à un intervalle de 13 heures 30 minutes et 25 secondes, saisissez 13 dans le champ Heures, puis 30 et 25 dans les deux champs non libellés suivants.
Heure	Heure de la journée à laquelle la tâche planifiée doit s'exécuter, indiquée en heures, minutes et secondes dans un format de 24 heures. La sélection que vous effectuez dans le champ Fuseau horaire détermine le fuseau horaire de cette entrée.
Fuseau horaire	Fuseau horaire à utiliser avec l'entrée du champ Heure lorsque vous spécifiez l'heure à laquelle la tâche planifiée doit être exécutée. Sélectionnez une entrée de fuseau horaire : ○ -Aucun- : utilisez le fuseau horaire par défaut de l'utilisateur connecté qui crée la tâche planifiée. Par exemple, la tâche planifiée s'exécute à 16 h 45, heure US/Pacific, s'il s'agit du fuseau horaire affecté à l'utilisateur et que vous entrez 16:45 dans le champ Heure. ○ Utiliser le fuseau horaire du système : utilisez le fuseau horaire du système par défaut spécifié pour l'instance dans laquelle il s'exécute. Par exemple, la tâche planifiée s’exécute à 22h15, heure de Londres, si Europe/Londres est le fuseau horaire système par défaut pour l’instance, et vous saisissez 22h15 dans le champ Heure. ○ Fuseau horaire actuel. ○ Par exemple, la tâche planifiée s’exécute à 13h30 dans le fuseau horaire de l’Est des États-Unis si vous sélectionnez US/Est et entrez 13h30 dans le champ Heure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
run_as	Par défaut, la valeur du champ run_ en tant que est vide. Vous pouvez définir la valeur comme la valeur de l'utilisateur du domaine requis pour créer un problème pour un domaine spécifique.

Intégration Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

L'intégration Prisma Cloud Compute vous permet d'analyser les hôtes pour détecter les vulnérabilités.

À partir de la version 24.02.0 de , Réponse aux vulnérabilités vous pouvez utiliser l'intégration de calcul dans le cloud Prisma pour importer des vulnérabilités sur les hôtes en cours d'exécution. Les API hôtes Prisma permettent de récupérer des informations complètes sur les vulnérabilités d'un hôte spécifique et fournissent également un instantané des vulnérabilités de l'hôte à un moment précis. Cette API permet une synchronisation régulière entre Prisma et l'instance ServiceNow. Comme Prisma est proposé à la fois en tant que logiciel en tant que service (SaaS) et en tant que solution sur site, l'utilisation d'un serveur MID est nécessaire pour appeler les API Prisma à partir de l'instance ServiceNow. En outre, vous devez utiliser un Serveur MID si le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute produit et votre ServiceNow AI Platform instance ne se trouvent pas dans le même environnement. Pour plus d'informations, consultez Configuration système requise pour le Serveur MID .

Vous pouvez également afficher des rapports sur les vulnérabilités et les éléments vulnérables sur les tableaux de Réponse aux vulnérabilités bord. Ces vulnérabilités peuvent ensuite être classées par ordre de priorité et corrigées.

Affichage des intégrations

Vous pouvez afficher les intégrations qui font partie du Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute. Pour afficher les intégrations, accédez à **Tous** > **Intégration des calculs dans le cloud Prisma** > **Intégrations**.

Les intégrations suivantes sont disponibles.

Séquence d'exécution	Planifier	Intégration	Description
1	Quotidien	Intégration des hôtes de calcul dans le cloud Prisma	Récupère les vulnérabilités des hôtes et crée des VIT, des détections et des éléments découverts pour les hôtes.

Remarque : Si le module d'extension Container Vulnerability Response est installé, vous pouvez également afficher les intégrations liées à Container Vulnerability Response.

Processus d'intégration Prisma

Lors de l'exécution Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute , il vérifie s'il existe une vulnérabilité et une exposition communes (CVE) dans la table Base de données de vulnérabilité nationale (NVD). Si elles sont déjà présentes, les informations existantes sont utilisées. Toutefois, si le CVE n'est pas trouvé, des enregistrements d'espace réservé sont générés dans la table NVD. Lors de la création de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ces enregistrements NVD d'espace réservé, seuls les CVE et leur nom sont initialement renseignés. D'autres détails ne sont pas renseignés en supposant que l'intégration NVD les renseigne ultérieurement. Si le paramètre *update_nvd* d'instance d'intégration est défini sur vrai, les enregistrements NVD de l'espace réservé sont mis à jour. Par défaut, le paramètre d'instance est défini sur false. Cependant, au moins jusqu'à ce que l'intégration NVD s'exécute et renseigne ces détails, une certaine compréhension des CVE, telles que sa gravité ou des informations de base sur le problème est nécessaire. Pour répondre à cette exigence, les champs **Exploit existent** et les **notes de rattrapage** sont renseignées avec les détails obtenus à partir de Prisma. De plus, cette configuration est personnalisable, ce qui vous permet de spécifier tous les autres champs que vous souhaitez renseigner dans l'entrée NVD en fonction des informations fournies par Prisma.

Préparation pour le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

Vous pouvez vous préparer en effectuant des Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute tâches de configuration.

Avant de commencer

Pour installer et configurer l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute , vous pouvez imprimer la liste de vérification suivante. Vérifiez que les éléments énumérés sont terminés avant d'installer l'application et importez les données de vulnérabilité dans votre ServiceNow AI Platform® instance.

Liste de vérification de la préparation de l'intégration

Tâche	Description
☐	Vérifiez que vous disposez des ensembles d'informations suivants : • URL de base de l'API • Nom d'utilisateur et mot de passe. Ces informations d'identification sont utilisées pour extraire les vulnérabilités de l'intégration Prisma Cloud Compute. Pour plus d'informations, voir https://pan.dev/compute/api/ **Remarque :** Serveur MID est facultatif. Les informations d'identification de l'utilisateur utilisées pour l'intégration de Prisma Cloud Compute ont besoin d'une autorisation pour surveiller les images. Consultez le code suivant : `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Si elle n'est pas déjà installée et activée, installez l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour plus d'informations sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration requiert la version 16.1 ou Réponse aux vulnérabilités ultérieure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
☐	Obtenez les autorisations et téléchargez l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute sur votre ServiceNow AI Platform® instance.
☐	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance ou si vous avez besoin d'aide, contactez ServiceNow l'assistance technique.
☐	Vérifiez que vous disposez des groupes ou utilisateurs suivants pour gérer les intégrations et corriger les éléments vulnérables : **administrateur** Installez l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute. S'il n'est pas affecté, l'administrateur affecte le rôle d'administrateur de vulnérabilité du conteneur (sn_vul_container.vulnerability_admin) et d'autres rôles. **sn_vul_container.vulnerability_admin** Termine la configuration de l'intégration des calculs dans le cloud Prisma. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités pour conteneurs (CVR) et à ses enregistrements. Cet administrateur configure les intégrations et les règles dans Réponse aux vulnérabilités pour conteneurs. **Groupe de réponse aux vulnérabilités** Par défaut, le groupe Vulnerability Response est disponible. Les utilisateurs affectés au groupe Réponse aux vulnérabilités héritent de sn_vul.read_all sn_vul_container.read_all. **Groupe propriétaire du rattrapage de conteneur** Par défaut, le groupe propriétaire du rattrapage de conteneurs est disponible. Les utilisateurs affectés à ce groupe héritent du sn_vul_container.remediation_owner. Le propriétaire de rattrapage de conteneur corrige les vulnérabilités des conteneurs qui lui sont affectées ou qui sont affectées à un groupe auquel il appartient. **Analyste de vulnérabilité** Les utilisateurs affectés au groupe d'analystes de vulnérabilité de conteneur héritent de sn_vul.vulnerability_analyst. L'analyste de vulnérabilité surveille le rattrapage de tous les éléments vulnérables. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance. Pour plus d'informations, consultez Créer un groupe d'utilisateurs .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
☐	Installez l'intégration Réponse aux vulnérabilités avec NVD et exécutez l'API d'intégration de la base de données des vulnérabilités nationale du NIST (CVE UNIQUEMENT).

Vous êtes prêt à Configurer l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute.

Installer Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que le produit Prisma Cloud Compute s'intègre correctement à Réponse aux vulnérabilités et Réponse aux vulnérabilités pour conteneurs. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Rôle requis : admin

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute .
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez une Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute application.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Lisez les sections **Autres exigences** et **dépendances** , au besoin.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Mettez à jour le **nom de l'instance** et la **raison d'être des champs Instance** , puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Votre application est automatiquement installée sur votre instance.

Que faire ensuite
Configurez le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute pour votre environnement. Consultez Configurer l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute.

Configurer l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

Installez et configurez l'application pour importer des Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute données à partir de Prisma Cloud Compute. Vous pouvez utiliser les données importées pour classer par ordre de priorité et corriger les vulnérabilités de vos hôtes.

Avant de commencer
Rôle requis : admin

Procédure

1. Ouvrez l'e-mail que vous avez reçu au sujet de ServiceNow l'intégration.
2. Connectez-vous à votre instance en tant qu'administrateur.
3. Suivez les instructions dans l'e-mail pour obtenir le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute.
4. Accédez à la **Tous** > **Intégration des calculs dans le cloud Prisma** > **Administration** > **Configuration**.
   Renseignez les champs du formulaire Configuration de calcul dans le cloud Prisma. Pour plus d'informations, consultez Formulaire Configuration des calculs dans le cloud Prisma.
5. Dans la liste Projets, sélectionnez **Tous les projets** ou **Projets spécifiques** pour configurer respectivement tous les projets ou les projets sélectionnés.
   Si vous sélectionnez **Projets spécifiques**, vous pouvez sélectionner les projets dans la liste Disponibles.
6. Pour terminer la configuration, sélectionnez **Terminer** ou **Enregistrer et tester les informations d'identification**.
   - Si vous avez configuré un projet, sélectionnez **Terminer**.
   - Si vous n'avez pas configuré de projet, sélectionnez **Enregistrer et tester les informations d'identification**
7. Affichez l'instance nouvellement créée en accédant à **Intégration des calculs dans le cloud Prisma** > **Administration** > **Instances d'intégration**.
8. Affichez les projets que vous avez configurés précédemment en sélectionnant **Paramètres d'instance d'intégration**.
9. Exécutez l'instance d'intégration nouvellement créée pour importer les éléments vulnérables.
   Les VIT sont ensuite créés en fonction de la granularité.
10. Configurer la granularité d'un élément vulnérable.
    a. Accédez à la **Intégration des calculs dans le cloud Prisma** > **Configurer les clés de vulnérabilité de l'image**
    b. Configurez la granularité des VIT en cochant les cases requises.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les éléments vulnérables sont créés en fonction des clés sélectionnées lors de l'importation suivante.

Remarque : Par défaut, un VIT est créé pour une combinaison de Référentiel d'images,] Vulnérabilité et Balise d'image. Vous pouvez ajouter des composants à la clé pour plus de granularité. Par exemple, vous pouvez créer une CVIT pour une combinaison de référentiel d'images, vulnérabilité, balise d'image et grappe. Une fois les éléments vulnérables ou les conclusions d'éléments vulnérables créés, les cases ne sont plus modifiables.

Tableau de l'état d'exécution de l'intégration pour l'intégration des calculs dans le cloud Prisma

Le module État de l'exécution de l'intégration des calculs dans le cloud Prisma vous fournit une vue graphique de l'état des exécutions de l'intégration des calculs dans le cloud Prisma.

Dans le graphique, pointez sur n'importe quelle partie du graphique pour afficher un résumé des données spécifiques à cette partie. Si vous cliquez sur une partie du graphique à barres, une liste s'ouvre pour fournir des informations plus détaillées.

Rôle requis : administrateur de vulnérabilité

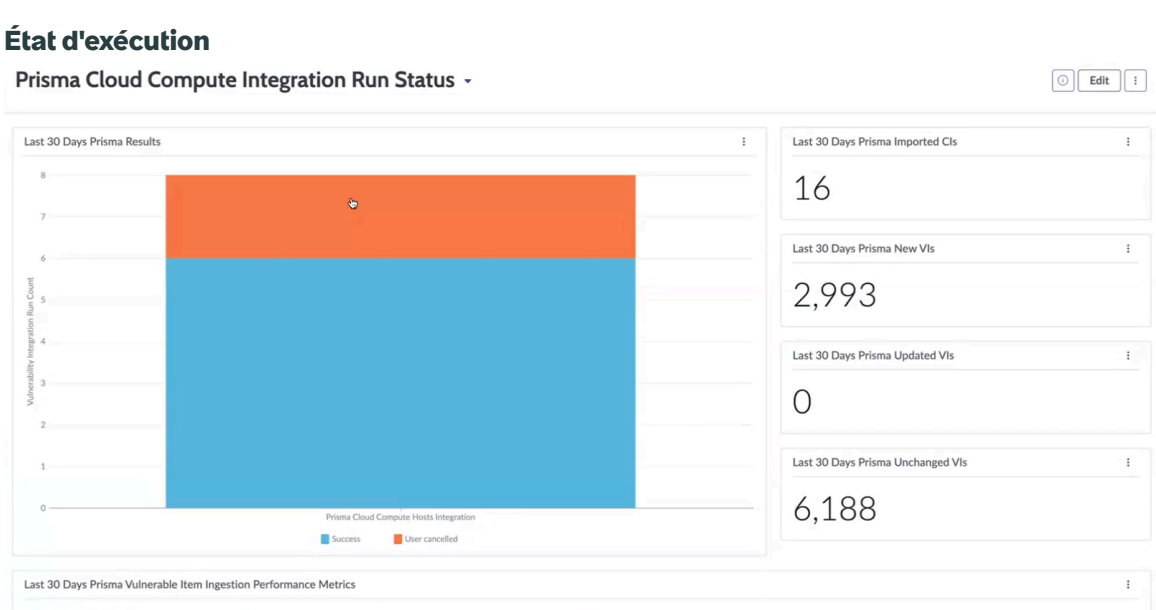
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher les données, accédez à **Tous** > **Intégration des calculs dans le cloud Prisma** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports de graphiques d'état d'exécution de l'intégration de calcul dans le cloud Prisma

Nom	Description
Résultats Prisma au cours des 30 derniers jours	Nombre d'exécutions d'intégration terminées pour l'intégration. Affiche les exécutions réussies et échouées. Chaque exécution s'affichait sous la forme d'une barre dans le graphique.
CI importés Prisma au cours des 30 derniers jours	Nombre d'éléments de configuration (CI) importés par Prisma au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Nouveaux VI Prisma au cours des 30 derniers jours	Nombre de nouveaux éléments vulnérables importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour Prisma au cours des 30 derniers jours	Nombre d'éléments vulnérables (VI) mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI non modifiés Prisma au cours des 30 derniers jours	Nombre d'éléments vulnérables en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Mesures de performance d'ingestion d'élément vulnérable Prisma au cours des 30 derniers jours	Mesures des performances quotidiennes des éléments vulnérables comparées aux 30 derniers jours.

Présentation de Wiz Réponse aux vulnérabilités l'intégration

Importez des données de vulnérabilité et de conformité à partir de Wiz scanners dans votre ServiceNow® instance de plateforme IA pour vous aider à obtenir des informations plus approfondies sur les risques de votre infrastructure dans le cloud. Ces intégrations vous fournissent une évaluation complète de votre posture globale de sécurité dans le cloud et vous aident à mener des actions de rattrapage directement à partir de votre instance.

Intégrations incluses avec l'intégration Réponse aux vulnérabilités avec Wiz

L'intégration Réponse aux vulnérabilités comprend Wiz les intégrations suivantes qui importent des données de vulnérabilité et de conformité :

- Wiz Intégration de vulnérabilité de l'hôte
- Wiz Réponse aux vulnérabilités pour conteneurs Intégration
- Wiz Conformité de la configuration (résultats des tests) Intégration et intégration des problèmes

Avantages et utilisateurs pour les intégrations

Avantage	Wiz Intégration	Utilisateurs
Importez et évaluez les détections précoces des vulnérabilités de l'hôte et des vulnérabilités des hôtes en cours d'exécution. L'intégration de la vulnérabilité de l'hôte importe les résultats relatifs aux ordinateurs virtuels et aux actifs sans serveur dans votre environnement cloud. Ces résultats sont mappés aux éléments vulnérables de	Wiz Intégration de la vulnérabilité de l'hôte.	Responsables des vulnérabilités, analystes et équipes de sécurité du cloud

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avantage	Wiz Intégration	Utilisateurs
l'hôte (VIT) dans l'application pour prendre en charge les Réponse aux vulnérabilités workflows de rattrapage.		
Importez et évaluez les données de vulnérabilité d'image de conteneur pour détecter les actifs vulnérables et non conformes dans votre infrastructure cloud. Les résultats sont mappés aux éléments vulnérables de conteneur (CVIT) pour prendre en charge les workflows de triage, de hiérarchisation des risques et de rattrapage ciblé pour les charges de travail basées sur des conteneurs.	Wiz Intégration de la vulnérabilité du conteneur.	Responsables des vulnérabilités, analystes et équipes de sécurité du cloud
Importez et évaluez les résultats des tests de configuration pour Wiz détecter les configurations dans le cloud non conformes. Les résultats sont mappés aux résultats des tests dans le cloud (CTR) dans l'application Conformité de la configuration pour vous aider à appliquer les politiques et les normes de sécurité dans votre environnement cloud. **Remarque :** Les configurations d'hôte ne Wiz sont pas importées.	Wiz Conformité de la configuration Intégration (Wiz résultats des tests).	Responsables des vulnérabilités, analystes et équipes de sécurité du cloud
Problèmes d'importation Wiz qui identifient les actifs impliqués dans des combinaisons toxiques de vulnérabilités et d'erreurs de configuration. Ces résultats sont mappés aux CTR et étiquetés avec Wiz Issues comme source pour vous aider à suivre et à corriger les actifs qui peuvent présenter des risques complexes et multivectoriels.	Wiz Intégration des problèmes.	Responsables des vulnérabilités, analystes et équipes de sécurité du cloud
Appliquez des étapes de rattrapage sur les éléments vulnérables d'hôte (VIT), les éléments vulnérables de conteneurs (CVT), les résultats des tests dans le cloud (CTR) et les CTR étiquetés Problèmes Wiz.	Réponse aux vulnérabilités, Réponse aux vulnérabilités pour conteneurs et les Conformité de la configuration applications.	Propriétaires des rattrapages

Ce qu'il faut explorer ensuite

Pour plus d'informations sur l'installation, la configuration et l'affichage des données importées avec Vulnerability Wiz Response Integration, consultez :

- Activer l'application Wiz Réponse aux vulnérabilités Intégration
- Configurer l'intégration Wiz Réponse aux vulnérabilités

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Définir le filtrage pour l'intégration des vulnérabilités de l'hôte Wiz
- Définir le filtrage pour l'intégration des vulnérabilités du Wiz conteneur
- Définir le filtrage pour l'intégration des résultats des Wiz tests
- Définir le filtrage pour l'intégration Wiz des problèmes
- Mappage de champs pour les Wiz intégrations de Réponse aux vulnérabilités

Activer l'application Wiz Réponse aux vulnérabilités Intégration

Activez l'application requise.

Avant de commencer

Vérifiez que vous avez examiné les listes de vérification et installé les applications suivantes ServiceNow® :

- Installation et prise en charge des Réponse aux vulnérabilités applications qui incluent l'intégration NVD, Réponse aux vulnérabilités l'intégration avec CISA et la tâche planifiée CWE.
- Vulnerability Response et Configuration Compliance pour conteneurs.
- Conformité de la configuration.

Ces applications sont disponibles sous forme d'abonnements distincts. Pour plus d'informations sur l'installation des applications du Store, reportez-vous à la section Installer une ServiceNow Store application .

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles**.
2. Localisez l'application Wiz Réponse aux vulnérabilités Integration.
3. Sélectionnez la carte pour l'ouvrir, puis sélectionnez **Installer**.
   Pour plus d'informations sur l'installation des applications du Store, reportez-vous à la section Installer une ServiceNow Store application .
   La boîte de dialogue Liste de vérification des dépendances s'affiche. Sélectionnez des liens **(qui doivent être installés)** pour installer les dépendances requises que vous n'avez pas encore installées.
4. Sélectionnez **Installer** dans la boîte de dialogue Installation de l'application.
   Un message s'affiche une fois l'installation de l'application réussie. Vous êtes prêt à Configurer l'intégration Wiz Réponse aux vulnérabilités.
5. Accédez à la **Tous** > **Intégration de vulnérabilité Wiz** > **Administration** > **Intégrations**.
6. Vérifiez que les intégrations avec lesquelles vous souhaitez importer des données sont activées (colonne active définie sur vrai).
7. Sélectionnez un enregistrement pour l'ouvrir et activer ou désactiver les intégrations.

Configurer l'intégration Wiz Réponse aux vulnérabilités

Configurez l'intégration dans votre Wiz compte de service et affectez des rôles dans votre ServiceNow instance de plateforme IA.

Avant de commencer

Vous devez configurer la vignette d'intégration dans votre Wiz compte qui a été créé pour cette intégration avec les autorisations présélectionnées. Consultez la documentation produit Wiz pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis :

- administrateur pour affecter des rôles dans votre ServiceNow instance de plateforme IA.

Procédure

1. Affectez des rôles aux utilisateurs pour l'intégration Wiz et pour les applications qui prennent en charge l'intégration dans votre ServiceNow instance de plateforme IA.

   a. Accédez à la **Administration utilisateurs** > **Utilisateurs**

   b. Affectez les rôles suivants.

   - sn_vul.vulnerability_admin pour configurer les Réponse aux vulnérabilités applications et Réponse aux vulnérabilités pour conteneurs .
   - sn_vulc.admin
   - sn_vul_wiz.configure_integration pour configurer l'intégration.
   - sn_vul_wiz.read_integration pour les utilisateurs de votre organisation auxquels vous souhaitez afficher les données et les enregistrements pour cette intégration.

   c. Pour plus d'informations sur la création d'utilisateurs et la gestion des rôles, reportez-vous à la rubrique Administration utilisateurs .

2. En tant qu'utilisateur disposant du rôle sn_vul_wiz.configure_integration, accédez à **Tous** > **Intégration de vulnérabilité Wiz** > **Administration** > **Configuration** dans votre instance.
3. Renseignez les champs.

Champ	Description
Instance d'intégration	Intégration de Vulnerability Response avec Wiz.
URL d'authentification	URL d'authentification que vous avez saisie dans votre Wiz environnement.
URL D'API	URL d'API que vous avez saisie dans votre Wiz environnement.
ID client	ID client que vous souhaitez utiliser pour l'intégration que vous avez saisie dans votre Wiz environnement.
Secret client	Clé secrète client que vous souhaitez utiliser pour l'intégration que vous avez saisie dans votre Wiz environnement.

4. **Sélectionnez Enregistrer et tester**.
   Un message s'affiche si les informations d'identification ont été enregistrées et validées avec succès. Vous pouvez sélectionner le filtrage pour les importations d'intégration.

Définir le filtrage pour l'intégration des vulnérabilités de l'hôte Wiz

Définissez les valeurs de filtrage pour importer les données de vulnérabilité d'hôte souhaitées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul_wiz.configure_integration

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Wiz** > **Administration** > **Configuration**.
2. Si ce n'est pas déjà fait, sélectionnez l'onglet **Configuration des vulnérabilités de l'hôte** .
3. Renseignez les champs.
   Ces champs qui s'affichent vous fournissent des filtres pour importer des données de base sur la vulnérabilité de l'hôte. Pour afficher plus d'options de filtrage, cochez la case **Avancé** et reportez-vous à la table suivante pour plus d'informations.

Champ	Description
Premier	Pagination. Saisissez une valeur. Vous préférerez peut-être commencer par 1000.
Gravité	Trouver la gravité. Aucun est la valeur par défaut. Si cette option est sélectionnée, cela indique que vous ne souhaitez importer aucune donnée pour ce champ. Vous pouvez spécifier plusieurs valeurs : ○ AUCUN : renvoie les actifs sans valeur de gravité disponible. ○ FAIBLE ○ MOYEN ○ ÉLEVÉ ○ CRITIQUE
État des ressources	Renvoyer uniquement les résultats de vulnérabilité pour les actifs avec ces états. Vous pouvez spécifier plusieurs valeurs : ○ Aucun (par défaut) : si cette option est sélectionnée, cela indique que vous ne souhaitez importer aucune donnée pour ce champ. ○ Actif ○ Erreur ○ Inactif
Type de ressource	Filtrez sur ces types d'objets. Vous pouvez spécifier les deux valeurs : ○ Aucun (par défaut) : si cette option est sélectionnée, cela indique que vous ne souhaitez importer aucune donnée pour ce champ. ○ VIRTUAL_MACHINE ○ SANS SERVEUR

4. Cochez la case Avancé pour afficher plus d'options de filtrage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour la plupart des champs, vous pouvez spécifier plusieurs valeurs. --Aucun-- est la valeur (par défaut). Si --Aucun-- reste sélectionné pour un champ, aucune donnée n'est importée pour ce champ.

Champ	Description
Statut	Filtrer par état des résultats : ○ OUVRIR ○ REJETÉ ○ RÉSOLU
Méthode de détection	Filtrez sur les résultats de vulnérabilité trouvés par ces méthodes de détection : ○ PACKAGE ○ DEFAULT_PACKAGE ○ BIBLIOTHÈQUE ○ Systèmes d'exploitation ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ FILE_PATH
Gravité du problème connexe	○ CRITIQUE ○ ÉLEVÉ ○ INFORMATIONNEL ○ FAIBLE ○ MOYEN
Vulnérabilité	Filtrez les résultats de vulnérabilité avec le ou les ID externes correspondants que vous saisissez, par exemple CVE-1234-5678, CVE-9110-26117.
A un exploit public	Filtrez les résultats de vulnérabilité pour les vulnérabilités avec un exploit disponible : (vrai/faux).
ID de projet	Filtrez les résultats de vulnérabilité avec des chaînes que vous saisissez pour les projets donnés.
A un correctif	Filtrez les résultats de vulnérabilité pour les vulnérabilités avec un correctif disponible (vrai/faux).
Ressource	Filtrez sur une ressource que vous entrez.
La ressource a des privilèges d'administrateur	Filtrez les résultats de vulnérabilité pour les actifs qui disposent de privilèges d'administrateur (vrai/faux).
Abonnement	Importez les résultats à partir des chaînes suivantes pour les abonnements externes : (compte AWS, abonnement Azure, projet GCP et compartiment

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	OCI). Vous pouvez spécifier plusieurs valeurs dans un tableau. Si vous ne fournissez pas de valeur, tous les abonnements sont renvoyés.
A un exploit CISA KEV	Filtrez les résultats de vulnérabilité pour les vulnérabilités avec un exploit CISA KEV disponible (vrai/faux).
La ressource a des privilèges élevés	Filtrez les résultats de vulnérabilité pour les actifs qui disposent de privilèges élevés (vrai/faux).
La ressource a une large exposition à Internet	Filtrez les résultats de vulnérabilité pour les actifs qui ont une exposition élevée à Internet (vrai/faux).
La ressource a une exposition limitée à Internet	Filtrez les résultats de vulnérabilité pour les actifs qui ont une faible exposition à Internet (vrai/faux).
Première observation à (après)	Filtrez par actifs affichés à partir de la date que vous avez sélectionnée.
Résolu à (après)	Filtrez par actifs avec des vulnérabilités qui ont été résolues en commençant par la date que vous sélectionnez.
Mis à jour à (après)	Filtrez par actifs qui ont été mis à jour en commençant par la date que vous sélectionnez.

5. **Sélectionnez Enregistrer et tester**.
   Si les informations d'identification ont été enregistrées et validées avec succès, un message s'affiche. Vous pouvez sélectionner le filtrage pour une autre importation d'intégration.

Définir le filtrage pour l'intégration des vulnérabilités du Wiz conteneur

Définissez les valeurs de filtrage pour importer les données de vulnérabilité de conteneur souhaitées.

Avant de commencer

Rôle requis : sn_vul_wiz.configure_integration

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Wiz** > **Administration** > **Configuration**.
2. Sélectionnez l'onglet **Configuration des vulnérabilités du conteneur** .
3. Renseignez les champs.

   Pour certains champs, vous pouvez spécifier plusieurs valeurs. --Aucun-- est la valeur (par défaut). Si --Aucun-- reste sélectionné pour un champ, aucune donnée n'est importée pour ce champ.

Champ	Description
Premier	Pagination. Saisissez une valeur. Vous préférerez peut-être commencer par 1000.
A un exploit public	Filtrez les résultats de vulnérabilité pour les vulnérabilités avec un exploit disponible : (vrai/faux).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Abonnement	Importez les résultats à partir des chaînes suivantes pour les ID d'abonnement externes : (compte AWS, abonnement Azure, projet GCP et compartiment OCI). Si vous ne fournissez pas de valeur, tous les abonnements sont renvoyés.
A un correctif	Importez les résultats de vulnérabilité pour les vulnérabilités avec un correctif disponible (vrai/faux).
Vulnérabilité	Importez les résultats de vulnérabilité avec le ou les ID externes correspondants, par exemple, CVE-1234-5678, CVE-9110-26117.
A un exploit CISA KEV	Importez uniquement les résultats de vulnérabilité pour les vulnérabilités avec un exploit CISA KEV disponible (vrai/faux).
ID de projet	Importez uniquement les résultats de vulnérabilité pour les projets donnés (chaînes).
La ressource a des privilèges élevés	Renvoyer uniquement les résultats de vulnérabilité qui disposent de privilèges élevés (vrai/faux).
État des ressources	Renvoyer uniquement les résultats avec ces états. Vous pouvez spécifier plusieurs valeurs : ○ Actif ○ Erreur ○ Inactif
La ressource a des privilèges d'administrateur	Renvoyer uniquement les résultats de vulnérabilité qui disposent de privilèges d'administrateur. (vrai/faux)
Méthode de détection	Filtrez sur les résultats de vulnérabilité trouvés par ces méthodes de détection : ○ DEFAULT_PACKAGE ○ FILE_PATH ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ BIBLIOTHÈQUE ○ Systèmes d'exploitation ○ PACKAGE
La ressource a une exposition limitée à Internet	Filtrez les résultats de vulnérabilité qui ont une faible exposition à Internet (vrai/faux).
Gravité de la vulnérabilité	Filtrer les résultats par gravité de vulnérabilité : ○ CRITIQUE ○ ÉLEVÉ ○ FAIBLE ○ MOYEN

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Statut	Filtrer les résultats par état : ○ OUVRIR ○ RÉSOLU

4. **Sélectionnez Enregistrer et tester**.
   Si les informations d'identification ont été enregistrées et validées avec succès, un message s'affiche. Vous pouvez sélectionner le filtrage pour une autre importation d'intégration.
5. **Facultatif :** Configurez la granularité des éléments vulnérables de conteneur (CVIT) en spécifiant la combinaison de clés.

   (Optional) Une CVIT est créée par défaut en combinant le référentiel d'images, la vulnérabilité et l'image. Vous pouvez ajouter des composants à la clé pour plus de granularité. Par exemple, une CVIT est destinée à une combinaison de référentiel d'images, de vulnérabilité, d'image et de grappe.

   Pour configurer la granularité, accédez à **Tous** > **Intégration de vulnérabilité Wiz** > **Administration** > **Configurer la granularité VI en fonction du CVR**.

   Sélectionnez les clés que vous souhaitez ajouter. Si les données sont importées, les clés sont prises en compte et les CVIT sont créés.

Définir le filtrage pour l'intégration des résultats des Wiz tests

Définissez les valeurs de filtrage pour importer les données de résultats des tests dans le cloud que vous souhaitez.

Avant de commencer

Rôle requis : sn_vul_wiz.configure_integration

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Wiz** > **Administration** > **Configuration**.
2. Sélectionnez l'onglet **Configuration des résultats des tests** .
3. Renseignez les champs.

   Pour certains champs, vous pouvez spécifier plusieurs valeurs. --Aucun-- est la valeur (par défaut). Si --Aucun-- reste sélectionné pour un champ, aucune donnée n'est importée pour ce champ.

   Remarque : Les configurations d'hôte ne Wiz sont pas importées.

Champ	Description
Gravité	Choisissez-en un pour le filtrage de gravité : ○ FAIBLE ○ MOYEN ○ ÉLEVÉ ○ CRITIQUE ○ AUCUN : renvoie des résultats sans valeur de gravité disponible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Vous préférerez peut-être commencer par ÉLEVÉ ou CRITIQUE pour limiter votre importation aux résultats d'importance critique.
ID de projet	Spécifiez uniquement les résultats de configuration dans le cloud pour les projets, par exemple, nommés « ID de projet ».
Plateforme cloud	Résultats de configuration par plateforme cloud. Vous pouvez spécifier plusieurs valeurs, par exemple, AWS, GitHub, Terraform, OpenAI, GKE, OKE, EKS, AKS.
ID d'abonnement	Spécifiez en saisissant l'ID d'abonnement. Vous pouvez spécifier plusieurs valeurs dans un tableau.
État des ressources	Spécifiez par état : ○ Actif ○ Erreur ○ Inactif
Catégorie de cadre de travail	Saisissez des cadres de travail de sécurité, des sous-catégories de sécurité ou des catégories de sécurité. Vous pouvez spécifier plusieurs valeurs.
Type de ressource	Types d'entité. Vous pouvez spécifier plusieurs valeurs, par exemple, BUCKET,DATABASE
Type natif	Spécifiez les résultats en fonction du type natif de la ressource dans le cloud, par exemple, catégorie.
Dispose de rattrapage	Spécifiez les résultats avec ou sans (FAUX) instructions de rattrapage.
Premier	Pagination. Saisissez une valeur. Vous préférerez peut-être commencer par 1000.
Analysé après	Filtrez les résultats qui ont été analysés en commençant par la date que vous sélectionnez.
Statut	Filtrer par état : ○ OUVRIR ○ RÉSOLU

Traduction automatique

4. **Sélectionnez Enregistrer et tester**.
   Si les informations d'identification ont été enregistrées et validées avec succès, un message s'affiche. Vous pouvez sélectionner le filtrage pour une autre importation d'intégration.

Définir le filtrage pour l'intégration Wiz des problèmes

Définir les valeurs de filtrage sur importer Wiz les problèmes qui identifient les actifs impliqués dans des combinaisons toxiques de vulnérabilités et des erreurs de configuration.

Avant de commencer
Rôle requis : sn_vul_wiz.configure_integration

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Wiz** > **Administration** > **Configuration**.
2. Sélectionnez l'onglet **Configuration des problèmes** .
3. Renseignez les champs.

   Pour certains champs, vous pouvez spécifier plusieurs valeurs. `--Aucun--` est la valeur (par défaut). Si `--Aucun--` reste sélectionné pour un champ, aucune donnée n'est importée pour ce champ.

Champ	Description
Gravité	Filtrer par gravité de résultat. ○ FAIBLE ○ MOYEN ○ ÉLEVÉ ○ CRITIQUE ○ INFORMATIONNEL
ID de projet	Importer uniquement les résultats pour les projets donnés (chaînes).
Type de problème	Problèmes par type de règle par lequel ils sont générés. ○ CLOUD_CONFIGURATION ○ THREAT_DETECTION ○ TOXIC_COMBINATION
ID d'abonnement	Spécifiez les conclusions en saisissant un ID d'abonnement. Vous pouvez spécifier plusieurs valeurs dans un tableau.
Plateforme cloud	Résultats de configuration par plateforme cloud. Vous pouvez spécifier plusieurs valeurs, par exemple, AWS, GitHub, Terraform, OpenAI, GKE, OKE, EKS, AKS.
Catégorie de cadre de travail	Saisissez des cadres de travail de sécurité, des sous-catégories de sécurité ou des catégories de sécurité. Vous pouvez spécifier plusieurs valeurs.
Type natif	Problèmes basés sur le type natif de la ressource cloud, par exemple, `catégorie`.
Premier	Pagination. Saisissez une valeur. Vous préférerez peut-être commencer par 1000.
Statut	Filtrer par état : ○ OUVRIR ○ EN COURS ○ RÉSOLU

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. **Sélectionnez Enregistrer et tester**.
   Si les informations d'identification ont été enregistrées et validées avec succès, un message s'affiche. Vous pouvez sélectionner le filtrage pour une autre importation d'intégration.

Mappage de champs pour les Wiz intégrations de Réponse aux vulnérabilités

Examinez les champs source et cible et affichez les données importées sur des tables et des enregistrements dans votre ServiceNow instance IA Now Platform.

Mappage de champ d'intégration de vulnérabilité de l'hôte

Champ Wiz	ServiceNow Colonne de table	ServiceNow colonne de champ
description	sn_vul_detection	proof
état	sn_vul_detection	source_status
lastDetectedAt	sn_vul_detection	last_found
firstDetectedAt	sn_vul_detection	first_found
vulnerableAsset.name	sn_vul_detection	dns
remédiation	sn_vul_detection	solution_summary
vulnerableAsset.ipAddresses[0]	sn_vul_detection	ip_address
vendorSeverity	sn_vul_detection	source_severity
version fixe	sn_vul_detection	fixed_version
état	sn_vul_detection	is_ignored
état	sn_vul_detection	état
nom	sn_vul_nvd_entry	id
score	sn_vul_nvd_entry	v3_base_score
CVEDescription	sn_vul_nvd_entry	résumé
vendorSeverity	sn_vul_nvd_entry	source_severity
cvssv3.attackVector	sn_vul_nvd_entry	v3_attack_vector
cvssv3.attackComplexity	sn_vul_nvd_entry	v3_attack_complexity
CVSSv3.ImpactConfidentialité	sn_vul_nvd_entry	v3_confidentiality_impact
cvssv3.privilegesRequired	sn_vul_nvd_entry	v3_privileges_required
cvssv3.integrityImpact	sn_vul_nvd_entry	v3_integrity_impact
cvssv3.userInteractionRequired	sn_vul_nvd_entry	v3_user_interaction
hasExploit	sn_vul_nvd_entry	exploit
hasCisaKevExploit	sn_vul_nvd_entry	cisa_exists
vulnerableAsset.tags	sn_sec_cmn_src_ci	host_tag
vulnerableAsset.id	sn_sec_cmn_src_ci	source_id
vulnerableAsset.name	sn_sec_cmn_src_ci	nom
vulnerableAsset.region	sn_sec_cmn_src_ci	cloud_region

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ Wiz	ServiceNow Colonne de table	ServiceNow colonne de champ
vulnerableAsset.providerUniqueId	sn_sec_cmn_src_ci	resource_id
vulnerableAsset.cloudPlatform	sn_sec_cmn_src_ci	cloud_service_provider
vulnerableAsset.type	sn_sec_cmn_src_ci	assetType
relatedIssueAnalytics	sn_sec_cmn_src_ci	source_data
vulnerableAsset.nativeType	sn_sec_cmn_src_ci	cloud_resource_type
vulnerableAsset.subscriptionExternalId	sn_sec_cmn_src_ci	cloud_account
vulnerableAsset.name	sn_sec_cmn_src_ci	resource_name
vulnerableAsset.imageName	sn_sec_cmn_src_ci	image_id
Actifvulnérable.*	sn_sec_cmn_src_ci	source_data
lastDetectedAt	sn_sec_cmn_src_ci	source_data

Mappage de champ d’intégration de vulnérabilité du conteneur

Champ Wiz	ServiceNow Colonne de table	ServiceNow colonne de champ
imageId	sn_vul_container_image	image_id
vulnerableAsset.name	sn_vul_container_image	image_name
vulnerableAsset.repository.externalId après ##	sn_vul_container_image	registre
vulnerableAsset.repository.externalId avant ##	sn_vul_container_image	réf.
vulnerableAsset.tags	sn_vul_container_image	image_labels
projets	sn_vul_container_image	image_projects
vulnerableAsset.region	sn_vul_container_image	cloud_regions
vulnerableAsset.cloudPlatform	sn_vul_container_image	cloud_providers
vulnerableAsset.subscriptionExternalId	sn_vul_container_image	cloud_account_ids
vulnerableAsset.executionControllers.ancestors.name	sn_vul_container_image	image_namespace
vulnerableAsset.executionControllers.ancestors.name	sn_vul_container_image	image_clusters
vulnerableAsset.executionControllers.ancestors.name	sn_vul_container_image_vulnerable_image	image_clusters
vulnerableAsset.executionControllers.ancestors.name	sn_vul_container_image_vulnerable_image	image_namespace
vulnerableAsset.repository.externalId avant ##	sn_vul_container_image_vulnerable_image	image_repository
layerMetadata.isBaseLayer	sn_vul_container_image_findings	is_base_image
firstDetectedAt	sn_vul_container_image_findings	first_found
lastDetectedAt	sn_vul_container_image_findings	last_found
nom detailedName	sn_vul_container_image_package	nom
version	sn_vul_container_image_package	version
Chemin d’accès de l’emplacement	sn_vul_container_image_package	chemin d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ Wiz	ServiceNow Colonne de table	ServiceNow colonne de champ
nom	sn_vul_nvd_entry	id
score	sn_vul_nvd_entry	v3_base_score
CVEDescription	sn_vul_nvd_entry	résumé
VendorSeverity	sn_vul_nvd_entry	source_severity
cvssv3.attackVector	sn_vul_nvd_entry	v3_attack_vector
cvssv3.attackComplexity	sn_vul_nvd_entry	v3_attack_complexity
CVSSv3.ImpactConfidentialité	sn_vul_nvd_entry	v3_confidentiality_impact
cvssv3.privilegesRequired	sn_vul_nvd_entry	v3_privileges_required
cvssv3.integrityImpact	sn_vul_nvd_entry	v3_integrity_impact
cvssv3.userInteractionRequired	sn_vul_nvd_entry	v3_user_interaction
hasExploit	sn_vul_nvd_entry	hasExploit
layerMetadata.isBaseLayer	sn_vul_container_image_layer	Couche de base
layerMetadata.details	sn_vul_container_image_layer	instruction
layerMetadata.id	sn_vul_container_image_layer	id
état	sn_vul_container_image_findings	is_ignored
validate_at_runtime	sn_vul_container_image_findings	validate_at_runtime
id	sn_vul_container_image_findings	unique_key

Conformité de la configuration Mappage de champs d'intégration des résultats des tests

Champ Wiz	ServiceNow Colonne de table	ServiceNow colonne de champ
rule.id	sn_vulc_test	source_id
rule.name	sn_vulc_test	short_description
rule.remediationInstructions	sn_vulc_test	remédiation
règle.description	sn_vulc_test	description
severity	sn_vulc_test	source_criticality
état	sn_vulc_result	résultat
id	sn_vulc_result	source_id
analyzedAt	sn_vulc_result	last_seen
firstSeenAt	sn_vulc_result	first_seen
rule.remediationInstructions	sn_vulc_result	remédiation
resource.nativeType	sn_sec_cmn_src_ci	source_data
Type.ressource	sn_sec_cmn_src_ci	source_data
id	sn_vulc_result	description
id	sn_vulc_result	source_id

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ Wiz	ServiceNow Colonne de table	ServiceNow colonne de champ
securitySubCategories.category.framework.id	sn_vulc_auth_src	source_id
securitySubCategories.category.framework.name	sn_vulc_auth_src	short_description
securitySubCategories.category.framework.description	sn_vulc_auth_src	description
securitySubCategories.id	sn_vulc_citation	section
securitySubCategories.title	sn_vulc_citation	section_name
Ressource.Projets	sn_sec_cmn_src_ci	projets
état	sn_vulc_result	is_ignored

Mappage de champs d'intégration des problèmes

Remarque : Les données mappées pour l'intégration des problèmes aux résultats des tests dans le cloud (CTR) sont étiquetées avec Problèmes Wiz comme source pour vous aider à différencier ces CTR des CTR de l'intégration des résultats des tests.

Champ Wiz	ServiceNow Colonne de table	ServiceNow colonne de champ
sourceRule.id	sn_vulc_test	source_id
sourceRule.name	sn_vulc_test	short_description
sourceRule.resolutionRecommendation sourceRule.remediationInstructions	sn_vulc_test	remédiation
sourceRule.description	sn_vulc_test	description
severity	sn_vulc_test	source_criticality
createdAt	sn_vulc_result	first_seen
updatedAt	sn_vulc_result	last_seen
état	sn_vulc_result	résultat
id	sn_vulc_result	source_id
sourceRule.resolutionRecommendation sourceRule.remediationInstructions	sn_vulc_result	remédiation
sourceRule.controlDescription	sn_vulc_result	description
entitySnapshot.nativeType	sn_sec_cmn_src_ci	source_data
entitéInstantané.type	sn_sec_cmn_src_ci	source_data
Problème Wiz'	sn_vulc_result	result_type
id	sn_vulc_result	description
severity	sn_vulc_test	source_criticality
id	sn_vulc_result	source_id
sourcerule.securitySubCategories.category.framework.id	sn_vulc_auth_src	source_id
sourcerule.securitySubCategories.category.framework.name	sn_vulc_auth_src	short_description
sourcerule.securitySubCategories.category.framework.description	sn_vulc_auth_src	description
sourcerule.securitySubCategories.id	sn_vulc_citation	section

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ Wiz	ServiceNow Colonne de table	ServiceNow colonne de champ
sourcerule.securitySubCategories.title	sn_vulc_citation	section_name
projets	sn_sec_cmn_src_ci	projets
état	sn_vulc_result	is_ignored

Mappage sur l'élément vulnérable et les enregistrements de résultats des tests

- Les résultats de vulnérabilité de l'hôte sont mappés aux éléments vulnérables de l'hôte (VIT).
- Les résultats de vulnérabilité de conteneurs sont mappés aux éléments vulnérables de conteneurs (CVIT).
- Les résultats des tests de configuration sont mappés aux enregistrements de résultats des tests dans le cloud (CTR) dans l'application Conformité de la configuration .
- Les résultats des problèmes sont mappés aux enregistrements de résultats des tests (CTR) dans le cloud dans l'application Conformité de la configuration .

Créer manuellement une intégration de vulnérabilité

Les intégrations de vulnérabilité offrent aux clients et aux fournisseurs la possibilité d'enrichir les données de vulnérabilité sur leur instance en récupérant les données de systèmes et de fournisseurs externes. Cette capacité peut simplifier le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Pour obtenir des instructions détaillées sur la création d'intégrations, reportez-vous à la section Définir une nouvelle intégration de vulnérabilité.

Définir une nouvelle intégration de vulnérabilité

Une intégration de vulnérabilité extrait les données de rapport d'un système tiers, généralement pour récupérer les données de vulnérabilité, et traite ces données de rapport à l'aide de sources de données ou d'un processeur personnalisé.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Administration** > **Intégrations**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs nécessaires.

Intégration de vulnérabilité

Champ	Description
Nom	Un nom descriptif pour l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Indique si l'intégration est active. Si vous ne souhaitez pas qu'il s'exécute pendant une période spécifique, vous pouvez configurer les paramètres que vous souhaitez utiliser et désactiver la tâche.
Exécuter	Fréquence à laquelle vous souhaitez que l'intégration s'exécute : Quotidien, Hebdomadaire, Périodiquement, etc. Comme indiqué, les champs suivants sont affichés ou non en fonction de votre paramètre dans ce champ.
Jour	Le jour où vous souhaitez que l'intégration s'exécute. ○ Si vous avez sélectionné **Hebdomadaire** dans le champ **Exécuter** , ce champ affiche les jours de la semaine. ○ Si vous avez sélectionné **Tous les mois** dans le champ **Exécuter** , ce champ affiche les jours du mois.
Heure	Heure à laquelle vous souhaitez que l'intégration commence. Ce champ s'affiche uniquement si vous avez sélectionné **Quotidien**, **Hebdomadaire** ou Mensuel dans le champ **Exécuter**.
Application	[Lecture seule] Le nom de l'application pour laquelle cette intégration a été créée.
Intervalle de répétition	Si vous avez sélectionné **Périodiquement** dans le champ **Exécuter** , ce champ affiche le nombre de jours et d'heures avant que l'intégration ne s'exécute à nouveau.
En cours de démarrage	Si vous avez sélectionné **Périodique** dans le champ **Exécuter** , ce champ affiche les dates et l'heure à utiliser comme point de départ pour les mises à jour périodiques.
Conditionnel	Sélectionnez ce champ si vous souhaitez ajouter des paramètres conditionnels.
Condition	Si vous avez coché la case **Conditionnel** , entrez les conditions ici.
Détails de l'intégration	
Script d'intégration	Sélectionnez l'include de script qui étend VulnerabilityIntegrationBase à exécuter lorsque l'intégration s'exécute. Ce script définit comment récupérer les données à partir d'un système tiers.
Script de l'instanciateur d'intégration	Entrez un script qui définit le mode de construction de l'include de script sélectionné pour le **script d'intégration**. Pour plus d'informations, consultez Champs de script de l'instanciateur d'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Les scripts nécessitent à la fois ServiceNow une expertise et Réponse aux vulnérabilités une expertise.
Stratégie de processeur de rapport	Sélectionnez la stratégie que vous souhaitez utiliser pour gérer les données renvoyées par le script d'intégration lors de l'exécution de l'intégration. ○ Sélectionnez **Pièce jointe de source de données** si vous souhaitez traiter les données à l'aide d'une source de données. ○ Sélectionnez **Processeur de rapport personnalisé** pour sélectionner un processeur personnalisé.
Script de processeur de rapport	Si vous avez sélectionné **Processeur de rapport personnalisé** dans le champ **Stratégie de processeur de rapport** , sélectionnez l'include de script qui étend l'include de script VulnerabilityReportProcessorBase à exécuter lorsque l'intégration s'exécute. Ce script définit la manière de traiter les données renvoyées par le script d'intégration.
Script de l'instanciateur de processeur	Entrez un script qui définit le mode de construction de l'include de script sélectionné pour le **processeur de rapports**.

4. Cliquez sur **Envoyer**.

Information associée

Script d'intégration de vulnérabilité

Stratégies de processeur de rapport

Champs de script de l'instanciateur d'intégration

Exécuter manuellement une intégration de vulnérabilité

Script d'intégration de vulnérabilité

Sur le formulaire d'intégration de vulnérabilité, le script d'intégration fait référence à un include de script qui étend l'include de script VulnerabilityIntegrationBase.

La fonctionnalité contenue dans ce script est appelée par le VulnerabilityIntegrationController pour gérer les moyens par lesquels les données sont récupérées à partir d'une source de données externe. Chaque sous-classe de VulnerabilityIntegrationBase a accès à des informations contextuelles sur le processus d'appel. Ces informations sont disponibles via les variables membres suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- integrationGr : GlideRecord de l'enregistrement d'intégration de vulnérabilité qui a demandé l'exécution de l'intégration.
- integrationProcessGr : un GlideRecord qui fournit des informations contextuelles sur le processus actuel d'une intégration.

Le processus de vulnérabilité contient des paramètres spéciaux à utiliser au sein d'une intégration, généralement à des fins de pagination. Chaque exécution d'une intégration de vulnérabilité (appelée exécution d'intégration de vulnérabilité) a au moins un processus d'intégration de vulnérabilité associé. Pour les intégrations multi-appels, il existe un ou plusieurs enregistrements de processus d'intégration de vulnérabilité pour chaque exécution de l'intégration de vulnérabilité.

L'include de script doit fournir une implémentation pour la méthode `retrieveData()` et renvoyer un objet traité par le script de processeur de rapports. L'objet renvoyé par retrieveData est un objet simple avec des propriétés pour content, contentType et extension.

Voici une capture d'écran de VulnerabilityIntegrationBase.retrieveData() :

VulnérabilitéIntegrationBase.retrieveData()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

La logique dans `retrieveData()` dépend de l'interface requise pour récupérer les données. Par exemple, si la source des données extraites a une API REST, le corps de cette méthode pourrait appeler le point de terminaison REST, probablement via RESTMessageV2. La réponse de l'appel peut ensuite être analysée ou placée dans une pièce jointe, et les détails peuvent être utilisés pour construire l'objet de retour.

Intégrations d'appels uniques

Les scripts d'intégration d'appel unique (page unique) sont les types d'intégration les plus simples. Ils nécessitent un appel, souvent vers une source externe de données, pour récupérer les données. Seul retrieveData() doit être implémenté pour les intégrations à page unique/appel unique.

Voici un exemple qui illustre un script d'intégration d'appel unique simple. Il crée un RESTMessageV2 et l'exécute. Il renvoie ensuite un objet en utilisant le corps de la réponse comme contenu, ainsi qu'un contentType et une extension supposés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Script d'intégration d'appel unique

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```

Intégrations d'appels multiples

Les scripts d'intégration à appels multiples (ou à plusieurs pages) sont un peu plus compliqués. Elles nécessitent plusieurs appels à une source de données pour récupérer les données.

Comme une intégration d'appel unique, une intégration d'appel multiple doit également avoir retrieveData() implémenté. Dans le corps de retrieveData(), l'intégration utilise les méthodes hasMoreData() et setNextRunParameters() fournies par VulnerabilityIntegrationBase.

La méthode hasMoreData() accepte un seul booléen qui demande au VulnerabilityIntegrationController d'insérer plus de processus pour extraire plus de données. Lors de la transmission de true à hasMoreData(), un appel à setNextRunParameters() est effectué pour fournir un contexte au processus suivant.

La méthode setNextRunParameters() accepte un seul objet qui fournit des informations de contexte à utiliser par le prochain appel à retrieveData(). Cet objet est utilisé pour passer l'état aux appels ultérieurs pour retrieveData(). Un exemple de cas d'utilisation consiste à transmettre un objet qui indique le numéro de page et la taille de page actuels à un service Web.

Pour les intégrations d'appels multiples, chaque appel retrieveData() vérifie d'abord les paramètres de processus actuels. La méthode _getProcessParameters() est fournie à tous les VulnerabilityIntegrationBase pour faciliter l'obtention des paramètres définis par le processus précédent. S'il n'y a pas de paramètres, cela indique qu'il s'agit du premier processus.

Voici une capture d'écran d'un exemple de script d'intégration d'appels multiples. Dans le prolongement de l'exemple d'intégration d'appel unique, ce script montre comment effectuer des appels vers un point de terminaison REST qui prend en charge la pagination de base. Il montre comment obtenir une seule page de données, reconnaître qu'il y a plus de données à récupérer, puis indiquer au processus suivant quelle page récupérer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Script d'intégration d'appels multiples

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

Les pièces jointes en tant que valeurs de retour retrieveData()

Parfois, il est préférable de renvoyer une pièce jointe à partir de retrieveData(). La logique de création et/ou de récupération d'une pièce jointe est spécifique à l'implémentation, mais une fois que la pièce jointe est connue, ses informations peuvent être renvoyées.

Pour fournir une pièce jointe, retrieveData() renvoie un objet comme :

```
{
    contents: "attachment-sys-id",
    contentType: "sys_attachment"
}
```

Voici un exemple qui prolonge l'exemple précédent, mais enregistre le corps de la réponse du message REST dans l'enregistrement du processus d'intégration. Il renvoie ensuite cet identificateur de pièce jointe comme contenu de l'objet de retour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renvoyer la pièce jointe à partir de retrieveData

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Stratégies de processeur de rapport

Le champ **Stratégie de processeur de rapport** du formulaire Intégration de vulnérabilité est utilisé pour sélectionner la méthode de traitement des données retournées par le script d'intégration de vulnérabilité lors de l'exécution du processus d'intégration de vulnérabilité.

La valeur par défaut est **Pièce jointe de source de données**. Cette méthode est l'implémentation de base de référence qui prend les données récupérées et les transmet à une source de données à importer dans le système. La sélection du **processeur de rapport personnalisé** vous permet de sélectionner un script de processeur personnalisé pour le traitement des données.

Utiliser la stratégie de processeur de rapport de pièce jointe de source de données

La stratégie de processeur de rapport de pièce jointe de source de données est utilisée pour transmettre les données récupérées par le script d'intégration aux sources de données configurées.

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Administration** > **Intégrations** et créer une intégration.
2. Dans le champ **Stratégie de processeur de rapport** , sélectionnez **Pièce jointe de source de données**.
3. Cliquez avec le bouton droit dans l'en-tête du formulaire, puis cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la liste connexe **Sources de données d'intégration de vulnérabilité** , cliquez sur **Nouveau**.
5. Définissez la source de données à utiliser.
6. Cliquez sur **Envoyer**.
7. Répétez les étapes 4 à 6 si vous avez besoin de sources de données supplémentaires.
   Assurez-vous de spécifier l'ordre dans lequel les sources de données multiples envoient les informations dans le champ **Commande** .
8. Cliquez sur **Mettre à jour**.

À propos des scripts de processeur de rapport personnalisé

Sur le formulaire d'intégration de vulnérabilité, le processeur de rapport est une référence à un include de script qui étend l'include de script VulnerabilityReportProcessorBase. La fonctionnalité contenue dans ce script est appelée par le VulnerabilityIntegrationController et définit le moyen par lequel les données renvoyées par le script d'intégration sont traitées.

Chaque sous-classe de VulnerabilityReportProcessorBase a accès à des informations contextuelles sur le processus d'appel. Ces informations sont disponibles via les variables membres suivantes :

- integrationGr : un GlideRecord de l'enregistrement d'intégration de vulnérabilité qui a demandé l'exécution de l'intégration.
- integrationProcessGr : GlideRecord du processus de vulnérabilité qui fournit des informations contextuelles sur le processus actuel d'une intégration.

Le script include doit fournir une implémentation pour la méthode `processReport( )`. L'objet passé à processReport() est l'objet renvoyé par retrieveData et, en tant que tel, est un objet simple avec des propriétés pour content, contentType et extension. La logique réelle dans processReport() est spécifique à l'implémentation et dépend des données de rapport fournies.

Voici une capture d'écran de VulnerabilityReportProcessorBase.processReport() :

Script de processeur de rapport personnalisé

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

Champs de script de l'instanciateur d'intégration

Le formulaire d'intégration de vulnérabilité contient le script de l'instanciateur d'intégration et, lorsque la stratégie de processeur de rapports **du processeur** de rapports personnalisé est sélectionnée, le script de l'instanciateur de processeurs. Ces champs sont utilisés pour fournir la logique permettant d'instancier réellement l'objet défini par les champs de référence de l'include de script, le script d'intégration et le processeur de rapport, respectivement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque l'include de script est sélectionné, les deux champs sont pré-remplis avec un appel de constructeur sans argument. Souvent, c'est suffisant, mais il peut arriver que plus de logique soit nécessaire pour instancier l'objet script.

L'enregistrement integrationProcessGr est exposé aux champs de script de l'instanciateur afin que les informations spécifiques au processus puissent être utilisées, selon les besoins.

Exécuter manuellement une intégration de vulnérabilité

Intégrations de vulnérabilité pour et Réponse aux vulnérabilités des applications sont configurées pour Réponse aux vulnérabilités s'exécuter de manière planifiée. Toutefois, vous pouvez les exécuter manuellement si nécessaire.

Avant de commencer
Rôles requis :

- sn_vul.read_integrations (Réponse aux vulnérabilités)
- sn_vul.app_read_integrations(Réponse aux vulnérabilités des applications)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche
Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations**.
2. Ouvrez l'enregistrement de l'intégration que vous souhaitez exécuter.
3. Cliquez sur **Exécuter maintenant**.

Ingestion manuelle des vulnérabilités

Ingérer manuellement les vulnérabilités dans l'application afin de pouvoir les corriger rapidement sans avoir à attendre les résultats de l'analyse Réponse aux vulnérabilités .

Les analyseurs tiers, tels que ceux qui Rapid7 permettent d'importer des données de vulnérabilité et Réponse aux vulnérabilités de traiter les données pour signaler les résultats. Avec l'intégration de l'ingestion manuelle, vous pouvez ingérer de manière proactive les vulnérabilités et les corriger au lieu d'attendre que les analyseurs signalent les actifs à risque. L'ingestion manuelle des vulnérabilités protège efficacement les actifs contre les menaces inconnues telles que les exploits zero-day.

Ingestion manuelle des vulnérabilités

Vous pouvez importer les données de vulnérabilité en chargeant un modèle dans les formats de fichier suivants :

- Excel
- Valeur séparée par des virgules (CSV)

Pour accéder au modèle et le télécharger, accédez à **Tous** > **Réponse aux vulnérabilités** > **Ingestion manuelle d'éléments de vulnérabilité** > **Interface utilisateur, charger le fichier**.

Assurez-vous de suivre ces points clés lors du remplissage des enregistrements dans le modèle :

- N'effectuez aucune erreur de saisie dans les enregistrements de la colonne Gravité/État. En cas d'erreur de frappe, l'enregistrement est ignoré.
- Ne modifiez pas les noms de colonnes.
- Ne placez pas de noms de colonnes dans les lignes, à l'exception de la première ligne.
- Ne modifiez pas l'ordre des feuilles dans le Microsoft Excel modèle. Les données de vulnérabilités doivent toujours être présentes dans la deuxième feuille.
- Ne placez les détails des vulnérabilités dans aucune feuille, à l'exception de la feuille Détecter manuellement l'entrée.
- N'utilisez aucun caractère à l'exception des caractères alphanumériques et spéciaux tels que le tiret (-), le point (.), le point (+), le trait de soulignement (_), l'espace, les crochets '(' ')' et le symbole arobase (@) pour le nom de fichier.

Pour obtenir des instructions sur la façon de remplir les données dans le modèle, reportez-vous à la section Modèle d'ingestion manuelle des vulnérabilités.

À partir de la version 24.0.6 de Réponse aux vulnérabilités, vous pouvez également créer des colonnes supplémentaires dans le Microsoft Excel modèle. Pour plus d'informations, consultez KB1646630 .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de l'ingestion manuelle

L'intégration est déclenchée lorsqu'un fichier est téléchargé. En fonction du type de fichier téléchargé, l'intégration connexe est déclenchée.

Pour afficher les intégrations, accédez à **Tous** > **Réponse aux vulnérabilités** > **Ingestion manuelle d'éléments de vulnérabilité** > **Intégrations**.

Les intégrations d'ingestion manuelle du système de base suivantes sont disponibles par défaut.

Intégrations

Type d'intégration	Description
Intégration Excel de l'ingestion manuelle	Récupère les données en récupérant le dernier Microsoft Excel fichier chargé à partir de la table File d'attente push d'ingestion de vulnérabilité et copie la pièce jointe dans l'exécution d'intégration respective.
Intégration CSV de l'ingestion manuelle	Récupère les données en récupérant le dernier fichier CSV chargé à partir de la table File d'attente push d'ingestion de vulnérabilité et copie la pièce jointe dans l'exécution d'intégration respective.

L'intégration tierce d'ingestion manuelle crée une instance d'intégration par défaut, avec les deux paramètres d'instance d'intégration suivants :

- max_input_records : définit le nombre d'enregistrements qui peuvent être créés dans le modèle. Si vous ajoutez plus d'enregistrements que ce qui est spécifié dans ce paramètre, les enregistrements supplémentaires sont ignorés. Le nombre d'enregistrements peut être mis à jour dans la colonne Valeur. Le nombre recommandé de créations d'enregistrements dans le modèle est de 1 000. Tout ce qui est supérieur à cette valeur peut poser des problèmes de performance.
- insert_fixed : importe les détections de vulnérabilité corrigées.

Pour afficher les paramètres d'instance d'intégration, accédez à **Tous** > **Réponse aux vulnérabilités** > **Ingestion manuelle d'éléments de vulnérabilité** > **Intégrations** et cliquez sur l'instance source d'une intégration. Vous pouvez également accéder à **Tous** > **Réponse aux vulnérabilités** > **Instances d'intégration** et cliquez sur **Ingestion manuelle**.

Ingérer manuellement les vulnérabilités

Ingérer manuellement les vulnérabilités en chargeant un modèle avec des données de vulnérabilité.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Interface utilisateur, charger le fichier**.
2. Cliquez sur les liens Excel ou CSV et téléchargez le modèle dans le format respectif.
3. Dans le modèle, saisissez les données de vulnérabilité dans les enregistrements.
   Pour obtenir des instructions sur la façon de remplir les données dans le modèle, reportez-vous à la section Modèle d'ingestion manuelle des vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Importer le fichier** et chargez le modèle mis à jour.
5. Cliquez sur **Envoyer**.
   La page Files d'attente push d'intégration de vulnérabilité s'affiche. Vous pouvez afficher la liste des instances d'intégration, l'état des exécutions de l'intégration et les notes du journal une fois l'exécution de l'intégration terminée.

Que faire ensuite

Après avoir téléchargé le fichier, accédez à **Tous** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Intégrations**. Vérifiez que l'exécution de l'intégration a réussi.

Vérifier l'exécution manuelle de l'intégration

Vérifiez que l'exécution de l'intégration a réussi. Affichez le nombre de détections individuelles et les éléments vulnérables (VI) créés ou mis à jour en raison de l'exécution de l'intégration.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Intégrations**.
2. Cliquez sur le nom de l'intégration en fonction du type de fichier téléchargé.
3. Cliquez sur l'onglet **Exécutions d'intégration de vulnérabilité** .
4. Cliquez sur le numéro d'exécution de l'intégration.
5. Cliquez sur l'onglet **Éléments** .
6. Passez en revue les informations de l'onglet **Éléments** .

Onglet Éléments

Onglet/champ	Description
Onglet Éléments	Affiche le nombre total de VI importés. Vous pouvez voir le nombre total de détections importées en ajoutant les nombres répertoriés sous l'onglet Détections.
Nouveaux éléments	Affiche le nombre d'éléments vulnérables créés à partir de l'exécution de cette intégration.
Éléments importés	Affiche la somme de tous les champs dans cette section.
Éléments en double	Affiche les éléments en double. Ce champ n'est plus renseigné.
Éléments mis à jour	Affiche le nombre de fois où les éléments vulnérables sont mis à jour au cours de l'exécution de cette intégration. Cette valeur n'est pas le nombre d'éléments vulnérables uniques qui sont mis à jour. Si, par exemple, un élément vulnérable est mis à jour deux fois pendant l'exécution de l'intégration, il est compté deux fois et affiché sous la forme de 2 éléments mis à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet/champ	Description
Éléments inchangés	Affiche les éléments vulnérables trouvés pendant l'exécution de l'intégration qui existent dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Que faire ensuite

Après avoir vérifié que l'exécution de l'intégration réussit, accédez à **Tous** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Historique des fichiers chargés**. Vérifiez s'il existe des enregistrements ayant échoué dans les notes.

Configurer les détections manuelles de fermeture automatique

Activez les détections manuelles à fermeture automatique pour fermer automatiquement les détections manuelles périmées.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Interface utilisateur, charger le fichier**.
2. Cliquez sur **Modifier la configuration de fermeture automatique**.
3. Cliquez sur l'onglet **Détections manuelles** .
4. Assurez-vous que la case **Fermer automatiquement les détections manuelles** est cochée.
5. Dans le champ **Dernières détections manuelles trouvées (en jours),** entrez le nombre de jours après lesquels les détections manuelles doivent être fermées.
   La valeur par défaut est de 90 jours. Vous pouvez saisir n'importe quelle valeur positive pour le nombre de jours.

Vérifier l'état du chargement

Vérifiez si l'exécution de l'intégration de vulnérabilité a réussi, partiellement réussi ou échoué.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Ingestion d'élément vulnérable manuelle** > **Historique des fichiers chargés**.
2. Dans la table Files d'attente push de l'intégration de vulnérabilité, vérifiez l'heure du chargement et l'état du chargement dans les colonnes Créé et État respectivement.
3. **Facultatif :** Dans le champ **Notes** , affichez le motif de l'échec.

Modèle d'ingestion manuelle des vulnérabilités

Le modèle fournit des colonnes qui doivent être remplies avec des données de vulnérabilité et d'éléments de configuration (CI). Une fois le modèle renseigné et chargé, les données sont traitées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Instructions pour remplir le modèle

Pour entrer les détails dans le modèle, suivez les instructions fournies dans la table suivante.

Instructions relatives au modèle

Colonne	Obligatoire/ Facultatif ?	Longueur de la chaîne (max)/ Valeurs valides	Description
ID de l'actif	Facultatif	255	Identificateur unique universel (UUID) ou ID d'actif. Il peut s'agir de la valeur générée par un scanner.
Entrez des informations dans au moins une des cinq colonnes suivantes :			
Adresse MAC	Obligatoire	24	Informations sur l'hôte ou la ressource. La combinaison de toutes les valeurs fournies doit être unique pour un actif.
FQDN	Obligatoire	255	
NETBIOS	Obligatoire	255	
Adresse IP	Obligatoire	255	
Nom d'hôte	Obligatoire	255	
Les colonnes restantes ne dépendent pas les unes des autres.			
ID de la vulnérabilité	Obligatoire	255	Représente une vulnérabilité dans la base de données de vulnérabilité nationale (NVD) ou un ID renvoyé par un scanner tiers.
Résumé de la vulnérabilité	Facultatif	512	Brève description de la vulnérabilité. Il est ajouté à la base de données uniquement lorsque l'ID de vulnérabilité n'est pas disponible.
Gravité	Facultatif	Critique, Élevé, Moyen, Faible, Aucun	Gravité de la vulnérabilité. Il est ajouté à la base de données uniquement lorsque l'ID de vulnérabilité n'est pas disponible. Si l'enregistrement est vide, il est considéré comme critique par défaut.
Port	Facultatif	Non applicable	Port à partir duquel la vulnérabilité est détectée. La valeur doit être un nombre entier valide. Si une entrée n'est pas valide, l'enregistrement est ignoré.
Protocole	Facultatif	40	Type de protocole réseau utilisé.
Preuve	Facultatif	4 000	Représente l'emplacement ou le chemin système de la vulnérabilité.
État	Facultatif	Ouvert, Fixe	État de la détection. Si l'enregistrement est vide, il est considéré comme ouvert par défaut.

Traduction automatique

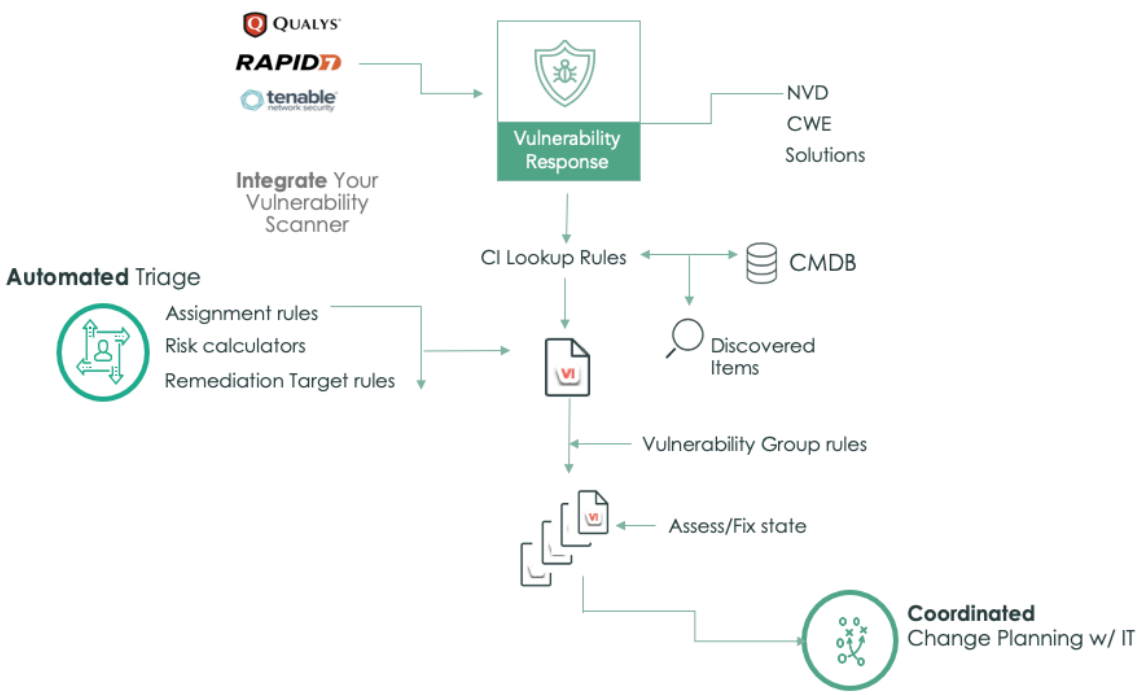
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités Vue d'ensemble du rattrapage

Réponse aux vulnérabilités La correction est un processus par étapes qui consiste à vérifier l'achèvement de l'importation, à trier les nouvelles vulnérabilités et à surveiller la progression jusqu'à l'achèvement. Abordé de cette manière, le rattrapage devient gérable, rapide et, à bien des égards, automatisé.

Comprendre votre posture de sécurité sur les actifs de l'entreprise vous aide à identifier les vulnérabilités les plus critiques pour le rattrapage. Ce processus de rattrapage requiert cela Réponse aux vulnérabilités et une intégration tierce comme le Qualys Vulnerability Integration sont installés et configurés.

Flux de processus d'intégration de Vulnerability Response



Vérifier la réussite des importations d'intégration tierce

La première phase de ce processus consiste à s'assurer que tout fonctionne correctement. Réponse aux vulnérabilités est prédéfini pour télécharger les vulnérabilités de la base de données de vulnérabilité nationale (NVD) et de la faiblesse CWE (Common Enumeration Weakness). Les importations tierces vous fournissent les données dont vous avez besoin pour créer des éléments vulnérables et des tâches de correction. La réussite du rattrapage dépend de l'importation cohérente et réussie des vulnérabilités et des éléments vulnérables.

Pendant l'importation, les règles de recherche de CI font correspondre les actifs tiers aux actifs dans le Base de données de gestion des configurations (CMDB). Tous les actifs sont stockés dans le module Éléments détectés. Les informations sur les CI sont essentielles à l'implémentation de la solution.

Remarque : Une fois qu'une intégration tierce a été installée et configurée, il existe quelques cas où une importation peut échouer, par exemple, si le fournisseur tiers limite ses appels d'API. Lorsque les importations échouent, elles nécessitent une attention immédiate.

Les rapports d'exécution de l'état d'intégration pour les intégrations tierces prises en charge sont fournis avec les applications pour vous donner une vue d'ensemble graphique de vos importations. Utilisez ce rapport, ou créez le vôtre, pour déterminer facilement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

si votre dernière importation a réussi. Pour en savoir plus sur les intégrations prises en charge, reportez-vous à la section Intégrations de Réponse aux vulnérabilités.

Examiner et trier les vulnérabilités et les éléments vulnérables

La phase suivante du rattrapage nécessite l'examen des nouvelles vulnérabilités et des éléments vulnérables. Un élément vulnérable (VI) est une combinaison détectée de vulnérabilité et d'élément de configuration (CI). Au fur et à mesure que les éléments vulnérables sont formés, diverses règles sont exécutées pour affecter des VI, déterminer le risque qu'ils posent et définir des cibles de rattrapage. Ajustez toutes les règles, au besoin, pour vous assurer que les éléments vulnérables ont été triés avec succès.

Surveiller la progression du rattrapage des vulnérabilités existantes

La dernière phase du rattrapage consiste à suivre votre progression.

- Examinez l'état des importations pour les implémentations de correctifs qui ne se sont pas présentées et effectuez un suivi auprès des opérations IT.
- Suivre l'évolution des obligations de conformité réglementaire et s'assurer de leur réalisation.
- Examiner l'état de l'élément différé et réviser ou implémenter des correctifs.
- Surveillez les tableaux de bord de gestion de la vulnérabilité. Pour examiner les tendances, afficher les rapports en temps réel et utiliser des mesures qui suivent vos taux de réalisation des objectifs de rattrapage, vous préférez peut-être surveiller vos processus avec l'application Analyse des performancespour Vulnerability Response .
- Fermeture des détections obsolètes dans Réponse aux vulnérabilités.

Vérifier la réussite des importations d'intégration Réponse aux vulnérabilités

Pour déterminer si vos importations ont réussi, la façon la plus simple consiste à utiliser un tableau de bord État de l'exécution de l'intégration. Le tableau de bord État de l'exécution de l'intégration fournit un exemple de vue graphique de l'état des exécutions d'intégration tierce.

Les Qualys intégrations de vulnérabilité et Rapid7 disposent d'un tableau de bord de l'état d'exécution de l'intégration. Voir Qualys Graphique de l'état d'exécution de l'intégration ou Intégration des vulnérabilités Rapid7 Graphique d'état d'exécution pour des informations détaillées sur le contenu du graphique.

Remarque : Les graphiques, pour les intégrations non fournies par ServiceNow®, peuvent être créés à partir des rapports d'un tableau de bord, mais peuvent nécessiter ServiceNow une expertise. Pour plus d'informations sur la création de rapports et de tableaux de bord, voir Introduction aux rapports et aux tableaux de bord .

Afficher les Réponse aux vulnérabilités données de détection des éléments vulnérables

Les données complètes recueillies par vos intégrations de scanners Réponse aux vulnérabilités tiers sont affichées dans les onglets Détections et Détections initiales des enregistrements d'éléments vulnérables (VIT). Il s'affiche également sur les enregistrements de détection de la liste de détection des éléments vulnérables de votre ServiceNow AI Platform® instance.

Avant de commencer

Les intégrations tierces récupèrent les données de détection des éléments vulnérables. Les détections sont des occurrences distinctes de vulnérabilités telles que signalées par les scanners. Les données de détection sont associées aux éléments vulnérables et l'état du VI est mis à jour en fonction de l'état des détections. Si aucun VI n'est trouvé, un nouveau

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

VI est créé. Les détections ne sont ouvertes ou fermées que par les données trouvées directement par un scanner.

Rôle requis :

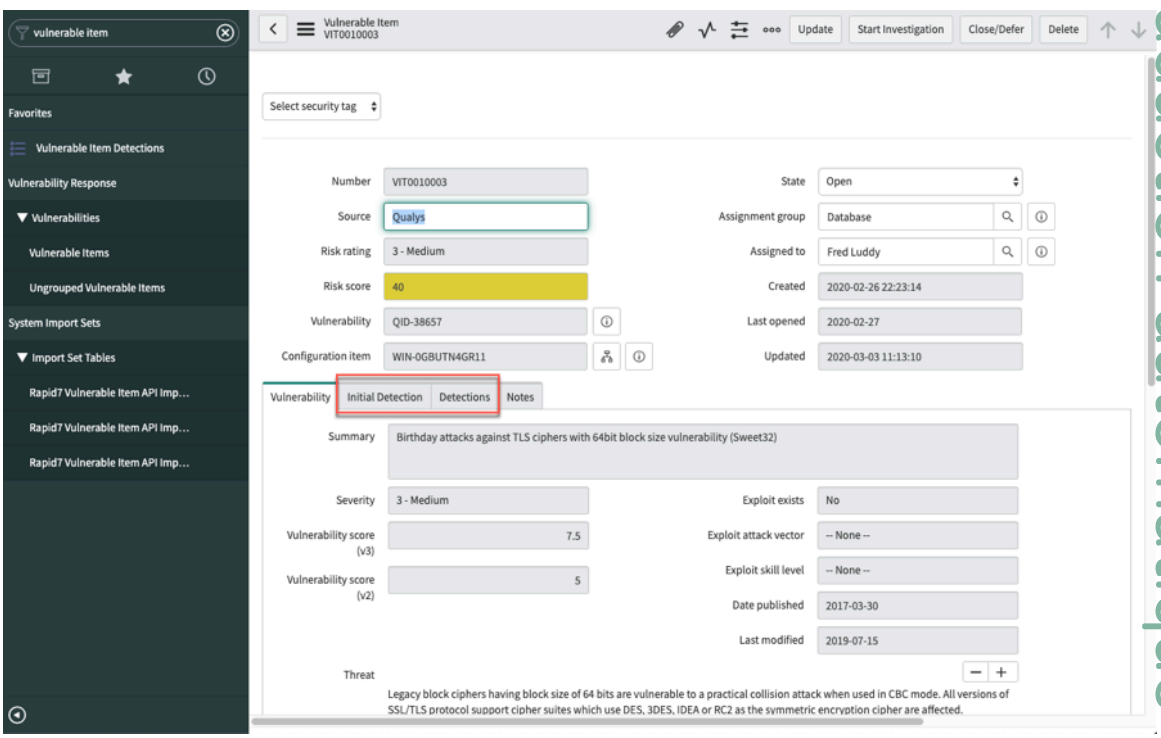
- sn_vuln.admin lance les exécutions d'intégration et affiche les données de détection des éléments vulnérables.
- sn_vul.remediation_owner se voit affecter des éléments vulnérables créés à partir de détections d'éléments vulnérables et affiche les données sur les enregistrements de VI.

Procédure

1. Pour afficher les données de détection d'éléments vulnérables, accédez à un enregistrement d'éléments vulnérables et ouvrez-le.

   L'enregistrement s'affiche avec les onglets Détections initiales et Détections.

   Remarque : Les données précédemment affichées dans l'onglet Détails de la configuration s'affichent avec d'autres données de détection dans les onglets Détection initiale et Détections.

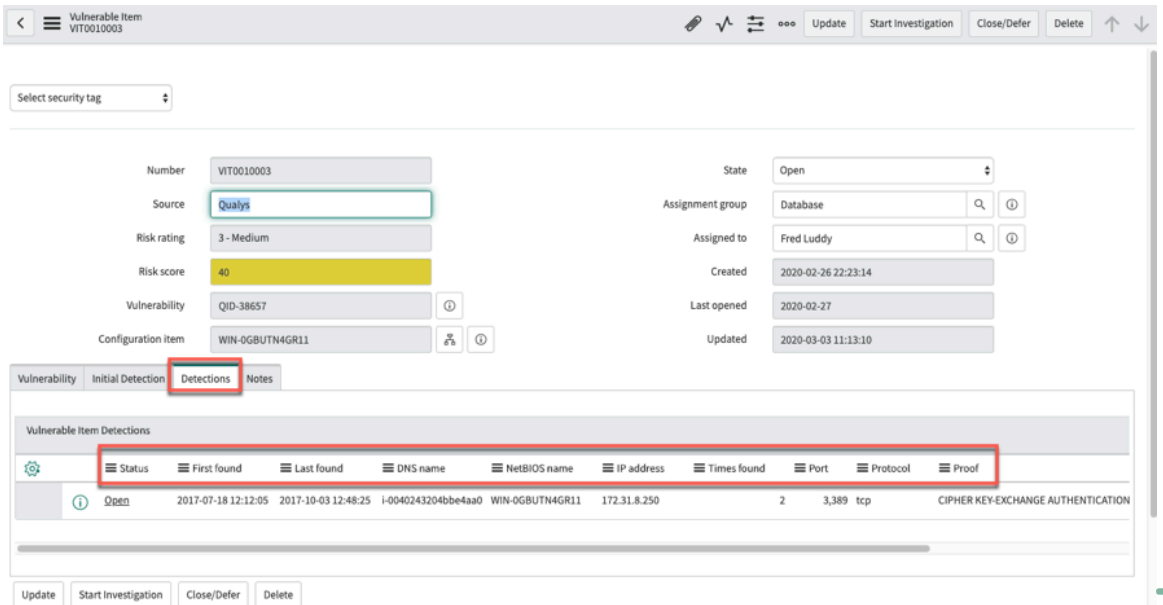


2. Cliquez sur l'onglet **Détections** .

   Lorsqu'un élément vulnérable est créé à partir des résultats d'une analyse tierce, les données de l'analyse sont affichées sur l'enregistrement de détection, comme illustré dans la figure suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Chaque ligne de la section Détections d'éléments vulnérables représente les données d'une détection distincte. Dans la colonne Premier trouvé, la date à laquelle l'élément vulnérable est détecté pour la première fois par le scanner s'affiche. Dans la colonne Dernier trouvé, la date de la détection la plus récente s'affiche. Le champ Source affiche le scanner qui a récupéré les données.

Remarque : Pour Qualys, avec les détections d'éléments vulnérables, les champs suivants sont déconseillés sur l'enregistrement de VI et ne sont plus renseignés :

- Qualys sévérité
- Dernière mise à jour par source

Qualys De même, comme illustré dans la figure précédente, lorsqu'un VI est créé à partir d'un scan, la valeur du scan pour les résultats est affichée dans la colonne Preuve de l'enregistrement de détection. Toutefois, cette valeur n'est pas affichée dans la partie supérieure de l'enregistrement de VI.

Pour Rapid7, lorsqu'un VI est créé à partir d'un scan, la valeur de Preuve du scan peut être affichée à la fois dans la colonne Preuve de l'enregistrement de détection et dans la partie supérieure de l'enregistrement du VI, mais pas par défaut. Pour afficher cette valeur dans la partie supérieure de l'enregistrement de VI, sélectionnez le champ Preuve dans la mise en page du formulaire.

3. **Facultatif :** Pour configurer la mise en page de l'onglet Détections sur l'enregistrement, procédez comme suit.

   a. Les colonnes suivantes s'affichent par défaut dans l'onglet Détections.

   - Statut
   - Premier trouvé (données)
   - Dernière occurrence trouvée (date)
   - Nom DNS
   - Nom du BIOS réseau
   - Adresse IP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Durées trouvées
- Port
- Protocole
- Preuve
- SSL

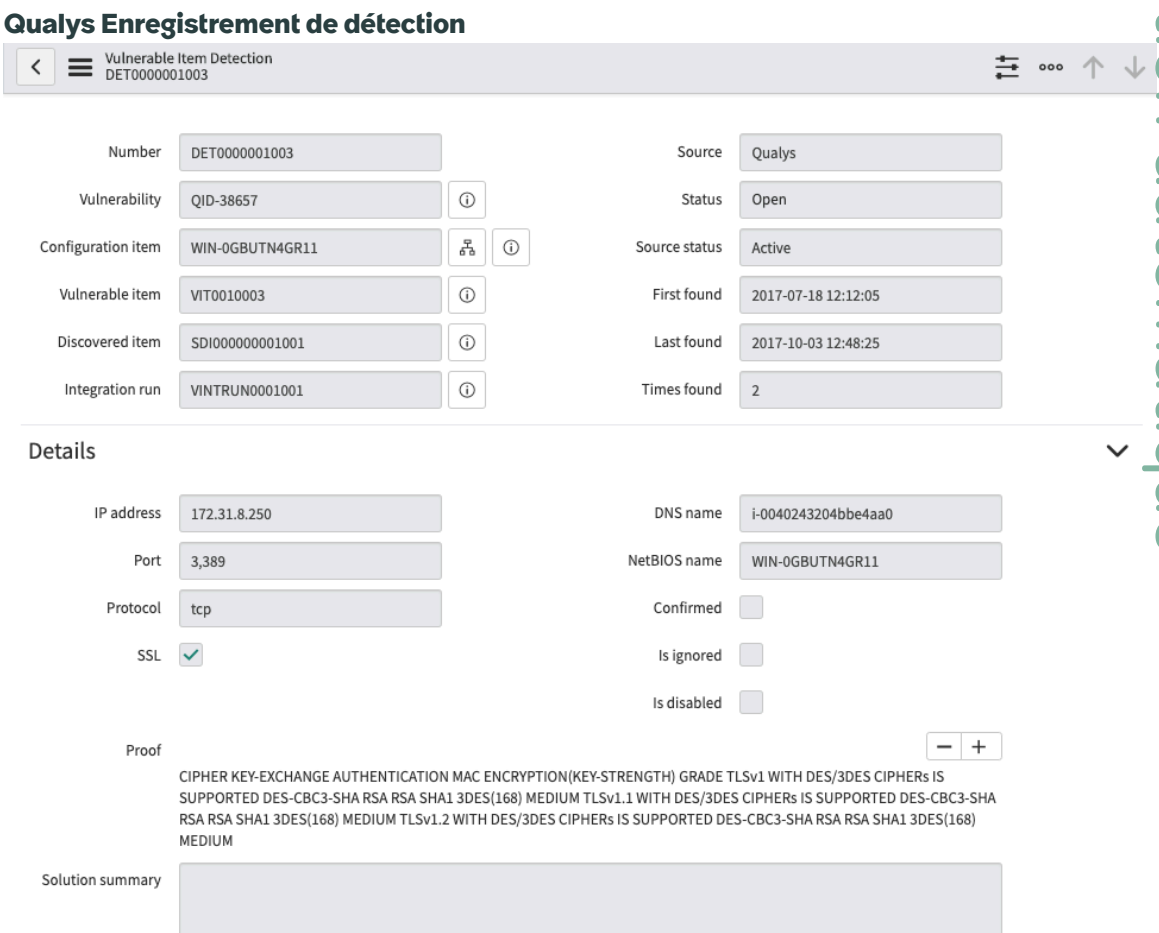
Remarque :

Remarque : s'il n'y a aucune valeur dans une colonne, les données de ce champ n'ont pas été détectées par le scanner.

b. Cliquez sur l'icône Engrenage (icône) pour personnaliser votre vue.

c. Sélectionnez les colonnes de la zone de liste double pour afficher des données spécifiques, puis cliquez sur **OK.**

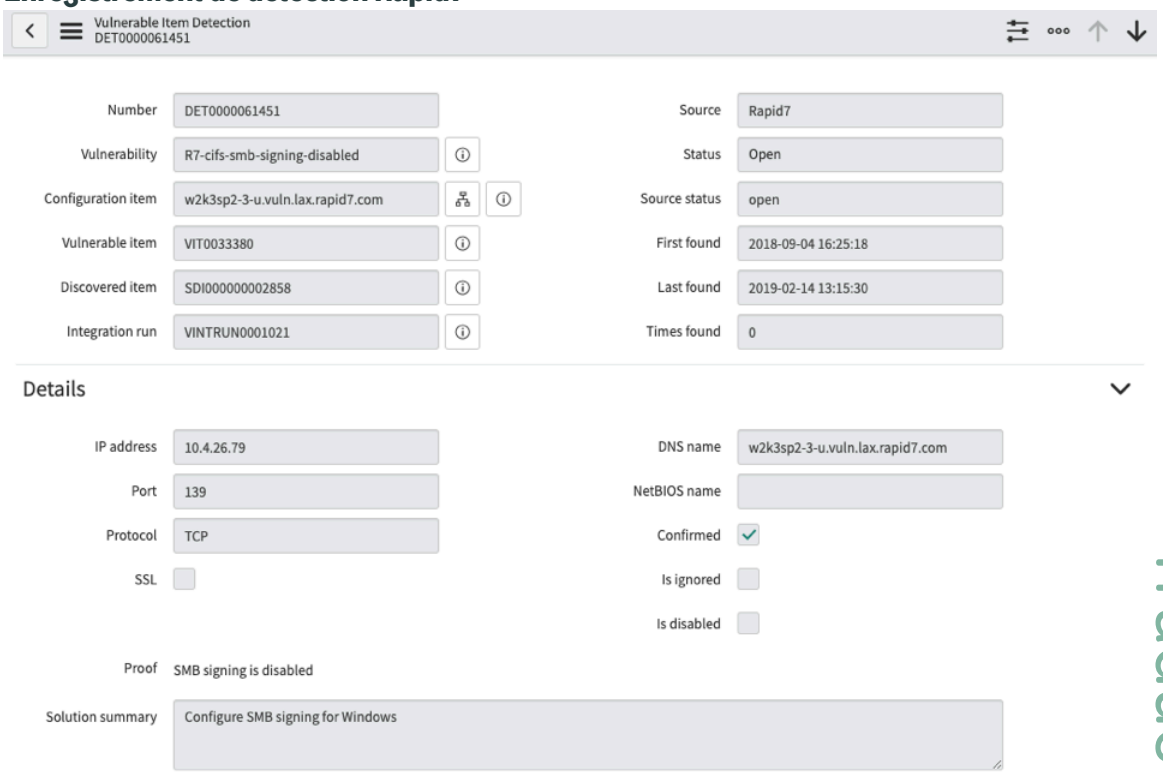
4. Une fois l'onglet Détections sélectionné, dans la colonne État, cliquez sur un élément pour ouvrir l'enregistrement de détection et afficher les détails associés à cet élément vulnérable, y compris un résumé de la solution (intégration Rapid7 InsightVM uniquement).



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrement de détection Rapid7

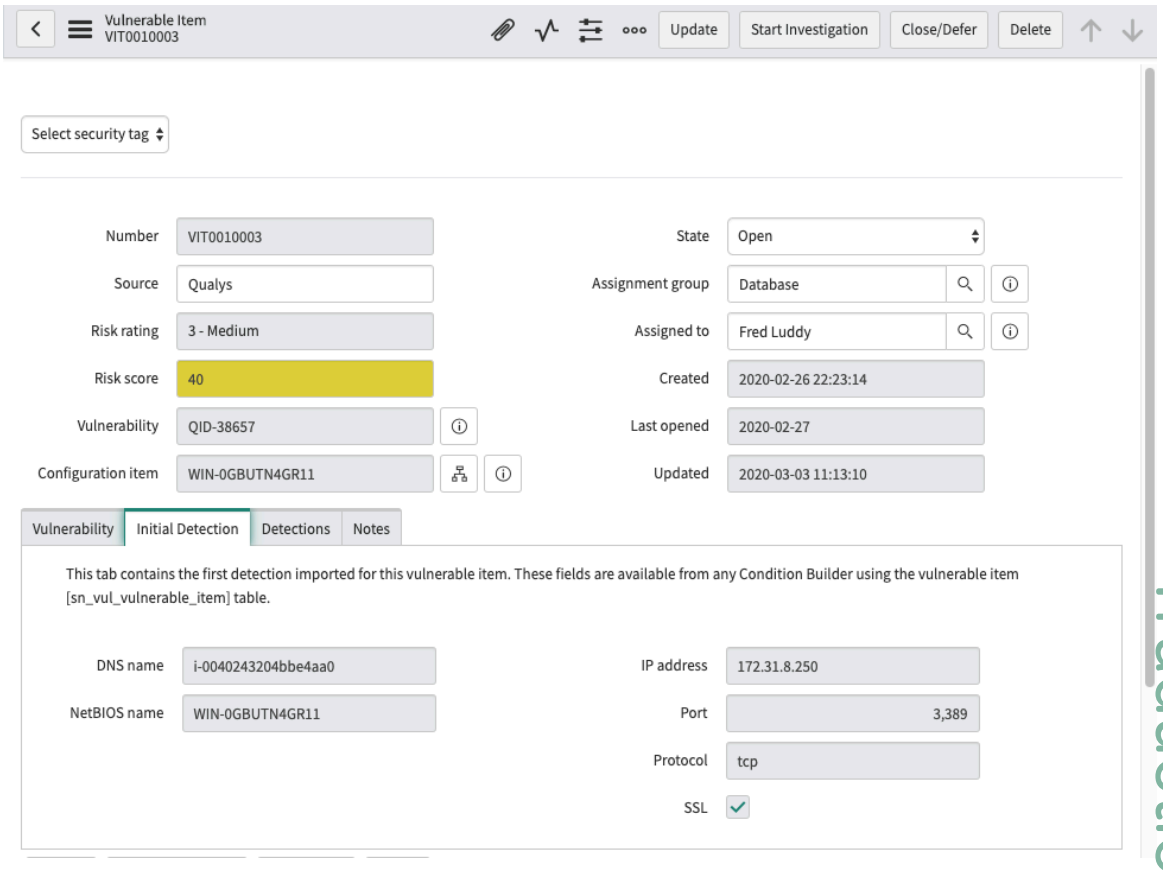


5. Revenez à l'enregistrement et sélectionnez l'onglet Détection initiale.

L'onglet Détections initiales affiche les données importées à partir du scanner tiers lors de la première occurrence de la détection. Ces informations de l'onglet de détection initiale ne changent pas lorsque les données de détection sont mises à jour.

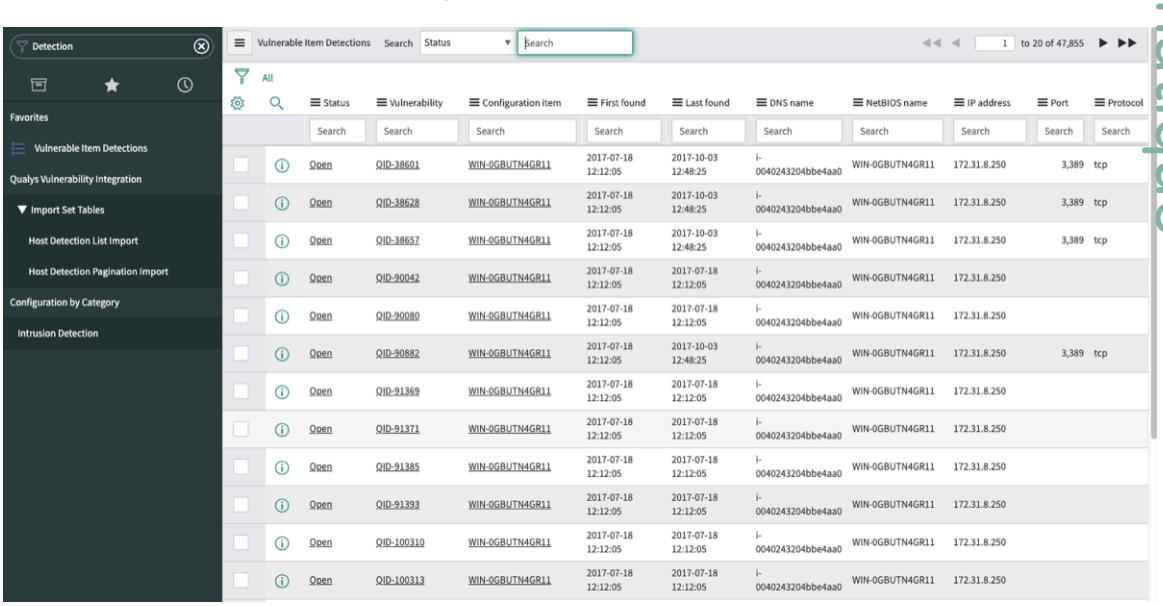
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. **Facultatif :** Accédez à Détection des éléments vulnérables pour afficher la liste de détection des éléments vulnérables.

   (Optional) La liste de détection des éléments vulnérables s'affiche. Chaque ligne de la liste de détections des éléments vulnérables représente une détection distincte. Les colonnes affichent les mêmes données que l'enregistrement de VI.



Les détections ne sont ouvertes ou fermées que par les données trouvées par un scanner, elles ne sont pas déployées à partir des VI. Au fur et à mesure que les détections sont importées, elles sont utilisées pour créer des éléments vulnérables et mettre à jour leurs états. Si toutes les détections sont fermées pour un élément

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérable, cet élément vulnérable sera fermé. Sur l'enregistrement du VI, l'état est fermé et le sous-état est fixe.

Remarque : Les erreurs sont consignées pendant que :

- Traitement des pièces jointes récupérées à partir du scanner.
- Création ou mise à jour de détections ou d'éléments vulnérables.

Pour plus d'informations sur la gestion des erreurs de détection, reportez-vous à la section Gestion des erreurs pour les détections.

Lorsque tous les VI sont fermés pour une tâche de rattrapage, la tâche de rattrapage est fermée.

Les VI fermés avec un sous-état **fixe** ou **périmé** sont rouverts si une nouvelle détection est créée et que les VI peuvent être mis en correspondance avec la nouvelle vulnérabilité.

Les éléments vulnérables définis sur **Résolu** dans votre instance, mais pas transitionnés à **l'état Fermé/Corrigé** par les exécutions d'intégration suivantes sont rouverts s'ils sont détectés lors des nouvelles analyses.

Lorsque tous les VI sont fermés pour une tâche de rattrapage, l'enregistrement est fermé.

Les éléments vulnérables définis sur « Résolu » dans votre instance, mais pas transitionnés vers « Fermé/Corrigé » par les exécutions d'intégration suivantes sont rouverts s'ils sont détectés lors des nouvelles analyses.

Pour Rapid7 les détections, une option est maintenant disponible sur la page de configuration Rapid7 de votre instance pour rouvrir les VI résolus par âge. Si cette option est activée, les VI définis sur **Résolu** , mais ne sont pas transitionnés à **l'état Fermé/Corrigé** par les analyses suivantes et reviennent à **l'état Ouvert** après le nombre de jours que vous entrez.

En ce Qualys qui concerne les détections, si le scanner continue de trouver des VI qui ont été définis sur « Résolu », mais qui ne sont pas passés à **l'état Fermé/Corrigé** par les analyses suivantes, ces VI retournent à l'état **Ouvert** lorsque la dernière date trouvée est postérieure à la date de résolution.

Que faire ensuite

Pour afficher plus de données, y compris le nombre d'éléments et de détections, vous pouvez Vérifier les Réponse aux vulnérabilités données de détection d'éléments vulnérables sur les enregistrements de l'exécution de l'intégration (VINTRUN).

Vérifier les Réponse aux vulnérabilités données de détection d'éléments vulnérables sur les enregistrements de l'exécution de l'intégration (VINTRUN)

À partir des enregistrements d'exécution d'intégration de votre ServiceNow AI Platform® instance, vous pouvez localiser les données de détection d'éléments vulnérables d'intégration tierce en fonction de la date et de l'heure des analyses. Vérifiez que l'analyse a été effectuée avec succès, affichez le nombre de détections individuelles, ainsi que tous les éléments vulnérables (VI) créés ou mis à jour directement à la suite des analyses.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vuln.admin (obsolète)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Vous préférerez peut-être que les informations d'exécution de l'intégration, soit la date et l'heure de l'analyse, soit le numéro d'enregistrement de l'exécution de l'intégration (VINTRUN#) de l'élément vulnérable ou des enregistrements de détection pour vous aider à localiser des enregistrements spécifiques dans les listes suivantes.

Procédure

1. Choisissez-en un pour continuer.

Intégration	Description
Accédez à la **Rapid7 Vulnerability Integration** > **Administration** > **Intégrations**	Dans la liste Intégrations Rapid7, choisissez l'intégration pour laquelle vous souhaitez afficher les résultats de l'analyse de détection. **a.** Entrepôt de données Rapid7 : ▪ Intégration des éléments vulnérables Rapid7 ▪ Intégration de résolution des éléments vulnérables Rapid7 ▪ Intégration complète des éléments vulnérables Rapid7 **b.** Intégration de résolution d'élément vulnérable Rapid7 (InsightVM) ▪ Intégration des éléments vulnérables Rapid7 : API ▪ Intégration complète des éléments vulnérables Rapid7 : API
Accédez à la **Qualys** > **Intégration de Qualys Vulnerability** > **Intégrations principales**	Dans la liste Intégrations Qualys, choisissez parmi : ○ Intégration de la détection d'hôte Qualys ○ Intégration complète de la détection d'hôte Qualys
Accédez à la **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**	Dans la liste Intégrations Tenable, choisissez l'intégration pour laquelle vous souhaitez afficher les résultats de l'analyse de détection.
Accédez à la **Intégration de vulnérabilité Microsoft TVM** > **Administration** > **Intégrations**	Dans la liste Intégrations Microsoft TVM, choisissez l'intégration pour laquelle vous souhaitez afficher les résultats de l'analyse de détection.

2. En bas de la page qui s'affiche, cliquez sur l'onglet**Exécutions d'intégration de vulnérabilité**.

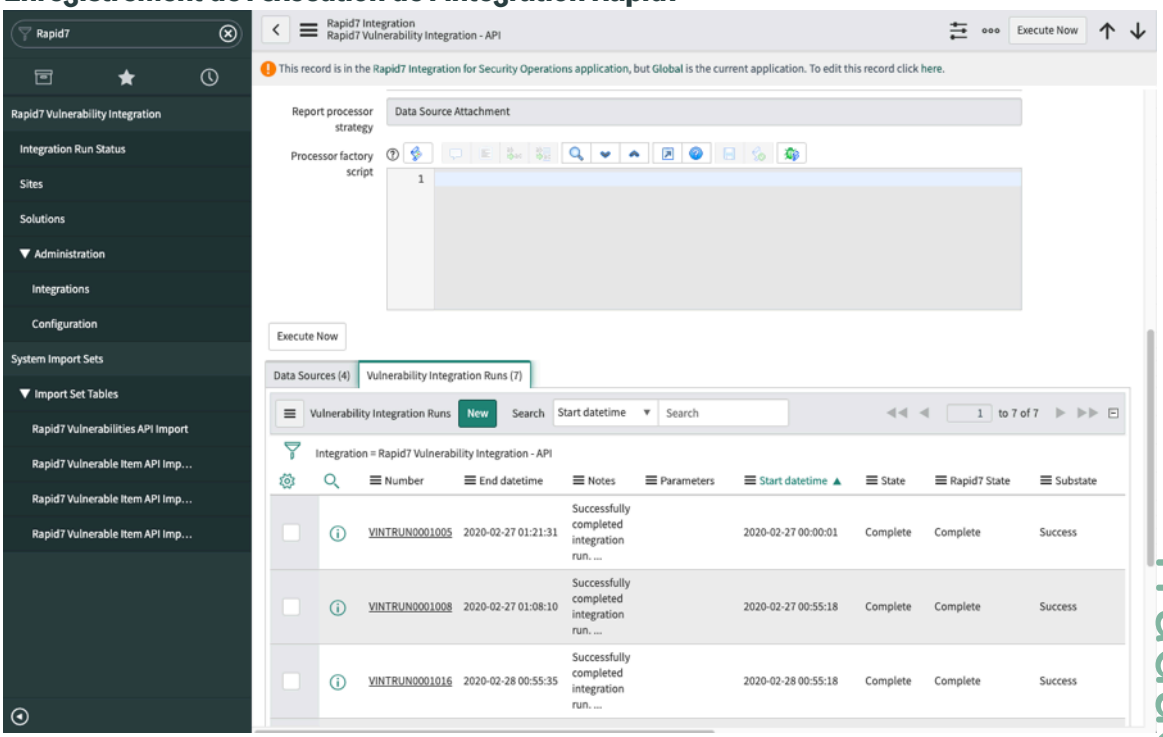
3. Cliquez sur un élément dans les colonnes Numéro ou Source de l'importation pour ouvrir un enregistrement.

L'enregistrement de l'exécution de l'intégration s'affiche.

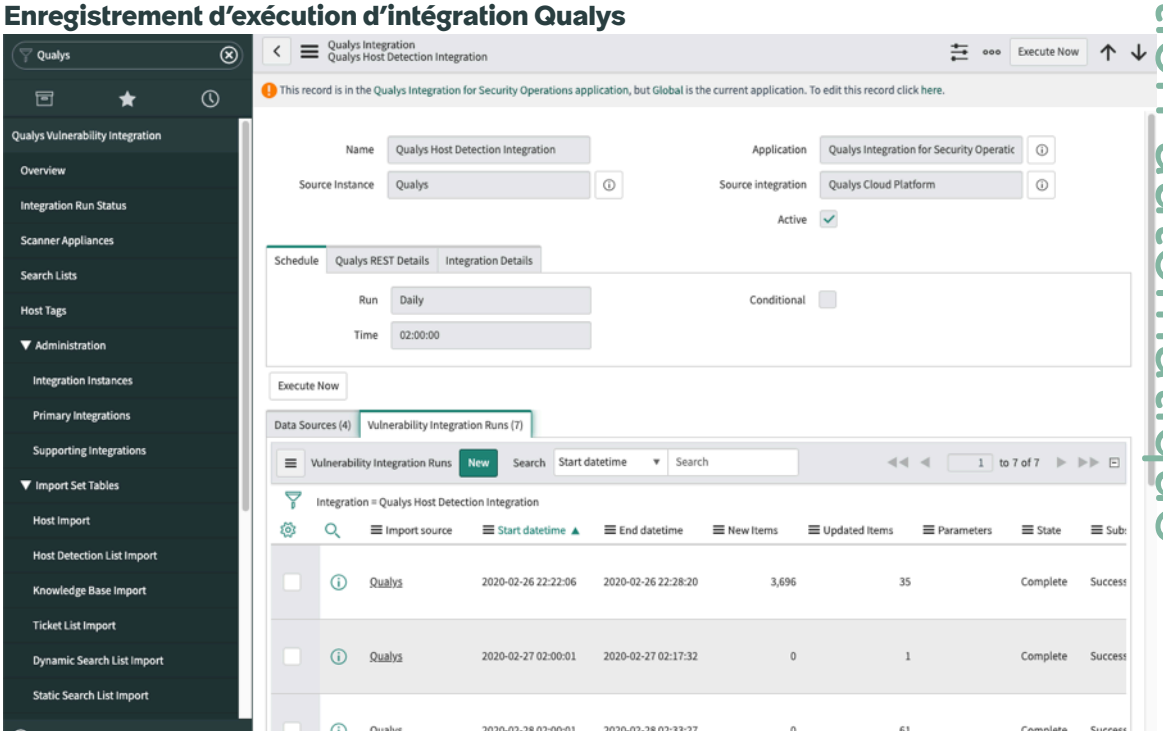
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrement de l'exécution de l'intégration Rapid7



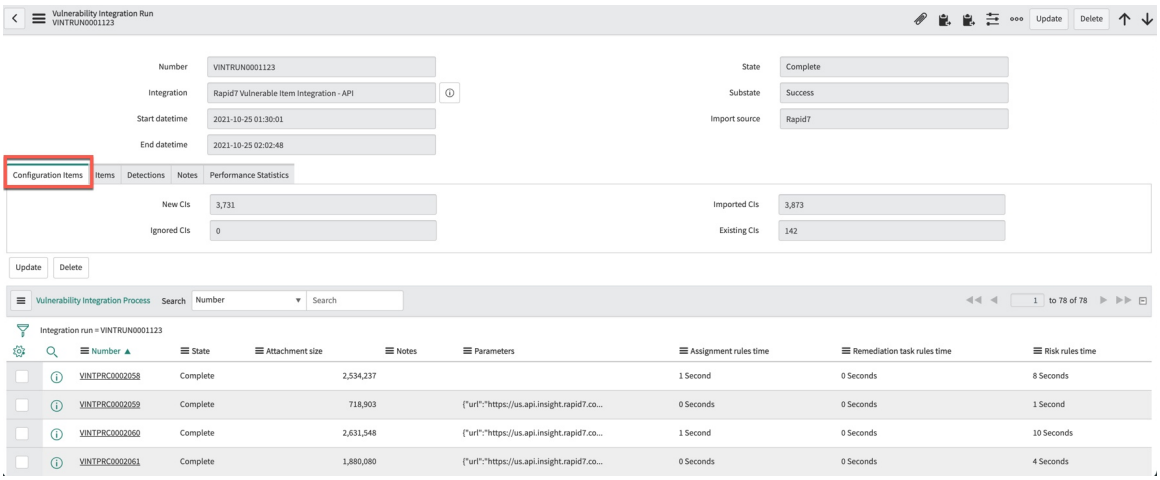
Enregistrement d'exécution d'intégration Qualys



L'enregistrement de l'exécution de l'intégration s'affiche. Vous pouvez vérifier dans le champ État que l'intégration s'est correctement exécutée. Sélectionnez l'onglet **Éléments de configuration** .

Traduction automatique

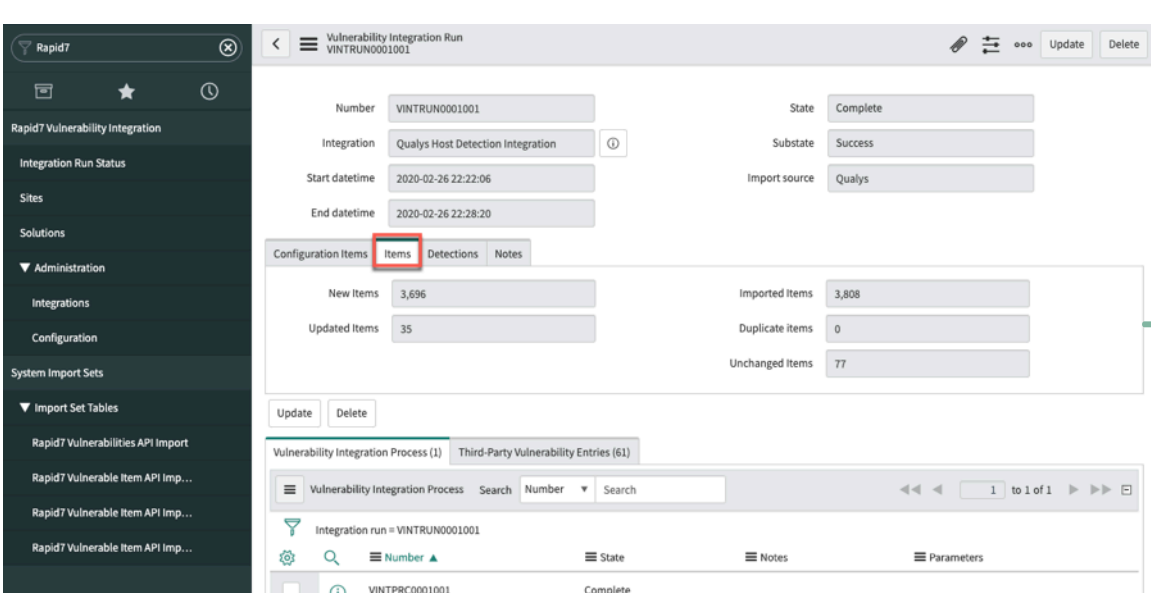
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L’onglet Éléments de configuration affiche les informations suivantes :

- L’onglet Éléments de configuration affiche le nombre total d’éléments de configuration importés.
- Le champ Nouveaux CI affiche le nombre de CI créés dans le cadre de cette exécution d’intégration.
- Le champ CI importés affiche la somme de tous les CI de cette section.
- La valeur du champ CI ignorés est toujours de 0 pour les Réponse aux vulnérabilités intégrations.
- Le champ CI existants affiche le nombre total de CI qui existent déjà.

Cliquez sur l’onglet **Éléments** .



L’onglet Éléments affiche les informations suivantes :

- L’onglet Éléments affiche le nombre total de VI importés. Vous pouvez voir le nombre total de détections importées en ajoutant les nombres répertoriés sous l’onglet Détections.
- Le champ Nouveaux éléments affiche le nombre d’éléments vulnérables créés à partir de l’exécution de cette intégration.
- Le champ Éléments importés affiche la somme de tous les champs de cette section.

Traduction automatique

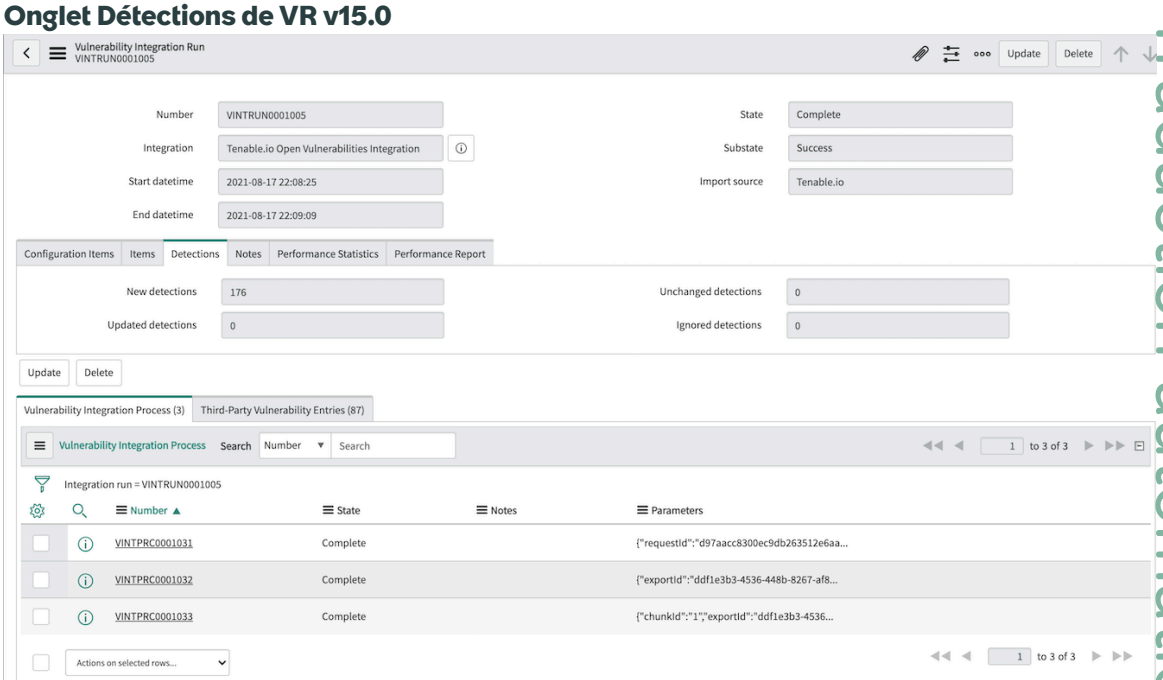
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le champ Éléments en double n'est plus renseigné.
- Le champ Éléments mis à jour affiche le nombre de fois où les éléments vulnérables sont mis à jour au cours de cette exécution d'intégration. Cette valeur n'est pas le nombre d'éléments vulnérables uniques qui sont mis à jour. Si, par exemple, un élément vulnérable est mis à jour deux fois pendant l'exécution de l'intégration, il est compté deux fois et affiché sous la forme de 2 éléments mis à jour.
- Le champ Éléments inchangés affiche les éléments vulnérables trouvés pendant l'exécution de l'intégration qui existent déjà dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

4. Cliquez sur l'onglet **Détections** .

   Cet onglet n'est affiché que si l'exécution de l'intégration comporte des détections. Vous pouvez vérifier le nombre total de détections importées en ajoutant les numéros répertoriés.

Onglet Détections de VR v15.0



Remarque : Avant la version 15.0, il n'existait aucun champ pour les détections ignorées.

L'onglet Détections affiche les informations suivantes :

- À partir de la version v15, un nouveau champ Détections ignorées a été ajouté pour suivre les détections, qui étaient auparavant ignorées. Avec cette implémentation, le nombre de détections importées et le nombre suivi sur les enregistrements d'exécution de l'intégration deviennent cohérents. Cette fonctionnalité a été implémentée pour tous les scanners, Qualys Vulnerability Integration c'est-à-dire , Intégration des vulnérabilités Rapid7Tenable Vulnerability Integration et Microsoft TVM.
- Le champ Nouvelles détections affiche les nouvelles détections créées au cours de cette exécution d'intégration.
- Le champ Détections non modifiées affiche les détections trouvées pendant l'exécution de l'intégration qui existent déjà dans la base de données, mais qui n'ont pas été mises à jour, car aucune des valeurs de champ pertinentes n'a changé.
- Le champ Détections mises à jour affiche le nombre de fois où les détections sont mises à jour au cours de cette exécution d'intégration. Cette valeur n'est pas le nombre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de détections uniques mises à jour. Si, par exemple, une détection est mise à jour deux fois dans le cadre de l'exécution de l'intégration, elle est comptée deux fois et s'affiche sous la forme de 2 détections mises à jour.

Remarque : Les détections qui ne sont pas affichées dans ces comptages sont des détections qui sont à l'état fermé (Fixe), car les enregistrements fixes sont utilisés pour mettre à jour les VI existants. Si vous voulez plus de visibilité sur ces enregistrements de détection, vous pouvez afficher les VI fermés qui sont créés lorsqu'il n'y a pas de VI correspondant existant à l'état ouvert. Pour en savoir plus sur les vulnérabilités à l'état fixe que vous pouvez activer dans l'assistant de configuration pour l'intégration Qualys, reportez-vous à la section Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration.

5. Cliquez sur un élément dans les colonnes Numéro ou Source de l'importation pour ouvrir un enregistrement.

Affichage des données de correctifs et planification des correctifs dans Réponse aux vulnérabilités

À partir de la version 16.1 de Réponse aux vulnérabilités, vous pouvez planifier des correctifs et afficher les données des correctifs ainsi que les informations sur la solution et d'autres vulnérabilités sur les enregistrements dans l'environnement classique et les Réponse aux vulnérabilités espaces de travail de votre ServiceNow AI Platform instance.

Rôles requis

Les utilisateurs ont besoin de rôles spécifiques à l'intégration d'orchestration de correctifs que vous utilisez pour importer vos correctifs afin d'afficher les données et de planifier les correctifs. Consultez les intégrations prises en charge pour plus d'informations.

- Présentation de l'intégration de l'orchestration de correctifs HCL BigFix avec Réponse aux vulnérabilités et Présentation de l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs à Microsoft SCCM.
- Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord dans l'environnement classique.
- Affichez les données sur les tableaux de résultats dans le Réponse aux vulnérabilités Espaces de travail.

Planification des correctifs

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- Mise à jour de correctif (VPU)
- Tâche de rattrapage (RT)
- Élément détecté (SDI)

Patcher les données dans l'environnement classique

Depuis l'environnement classique de l'application Réponse aux vulnérabilités :

- Pour afficher les enregistrements de mise à jour de correctifs, accédez à **Tous** > **Réponse aux vulnérabilités** > **Correctifs**.
- Pour afficher les solutions, accédez à **Tous** > **Réponse aux vulnérabilités** > **Solutions**.
- Pour afficher les VI qui vous sont affectés et qui possèdent des correctifs, accédez à **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Affecté à moi avec correctifs**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour afficher les tâches de rattrapage, accédez à **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Affecté à moi avec correctifs**
- Pour afficher les enregistrements d'éléments détectés, accédez à **Tous** > **Security Operations** > **Éléments découverts**.

Données de correctif et déploiement d'état pour l'orchestration de correctifs dans Réponse aux vulnérabilités

À partir de la version 16.1, les données et les états des correctifs sont déployés dans la mise à jour du Réponse aux vulnérabilités correctif et d'autres enregistrements dans l'application Réponse aux vulnérabilités .

Enregistrements de mise à jour de correctif dans les espaces de travail de l'environnement classique dans Réponse aux vulnérabilités

Les informations sur les correctifs, les solutions de vulnérabilité et les vulnérabilités sont toutes connectées dans l'application Réponse aux vulnérabilités .

Les données de correctif et les données et l'état de déploiement de correctif s'affichent sur les enregistrements de votre instance. Les enregistrements de correctifs sont inclus dans le cadre de la fonctionnalité d'orchestration des correctifs de cette intégration avec Réponse aux vulnérabilités. Affichez les enregistrements Correctif (VPU) dans les espaces de travail Réponse aux vulnérabilités à partir de la vue Liste dans l'espace de travail Rattrapage informatique. Les enregistrements de mise à jour de correctif dans la vue classique et dans les espaces de travail Réponse aux vulnérabilités incluent les données suivantes :

- Données et informations de solutions de vulnérabilité provenant des fournisseurs de correctifs importées par l'application Gestion des solutions de vulnérabilité.
- État du rattrapage à la source qui inclut le nombre total d'appareils présentant une vulnérabilité pouvant être corrigée par un correctif, ainsi que tous les appareils pour lesquels il manque des mises à jour.
- État de rattrapage qui inclut le % de VI rattrapés et le nombre total de VI qui ont un correctif comme correctif préféré.
- Appareils associés, éléments vulnérables, déploiements de correctifs et demandes de correctifs sur les liens connexes des enregistrements dans la vue de classe. Ces données sont affichées sur les onglets des enregistrements dans les espaces de travail Réponse aux vulnérabilités.
- Demandes de correctifs que les propriétaires de rattrapage ont soumises pour approbation.

Rôles requis

Les utilisateurs ont besoin de rôles spécifiques à l'intégration d'orchestration de correctifs que vous utilisez pour afficher les données et planifier les correctifs. Consultez les intégrations prises en charge pour plus d'informations.

- Présentation de l'intégration de l'orchestration de correctifs HCL BigFix avec Réponse aux vulnérabilités et Présentation de l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs à Microsoft SCCM.
- Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord dans l'environnement classique.
- Affichez les données sur les tableaux de résultats dans le Réponse aux vulnérabilités Espaces de travail.

Traduction automatique

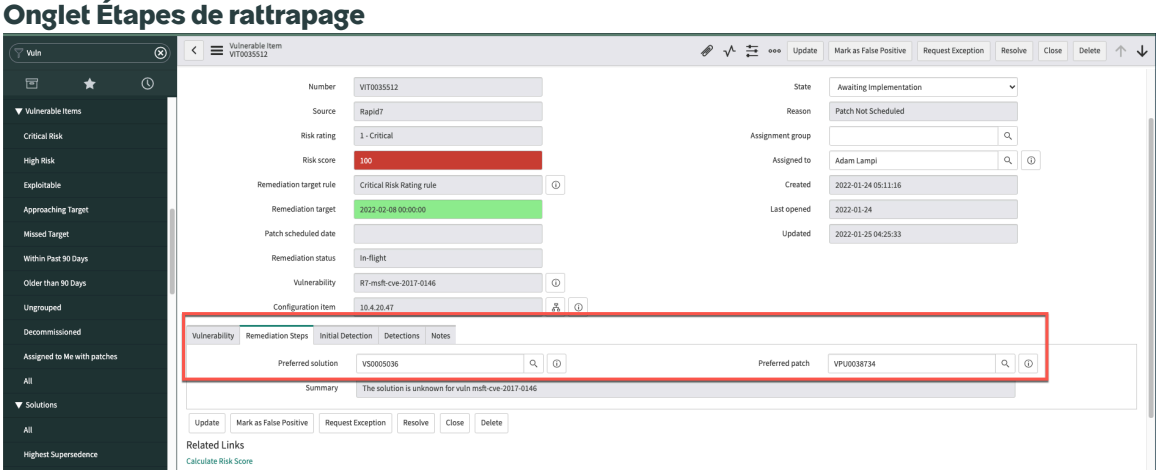
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Données du correctif et déploiement de l'état

Pour afficher les éléments vulnérables qui ont des correctifs et qui vous sont affectés dans l'environnement classique, accédez à **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Affecté à moi avec correctifs**.

Si un enregistrement d'élément vulnérable est renseigné avec un correctif préféré, il passe automatiquement à **En attente d'implémentation** uniquement si l'état du VI n'est pas **Fermé**, **Résolu**, **Différé** ou **En cours de révision**. Pour explorer les données afin d'afficher la solution préférée et d'autres données, cliquez sur l'onglet **Rattrapage** sur l'enregistrement de VI.

Onglet Étapes de rattrapage



Un VI avec un correctif préféré passe à **En attente d'implémentation** dans les cas suivants :

- Si un correctif est planifié pour être déployé sur un CI qui fait partie d'une importation de collection et que le CI est associé à un VI, la raison pour laquelle le VI est **en attente d'implémentation** est **Correctif planifié**.
- Si un correctif est planifié pour être déployé sur un CI qui fait partie d'une importation de collection, et que le CI a un VI associé et que la date cible de rattrapage (échéance) est ultérieure à la date de délai de rattrapage (TTR), l'état du VI est **En attente d'implémentation** avec le motif **Correctif planifié (date cible manquante)**.
- Si un correctif n'est pas planifié pour le déploiement sur un CI qui fait partie d'une importation de collection, l'état du VI est **En attente d'implémentation**, avec le motif **Correctif non planifié**.

Cliquez sur l'icône d'informations sur le **correctif préféré** pour ouvrir les mises à jour du correctif et afficher les informations suivantes sur les liens connexes :

Éléments vulnérables

Éléments vulnérables associés à ce correctif.

Appareils associés

Les appareils qui ont des mises à jour et ceux qui n'ont pas de mises à jour.

Déploiements de correctifs

Déploiements planifiés pour ce correctif sur des ordinateurs individuels (actifs) ou sur des groupes d'actifs.

Demandes de correctifs

Une liste des demandes de correctifs qui ont été envoyées pour approbation avant leur planification de déploiement.

Correctifs potentiels

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Correctifs susceptibles de corriger une vulnérabilité.

Cliquez sur l'icône d'informations sur le **correctif préféré** pour ouvrir l'enregistrement et afficher les informations énumérées précédemment, en plus des données de mise à jour des correctifs suivantes :

État du rattrapage de la source

Nombre total d'appareils qui nécessitent ce correctif et tous les appareils auxquels il est manquant.

État du rattrapage

État (VI totaux, % rattrapés, VI différés) des VI qui ont ce correctif préféré.

Correctifs et solutions préférés

Lorsqu'une vulnérabilité importée correspond à un actif dans votre Base de données de gestion des configurations (CMDB), un élément vulnérable (VI) est créé dans Réponse aux vulnérabilités. Si l'élément de configuration (CI) associé à ce VI est également importé d'un fournisseur de correctif tiers et s'affiche comme ayant un correctif manquant pour la même vulnérabilité, un correctif préféré est répertorié et déployé sur vos solutions. Ces informations vous permettent de savoir qu'un actif (CI) a un correctif à partir d'un correctif disponible qui correspond le mieux à sa vulnérabilité.

Affichage des correctifs sans solutions

Après une importation, si aucune donnée de solution de vulnérabilité n'est disponible, le champ **Solution de vulnérabilité** de l'enregistrement de mise à jour de correctif est laissé vide. Pour plus d'informations sur l'affichage des informations relatives à ces types de patchs, reportez-vous à la section Afficher les correctifs sans solutions dans Réponse aux vulnérabilités.

Afficher les correctifs sans solutions dans Réponse aux vulnérabilités

À partir de la version 16.0 de , pour les correctifs qui n'ont pas de solution après une importation, le système recherche ensuite les ID de correctifs dans les données de référence de Réponse aux vulnérabilités vulnérabilité afin que vous puissiez afficher ces correctifs sur les enregistrements de vulnérabilité.

Correctifs sans solutions

Rôle requis : sn_vul.vulnerability_admin.

Les données importées à partir des applications d'orchestration des correctifs et de solutions de vulnérabilité, ainsi que des intégrations de scanners de correctifs, sont traitées, connectées et affichées dans l'application sur les enregistrements de mise à jour des Réponse aux vulnérabilités correctifs.

Lorsqu'une solution existe pour une vulnérabilité, les informations connexes sont corrélées dans votre instance et sont déployées à partir des correctifs, des solutions de vulnérabilité et des vulnérabilités. Pour afficher ces informations, accédez à **Tous** > **Réponse aux vulnérabilités** > **Correctifs** > **Tous**.

Après une importation, si aucune donnée de solution de vulnérabilité n'est disponible, le champ **Solution de vulnérabilité** de l'enregistrement de mise à jour de correctif est laissé vide. Afin que vous puissiez afficher les informations de solutions connexes pour ces correctifs, une propriété système, [**sn_vul_patch_orch.no_solution_patch_rollup**], est activée par défaut dans votre instance. Cette propriété recherche les ID de bulletin et les ID d'article dans les données de référence de vulnérabilité à partir des importations de scanner. Si une correspondance est trouvée, les données associées sont renseignées dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la table des correctifs potentiels et ces informations sont affichées sur les listes connexes des enregistrements de vulnérabilité.

Si vous avez un grand nombre de vulnérabilités ou si la tâche planifiée de déploiement prend beaucoup de temps, vous préférerez peut-être désactiver cette propriété système pour éviter d'éventuels problèmes de performances. Toutefois, notez que si vous désactivez cette propriété système, les données de solution importées ne sont ni recherchées ni déployées sur vos vulnérabilités sans solution.

En tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin, pour désactiver la propriété système, procédez comme suit :

1. Accédez à la **liste.propriétés.système**.
2. Recherchez **sn_vul_patch_orch.no_solution_patch_rollup** et cliquez dessus pour ouvrir l'enregistrement.
3. Dans le champ Valeur, tapez `faux`.
4. Cliquez sur **Mettre à jour**.

Affichage des données d'orchestration des correctifs sur les Réponse aux vulnérabilités tableaux de bord

À partir de la version 16.1, vous pouvez afficher les données de mise à jour de correctifs dans l'environnement classique sur les tableaux de bord inclus avec l'application Réponse aux vulnérabilités .

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à surveiller la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en affichant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Voir Espace de travail du gestionnaire de vulnérabilités et Exploration de l'Espace de travail de remédiation IT pour plus d'informations.

Vous pouvez également afficher ces données sur les tableaux de bord CISO et Gestion des vulnérabilités (PA) si vous avez un abonnement à Analyse des performances.

Vous pouvez également afficher les données des correctifs dans l'environnement classique. Pour en savoir plus sur les rôles requis et sur la manière d'afficher les données sur les tableaux de bord de l'environnement Réponse aux vulnérabilités classique inclus avec l'application Réponse aux vulnérabilités et sur ceux qui nécessitent un abonnement distinct, reportez-vous à la section Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.

Afficher une solution

Affichez toutes les solutions, les solutions à priorité élevée et les solutions associées à des éléments vulnérables pour éclairer vos activités de rattrapage.

Avant de commencer

Rôle requis : sn_vul.read, sn_vul.vulnerability_admin ou sn_vul.remediation_owner

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

En tant qu'analyste des vulnérabilités ou propriétaire du rattrapage, vous pouvez afficher différents ensembles de solutions liés aux éléments vulnérables.

Remarque : Les enregistrements de solutions sont en lecture seule, à l'exception des **notes** de la section **Notes internes** ou des solutions créées par l'utilisateur.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Solutions**.
2. Choisissez une liste de solutions.

   Remarque : Vous pouvez filtrer une liste de solutions à l'aide de caractères génériques pour le nom du produit.

3. Pour passer en revue, cliquez sur chaque élément.
4. **Facultatif :** Saisissez des notes sous l'onglet **Notes** et cliquez avec le bouton droit sur **Enregistrer** pour rester sur la page ou cliquez sur **Mettre à jour** pour enregistrer et revenir à la liste **des solutions en matière de vulnérabilité** .

   Remarque : Si vous n'avez que le rôle sn_vul.read, vous ne serez pas en mesure d'effectuer cette étape.

Créer une solution de vulnérabilité

Créez une solution de vulnérabilité afin de pouvoir suivre les solutions de vulnérabilité qui ne sont pas couvertes par le contenu de solution tierce.

Avant de commencer

Rôle requis : admin, sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou vulnerability.write

Gestion des solutions pour vulnérabilités est une fonctionnalité disponible au sein de l'application Réponse aux vulnérabilités . Gestion des solutions pour vulnérabilités Nécessite un abonnement distinct.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer une solution à partir de n'importe quelle liste de solutions. Vous devez installer l'application Gestion des solutions de vulnérabilité avant de pouvoir créer une solution.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Solutions**.
2. Choisissez une liste de solutions : **Toutes**, **Priorité la plus élevée** ou **Avec éléments vulnérables**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs modifiables du formulaire, le cas échéant.
   Vous pouvez laisser tous les champs inutilisés vides. Pour plus d'informations sur les champs individuels, reportez-vous à la section Champs du formulaire Solution.
5. Cliquez avec le bouton droit sur **Enregistrer** dans l'en-tête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’enregistrement de solution est ajouté et apparaît dans les listes **Tout** et **Priorité la plus élevée** , par défaut.

6. Les listes connexes s’affichent.

   Vous pouvez associer cette solution aux listes connexes suivantes : **Éléments vulnérables**, **Vulnérabilités tierces**, **CVE**, **Solutions de remplacement** et **Solutions précédentes**. Choisissez une vulnérabilité ou une solution, puis cliquez sur **Soumettre**.

Remarque :

Gestion des solutions pour vulnérabilités Associe automatiquement les éléments vulnérables et les tâches de rattrapage aux solutions lorsque les enregistrements de vulnérabilité sont associés manuellement aux solutions.

Les éléments vulnérables réaffectés manuellement à une autre solution ne sont pas automatiquement mis à jour avec les changements de solution au niveau de vulnérabilité.

Si vous souhaitez exclure la relation entre une vulnérabilité tierce et une solution parce qu’elle n’est pas pertinente pour le CI que vous corrigez ou qu’elle ne pose pas problème dans votre environnement, reportez-vous à la section Exclure manuellement les solutions des enregistrements tiers et vice versa.

Exclure manuellement les solutions des enregistrements tiers et vice versa

Excluez la relation entre une vulnérabilité tierce et une solution, car elle n’est pas pertinente pour le CI que vous corrigez ou ne constitue pas un problème dans votre environnement. Excluez manuellement les solutions utilisant une vulnérabilité tierce ou un enregistrement de solution.

Avant de commencer

Rôle requis :

- sn_vul.écriture
- sn_vul.remediation_owner

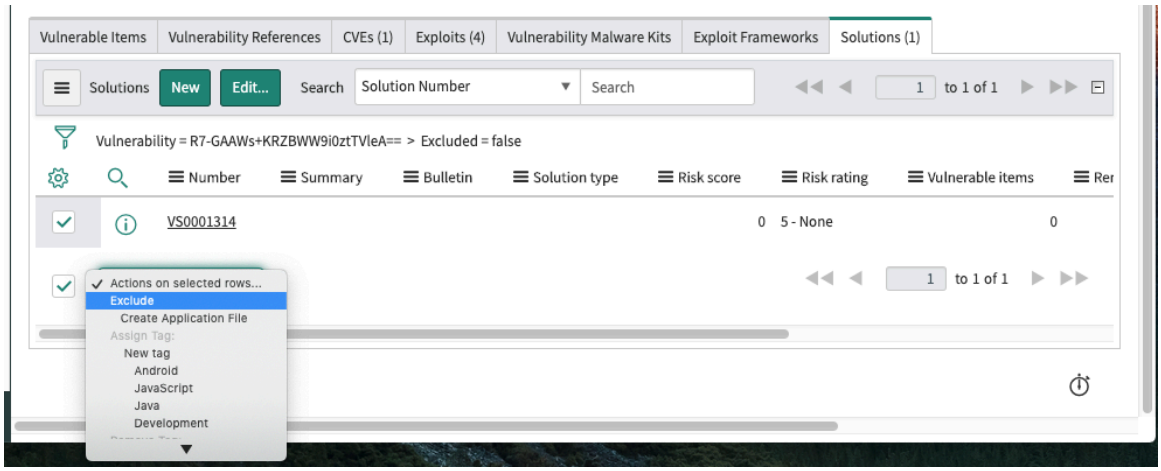
Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l’application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l’Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l’aide de l’assistant Réponse aux vulnérabilités de configuration. Pour plus d’informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** ou **Réponse aux vulnérabilités** > **Toutes les solutions**
2. Ouvrez un enregistrement de vulnérabilité ou de solution tiers.
   a. Pour un enregistrement tiers : **sélectionnez l’onglet** Solutions connexes.
   b. Pour un enregistrement de solution : Sélectionnez l’onglet connexe **Vulnérabilités tierces** .
3. Cochez la case en regard de chaque enregistrement de vulnérabilité ou de solution que vous souhaitez exclure.
4. Dans le menu déroulant **Actions sur les lignes sélectionnées** , choisissez **Exclure**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'enregistrement de tiers ou de solution n'apparaît plus dans l'onglet connexe.

Les relations de vulnérabilité tierce aux solutions sont également exclues lorsque les solutions sont mises à jour ou si la tâche de nuit est activée.

Les relations de vulnérabilité de tiers aux solutions sont exclues pendant la tâche planifiée nocturne.

L'exclusion des vulnérabilités tierces signifie que la solution n'est plus un facteur d'évaluation de solution privilégiée. Impacts de l'exclusion :

- Tous les comptes pour les solutions puisque la vulnérabilité tierce, les éléments vulnérables (VI) et les éléments de configuration (CI) attachés à la vulnérabilité tierce ne comptent plus dans la solution.
- Détermination de la solution préférée pour la vulnérabilité tierce et, par extension, de la solution préférée de tous les VI joints et des tâches de rattrapage contenant le VI.

Triage automatique des vulnérabilités

L'examen et le tri des nouvelles vulnérabilités sont nécessaires pour garantir la réussite du rattrapage. Transformez les importations de vulnérabilité en tâches de rattrapage avec l'affectation automatisée des éléments vulnérables (VI), le calcul des risques, les cibles de rattrapage et le regroupement des VI.

En commençant par les vulnérabilités importées, rapprochez les actifs introuvables dans la CMDB, hiérarchisez les résultats, traduisez-les en activités de rattrapage qui sont automatiquement affectées, orchestrez le processus de rattrapage et confirmez l'achèvement avec une analyse de validation.

Les nouveaux éléments vulnérables sont généralement triés en tâches de remédiation lors de l'importation, en fonction des règles de tâches de remédiation. Parfois, les éléments vulnérables ne peuvent pas être regroupés ou ne contiennent pas d'élément de configuration reconnu.

Une vue d'ensemble du processus de triage des vulnérabilités :

- Connectez-vous à votre instance Réponse aux vulnérabilités.
- Vérifiez que vos règles (Recherche de CI, Affectation) pour l'élément vulnérable fonctionnent comme prévu. Pour plus d'informations sur la révision des règles de recherche de CI, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces. Pour en savoir plus sur les règles d'affectation, reportez-vous à la section Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : En raison du volume important d'importations de données, il convient de veiller à l'affectation automatisée des éléments vulnérables.

- Validez que vos cibles de rattrapage sont correctes. Consultez Réponse aux vulnérabilités Règles de cibles de rattrapage pour en savoir plus sur le fonctionnement des règles de cibles de rattrapage et sur la manière de les réviser.
- Affichez les éléments vulnérables non groupés.
  - En examinant les éléments vulnérables dissociés, envisagez de réviser vos règles de groupe et d'effectuer une nouvelle analyse. Consultez Créer ou modifier des Réponse aux vulnérabilités règles de tâche de rattrapage pour plus d'informations.
  - Regroupez manuellement les éléments vulnérables. Créer manuellement une tâche de rattrapage dans Réponse aux vulnérabilités pour plus d'informations.
  - Révisez les scores de risque pour les éléments vulnérables dans vos tâches de rattrapage. Consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité pour plus d'informations.
  - Fermez les éléments vulnérables plus anciens qui n'ont pas été détectés récemment par vos intégrations tierces. Consultez Fermeture automatique des éléments vulnérables et des détections pour plus d'informations.
- Afficher et reclasser les éléments de configuration sans correspondance.
- Recherchez ce qui doit être fait pour y remédier.

  Cette étape peut inclure :

  - Déterminez ce qu'il faut traiter maintenant et ce que vous pouvez différer. Cette détermination est souvent basée sur le score de risque, les systèmes affectés et les correctifs avec des fenêtres de changement.

    Remarque : Les règles de cibles de rattrapage appartiennent aux éléments vulnérables. Ces règles sont exécutées lorsque l'élément vulnérable est importé. Ces règles ont été créées précédemment dans l'assistant de configuration.

  - Actualisez les éléments vulnérables, si nécessaire, et Afficher l'état de la cible de rattrapage d'un Réponse aux vulnérabilités élément vulnérable.
  - Créez une **demande de changement** et affectez la tâche de rattrapage à un groupe d'affectation (Opérations IT) pour le rattrapage.

    Remarque : Si la vulnérabilité constitue un incident de sécurité et que le module d'extension Réponse aux incidents de sécurité (com.snc.security_incident) est activé, vous pouvez plutôt créer des enregistrements d'incidents de sécurité à partir des tâches de rattrapage.

  - Après avoir soumis une ou plusieurs demandes de changement, passez l'état du groupe à En cours d'examen.

Modifier des éléments vulnérables en bloc dans Réponse aux vulnérabilités

Modifiez les éléments vulnérables en bloc pour gagner du temps en sélectionnant des champs et en exécutant une tâche de modification en bloc asynchrone en arrière-plan.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Important : La fonction de modification en bloc est disponible pour les éléments vulnérables d'hôte dans le Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Utilisation de la modification en bloc dans le Espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Vulnérabilités** > **Éléments vulnérables**.
2. Sélectionnez les éléments vulnérables en effectuant l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Uniquement les éléments sélectionnés** dans le #unique_154_Connect_42_entry-be-record-selection champ.
   - Appliquez des filtres si vous souhaitez utiliser l'option de **filtre Tous les éléments vulnérables qui correspondent** au #unique_154_Connect_42_entry-be-record-selection champ .
3. Sélectionnez le bouton **Modifier en bloc** .
4. Renseignez les champs de la fenêtre modale Modifier en bloc.

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ○ Uniquement les éléments vulnérables sélectionnés ○ Tous les éléments vulnérables qui correspondent au filtre ○ Tâche de rattrapage ○ Entrée de vulnérabilité
État	Changement de **l'état** de l'élément vulnérable. Les choix possibles sont les suivants : ○ Ne pas mettre à jour ○ Ouvert ○ En cours d'examen ○ En attente d'implémentation ○ Différé **Remarque :** ▪ Lorsque vous sélectionnez cette option, les champs Motif, Description brève, Jusqu'à et Informations supplémentaires s'affichent. ▪ Lorsque vous différez des VIT, une tâche de rattrapage est créée et cette tâche est envoyée pour approbation. ○ Fermé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ▪ Lorsque vous sélectionnez cette option pour marquer les enregistrements comme faux positifs, les champs Motif, Description brève, Jusqu'à et Informations supplémentaires s'affichent. ▪ Lorsque vous marquez les enregistrements comme faux positifs, une tâche de rattrapage est créée et cette tâche est envoyée pour approbation. ○ Résolu
Solution privilégiée	Solution ciblée pour corriger tous les éléments vulnérables sélectionnés pour une modification en bloc. Sélectionnez le changement pour le champ **Solution privilégiée** dans l'élément vulnérable (VIT). Les choix proviennent d'une liste de recherche de solutions privilégiées disponibles pour les VIT sélectionnés. **Remarque :** ○ L'ensemble des solutions privilégiées disponibles est une intersection de toutes les solutions potentielles des vulnérabilités dans tous les VIT sélectionnés. ○ Lors de la sélection de **Sélection d'enregistrement** > **Entrée de vulnérabilité** pour une modification en bloc, tous les VIT pour la vulnérabilité seront définis sur la solution privilégiée sélectionnée. **Remarque :** Cette opération ne définit pas la **solution privilégiée** au niveau d'entrée de vulnérabilité. Définir la **solution privilégiée** au niveau d'entrée de vulnérabilité définirait la **solution privilégiée** pour tous les nouveaux VIT à l'avenir. La modification en bloc ne modifie que l'ensemble actuel des VIT. ○ Les vulnérabilités distinctes dans les critères de sélection sont limitées à 500. S'il existe plus de 500 vulnérabilités distinctes, un message d'avertissement s'affiche vous demandant de sélectionner des VIT avec des critères différents pour définir la **solution privilégiée**. ○ Le nombre total de solutions pouvant être affichées dans la liste de recherche est limité à 170. S'il y a plus de 170 solutions, un message d'avertissement s'affiche. La valeur mise à jour est affichée dans la vue de liste Élément vulnérable.
Correctif préféré	Correctif destiné à corriger tous les éléments de vulnérabilité sélectionnés pour une modification en bloc.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ◦ Vous devez installer Patch Orchestration pour afficher la liste des correctifs préférés. ◦ L'ensemble des correctifs préférés disponibles est une intersection de tous les correctifs potentiels dans tous les VIT sélectionnés. ◦ Les vulnérabilités distinctes dans les critères de sélection sont limitées à 500. S'il existe plus de 500 vulnérabilités distinctes, un message d'avertissement s'affiche vous demandant de sélectionner des VIT avec des critères différents pour définir le **correctif préféré**. ◦ Le nombre total de correctifs pouvant être affichés dans la liste de recherche est limité à 170. S'il y a plus de 170 correctifs, un message d'avertissement s'affiche.
Motif	Motif du report des enregistrements : ◦ En attente de fenêtre de maintenance ◦ Correctif non disponible ◦ Risque accepté ◦ Contrôle d'atténuation en place ◦ Autre Motif de la fermeture des dossiers : ◦ Faux positif **Remarque :** ▪ Lorsque vous sélectionnez cette option, les champs Description brève, Jusqu'à et Informations supplémentaires s'affichent. ▪ Une tâche de rattrapage est créée lorsque vous marquez les enregistrements comme faux positifs et que cette tâche est envoyée pour approbation. ◦ Annulé ◦ Fixe **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé ou Fermé.
Description brève	Brève note décrivant le motif du report et des demandes fermées-faux positifs. Ces informations sont reflétées dans le champ Description de la tâche de rattrapage créée pour les demandes de report et de faux positifs fermés. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé et Fermé-Faux positif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Jusqu'à	Date jusqu'à laquelle l'enregistrement reste reporté. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé.
Informations supplémentaires	Toute autre information nécessaire. Ces informations sont reflétées dans le champ Informations supplémentaires de l'onglet Vue d'ensemble. Si votre demande de report est approuvée, ces informations supplémentaires apparaissent sous forme de notes de report dans la VIT et la tâche de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé et Fermé-Faux positif.
Annuler l'affectation	Tous les éléments sélectionnés sont désaffectés pour le groupe d'affectation et le propriétaire du rattrapage. Pour plus d'informations sur la façon dont un propriétaire de rattrapage peut supprimer les affectations des éléments vulnérables, consultez Supprimer les affectations des éléments vulnérables pour vous ou vos groupes. **Remarque :** ○ Ce champ s'affiche lorsque vous sélectionnez l'état Ne pas mettre à jour. ○ Lorsque vous annulez l'affectation d'enregistrements, une tâche de rattrapage est créée et cette tâche est envoyée pour approbation.
Groupe d'affectation	Groupe d'affectation pour le VIT. Sélectionnez manuellement ou utilisez les recommandations d'affectation si cette option est activée. **Remarque :** Ce champ est désactivé lorsque vous cochez la case **Annuler l'affectation** .
Notes de travail	Texte que vous saisissez pour décrire les changements.

5. Sélectionnez **OK**.
   Une tâche de modification en bloc asynchrone met à jour les enregistrements sélectionnés. Le numéro de la tâche avec un lien s'affiche sur la page Éléments vulnérables où vous pouvez consulter son état. Une tâche de rattrapage est créée avec les éléments vulnérables sélectionnés lorsque vous différez, annulez l'affectation ou fermez des éléments vulnérables (faux positifs) en bloc. Et cette tâche de rattrapage est envoyée pour approbation.

Éléments vulnérables dégroupés Réponse aux vulnérabilités

Les éléments vulnérables sont automatiquement affectés à une tâche de rattrapage lorsqu'ils sont importés. Cependant, parfois, si un élément vulnérable (VI) est créé manuellement, par exemple, le VI peut devenir orphelin. Le module **Élément vulnérable dégroupé répertorie** les éléments vulnérables sans groupe.

Remarque : Les processus automatisés d'intégration ne créent pas d'orphelins, c'est pourquoi ce cas d'utilisation est censé être petit.

La dissociation se produit si un élément vulnérable a été créé sans vulnérabilité, ou s'il n'existe aucune règle de tâche de rattrapage qui affecte le VI à un groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans ce cas, passez en revue la liste des éléments vulnérables dégroupés en accédant à **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Dégroupés**.

Après vérification, vos choix sont les suivants :

- Vous pouvez Créer ou modifier des Réponse aux vulnérabilités règles de tâche de rattrapage récupérer tous les éléments qui apparaissent sur cette liste.
- Vous pouvez Créer manuellement une tâche de rattrapage dans Réponse aux vulnérabilités ajouter manuellement des éléments de cette liste au groupe ou définir une condition qui correspond à ces éléments.
- Vous pouvez ouvrir une tâche de rattrapage existante et ajouter tous les éléments vulnérables pertinents au groupe tant qu'il est à l'état Ouvert ou En cours d'examen.

Remarque : Les éléments vulnérables ajoutés manuellement ne sont pas automatiquement supprimés des tâches de rattrapage par les règles de tâche de rattrapage ou les conditions de groupe.

Pour plus d'informations sur le comportement des tâches de rattrapage et des règles de tâche, reportez-vous à la section Réponse aux vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage.

Afficher les éléments vulnérables non groupés Réponse aux vulnérabilités

Les éléments vulnérables qui ne sont pas affectés à un groupe sont placés dans une liste consultable.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Vulnérabilités** > **Éléments vulnérables dégroupés**.
2. Examinez les éléments vulnérables de la liste.
3. Cliquez sur chaque élément vulnérable pour l'afficher et déterminer comment l'inclure dans un groupe.

Ajouter manuellement un élément vulnérable à une tâche de rattrapage

Si un élément vulnérable n'est pas dissocié, vous pouvez l'ajouter à une tâche de rattrapage.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Enregistrez le nombre vulnérable.
2. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
3. Choisissez une tâche de rattrapage (VUL) pour votre élément vulnérable.
4. Sélectionnez **Modifier** en bas à droite.
5. Saisissez le numéro de **l'élément vulnérable** dans le champ de recherche Collecte.
6. Sélectionnez l'élément vulnérable dans la collection et ajoutez-le à la liste.
7. Cliquez sur **Enregistrer**.

Supprimer les affectations des éléments vulnérables et des tâches de rattrapage

Effacez les champs **Affecté à** et **Groupe d'affectation** des enregistrements d'éléments vulnérables dans les Réponse aux vulnérabilités applications , Réponse aux vulnérabilités des applications et Réponse aux vulnérabilités pour conteneurs .

Avant de commencer

Rôles requis :

- sn_vul.remediation_owner ou sn_vul.vulnerability_analyst pour les éléments vulnérables (VIT) et les tâches de rattrapage (VUL).
- sn_vul.app_sec_manager pour Réponse aux vulnérabilités des applications les éléments vulnérables (AVIT) et les tâches de rattrapage (AVUL).
- sn_vul_container.remediation_owner ou sn_vul_container.vulnerability_analyst pour les éléments vulnérables (CVIT) et les tâches de rattrapage (CVUL) de conteneurs.

Pourquoi et quand exécuter cette tâche

L'action d'interface utilisateur **Annuler l'affectation** est prise en charge à la fois dans l'environnement classique et dans les espaces de travail pour les enregistrements suivants, quel que soit l'état Fermé ou Résolu :

- Tâches de rattrapage (VUL, AVUL ET CVUL). Si une tâche de rattrapage est mise à jour avec cette fonctionnalité, les champs **Affecté à** et **Groupe d'affectation** de tous ses VIT associés qui ont le même groupe d'affectation sont également effacés.
- Éléments vulnérables (VIT).
- Éléments vulnérables de l'application (AVIT).
- Éléments vulnérables de conteneurs (CVIT).

Important : Vous pouvez annuler l'affectation d'éléments vulnérables d'hôte en bloc dans le Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Utilisation de la modification en bloc dans le Espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Dans l'environnement classique ou dans l'espace de travail du propriétaire de rattrapage informatique, accédez à un enregistrement d'élément vulnérable (VIT) qui vous est affecté et dont l'état n'est pas Fermé ou Résolu.
2. Pour effacer les champs **Affecté à** et **Groupe d'affectation** de la vue classique, sélectionnez **Annuler l'affectation** en haut de l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Vous pouvez également accéder à l'enregistrement d'un élément vulnérable (VIT, AVIT ou CVIT) dans l'espace de travail Rattrapage informatique qui vous est affecté ou à vos groupes, puis cliquer sur **Annuler l'affectation** dans le menu Autres options () pour effacer les champs d'affectation.
4. Pour les enregistrements de tâches de rattrapage dans l'espace de travail qui sont affectés à vous ou à vos groupes, ouvrez un enregistrement et sélectionnez **Annuler l'affectation** dans le menu Autres options () pour effacer les champs d'affectation.
5. Dans la boîte de dialogue Annuler l'affectation pour les éléments vulnérables et les tâches de rattrapage, fournissez des notes de travail et sélectionnez **Soumettre**.
   La demande d'approbation de changement d'état est soumise pour approbation.

   Remarque : Pour les tâches de rattrapage, vous êtes informé que les champs **Affecté à** et **Groupe d'affectation** de tous les VIT associés à une tâche de rattrapage sont également effacés.

   Une fois que la demande d'effacement des champs est approuvée pour une tâche de rattrapage, tous les champs **Affecté à** et **Groupe d'affectation** de ses éléments vulnérables qui ont le même groupe d'affectation sont également désaffectés. Si un élément vulnérable a un groupe d'affectation différent de celui de sa tâche de rattrapage associée, il n'est pas désaffecté. Dans la plupart des cas, ces éléments vulnérables ont été affectés manuellement.

6. Affichez les informations suivantes :
   - Les notes de travail que vous avez fournies s'affichent dans la section Notes.
   - Dans l'onglet **Approbation de changement d'état** , l'enregistrement de l'approbation de changement d'état s'affiche avec l'état En cours de révision, ce qui aide à suivre le workflow d'approbation.
   - Sous l'onglet **Approbations demandées** , votre demande de suppression de vous ou de votre groupe d'affectation s'affiche à l'état Demandé.

Résultats

La demande est approuvée à l'aide d'un workflow d'approbation unique par défaut. Pour plus d'informations, consultez Approuver ou rejeter une demande de désaffectation dans Réponse aux vulnérabilités.

- Si votre demande est approuvée, l'enregistrement d'approbation du changement d'état et l'enregistrement de l'approbation demandée passent à l'état Approuvé. Vos groupes et vous êtes retirés des champs **Affecté à** et **Groupe d'affectation** . Non affecté s'affiche dans le champ **Type d'affectation** , et la tâche de rattrapage et les VIT sont affichés dans la liste du module Non affecté pour chaque produit.

  Les notifications indiquant que des enregistrements ne sont pas affectés sont envoyées automatiquement aux gestionnaires de vulnérabilité ou aux analystes du groupe de notification Annuler l'affectation. Pour configurer le marqueur d'approbation, les notifications et le groupe d'affectation par défaut, consultez Suppression des affectations des éléments vulnérables et des tâches de rattrapage.

- Si votre demande est rejetée, l'état de l'enregistrement de l'approbation des changements et de l'enregistrement de l'approbation demandée passe à l'état Rejeté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : En tant qu'administrateur de vulnérabilités, vous pouvez définir la *sn_vul.unassign_vr.approval_required* propriété système sur **false** pour désactiver le processus d'approbation.

Que faire ensuite

Accédez aux modules non affectés pour les applications andRéponse aux vulnérabilités des applications Réponse aux vulnérabilités pour conteneurs, surveillez les enregistrements non affectés à la recherche d'éléments susceptibles d'entrer Réponse aux vulnérabilités dans votre champ d'application et réaffectez-les à vous-même.

Approuver ou rejeter une demande de désaffectation dans Réponse aux vulnérabilités

Approuvez les demandes de suppression d'éléments vulnérables d'un groupe d'affectation ou d'un utilisateur individuel dans l'application Réponse aux vulnérabilités .

Avant de commencer

Rôle requis : pour les approbations non affectées, un approbateur est requis dans le groupe Approbateur de niveau 1.

- sn_vul.unassign_approver pour AVIT et VIT
- sn_vul_container.unassign_approver pour CVIT

Pourquoi et quand exécuter cette tâche

Par défaut, une configuration d'approbation est fournie et un groupe d'approbation de désaffectation est créé. Les utilisateurs du groupe Annuler l'affectation de l'approbateur - Niveau 1 peuvent approuver la demande. Ce groupe contient un rôle d'approbateur de désaffectation, sn_vul.unassign_approver, par défaut. Vous pouvez modifier ou créer un nouveau groupe et mettre à jour la configuration de l'approbation. Pour configurer une règle d'approbation, sélectionnez l'une des règles d'approbation suivantes dans le module Règles d'approbation et accédez à la configuration de l'approbation dans l'onglet **Configurations d'approbation** :

- *Vulnerable item field change request* pour un élément vulnérable.
- *Vulnerability field change request* pour une tâche de rattrapage.
- *Application vulnerability field change request* pour un élément vulnérable de l'application (AVIT).
- *Approval for container management* pour un élément vulnérable de conteneur (CVIT).

Pour plus d'informations sur les règles d'approbation et les configurations, reportez-vous à la section Configurations de workflow d'approbation pour la demande de désaffectation.

Important : Vous pouvez approuver ou rejeter des demandes dans le Espace de travail du gestionnaire de vulnérabilités. .

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Mes approbations** pour les VIT et les AVIT. Vous pouvez également accéder à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Mes approbations** pour les CVIT.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande en ajoutant les commentaires appropriés.

Fermeture automatique des éléments vulnérables et des détections

Vous pouvez fermer automatiquement les détections périmées et les éléments vulnérables (VI) associés à des CI hors service à l'aide du module Règles de fermeture automatique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez fermer automatiquement les détections périmées et les VI dans les scénarios suivants :

- Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités
- Fermer automatiquement les éléments vulnérables associés aux CI hors service

Pour plus d'informations sur l'utilisation d'éléments de configuration mis hors service, reportez-vous aux sections Utiliser des éléments de configuration mis hors service et Créer des règles de fermeture automatique.

Utiliser des éléments de configuration mis hors service

Les éléments de configuration (CI) désactivés passent à l'état Mis hors service, Archivé ou Supprimé dans le Base de données de gestion des configurations (CMDB). Réponse aux vulnérabilités contient des éléments vulnérables (VI) qui sont constitués de CI. Lorsque l'état d'un CI est mis à jour sur Hors service, les VI associés sont fermés avec le sous-état « CI désactivé ».

Remarque : À partir de la version 25.0.3 de , une nouvelle règle de Réponse aux vulnérabilités fermeture automatique « CI désactivé » est introduite pour fermer les éléments vulnérables et les détections associés aux CI désactivés.

Si la CMDB modifie l'état de l'étape du cycle de vie d'un CI en mis hors service, vous pouvez choisir de fermer automatiquement les VI associés. Pour plus d'informations sur la fermeture automatique des VI associés, reportez-vous à la section Fermer automatiquement les éléments vulnérables associés aux CI hors service.

Le CI mis hors service est finalement archivé ou définitivement supprimé du CMDB.

Impact de la mise hors service des CI :

- **Impact sur les éléments découverts :** Lorsque le CI est mis hors service, l'élément détecté (DI) connexe est marqué comme « CI désactivé ».
- **Impact sur les éléments vulnérables :** Lorsque l'état d'un élément de données est mis à jour sur « CI désactivé », l'élément vulnérable associé est fermé et la section Notes est automatiquement mise à jour.

  Remarque : L'état d'un élément de données est automatiquement mis à jour sur « CI désactivé » à chaque fois que l'état du cycle de vie d'un CI est mis à jour. D'autre part, l'état d'un VI est mis à jour sur Fermé uniquement lorsque **l'option Fermer automatiquement les VI liés aux CI hors service** est activée. Pour plus d'informations sur la fermeture automatique des VI associés, reportez-vous à la section Fermer automatiquement les éléments vulnérables associés aux CI hors service.

La tâche *`Close detections/VIs for decommissioned CIs`* planifiée est exécutée quotidiennement pour les éléments de données mis à jour. Si l'option de configuration de fermeture automatique est activée pour les CI hors service, elle identifie le DI contenant un CI désactivé et ferme le VI connexe avec le sous-état « CI désactivé ». Si tous les VI d'une tâche de rattrapage sont fermés et que leur sous-état est CI désactivé, la tâche de rattrapage est également fermée avec le sous-état « Annulé ». Pour afficher les VI mis hors service, accédez à **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Désactivé**.

Remarque : Si un CI revient à l'état d'origine à partir de l'état « Mis hors service », l'entrée « Éléments détectés » est également mise à jour. Les VI sont automatiquement ouverts lorsque les données sont à nouveau ingérées à partir du scanner.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fermer automatiquement les éléments vulnérables associés aux CI hors service

Si l'émetteur Base de données de gestion des configurations (CMDB) modifie l'état de l'étape du cycle de vie d'un élément de configuration (CI) sur mis hors service, vous pouvez choisir de fermer automatiquement les éléments vulnérables (VI) et les détections associés.

Avant de commencer
Rôle requis : sn_vul.admin

Pourquoi et quand exécuter cette tâche
À partir de la version 22.0 de Réponse aux vulnérabilités, pour fermer automatiquement les VI et détections associés, vous devez activer la propriété *sn_vul_cmn.auto_close_vis_linked_retired_cis* système pour fermer automatiquement les VI associés aux CI mis hors service. Pour activer l'option, définissez le champ Valeur sur « 1 ». Inversement, pour désactiver l'option, définissez le champ Valeur sur « 0 ».

Lors d'une mise à niveau, si la propriété *sn_vul_cmn.auto_close_vis_linked_retired_cis* système est sélectionnée dans la version 21.0 de Réponse aux vulnérabilités, la valeur reste « 1 ». Lorsque cette option est activée, tous les VI et détections, nouveaux ou existants, signalés pour le même CI sont automatiquement créés ou mis à jour avec l'état « Fermé ». Ceci est basé sur l'ID d'actif dans la charge utile du scanner et sur l'état de l'entrée Éléments détectés. Pour plus d'informations sur l'impact des CI mis hors service, voir Utiliser des éléments de configuration mis hors service

.

Remarque :

- L'état d'un élément de données est mis à jour sur « CI désactivé » chaque fois que l'état du cycle de vie d'un CI est mis à jour. D'autre part, l'état d'un VI est mis à jour sur Fermé uniquement lorsque **l'option Fermer automatiquement les VI liés aux CI hors service** est activée.
- Les informations fournies dans la procédure suivante ne s'appliquent qu'aux versions antérieures à la v22.0 de Réponse aux vulnérabilités. À partir de la version 22.0 de , vous avez la possibilité de Réponse aux vulnérabilités configurer des options de recherche supplémentaires. Consultez Créer des règles de fermeture automatique pour plus d'informations.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Configuration de fermeture automatique** > **Cycle de vie de l'élément de configuration**.
2. Pour fermer automatiquement les éléments vulnérables associés aux CI hors service, cochez la case **Fermer automatiquement les VI liés aux CI hors service** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **Mettre à jour**.

> **Remarque :** Si un CI est déjà mis hors service avant que l'option **Fermer automatiquement les VI liés aux CI hors service** ne soit activée, les VI sont créés uniquement pour les nouvelles détections à partir des scanners. L'état de ces VI est Fermé et le sous-état est CI désactivé.
>
> Vous ne pouvez pas rouvrir manuellement les VI dont l'état est CI désactivé, à l'aide des options **Rouvrir** ou **Modifier en bloc** .
>
> Les VI fermés avec un sous-état fixe ou périmé sont rouverts si une nouvelle détection est créée et que les VI peuvent être mis en correspondance avec la nouvelle vulnérabilité. Consultez Détections, tâches de rattrapage et états des éléments vulnérables pour plus d'informations.

Fermeture des détections obsolètes dans Réponse aux vulnérabilités

Le module Fermer automatiquement les détections périmées vous aide à nettoyer automatiquement les détections vulnérables anciennes et périmées qui n'ont pas été trouvées récemment par vos intégrations tierces. Le déplacement de ces détections vers Fermé réduit le nombre d'éléments vulnérables actifs et de tâches de rattrapage dans votre ServiceNow AI Platform instance et vous aide à rapprocher les actifs dans votre CMDB.

Vue d'ensemble et termes clés

Afin de déployer plus précisément les données de détection sur vos éléments vulnérables, le module Fermer automatiquement les détections d'éléments vulnérables périmées vous aide à nettoyer les détections d'éléments vulnérables anciennes et périmées qui n'ont pas été trouvées récemment par vos intégrations tierces. Pour plus d'informations sur cette fonctionnalité, consultez le cas d'utilisation ci-dessous.

Dans les versions précédentes de , le module Fermer Réponse aux vulnérabilités automatiquement les éléments vulnérables faisait automatiquement passer les éléments vulnérables qui n'avaient pas été trouvés récemment ou mis à jour par vos intégrations d'analyseurs tiers à l'état Fermé - Périmé.

Avant d'activer la fonctionnalité Fermer automatiquement les détections périmées, examinez les termes suivants, la manière dont les états se déploient pour les éléments vulnérables et les tâches de rattrapage, ainsi que les prérequis pour vos intégrations tierces qui importent des données de détection.

Pour activer cette fonctionnalité, reportez-vous à la section Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités.

Termes clés

Détections périmées

Désigne les détections associées aux éléments vulnérables de votre ServiceNow AI Platform® instance qui sont vieillies et n'ont pas été trouvées, mises à jour ou détectées par des analyses d'intégration tierces depuis une période significative.

Dernières détections trouvées

Cette option de recherche utilise une date et une heure fournies par le scanner tiers. Ce terme fait référence à la date et à l'heure les plus récentes ou les plus récentes auxquelles les détections ont été retrouvées par le scanner.

Derniers actifs numérisés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette option de recherche utilise une date et une heure fournies par le scanner tiers. Ce terme désigne la date et l'heure les plus récentes auxquelles un actif a été analysé pour la dernière fois par un scanner tiers.

Cas d'utilisation

Parfois, les actifs (éléments de configuration) peuvent être mis hors service dans votre environnement ou purgés par des scanners tiers, et leurs détections associées ne sont pas mises à jour par les détections d'éléments vulnérables. Par conséquent, les détections et leurs éléments vulnérables connexes ne sont pas mis à jour dans l'application Réponse aux vulnérabilités et deviennent inactifs (périmés).

Pour fermer ces détections âgées qui ont des données d'élément vulnérable inchangées et ensuite réduire le nombre de VI actifs et de tâches de rattrapage (RT), activez Fermer automatiquement les détections périmées. Cette fonctionnalité ferme automatiquement les détections d'éléments vulnérables qui n'ont pas été trouvées ou mises à jour récemment par vos intégrations d'analyseurs tiers en fonction des critères de recherche et d'un âge en nombre de jours que vous définissez.

Par exemple, supposons qu'un élément de configuration (CI) particulier possède plusieurs ID d'actifs et que l'un de ces ID n'a pas été importé sur une détection à partir d'un scanner tiers au cours des 90 derniers jours. Cette fonctionnalité ferme automatiquement cette détection qui n'a pas de nouvelles données de vulnérabilité afin que le VI associé puisse être fermé.

Étant donné qu'un VI peut être associé à plusieurs détections, cette fonctionnalité ne fait que passer les détections jugées périmées par les paramètres que vous avez définis. Par exemple, si quatre détections sont associées à un VI et que deux détections sont périmées, c'est-à-dire qu'aucune nouvelle donnée de vulnérabilité n'a été importée au cours des 90 derniers jours, cette fonctionnalité ferme uniquement les détections périmées. Pour pouvoir fermer le VI, vous devez d'abord corriger les deux autres détections ouvertes.

Déploiement des états de détection sur les VI

Pour différencier les détections fermées automatiquement des détections fermées par des scanners tiers, une nouvelle valeur pour le champ État, Périmé, a été ajoutée. Les valeurs possibles pour ce champ sont Ouvert, Fermé et Périmé. Périmé indique qu'une détection a été fermée par la fonction de détection de fermeture automatique.

Priorité d'État : Ouvert > Fermé > Périmé.

1. Si des détections sont ouvertes, l'état du VI associé reste ouvert.
2. Si aucune détection n'est ouverte, certaines sont fermées et d'autres sont périmées, l'état du VI associé passe à l'état Fermé - Corrigé.
3. Si toutes les détections sont périmées, l'état du VI associé passe à Fermé - Périmé.

À partir de Réponse aux vulnérabilités la version 20.0, si la détection est périmée et que son VI associé est à l'état Fermé, l'état du VI ne passe pas à l'état Fermé - Périmé. Cela permet d'éviter que le VI ne se rouvre lorsqu'une nouvelle détection est identifiée afin que vous puissiez éviter de passer par l'ensemble du processus de demande et d'approbation de faux positif. Pour inverser ce comportement, décochez la case **Ignorer les détections obsolètes pour les VI fermés** dans le formulaire Configuration de fermeture automatique. Pour plus d'informations, consultez Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déploiement des états des VI sur les tâches de remédiation (VUL)

Priorité d'État : Ouvert > Fermé : Corrigé > Fermé : Périmé.

1. Si des VI dans une VUL (tâche de rattrapage) sont ouverts, l'état de la VUL n'est pas modifié.
2. Si au moins un VI est Fermé - Corrigé et que les autres sont Fermé - Périmé, l'état de la VUL passe à Fermé - Corrigé.
3. Si tous les VI d'une VUL sont Fermé - Périmé, l'état de la VUL passe à Fermé - Annulé.
4. Si des VI sont fermés comme Fermés – Faux positif, la VUL ne se ferme pas automatiquement.

Pour plus d'informations sur les scénarios de déploiement et de déploiement d'état, reportez-vous à la section Scénarios de déploiement et de réduction de l'état.

Détection de fermeture automatique et exigences d'intégration tierce

Utilisateurs Microsoft TVM et fermeture automatique des détections obsolètes

Élément de liste de vérification	Description
L'intégration de vulnérabilité Microsoft TVM	Avec Microsoft TVM Vulnerability Integration, si vous sélectionnez **les dernières détections trouvées** pour baser votre recherche, cette fonctionnalité nécessite une exécution réussie de l'intégration des vulnérabilités de la machine Microsoft TVM (importation complète) au cours des sept derniers jours. Cette intégration a lieu chaque semaine. Si la fermeture automatique des détections périmées est activée et configurée pour **les dernières détections trouvées**, et que l'intégration des vulnérabilités des ordinateurs Microsoft TVM est désactivée ou qu'une importation de données n'est pas effectuée avec succès au cours des sept derniers jours, la tâche planifiée de fermeture des détections s'exécute toujours quotidiennement, mais certaines détections périmées peuvent ne pas être fermées comme prévu. Si vous sélectionnez **Derniers actifs numérisés** pour baser votre recherche, l'exécution de l'intégration des vulnérabilités de la machine Microsoft TVM n'est pas requise. Pour activer cette intégration : 1. Accédez à la **Intégration de vulnérabilité Microsoft TVM** > **Administration** > **Intégration**. 2. Localisez et activez **l'intégration des vulnérabilités de la machine Microsoft TVM (importation complète).**
(Facultatif) Déployez plusieurs instances des intégrations Microsoft TVM dans votre environnement.	Vous pouvez éventuellement déployer plusieurs instances des intégrations dans votre environnement. La fermeture automatique des détections périmées n'est pas spécifique à l'instance et est activée ou désactivée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément de liste de vérification	Description
	dans votre environnement. Les détections périmées passent automatiquement à l'état Périmé sur les instances dont l'exécution de l'intégration s'est terminée avec succès. Si la fermeture automatique des détections périmées est activée et que vous désactivez les intégrations qui s'exécutent chaque semaine dans une instance, la tâche planifiée de fermeture des détections s'exécute toujours quotidiennement, mais certaines détections peuvent ne pas passer automatiquement à l'état périmé comme prévu.

Qualys utilisateurs et Fermer automatiquement les éléments vulnérables périmés

- Toutes les intégrations tierces activées Qualys qui récupèrent des données de détection peuvent s'exécuter avec ce module. Aucune application spécifique Qualys n'est requise.
- Vous pouvez éventuellement déployer plusieurs instances des Qualys intégrations dans votre environnement.
- La fermeture automatique des détections périmées n'est pas spécifique à l'instance et est activée ou désactivée dans votre environnement. Les détections périmées passent automatiquement à l'état Périmé sur toutes les instances.

Rapid7 utilisateurs et fermer automatiquement les détections obsolètes

Élément de liste de vérification	Description
L'intégration Rapid7 de vulnérabilité	Si vous sélectionnez **Dernières détections trouvées** pour baser votre recherche, cette fonctionnalité nécessite une exécution réussie de l'une Rapid7 des intégrations complètes d'éléments vulnérables au cours des sept derniers jours. Ces intégrations complètes s'exécutent chaque semaine : • Pour Rapid7 Nexpose l'entrepôt de données, une exécution réussie à partir de l'intégration Rapid7 complète des éléments vulnérables est requise. • Pour Rapid7 InsightVM, une exécution réussie de l'API d'intégration Rapid7 complète des éléments vulnérables est requise. Si la fermeture automatique des détections périmées est activée et configurée pour **les dernières détections trouvées**, et que les intégrations complètes d'éléments Rapid7 vulnérables sont désactivées, ou qu'une importation de données n'est pas effectuée avec succès au cours des sept derniers jours, la tâche planifiée de fermeture des détections s'exécute toujours quotidiennement, mais certaines détections périmées peuvent ne pas être fermées comme prévu. Si vous sélectionnez **la dernière numérisation des actifs** pour baser votre recherche, aucune exécution d'intégration complète Rapid7 n'est requise. Pour activer ces intégrations :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Élément de liste de vérification	Description
	1. Accédez à la **Rapid7 Vulnerability Integration** > **Administration** > **Intégration**. 2. Localisez et activez l'intégration Rapid7 complète des éléments vulnérables dont vous avez besoin. **Remarque :** Outre ces intégrations qui s'exécutent chaque semaine et Rapid7 InsightVM qui ont chacune des intégrations de VI qui s'exécutent quotidiennement, Rapid7 Nexpose l'intégration d'éléments vulnérables Rapid7 et l'API d'intégration d'éléments vulnérables Rapid7. Si les intégrations quotidienne et hebdomadaire Rapid7 sont activées, une seule intégration s'exécute à la fois. Si l'une de ces tâches d'intégration est en cours d'exécution, la tâche de l'autre intégration est ignorée jusqu'à la prochaine tâche planifiée.
(Facultatif) Déployez plusieurs instances des Rapid7 intégrations dans votre environnement.	Vous pouvez éventuellement déployer plusieurs instances des intégrations complètes dans votre environnement. La fermeture automatique des détections périmées n'est pas spécifique à l'instance et est activée ou désactivée dans votre environnement. Les détections périmées passent automatiquement à l'état Périmé sur les instances dont l'exécution de l'intégration s'est terminée avec succès. Si la fermeture automatique des détections périmées est activée et que vous désactivez les intégrations qui s'exécutent chaque semaine dans une instance, la tâche planifiée de fermeture des détections s'exécute toujours quotidiennement, mais certaines détections peuvent ne pas passer automatiquement à l'état Périmé comme prévu.

Utilisateurs d'intégration de vulnérabilité Tenable et fermeture automatique des éléments vulnérables périmés

- Toutes les intégrations activées à partir de l'intégration de vulnérabilité Tenable qui récupèrent des données de détection peuvent s'exécuter avec ce module. Aucune intégration de vulnérabilité Tenable spécifique n'est requise.
- Vous pouvez éventuellement déployer plusieurs instances de Tenable Vulnerability Integration dans votre environnement.
- La fermeture automatique des détections périmées n'est pas spécifique à l'instance et est activée ou désactivée dans votre environnement. Les détections périmées passent automatiquement à **l'état Périmé** sur toutes les instances.

Après avoir vérifié que vos intégrations sont correctement configurées, consultez Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités pour activer la fonctionnalité.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mettre à niveau les informations de Fermer automatiquement les éléments vulnérables périmés vers Fermer automatiquement les détections obsolètes

Pour le module Fermer automatiquement les détections périmées, si vous avez précédemment utilisé Fermer automatiquement les éléments vulnérables périmés :

- La valeur du nombre de jours que vous avez saisi pour l'option **Dernière analyse des actifs** à partir de Fermer automatiquement les éléments vulnérables périmés est conservée automatiquement pour la **dernière numérisation des actifs** dans Fermer automatiquement les détections périmées.
- La valeur du nombre de jours que vous avez saisi pour l'option **Derniers éléments vulnérables trouvés** à partir de Fermer automatiquement les éléments vulnérables périmés est conservée automatiquement pour **les dernières détections trouvées** dans Fermer automatiquement les détections périmées.
- Les détections ouvertes existantes avec des éléments vulnérables comme Fermé : périmé passeront à l'état Périmé selon les paramètres de configuration de fermeture automatique lorsque la tâche planifiée s'exécute après la *`Auto-Close Stale Detections`* mise à niveau.

Informations sur le déploiement

- Si un élément vulnérable était fermé - périmé avant la mise à niveau et que toutes ses détections sont marquées comme périmées après la mise à niveau, l'état du VI reste fermé - périmé.
- Si un élément vulnérable était fermé : périmé avant la mise à niveau, et que seules certaines de ses détections sont marquées comme périmées après la mise à niveau et que le reste a été fermé par le scanner, l'élément vulnérable passe à l'état Fermé : corrigé selon la logique de déploiement.

Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités

Activez la fermeture automatique des détections périmées pour fermer automatiquement les détections vulnérables périmées non trouvées récemment par vos intégrations tierces.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vuln.admin (obsolète), ou un responsable des vulnérabilités avec le rôle granulaire sn_vul.manage_auto_close_stale_vi.

Pour plus d'informations sur cette fonctionnalité, les termes clés et toute configuration qui peut être requise pour vos intégrations tierces qui importent des données de détection, voir Fermeture des détections obsolètes dans Réponse aux vulnérabilités pour plus d'informations.

Remarque : Les informations fournies dans la procédure suivante ne s'appliquent qu'aux versions antérieures à la v22.0 de Réponse aux vulnérabilités. À partir de la version 22.0 de , vous avez la possibilité de Réponse aux vulnérabilités configurer des options de recherche supplémentaires. Consultez Créer des règles de fermeture automatique pour plus d'informations.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Administration** > **Configuration de fermeture automatique** > **Détections périmées**.
   Le formulaire Fermer automatiquement la configuration périmée s'affiche.
2. Renseignez les champs.
3. Pour l'option **Fermer automatiquement les détections obsolètes en fonction du** champ, choisissez une option pour votre recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les deux recherches correspondent à l'âge des détections anciennes et périmées en nombre de jours à une date fournie par votre scanner.

Remarque : À partir de la version 22.0 de Réponse aux vulnérabilités, les options **Dernière détection trouvée** et **Dernière ressource numérisée** sont créées sous forme de liste.

- **Dernières détections trouvées**. Cette option recherche la date la plus récente ou la plus récente à laquelle les détections ont été retrouvées par le scanner.

  Remarque : Pour Rapid7 les utilisateurs de Microsoft TVM, un message d'avertissement s'affiche concernant la nécessité d'obtenir des informations de détection actuelles.

  Si vous sélectionnez **Dernières détections trouvées** pour baser votre recherche, cette fonctionnalité nécessite une exécution réussie de l'intégration Rapid7 de l'une des intégrations complètes d'éléments vulnérables au cours des sept derniers jours.

  Si vous sélectionnez **Dernières détections trouvées** pour baser votre recherche, cette fonctionnalité nécessite une exécution réussie de l'intégration des vulnérabilités de la machine Microsoft TVM (importation complète) au cours des sept derniers jours.

- **Derniers actifs analysés**. Cette option recherche la date la plus récente à laquelle un actif a été analysé pour la dernière fois par un scanner tiers.

4. Pour Rapid7 les utilisateurs et Microsoft TVM uniquement, vérifiez que toutes les intégrations requises sont activées.
   Voir Présentation de Intégration des vulnérabilités Rapid7 et Présentation de Microsoft Threat and Vulnerability Management Intégration des vulnérabilités pour plus d'informations.
5. Pour activer le module, cochez la case Actif pour le sélectionner.
6. Dans le champ **Dernières détections trouvées (en jours),** saisissez l'âge des détections anciennes et périmées en nombre de jours.

   La valeur par défaut est de 90 jours. Vous pouvez saisir n'importe quelle valeur positive pour le nombre de jours. Cette valeur est utilisée pour correspondre à une date fournie par votre scanner. Avec 90 et **les dernières détections trouvées** affichées, toutes les détections introuvables au cours des 90 derniers jours sont automatiquement fermées. Lorsque 90 et **la dernière numérisation des actifs sont affichées** , toutes les détections associées à des actifs non analysés au cours des 90 derniers jours sont automatiquement fermées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Il existe une relation entre le champ **Dernières détections trouvées/Dernières ressources numérisées (il y a plusieurs jours)** pour cette fonctionnalité et le champ **Importer depuis** de l'API Intégration complète des éléments vulnérables Rapid7 et l'intégration des vulnérabilités des machines Microsoft TVM.

Pour ces intégrations, le champ **Importer depuis** des pages de configuration est vide par défaut.

Si vous ne saisissez pas de valeur ou si le champ n'en contient pas, les données du nombre de jours configurées dans le champ **Dernières détections trouvées/Dernières ressources numérisées (il y a plusieurs jours)** sont utilisées.

Par exemple, si le nombre de jours défini dans le formulaire de configuration de fermeture automatique est de 90 et que le champ **Importer depuis** est vide sur les pages de configuration de l'intégration, la première exécution de l'intégration importe les données des 90 derniers jours. Les champs **Importer depuis** que l'API Rapid7 et l'intégration des vulnérabilités de la machine Microsoft TVM sont modifiables. Vous pouvez donc également fournir les valeurs que vous voulez. La valeur de 90 jours est fournie par défaut si le champ reste vide afin que la fonctionnalité de fermeture automatique ne ferme pas les faux positifs.

Cette relation entre ces champs ne s'applique qu'à la première exécution d'intégration. Après cela, la modification **du champ Dernières détections trouvées/Dernières ressources numérisées (il y a x jours)** sur le formulaire Fermer automatiquement les détections vulnérables périmées n'affecte pas le champ **Importer depuis** sur les pages de configuration de l'intégration. Le champ est modifié à l'heure de début de la première exécution afin que les exécutions d'intégration suivantes importent uniquement les informations delta.

7. **Facultatif :** Cochez la case **Ignorer les détections obsolètes pour les VI différés** pour ignorer les détections obsolètes qui sont mappées sur les VI différés ou sur les VI actuellement en cours d'examen pour report.

   (Optional) Si vous laissez cette option désactivée, toutes les détections qui correspondent à vos critères seront fermées et mappées aux VI différés ou aux VI en cours d'examen pour report. Les VI différés, ou les VI en cours de révision qui correspondent à ces détections sont également fermés automatiquement en fonction de la logique de déploiement. Pour plus d'informations sur la logique de déploiement, reportez-vous à la section Fermeture des détections obsolètes dans Réponse aux vulnérabilités et Scénarios de déploiement et de réduction de l'état.

   Si vous activez cette option, toutes les détections correspondant à vos critères qui correspondent à des VI différés ou à des VI en cours d'examen pour report sont ignorées lors de la fermeture automatique.

8. **Facultatif :** Décochez la case **Ignorer les détections obsolètes pour les VI fermés** .

   (Optional) Par défaut, cette case est cochée afin que le VI fermé ne soit pas rouvert lorsqu'une nouvelle détection associée à ce VI fermé est identifiée. Pour plus d'informations sur la logique de déploiement, reportez-vous aux sections Fermeture des détections obsolètes dans Réponse aux vulnérabilités et Scénarios de déploiement et de réduction de l'état.

9. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La tâche planifiée *Auto-Close Stale Detections* s'exécute quotidiennement. La tâche détermine si vous avez sélectionné la date à laquelle les détections ont été trouvées pour la dernière fois ou la date à laquelle les actifs ont été analysés pour la dernière fois. Il fait ensuite passer les détections correspondantes à l'état Périmé. Il est important de noter que la fonctionnalité de fermeture automatique de la détection obsolète ne ferme les détections obsolètes que pour les instances d'intégration actives. Les éléments vulnérables et les détections associés aux instances d'intégration actives sont fermés. À partir de Réponse aux vulnérabilités la version 22.0, le travail planifié a été modifié pour prendre en compte la table commune [sn_vul_cmn_auto_close_rule].

Une fois que les détections sont marquées comme périmées, si le scanner signale avoir détecté à nouveau, le champ État des détections passe à Ouvert. Les éléments vulnérables correspondants de la détection sont également rouverts.

En outre, si la détection est marquée comme périmée et que le scanner détecte qu'elle est fixe, la détection passe à l'état Fermé. L'État s'étend également aux VI.

Créer des règles de fermeture automatique

Utilisez les règles de fermeture automatique pour fermer automatiquement les détections plus anciennes en fonction des conditions de filtre que vous définissez.

Avant de commencer

Rôle requis : sn_vul.manage_auto_close_stale_vi

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles de fermeture automatique**.

   Le système de base fournit les règles de fermeture automatique suivantes :

   - **Derniers actifs analysés** : les détections associées aux actifs qui n'ont pas été analysés au cours des 90 derniers jours passent à l'état **Périmé.**
   - **Dernières détections manuelles trouvées** : détections manuelles qui n'ont pas été trouvées au cours des 90 derniers jours. Si vous activez **l'enregistrement des détections du dernier trouvé** , cette fonctionnalité nécessite une exécution réussie de l'intégration des intégrations complètes d'éléments vulnérables et de l'intégration des vulnérabilités des Rapid7 ordinateurs Microsoft TVM (importation complète) au cours des sept derniers jours.
   - **Dernières détections trouvées** : détections qui n'ont pas été trouvées au cours des 90 derniers jours.

2. Sélectionnez **Nouveau** pour créer une nouvelle règle de fermeture automatique.
3. Renseignez les champs du formulaire.

Champ	Valeur
Nom	Nom de la règle de fermeture automatique.
Actif	Option permettant d'activer la règle. Si elle est activée, elle ferme automatiquement toutes les détections correspondant à ses critères de filtre.
Ignorer les éléments différés	Si cette option est sélectionnée, toutes les détections mappées aux états **En cours de révision** ou **Différé** sont ignorées et non fermées. Si

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
	vous décochez cette option, toutes les détections correspondant à vos critères sont fermées.
Ordre d'exécution	Valeur unique pour l'exécution de la règle de fermeture automatique. Cette valeur détermine l'ordre d'exécution. La valeur par défaut est 100.
Description	Description de la règle de fermeture automatique.
Condition	Conditions de filtre utilisées pour identifier les détections qui doivent être fermées.

4. Sélectionnez **Soumettre**.

La tâche planifiée *`Auto-Close Stale Detections`* s'exécute quotidiennement. Il identifie les détections en fonction des conditions spécifiées et fait passer celles qui correspondent à l'état **Périmé.** Le travail gère les scénarios suivants :

- Si toutes les détections au sein d'un élément vulnérable (VIT) sont marquées comme périmées, le VIT est fermé avec le sous-état défini sur « Périmé ».
- Si au moins une détection reste ouverte dans un VIT, tandis que d'autres sont à l'état Périmé, le VIT reste ouvert.
- Dans les cas où il y a des détections avec des statuts « Fermé » et « Périmé » dans un VIT, le VIT est fermé avec le sous-état défini sur « Fixe ».

Lorsque vous effectuez une mise à niveau vers la dernière version de , les conditions définies dans vos règles de Réponse aux vulnérabilités fermeture automatique sont également mises à jour en conséquence. En outre, si les règles sont associées à différents domaines, les règles sont créées spécifiquement à l'intérieur de ces domaines.

Reclassifier le matériel non classé

Reclassifiez le matériel non classé en mettant à jour les règles de recherche de CI.

Avant de commencer

Rôle requis : sn_sec_cmn.admin

Pourquoi et quand exécuter cette tâche

La table Carte d'importation d'hôte [sn_sec_cmn_src_cmdb_map] affiche les variables entrantes de la charge utile et leurs affectations correspondantes dans la table Éléments détectés. Parfois, des différences dans les conventions de dénomination entre le scanner et Discovery peuvent conduire à ce que le matériel ne soit pas classifié. Lors de la création d'un nouveau CI matériel non classé, assurez-vous que le nom dans la charge utile contient uniquement le nom d'hôte. Plus tard, lorsque la découverte identifie l'actif, il peut être reclassé dans la classe de CI appropriée. Si nécessaire, un script peut être écrit pour générer une valeur dérivée qui s'aligne sur le nom des CI à la fois dans Découverte et dans la Base de données de gestion des configurations (CMDB).

Si le moteur Identification et réconciliation (IRE) est activé, l'option de reclassification des éléments détectés n'est pas prise en charge.

Procédure

1. Accédez à la table Cartes d'importation d'hôte [sn_sec_cmn_src_cmdb_map].
2. Sélectionnez une source.
3. Dans la liste des champs Cible, sélectionnez **Nom**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La case **à cocher Utiliser le script** devient visible.

Remarque :

- Le script n'est disponible que si le **nom** est sélectionné dans la liste des champs cibles.
- Pour ajouter un script pour d'autres options dans la liste du champ Cible, vous devez désactiver la politique d'interface utilisateur en :
  - Désactiver « Définir l'utilisation du script comme faux ».
  - Désactiver « Afficher ou masquer le script d'utilisation ».
  - Suppression de la condition « le champ cible est le nom » dans « Afficher ou masquer la politique de script ».
- La table Cartes d'importation d'hôte est mise à jour avec deux nouvelles colonnes : Script et Utiliser un script.

4. Cochez la case **Utiliser le script** .
   Le champ **Script** affiche le script par défaut, mais vous pouvez en créer un personnalisé. Dans ce champ, vous pouvez spécifier la source et les valeurs dérivées pour qu'elles s'alignent sur la convention de dénomination de la base de données. La valeur générée par le script est stockée dans sourcePayload['DERIVED'][rule.source_field]. Assurez-vous que les règles de recherche de CI sont ajustées pour utiliser les valeurs de charge utile source, dérivées et d'attributs ciblés lors de l'archivage dans les tables correspondantes.
5. Pour appliquer le script à des enregistrements en double plus anciens, procédez comme suit :
   a. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments détectés**.
   b. Sélectionnez les enregistrements en double.
   c. Dans la liste Action sur les lignes sélectionnées, sélectionnez **Réappliquer les règles de recherche de CI**.
   Cela indique une correspondance avec un actif existant.
6. Pour appliquer le script pour Tenable.io, procédez comme suit :
   a. Accédez à la **Réponse aux vulnérabilités Cartes d'importation d'hôtes**.
   b. Sélectionnez le script de la ligne avec le nom NetBIOS, HOSTNAMES et FQDNS comme champ **Source** .
   c. Mettez à jour le script pour chaque élément.

   Remarque : Pour Tenable.io, le scanner renvoie un tableau pour NetBIOS, HOSTNAMES et FQDNS, pour lesquels le script ne fonctionne pas comme prévu.

   Étant donné que la carte d'importation d'hôte contient Tenable.io**netbios_name** dans le champ **Source** , vous devez écrire un script. Lors de la recherche, un autre champ source, **NETBIOS** , est utilisé, qui contient un tableau de valeurs. Ainsi, une nouvelle ligne est ajoutée dans la table, et la même logique doit être écrite en boucle dans le script. De même, pour **les FQDN** et **les HOSTNAMES.**
7. Pour appliquer le script pour Rapid7, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tous** > **Réponse aux vulnérabilités Cartes d'importation d'hôtes**.

b. Pour Rapid7 les lignes avec FQDN et HostName, mettez à jour la méthode de recherche sur Script.

Remarque : Pour Rapid7, la méthode de recherche de CI est définie sur Correspondance de champ pour le nom de domaine complet et le nom d'hôte, ce qui permet d'empêcher l'utilisation du script.

Créer manuellement une tâche de rattrapage dans Réponse aux vulnérabilités

La création manuelle d'une tâche de rattrapage est effectuée lorsque vous souhaitez regrouper les éléments vulnérables en fonction d'autres critères que les règles de la tâche de rattrapage. Par exemple, vous pouvez créer des tâches pour un gestionnaire particulier ou pour de nouveaux exploits actifs, tels que des ransomwares qui incluent différentes vulnérabilités. Vous pouvez également l'utiliser pour regrouper des éléments vulnérables non groupés.

Important : Vous pouvez créer des tâches de rattrapage d'hôte dans :

- Espace de travail du gestionnaire de vulnérabilités en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.
- Espace de travail de remédiation IT en tant qu'utilisateur disposant du rôle sn_vul.remediation_owner.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.

Les règles de tâche de rattrapage fonctionnent de la même façon que les règles de tâche de rattrapage précédentes et elles sont toujours disponibles. Toutefois, vous préférez peut-être laisser les règles de tâche de rattrapage inactives le temps que vous vous habituiez aux fonctionnalités disponibles pour vos gestionnaires de sécurité et vos équipes informatiques dans les espaces de travail.

2. Sélectionnez l'une des catégories de tâches pour ouvrir la liste.

3. Cliquez sur **Nouveau**.

4. Renseignez les champs du formulaire comme il convient.
Pour plus d'informations sur des champs spécifiques, reportez-vous à la section Champs du formulaire de tâche de rattrapage.

5. Cliquez sur **Envoyer**.
Lorsque la tâche est créée, à l'aide du type de filtre **Condition** ou **Groupe de filtres** , la liste connexe **Élément vulnérable** recherche et affiche tous les éléments vulnérables correspondants.

Vous pouvez utiliser le lien connexe, **Analyser à nouveau pour rechercher des vulnérabilités** pour déclencher manuellement une ServiceNow® analyse lancée. Pour en savoir plus sur la configuration d'un scanner de vulnérabilité, reportez-vous à la section Configurer et gérer Qualys les scanners et analyses de vulnérabilité.

Pour une intégration de vulnérabilité Qualys, un scanner par défaut est préinstallé dans le module **Scanners de vulnérabilité** . Ce scanner est désactivé par défaut. Cochez les cases **Actif** et **Par défaut** pour activer le scanner Qualys afin qu'il fonctionne à l'aide du lien connexe **Analyser les vulnérabilités** sur la tâche de rattrapage et les formulaires d'élément vulnérable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le lien connexe État de la **mise à jour** affiche la date et l'heure de dernière mise à jour. Il regroupe les informations des VI dans la tâche de rattrapage. Consultez Champs du formulaire de tâche de rattrapage pour plus d'informations. Lorsqu'une tâche est formée en fonction d'une vulnérabilité spécifique, cette vulnérabilité est répertoriée sur le formulaire de tâche de rattrapage.

Si vous ouvrez un élément vulnérable associé, toutes les entrées de tâche de rattrapage associées apparaissent sous l'onglet de liste connexe **Tâche de rattrapage** .

Ajouter des utilisateurs au groupe Réponse aux vulnérabilités

Lorsque la fonctionnalité Fermer/Différer est utilisée pour différer ou fermer un élément vulnérable sans nécessiter d'analyse, le Réponse aux vulnérabilités groupe est invité à approuver ou à rejeter la demande. Vous pouvez affecter les utilisateurs appropriés.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Groupes**.
2. Ouvrir le Réponse aux vulnérabilités groupe.
3. Cliquez sur la liste connexe **Membres du groupe** , puis sur **Modifier**.
4. Sélectionnez un ou plusieurs noms dans la liste **Collection** .
5. Cliquez sur **Ajouter**.
6. Cliquez sur **Enregistrer**.

Information associée

Créer un utilisateur

Gérer manuellement les éléments vulnérables individuels

Les éléments vulnérables représentent un élément de configuration (CI) avec une vulnérabilité donnée. Les éléments vulnérables sont importés de sources tierces ou à l'aide des informations NVD SAM (lien) pour comparer les entrées de vulnérabilité aux enregistrements logiciels récupérés à partir du module Logiciel Gestion des actifs .

Les éléments vulnérables sont contenus dans les tâches de rattrapage définies par les règles de vulnérabilité. En règle générale, les tâches de rattrapage sont l'endroit où les groupes d'éléments vulnérables sont affectés et traités.

Les éléments vulnérables peuvent être affichés et modifiés en bloc à partir du module **Éléments vulnérables** . Les enregistrements d'éléments vulnérables affichent les informations relatives à la vulnérabilité dans l'onglet **Vulnérabilité** . Cet onglet peut indiquer s'il existe des exploits publics ou actifs pour celui-ci. Il indique également s'il peut être corrigé via un correctif, un changement de configuration ou une combinaison des deux. Si des adresses IP sont trouvées lors de la déduplication, elles apparaissent dans une liste connexe.

Si un CI est supprimé de la CMDB, tous les éléments vulnérables associés sont également supprimés.

Lorsqu'un élément vulnérable est ajouté à une tâche de rattrapage, le groupe apparaît dans la liste des éléments vulnérables **Tâches de rattrapage** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsqu'une tâche affectant un élément vulnérable est créée, la tâche apparaît dans la liste connexe des **éléments vulnérables Tâches affectées** .

Les éléments vulnérables peuvent être créés manuellement. Vous pouvez créer des incidents de sécurité ou des demandes de changement et les fermer manuellement ou les différer. Les règles de tâche de rattrapage peuvent être appliquées aux éléments vulnérables créés manuellement.

Les tâches de rattrapage et les règles de tâche de rattrapage ont été améliorées pour prendre en charge la fonctionnalité de tâche. Les éléments vulnérables ne peuvent pas être liés en tant que tâche parente.

Créer des Réponse aux vulnérabilités éléments vulnérables

Plusieurs méthodes créent des éléments vulnérables (VI). Le plus souvent, une intégration à un scanner de vulnérabilité est installée et configurée pour importer les résultats tous les soirs. Il y a des cas, comme les vulnérabilités de sécurité physique, où vous préférez peut-être ajouter manuellement des enregistrements d'éléments vulnérables.

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Pourquoi et quand exécuter cette tâche

Les éléments vulnérables que vous créez manuellement et les éléments vulnérables créés automatiquement sont automatiquement ajoutés et supprimés des tâches de rattrapage en fonction des règles de tâche de rattrapage et des conditions de groupe.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Sélectionnez une catégorie pour ouvrir la liste.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.
   Pour en savoir plus sur les champs Éléments vulnérables, Réponse aux vulnérabilités Champs de formulaire d'élément vulnérable reportez-vous à la section .
5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.

   Les règles de la tâche de rattrapage évaluent l'élément vulnérable et l'ajoutent à une tâche existante ou créent une nouvelle tâche. Si l'évaluation échoue, l'élément vulnérable est ajouté à la liste **des éléments vulnérables dégroupés** .

   Lorsque vous enregistrez un nouvel élément vulnérable, tous les calculateurs activés s'exécutent.

   Remarque : Un seul calculateur par **champ cible** est autorisé à être actif à la fois. Lorsque vous en activez un, tous les autres ayant le même **champ Cible** sont désactivés.

6. Vous pouvez cliquer sur l'une des listes connexes pour afficher des informations supplémentaires.

   Vous pouvez utiliser le lien connexe, **Rechercher des vulnérabilités** pour déclencher manuellement une ServiceNow® analyse initiée. Pour en savoir plus sur la configuration d'un scanner de vulnérabilité, reportez-vous à la section Configurer et gérer Qualys les scanners et analyses de vulnérabilité.

   Pour une intégration de vulnérabilité Qualys, un scanner par défaut est préinstallé dans le module **Scanners de vulnérabilité** . Ce scanner est désactivé par défaut. Cochez les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

cases **Actif** et **Par défaut** pour activer le scanner Qualys afin qu'il fonctionne à l'aide du lien connexe **Analyser les vulnérabilités** sur la tâche de rattrapage et les formulaires d'élément vulnérable.

Les options de modification et de correction suivantes sont disponibles dans la barre d'en-tête :

- Mettre à jour : enregistre les mises à jour dans le formulaire.
- Créer un incident de sécurité : crée un incident de sécurité.
- Fermer : ferme l'élément. Si tous les éléments de son groupe sont fermés, la tâche de rattrapage se ferme automatiquement.
- Demande d'exception : soumet une demande de report d'un élément.
- Résoudre : résout l'élément.
- Supprimer : supprime l'élément vulnérable.

Information associée

Modifier des éléments vulnérables en bloc dans Réponse aux vulnérabilités

Différer un élément vulnérable

Si vous déterminez que le problème associé à un élément vulnérable (VIT) présente un risque faible et peut être immédiatement différé sans analyse supplémentaire, vous pouvez utiliser la fonctionnalité **Différer** .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Une tâche planifiée s'exécute tous les jours pour rechercher les éléments vulnérables différés qui ont atteint leur date de réouverture. Le jour où le report du VI doit expirer, l'enregistrement est rouvert.

À partir de Réponse aux vulnérabilités la version 20.0, avant de rouvrir un VI différé, la tâche planifiée Vérifier l'expiration des éléments vulnérables et des groupes vérifie si une règle d'exception est applicable sur un VI différé et met à jour les champs **Motif** et **Jusqu'à** conformément à la règle d'exception. L'état du VI reste Différé jusqu'à la dernière date d'expiration.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Ouvrez un élément vulnérable.
3. Cliquez sur **Demande d'exception**.
4. Renseignez les champs du formulaire comme il convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Jusqu'à	Sélectionnez la date à laquelle l'état Différé expire et la tâche de rattrapage est réactivée. **Remarque :** À partir de la version 18.0 de Réponse aux vulnérabilités (VR), si un élément vulnérable différé est fermé et rouvert par un scanner avant l'expiration de la fenêtre d'exception, l'état du VIT revient à l'état différé respectant la fenêtre d'exception active. Pour activer cette fonctionnalité, définissez la valeur de la propriété système sn_vul.auto_defer_vit_in_active_exception_window sur vrai. En outre, la date de fin différée persiste même après la fermeture de l'élément vulnérable ou l'expiration de l'exception. Le rôle requis est sn_vul.manage_exception_configuration pour la lecture et l'écriture. Une fois l'enregistrement envoyé, si les notifications par e-mail sont définies, les Réponse aux vulnérabilités membres du groupe reçoivent un e-mail indiquant que la date d'expiration est dans moins d'une semaine. Lorsque la date de report expire, l'élément vulnérable est redéfini sur Ouvert et une deuxième notification par e-mail est envoyée.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants : ○ En attente de fenêtre de maintenance ○ Faux positif ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Cliquez sur **Envoyer**.
   Le groupe est marqué **En cours de révision**. Un lien connexe **Rouvrir** s'affiche. La date et le motif de réouverture apparaissent dans les notes de travail sous l'onglet **Approbations de changement de l'état** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander une extension pour un élément vulnérable différé

Demandez une extension pour un élément vulnérable différé avant qu'il n'atteigne sa date d'échéance différée. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Ouvrez un élément vulnérable différé.
3. Sélectionnez **Demande d'extension**.

   Remarque : Le bouton Demande d'extension n'est visible que lorsque l'état de l'élément vulnérable est Différé.

4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'élément vulnérable différé doit être prolongé pour correction.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants : ○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Un e-mail est déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

   Remarque :
   - La demande passe par deux niveaux d'approbation.
   - Si une règle d'exception différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

6. Une fois la demande approuvée, les notes Jusqu'à, Motif et Report sont mises à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actualiser Réponse aux vulnérabilités les éléments vulnérables

Le lien connexe Mettre **à jour le statut** permet d'inspecter les éléments vulnérables afin de déterminer s'il existe des éléments vulnérables supplémentaires qui appartiennent à une tâche de rattrapage. Utilisez-le si une mise à jour est justifiée en dehors de la tâche planifiée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_write ou sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Le lien connexe **Mettre à jour l'état** n'est modifiable que sur le formulaire de tâche de rattrapage dans les états **Ouvert** ou **En cours d'examen** , à l'aide d'un groupe de filtres ou lorsque le type de filtre est condition. Cette inspection est effectuée quel que soit l'état de la case **à cocher Actualiser automatiquement les éléments vulnérables** .

À partir de la version 22.0 de , le bouton **Mettre à jour l'état**Réponse aux vulnérabilités est disponible en mode Enregistrement pour les tâches de rattrapage dans le et Espace de travail de remédiation IT.Espace de travail du gestionnaire de vulnérabilités

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Ouvrez n'importe quel enregistrement à l'état **Ouvert** ou **En cours d'examen** .
3. Cliquez sur le lien Mettre **à jour l'état** .
   De nouveaux éléments vulnérables apparaissent sous l'onglet **Éléments vulnérables** .

Identifier et escalader les problèmes de sécurité dans les logiciels tiers

Vous pouvez afficher les vulnérabilités logicielles renvoyées par des entrées tierces pour déterminer le rattrapage. Utilisez ces informations pour faire correspondre les entrées de logiciel vulnérables à un modèle de détection de logiciels Gestion des actifs .

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Bibliothèques** > **Tiers**.
   Une liste des logiciels vulnérables téléchargés s'affiche.
2. Cliquez sur un enregistrement logiciel pour afficher les informations sur les vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur les listes connexes suivantes pour obtenir plus d'informations sur l'identification des vulnérabilités.

Liste connexe	Description
Éléments vulnérables	Répertorie tous les éléments vulnérables, qui consistent en des appariements d'un élément de configuration et d'un logiciel potentiellement vulnérables. Pour obtenir plus d'informations sur un appairage, cliquez sur l'icône d'informations (icône). **Remarque :** Si le logiciel est supprimé, tous les éléments vulnérables associés sont fermés et supprimés de la liste connexe **des éléments vulnérables** .
Entrées de vulnérabilité	Répertorie les entrées de vulnérabilité pour l'enregistrement logiciel sélectionné. Cliquez sur un enregistrement pour en afficher les détails.

Si des vulnérabilités ont été identifiées et que des éléments vulnérables ont été créés, vous pouvez Résoudre les tâches de rattrapage, si nécessaire.

Identifier et escalader les problèmes de sécurité à l'aide de NVD

Lorsque les enregistrements de l'identificateur commun de vulnérabilité et d'exposition (CVE-ID) sont téléchargés à partir de la base de données de vulnérabilité nationale (NVD), ils sont comparés au logiciel du réseau de votre entreprise, tel qu'identifié par le modèle de détection des actifs logiciels. Lorsqu'un CVE-ID correspond à un logiciel ou à un élément de configuration vulnérable dans votre réseau, un élément vulnérable est créé. Vous utilisez les informations contenues dans l'enregistrement CVE-ID pour décider s'il y a lieu d'escalader l'élément vulnérable pour y remédier.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Bibliothèques** > **NVD**.
   Une liste des CVE-ID qui ont été téléchargés à partir du NVD s'affiche. Les mises à jour du NVD peuvent être effectuées à la demande et par des exécutions planifiées à partir des enregistrements d'intégration de la base de données des vulnérabilités nationale du NIST situés à l'adresse **Tous** > **Administration** > **Intégrations**.
2. Cliquez sur un enregistrement CVE pour afficher les informations suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- un résumé pour le CVE-ID.
- une référence à une entrée Common Weakness Enumeration (CWE), le cas échéant.
- le score de vulnérabilité du CVE-ID sur le système commun de notation des vulnérabilités (CVSS). Pour plus d'informations sur le CVSS, consultez le site Web de la base de données de vulnérabilité nationale .

3. Cliquez sur les listes connexes pour plus d'informations sur les vulnérabilités.

   Références de vulnérabilité

   Nom, description et URL de la vulnérabilité donnée et de l'endroit où elle est référencée.

   Exploite

   Détails.

   Faiblesses

   Liste des faiblesses CWE.

4. Cliquez sur les listes connexes suivantes pour obtenir plus d'informations sur l'identification des vulnérabilités.

Liste connexe	Description
Éléments vulnérables	Répertorie tous les éléments vulnérables, qui consistent en des appariements d'un élément de configuration et d'un logiciel potentiellement vulnérables. Pour obtenir plus d'informations sur un appairage, cliquez sur l'icône d'informations (icône). **Remarque :** Si le logiciel est supprimé, tous les éléments vulnérables associés sont fermés et supprimés de la liste connexe **des éléments vulnérables** .
Entrées de vulnérabilité	Répertorie les entrées de vulnérabilité pour l'enregistrement logiciel sélectionné. Cliquez sur un enregistrement pour en afficher les détails.

Si des vulnérabilités ont été identifiées et que des éléments vulnérables ont été créés, vous pouvez Résoudre les tâches de rattrapage, si nécessaire.

Identifier et escalader les problèmes de sécurité à l'aide de CWE

Affichez la bibliothèque d'enregistrements Common Weakness Enumeration (CWE) de la base de données de vulnérabilité nationale (NVD) pour comprendre comment ils sont liés aux enregistrements de vulnérabilité et d'exposition communes (CVE). Utilisez ensuite ces informations pour faire correspondre les entrées de logiciel vulnérables à un modèle de détection de logiciels Gestion des actifs .

Avant de commencer

Rôle requis : sn_vul.vulnerability_write

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Bibliothèques** > **CWE**.
   Une liste des logiciels vulnérables téléchargés s'affiche.
2. Cliquez sur un enregistrement logiciel CWE pour afficher les informations sur les vulnérabilités.
3. Cliquez sur les listes connexes suivantes pour obtenir plus d'informations sur l'identification des vulnérabilités.

Liste connexe	Description
Éléments vulnérables	Répertorie tous les éléments vulnérables, qui consistent en des appariements d'un élément de configuration et d'un logiciel potentiellement vulnérables. Pour obtenir plus d'informations sur un appairage, cliquez sur l'icône d'informations (icône). **Remarque :** Si le logiciel est supprimé, tous les éléments vulnérables associés sont fermés et supprimés de la liste connexe **des éléments vulnérables** .
Entrées de vulnérabilité	Répertorie les entrées de vulnérabilité pour l'enregistrement logiciel sélectionné. Cliquez sur un enregistrement pour en afficher les détails.

Si des vulnérabilités ont été identifiées et que des éléments vulnérables ont été créés, vous pouvez Résoudre les tâches de rattrapage, si nécessaire.

Afficher l'état de la cible de rattrapage d'un Réponse aux vulnérabilités élément vulnérable

Lorsqu'un élément vulnérable a presque atteint (ou dépassé) sa date cible de rattrapage, telle que définie par une règle de cible de rattrapage, l'enregistrement de l'élément vulnérable est mis à jour avec un état. Ces informations peuvent aider l'analyste à surveiller de manière proactive les activités de rattrapage à venir.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_admin
- sn_vul.read_remediation_target_rules [lecture seule]

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Une tâche planifiée appelée **Évaluer les cibles de rattrapage** s'exécute une fois par jour pour comparer la date actuelle à la date de rattrapage de l'élément vulnérable spécifiée dans la règle de cible de rattrapage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

associée. Lorsque la date actuelle tombe dans le nombre de jours avant l'échéance du rattrapage, un état de rattrapage est ajouté à l'enregistrement d'élément vulnérable.

Pour plus d'informations sur les règles de cibles de rattrapage, reportez-vous à la section Réponse aux vulnérabilités Règles de cibles de rattrapage.

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Éléments vulnérables**.
2. Cliquez sur l'élément vulnérable que vous souhaitez examiner.
   Si la date de rattrapage de l'élément vulnérable se situe dans la plage des conditions définies dans la règle de cible de rattrapage, l'onglet État de la **cible de rattrapage** est visible.
3. Cliquez sur l'onglet État de la **cible de rattrapage** .
4. Cliquez sur l'enregistrement de l'état de la cible de rattrapage pour l'examiner.

Remarque : Pour afficher le nombre d'éléments vulnérables proches de la cible, en cours et dépassant la cible, reportez-vous à la section Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.

Information associée

Créer ou modifier Réponse aux vulnérabilités des règles de cibles de rattrapage

Travailler avec des CI sans correspondance

En tant que responsable et analyste des vulnérabilités, vous pouvez afficher et reclasser les éléments de configuration (CI) sans correspondance, rapprocher les éléments détectés sans correspondance, réappliquer des règles de recherche de CI sur les éléments détectés sélectionnés et dédupliquer les CI existants.

Afficher et reclasser les éléments de configuration sans correspondance

Les éléments de configuration (CI) qui ne se trouvent pas dans le Base de données de gestion des configurations (CMDB) sont placés dans une liste consultable des éléments détectés. Cette liste offre un moyen pratique de reclasser les CI sans correspondance.

Avant de commencer

Rôle requis :
sn_vul.read (minimum pour afficher les CI sans correspondance)
et

itil ou actif (à reclasser)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

En tant qu'analyste de vulnérabilité, vous pouvez afficher les CI sans correspondance.

L'action de reclassification n'est disponible que sur `sn_sec_cmn_unmatched_ci` les CI de classe, lorsque vous disposez du rôle itil ou asset. Une fois qu'un CI a été reclassifié, il ne peut pas être reclassé à l'aide de l'interface utilisateur. Vous pouvez effectuer un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

reclassement, à partir du formulaire CI ou de la vue de liste CI, en modifiant la valeur de **la classe** . Pour en savoir plus, reportez-vous à Reclassifier un CI .

Procédure

1. Accédez à la **Tous** > **Security Operations** > **CMDB** > **Éléments détectés**.
2. Pour passer en revue, cliquez sur chaque élément.
3. Pour apporter des corrections aux informations contenues dans les champs du formulaire **Élément détecté** , modifiez dans cette page, puis cliquez avec le bouton droit sur **Enregistrer**.
   Toutes les données ajoutées ou laissées dans ces champs sont transférées à **l'élément de configuration** résultant lorsqu'il est reclassé.
4. Si tout semble correct, cliquez sur **Reclassifier**.
5. Dans la liste de choix, sélectionnez un **nom de classe** et cliquez sur **Soumettre**.
   La **classed'élément détecté** est mise à jour, le champ **État** passe à Reclassé et toutes les données se trouvent dans la CMDB.

Rapprocher les éléments détectés sans correspondance

Créer une tâche planifiée pour rapprocher les éléments détectés sans correspondance

Avant de commencer
Rôles requis : admin

Pourquoi et quand exécuter cette tâche
Un élément vulnérable (VI) se compose d'une vulnérabilité et d'un élément de configuration (CI). Lorsqu'un VI est créé, le CI qui lui est ajouté au moment de la création peut être obsolète. Les informations de CI sans correspondance ne sont pas rapprochées si les informations dans la CMDB changent. Pour le rapprochement, appliquez des règles de recherche d'éléments de configuration (CI) sur les éléments qui sont dans un état sans correspondance lorsque la CMDB est mise à jour avec les derniers CI.

Vous pouvez exécuter une demande de tâche planifiée pour réappliquer la règle de correspondance CI aux éléments détectés dans un état sans correspondance. Si le CI change après réapplication des règles de recherche, les éléments détectés sont mis à jour avec le nouveau CI. Les détections impactées et les éléments vulnérables sont également mis à jour. Pour plus de détails, voir Changements de CI pour les éléments détectés.

Procédure

1. Accédez à la **Tous** > **Security Operations > rapprocher les éléments détectés sans correspondance**.
2. Sur la page Tâches en arrière-plan, cliquez sur **Créer une tâche de rapprochement**.
3. Remplissez les champs du formulaire.

Remarque : Vous ne pouvez modifier que le champ **Paramètres** .

Formulaire de tâche en arrière-plan

Champ	Description
Numéro	Numéro de tâche unique.
Créé par	Utilisateur qui a créé la tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Paramètres	Paramètres pour rapprocher les éléments détectés sans correspondance : ○ limite : nombre maximal d'éléments détectés à rapprocher. Si vous ne saisissez pas de valeur, 10 000 éléments détectés sont rapprochés. ○ firstDiscovereditem : premier élément détecté qui doit être rapproché. Si vous ne saisissez pas de valeur, le processus de rapprochement commence à partir du premier élément détecté.
État	État actuel de la tâche en arrière-plan.
Description d'état	Description de l'état actuel de la tâche en arrière-plan.
Type de tâche	Type de tâche. La valeur est **Rapprocher les éléments détectés sans correspondance**
Démarré à	Heure de début de la tâche.
Heure de fin	Heure à laquelle la tâche a été terminée.
Durée de la tâche	Temps total nécessaire pour terminer la tâche.
Sous-état	Sous-état de l'état sélectionné.
Notes	Nombre d'enregistrements qui ont été traités.

4. Cliquez sur **Envoyer**.

   Remarque :
   - Pour arrêter l'exécution de la tâche, cliquez sur **Annuler**.
   - Vous ne pouvez pas rapprocher les CI sans correspondance ou réappliquer des règles de recherche de CI pendant l'importation d'hôtes ou d'éléments vulnérables.

5. Réponse aux vulnérabilités À partir de la version 26.0.11, vous pouvez « Réappliquer des règles de recherche » pour les éléments sélectionnés ou filtrés dans la vue de table des éléments détectés.

   Remarque : À partir de la version mentionnée ci-dessus, la tâche planifiée de rapprochement des éléments détectés sans correspondance est mise hors service.

6. **Facultatif :** Sélectionner **Tous** > **Opérations de sécurité >Réappliquez des règles de recherche** pour les éléments sélectionnés ou filtrés dans la table des éléments détectés.

   Remarque : Si aucun filtre n'est appliqué, l'option Réappliquer sera désactivée.

   Après une nouvelle demande, une URL de tâche en arrière-plan ou un message d'erreur apparaîtra, une fois l'intégration en cours d'exécution.

Réappliquer des règles de recherche de CI sur les éléments découverts sélectionnés

Réappliquez les règles de recherche d'éléments de configuration (CI) sur les éléments détectés sélectionnés à partir des actions de sélection de la vue de liste des éléments

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

détectés. Si le CI change après la réapplication des règles, les éléments détectés sont mis à jour avec le nouveau CI et les détections impactées. Les éléments vulnérables sont également mis à jour.

Avant de commencer

Rôles requis : admin

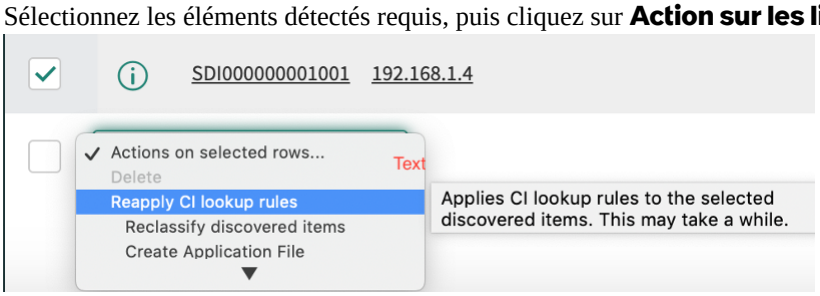
Pourquoi et quand exécuter cette tâche

Pour plus d'informations, consultez Changements de CI pour les éléments détectés.

Pour plus d'informations sur les concepts de correspondance de CI et de CMDB, la recherche d'éléments détectés, l'identification basée sur des règles et d'autres informations détaillées sur le fonctionnement de la correspondance de CI, consultez l'article Correspondance de CI dans Réponse aux vulnérabilités [KB0998706] de la base de connaissances HI.

Procédure

1. Accédez à la **Tous** > **Opérations de sécurité** > **CMDB** > **Éléments détectés**.
2. Sélectionnez les éléments détectés requis, puis cliquez sur **Action sur les lignes sélectionnées**.



3. Dans la liste, sélectionnez **Réappliquer les règles de recherche de CI**.

Remarque :

Réponse aux vulnérabilités À partir de la version v24.0.6, vous pouvez ignorer la réapplication des règles de recherche de CI sur les éléments détectés avec le sous-état « CI désactivé » en activant la propriété *sn_sec_cmn.skipItemsWithCIDecommissioned*système.

Les règles sont réappliquées à ces éléments détectés.

4. Cliquez sur **Afficher l'état** dans le message.

L'état s'affiche sur le formulaire de tâche en arrière-plan.

Remarque : Dans le champ **Notes** , les éléments détectés n'ont pas pu être traités en raison d'un attribut d'exception avec une valeur non nulle indique qu'une erreur ou une exception s'est produite lors de la réapplication d'une règle de recherche de CI. Consultez les journaux système pour en savoir plus.

5. La nouvelle application s'applique uniquement aux éléments analysés au cours des 90 derniers jours en fonction de la colonne **last_scan_date, last_comp_scan_date, non_infra_last_scan_date non_infra_last_comp_scan_date** .

Ajout d'une propriété système ci_lifecycle_status_source (champ d'application = sn_sec_cmn) pour configurer les colonnes d'état du cycle de vie des CI (par exemple, État d'installation, État opérationnel). Vous pouvez configurer des colonnes supplémentaires pour mettre hors service des CI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des colonnes sont ajoutées à la vue de liste des tâches en arrière-plan :

- Temps écoulé (ms) : temps nécessaire au traitement de la tâche en arrière-plan.
- Éléments traités : nombre d'éléments traités jusqu'à maintenant.
- Nombre total d'éléments à traiter : nombre total d'éléments restant à traiter.
- Délai jusqu'à l'achèvement (ms) : temps restant avant le traitement de la tâche en arrière-plan. Ces colonnes offrent une visibilité sur l'avancement des tâches. Ces colonnes sont disponibles pour chaque vue de formulaire que vous pouvez ajouter selon vos besoins.

Réappliquer les améliorations des règles de recherche de CI

Réappliquez les règles de recherche d'éléments de configuration (CI) sur les éléments détectés sélectionnés tels que OS et NetBIOS.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

- Les valeurs de système d'exploitation et NetBIOS présentes dans les données sources doivent être renseignées avant l'élément de configuration lors du remplissage de ces champs dans l'élément détecté.
- En cas de valeurs SE et NETBIOS vides dans les données sources, les valeurs sont extraites de l'élément de configuration lors du remplissage de ces champs dans la table des éléments détectés.

Procédure

1. Accédez à la **Tous** > **Opérations de sécurité** > **CMDB** > **Éléments détectés**.
2. Sélectionnez les éléments détectés requis, puis cliquez sur **Action sur les lignes sélectionnées**.
3. Dans la liste, sélectionnez **Réappliquer les règles de recherche de CI**.

   Les règles sont réappliquées à ces éléments détectés.

Étapes pour empêcher les enregistrements dupliqués ou orphelins après l'exécution Réponse aux vulnérabilités de règles de recherche de CI

Prenez des mesures pour éviter les enregistrements en double ou orphelins résultant de la mise en correspondance (éléments de configuration (CI) dans le CMDB.

L'importation de données de vulnérabilité peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer des correspondances dans la CMDB peut entraîner de longs délais de traitement. Un test et un débogage approfondis des scripts de traitement dans les règles permettent d'atténuer le risque de problèmes ultérieurs dans le processus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Empêcher les enregistrements dupliqués ou orphelins

- Utilisez de petits sous-ensembles de données spécifiques à la règle de recherche de CI testée.
  - Définissez toutes les règles de recherche de CI, autres que celle en cours de test, sur Inactives.
  - Analysez les CI importés pour vous assurer que vous observez le comportement attendu et que la correspondance se produit correctement.
- Examiner les CI correspondants
  - Examinez le nombre de CI correspondants par rapport aux CI sans correspondance. Assurez-vous que le pourcentage est acceptable. Ne vous contentez pas de regarder la première page, c'est probablement la première insérée.
  - Recherchez manuellement certains CI.
  - Vérifiez s'il existe des problèmes de nom ou de champ (tels que la recherche d'un domaine spécifique).

    Si cela semble approprié, ajoutez des règles de correspondance supplémentaires.
- Examiner les CI sans correspondance
  - Accédez à la table CI sans correspondance.
  - Regroupement par classe d'élément de configuration.
  - Examinez toutes les classes qui ne semblent pas correctes (certificats, cartes réseau, images).
    - Déterminez pourquoi ils ne correspondaient pas au CI correct ?
    - La classe doit-elle être exclue ?
    - La classe doit-elle être élevée à une classe connexe ?
- Examinez les états des CI tels que **Mis hors service**.
- Supprimer les données de test
  - Une fois que vous commencez à observer le comportement correct ou attendu dans la correspondance de CI, recommencez.
  - Recommencer par : Suppression des données utilisées pour le test : (voir la section **Suppression des données des tables**)
    - Éléments détectés
    - Éléments vulnérables
    - Tâches de rattrapage
  - Réexécution manuelle de toutes les règles de correspondance de CI.

Pour en savoir plus sur les règles de recherche de CI et Qualys, consultez l'article KB0750656 .

Pour plus d'informations sur les règles de recherche de CI et Rapid7, consultez le KB0818096 .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suppression des données des tables

Parfois, vous avez importé des données et vous vous rendez compte que quelque chose ne va pas. Si quelque chose ne va pas dans un environnement de développement ou de performance, vous pouvez vous retirer d'un meilleur environnement, mais ce n'est pas toujours une option.

Remarque : L'exécution de ces actions nécessite une ServiceNow expertise.

Il existe quatre options pour supprimer des données des tables :

- Utilisation de **Supprimer tous les enregistrements dans laconfiguration de table**.
- Configurez le **nettoyeur de table** en accédant à **Purges automatiques** (sys_auto_flush.list) et en créant un nouvel enregistrement **Purge automatique** .
- Tronquez la table gs.truncateTable à l'aide d'un script en arrière-plan.

  L'utilisation `truncateTable` nécessite de désactiver la case à cocher Enregistrement pour la restauration dans les scripts en arrière-plan. Sinon, une copie de la table et des tables en cascade connexes est créée, prend trop de temps et échoue très probablement.

  Remarque : Ne jamais utiliser `truncateTable` dans un environnement de production. Consultez votre représentant de l'assistance avant d'effectuer des suppressions importantes dans des environnements de production ou partagés.

Déduplication des éléments de configuration existants

Chaque fois que des éléments de configuration (CI) sont mis à jour via une tâche de déduplication, les éléments détectés (DI) associés à ces CI sont également mis à jour. Les éléments vulnérables (VI) et les détections sont également mis à jour avec le CI.

Pour plus d'informations, consultez Changements de CI pour les éléments détectés.

Information associée

Rattraper une tâche de déduplication

Résoudre les tâches de rattrapage

La flexibilité inhérente Réponse aux vulnérabilités vous permet de corriger les vulnérabilités de la manière qui convient à votre organisation de sécurité.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche

Une fois que vous êtes informé qu'une demande de changement est résolue, passez l'état de la tâche de rattrapage sur Résolu et attendez la prochaine analyse. Les nouvelles analyses sont déclenchées automatiquement par le calendrier d'importation tierce configuré dans l'assistant de configuration.

Remarque :

Si la synchronisation de l'état est activée, les tâches de rattrapage passent automatiquement à l'état Résolu après l'implémentation d'une demande de changement associée à une tâche de rattrapage (VUL) et à l'état Réviser. Consultez Change Management pour Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de rattrapage** > **Mes affectations**.
2. Cliquez sur un enregistrement à l'état Ouvert.

   L'état Ouvert indique que l'enregistrement n'a pas encore été traité. Le formulaire affiche les éléments suivants :

   - Informations sur la tâche de rattrapage
   - Détails de la configuration du groupe
   - Notes
   - Éléments vulnérables associés
   - SLA de tâche
   - Demandes de changement
3. Effectuez votre analyse du groupe.
4. Lorsque vous êtes prêt à commencer à travailler sur l'enregistrement, choisissez l'une des options suivantes.

Option	Description
Si l'élément vulnérable présente un risque pour votre environnement informatique, créez un enregistrement CHG et escaladez le problème à l'équipe Gestion des changements .	Affectez le groupe au groupe ou à la personne approprié, puis cliquez sur **Créer un changement**.
Si l'élément vulnérable représente un risque de sécurité potentiel pour votre organisation, créez un enregistrement d'incident de sécurité et escaladez le problème à l'équipe Réponse aux incidents de sécurité .	Cliquez sur **Créer un incident de sécurité**. Ce bouton n'est affiché que lorsqu'il Réponse aux incidents de sécurité est activé. Un calcul d'impact sur l'entreprise est appliqué, l'incident est affecté et l'incident de sécurité est créé.

   Après avoir créé une demande de changement, l'enregistrement approprié apparaît dans la liste connexe **Demandes de changement** sur le formulaire Groupe de vulnérabilité.
5. Si vous déterminez que le problème présente un risque faible et qu'il peut être reporté, cliquez sur **Demande d'exception**.
   Pour en savoir plus sur le report d'une tâche de rattrapage, reportez-vous à la section Différer une tâche de rattrapage.
6. Si vous déterminez que le problème peut être fermé immédiatement sans analyse supplémentaire, cliquez sur **Fermer**.
   Pour plus d'informations sur la fermeture d'une tâche de rattrapage, reportez-vous à la section Fermer une tâche de rattrapage. À partir de la version 23.0 de , le bouton **Fermer** a été supprimé pour une tâche de Réponse aux vulnérabilités rattrapage.

   Une tâche planifiée d'intégration tierce met à jour et analyse automatiquement les enregistrements à un intervalle défini. Les éléments vulnérables sont analysés aux prochaines date et heure planifiées. Vous pouvez également lancer manuellement une analyse des vulnérabilités à l'aide du lien connexe **Rechercher des vulnérabilités** .

   Si l'analyse détecte à nouveau la vulnérabilité dans l'élément de configuration et ne le marque pas comme Corrigé, l'élément vulnérable revient à l'état En cours d'examen. Contactez les opérations IT pour rouvrir la demande de changement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si l'analyse ne détecte pas la vulnérabilité et renvoie que l'élément vulnérable a été marqué comme Fixe, l'élément vulnérable passe à l'état Fermé-Corrigé et est fermé pendant l'importation.

Ce n'est que lorsque tous les éléments vulnérables d'une tâche sont à l'état Fermé-Corrigé que la tâche de rattrapage se ferme automatiquement. Les tâches de rattrapage avec des éléments vulnérables dont l'état est Fermé autre que Corrigé doivent être fermées manuellement.

Différer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage (VUL) est de priorité basse et peut être immédiatement différé sans analyse supplémentaire, vous pouvez utiliser la fonctionnalité **Demande d'exception** .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche

Vous pouvez différer une tâche de rattrapage à partir d'un enregistrement de tâche de rattrapage dans les espaces de Réponse aux vulnérabilités travail. Une fois la demande envoyée, elle est envoyée pour approbation. Consultez Demander une exception dans le Espace de travail de remédiation IT.

Une tâche planifiée s'exécute tous les jours pour rechercher les tâches de rattrapage différées qui ont atteint leur date de réouverture. Le jour où le report de la tâche doit expirer, la tâche est rouverte.

Remarque : Vous pouvez déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement les tâches de rattrapage des états Fermé ou Différé.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Ouvrez un enregistrement.
3. Cliquez sur **Demande d'exception**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Jusqu'à	Sélectionnez la date à laquelle l'état de report expire et la tâche de rattrapage est réactivée. Une fois l'enregistrement envoyé, si les notifications par e-mail sont définies, les Réponse aux vulnérabilités membres du groupe reçoivent un e-mail indiquant que la date d'expiration est dans moins d'une semaine. Lorsque la date de report expire, la tâche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	de rattrapage est redéfinie sur **Ouvert** et une deuxième notification par e-mail est envoyée.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants : ○ En attente de fenêtre de maintenance ○ Faux positif ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Cliquez sur **Envoyer**.
   Le groupe est marqué En cours de révision. Un lien connexe **Rouvrir** s'affiche. La date et le motif de réouverture apparaissent dans les notes de travail sous l'onglet **Approbations de changement de l'état** .

Demander une extension pour une tâche de rattrapage différée

Demander une extension pour une tâche de rattrapage différée (VUL) avant qu'elle n'atteigne sa date d'échéance différée. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche
Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Ouvrez une tâche de rattrapage différée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'état de report expire et la tâche de rattrapage est réactivée.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Une fois la demande approuvée, les changements apportés à la tâche de rattrapage sont également reportés sur les éléments vulnérables, qui font partie de la tâche de rattrapage. Toutefois, les éléments vulnérables doivent être à l'état Différé et jusqu'à ce que les données précèdent la Date de fin de mise à jour. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une tâche de rattrapage différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Fermer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage peut être fermé immédiatement sans analyse supplémentaire, vous pouvez utiliser la fonction **Fermer** . À partir de la version 23.0 de , le bouton **Fermer** a été supprimé pour une tâche de Réponse aux vulnérabilités rattrapage et la fermeture d'une tâche de rattrapage est pilotée par le scanner.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Dans les espaces de Réponse aux vulnérabilités travail, une tâche de rattrapage passe par les mêmes états que dans les versions précédentes de Réponse aux vulnérabilités. Lorsque tous les éléments vulnérables (VIT) d'une tâche de rattrapage sont fermés, la tâche de rattrapage passe à l'état Inactif.

Important : Vous pouvez déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement les tâches de rattrapage des états Fermé ou Différé .

Procédure

1. Ouvrez l'enregistrement pour lequel vous souhaitez demander une révision.
2. Sélectionnez le bouton **Fermer/Différer** .
3. Renseignez les champs du formulaire comme il convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
État	Sélectionnez un état. Les choix possibles sont les suivants : ○ Différé ○ Fermé
Jusqu'à	Disponible uniquement dans la fenêtre contextuelle **État de report** . Sélectionnez la date à laquelle l'état **de report** expire et la tâche de rattrapage est réactivée. Une fois l'enregistrement envoyé, si les notifications par e-mail sont définies, les Réponse aux vulnérabilités membres du groupe reçoivent un e-mail indiquant que la date d'expiration est dans moins d'une semaine. Lorsque la date de report expire, l'élément vulnérable est redéfini sur **Ouvert** et une deuxième notification par e-mail est envoyée.
Motif	Entrez le motif de la fermeture du problème.
Informations supplémentaires	Entrez toute autre information pertinente.

4. Sélectionnez **Soumettre**.
   La tâche de rattrapage est marquée comme **fermée**.

Identification des éléments vulnérables en double à partir de plusieurs scanners

Si vous utilisez plusieurs scanners sur le même actif pour détecter les vulnérabilités, plusieurs éléments vulnérables (VI) peuvent être créés. Vous pouvez identifier ces VI en double pour vous assurer que les vulnérabilités en double ne sont pas affectées aux propriétaires de rattrapage.

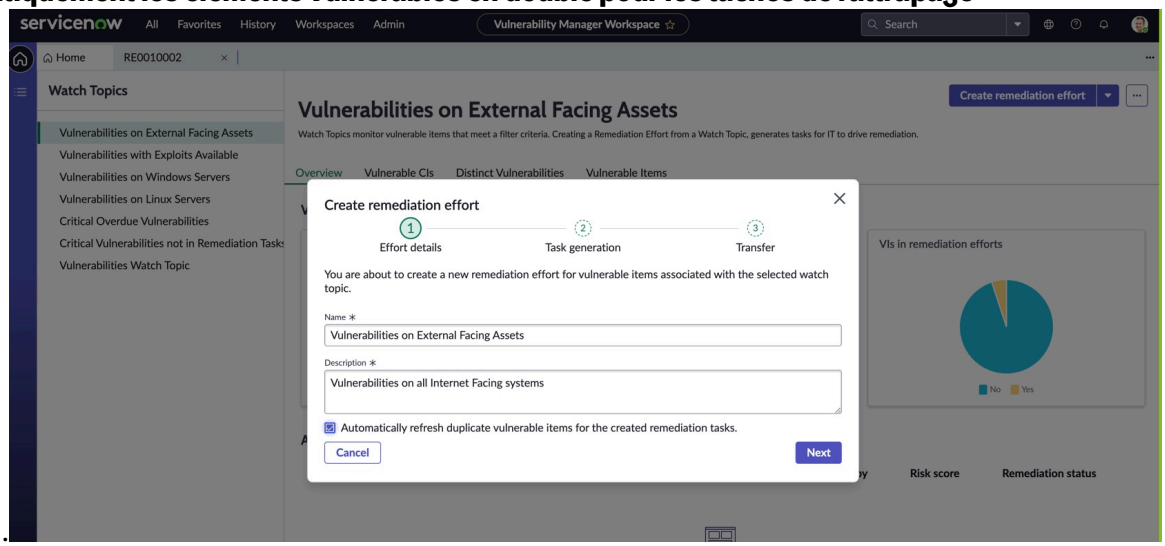
Cette résolution n'est possible que si les mêmes vulnérabilités, telles que les mêmes vulnérabilités et expositions courantes (CVE) sont détectées. La combinaison de vulnérabilité dépend des scanners utilisés. Par exemple, Qualys et Tenable ont leur propre type de vulnérabilité, c'est-à-dire des entrées tierces (TPE), et d'autres scanners tels que Microsoft Defender for Endpoint détectent les vulnérabilités basées sur les CVE.

À partir de la version 17.1, lors de la création d'un effort de rattrapage, vous pouvez actualiser automatiquement les éléments vulnérables en double sur les tâches de rattrapage créées. Pour actualiser automatiquement les éléments vulnérables en double, vous devez sélectionner l'option **Actualiser**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

automatiquement les éléments vulnérables en double pour les tâches de rattrapage créées .



Afficher les VI en double : identifiez les éléments vulnérables en double signalés par plusieurs scanners dans le système. Vous pouvez marquer le VI en double comme résolu. Pour en savoir plus, reportez-vous à Résoudre automatiquement les vulnérabilités en double. Les entrées en double ne sont affichées que lorsque la combinaison de vulnérabilités est créée à l'aide de CVE. Pour plus d'informations, consultez la tâche de rattrapage et les états des éléments vulnérables de Vulnerability Response.

Les doublons potentiels sont identifiés pour les combinaisons de vulnérabilité suivantes :

Combinaison de scanners	Type de vulnérabilité
Scanner 1 et scanner 2	CVE
Scanner 1 et scanner 2	CVE et TPE

Résoudre automatiquement les vulnérabilités en double

À partir de Réponse aux vulnérabilités (VR) v17.1, vous pouvez résoudre automatiquement toutes les vulnérabilités en double sur un actif.

Lorsqu'un actif est analysé avec plusieurs scanners, il est possible d'identifier la même vulnérabilité que les doublons par les différents scanners. Par exemple, si les scanners Qualys et Microsoft identifient la même vulnérabilité, vous pouvez choisir de résoudre automatiquement la vulnérabilité en double.

Exemple de scénario

VR crée un enregistrement, VI1, pour la vulnérabilité 1 à partir du scanner Microsoft Defender for Endpoint. Un deuxième enregistrement, VI2, est créé à partir de l'analyse Qualys pour la même vulnérabilité. L'équipe de rattrapage applique les correctifs susceptibles de résoudre les enregistrements VI1 et VI2. Si vous configurez le calendrier d'analyse Qualys au-delà d'une journée, à ce moment-là, Microsoft Defender fournit les informations sur la vulnérabilité corrigée et VR ferme l'enregistrement VI1 comme Fermé/Corrigé.

Dans ce scénario, l'enregistrement VI2 est toujours à l'état Ouvert et VR attend les résultats de l'analyse Qualys. Dans ce cas, les enregistrements de VI du deuxième scanner restent à l'état Ouvert même si le correctif est appliqué et que le VI est confirmé comme réparé par l'autre scanner.

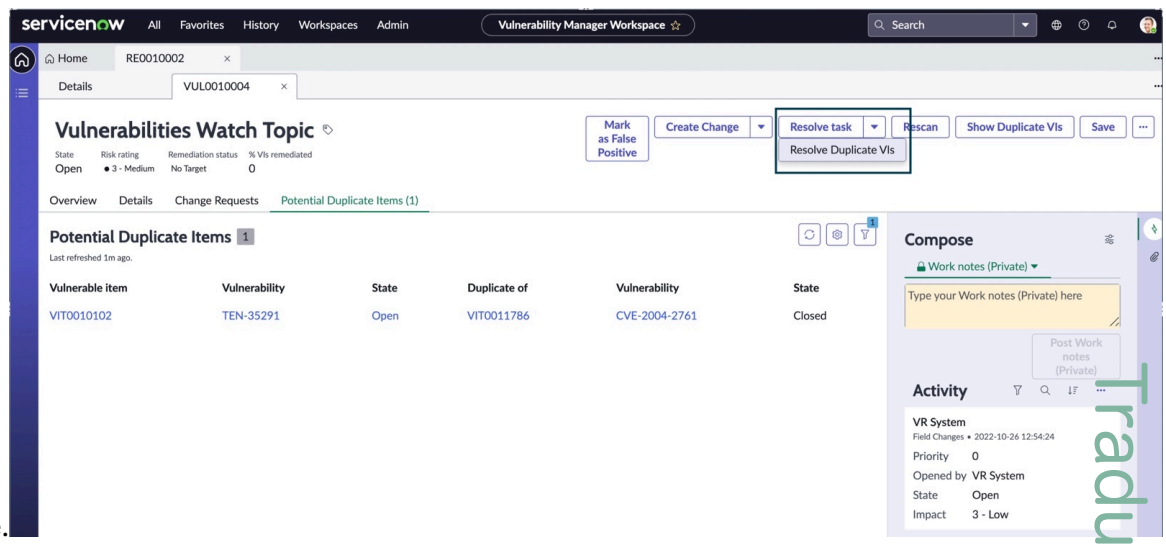
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour remédier à cette situation, vous pouvez envisager de résoudre l'enregistrement de vulnérabilité en double à condition que la vulnérabilité soit fermée par le premier scanner.

Résolvez les vulnérabilités de la manière suivante :

- Sur demande : sélectionnez l'action d'interface utilisateur **Résoudre les VI en double** sur la tâche de rattrapage.



- Automatisé : activez la propriété système `sn_vul.auto_resolve_duplicate_vit` pour résoudre automatiquement les éléments vulnérables en double. La tâche planifiée quotidienne « Actualiser et résoudre les VIT en double lors de la tâche de rattrapage » actualise automatiquement les éléments en double.

Les VI en double sont alors marqués comme résolus.

Remarque : L'enregistrement de l'élément de vulnérabilité résolu est rouvert si le scanner l'identifie comme **Non résolu**.

Créer et modifier un groupe de classification

Créez des groupes afin que les règles sous-jacentes de ce groupe puissent classer les enregistrements de table en fonction des conditions. Les règles peuvent être utilisées pour sélectionner n'importe quel champ dans la table correspondante.

Avant de commencer
Rôle requis : sn_vul.manage_classification_rule

Procédure

1. Accédez à la table Propriétés système.
2. Dans la *`sn_sec_cmn.classificationTables`* propriété système, ajoutez le nom de la table pour laquelle vous souhaitez créer le groupe de classification.
3. Créez une règle métier en ajoutant l'extrait de code suivant à la règle métier sur la table définie dans le groupe :
   `var classificationCalc = nouveau sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_group','sn_vul_classification_rule') ; classificationCalc.calculate() ;`

   Remarque : Des règles métier sont fournies pour exécuter la classification pendant l'ingestion pour les tables Éléments détectés et Entrée de vulnérabilité. Pour les autres tables, pour disposer des règles de classification lors de l'ingestion, vous devez ajouter les règles métier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles de classification**.
5. Dans le menu contextuel Groupes de classification, cliquez sur **Nouveau**.
6. Remplissez les champs du formulaire.

Formulaire de groupe de classification de vulnérabilité

Champ	Description
Nom	Nom du nouveau groupe de classification.
Actif	Option permettant d'activer le groupe.
Description	Description du nouveau groupe de classification.
Table	Table basée sur laquelle les règles sont exécutées. **Remarque :** Le système de base de Vulnerability Response inclut des groupes de classification pour les éléments découverts et les vulnérabilités.

Créer et modifier une règle de classification

Créez des règles pour classer automatiquement les vulnérabilités entrantes vers les équipes appropriées pour la correction.

Avant de commencer

Rôle requis : sn_vul.manage_classification_rule

Pourquoi et quand exécuter cette tâche

Lorsqu'elles sont créées, ces règles classent les vulnérabilités comme appartenant soit à une plateforme, soit à une application. Vous pouvez configurer ces règles pour remplacer la valeur d'un champ spécifique sur l'entrée de vulnérabilité.

Utilisez ces règles pour déplacer le calcul en amont vers la table Entrée de vulnérabilités tierces afin de permettre la réutilisation du contenu.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles de classification**.
2. Pour afficher un groupe de classification, cliquez sur ce groupe.
3. Dans le menu contextuel Règles de classification, cliquez sur **Nouveau**.
4. Remplissez les champs du formulaire.

Formulaire Règle de classification de vulnérabilité

Champ	Description
Nom	Nom de la nouvelle règle de classification.
Actif	Option permettant d'activer la règle.
Description	Description de la nouvelle règle de classification.
Ordre d'exécution	Ordre dans lequel la règle doit être exécutée.
Vue avancée	Option permettant d'afficher des champs supplémentaires dans les sections à onglets.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Quand cette condition est remplie	
Type de condition	Type de condition pour la règle. Les choix sont les suivants : ○ **Filtre** : conditions de filtre de base pour déterminer s'il faut utiliser la règle ou non. ○ **Groupe de filtres** : ensemble de plusieurs conditions utilisées ensemble. La règle est évaluée en fonction des conditions définies dans le groupe de filtres. ○ **Script** : condition de script utilisée pour déterminer quand appliquer cette règle. Ce champ s'affiche uniquement lorsque l'option Vue **avancée** est sélectionnée.
Condition	Condition de la règle. Définissez les conditions en fonction de la colonne sélectionnée dans la colonne d'entrée de vulnérabilité requise. Vous pouvez ajouter plusieurs conditions pour affiner la règle. Ce champ s'affiche uniquement lorsque **Filtre** est sélectionné dans le champ **Type de condition** . **Remarque :** Lors de la définition de plusieurs conditions ou modèles, vous pouvez sélectionner uniquement à partir d'une table parente et d'une table enfant. Vous ne pouvez pas sélectionner parmi deux tables enfants ou plus.
Groupe de filtres	Groupe de filtres. Le groupe est défini lorsqu'un ensemble de conditions est utilisé à plusieurs reprises dans plusieurs endroits. Cliquez sur la recherche à l'aide de l'icône de liste (icône de) pour sélectionner le groupe de filtres. Pour plus d'informations, consultez Créer et définir des groupes de filtres dans Security Operations. Ce champ s'affiche uniquement lorsque Groupe de **filtres** est sélectionné dans le champ **Type de condition** .
Script	Script évalué pour déterminer quand appliquer cette règle. Vous pouvez écrire votre code et définir la réponse sur vrai ou faux. Ce champ apparaît uniquement lorsque **le script** est sélectionné dans le champ **Type de condition**
Définir ces valeurs	
Classification	Classification de la règle. Pour sélectionner une option, cliquez sur l'icône de l'ampoule (icône). La liste affiche les options pour Plateforme et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Application. Vous pouvez également entrer votre propre classification qui n'est pas dans la liste.
Type de classification	Type de classification. Ce champ affiche la liste filtrée des types de classification en fonction de la valeur que vous avez sélectionnée pour le champ **Classification** .
Type de valeur	Type de la valeur affectée à l'aide de cette règle. Les choix sont les suivants : ○ **Modèle** : sélectionnez un modèle. Vous pouvez utiliser un modèle requis. ○ **Script** : sélectionnez un script préexistant ou écrivez votre propre script personnalisé. Ce champ s'affiche uniquement lorsque l'option Vue **avancée** est sélectionnée.
Modèle	Une autre condition pour la règle en dehors des champs **Classification** et **Type de classification** . Sélectionnez une combinaison de champs et de valeurs que vous souhaitez définir lors de l'évaluation de la règle. Ce champ s'affiche uniquement lorsque **le modèle** est sélectionné dans le champ **Type de valeur** .
Valeur de script	Script pour définir des valeurs sur l'enregistrement actuel. Ce champ définit les valeurs à définir sur les champs dans les entrées de vulnérabilité. Ce champ s'affiche uniquement lorsque **le script** est sélectionné dans le champ **Type de valeur** .

5. Pour créer la nouvelle règle, cliquez sur **Soumettre**.

Example:
Utilisez les règles de classification VR pour ajouter la logique aux tables en amont telles que Vulnérabilité et Éléments détectés et la calculer. Vous pouvez réutiliser la sortie plusieurs fois, ce qui améliore les performances des règles telles que les règles d'affectation. Par exemple, classez l'entrée tierce (TPE) comme Java et réutilisez la sortie dans les règles d'affectation plusieurs fois. Exemple de règle d'affectation :

```
VI.TPE.Classfication Type
        | IS | Java
```

Appliquer une règle à une vulnérabilité existante

Lorsque vous modifiez une règle de classification, réexécutez toutes les règles actives sur toutes les entrées de vulnérabilité. Vous pouvez également ajuster les vulnérabilités existantes en appliquant les règles de classification nouvellement créées aux vulnérabilités existantes.

Avant de commencer
Rôle requis : sn_vul.manage_classification_rule

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Administration** > **Règles de classification de vulnérabilité**.
2. Pour sélectionner une règle, cochez la case en regard de celle-ci.
3. Cliquez sur **Appliquer les changements**.
4. Cliquez sur **Réappliquer**.

Désactiver ou supprimer une règle de classification

Désactivez ou supprimez une règle de classification si elle n'est plus nécessaire ou pertinente.

Avant de commencer

Rôle requis : sn_vul.manage_classification_rule

Pourquoi et quand exécuter cette tâche

Lorsqu'une règle de classification est désactivée ou supprimée, les données qui ont été renseignées dans les champs **Classification** et **Classification_type** par cette règle supprimée restent dans leurs tables respectives.

Si vous souhaitez effacer ces données, créez une règle avec des valeurs vides dans les champs **Classification** et **Classification_type** et réappliquez le groupe. Une fois cette nouvelle règle réappliquée, les changements sont reflétés sur tous les enregistrements auxquels elle s'applique, en fonction des conditions de la règle.

À partir de la version 24.0.6 de , si une règle de Réponse aux vulnérabilités classification est supprimée ou désactivée, elle n'est plus appliquée à l'élément détecté ou à l'entrée de vulnérabilité et les données des champs **Classification** et **Classification_type** sont effacées.

Procédure

1. Accédez à la **Tous** > **Vulnérabilité** > **Administration** > **Règles de classification de vulnérabilité**.
2. Pour sélectionner la règle que vous souhaitez supprimer, cochez la case située en regard de la règle.
3. Pour supprimer la règle, effectuez l'une des opérations suivantes :
   - Dans la liste Action sur les lignes sélectionnées, cliquez sur **Supprimer**.
   - Sélectionnez la règle et cliquez sur le bouton **Supprimer** .
4. Cliquez sur **Appliquer les changements**.

> **Remarque :** Si vous ne cliquez pas sur ce bouton, la règle continue de résider dans le système. Les vulnérabilités référencées par la règle continuent de les référencer.

Créer une règle d'exclusion

Créez une règle pour filtrer ou empêcher les détections d'être converties en éléments vulnérables (VIT) lors de l'ingestion.

Avant de commencer

Rôle requis : administrateur de vulnérabilité

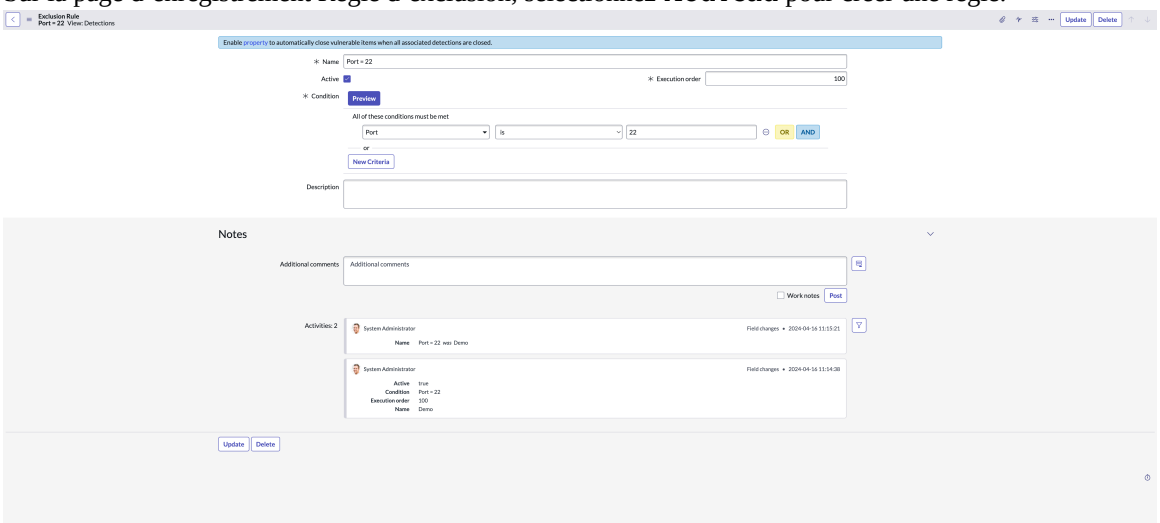
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Règles d'exclusion**.
2. Sur la page d'enregistrement Règle d'exclusion, sélectionnez **Nouveau** pour créer une règle.



Un message indiquant « Activer la propriété pour fermer automatiquement les éléments vulnérables lorsque toutes les détections associées sont fermées » s'affiche. Par défaut, la propriété est inactive. Pour activer, sélectionnez le lien de la propriété et entrez la valeur Vrai dans le champ **Valeur** .

3. Remplissez les champs du formulaire.

Formulaire Règle d'exclusion

Champ	Description
Nom	Nom de la règle d'exclusion.
Actif	Option permettant d'activer la règle d'exclusion.
Ordre d'exécution	Ordre unique pour chaque règle d'exclusion.
Condition	Conditions de filtre pour les détections qui peuvent être définies lors de leur traitement. **Remarque :** Vous ne pouvez pas sélectionner les conditions de champ Règle d'exclusion ou Élément de vulnérabilité.
Description	Description de la règle d'exclusion.

4. Sélectionnez **Soumettre**.
   L'activité est enregistrée dans le système.

Remarque : Une fois qu'une règle d'exclusion est créée, elle s'applique aux détections à partir de l'ingestion suivante.

Gestion des changements Tâches pour Réponse aux vulnérabilités

À partir de tâches de rattrapage (RT), créez des demandes de changement, associez des RT à des demandes de changement existantes ou divisez les tâches de rattrapage en nouvelles tâches avec des sous-ensembles d'éléments vulnérables (VI).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créez et gérez des demandes de changement directement à partir d'une tâche de rattrapage si un processus manuel et contrôlé de quelque nature que ce soit est nécessaire pour modifier ou supprimer des éléments de configuration (CI) pris en charge dans votre CMDB. La création et la gestion des demandes de changement directement à partir d'un enregistrement vous aident à enquêter et à résoudre rapidement les vulnérabilités.

Pour obtenir une vue d'ensemble du fonctionnement de Gestion des changements avec l'application et la Réponse aux vulnérabilités configuration requise, reportez-vous Change Management pour Réponse aux vulnérabilités à la section .

Consultez les rubriques suivantes pour savoir comment créer des demandes de changement, associer des tâches de rattrapage à des demandes de changement existantes et diviser les tâches de rattrapage. Consultez la rubrique Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage pour plus d'informations sur la façon dont les champs d'état sur les demandes de changement (CHG) résolvent automatiquement les tâches de rattrapage.

Créer une demande de changement à partir d'une tâche de rattrapage

En tant que propriétaire d'un rattrapage informatique, créez une demande de changement (CHG) directement à partir d'une tâche de rattrapage (VUL) pour tous les éléments vulnérables du groupe. Créez une demande de changement avec des informations pré-renseignées qui incluent la solution privilégiée pour accélérer votre enquête sur les vulnérabilités qui nécessitent une intervention manuelle.

Avant de commencer
Rôles requis : Pour créer une demande de changement : tout utilisateur disposant du rôle itil. Le rôle sn_vul.remediation_owner est également automatiquement attribué lorsque le rôle itil est attribué à un utilisateur.

Rôle requis : pour l'approbation des demandes de changement : utilisateurs disposant de rôles itil, admin, sn_change_write change_manager.

Pourquoi et quand exécuter cette tâche
Pour en savoir plus sur la création d'une demande de changement à partir des espaces de travail, reportez-vous à la Réponse aux vulnérabilités section Créer une demande de changement dans Espace de travail de remédiation IT.

Pour créer une demande de changement à partir de l'environnement classique, suivez les étapes ci-dessous.

Vous pouvez créer, approuver, implémenter, examiner et fermer des demandes de changement directement à partir d'une tâche de rattrapage. Vous pouvez créer trois types de demandes de changement avec des informations pré-remplies à partir d'une tâche de rattrapage :

- Standard. Un changement pré-autorisé à risque faible, relativement commun et qui suit une procédure ou une instruction de travail spécifique.
- Normal. Les demandes de changement normal suivent un processus prescriptif qui requiert deux niveaux d'approbation avant leur implémentation, revue et fermeture.
- Urgence. Un changement pour résoudre un incident majeur.

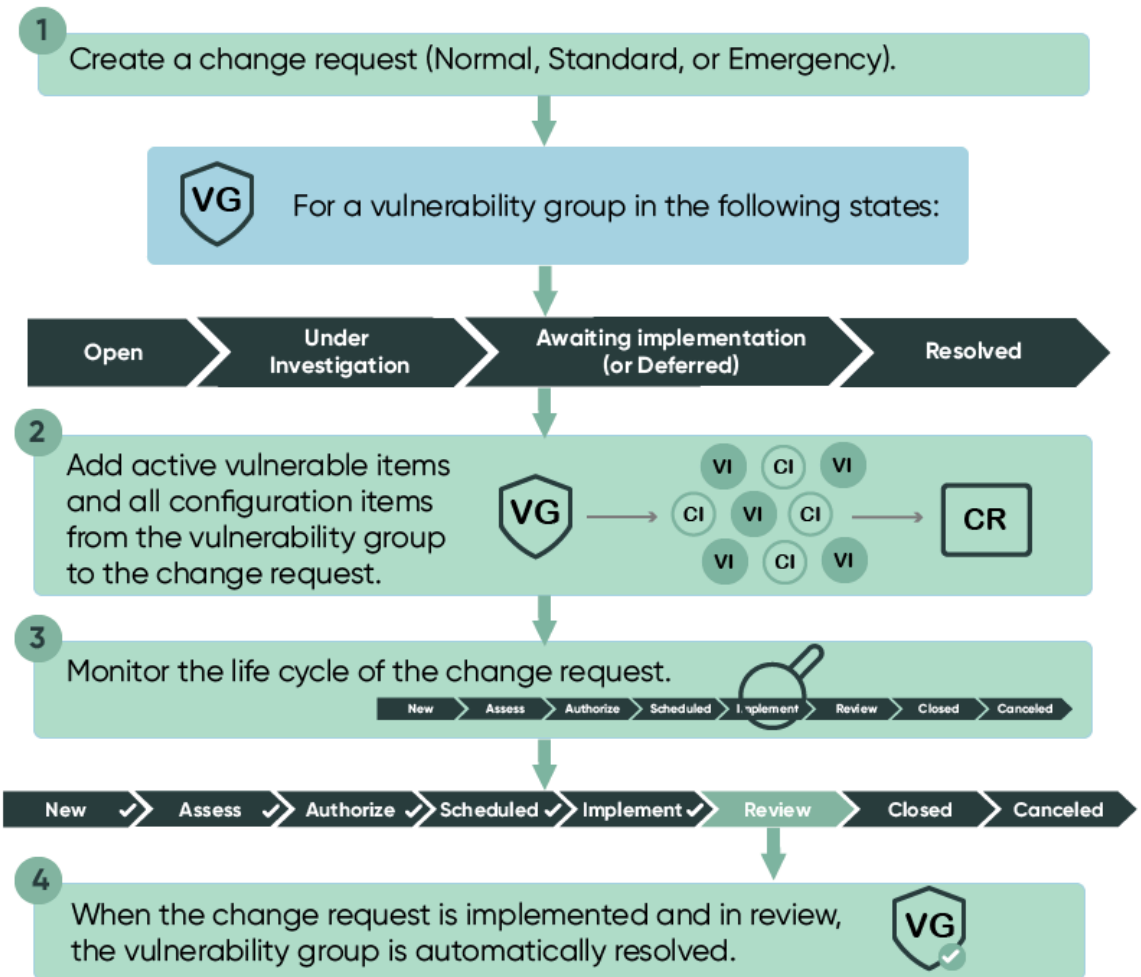
L'image suivante illustre le flux de base pour créer une demande de changement à partir d'une VUL (tâche de rattrapage). Les étapes détaillées de ce flux suivent l'image.

L'enregistrement de tâche de rattrapage est appelé VUL dans les sections suivantes. Dans les versions précédentes de , les tâches de rattrapage étaient appelées groupes de Réponse

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

aux vulnérabilités vulnérabilité (VG). Dans les images suivantes, VG = tâche de rattrapage ou un enregistrement VUL.



Remarque : Points clés sur la création de nouvelles demandes de changement :

- Vous pouvez créer de nouvelles demandes de changement pour n'importe quelle tâche de rattrapage (VUL) dont l'état n'est pas Fermé.
- Vérifiez que vous disposez d'un approbateur pour les demandes de changement autres que Standard (pré-approuvées) que vous créez ou associez à une VUL. Cela accélère le passage de la VUL à la résolution. Pour plus d'informations sur l'ajout d'utilisateurs, reportez-vous à la section Ajouter des utilisateurs au groupe Réponse aux vulnérabilités.
- Avant qu'une tâche de rattrapage puisse être résolue, toutes les tâches sur au moins un CHG associé à la VUL doivent être terminées afin que la demande de changement puisse être implémentée et passer à l'état Réviser .

Procédure

1. Pour créer une demande de changement complète à partir d'un enregistrement de tâche de rattrapage existant, accédez à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**.
   La liste des tâches de rattrapage affectées à votre groupe d'affectation s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. **Facultatif :** Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Aperçu du rattrapage** pour afficher le tableau de bord Vue d'ensemble du rattrapage et localiser une VUL qui vous est affectée ou qui est affectée à votre groupe d'affectation.
3. Sinon, dans la colonne Nombre, cliquez sur une tâche de rattrapage pour ouvrir l'enregistrement et afficher les détails.
   L'enregistrement s'affiche.
4. Une fois l'enregistrement VUL affiché pour lequel vous souhaitez créer la demande de changement, dans l'angle supérieur droit de l'enregistrement, cliquez sur **Créer un changement**.
   Le formulaire Créer une demande de changement s'affiche.
5. Renseignez les champs.

   a. Dans la liste de choix du champ S'applique à, choisissez-en un pour continuer.

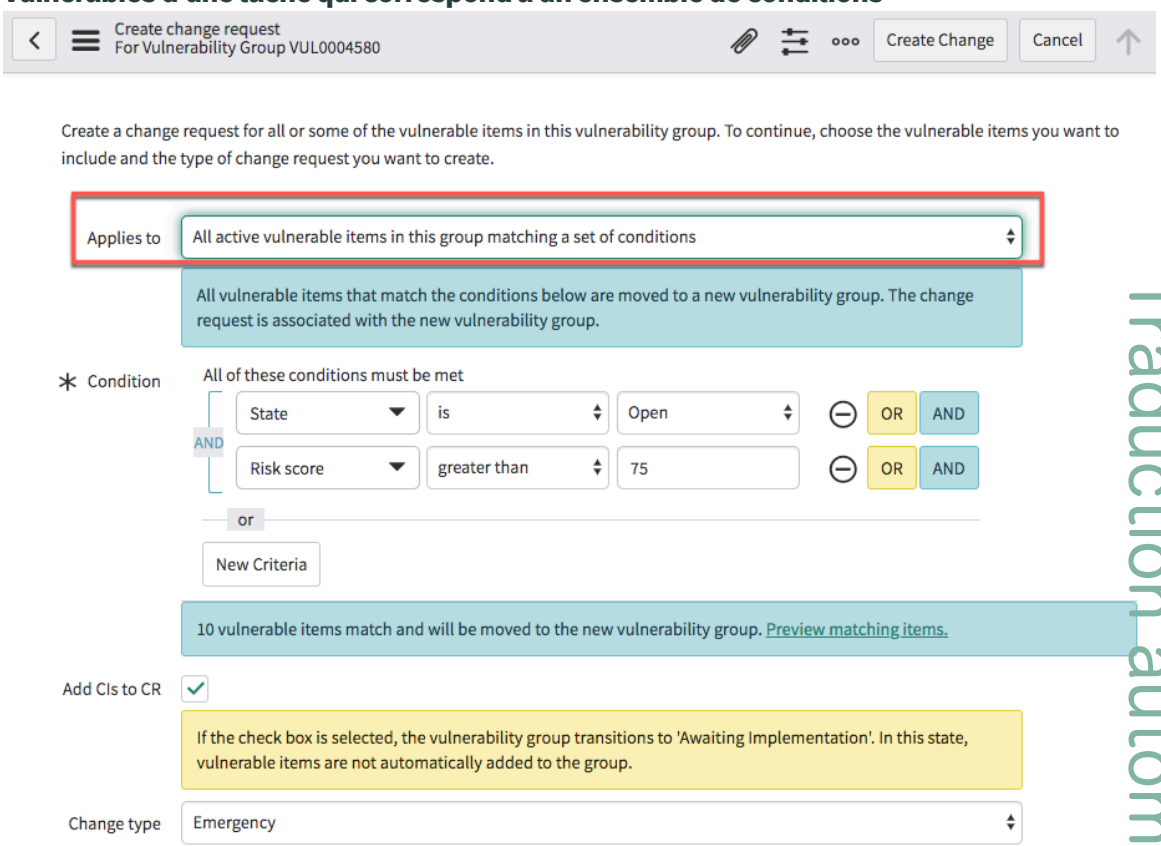
Option	Description
Tous les éléments vulnérables actifs dans ce groupe	Si cette option est sélectionnée, tous les éléments vulnérables actifs de cette tâche de rattrapage dont l'état n'est pas Fermé sont ajoutés automatiquement à la demande de changement une fois que vous avez cliqué sur **Créer un changement**.
Tous les éléments vulnérables de ce groupe correspondant à un ensemble de conditions	S'il est sélectionné, le générateur de conditions s'affiche comme illustré dans la deuxième figure ci-dessous. Entrez des critères de filtre pour identifier les éléments vulnérables que vous souhaitez pour la nouvelle demande de changement. Un exemple de filtre peut inclure uniquement les éléments vulnérables qui correspondent à des critères de recherche spécifiques : **L'état est Ouvert** et le **score de risque est supérieur à 75**. Une fois que vous avez entré vos conditions, un message s'affiche avec le nombre d'éléments vulnérables qui correspondent à vos critères (10). Un lien (**Afficher l'aperçu des éléments correspondants**) permettant de prévisualiser les éléments correspondants s'affiche. Si aucun élément ne correspond à vos conditions de filtre, un message s'affiche sous le générateur de conditions pour vous demander d'ajuster votre filtre. Une fois que vous avez cliqué sur **Créer un changement**, tous les éléments vulnérables qui correspondent à ce filtre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	de condition sont déplacés vers une nouvelle tâche de rattrapage. Cette demande de changement est associée à la nouvelle tâche de rattrapage.

Créer un formulaire de demande de changement pour les éléments vulnérables d'une tâche qui correspond à un ensemble de conditions



b. Facultatif : S'il est affiché sur le formulaire, cliquez sur le lien **Aperçu des éléments correspondants** pour obtenir une liste des éléments vulnérables qui correspondent à vos critères de filtre.
L'aperçu de la liste des tâches de rattrapage s'affiche. Vous pouvez sélectionner des éléments dans cette liste d'aperçu et y effectuer des actions d'interface utilisateur, mais ces actions sont également effectuées sur la VUL. Par exemple, si vous supprimez un VI de la liste d'aperçu, ce VI est également supprimé de la VUL.

c. Une fois que vous avez terminé votre aperçu, fermez la fenêtre du navigateur pour renvoyer le formulaire de demande de changement.

d. Pour la case à cocher Ajouter des CI au CR, choisissez-en un pour continuer.

Option	Description
Case à cocher Ajouter des CI au CR sélectionnée	Sélectionné par défaut. Si la case à cocher est sélectionnée, tous les éléments de configuration (CI) qui appartiennent aux éléments vulnérables actifs dans cette tâche de rattrapage sont ajoutés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	à cette demande de changement. La VUL passe automatiquement à l'état En attente d'implémentation .
Case Ajouter des CI au CR décochée	Décochez la case si vous ne souhaitez pas que les CI des éléments vulnérables actifs de cette tâche de rattrapage soient ajoutés à la nouvelle demande de changement. Lorsqu'elle est désactivée, l'état de la demande de changement n'est pas synchronisé avec la VUL et la VUL reste dans son état actuel.

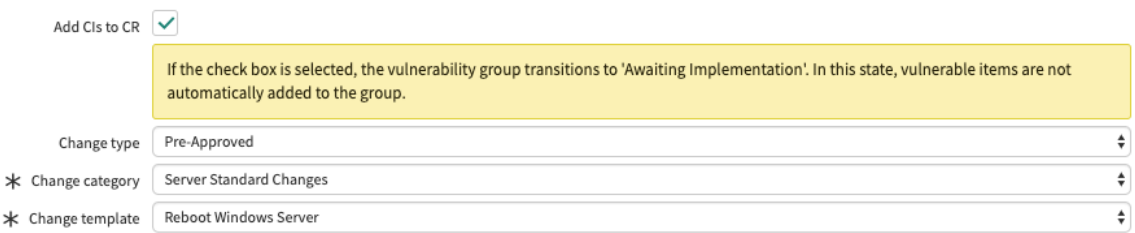
e. Dans la liste de choix du champ Type de changement, choisissez-en un pour continuer.

Type de changement	Description
Urgence	Un changement pour résoudre un incident majeur.
Normal	Type de changement utilisé pour implémenter un changement apporté à un service qui n'est ni standard ni urgent.
Standard	Demande de changement préautorisée et à faible risque fréquemment implémentée. Les demandes de changement standard approuvées peuvent être prédéfinies dans un catalogue de modèles pour améliorer l'accès et le processus de demande d'un changement standard. Si cette option est sélectionnée, deux champs s'affichent comme illustré dans la figure suivante. Sélectionnez-en un dans chaque liste de choix pour remplir ces champs : ▪ Catégorie de changement : sélectionnez une catégorie pour le changement dans votre catalogue existant, par exemple, Matériel, Changements standard du serveur, Logiciel. Dans cet exemple, l'option Appliquer des correctifs aux changements standard est sélectionnée. ▪ Modèle de changement : sélectionnez un modèle disponible pour les demandes de changement avec des tâches de prise en charge prédéfinies à partir de votre catalogue. Dans cet exemple, le modèle du cycle d'application de correctif mensuel Microsoft est sélectionné. Pour en savoir plus sur les catégories de demandes de changement ITSM, les modèles et les types de changements, consultez Types de changements .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La fonctionnalité lit automatiquement les types de demandes de changement que vous configurez dans votre catalogue dans Gestion des changements ITSM. Par exemple, si vous changez le nom de vos demandes de changement standard dans ITSM de Standard à Préapprouvé, votre nouveau nom s'affiche automatiquement dans la liste de choix Type de changement de l'onglet Créer une demande de changement à partir de comme illustré dans la figure suivante.



Les champs de la section Aperçu de la demande de changement du formulaire sont pré-remplis avec des informations provenant de la VUL. Si nécessaire, ces valeurs de champ peuvent être modifiées. Par exemple, examinez les valeurs dans les champs de la figure suivante :

Date de fin prévue

Cette date (10/10/2019) est la même que celle affichée dans le champ Date cible de rattrapage de la VUL. Cette valeur est dérivée de la date cible de rattrapage la plus précoce des éléments vulnérables qui appartiennent à la VUL. Si vous créez une demande de changement pour un problème critique qui nécessite une date de rattrapage antérieure, vous préférez peut-être modifier cette valeur et la valeur dans le champ Priorité.

Justification

Ce champ affiche le nombre de CI ajoutés au CHG. Si vous souhaitez ajouter des informations supplémentaires, vous préférerez peut-être modifier ce texte. Par exemple, vous préférerez peut-être ajouter une note dans ce champ sur le filtre que vous avez utilisé pour créer la nouvelle VUL, par exemple, un score de risque supérieur à 75. Ce texte peut vous aider à localiser votre nouvelle demande de changement et tâche de rattrapage.

Plan d'implémentation

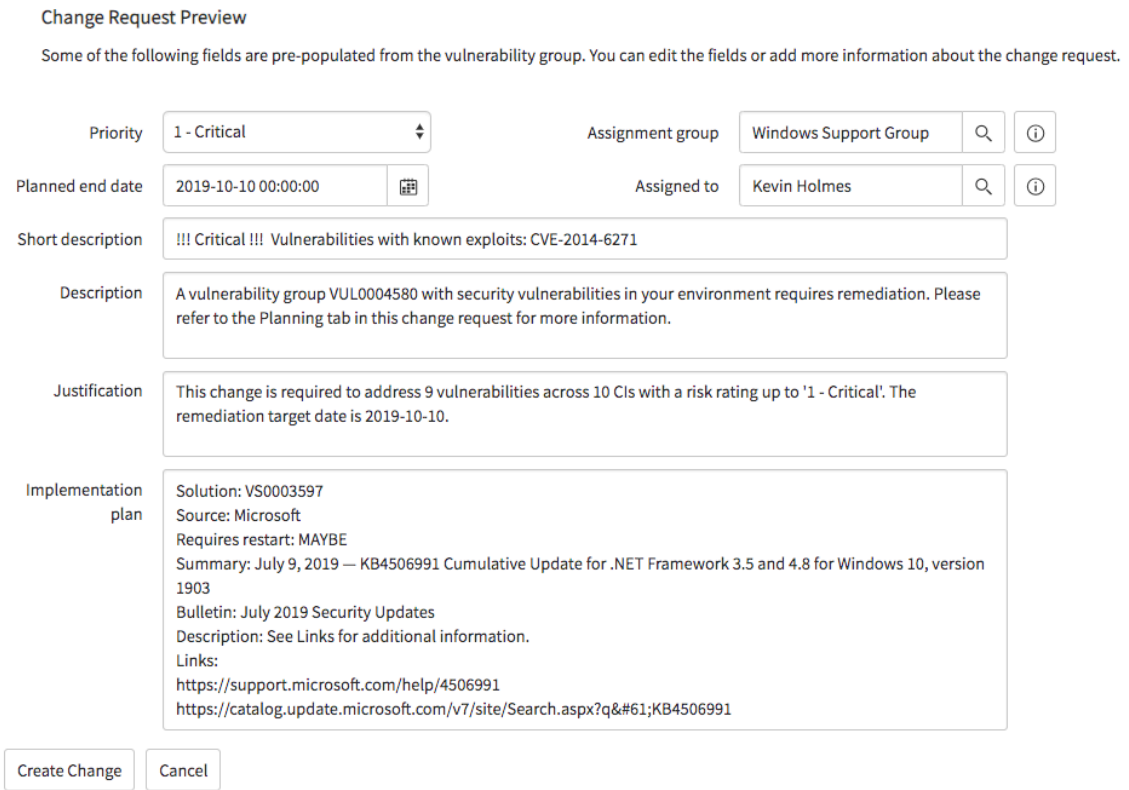
Ce champ affiche la solution préférée pour la vulnérabilité.

Groupe d'affectation et Affecté à

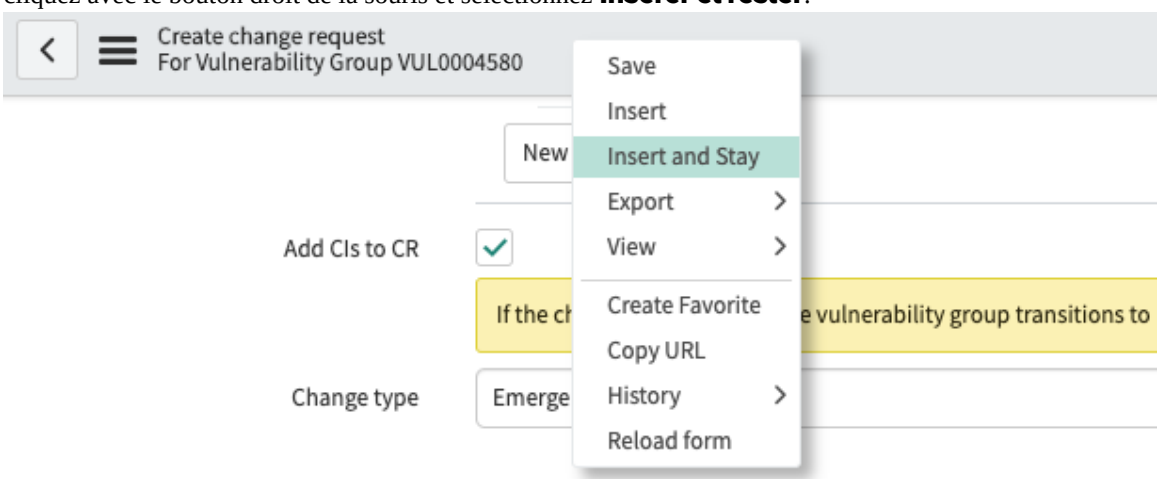
Modifiez ces champs pour modifier le groupe d'affectation ou réaffecter cette demande de changement à un utilisateur de l'un de vos groupes d'affectation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Continuez à prévisualiser et modifiez les champs au besoin.
7. Pour enregistrer vos changements et rester sur cette page, dans la bannière grise en haut du formulaire, cliquez avec le bouton droit de la souris et sélectionnez **Insérer et rester**.



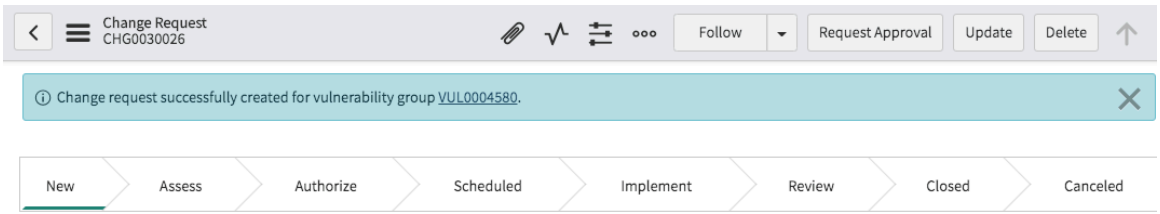
8. Une fois vos modifications terminées, choisissez-en une pour continuer.

Option	Description
Créer un changement	Votre demande de changement est créée et la nouvelle demande de changement s'affiche dans l'état Nouveau . En haut, des messages indiquant que la demande de changement a été créée avec succès avec le nombre d'éléments vulnérables qui ont été ajoutés, comme illustré dans la figure suivante, s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Si la synchronisation de l'état est activée et que la VUL n'est pas déjà dans l'état En cours d'examen, la VUL est automatiquement déplacée dans l'état En cours d'examen et une note de travail est publiée.
Annuler	La demande de changement n'est pas créée et la VUL s'affiche.



Remarque :

Pour une tâche de rattrapage à l'état Ouvert avec le groupe d'affectation et les champs Affecté à non affecté (vide), l'utilisateur connecté actuel est automatiquement affecté à la tâche une fois que vous avez cliqué sur **Créer un changement**. En outre, la case Ajouter des CI au CR doit être cochée. En haut de la VUL, un message de confirmation bleu s'affiche qui indique cette affectation.

Que faire ensuite

Surveillez la demande de changement et les tâches de changement pour vérifier qu'elles sont terminées et que la demande de changement est implémentée. Une fois que ce CHG est implémenté et déplacé vers l'état de révision , si la synchronisation de l'état est activée, la VUL passe automatiquement à l'état Résolu. Pour plus d'informations sur la synchronisation de l'état, reportez-vous à la section Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.

Associer une tâche de rattrapage à une demande de changement existante

En tant que propriétaire d'un rattrapage informatique, évitez de créer des demandes de changement en double (CHG) lorsque vous travaillez à résoudre vos tâches de rattrapage en associant une tâche de rattrapage (VUL) à une demande de changement déjà disponible dans votre instance.

Avant de commencer

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : tout utilisateur disposant du rôle itil. Le rôle sn_vul.remediation_owner est également affecté automatiquement à un utilisateur lorsque le rôle itil est affecté.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur l'association d'une tâche de rattrapage à une demande de changement existante, reportez-vous à la section Créer une demande de changement dans Espace de travail de remédiation IT.

Traduction automatique

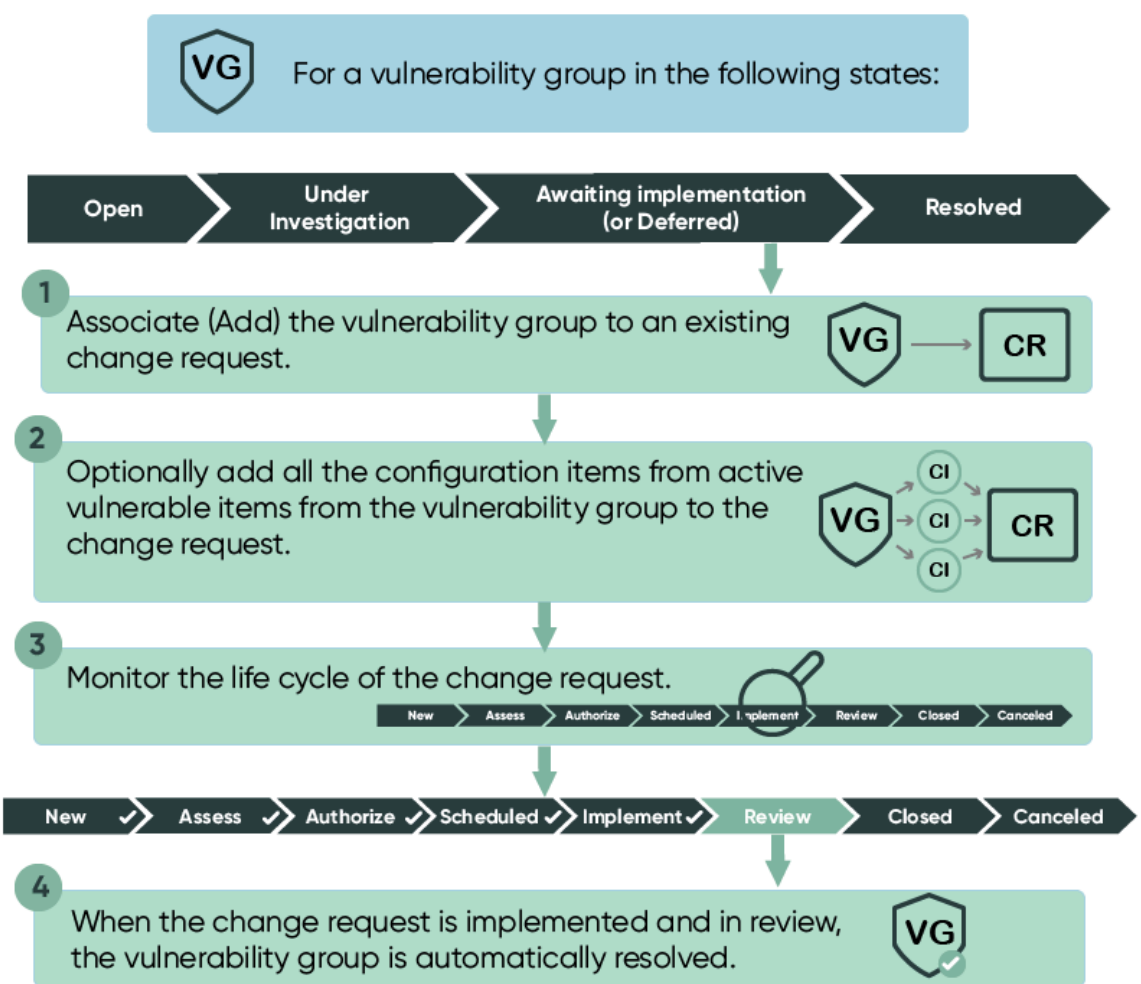
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'enregistrement de tâche de rattrapage est appelé VUL dans les sections suivantes. Dans les versions précédentes de , les tâches de rattrapage étaient appelées groupes de Réponse aux vulnérabilités vulnérabilité (VG). Dans les images suivantes, VG = tâche de rattrapage ou un enregistrement VUL.

Pour plus d'informations sur l'association d'une tâche de rattrapage à une demande de changement existante, reportez-vous à la section Créer une demande de changement dans Espace de travail de remédiation IT.

En tant que propriétaire de rattrapage, vous pouvez associer les tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe d'affectation aux demandes de changement existantes directement à partir des enregistrements de tâche de rattrapage. L'image suivante illustre le flux de base pour associer une demande de changement à une VUL (VG) existante. Les étapes détaillées de ce flux suivent l'image.

Workflow permettant d'associer une tâche de rattrapage à une demande de changement existante



Traduction automatique

Remarque : Vous pouvez associer une demande de changement existante à une VUL dans n'importe quel état (Ouvert, En cours d'examen, En attente d'implémentation, Fermé et Différé). Lorsque vous associez une demande de changement à une VUL existante, seuls les VI actifs sont ajoutés à la demande de changement.

Avant de commencer, afin d'éviter de créer des demandes de changement en double, vous pouvez préférer afficher toutes les demandes de changement existantes déjà associées à une VUL. Pour suivre facilement le nombre de demandes de changement associées

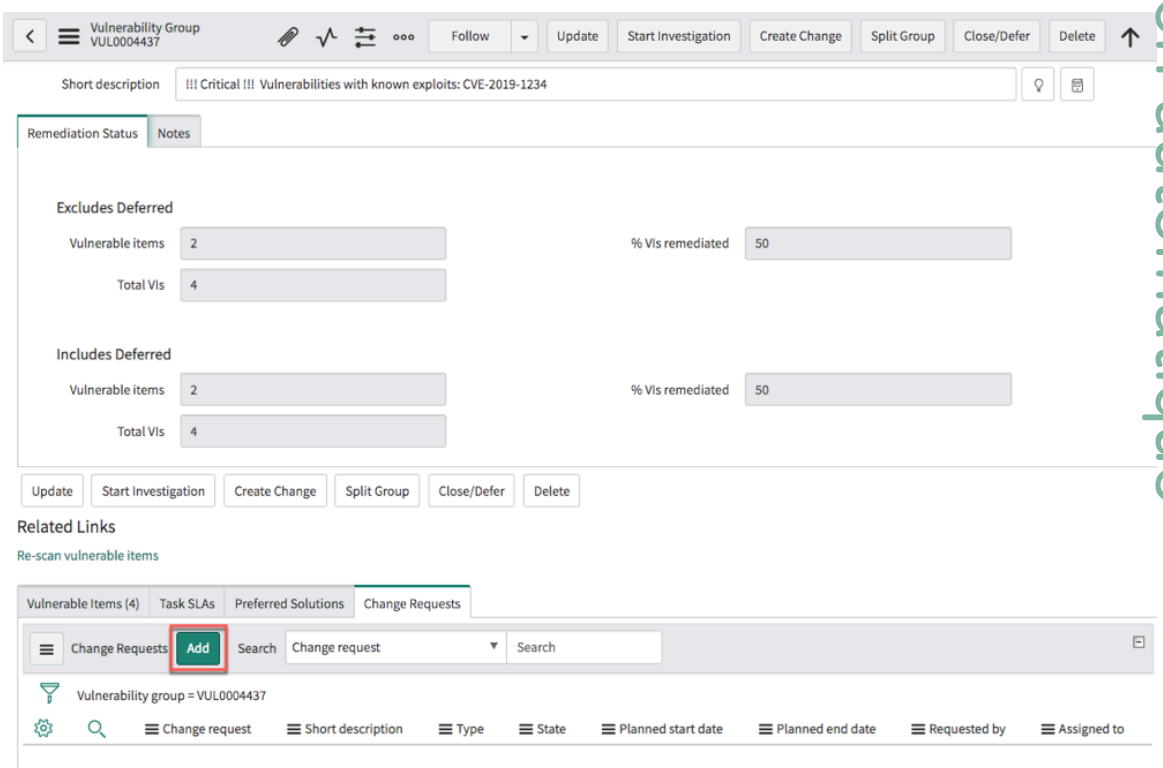
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à une VUL spécifique, reportez-vous à la colonne Nombre de CR de la liste Tâches de remédiation. S'il n'est pas affiché, cliquez sur l'icône Paramètres (icône en haut à droite. Déplacez la colonne Nombre de CR de Disponible à Sélectionné et cliquez sur **OK**.

Pour remplir automatiquement la nouvelle colonne, pour les clients ayant des données existantes dans cette table, exécutez le travail planifié : Remplir la nouvelle colonne Nombre de CR.

Procédure

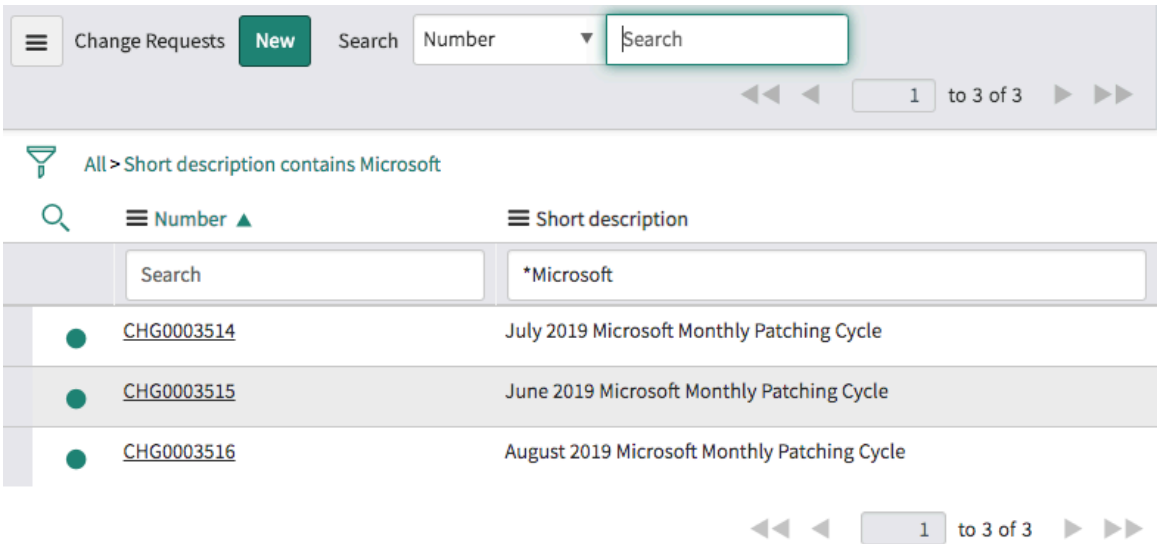
1. Pour associer une tâche de rattrapage à une demande de changement existante, accédez à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Localisez la tâche de rattrapage avec laquelle vous travaillez.
3. **Facultatif :** Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Aperçu du rattrapage** pour afficher le tableau de bord Vue d'ensemble du rattrapage et localiser une VUL qui vous est affectée ou qui est affectée à votre groupe d'affectation.
4. Dans la colonne Numéro, cliquez sur un enregistrement VUL pour l'ouvrir.
   L'enregistrement VUL s'affiche.
5. Une fois l'enregistrement ouvert affiché, s'il ne l'est pas déjà, accédez à la liste connexe Demandes de changement et sélectionnez-la.
   Toutes les demandes de changement associées à la VUL sont affichées avec le bouton **Ajouter** . Dans la figure suivante, aucune demande de changement n'est déjà associée à cette VUL.



6. Pour associer la VUL à un CHG existant, cliquez sur **Ajouter**.
   Le formulaire Ajouter une demande de changement existante à une tâche de rattrapage s'affiche.
7. Dans le formulaire, cliquez sur l'icône de recherche.
   Une vue de liste des demandes de changement existantes s'affiche dans une nouvelle fenêtre, comme illustré dans la figure suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Sélectionnez un élément dans la liste affichée, ou cliquez sur le filtre (icône et entrez des conditions pour limiter les résultats de votre recherche.
9. Pour la case à cocher Ajouter des CI au CR, choisissez-en un pour continuer.

Remarque : Cette case à cocher s'affiche uniquement pour les demandes de changement existantes dans l'état Nouveau .

Option	Description
Case à cocher Ajouter des CI au CR sélectionnée	Sélectionné par défaut. Si la case à cocher est sélectionnée, tous les éléments de configuration (CI) qui appartiennent aux éléments vulnérables actifs dans cette tâche de rattrapage sont ajoutés à cette demande de changement. Lorsque cette option est sélectionnée, l'état de la demande de changement est synchronisé avec la VUL. Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.
Case Ajouter des CI au CR décochée	Décochez la case si vous ne souhaitez pas que les CI des éléments vulnérables actifs de cette tâche de rattrapage soient ajoutés à la nouvelle demande de changement. Lorsqu'elle est désactivée, l'état de la demande de changement n'est pas synchronisé avec la VUL et la VUL reste dans son état actuel.

10. Une fois le numéro de demande de changement que vous souhaitez afficher dans le champ Rechercher une demande de changement, cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La VUL s'affiche. En haut de l'enregistrement, le message bleu de confirmation s'affiche, indiquant que la demande de changement que vous avez sélectionnée est correctement associée à la VUL.

Remarque : Pour une VUL à l'état Ouvert avec le groupe d'affectation et les champs Affecté à non affectés (vides), l'utilisateur connecté actuel est automatiquement affecté à la VUL après avoir cliqué sur **Ajouter**. En outre, la case Ajouter des CI au CR doit être cochée. En haut de la VUL, un message de confirmation bleu s'affiche et indique que l'utilisateur actuel est affecté.

Que faire ensuite

Examinez l'enregistrement VUL. Dans la colonne Demande de changement de la liste connexe Demandes de changement, cliquez sur le lien du nouveau CHG pour afficher l'enregistrement CR. Dans l'enregistrement CHG ouvert, vous pouvez surveiller l'état de la demande de changement. Les éléments de configuration (CI) affectés et les tâches de rattrapage sont affichés dans les listes connexes CI affectés et tâches de rattrapage.

Fractionner une tâche de rattrapage

En tant que propriétaire d'un rattrapage informatique, à partir d'une tâche de rattrapage existante (VUL), identifiez un sous-ensemble d'éléments vulnérables (VI) que vous souhaitez déplacer vers un nouveau groupe.

Avant de commencer

Remarque :

Les cas d'utilisation pour diviser les VI à partir de VUL existants en nouvelles tâches de rattrapage peuvent inclure les exemples suivants :

- Lorsque vous souhaitez créer une demande de changement ou des demandes de changement pour une tâche fractionnée.
- Lorsque vous réaffectez un groupe divisé à un autre utilisateur de votre groupe d'affectation.
- Lorsque vous demandez un report ou une exception pour une tâche fractionnée, car vous savez que certaines vulnérabilités sur des éléments de configuration (CI) spécifiques ne peuvent pas être corrigées dans un délai donné.

Rôle requis : tout utilisateur ayant le rôle itil pour fractionner une VUL.

Remarque : Le rôle sn_vul.remediation_owner est également automatiquement attribué lorsque le rôle itil est attribué à un utilisateur.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la division des tâches de rattrapage dans les espaces de travail, reportez-vous à la Réponse aux vulnérabilités section Fractionner une tâche de rattrapage dans le Espace de travail de remédiation IT.

Pour diviser une tâche de rattrapage dans l'environnement classique ou pour des versions de Réponse aux vulnérabilités.

Vous pouvez diviser les tâches de rattrapage existantes avec plusieurs éléments vulnérables à l'état Ouvert, En cours d'examen ou En attente d'implémentation. En créant une nouvelle VUL avec des éléments vulnérables qui correspondent à des critères spécifiques, vous pouvez travailler avec un groupe spécifique d'éléments vulnérables sans impact sur la tâche de rattrapage d'origine.

Lorsque vous spécifiez les conditions pour les éléments vulnérables que vous souhaitez déplacer vers une nouvelle tâche de rattrapage avec le générateur de conditions, seuls les VI actifs qui correspondent à vos critères sont déplacés vers le nouveau groupe.

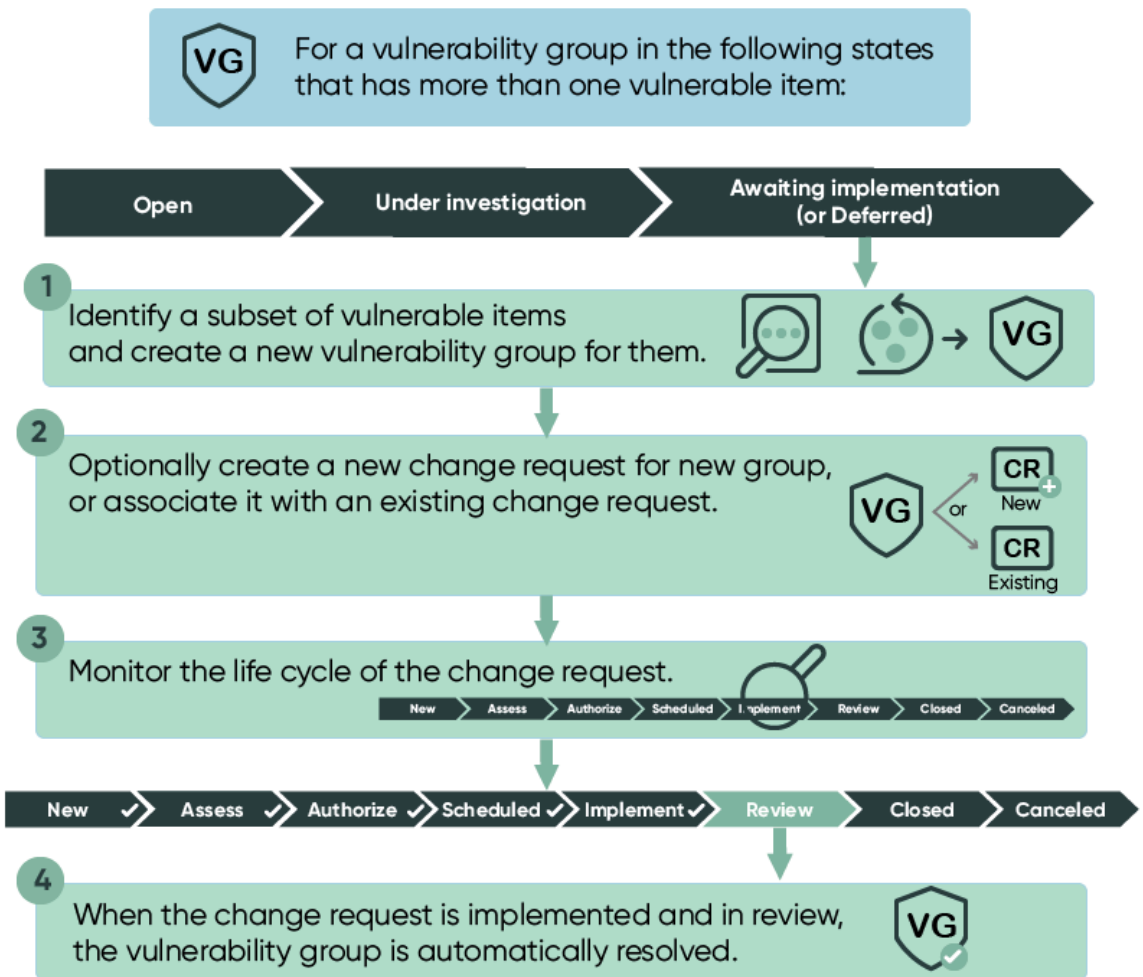
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous n'êtes pas tenu de créer des demandes de changement (CHG) lorsque vous fractionnez une VUL. Vous avez la possibilité de diviser une VUL en même temps que vous créez une demande de changement, ou vous pouvez diviser une VUL sans créer de demande de changement. L'image suivante illustre le flux de base pour diviser une tâche de rattrapage. Les étapes détaillées de ce flux suivent l'image.

L'enregistrement de tâche de rattrapage est appelé VUL dans les sections suivantes. Dans les versions précédentes de , les tâches de rattrapage étaient appelées groupes de Réponse aux vulnérabilités vulnérabilité (VG). Dans les images suivantes, VG = tâche de rattrapage ou un enregistrement VUL.

Workflow pour diviser une tâche de rattrapage

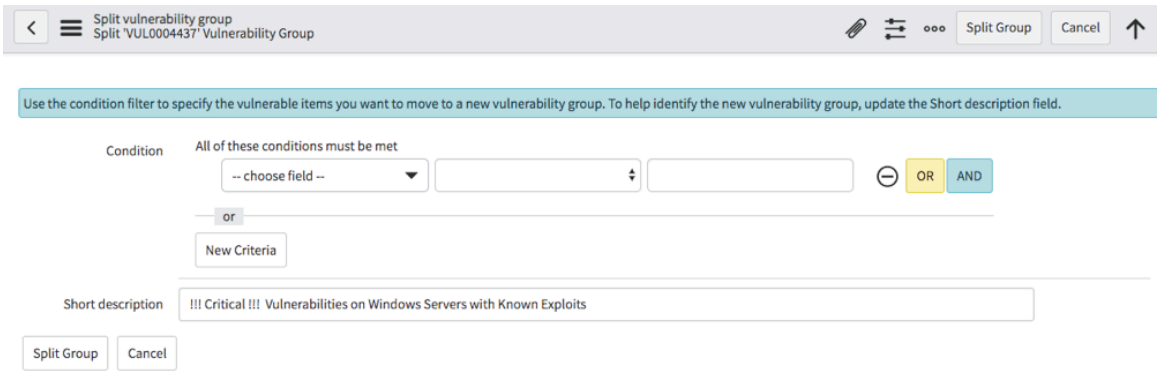


Traduction automatique

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**.
   La liste des tâches de remédiation s'affiche.
2. Dans la colonne Nombre, cliquez sur un enregistrement pour l'ouvrir.
   L'enregistrement s'affiche.
3. En haut à droite de la VUL, cliquez sur **Fractionner la tâche**.
   Le formulaire Diviser le formulaire de tâche de rattrapage s'affiche.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

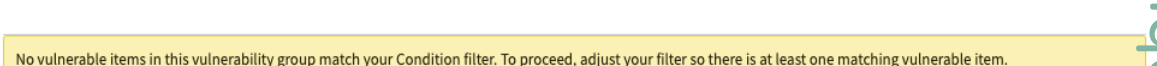


4. Une fois le filtre de condition affiché, spécifiez les conditions pour les éléments vulnérables que vous souhaitez déplacer vers une nouvelle tâche.
   Par exemple, vous préférez peut-être filtrer uniquement les éléments vulnérables qui correspondent aux conditions suivantes :
   - Dans les états ouverts .
   - Scores de risque supérieurs à 80.
   - Éléments de configuration contenant « WINSV ».
   - Situé à San Diego.

   Par exemple, pour les conditions, vous pouvez saisir :
   - État : est : ouvert
   - Le score de risque est supérieur ou égal à 80
   - Élément de configuration . Nom - contient - WINSV
   - Élément de configuration . Emplacement - est - San Diego

   Si les éléments vulnérables correspondent à votre filtre après avoir saisi les conditions, un message s'affiche avec le nombre d'éléments vulnérables correspondants.

   Remarque : Si un message indiquant qu'aucun élément vulnérable ne correspond à votre filtre, ajustez les conditions de sorte qu'au moins un élément vulnérable corresponde à vos critères de filtre.

5. **Facultatif :** Ajustez le filtre selon vos besoins.
6. **Facultatif :** Pour vous aider à identifier la nouvelle VUL après sa création, vous pouvez préférer mettre à jour le champ Brève description.
   S'il est modifié, utilisez le champ Description brève comme critère de recherche pour la nouvelle VUL afin de vous aider à la localiser après sa création, par exemple, SITUÉ À SAN DIEGO.
7. **Facultatif :** Pour prévisualiser les détails des éléments vulnérables qui correspondent à vos critères de filtre, procédez comme suit avant de cliquer sur **Diviser la tâche** pour créer la nouvelle VUL.
   Ces détails incluent les demandes de changement existantes qui sont déjà associées à ce sous-ensemble et les VUL avec ces éléments vulnérables. L'affichage de ces informations dans l'aperçu peut vous empêcher de créer des VUL en double.

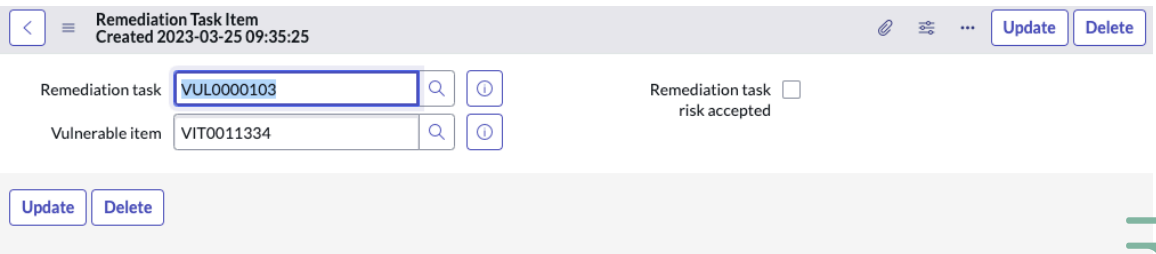
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans le message de confirmation bleu sur le formulaire de tâche de rattrapage fractionné, cliquez sur **Afficher l'aperçu des éléments correspondants**.
La liste des éléments de la tâche de rattrapage s'affiche dans une nouvelle fenêtre dans votre navigateur avec une liste des éléments vulnérables qui correspondent à vos conditions.

b. Dans la colonne Numéro, cliquez sur un élément pour ouvrir l'enregistrement.

c. Dans l'enregistrement qui s'affiche, à droite des champs du groupe de vulnérabilité ou de l'élément de vulnérabilité, cliquez sur l'icône d'informations de l'élément vulnérable pour afficher les enregistrements.



d. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement**.
Les informations relatives à la date cible de rattrapage s'affichent. Dans la section Listes connexes, cliquez sur une liste connexe pour afficher plus d'informations sur le VI.

8. Lorsque vous êtes prêt à créer la nouvelle VUL avec le ou les VI qui répondent à vos conditions, fermez la fenêtre d'aperçu pour revenir au formulaire de fractionnement de tâche dans l'autre fenêtre et, en haut du formulaire, cliquez sur **Fractionner la tâche**.

Remarque :

Pour les VI inférieurs à 200, l'opération de division est effectuée de manière synchrone.

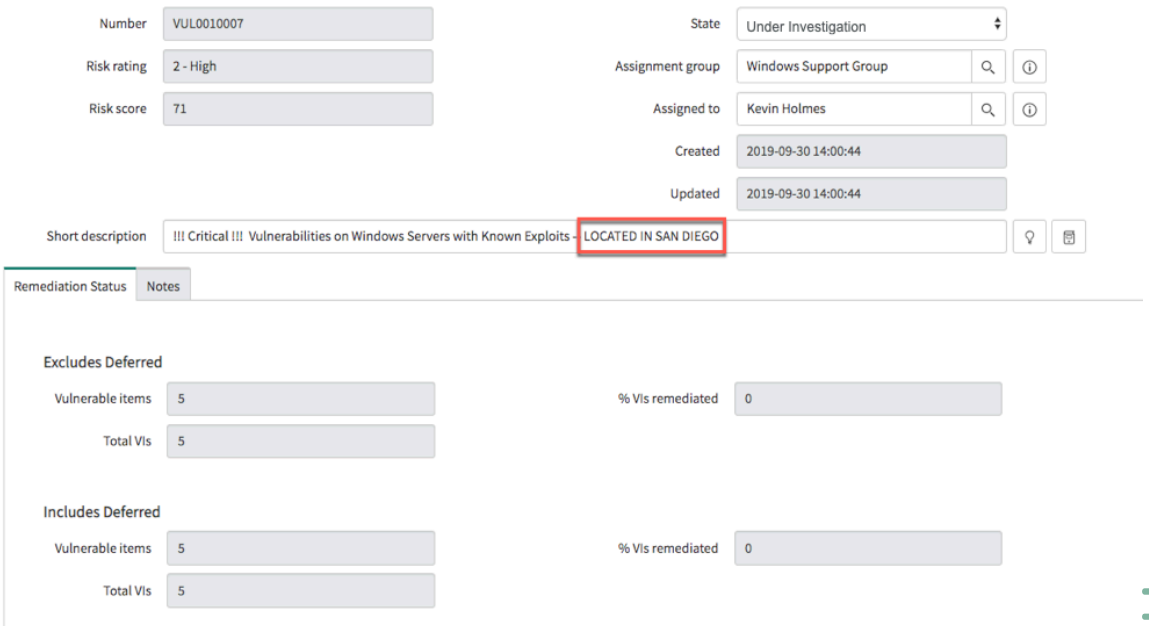
Pour plus de 200 VI, l'opération de division est effectuée de manière asynchrone en arrière-plan, et l'apparition des VI dans le nouveau groupe peut prendre quelques secondes.

Un message de confirmation s'affiche et affiche tous les VI actifs qui sont déplacés vers le nouveau groupe. Le nouveau numéro de tâche de rattrapage est également affiché. S'il n'est pas déjà dans En cours d'examen, le VUL est déplacé vers En cours d'examen. Vérifiez le champ Brève description pour le texte que vous avez saisi pour la nouvelle VUL dans le (SITUÉ À SAN DIEGO).

Des calculs de déploiement sur le nouveau groupe sont effectués pour calculer son nouveau score de risque, sa date cible de rattrapage et d'autres valeurs de champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les éléments vulnérables, les solutions privilégiées et les demandes de changement sont affichés dans les listes connexes situées au bas de l'enregistrement. Traitez et surveillez cette nouvelle tâche comme vous le feriez avec n'importe quelle tâche de rattrapage.

9. **Facultatif :** Faites défiler la page jusqu'à la liste connexe **Notes** et cliquez pour la sélectionner. Confirmez que le nombre d'éléments vulnérables de la tâche de rattrapage initiale a été déplacé vers le nouveau groupe dans le flux d'activité.
10. **Facultatif :** Sur la nouvelle VUL, pour sélectionner et diviser à nouveau les VI à partir de la liste connexe Éléments vulnérables, faites défiler jusqu'au bas de l'enregistrement de tâche de rattrapage et, avec les VI que vous souhaitez déplacer sélectionnés dans la colonne Élément vulnérable de la liste connexe Éléments vulnérables, dans la liste de choix Actions sur les lignes sélectionnées, sélectionnez **Fractionner la tâche**. Le formulaire Diviser le formulaire de tâche de rattrapage s'affiche.
11. Pour diviser à nouveau le groupe et déplacer les éléments sélectionnés vers un nouveau groupe, cliquez sur **Fractionner la tâche**.
Les VI sélectionnés sont déplacés vers une autre tâche de rattrapage, le message de confirmation s'affiche et le nouveau groupe s'affiche.
12. Choisissez-en un pour poursuivre votre examen ou votre correction.

Option	Description
Créer un incident de sécurité	Créer un incident de sécurité.
Créer un changement	Créez une demande de changement pour cette tâche de rattrapage.
Fractionner la tâche	Si le nouveau groupe a plusieurs VI, divisez à nouveau cette tâche de rattrapage pour créer un autre sous-ensemble d'éléments vulnérables.
En attente d'implémentation	Si affiché, déplacez la tâche de l'état En cours d'examen à l'état En attente d'implémentation.
Fermer ou demander une exception	Fermez ou reportez la tâche de rattrapage. Une boîte de dialogue de confirmation s'affiche avec les champs obligatoires suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	○ État ○ Motif ○ Informations supplémentaires Renseignez les champs pour fermer ou différer le groupe, puis cliquez sur **Soumettre**.
Supprimer	Supprimer cette tâche de rattrapage.
État	Déplacez l'enregistrement vers un autre état affiché dans la liste de choix et cliquez sur **Mettre à jour** pour enregistrer vos modifications dans l'enregistrement. **Remarque :** Vous pouvez faire passer manuellement la nouvelle VUL d'un état de cycle de vie à l'autre. Toutefois, si la synchronisation d'état est activée et que le système enregistre qu'une demande de changement associée à la VUL a changé d'état, ou si vous ajoutez un CHG ou le supprimez de la VUL, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.
Groupe d'affectation	Réaffectez la VUL à un groupe d'affectation et cliquez sur **Mettre à jour** pour enregistrer vos changements dans l'enregistrement.
Affecté à	Affectez la VUL à vous-même ou à un utilisateur spécifique d'un autre groupe d'affectation et cliquez sur **Mettre à jour** pour enregistrer vos modifications dans l'enregistrement.

Traduction automatique

Que faire ensuite

Surveillez l'état de la nouvelle VUL pour accélérer sa résolution.

Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage

Il existe une relation synchronisée entre les champs État des tâches de rattrapage (VUL) et les champs État des demandes de changement (CHG) dans le Réponse aux vulnérabilités produit. Au fur et à mesure qu'une demande de changement progresse dans son cycle de vie, elle modifie automatiquement l'état de toutes les tâches de rattrapage connexes.

Synchronisation de l'état

L'enregistrement de tâche de rattrapage est appelé VUL dans les sections suivantes. Dans les versions précédentes de , les tâches de rattrapage étaient appelées groupes de Réponse aux vulnérabilités vulnérabilité (VG). Dans les images suivantes, VG = tâche de rattrapage ou un enregistrement VUL.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La synchronisation de l'état est activée par défaut par une propriété système (sn_vul.cr_state_synch) dans votre instance lorsque vous téléchargez l'application Réponse aux vulnérabilités .

Lorsque la synchronisation de l'état est activée, le champ État du CHG modifie automatiquement le champ État de la tâche de rattrapage dans les cas suivants :

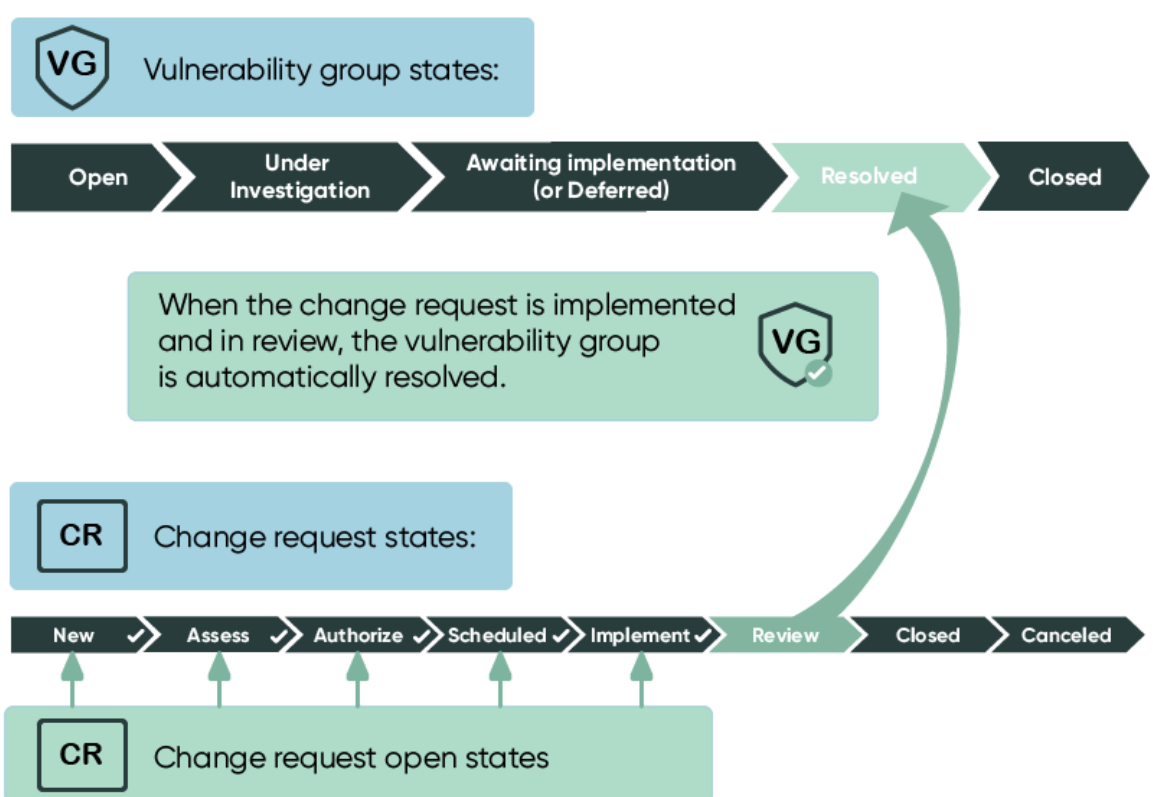
- Lorsqu'un nouveau CHG est créé pour une tâche de rattrapage (VUL), s'il n'est pas en attente d'implémentation, l'état de la VUL passe à En attente d'implémentation.
- Lorsqu'un CHG existant est associé à une VUL, s'il n'est pas en attente d'implémentation, l'état de la VUL passe à l'état En attente d'implémentation.
- Une fois que les tâches d'un CHG sont terminées (implémentées) et que le CHG est passé à l'état de révision , la VUL passe à l'état Résolu.

Pour plus d'informations et d'exemples de synchronisation d'état, consultez les sections suivantes.

Remarque : Vous pouvez toujours déplacer manuellement les CHG et les VUL d'un état à l'autre de leurs cycles de vie sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une VUL, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la VUL des états Fermé ou Différé .

Synchronisation de l'état vers le bas

L'image suivante illustre comment les états CHG déplacent automatiquement les états VUL dans un cycle de vie en avant, c'est-à-dire d'Ouvert à Résolu.



Vous pouvez créer de nouvelles demandes de changement pour n'importe quelle tâche de rattrapage dont l'état n'est pas Fermé. La synchronisation d'état déplace automatiquement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la VUL de manière bidirectionnelle entre les états Ouvert, En cours d'examen, En attente d'implémentation et Résolu . Ce déplacement est basé sur certaines valeurs du champ État de la demande de changement. La synchronisation de l'état entre la demande de changement et la tâche de rattrapage est invoquée automatiquement sauf si la case à cocher (Ajouter des CI au CR) s'affiche sur un formulaire et que vous choisissez de la décocher.

La VUL ne passe pas à l'état Résolu lorsqu'un CHG est dans ses états ouverts. Tous les CHG dont l'état est antérieur à la révision dans leur cycle de vie, tels que Nouveau, Évaluer, Autoriser, Planifié ou Implémenter , comme illustré dans la figure précédente, sont considérés comme des états ouverts pour le CHG. Les états ouverts ne déplacent pas le champ d'état sur la VUL, car les enquêtes ou les tâches sur le CHG ne sont pas terminées. La synchronisation d'état est invoquée lorsqu'un CHG est créé pour ou associé à la VUL, ou que l'état d'une relation existante change sur le CHG. Les états CHG terminés sont Examiner et Fermé avec succès. Lorsqu'un CHG est fermé avec succès, ses codes fermés sont : Réussi ou Réussi avec problèmes, auquel cas la VUL passe à l'état Résolu.

Synchronisation de l'état en arrière

Au fur et à mesure qu'un CHG est traité au cours de son cycle de vie, il peut être annulé à un moment donné. Dans ce cas, si le CHG est annulé ou fermé (avec un code de fermeture En échec), la VUL revient automatiquement à l'état En cours d'examen. La VUL revient à l'état En cours d'examen, car il n'existe aucun plan actif pour corriger la vulnérabilité.

Si une VUL est à l'état Résolu et que vous créez un nouveau CHG ou l'associez à un CHG existant dans l'un des états ouverts initiaux, le VUL revient automatiquement à l'état En attente d'implémentation. La VUL revient à cet état, car une plus grande partie du travail est maintenant affectée au CHG.

VUL avec plusieurs CHG

Si plusieurs CHG sont associés à une VUL en attente d'implémentation , la synchronisation de l'état est basée sur l'état du CHG dans l'état le plus précoce de son cycle de vie. Par exemple, une VUL est associée à quatre CHG, CHG1, CHG2, CHG3 et CHG4, comme indiqué dans la table suivante.

Numéro de CHG	État du changement
1	Implémenter
2	Annulé
3	Fermé (code de fermeture en échec)
4	Fermé (code de fermeture réussi)

La synchronisation d'état entre le CHG et la VUL dans ce cas est basée sur CHG1, qui est dans l'état le plus ancien des quatre CHG, (Implémenter). Dans ce cas, la VUL reste en attente d'implémentation.

Dans un autre exemple, si une VUL est à l'état Résolu et qu'un CHG existant a été implémenté et est à l'état Réviser , et qu'un nouveau CHG est créé, la VUL revient de Résolu à En attente d'implémentation. La synchronisation d'état est basée sur le CHG dans l'état Nouveau , qui est le CHG dans l'état le plus ancien.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro de CHG	État du changement
1	Revue
2	Nouveau

De plus, lorsque les VUL ont plus d'un CHG, l'état de la VUL change automatiquement dans les cas suivants :

- Lorsqu'un CHG passe à l'état Révision, si tous les autres CHG associés à la VUL sont en état Révision ou Fermé (avec un code de fermeture réussi), la VUL passe automatiquement à l'état Résolu. Tous les autres CHG associés qui sont annulés ou fermés sans succès sont ignorés.
- Lorsqu'un CHG passe à l'état Annulé ou Fermé (code de fermeture en échec), si tous les autres CHG associés à la VUL sont dans le même état, la VUL revient automatiquement à l'état En cours d'examen.

Pour en savoir plus sur les états des tâches de rattrapage et sur ce que vous pouvez faire dans chaque état, reportez-vous à la section Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables.

Évaluez votre exposition aux logiciels vulnérables

Vous pouvez fournir des informations sur l'éditeur et le produit dans le module d'évaluation de l'exposition pour évaluer votre exposition zero-day (jour actuel) de vos actifs à des logiciels vulnérables à l'aide de l'application Gestion des actifs logiciels ITSM (SAM) Foundation.

Important : Vous pouvez effectuer l'évaluation de l'exposition par logiciel et par CVE (Common Vulnerabilities and Exposures) pour tirer parti des options supplémentaires de l'espace de travail d'évaluation de la vulnérabilité. Pour plus d'informations, consultez Explorer l'espace de travail de l'évaluation de la vulnérabilité.

Avant de commencer

Rôle requis : administrateur de vulnérabilité (sn_vulnerability_write)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Mettez à disposition les informations suivantes sur le logiciel vulnérable que vous souhaitez évaluer :

- Éditeur
- Version
- Produit
- Édition

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la configuration requise, reportez-vous à Configurer l'évaluation de l'exposition à la vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichez le module d'évaluation de l'exposition logicielle et créez et modifiez des enregistrements d'évaluation de l'exposition à la demande pour les logiciels vulnérables dans votre ServiceNow AI Platform® instance.

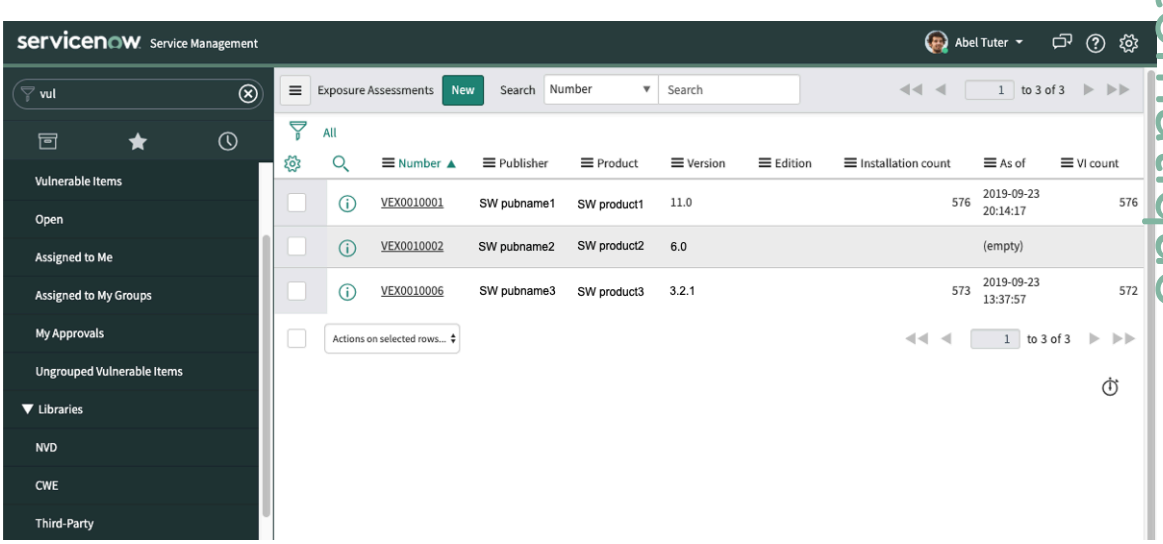
Vous gérez les activités de réponse aux vulnérabilités pour une grande opération responsable de nombreux actifs. Le centre des opérations de sécurité (SOC) de votre opération vous contacte au sujet d'une version du logiciel qu'il a appris être vulnérable. Vous découvrez qu'une analyse de vos actifs a récemment été effectuée et que cette vulnérabilité n'a pas été trouvée. L'équipe SOC a été informée de cette vulnérabilité par une source fiable en dehors de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou des autres bibliothèques tierces de votre instance, et vous craignez que votre scanner de vulnérabilité n'ait pas encore ajouté le module d'extension correspondant.

Vous êtes convaincu que les données de cette vulnérabilité seront bientôt mises à jour dans le NVD et importées afin que votre scanner puisse détecter cette vulnérabilité lors de la prochaine analyse, mais comme vous êtes préoccupé par l'étendue de votre exposition potentielle, vous souhaitez déterminer aujourd'hui si vous avez des actifs dans votre réseau sur lesquels ce logiciel est installé.

À partir de la version 23.0 de , si vous avez l'abonnement Pro ou Enterprise, vous êtes redirigé vers la page **Évaluation de l'exposition** dans les espaces de travail en fonction de votre rôle lors de Réponse aux vulnérabilités la sélection du lien Évaluation de **l'exposition** dans le menu **Tout**. Pour plus d'informations, consultez Configurer l'évaluation de l'exposition à la vulnérabilité.

Procédure

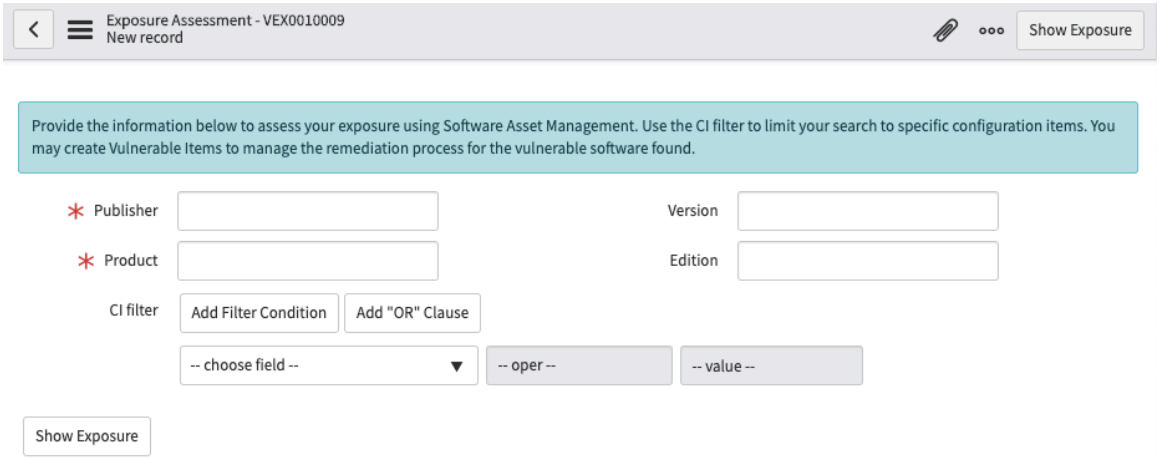
1. Pour créer une nouvelle évaluation de l'exposition, accédez à **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Évaluation de l'exposition**.
   La liste des évaluations de l'exposition s'affiche.



2. Sélectionnez **Nouveau**.
   Le formulaire d'évaluation de l'exposition s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



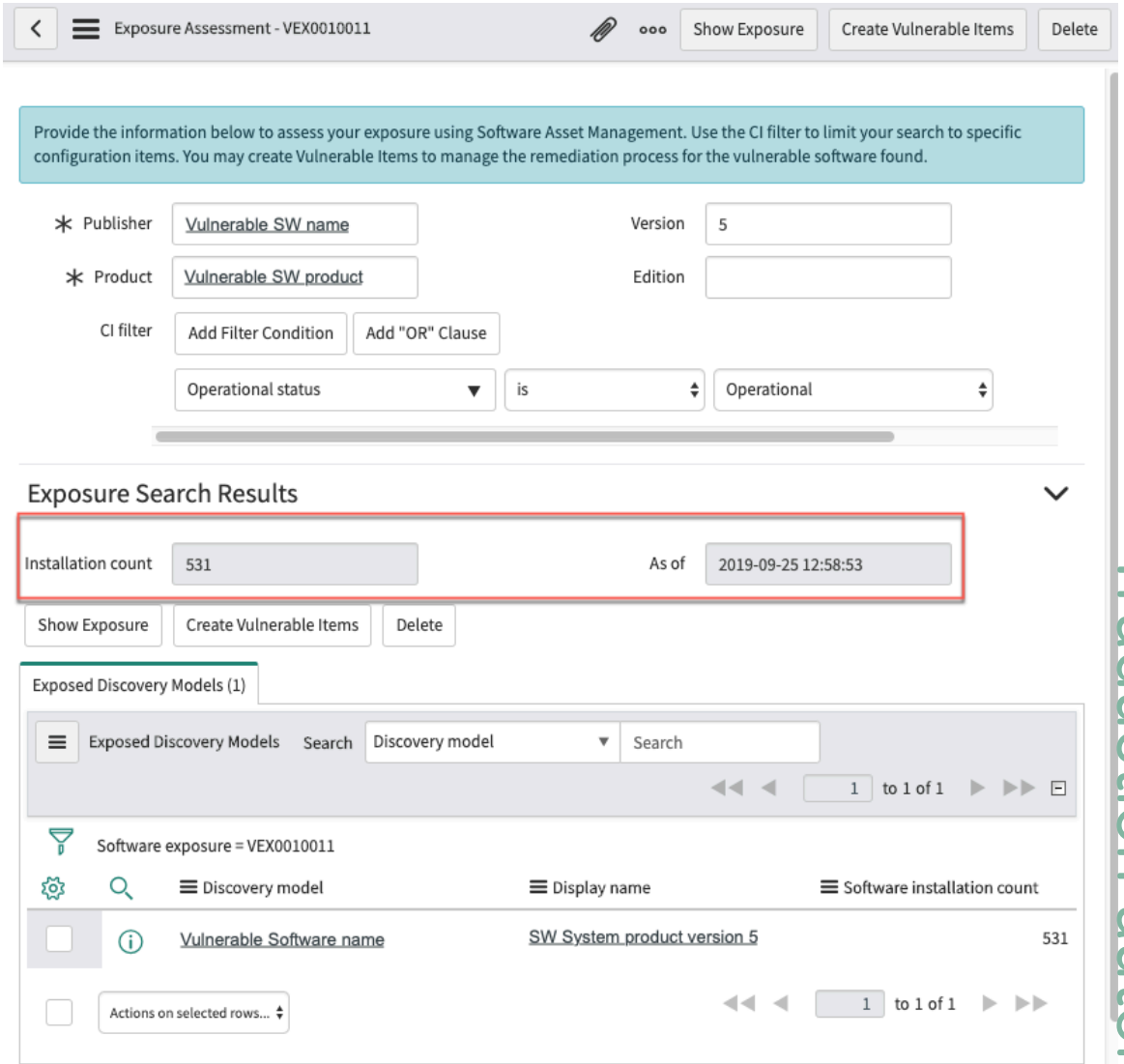
3. Remplissez le formulaire.

Champ	Description
Éditeur	Nom de l'éditeur du logiciel.
(Facultatif) Version	Entrez le numéro de version pour vous aider à affiner la recherche sur vos actifs.
Produit	Nom du produit logiciel.
(Facultatif) Édition	Entrez l'édition pour vous aider à affiner la recherche sur vos actifs.
Filtre de CI	Utilisez les listes de choix du filtre d'élément de configuration (CI) pour limiter votre recherche aux éléments de configuration spécifiques (ressources). Par exemple, vous pouvez soumettre une requête uniquement pour les actifs actifs sur lesquels ce logiciel est installé : L'état opérationnel est Opérationnel

4. Sélectionnez **Afficher l'exposition**.
L'enregistrement de l'évaluation de l'exposition avec votre modèle de détection et le nombre d'installations de logiciels sur vos actifs à la date spécifique s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Choisissez-en un pour continuer.

Option	Description
Afficher l'exposition	Ajoutez des conditions de filtre de CI supplémentaires et sélectionnez **Afficher l'exposition** pour affiner davantage les résultats de votre recherche.
Créer des éléments vulnérables	Créez des éléments vulnérables pour les éléments de configuration à partir de vos résultats de recherche. Si les éléments vulnérables sont créés avec succès, une tâche de rattrapage est créée pour tous les éléments vulnérables et affichée dans l'enregistrement d'évaluation de l'exposition.
Supprimer	Supprimez cet enregistrement et retournez à la liste des évaluations de l'exposition. Une boîte de dialogue de confirmation s'affiche.

6. Facultatif : Créez un élément vulnérable pour votre résultat de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Une fois que vous avez créé des éléments vulnérables, vous ne pouvez plus modifier les critères de recherche de cet enregistrement d'exposition.

7. Vous pouvez également réviser vos conditions de filtre et affiner davantage vos résultats de recherche.
8. Pour créer des éléments vulnérables, procédez comme suit :

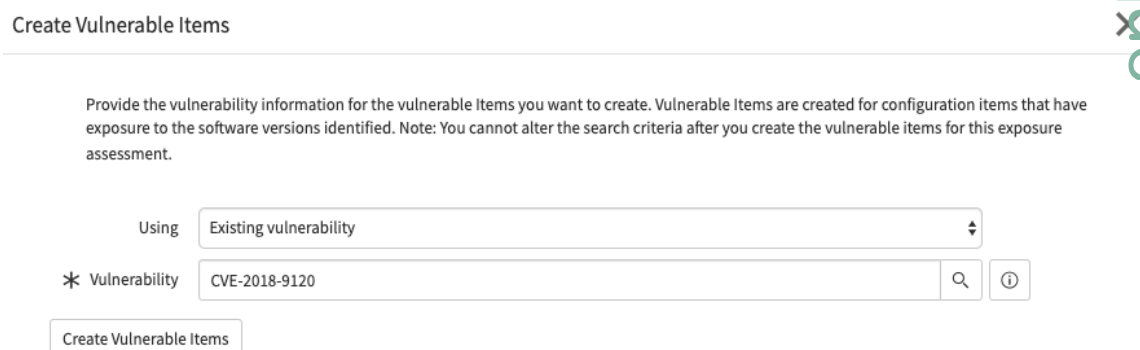
   a. Sélectionnez **Créer des éléments vulnérables**.
   La boîte de dialogue Créer des éléments vulnérables s'affiche.

   b. Renseignez les champs.

Champ	Description
Utilisant	Formez la liste de choix, choisissez-en un pour continuer. ▪ **Vulnérabilité existante**. À droite du champ Vulnérabilité, cliquez sur l'icône de recherche. Dans la liste qui s'affiche, sélectionnez le CVE-ID ou saisissez des critères de recherche pour localiser le CVE-ID existant, par exemple, CVE 2018-9120. **Remarque :** Il peut s'agir d'un CVE-ID provenant d'une base de données de vulnérabilité autre que le NVD. ▪ **Nouvelle vulnérabilité**. Entrez le CVE-ID de votre nouvelle vulnérabilité au format xxxx-xxxx, xxxx-xxxxx ou xxxx-xxxxxxx.
Résumé de la vulnérabilité (pour la nouvelle vulnérabilité uniquement)	Saisissez un résumé pour la nouvelle vulnérabilité, par exemple, Un attaquant peut exécuter un script sur le navigateur d'un utilisateur peu méfiant.

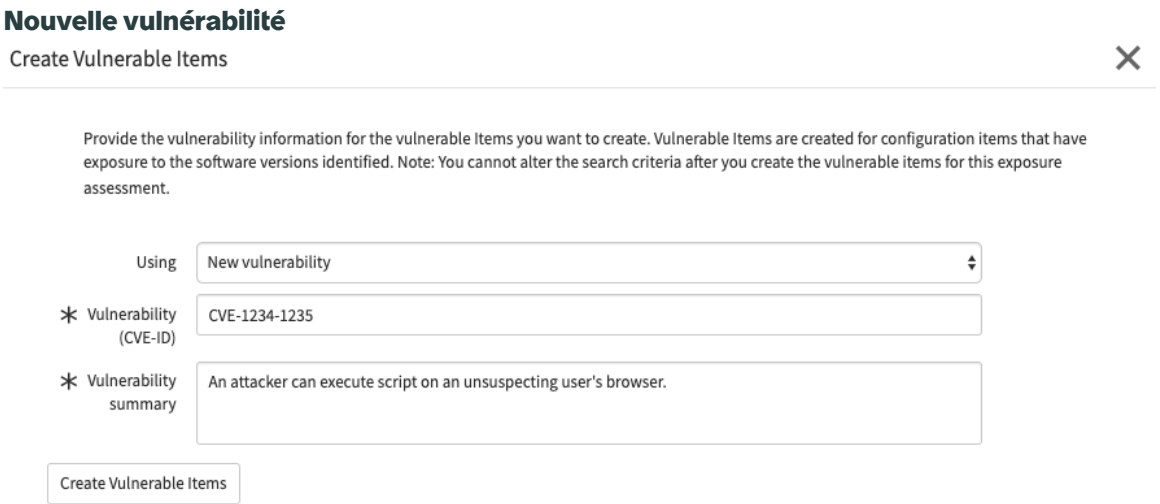
Les images suivantes montrent des exemples du formulaire rempli pour une vulnérabilité existante et une nouvelle vulnérabilité.

Vulnérabilité existante



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



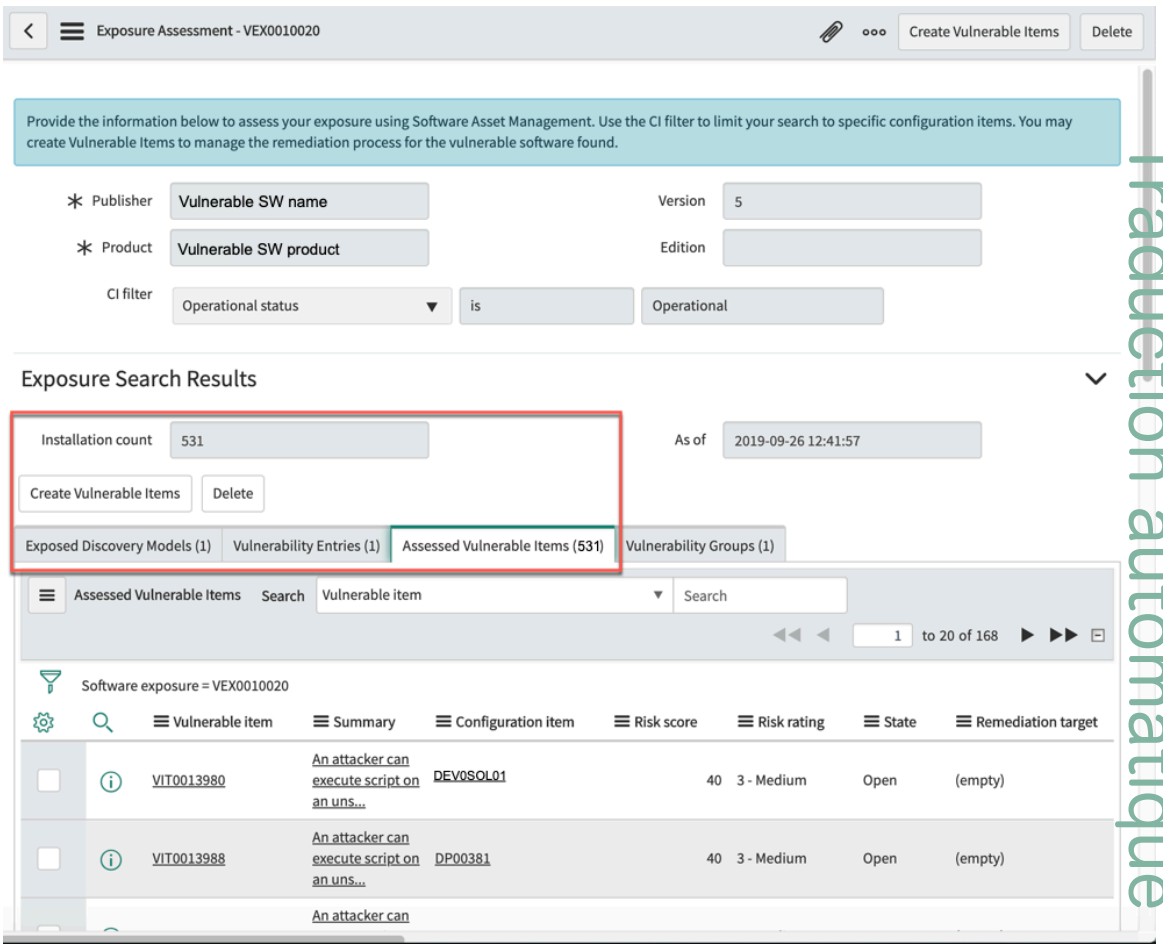
c. Sélectionnez **Créer des éléments vulnérables**.
L'enregistrement de l'évaluation de l'exposition s'affiche avec un message d'état qui indique que des éléments vulnérables sont en cours de création.

d. Après quelques secondes, en haut du formulaire, cliquez avec le bouton droit dans la bannière grise pour recharger la page.
Les nouveaux éléments vulnérables s'affichent comme illustré dans la figure suivante sous l'onglet Éléments vulnérables évalués (531). La nouvelle tâche de rattrapage créée pour ces éléments vulnérables s'affiche dans l'onglet Tâche de rattrapage (1).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Pour cet exemple, une tâche de rattrapage est créée en fonction des règles de groupe et des conditions de la règle de tâche de rattrapage appelée Vulnérabilité. Cette règle de groupe est la règle de tâche de rattrapage par défaut installée avec le produit Vulnerability Response dans votre ServiceNow AI Platform® instance. Dans cet exemple, les conditions de cette règle de groupe plaçaient tous les éléments vulnérables dans une seule tâche de rattrapage. Si vous préférez créer plusieurs tâches de rattrapage pour les éléments vulnérables qui correspondent aux résultats de recherche de votre évaluation de l'exposition, vous pouvez configurer des règles de tâche de rattrapage supplémentaires. La création de tâches de rattrapage supplémentaires peut vous aider à éviter la création de tâches de rattrapage avec un grand nombre d'éléments vulnérables. Pour en savoir plus sur les règles de tâche de rattrapage, reportez-vous aux sections Réponse aux vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage et Créer ou modifier des Réponse aux vulnérabilités règles de tâche de rattrapage.



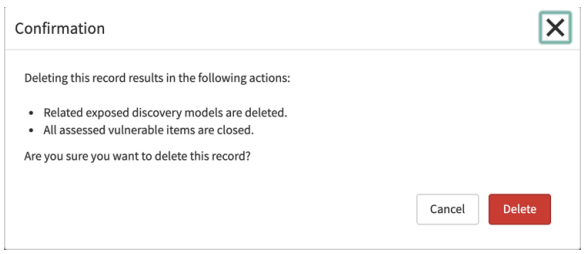
Traduction automatique

9. Choisissez-en un pour continuer.

Option	Description
Tâches de rattrapage	Une fois l'onglet Tâches de rattrapage sélectionné, dans la colonne Numéro, cliquez pour ouvrir l'enregistrement et examiner et affecter la tâche pour rattrapage. Pour plus d'informations sur les groupes d'affectation, reportez-vous à la section Création de groupes .
Éléments de vulnérabilité évalués	Une fois l'onglet Éléments vulnérables évalués sélectionné, dans la colonne Élément vulnérable, cliquez pour ouvrir les enregistrements et examiner et affecter des éléments vulnérables individuels.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Supprimer	Supprimez l’enregistrement de l’évaluation de l’exposition. Une boîte de dialogue de confirmation s’affiche. **Remarque :** Si vous supprimez l’enregistrement d’exposition après avoir créé des éléments vulnérables, tous les éléments vulnérables que vous créez pour cet enregistrement et qui ne sont pas associés à un autre enregistrement d’exposition sont automatiquement déplacés vers l’état Fermé . La raison de la fermeture est Annulé.



Que faire ensuite

Répondre à toutes les menaces zero-day (jour actuel) en fonction de votre évaluation de l’exposition. Pour plus d’informations sur les tâches de rattrapage et la gestion des changements pour , reportez-vous Réponse aux vulnérabilités Vue d’ensemble des tâches de rattrapage et des règles de tâche de rattrapage à Réponse aux vulnérabilités et Change Management pour Réponse aux vulnérabilités.

Affichage des recommandations d’affectation

Un groupe d’affectation est généralement alloué à un élément vulnérable à l’aide de règles d’affectation. Ces règles sont configurées par l’administrateur de vulnérabilité pour allouer les groupes d’affectation corrects en fonction des données reçues des analyseurs tiers.

Pour plus d'informations, consultez Réponse aux vulnérabilités Vue d’ensemble des règles d’affectation. Si un groupe d’affectation correspondant n’est pas disponible ou est incorrect, vous pouvez l’utiliser Recommandations d'affectation de vulnérabilité pour afficher d’autres groupes d’affectation.

Utilisez cette option Recommandations d'affectation de vulnérabilité pour effectuer les actions suivantes :

- Demander des recommandations de groupe d’affectation pour un élément vulnérable.
- Demander des recommandations de groupe d’affectation pour plusieurs éléments vulnérables.
- Demander des recommandations de groupe d’affectation pour une tâche de rattrapage.

Demander des recommandations de groupe d’affectation pour un élément vulnérable

Demandez Recommandations d'affectation de vulnérabilité à afficher les recommandations pour le groupe d’affectation. Vous pouvez demander des recommandations si un groupe d’affectation correspondant n’est pas disponible ou est incorrect pour un élément vulnérable (VI).

Avant de commencer

Rôle requis : sn_vul.remediation_owner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables** et ouvrez un VI.
   L'élément doit être à l'état Ouvert, Différé, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur l'icône) à côté du champ **Groupe d'affectation** pour obtenir des suggestions d'affectation pour ce VI.
3. Dans la boîte de dialogue Recommandations pour le groupe d'affectation, sélectionnez une recommandation basée sur le score de confiance.
   Le score de confiance prédit la pertinence de la correspondance pour le VI. Pour plus d'informations, consultez Solutions d'apprentissage machine pour Réponse aux vulnérabilités.
4. Cliquez sur **Affecter**.

Résultats

Le groupe sélectionné apparaît dans le champ **Groupe d'affectation** et le type d'affectation devient Recommandation.

Demander des recommandations de groupe d'affectation pour plusieurs éléments vulnérables

Utilisez cette fonction Recommandations d'affectation de vulnérabilité pour afficher les recommandations de groupe d'affectation pour plusieurs éléments vulnérables (VI) à l'aide d'une modification en bloc. Lorsque plusieurs VI sont sélectionnés, une prédiction est effectuée sur un échantillon aléatoire des VI sélectionnés.

Avant de commencer

Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche

Les recommandations et leurs scores de confiance peuvent différer légèrement d'une invocation à l'autre, en fonction des échantillons prélevés sur les VI sélectionnés. Le score de confiance évalue si le système est sûr que le groupe d'affectation recommandé est adapté pour résoudre la vulnérabilité. Utilisez la propriété système `assignment_recommendation_batchsize` pour définir la taille du lot lorsque vous demandez Recommandations d'affectation de vulnérabilité des tâches de rattrapage (VUL) et des VI à l'aide de l'option de modification en bloc. La valeur par défaut de cette propriété système est définie pour des performances de prédiction optimales.

Remarque : Si vous augmentez la valeur par défaut, le délai de réponse pour Recommandations d'affectation de vulnérabilité ces tickets peut changer.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Élément vulnérable** et sélectionnez plusieurs VI.
   Les éléments doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur **Modifier en bloc**.
3. Remplissez les champs du formulaire.

Formulaire Éléments vulnérables en bloc

Champ	Description
Sélection d'enregistrement	Enregistrements à sélectionner pour la modification en bloc.
Groupe d'affectation	Groupe d'affectation à définir pour les éléments vulnérables sélectionnés. Pour afficher les groupes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d’affectation recommandés, cliquez sur l’icône) en regard du champ. Sélectionnez une recommandation basée sur le score de confiance et cliquez sur **Affecter**.
Notes de travail	Notes à ajouter.

4. Cliquez sur **OK**.

Résultats
Le groupe sélectionné apparaît dans le champ **Groupe d’affectation** et le type d’affectation devient Recommandation pour tous les VI sélectionnés.

Demander des recommandations de groupe d’affectation pour une tâche de rattrapage

Utilisez cette propriété Recommandations d'affectation de vulnérabilité pour afficher les recommandations de groupe d’affectation pour une tâche de rattrapage (VUL).

Avant de commencer
Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche
Utilisez la propriété système `assignment_recommendation_batchsize` pour définir la taille du lot lorsque vous demandez Recommandations d'affectation de vulnérabilité des VUL et des éléments vulnérables (VI) à l’aide de l’option de modification en bloc. La valeur par défaut de cette propriété système est définie pour des performances de prédiction optimales.

Remarque : Si vous augmentez la valeur par défaut, le délai de réponse pour Recommandations d'affectation de vulnérabilité ces tickets peut changer.

Procédure
1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** et sélectionnez un VUL.
   Le groupe doit être à l’état Ouvert, En cours d’examen ou En attente d’implémentation.
2. Cliquez sur l’icône de recommandation (icône en regard du champ **Groupe d’affectation** pour les recommandations de groupe d’affectation pour la VUL sélectionnée.
   La boîte de dialogue Recommandations pour le groupe d’affectation affiche les groupes d’affectation recommandés avec le score de confiance moyen pour tous les VI de ce groupe.
3. Sélectionnez une recommandation dans la liste des groupes d’affectation en fonction du score de confiance.
   Le score de confiance prédit la pertinence de la correspondance pour la VUL sélectionnée.
4. Cliquez sur **Affecter**.
   Le groupe sélectionné apparaît dans le champ **Groupe d’affectation** .
5. Enregistrez la tâche de rattrapage avec les informations mises à jour.

Résultats
Tous les VI avec le même groupe d’affectation que la VUL sont affectés au groupe d’affectation sélectionné. Le type d’affectation devient Recommandation pour la VUL, ainsi que pour tous les VI modifiés.

Demande et approbation d’une exception

Vous pouvez demander de reporter le rattrapage d’un élément vulnérable ou d’une tâche de rattrapage pour une période spécifiée. Par exemple, en tant que propriétaire de rattrapage, vous pouvez demander une exception si un correctif n’est pas disponible pour une machine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les approbateurs disposant d'un accès peuvent approuver les demandes provenant d'autres utilisateurs.

Vous pouvez demander des exceptions aux espaces de Réponse aux vulnérabilités travail. Consultez Demander une exception dans le Espace de travail de remédiation IT.

- Demander une exception pour un élément vulnérable
- Demander une exception pour une tâche de rattrapage
- Demander une exception en bloc

Vous pouvez également demander des exceptions de politique à l'aide de GRC : Gestion de la politique et de la conformité:

- Demander une exception à l'aide de GRC : Gestion de la politique et de la conformité
- Demander une exception en bloc à l'aide de GRC : Gestion de la politique et de la conformité

Remarque :

Des notifications par e-mail sont envoyées à chaque étape de la gestion des exceptions, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'une exception est demandée, le demandeur reçoit un e-mail confirmant que la demande est soumise. L'approbateur reçoit également un e-mail indiquant qu'une exception a été demandée.

À partir de la version 21.0 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Demander une exception pour un élément vulnérable

Demander une exception pour un élément vulnérable (VI) qui ne peut pas être corrigé immédiatement. Par exemple, en tant que propriétaire de rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour un ordinateur.

Avant de commencer

Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche

Important : Vous pouvez demander des exceptions auprès des espaces de travail Gestionnaire des vulnérabilités et Rattrapage informatique. Pour plus d'informations, consultez Demander des exceptions pour les tâches et les enregistrements de rattrapage dans Espace de travail du gestionnaire de vulnérabilités et Demander une exception dans le Espace de travail de remédiation IT.

Vous pouvez également demander des exceptions pour les éléments vulnérables dans l'environnement classique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

À partir de la version 21.0 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Tous**.
2. Sélectionnez l'élément pour lequel vous souhaitez demander une exception.
   L'élément sélectionné doit être dans l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Sur le formulaire Élément vulnérable, cliquez sur **Demande d'exception**.
4. Si Réponse aux vulnérabilités est sélectionné dans l'écran Gestion des exceptions, renseignez les champs du formulaire Demande d'exception.

Formulaire de demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée sélectionnée dans le **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Gestion des exceptions** écran. Lorsque la demande d'exception expire, le groupe revient à l'état Ouvert. **Remarque :** À partir de la version 18.0 de (VR), si un élément vulnérable a été reporté pour correction à l'aide de la fonctionnalité de gestion des Réponse aux vulnérabilités exceptions, s'il est rouvert par le scanner, la date de report définie sur la vulnérabilité sera toujours conservée. Pour activer cette fonctionnalité, définissez la valeur de la propriété `sn_vul.auto_defer_vit_in_active_exception_win` système sur vrai. En outre, la date de **fin** différée persiste même après la fermeture de l'élément vulnérable ou l'expiration de l'exception. Le rôle requis est sn_vul.manage_exception_configuration pour la lecture et l'écriture.
Motif	Motif de la demande. Les choix possibles sont les suivants : ○ Risque accepté ○ En attente de fenêtre de maintenance ○ Correctif non disponible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Contrôle d'atténuation en place ○ Autre Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir le mappage du motif de la politique.
Informations supplémentaires	Détails liés au motif pour lequel cette demande est effectuée. Ce champ obligatoire doit être mis à jour par le propriétaire du rattrapage.

5. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**.

Résultats

L'état de l'élément vulnérable passe à En cours de révision. Utilisez l'onglet **Approbation du changement d'état** pour suivre l'état de la demande d'exception.

Demander une exception pour une tâche de rattrapage

Demandez une exception pour différer une tâche de rattrapage pendant une période spécifiée si elle ne peut pas être résolue immédiatement.

Avant de commencer

Important :

Vous pouvez demander les exceptions auprès du gestionnaire des vulnérabilités et des espaces de travail de rattrapage informatique. Consultez Demander une exception dans le Espace de travail de remédiation IT.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions pour les tâches de rattrapage dans l'environnement classique.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de rattrapage** > **Tous**.
2. Sélectionnez le groupe pour lequel vous souhaitez demander une exception.
   La tâche sélectionnée doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Dans l'enregistrement de tâche de rattrapage (VUL), sélectionnez **Demande d'exception**.
4. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée d'exception définie dans la configuration.
Motif	Justification de la demande d'exception.
Informations supplémentaires	Détails liés au motif pour lequel cette demande est effectuée. Ce champ doit être mis à jour par le propriétaire du rattrapage.

5. Cliquez sur **Demander l'approbation**.

Demander une exception en bloc

Utilisez l'option de modification en bloc pour demander une exception pour plusieurs éléments vulnérables (VIT) au lieu de sélectionner manuellement chaque élément.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst

Pourquoi et quand exécuter cette tâche

Lorsque plusieurs VIT sont sélectionnés, une tâche de rattrapage (VUL) est formée avec ces éléments. Voir Modifier des éléments vulnérables en bloc dans Réponse aux vulnérabilités pour plus d'informations sur la modification de plusieurs VIT.

Important : Vous pouvez demander une exception pour :

- a VIT du Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT. Pour plus d'informations, consultez Demander une exception dans le Espace de travail de remédiation IT.
- plusieurs VIT du Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Demander une exception en bloc dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Tous** et sélectionnez les éléments pour lesquels vous souhaitez demander une exception.
   Les éléments sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur **Modifier en bloc**.
3. Remplissez les champs du formulaire.

Formulaire de modification en bloc de l'élément vulnérable

Champ	Description
Sélection d'enregistrement	Enregistrements que vous avez sélectionnés pour une modification en bloc.
État	État de l'élément vulnérable. Sélectionnez l'état Différé pour demander une exception pour les éléments sélectionnés.
Motif	Sous-état de l'état que vous avez sélectionné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description brève	Nom de la tâche de rattrapage que vous créez.
Jusqu'à	Date de fin que vous spécifiez pour votre demande d'exception.
Informations supplémentaires	Détails supplémentaires que vous souhaitez mentionner pour informer l'approbateur des motifs de votre demande.
Solution privilégiée	Solution ciblée pour corriger tous les éléments vulnérables que vous avez sélectionnés pour une modification en bloc.
Groupe d'affectation	Groupe d'affectation pour le VI. Vous pouvez sélectionner un groupe manuellement ou utiliser les recommandations d'affectation si cette fonctionnalité est activée.
Notes de travail	Notes à ajouter.

4. Cliquez sur **OK**.
   Une tâche de rattrapage contenant les éléments vulnérables que vous avez sélectionnés est créée. Cette tâche de rattrapage est soumise pour approbation.

Demander une exception à l'aide de GRC : Gestion de la politique et de la conformité

Demandez des exceptions à la politique à l'aide de l'aptitude de GRC gestion des exceptions de politique de l'application à partir de Réponse aux vulnérabilités.Gestion de la politique et de la conformité

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions de politique, vous devez télécharger l'application à partir GRC : Gestion de la politique et de la conformité du ServiceNow Store.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions dans l'interface utilisateur classique :

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables** (ou **Tâches de remédiation**)>**Toutes**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.
   L'élément ou le groupe sélectionné doit être dans l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Sur le formulaire sélectionné, cliquez sur **Demande d'exception**.
3. Remplissez les champs du formulaire.

Formulaire de demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date actuelle. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert. **Remarque :** Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale de l'exception (jours)** que vous définissez pour la politique dans Politique et conformité. Pour plus d'informations, consultez Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés au motif pour lequel cette demande est effectuée. Ce champ obligatoire doit être renseigné par le propriétaire du rattrapage.

4. Cliquez sur **Envoyer**.
   Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez Configuration facultative de Policy and Compliance Management .

Demander une exception en bloc à l'aide de GRC : Gestion de la politique et de la conformité

Sélectionnez un groupe d'éléments vulnérables et soumettez une exception en bloc.

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions en bloc, vous devez télécharger l'application à partir GRC : Gestion de la politique et de la conformité du ServiceNow Store.

Remarque : Pour utiliser cette fonctionnalité, vous devez effectuer une mise à niveau GRC : Gestion de la politique et de la conformité avant de mettre à niveau Réponse aux vulnérabilités. Si vous avez déjà effectué une mise à niveau Réponse aux vulnérabilités antérieure GRC : Gestion de la politique et de la conformité et que vous souhaitez utiliser cette fonctionnalité, vous devez effectuer à nouveau les procédures de mise à niveau dans le bon ordre.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.remediation_owner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez également demander des exceptions dans l'environnement classique au format Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Tous** et sélectionnez les éléments pour lesquels vous souhaitez demander une exception.
   Les éléments sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur **Modifier en bloc**.
3. Remplissez les champs du formulaire.

Formulaire de modification en bloc de l'élément vulnérable

Champ	Description
Sélection d'enregistrement	Enregistrements que vous avez sélectionnés pour une modification en bloc.
État	État de l'élément vulnérable. Sélectionnez l'état Différé pour demander une exception pour les éléments sélectionnés.
Description brève	Nom de la tâche que vous créez.
Solution privilégiée	Solution que vous ciblez pour corriger tous les éléments vulnérables que vous avez sélectionnés pour la modification en bloc.
Groupe d'affectation	Groupe d'affectation pour le VI. Vous pouvez sélectionner un groupe manuellement ou utiliser les recommandations d'affectation si cette fonctionnalité est activée.
Notes de travail	Notes à ajouter.

4. Cliquez sur **OK**.
   Une tâche de rattrapage est créée avec les éléments vulnérables sélectionnés.
5. Remplissez les champs du formulaire.

Formulaire de demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date actuelle. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale de l'exception (jours)** que vous avez définie pour la politique dans GRC : Gestion de la politique et de la conformité. Pour plus d'informations, consultez Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés au motif pour lequel cette demande est effectuée. Ce champ obligatoire doit être renseigné par le propriétaire du rattrapage.

6. Cliquez sur **Envoyer**.
   Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez Configuration facultative de Policy and Compliance Management .

Approuver ou rejeter une demande d'exception dans Réponse aux vulnérabilités

Approuvez ou rejetez les demandes d'exception pour les éléments vulnérables ou les tâches de rattrapage qui ne peuvent pas être corrigés immédiatement. Vous devez évaluer ces demandes pour connaître le risque, puis approuver leur report jusqu'à ce qu'elles puissent être corrigées.

Important :

Vous pouvez approuver ou rejeter les demandes d'exception dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis : sn_vul.exception_approver

Vous pouvez également approuver des demandes d'exception dans l'environnement classique.

Remarque :

À partir de la version 21.0 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser une règle d’exception

Vous pouvez demander une exception pour les vulnérabilités, les éléments vulnérables (VI) ou les éléments de configuration (CI) qui ne peuvent pas être corrigés ou différés immédiatement. En automatisant le processus de report de VI, vous pouvez différer les VI correspondants en fonction de la règle lorsque le système les identifie.

Vous pouvez effectuer les tâches suivantes pour une règle d’exception :

- Créer une règle d'exception
- Approuver une demande de règle d'exception
- Activation d'une règle d'exception
- Rouvrir une règle d’exception
- Mettre à jour une règle d’exception approuvée
- Supprimer une règle d'exception

Remarque :

À partir de la version 21.0 de , vous pouvez configurer les délais d’approbation Réponse aux vulnérabilités des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l’approbateur et le demandeur après un nombre de jours défini. Lorsqu’une demande est émise, l’élément vulnérable passe à l’état En cours de révision et un enregistrement de changement d’état est créé. Si l’approbateur ne répond pas dans le délai configuré, l’élément vulnérable ou la tâche de rattrapage revient à l’état Ouvert. L’état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d’approbation pour la gestion des exceptions.

Créer une règle d'exception

Créez une règle pour demander automatiquement une exception pour une condition spécifique d’un groupe d’éléments vulnérables (EV), comme une règle avec une condition basée sur la gravité de vulnérabilité de ces VI. Avec cette règle, vous pouvez différer automatiquement les VI nouveaux et existants s’ils correspondent à la condition de règle approuvée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

La règle s’applique à partir de la date de début de validité jusqu’à la date de fin de validité. La tâche de rattrapage (VUL) est créée lorsque la règle est approuvée. La méthode de regroupement pour cette VUL est connue sous le nom de règles d’exception. La VUL est créée à l’état Différé. Vous ne pouvez pas fermer, rouvrir ou supprimer cette VUL. Les VI nouveaux et rouverts sont différés et ajoutés à cette VUL à partir de la date « Début de validité » jusqu’à l’expiration du groupe à la date « Fin de validité ».

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de la règle d’exception. Ces e-mails fournissent l’état et d’autres détails d’une demande. Par exemple, lorsqu’une règle d’exception est demandée, le demandeur reçoit un e-mail confirmant l’envoi de la demande.

Remarque : Si la règle est rejetée, vous pouvez la rouvrir à l’état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'exception**.
2. Sur la page Nouvel enregistrement de règle d’exception, cliquez sur **Nouveau** pour créer une règle.
3. Remplissez les champs du formulaire.

Formulaire Règle d’exception

Champ	Description
Nom	Nom de la règle d’exception.
Début de validité	Date à partir de laquelle cette règle est active pour différer les VI.
Date de fin de validité	Date à partir de laquelle la tâche de rattrapage arrête d’accepter de nouveaux VI.
Motif	Raison de la création de cette règle d’exception.
Groupe d'affectation	Groupe auquel la tâche de rattrapage créée pour le suivi des VI différés est affectée.
Informations supplémentaires	Informations supplémentaires que le demandeur souhaite fournir à l’approbateur. Ces informations sont renseignées dans le champ Description de la tâche de rattrapage.
Condition	Condition de filtre pour les éléments vulnérables qui peut être définie lors du traitement des éléments vulnérables.
Exécuter sur les données existantes	Option qui vous permet d’exécuter cette règle sur des données existantes la première fois que cette règle est exécutée.
Étape du workflow	État d’approbation actuel de la règle d’exception.
État	État de la règle d’exception.
Ordre d'exécution	Ordre unique pour chaque règle d’exception
Reporté jusqu'à	Date à laquelle les VUL et les VI sont reportés. À cette date, la VUL créée est fermée, tous les VI sont déplacés hors du groupe et les règles de groupe sont réappliquées.

4. Ajoutez le groupe d’affectation lorsque vous créez la règle.
5. Envoyez le formulaire pour approbation.
   L’état de la demande est défini sur En cours de révision. Tant que vous n’avez pas soumis la règle d’exception, elle reste à l’état Brouillon.

Approuver une demande de règle d'exception

Évaluez les demandes de règle d’exception des utilisateurs afin de pouvoir approuver ou rejeter ces demandes.

Avant de commencer

Rôle requis : sn_vul.exception_approver

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Approbateur d'exceptions Les membres du groupe d'utilisateurs de niveau 1 peuvent approuver les demandes de règle d'exception de niveau 1. De même, les membres du groupe d'utilisateurs de niveau 2 de l'approbateur d'exceptions peuvent approuver les demandes de règle d'exception de niveau 2. Les deux groupes d'utilisateurs héritent du rôle d'approbateur d'exceptions par défaut.

Remarque :

Si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et les faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec et expliquez pourquoi vous avez approuvé ou rejeté la demande. Une fois qu'une règle d'exception est approuvée, une tâche de rattrapage (RT) est créée par défaut dans l'état Différé. À partir de la date de début de validité, cette règle s'exécute sur tous les éléments vulnérables créés, ainsi que sur ceux qui sont déplacés de l'état Fermé à l'état Ouvert. Les éléments vulnérables qui correspondent aux conditions définies sont ajoutés au RT et différés pour la période spécifiée.

Remarque : Si la règle est rejetée, vous pouvez la rouvrir à l'état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Activation d'une règle d'exception

Une règle est activée à sa date de début de validité. Après l'activation, il automatise le processus d'exception pour les éléments vulnérables (VI).

La règle d'exception suit le cycle de vie suivant :

1. Les nouveaux éléments vulnérables (VI) que vous créez ou rouvrez et qui remplissent la condition spécifiée sont reportés. Si vous activez l'option Exécuter sur les données existantes lorsque vous exécutez la règle d'exception pour la première fois, tous les VI actifs et non différés qui correspondent à la condition de règle d'exception sont déplacés vers la tâche de rattrapage (RT) nouvellement créée et son état devient Différé.
2. Si un VI nouvellement créé correspond à la condition de la règle d'exception, il est déplacé vers le RT différé associé à la règle et la règle de groupe n'est pas exécutée dessus.
3. À la date de début de validité, les VI existants sont ajoutés si vous activez l'option Exécuter sur les données existantes.
4. Le RT cesse d'accepter de nouveaux VI lorsque la règle expire à la date « Fin de validité ». Le RT existe jusqu'à la date « Différé jusqu'à ».
5. La règle d'exception expire à la date « Fin de validité ».

Demander une extension pour une règle d'exception

Demandez une extension pour une règle d'exception différée avant qu'elle n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Règles d'exception**.
2. Sélectionnez une règle d'exception approuvée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle la règle d'exception doit être prolongée.
Motif	Entrez le motif du report de la règle d'exception. Les choix sont les suivants : ○ Risque accepté ○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lors de l’approbation de la demande, les champs Différé jusqu’à, Motif et Informations supplémentaires sont mis à jour sur la règle d’exception et les tâches de rattrapage et éléments vulnérables associés. Un e-mail est également déclenché lors de la soumission de la demande et de l’action ultérieure par l’approbateur.

Remarque :

- La demande passe par deux niveaux d’approbation.
- Le bouton Demande d’extension n’est pas disponible pour les tâches de rattrapage créées dans le cadre d’une règle d’exception.
- Si une règle d’exception différée est à nouveau étendue, le nombre de reports d’extension augmente dans le back-end.
- À partir de la version 21.0 de , vous pouvez configurer les délais d’approbation Réponse aux vulnérabilités des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l’approbateur et le demandeur après un nombre de jours défini. Lorsqu’une demande est émise, l’élément vulnérable passe à l’état En cours de révision et un enregistrement de changement d’état est créé. Si l’approbateur ne répond pas dans le délai configuré, l’élément vulnérable ou la tâche de rattrapage revient à l’état Ouvert. L’état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d’approbation pour la gestion des exceptions.

Rouvrir une règle d’exception

Rouvrez une règle d’exception qui a été rejetée, mais que vous souhaitez soumettre à nouveau. La réouverture de la règle la fait passer à l’état Brouillon.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Vous pouvez ensuite mettre à jour et soumettre à nouveau la règle pour approbation.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'exception**.
2. Recherchez la règle que vous souhaitez rouvrir, puis cliquez sur **Rouvrir**.
3. Mettez à jour le formulaire et soumettez-le à nouveau pour approbation.

Mettre à jour une règle d’exception approuvée

Annulez une règle approuvée pour pouvoir la mettre à jour. Par exemple, avant de pouvoir modifier des dates ou ajouter une condition à une règle approuvée, vous devez l’annuler afin que la tâche de rattrapage (VUL) soit supprimée et que les éléments vulnérables (VI) passent à l’état Ouvert.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Les règles de groupe sont réappliquées à ces VI. Soumettez la règle après avoir apporté les changements afin qu’elle repasse par le processus d’approbation.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'exception**.
2. Ouvrez la règle d’exception que vous souhaitez annuler, puis cliquez sur **Annuler**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la boîte de dialogue Annuler la règle, cliquez sur **Annuler la règle**.
   La règle revient à l'état Brouillon et la VUL associée est supprimée. Les VI associés sont rouverts et des règles de groupe sont appliquées aux VI individuels.

Supprimer une règle d'exception

Supprimez une règle d'exception qui n'est plus requise. Par exemple, vous pouvez supprimer une règle si vous ne souhaitez pas différer un élément vulnérable (VI) pendant l'ingestion.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
La suppression d'une règle annule la tâche de rattrapage associée (VUL). Les VI associés sont rouverts et des règles de groupe sont appliquées aux VI individuels.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Règles d'exception**.
2. Ouvrez la règle d'exception que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue Supprimer la règle, cliquez sur **Supprimer la règle** pour supprimer la règle sélectionnée.
   La tâche de rattrapage associée est également supprimée. Les VI associés sont rouverts et des règles de groupe sont appliquées aux VI individuels.

Marquer et approuver un faux positif

Les éléments vulnérables (VI) et les tâches de rattrapage (VUL) peuvent être marqués comme des faux positifs. Les approbateurs avec un accès en écriture peuvent approuver de telles demandes provenant d'autres utilisateurs.

- Marquer comme faux positif
- Modifier en bloc pour faux positif
- Approuver ou rejeter un faux positif

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de faux positif, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'un VI ou une tâche de rattrapage est marqué comme faux positif, le demandeur reçoit un e-mail de confirmation. Simultanément, l'approbateur reçoit un e-mail indiquant qu'un VI ou une tâche de rattrapage a été marqué comme faux positif.

À partir de la version 21.0 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Marquer comme faux positif

Marquez un élément vulnérable (VI) ou une tâche de rattrapage (VUL) comme faux positif si l'avertissement donné par le scanner n'est pas réellement un problème. Par exemple, si

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

un élément de configuration a été mis hors service, mais que le scanner soulève toujours un problème connexe, marquez-le comme faux positif.

Avant de commencer

Rôle requis : propriétaire du rattrapage

Vous pouvez demander des faux positifs à partir Réponse aux vulnérabilités des espaces de travail. Consultez Demander un faux positif pour un élément vulnérable ou une tâche de rattrapage.

Vous pouvez également demander des faux positifs dans l'environnement classique :

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Éléments vulnérables (ou tâches de rattrapage)** > **Tous**.
2. Ouvrez le VI ou la VUL que vous souhaitez marquer comme faux positif et cliquez sur **Marquer comme faux positif**.
   Le VI ou la VUL doit être dans un état **ouvert** .
3. Sur le formulaire Faux positif, saisissez les détails dans **Informations supplémentaires** et cliquez sur **Demander l'approbation**.
   La demande est envoyée pour approbation et l'état du VI ou de la VUL passe à **En cours de révision**.

Modifier en bloc pour faux positif

Utilisez la modification en bloc pour marquer plusieurs éléments vulnérables (VIT) comme faux positif. Si plusieurs VIT sont sélectionnés, une tâche de rattrapage est formée avec ces éléments.

Important : En tant qu'administrateur ou analyste, vous pouvez utiliser la fonctionnalité de modification en bloc dans l'espace de travail du gestionnaire de vulnérabilités pour marquer plusieurs VIT comme faux positifs. Pour plus d'informations, consultez Modifier en bloc le faux positif dans l'espace de travail du gestionnaire de vulnérabilité.

Avant de commencer

Rôle requis : propriétaire du rattrapage

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Vous pouvez également demander des faux positifs dans l'environnement classique :

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Éléments vulnérables** > **Tous** et sélectionnez les éléments que vous souhaitez marquer comme faux positif.
   Les éléments sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Cliquez sur **Modifier en bloc**.
3. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de modification en bloc de l'élément vulnérable

Champ	Description
Sélection d'enregistrement	Enregistrements à sélectionner pour la modification en bloc.
État	État des éléments vulnérables. Sélectionnez Fermé pour marquer comme faux positif.
Motif	Sous-état de l'état sélectionné. Si vous avez sélectionné Fermé comme état, sélectionnez Faux positif ici pour marquer comme faux positif.
Annuler l'affectation	Soumettez une demande d'effacement des champs Affecté à et Groupe d'affectation.
Solution privilégiée	Solution ciblée pour corriger tous les éléments vulnérables sélectionnés pour une modification en bloc.
Groupe d'affectation	Groupe d'affectation pour le VI. Sélectionnez manuellement ou à l'aide des recommandations d'affectation si cette option est activée.
Notes de travail	Notes à ajouter.

4. Cliquez sur **OK**.
   Une nouvelle tâche de rattrapage contenant les VI sélectionnés est créée et cette tâche est envoyée pour approbation.

Approuver ou rejeter un faux positif

En tant qu'approbateur de faux positif, vous pouvez approuver ou rejeter les demandes de faux positif d'autres utilisateurs.

Important :

En tant qu'approbateur de faux positif, vous pouvez approuver ou rejeter les demandes de faux positif dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vul.false_positive_approver pour les éléments vulnérables
- sn_vul.app_false_positive_approver pour les éléments vulnérables de l'application

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Vulnérabilités** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Remarque : Un faux positif peut être limité dans le temps. Seul l'approbateur peut définir la date de fin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Solutions d'analyse et de génération de rapports pour Réponse aux vulnérabilités

La surveillance du rattrapage des vulnérabilités implique l'affichage des tendances, la gestion des risques et la surveillance des groupes d'affectation. Vous pouvez passer en revue les problèmes à haut risque, les charges de travail des groupes d'affectation, les reports et les vulnérabilités récurrentes. Réponse aux vulnérabilités offre des outils, des rapports et des procédures pour rendre ce processus plus productif et efficace.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à surveiller la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en affichant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Consultez Espace de travail du gestionnaire de vulnérabilités et Exploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Les analystes de vulnérabilité peuvent également utiliser des tableaux de bord par défaut Réponse aux vulnérabilités pour **Tous** > **Réponse aux vulnérabilités** > **Vue d'ensemble**.

Important :

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord peut également être affiché dans la nouvelle interface utilisateur. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Tableaux de bord dans l'espace de travail du gestionnaire de vulnérabilité et Tableaux de bord dans l'espace de travail Rattrapage informatique.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Réponse aux vulnérabilités Processus de rattrapage

La plupart des rattrapages de vulnérabilités sont effectués à partir de l'enregistrement de tâche de rattrapage depuis les espaces de Réponse aux vulnérabilités travail. Parmi les tâches de rattrapage (RT) à l'état En cours d'examen, vous pouvez effectuer plusieurs tâches.

- Créer des demandes de changement.
- Ajoutez des notes de travail et des descriptions des vulnérabilités dans la tâche de rattrapage.
- Différez la tâche de rattrapage et les éléments vulnérables qu'elle contient à une date ultérieure.
- Fermez la tâche de rattrapage.
- Suivez les nouvelles obligations de conformité réglementaire, qui sont généralement urgentes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Connectez-vous à votre instance Réponse aux vulnérabilités.
- Examinez votre gestion des vulnérabilités et vos tableaux de bord et rapports tiers pour localiser les zones problématiques. Par exemple, affichez les tableaux de bord qui montrent l'ancienneté de la tâche de rattrapage par état ou les éléments vulnérables (VI) à haut risque au-delà de leur date cible de rattrapage.
- Examinez l'état des tâches de rattrapage, par ordre de risque.
- Révisez l'ordre de priorité des tâches en ajustant vos calculateurs de score de risque si le score de risque n'est pas calculé correctement ou en différant les VI ou les RT, selon les besoins. Consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité ou Différer une tâche de rattrapage pour plus d'informations sur ces options.
- Examinez les éléments vulnérables différés sur le point de rouvrir et prenez des mesures supplémentaires si nécessaire. Si vous souhaitez initier et suivre les activités de changement sur vos actifs, vos tâches de rattrapage et leurs éléments vulnérables correspondants, pour plus d'informations, consultez la rubrique Change Management pour Réponse aux vulnérabilités pour une action ultérieure.
- Examinez les commentaires des opérations IT.

  Une fois que vous êtes informé de la résolution d'une demande de changement, attendez la prochaine analyse. Les analyses sont déclenchées automatiquement par le calendrier d'importation tierce configuré dans l'assistant de configuration.

- Après une analyse, si l'état est Fixe, les éléments vulnérables sont automatiquement fermés pendant l'importation. Le groupe se ferme lorsque tous les éléments vulnérables du groupe sont corrigés.
- Après l'analyse, si l'état n'est pas Fixe, l'élément vulnérable est automatiquement renvoyé à l'état En cours d'examen.

- Les éléments vulnérables définis sur « Résolu » dans votre instance, mais qui ne sont pas passés à « Fermé/Corrigé » par les exécutions d'intégration tierces sont rouverts s'ils sont détectés lors des nouvelles analyses.

  En ce Qualys qui concerne les détections, si le scanner continue de trouver des VI qui ont été définis sur « Résolu », mais qui ne sont pas passés à « Fermé/Corrigé » par les analyses suivantes, ces VI repassent à « Ouvert » lorsque la dernière date trouvée est postérieure à la date de résolution.

  Pour Rapid7 les détections, une option est maintenant disponible sur la Rapid7 page de configuration de votre instance pour rouvrir les VI résolus par âge. Si cette option est activée, les VI sont définis sur « Résolu », mais ne sont pas transitionnés vers « Fermé/Corrigé » par les analyses suivantes qui reviennent à « Ouvert » après le nombre de jours que vous saisissez.

Gestion des solutions pour vulnérabilités Progression du déploiement

Les mesures de déploiement complètes pour les tâches de rattrapage et les entrées de vulnérabilité sont incluses dans Gestion des solutions pour vulnérabilités**le statut du rattrapage** dans les vulnérabilités, les éléments vulnérables. Identifiez facilement la tâche de rattrapage ou la vulnérabilité qui ralentit la progression de la résolution. Explorez la façon dont la vulnérabilité est identifiée ou quels aspects des actifs affectés peuvent être à l'origine du problème de rattrapage. Mettez à jour l'état de vos mesures à l'aide du lien connexe **Mettre à jour l'état** dans les formulaires de tâche de vulnérabilité, de solutions et de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités

Le Réponse aux vulnérabilités tableau de bord de vue d'ensemble (gestion des vulnérabilités) fournit une vue exécutive des vulnérabilités et des éléments vulnérables, ce qui aide l'administrateur de vulnérabilité à identifier rapidement les zones de préoccupation. Le Réponse aux vulnérabilités tableau de bord de remédiation (Vulnerability Remediation) permet à un spécialiste de la remédiation de se concentrer sur les tâches de remédiation et les éléments vulnérables qu'il possède.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

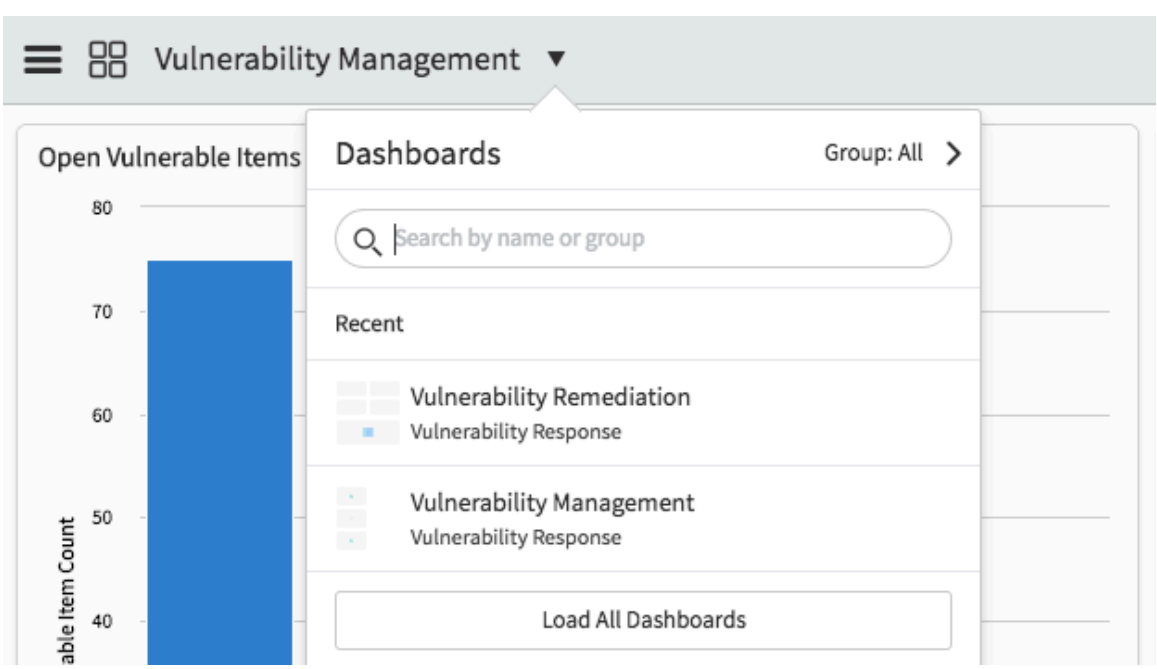
Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à surveiller la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en affichant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Consultez Réponse aux vulnérabilités Espaces de travail et Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Les analystes de vulnérabilité peuvent également utiliser des tableaux de bord par défaut Réponse aux vulnérabilités .

Rôles requis : sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst et les utilisateurs ayant sn_vul.vulnerability_read (ou qui héritent du rôle sn_vul.vulnerability_read) et pa_viewer.

Les tableaux de bord par défaut Réponse aux vulnérabilités dans l'environnement hérité

Ces rapports sont inclus dans le cadre de l'application Analyse des performances pour Réponse aux vulnérabilités et ne nécessitent pas d'abonnement distinct. Pour en ouvrir un, sélectionnez la liste de choix pour la développer et choisissez un tableau de bord. Vous pouvez également saisir le nom d'un tableau de bord dans le champ de recherche.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Lorsque Content Pack pour Réponse aux vulnérabilités l'application Analyse des performances est installé et activé, le tableau de bord Gestion de la vulnérabilité (PA) s'affiche automatiquement dans le module de vue d'ensemble. Ce tableau de bord contient des rapports couvrant toutes les étapes du cycle de vie de la gestion des vulnérabilités.

Pour plus d'informations sur les rapports inclus dans le pack de contenu Performance Analytics pour Réponse aux vulnérabilités, voir le tableau de bord Gestion de la vulnérabilité [PA].

Pour plus d'informations sur le tableau de bord des CISO et les rapports de couverture des analyses, consultez le tableau de bord des CISO de la gestion des vulnérabilités.

Tableau de bord de gestion des vulnérabilités

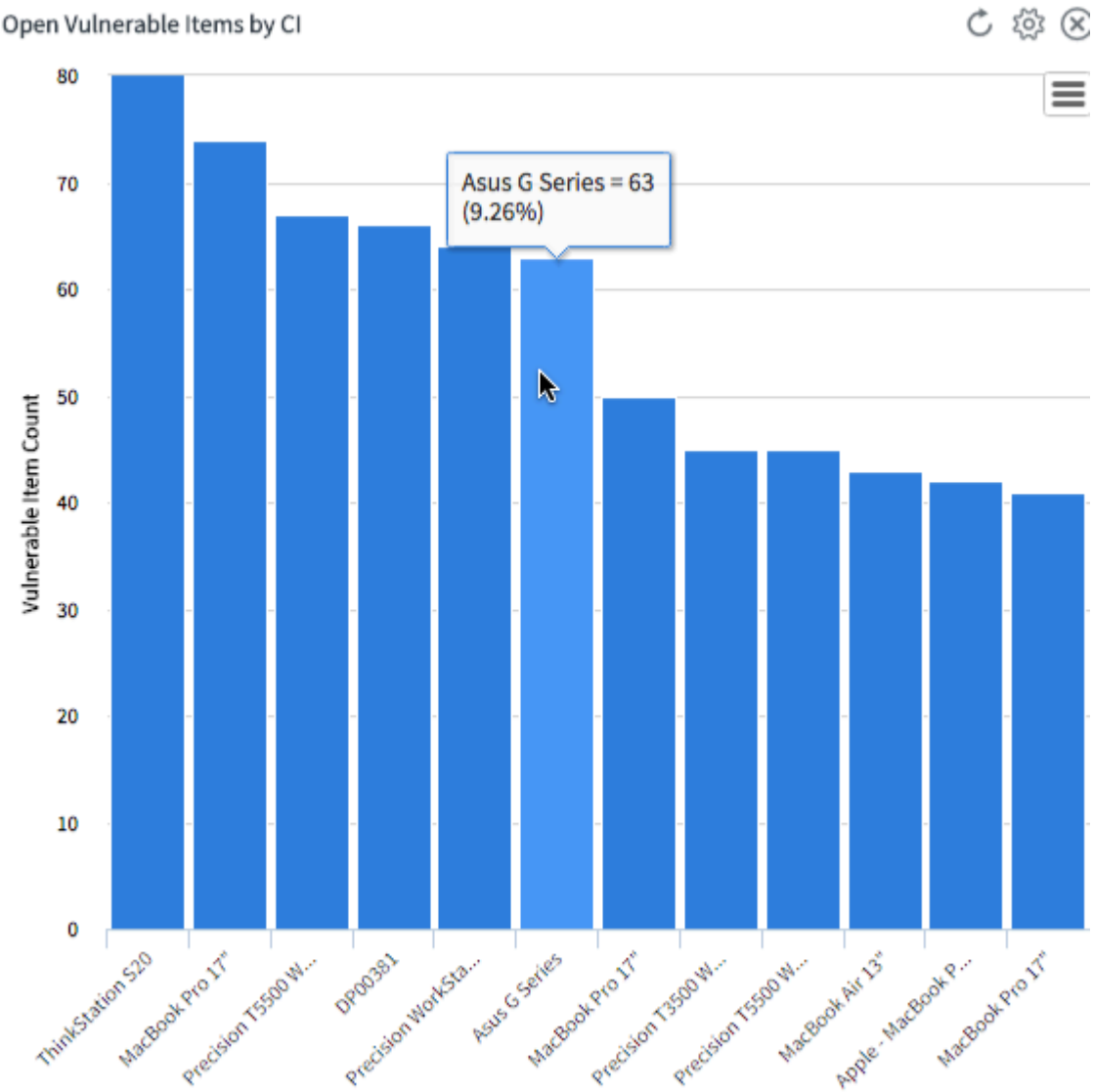
Dans chaque graphique, vous pouvez pointer vers n'importe quelle partie d'un graphique (barre, secteur, point de données, etc.) pour afficher des données générales spécifiques à cette partie. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Remarque :

Si des tableaux de bord personnalisés sont nécessaires, consultez Créer et utiliser des tableaux de bord pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Rapports Vue d'ensemble de la vulnérabilité

Nom	Visuel	Description
Ouvrir les éléments vulnérables par CI	À barres	Affiche le nombre d'éléments vulnérables ouverts enregistrés pour chaque élément de configuration (CI), du plus important au moins élevé.
Éléments vulnérables par état de la cible de rattrapage	À barres	Affiche le nombre d'éléments vulnérables qui approchent de la cible, en cours et au-delà de la cible. **Remarque :** Les éléments à l'état Différé, Résolu ou Fermé ne sont pas inclus.
Éléments vulnérables différés arrivant à expiration cette semaine	Graphique	Affiche le nombre d'éléments vulnérables différés planifiés pour être réactivés dans les sept jours.
Ouvrir les éléments vulnérables par vulnérabilité	À barres	Affiche le nombre d'éléments vulnérables ouverts pour chaque vulnérabilité, du plus au moins élevé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble de la vulnérabilité (suite)

Nom	Visuel	Description
Vulnérabilités par modèle	À barres	Affiche le nombre d'éléments vulnérables enregistrés pour chaque modèle (classe CI), du plus important au moins élevé.
Vulnérabilités par semaine	Graphique de tendance	Affiche le nombre d'entrées de vulnérabilité enregistrées chaque semaine.
Modèles les plus vulnérables	Couronne	Affiche les modèles (classes CI) avec les éléments les plus vulnérables.
Vulnérabilités par éditeur	À barres	Affiche le nombre d'éléments vulnérables enregistrés pour chaque éditeur, du plus important au moins élevé.
Vulnérabilités par impact	À barres	Affiche le nombre d'entrées de vulnérabilité pour les types de réseaux impactés.
Éditeurs les plus vulnérables	Couronne	Affiche les éditeurs avec les éléments les plus vulnérables.
CI les plus vulnérables	Couronne	Affiche les CI avec les éléments les plus vulnérables.
Vulnérabilités par score	À barres	Affiche le nombre d'entrées de vulnérabilité par scores de vulnérabilité.
Éléments vulnérables rouverts	Liste	Répertorie les éléments vulnérables rouverts ainsi que leur âge.
CI les plus vulnérables par classe	Couronne	Affiche les CI avec les éléments les plus vulnérables.
Âge de l'élément vulnérable	Liste	Répertorie le nombre de jours depuis la dernière ouverture des éléments vulnérables.
CI avec vulnérabilité par date	Liste	Répertorie les éléments de configuration qui ont été analysés au cours des 30 derniers jours.
CI pas analysés	Liste	Répertorie les éléments de configuration qui n'ont jamais été analysés pour détecter les vulnérabilités.

Tableau de bord de rattrapage de vulnérabilité

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Le tableau de bord Rattrapage de vulnérabilité contient les onglets suivants : **Affecté à mes groupes**, **Affecté à moi** et **Demandé par moi**. Les onglets Affecté à mes groupes et Affecté à moi affichent les mêmes rapports. Le premier onglet relève des groupes d'affectation auxquels vous appartenez et le second des éléments vulnérables ou des tâches de rattrapage qui vous sont affectées. L'onglet Requested by Me (Demandé par moi) signale les faux positifs et les exceptions que vous avez demandés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

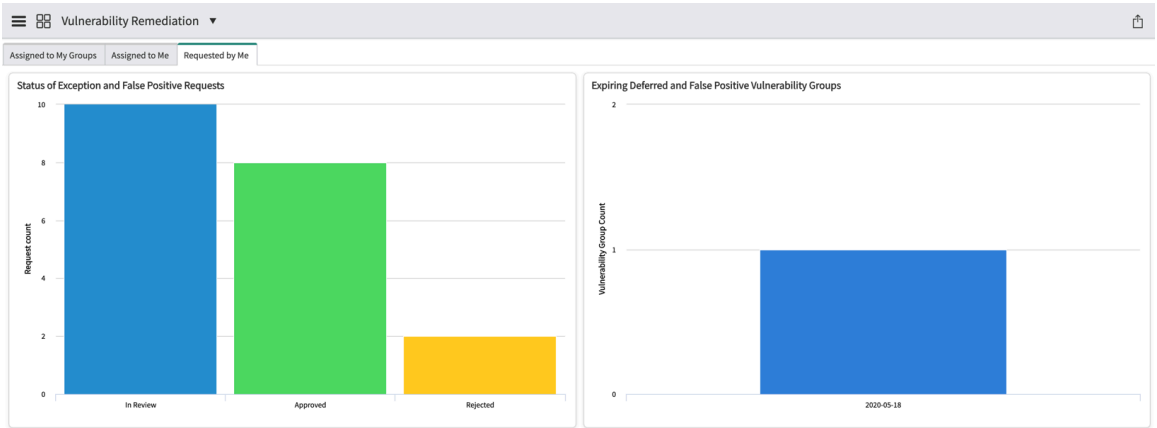
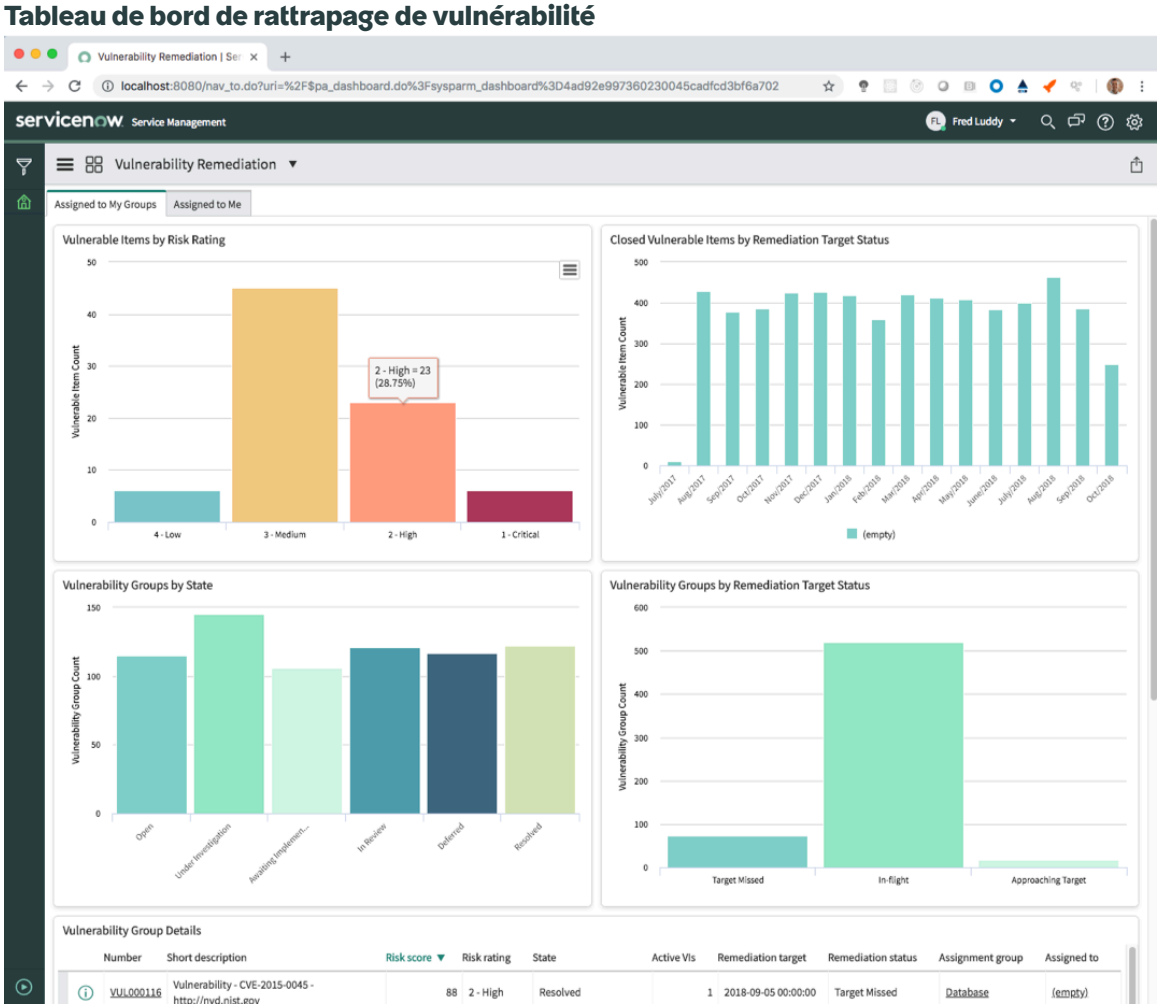


Tableau de bord de rattrapage de vulnérabilité



Traduction automatique

Rapports

Affecté à mes groupes et affecté à moi

Nom	Visuel	Description
Éléments vulnérables par cote de risque	Barre	Nombre d'éléments vulnérables actifs regroupés par cote de risque au cours de la période sélectionnée.
Éléments vulnérables fermés par état de la cible de rattrapage	Barre	Nombre d'éléments vulnérables fermés regroupés par état de la cible de rattrapage au cours de la période sélectionnée.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affecté à mes groupes et affecté à moi (suite)

Nom	Visuel	Description
Tâches de remédiation par état	Barre	Nombre de tâches de rattrapage (RT) actives regroupées par état.
Tâches de remédiation par état de la cible de remédiation	Barre	Nombre de temps de rattrapage actifs regroupés par état de la cible de rattrapage. Ce rapport exclut les éléments vulnérables différés.
Détails de la tâche de rattrapage		Détails d'enregistrement de tâche de rattrapage dans une liste.

Demandé par moi

Nom	Visuel	Description
État des demandes d'exception et de faux positifs	Barre	Nombre de demandes actives de votre part.
Tâches de remédiation et faux positifs différés arrivant à expiration	Barre	Nombre de tâches de rattrapage (RT) reportées et de faux positifs, regroupées par date de fin.

Tableau de bord des approbations de vulnérabilité

Le tableau de bord Approbations de vulnérabilité contient les rapports suivants pour les approbateurs d'exception et de faux positif.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Nom	Visuel	Description
Demandes d'exception et de faux positifs par âge en attente de mon approbation	Barre	Nombre d'approbations en attente pour vous, regroupées par date de création.
Mon approbation et mes demandes d'exception et de faux positifs rejetées	Barre	Nombre de demandes d'approbation approuvées ou rejetées, regroupées par état d'approbation.
Toutes les tâches de remédiation par cote de risque en attente d'approbation	Barre	Nombre de tâches de rattrapage en attente d'approbation, regroupées par cote de risque.
Toutes les demandes d'approbation en attente et de faux positifs regroupées par motif	Barre	Nombre de demandes d'approbation en attente regroupées par motif.

Platform Analytics et Reporting pour la gestion des vulnérabilités

Platform Analytics et Reporting comporte un contenu Analyse des performances et Reporting préparamétré pour être utilisé avec d'autres produits ServiceNow AI Platform. Cette solution d'analyse et de reporting vous permet de suivre le volume, les performances et la progression des vulnérabilités, de l'analyse initiale et de la détection au confinement ou à la correction. Vous pouvez filtrer les rapports par groupe d'affectation, exploits, cote de risque ou état.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le Analyse des performances pour Réponse aux vulnérabilités pack de contenu n'est pas automatiquement installé avec l'application Réponse aux vulnérabilités . Il est disponible sous forme d'abonnement ServiceNow Store séparé.

Analyse des performances pour Réponse aux vulnérabilités Contient deux tableaux de bord :

- Tableau de bord Gestion de la vulnérabilité (PA)
- Tableau de bord du responsable de la sécurité de l'information (CISO) de la gestion des vulnérabilités

Rôles requis, installation et affichage des tableaux de bord

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur ServiceNow AI Platform (admin) : installer et activer cette solution d'analyse et de génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Administrateur Analyse des performances (pa_admin) : passer en revue les indicateurs, les répartitions, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.

Pour installer cette application, consultez Installer et configurer l'application Analyse des performances pour Réponse aux vulnérabilités [PA].

Remarque : Configurez et testez les solutions d'analyse et de génération de rapports sur une instance de non-production avant de les activer en production.

Les solutions d'analyse et de génération de rapports nécessitent l'analyse des applications par défaut. Personnalisez ces enregistrements pour les utiliser dans votre environnement de production.

Pour afficher le tableau de bord Gestion de la vulnérabilité (PA), accédez à **Réponse aux vulnérabilités** > **Vue d'ensemble** > **.**

Pour afficher le tableau de bord du CISO de la gestion des vulnérabilités, accédez à **Réponse aux vulnérabilités** > **Tableau de bord des CISO** > **.**

Termes clés

Analyse des performances (PA)

Solution qui crée des tableaux de bord de gestion, des rapports sur les KPI et les mesures, et répond aux questions commerciales clés pour aider à améliorer la qualité et à réduire les coûts.

Élément vulnérable (VI)

Une vulnérabilité de sécurité signalée par un scanner de vulnérabilité tiers présent sur un élément de configuration (CI).

Tâche de rattrapage

Les tâches de rattrapage sont créées et affectées automatiquement aux équipes informatiques en fonction du groupe associé aux éléments vulnérables dans un effort de rattrapage. Les équipes informatiques et les propriétaires de rattrapage affichent les tâches de rattrapage dans l'espace de travail de rattrapage informatique. Pour plus d'informations, consultez Réponse aux vulnérabilités Espaces de travail

.

Indicateur PA

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définit une mesure de performance effectuée à intervalles réguliers d'un service d'entreprise, d'une activité ou d'un comportement organisationnel, par exemple, Éléments vulnérables critiques en retard non différés.

Source de l'indicateur PA

Ensembles de données qui filtrent les enregistrements d'une vue de table ou de base de données, par exemple, VI actif.

Afficher les visualisations de données en temps réel

Pour voir ce qui se passe aujourd'hui avec les éléments les plus critiques de votre Réponse aux vulnérabilités application, vous pouvez afficher certains rapports sur le tableau de bord Gestion des vulnérabilités (PA) en temps réel. L'affichage de ces rapports à la volée vous aide à gérer vos éléments vulnérables (VI) les plus importants et à les corriger rapidement. Vous pouvez afficher les rapports suivants en temps réel :

- Onglet Vue d'ensemble : éléments vulnérables par groupe d'affectation
- Onglet CI vulnérables
  - Éléments de configuration (CI) vulnérables sans propriétaires
  - CI mis hors service ou volés avec des VI actifs
- Onglet Exceptions
  - Éléments vulnérables différés par motif
  - Demandes de report sur le point d'expirer
  - Éléments vulnérables différés par gestionnaire DSI
- Onglet Rattrapage : éléments vulnérables non affectés

Pour plus d'informations, consultez Afficher Analyse des performances pour les rapports de Réponse aux vulnérabilités [PA] en temps réel.

Tableau de bord Gestion des vulnérabilités des CISO

Avec le tableau de bord Gestion des vulnérabilités CISO , affichez des données telles que les mesures clés des performances (KPI) pour la résolution de la vulnérabilité, consultez les risques les plus élevés, vérifiez la couverture des analyses et apprenez à réduire les risques.

Rôles ServiceNow AI Platform requis

- sn_vul.vulnerability_ciso pour afficher le tableau de bord.
- sn_vul.ciso_write pour modifier le tableau de bord.

Activer le tableau de bord des CISO

Pour activer le tableau de bord CISO, vous devez installer Analyse des performances et Réponse aux vulnérabilités activer la tâche Analyse des performances correspondante. Pour plus d'informations, consultez Solutions d'analyse et de reporting pour Vulnerability Response.

Cas d'utilisation

Utilisateur	Utilisation du tableau de bord
Responsables de la sécurité de l'information (CISO)	Les responsables de la sécurité de l'information (RSSI) peuvent utiliser le tableau de bord des CISO

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur	Utilisation du tableau de bord
	pour obtenir un aperçu du programme de gestion des vulnérabilités de leur organisation. Le tableau de bord fournit des données pour les aider à identifier en un coup d'œil comment ils peuvent les utiliser pour réduire les vulnérabilités de leurs environnements.

Utilisation du tableau de bord CISO

Les utilisateurs exécutifs, tels que les responsables de la sécurité de l'information (CISO) de votre organisation, peuvent consulter le tableau de bord des CISO pour Vulnerability Response afin de comprendre l'efficacité de leur programme de gestion des vulnérabilités. Vous pouvez afficher le tableau de bord des CISO en accédant à **Réponse aux vulnérabilités** > **Tableau de bord des CISO**. Utilisez les filtres de niveau supérieur pour filtrer les rapports par cote de risque, tranche d'âge ou accessible sur Internet. Certains rapports affichent des données de tendance sur une période de temps. Vous pouvez afficher régulièrement la tendance des mesures importantes, analyser le risque global de sécurité de l'entreprise et identifier les domaines à améliorer.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord peut également être affiché dans la nouvelle interface utilisateur. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Tableaux de bord dans l'espace de travail du gestionnaire de vulnérabilité et Tableaux de bord dans l'espace de travail Rattrapage informatique.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Exécution des travaux planifiés

Exécutez les travaux planifiés dans cet ordre pour mettre à jour les données dans les rapports :

1. Mettre à jour les tables du tableau de bord
2. [PA VR] Tableau de bord des CISO

Travaux planifiés pour le tableau de bord CISO

Nom de la tâche planifiée	Description
Mettre à jour les tables du tableau de bord	Tâche planifiée quotidienne que vous devez exécuter avant la tâche du tableau de bord des CISO [PA VR] AFIN DE POUVOIR COLLECTER LES DONNÉES CISO. En exécutant cette tâche planifiée, vous mettez à jour les rapports de couverture de l'analyse. Les informations mises à jour comprennent les éléments de configuration opérationnelle (CI) analysés au cours des 90 derniers jours, leurs classes et le nombre total de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Travaux planifiés pour le tableau de bord CISO (suite)

Nom de la tâche planifiée	Description
	CI opérationnels qui correspondent à ces classes. L'exécution de cette tâche planifiée met également à jour les rapports dans l'onglet **Actions recommandées** . **Remarque :** Les CI opérationnels désignent les CI dont le statut opérationnel est Opérationnel.
[PA VR] Tableau de bord des CISO	Une fois la tâche planifiée Mettre à jour les tables de tableau de bord terminée, exécutez cette tâche planifiée pour renseigner tous les rapports dans l'onglet **Vue d'ensemble du CISO** .

Onglets du tableau de bord du CISO

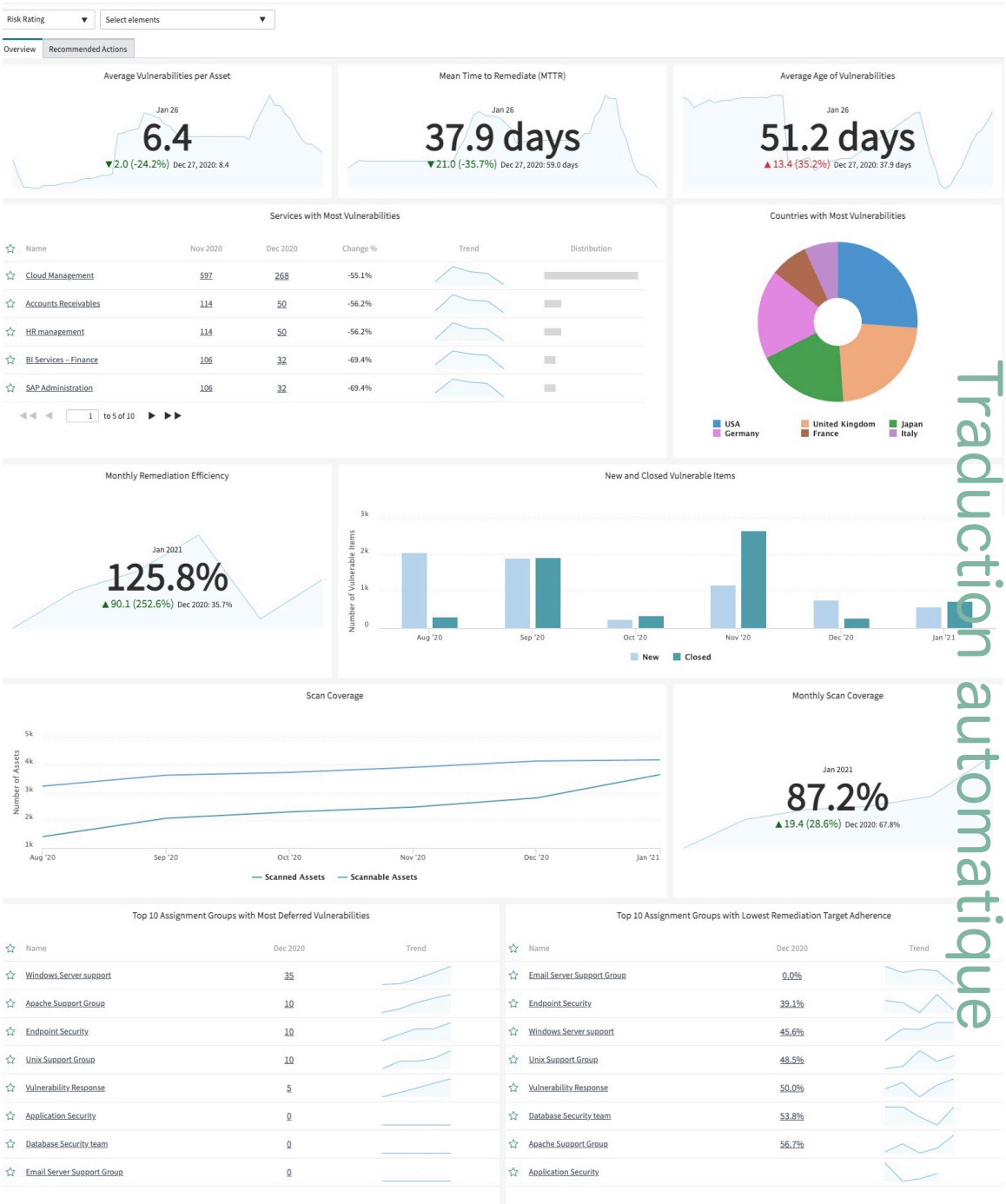
Ce tableau de bord fournit un aperçu des risques présents dans la gestion des vulnérabilités. Vous pouvez afficher les vulnérabilités et leurs données connexes par région, âge, services et autres répartitions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble

L'onglet Vue d'ensemble contient des rapports qui fournissent en un coup d'œil la posture de sécurité de votre organisation.



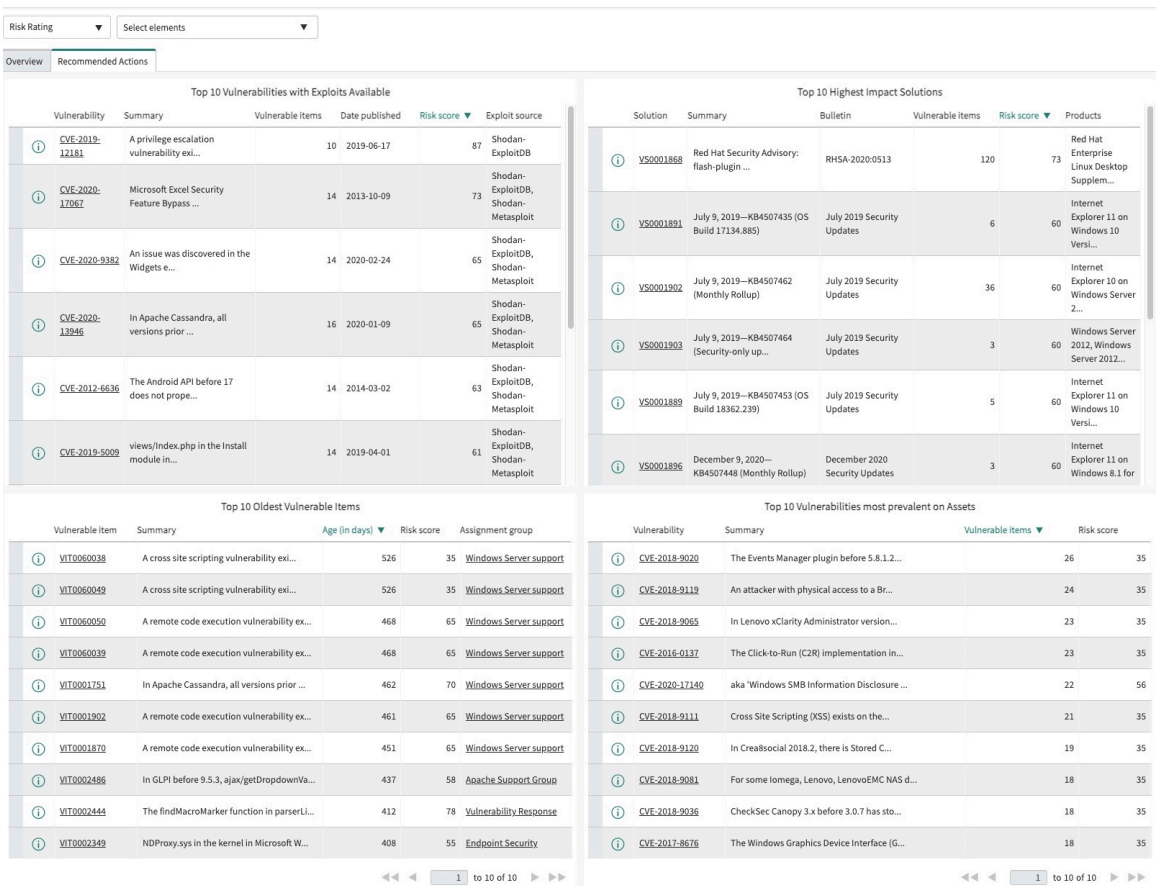
Remarque : Le filtre de niveau supérieur ne peut être utilisé que pour certains rapports.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Actions recommandées

L'onglet Actions recommandées contient des rapports qui fournissent des informations sur les vulnérabilités exploitables, vieillissantes et répandues. Il contient également des solutions qui recommandent des actions pour réduire les risques. Exécutez la tâche planifiée **Mettre à jour les tables de tableau de bord du CISO** pour mettre à jour les rapports de cet onglet.



Indicateurs

Pour afficher les indicateurs, naviguez vers **Analyse des performances** > **Indicateurs**.

1. Sur la page Indicateurs, recherchez le nom de l'indicateur requis dans la colonne Nom.
2. Cliquez sur le nom de l'indicateur pour ouvrir l'enregistrement et en afficher les détails.

   Les indicateurs du tableau de bord CISO ne collectent pas d'enregistrements par défaut. Vous pouvez choisir de collecter les enregistrements en cochant la case Collecter les enregistrements.

Durée totale des éléments vulnérables clôturés

La durée totale des VI fermés est mesurée quotidiennement en jours. L'objectif de cet indicateur est de minimiser le score.

Actifs analysables

La valeur Actifs analysés est mesurée quotidiennement en unité #. L'objectif de cet indicateur est de maximiser le score.

Services avec le plus de vulnérabilités

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La valeur Services avec le plus de vulnérabilités est mesurée quotidiennement en unité #. L’objectif de cet indicateur est de minimiser le score.

Nombre moyen de vulnérabilités par actif

[[Éléments vulnérables actifs]] / [[Éléments de configuration vulnérables actifs]

Éléments vulnérables clôturés

La valeur Éléments vulnérables fermés est mesurée quotidiennement en unité #. L’objectif de cet indicateur est de maximiser le score.

Délai moyen de remédiation des éléments vulnérables

[[Durée cumulée des éléments vulnérables fermés]] / [[Éléments vulnérables fermés]]

Couverture de l'analyse actuelle

Calcule la couverture de l’analyse actuelle en pourcentage.

Actifs analysés

La valeur Actifs analysés est mesurée quotidiennement en unité #. L’objectif de cet indicateur est de maximiser le score.

Éléments vulnérables clôturés (cible atteinte)

La valeur Éléments vulnérables fermés (cible atteinte) est mesurée quotidiennement en unité #. L’objectif de cet indicateur est de maximiser le score.

% d'éléments vulnérables clôturés ayant atteint leur cible

[[Éléments vulnérables fermés (cible atteinte) / SOMME par mois]] / [[Éléments vulnérables fermés / SOMME par mois]] *100

Éléments vulnérables actifs

La valeur Éléments vulnérables actifs est mesurée quotidiennement en unité #. L’objectif de cet indicateur est de minimiser le score.

Âge moyen des éléments vulnérables

La valeur Âge moyen des VI actifs est mesurée quotidiennement en unité Jours. L’objectif de cet indicateur est de minimiser le score.

Remarque : La personnalisation du calcul de l’âge et de l’âge fermé pour les éléments vulnérables (VI) peut entraîner une forte hausse ou une baisse des rapports d’Analyse des performances (PA) qui incluent ces mesures. Pour plus d’informations sur la personnalisation du calcul de l’âge et de l’âge fermé pour les VI, consultez l’article de la base de connaissances KB1703270 .

Éléments de configuration des éléments vulnérables actifs

La valeur CI vulnérables actifs est mesurée quotidiennement en unité #. L’objectif de cet indicateur est de minimiser le score.

Efficacité de la remédiation mensuelle

[Nombre d'éléments vulnérables fermés au cours d'un mois] / [Nombre d'éléments vulnérables nouveaux ou rouverts au cours du même mois]

Nouveaux éléments vulnérables

La valeur Nouveaux éléments vulnérables est mesurée quotidiennement en unité #. L’objectif de cet indicateur est de minimiser le score.

Éléments vulnérables différés

La valeur des VI différés est mesurée quotidiennement en unité #. L’objectif de cet indicateur est de minimiser le score.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Répartitions

- Groupe d'affectation : s'applique à certains rapports de VI.
- Cote de risque : s'applique aux rapports des VI.
- Tranche d'âge : s'applique aux déclarations de VI.
- Âge fermé : s'applique aux rapports des VI fermés.
- Accessible sur Internet : indique si le CI appartient à la classe des matériels et est accessible sur Internet.
- Région : le paramètre de CI CMDB utilisé est Emplacement. Cet emplacement indique le pays d'origine de l'élément de configuration.

Remarque : La personnalisation du calcul de l'âge et de l'âge fermé pour les éléments vulnérables (VI) peut entraîner une forte hausse ou une baisse des rapports d'Analyse des performances (PA) qui incluent ces mesures. Pour plus d'informations sur la personnalisation du calcul de l'âge et de l'âge fermé pour les VI, consultez l'article de la base de connaissances KB1703270 .

Visualisations des données

Nom	Type	Description
Nombre moyen de vulnérabilités par actif	Score unique	Nombre moyen d'éléments vulnérables actifs pour chaque élément de configuration
Délai moyen de rattrapage (MTTR)	Score unique	Le délai moyen de rattrapage (fermeture) d'un élément vulnérable, affiché comme moyenne d'exécution de 30 jours. **Remarque :** La valeur Âge à la fermeture est calculée lors de la collecte des données. La valeur est la différence entre la date de la dernière ouverture et la date et l'heure de la tâche de collecte.
Âge moyen des vulnérabilités	Score unique	Âge moyen des éléments vulnérables actifs en jours.
Services avec le plus de vulnérabilités	Liste et ligne	Moyenne mensuelle des éléments vulnérables actifs pour les services de l'organisation. **Remarque :** Pour plus d'informations sur la définition des classifications de service que vous souhaitez afficher dans les rapports de Réponse aux vulnérabilités et les listes connexes, consultez l'onglet Services dans le tableau de bord Gestion des vulnérabilités [PA].
Pays avec le plus de vulnérabilités	Icône de	Top 10 des pays ayant le plus grand nombre d'éléments vulnérables.
Efficacité de la remédiation mensuelle	Score unique	Pourcentage d'éléments vulnérables fermés divisés par de nouveaux éléments vulnérables au cours du mois en cours.
Éléments vulnérables nouveaux et fermés	Barre	Nombre de nouveaux éléments vulnérables importés et Nombre d'éléments vulnérables fermés en un mois.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Couverture de l'analyse	Ligne	Nombre d'actifs analysés par rapport au nombre total d'actifs analysables, affichés au fil du temps. Les classes CI incluses dans le widget sont spécifiées dans le module Configuration de la couverture d'analyse. Pour plus d'informations sur la configuration du module Couverture de l'analyse, voir Configurer les rapports de couverture de l'analyse.
Couverture de l'analyse mensuelle	Score unique	Pourcentage d'actifs analysés divisé par le nombre total d'actifs analysables pour le mois en cours. Pour plus d'informations sur la configuration du module Couverture de l'analyse, voir Configurer les rapports de couverture de l'analyse
10 premiers groupes d'affectation avec les vulnérabilités les plus différées	Liste et ligne	10 premiers groupes d'affectation ayant le nombre le plus élevé d'éléments vulnérables différés, différés en fonction de la moyenne mensuelle.
10 premiers groupes d'affectation avec l'adhésion à la cible de rattrapage la plus faible	Liste et ligne	10 premiers groupes d'affectation dont les éléments vulnérables adhèrent le moins à leurs cibles de rattrapage.

Actions recommandées

Nom	Type	Table source	Description
10 principales vulnérabilités avec exploits disponibles		Élément vulnérable principal [sn_vul_analytics_top_item]	Vulnérabilités actives avec exploits disponibles pour tous les fournisseurs de renseignements sur les menaces qui utilisent le cadre de travail d'exploit VR.
Top 10 des solutions les plus impactantes		Élément vulnérable principal [sn_vul_analytics_top_item]	Solutions ou correctifs préférés avec les scores de risque les plus élevés pour les éléments vulnérables actifs. Ce rapport utilise les fonctionnalités de Vulnerability Solution Management (VSM), qui établit une corrélation entre les correctifs de Microsoft et Red Hat et les vulnérabilités de l'environnement. VSM permet d'identifier la solution privilégiée pour les vulnérabilités.
10 principaux éléments vulnérables les plus anciens		Élément vulnérable principal [sn_vul_analytics_top_item]	Éléments vulnérables actifs ayant l'âge le plus élevé. Résolvez ces éléments pour abaisser l'âge moyen de vulnérabilité dans l'onglet Vue d'ensemble.
10 principales vulnérabilités les plus		Élément vulnérable principal [sn_vul_analytics_top_item]	Éléments vulnérables actifs disponibles pour le plus grand nombre d'actifs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions recommandées (suite)

Nom	Type	Table source	Description
répandues sur les actifs			

Configurer les rapports de couverture d'analyse

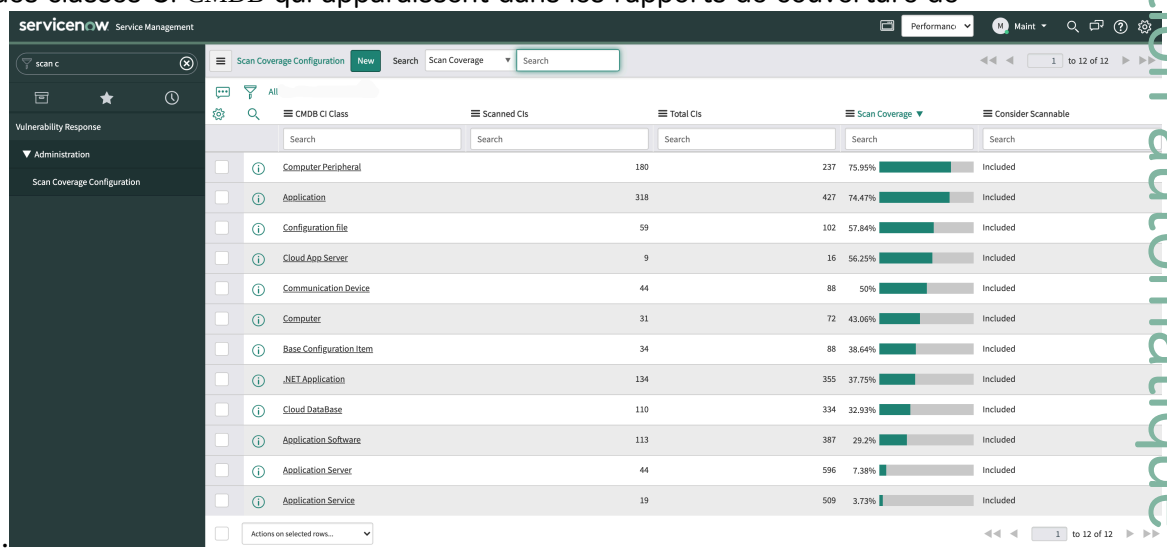
Permettez à vos utilisateurs d'exécuter des rapports de couverture d'analyse à partir du tableau de bord CISO. Grâce à ces rapports, vos utilisateurs peuvent voir quelle est la couverture d'analyse de l'organisation sur une période donnée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst

Pourquoi et quand exécuter cette tâche

La couverture de l'analyse indique le nombre d'actifs analysés par les analyseurs de vulnérabilité pour les différentes classes au cours des 90 derniers jours. Ces actifs sont comparés au nombre d'actifs analysables dans le Base de données de gestion des configurations (CMDB). Par défaut, le module Configuration de la couverture d'analyse inclut des CMDB classes CI, auxquelles au moins un actif analysé a été associé. Vous pouvez ajouter une classe CI à partir du rapport de couverture de l'analyse qui s'affiche sur le tableau de CMDB bord CISO. Vous pouvez inclure ou exclure des classes CI CMDB qui apparaissent dans les rapports de couverture de l'analyse.



Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Configuration de la couverture d'analyse**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Configuration de la couverture d'analyse

Champ	Description
Classe CI CMDB	Classe CI qui doit être ajoutée au rapport de couverture de l'analyse sur le tableau de bord CISO.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si une classe CI existe déjà dans le module Configuration de la couverture d'analyse, elle n'est pas incluse dans cette liste.
Considérer l'élément analysable	Option permettant de définir si la classe CI doit être incluse ou non. Incluez une classe CI si vous souhaitez que ses données soient ajoutées aux rapports de couverture de l'analyse. En cas d'exclusion, les données de cette classe CI ne sont pas ajoutées.

4. Cliquez sur **Envoyer**.

Configurer les indicateurs PA pour le tableau de bord CISO

Surveillez les indicateurs CISO automatisés et formulés afin de pouvoir gérer les données de vulnérabilité dans votre instance.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités comporte à la fois des indicateurs automatisés et des indicateurs formulés.

Termes clés

Indicateur

Définit une mesure de performance effectuée à intervalles réguliers d'un service d'entreprise, d'une activité ou d'un comportement organisationnel. Un exemple est un élément vulnérable actif.

Source de l'indicateur

Ensembles de données constitués d'enregistrements filtrés à partir d'une vue de table ou de base de données pour une efficacité accrue. Par exemple, VI.Active (accessible sur Internet).

Répartitions

Les répartitions filtrent et regroupent les scores des indicateurs à l'aide d'attributs qualitatifs tels que la priorité, la catégorie et le groupe d'affectation.

Travaux planifiés

Les travaux planifiés sont exécutés pour renseigner les données sources de l'indicateur. La tâche planifiée quotidienne du tableau de bord des CISO [PA VR] EST DÉSACTIVÉE PAR DÉFAUT. Vous devez l'activer pour collecter les scores d'indicateurs pour le tableau de bord CISO.

Procédure

1. Accédez à la **Tous** > **Analyse des performances** > **Indicateurs** et choisissez l'une des options suivantes :
   - Indicateurs automatisés
   - Indicateurs de formule

   Pour plus d'informations sur les indicateurs, consultez Indicateurs Analyse des performances .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Sur la page Indicateurs, recherchez le nom de l'indicateur requis dans la colonne Nom.
3. Cliquez sur le nom de l'indicateur pour ouvrir l'enregistrement et en afficher les détails.

Les indicateurs du tableau de bord CISO ne collectent pas d'enregistrements par défaut. Vous pouvez choisir de collecter les enregistrements en cochant la case **Collecter les enregistrements** .

Remarque : L'activation de la collecte des enregistrements dans un indicateur peut entraîner des problèmes de performances, tels que beaucoup plus de temps et de mémoire requis pour exécuter le travail de collecte de données.

Le nombre maximal de lignes que vous pouvez extraire pour une source d'indicateur est de 1 million de lignes.

Tableau de bord Intégrité de SecOps Vulnerability Response

Le tableau de bord Intégrité de Vulnerability Response est un outil conçu pour fournir aux organisations des aperçus complets de l'implémentation et de l'utilisation de leurs applications Vulnerability Response.

L'évaluation de l'intégrité globale est déterminée par l'agrégation de divers facteurs critiques dans la configuration, l'implémentation, l'intégration, les performances, les données et les processus. Affichez le tableau de bord agrégé pour chaque catégorie pour les applications suivantes :

- Réponse aux vulnérabilités
- Réponse aux vulnérabilités de l'application
- Réponse aux vulnérabilités du conteneur
- Conformité de la configuration

Installation du tableau de bord d'intégrité de SecOps Vulnerability Response

Pour installer et configurer le tableau de bord d'intégrité de SecOps Vulnerability Response pour Réponse aux vulnérabilités les applications dans votre ServiceNow AI Platform instance, accédez au module d'extension ServiceNow® Store SecOps Health Analytics (sn_sec_analytics) et activez-le.

Rôles ServiceNow AI Platform requis

Rôles requis : sn_sec_analytics.admin, sn_sec_analytics.read

Tâche planifiée

Pour afficher la tâche planifiée, accédez à **Tous** > **Planificateur système** > **Travaux planifiés** > **Collecter les mesures du tableau de bord d'intégrité**. La tâche planifiée « Collecter les mesures du tableau de bord d'intégrité » est exécutée quotidiennement à 00h00. Il génère les données du tableau de bord Intégrité de SecOps Vulnerability Response. Vous pouvez également choisir d'exécuter manuellement la tâche planifiée.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les personnes de votre organisation utilisent ce tableau de bord, consultez les cas d'utilisation suivants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur	Utilisation du tableau de bord
Administrateur de Vulnerability	Vous aide à mieux comprendre le score d'intégrité des Réponse aux vulnérabilités applications. Il est également utile de mettre en évidence les domaines qui doivent être améliorés. Le tableau de bord Intégrité de Vulnerability Response ne traite que de l'intégrité de l'implémentation et de l'utilisation. Il n'aide pas à la gestion des vulnérabilités ou des actifs.
Administrateur de l'assistance	Vous aide à identifier les problèmes de performances, de personnalisation et de configuration à l'aide des KPI. En fonction de l'intégrité de l'application, vous pouvez effectuer une analyse supplémentaire ou fournir une recommandation aux utilisateurs.
Partenaire d'implémentation	Vous aide à évaluer l'intégrité de l'implémentation Réponse aux vulnérabilités des configurations, des compléments, des personnalisations et des intégrations, et à fournir des recommandations d'amélioration aux utilisateurs.

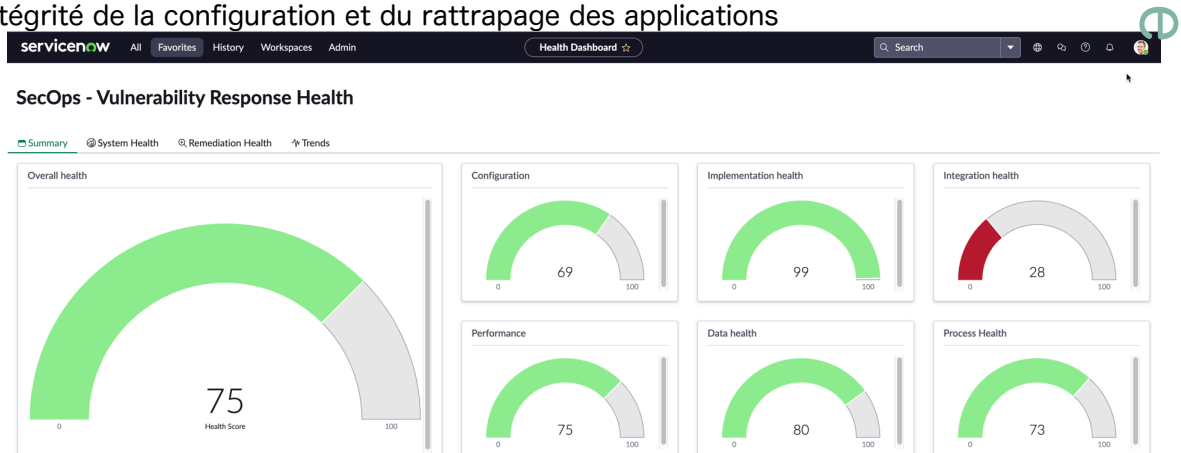
Onglets du tableau de bord Intégrité de SecOps Vulnerability Response

Pour afficher le tableau de bord Intégrité de SecOps Vulnerability Response, accédez à **Intégrité de Security Operations** > **Intégrité de Vulnerability Response**. Chaque couleur du tableau de bord représente les éléments suivants :

- Vert : Sûr
- Jaune : avertissement
- Rouge : critique

Onglet Résumé

Ce tableau de bord communique le score d'intégrité global pour l'intégrité de la configuration et du rattrapage des applications VR.

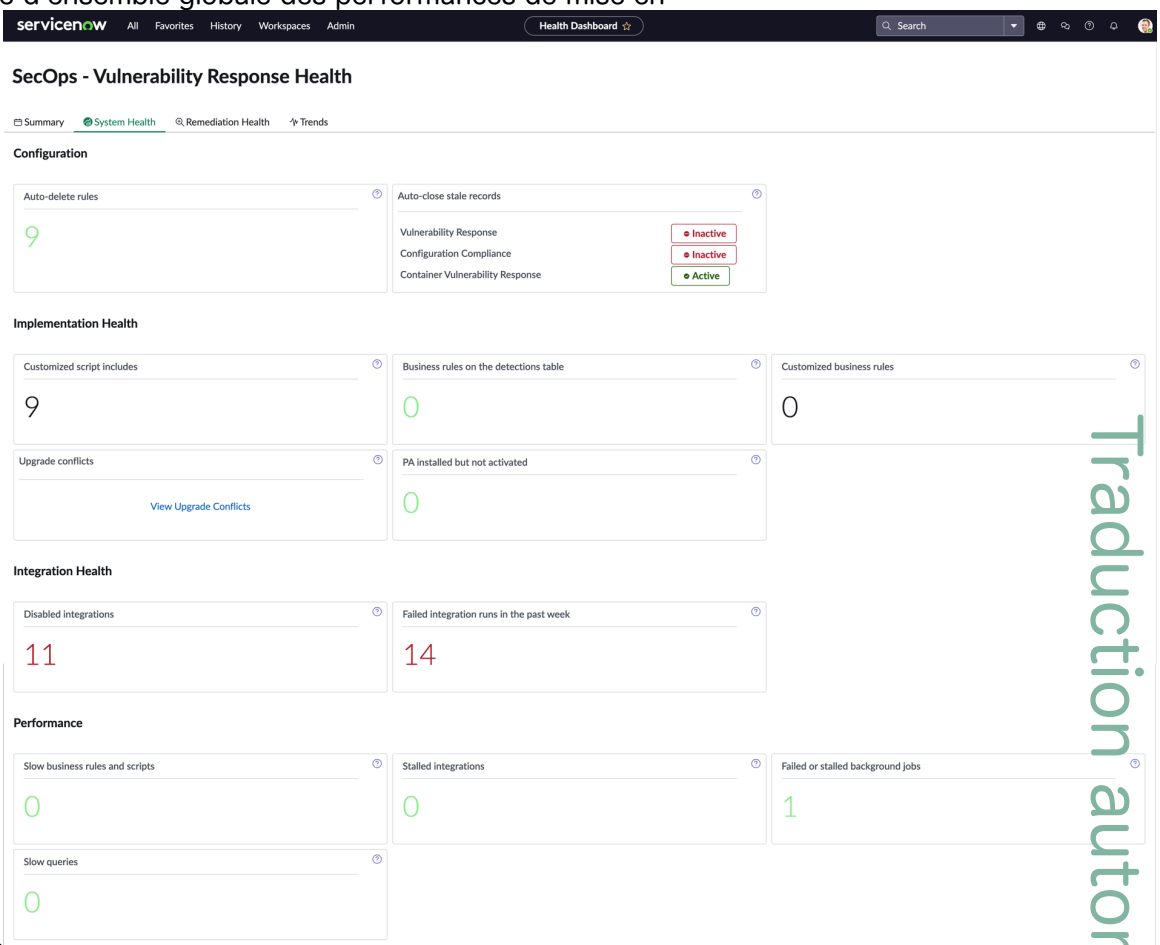


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Intégrité du système

Ce tableau de bord affiche l'intégrité de la configuration et de l'intégration de votre implémentation. Elle fournit une vue d'ensemble globale des performances de mise en œuvre.

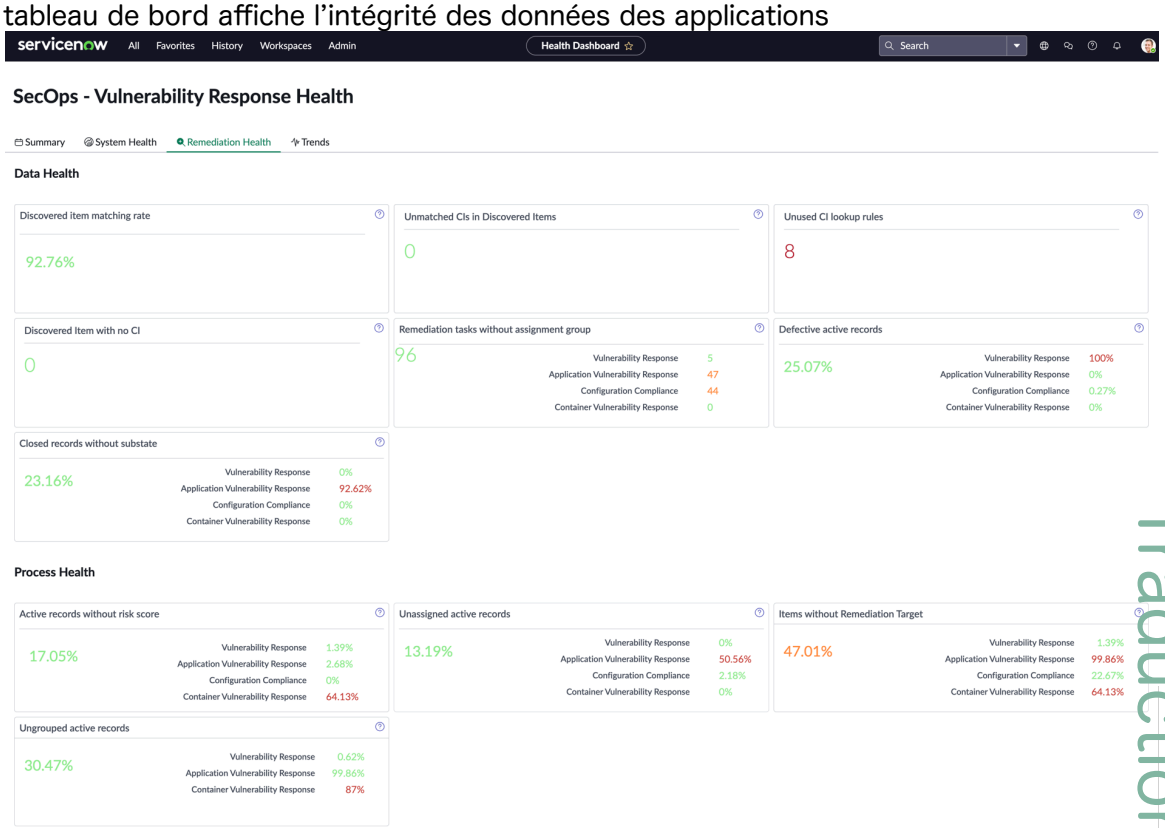


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

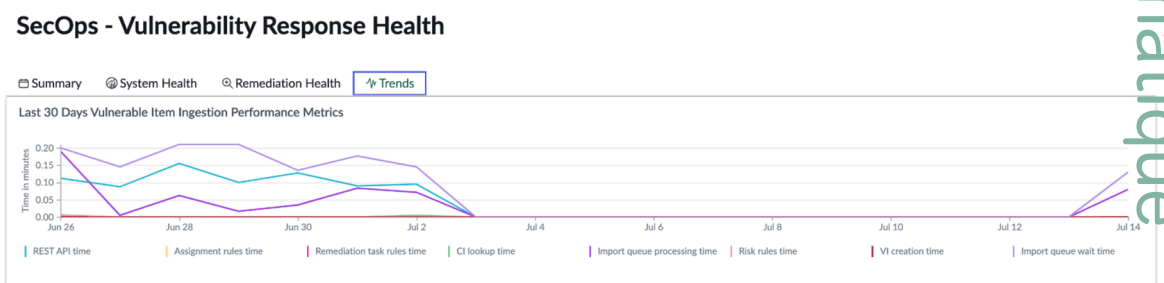
Onglet Intégrité du rattrapage

Ce tableau de bord affiche l'intégrité des données des applications VR.



Onglet Tendances

Ce tableau de bord affiche les tendances des mesures de performance d'ingestion d'éléments vulnérables au cours des 30 derniers jours pour les applications VR.



Rapports

Remarque : Les valeurs de seuil font partie du système de base. Vous pouvez configurer les valeurs en fonction de vos besoins.

Résumé

Titre	Description
Intégrité globale	Score d'intégrité global pour les applications VR. Pour plus d'informations, consultez les rapports pour les mesures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résumé (suite)

Titre	Description
Configuration	Intégrité globale de la configuration des applications VR.
Intégrité de l'implémentation	Intégrité globale de l'implémentation des applications VR.
Intégrité de l'intégration	Intégrité globale de l'intégration des applications VR.
Performances	Score d'intégrité des performances globales des applications VR.
Intégrité des données	Intégrité globale des données des applications VR.
Intégrité des processus	Score d'intégrité global des processus des applications VR.

Intégrité du système

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
Configuration				
Règles de suppression automatique	Affiche le nombre de règles de suppression automatique activées.	Examinez et résolvez les règles de suppression automatique inactives.	3	1
Fermer automatiquement les enregistrements obsolètes	Ferme automatiquement les détections obsolètes. Pour plus d'informations, consultez la rubrique « Fermer automatiquement les détections périmées dans Vulnerability Response » dans servicenow.com/docs.	Réduisez le volume des détections périmées. Activez cette option pour fermer les détections périmées qui ne sont pas fermées par les scanners.	3	1
Intégrité de l'implémentation				
Includes de script personnalisés	Nombre de « includes de script » personnalisés.	Réduisez les « includes de script » personnalisés pour faciliter les mises à niveau.	10	12
Règles métier sur la table de détections	Nombre de règles métier	Minimisez les règles métier pour faciliter les mises à niveau.	4	8

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrité du système (suite)

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
	personnalisées dans la table de détection.			
Règles métier personnalisées	Nombre de règles métier personnalisées avant la création d'enregistrements dans la CMDB.	Utilisez les règles métier par défaut sur les enregistrements.	5	8
Conflits de mise à niveau	Les conflits tels que les règles métier et les scripts identifiés lors d'une mise à niveau.	Examinez et résolvez les conflits de mise à niveau.	10	15
PA installé mais pas activé	Indique si le tableau de bord Analyse des performances n'est pas activé.	Activez le tableau de bord PA.	10	15
Intégrité de l'intégration				
Intégrations désactivées	Nombre d'intégrations qui ont été désactivées.	Examinez et activez les intégrations requises.	6	9
Échec de l'exécution de l'intégration au cours de la semaine écoulée	Nombre d'exécutions d'intégration qui ont échoué au cours de la semaine écoulée.	Examinez et résolvez la cause de l'échec des exécutions d'intégration.	9	12
Performances				
Règles métier et scripts lents	Règles métier et scripts dont le temps d'exécution moyen est supérieur à 10 ms et dont le nombre d'exécutions est supérieur à 10 000.	Examinez et résolvez les règles métier lentes.	10	15
Intégrations bloquées	Nombre d'intégrations qui ont expiré avant l'achèvement.	Examinez et résolvez la cause du blocage des intégrations.	10	15
Échec ou blocage des tâches en arrière-plan	Échec ou expiration des tâches en arrière-plan au cours de la dernière semaine.	Examinez et résolvez la cause des tâches ayant échoué.	5	10

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrité du système (suite)

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
Requêtes lentes	Requêtes dont le temps d'exécution moyen est supérieur à 10 ms et dont le nombre d'exécutions est supérieur à 10 000.	Examinez et résolvez les règles métier lentes.	10	15

Intégrité du rattrapage

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
Intégrité des données				
Taux de correspondance des éléments détectés	Nombre d'éléments détectés correspondant à des CI existants.	Examinez l'intégrité de votre CMDB et la logique des règles de recherche de CI.	50	20
CI sans correspondance dans les éléments détectés	Éléments détectés dont l'état est sans correspondance	Examinez l'intégrité de votre CMDB et la logique des règles de recherche de CI.	9	12
Règles de recherche de CI inutilisées	Règles de recherche de CI qui ne sont associées à aucun élément détecté.	Changez l'état des règles de recherche de CI inutilisées sur inactif.	4	6
Élément détecté sans CI	Élément détecté sans élément de configuration.	Examinez et réappliquez les règles de recherche de CI.	9	12
Enregistrements actifs défectueux	Enregistrements sans élément de configuration ni vulnérabilité.	Mettez hors service les CI à l'aide de l'option Gestion du cycle de vie des CI de la CMDB.	40	60

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrité du rattrapage (suite)

Titre	Description	Considérations relatives à l'amélioration des performances	Avertissement de seuil	Seuil critique
		Remarque : La suppression directe des CI peut entraîner la création de VIT orphelins.		
Tâches de rattrapage sans groupe d'affectation	Tâches de rattrapage actives dont le groupe d'affectation n'est pas encore affecté.	Affectez des tâches de rattrapage à un groupe d'affectation et passez en revue les règles d'affectation existantes.	40	60
Enregistrements fermés sans sous-état	Enregistrements qui sont fermés sans sous-état.	Fournissez des informations dans le champ Motif lors de la fermeture des enregistrements.	40	50
Intégrité des processus				
Enregistrements actifs sans score de risque	Enregistrements actifs avec un score de risque de 0 ou sans score de risque affecté.	Examinez et résolvez les règles de risque.	40	60
Enregistrements actifs non affectés	Enregistrements sans groupe d'affectation.	Affectez un groupe aux enregistrements et passez en revue les règles d'affectation existantes.	30	50
Éléments sans cible de rattrapage	Éléments sans date cible de rattrapage.	Examinez et résolvez les règles de cibles de rattrapage. Ces règles doivent inclure tous les enregistrements.	30	50
Enregistrements actifs dégroupés	Enregistrements qui ne sont pas inclus dans une règle de tâche de rattrapage.	Passez en revue les règles de la tâche de rattrapage.	40	60

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tendances

Titre	Description
Mesures de performance d'ingestion d'élément vulnérables au cours des 30 derniers jours	Temps moyen nécessaire pour ingérer des éléments vulnérables et traiter plusieurs règles au cours des 30 derniers jours.

Modifier les valeurs de seuil

Vous pouvez modifier les valeurs de seuil des données du tableau de bord Intégrité SecOps VR en fonction de vos préférences.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Intégrité de Security Operations** > **Configuration** > **Mesures**.
2. Sur la page Données du tableau de bord d'intégrité, ouvrez l'enregistrement que vous souhaitez modifier.
3. Mettez à jour l'enregistrement et enregistrez.

Tableau de bord Gestion des vulnérabilités (PA)

Suivez le volume, les performances et la progression des vulnérabilités, de l'analyse initiale et de la détection au confinement ou à la correction. Vous pouvez filtrer les rapports par groupe d'affectation, exploits, cote de risque ou état, par exemple. Obtenez rapidement un aperçu de votre exposition à la vulnérabilité et des services d'entreprise affectés.

Rôles ServiceNow AI Platform requis

Rôle requis : sn_vul.vulnerability_admin, sn_vul.vulnerability_analyst et les utilisateurs ayant sn_vul.vulnerability_read (ou qui héritent du rôle sn_vul.vulnerability_read) et pa_viewer.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Responsables informatiques, analystes informatiques, responsables de la résolution des vulnérabilités	Aidez votre organisation à faire face à l'augmentation des incidents de sécurité dus à des vulnérabilités exploitées en déterminant efficacement quels éléments vulnérables présentent le plus de risque. Ces tableaux de bord fournissent une vue graphique de l'activité des éléments vulnérables et aident à concevoir des plans de rattrapage et à progresser dans l'état. Vous pouvez vous concentrer sur les KPI associés aux actifs affectés critiques et aux vulnérabilités à haute visibilité.

Pour afficher le tableau de bord de la gestion de la vulnérabilité (PA), accédez à **Réponse aux vulnérabilités** > **Vue d'ensemble**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consultez les rapports qui affichent les données de tendance dans le temps. Les rapports contenant des données en temps réel sont énumérés ci-dessous. Consultez régulièrement les tendances des mesures importantes pour analyser vos processus business globaux et identifier les domaines d'amélioration.

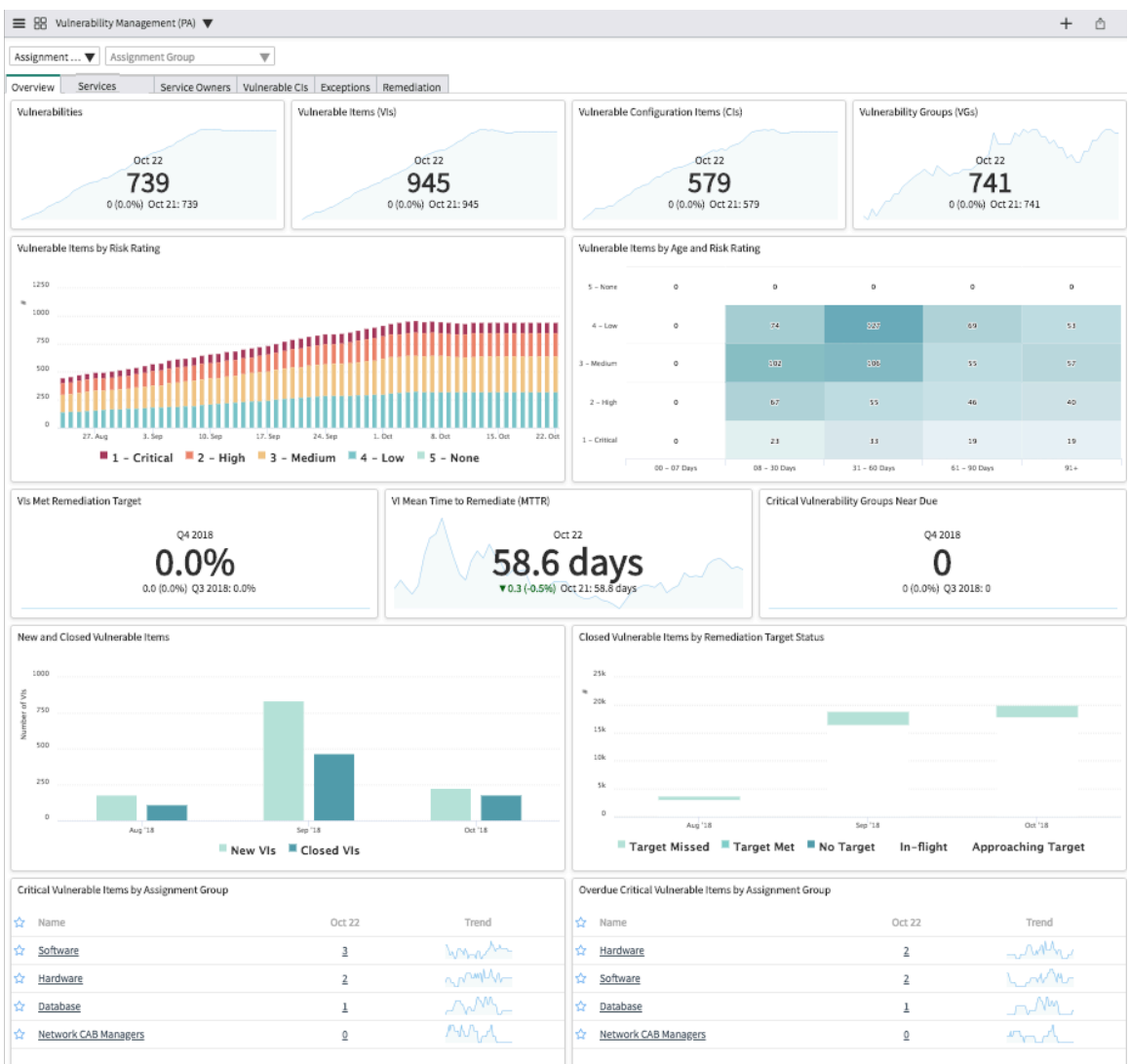
Pour plus d'informations sur l'affichage de vos rapports PA avec des scores en temps réel, consultez Afficher Analyse des performances pour les rapports de Vulnerability Response [PA] en temps réel.

Onglets du tableau de bord Gestion de la vulnérabilité [PA]

Onglet Vue d'ensemble

Ce tableau de bord communique les KPI pour le risque et la prévalence de la vulnérabilité, les actifs affectés, le respect de la cible de rattrapage et la progression du rattrapage.

Dans l'onglet Vue d'ensemble, vous pouvez afficher le rapport Éléments vulnérables critiques par groupe d'affectation qui est exécuté en fonction de la tâche planifiée.



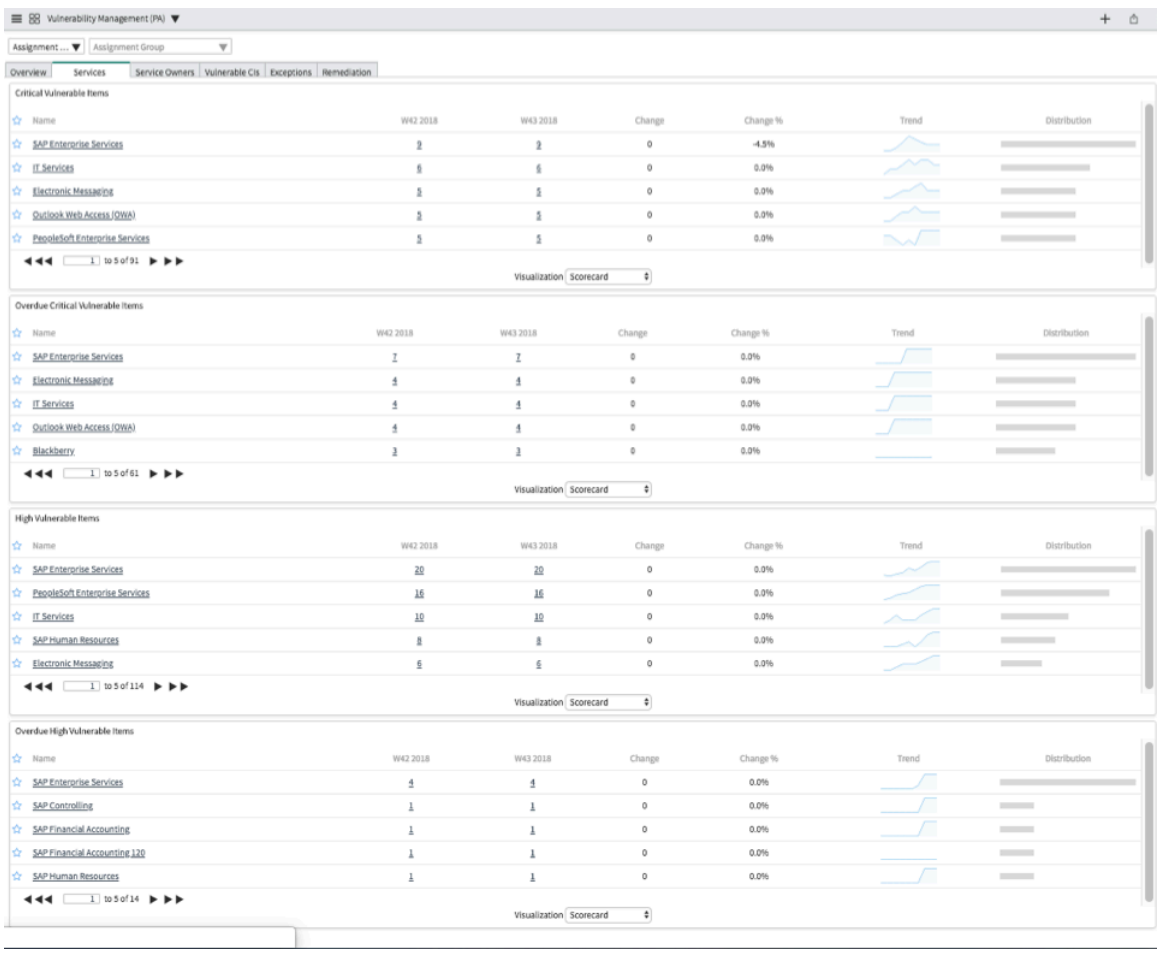
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Services d'entreprise

Ce tableau de bord expose le risque de vulnérabilité au niveau du service d'entreprise. Le partage de ces informations au sein de l'organisation peut aider les gestionnaires de services à corriger les vulnérabilités rapidement et de manière proactive, et conduire l'organisation vers un modèle de responsabilité partagée de la sécurité de l'information.

Vous pouvez modifier la classe de service en services techniques ou d'application à l'aide de la propriété système `sn_vul.service_classifications`.

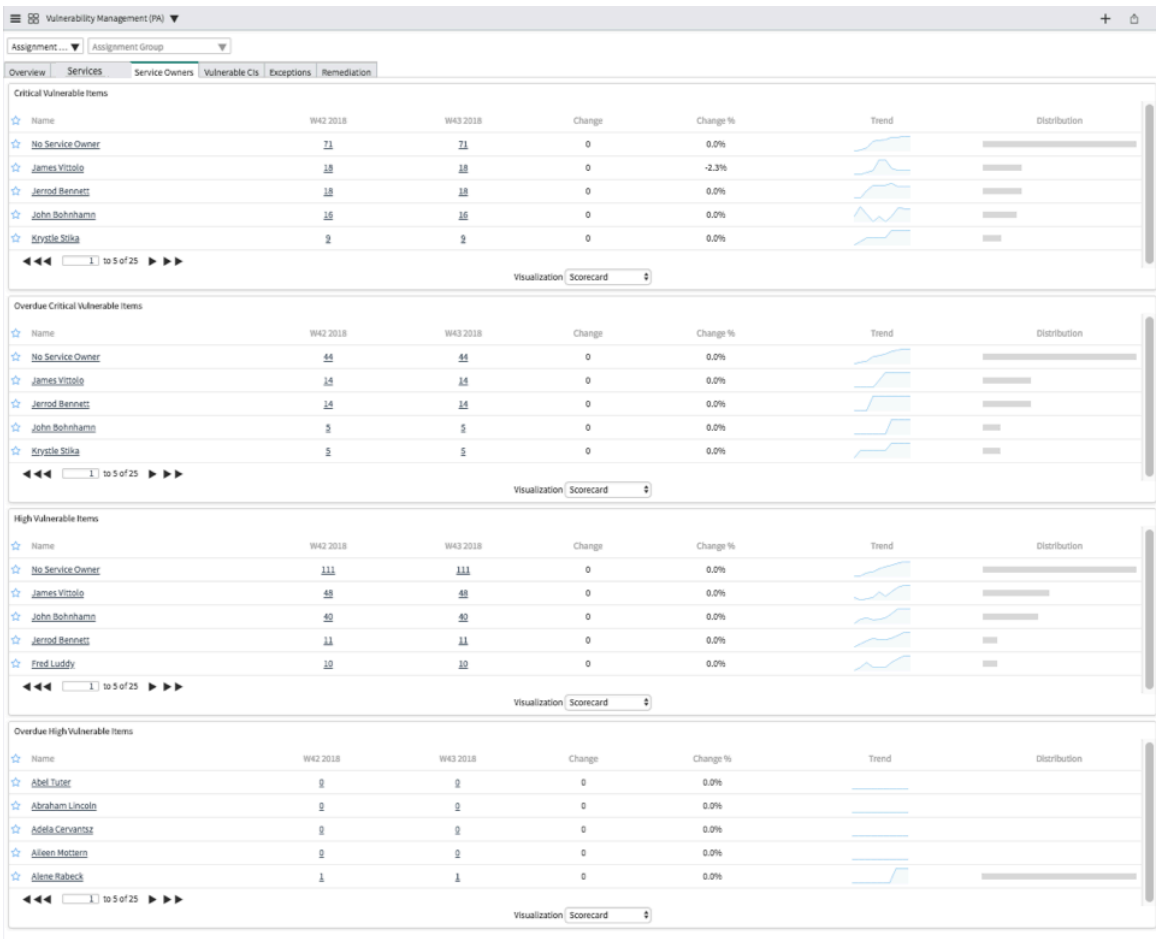


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Propriétaires de service

Ce tableau de bord agrège le risque de vulnérabilité du niveau de service d'entreprise jusqu'aux propriétaires de services, c'est-à-dire les cadres responsables de ces services d'entreprise. Il montre quels dirigeants assument le plus de risques de vulnérabilité et lesquels peuvent nécessiter le plus d'aide, encourageant des activités de rattrapage rapides.



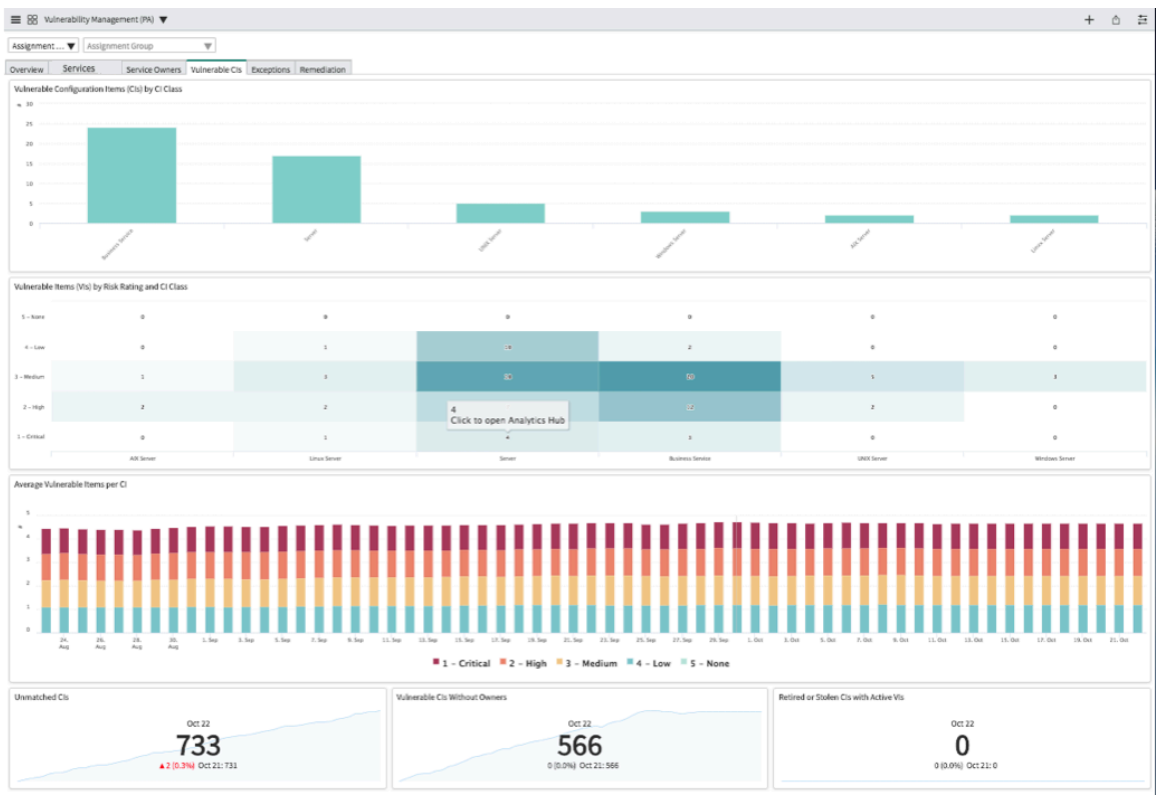
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet CI vulnérables

Ce tableau de bord indique l'étendue et la composition des CI présentant des vulnérabilités actives, ainsi que les catégories de CI nécessitant le plus d'attention. Identifiez les actifs mis hors service avec des éléments vulnérables actifs et confirmez que les actifs ont été mis hors service. Affichez le nombre de CI vulnérables qui n'ont pas d'informations sur la propriété, afin de pouvoir identifier de manière proactive les propriétaires de ces actifs avant qu'une vulnérabilité critique n'affecte ces systèmes.

Dans l'onglet CI vulnérables, vous pouvez afficher les rapports CI vulnérables sans propriétaires et CI hors service ou volés avec VI actifs en temps réel.



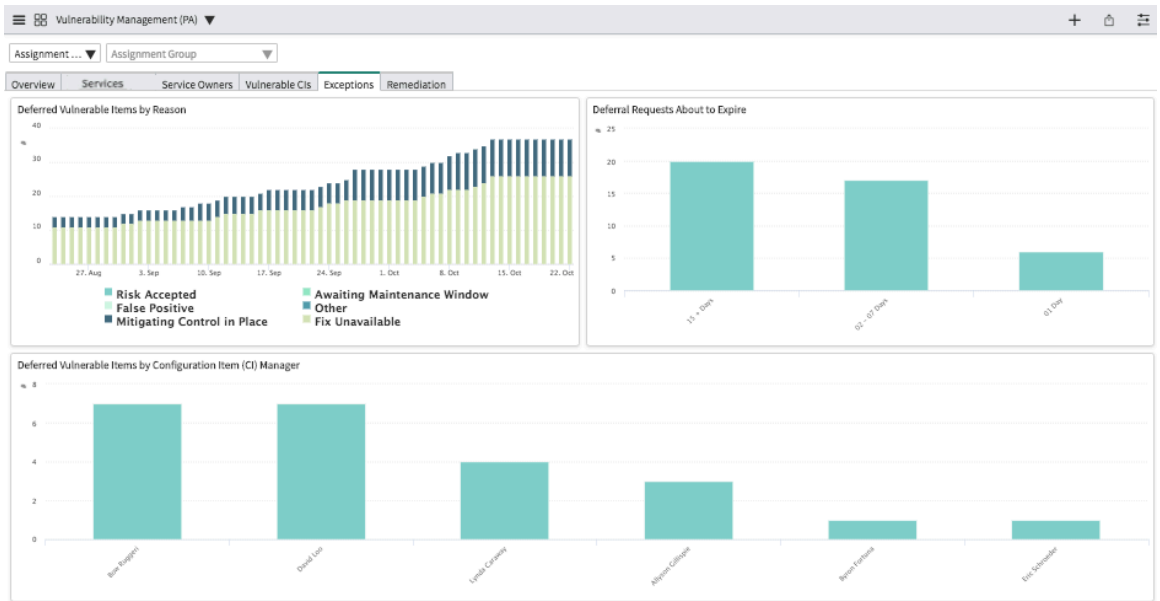
Onglet Exceptions

Ce tableau de bord vous aide à comprendre où votre organisation prend des risques en raison de reports potentiellement excessifs et à réexaminer les options de rattrapage.

Vous pouvez afficher les éléments vulnérables différés par motif, les demandes de report arrivant à expiration, les exceptions pour les éléments vulnérables critiques par groupe d'affectation et les demandes d'exception par rapport du demandeur.

Traduction automatique

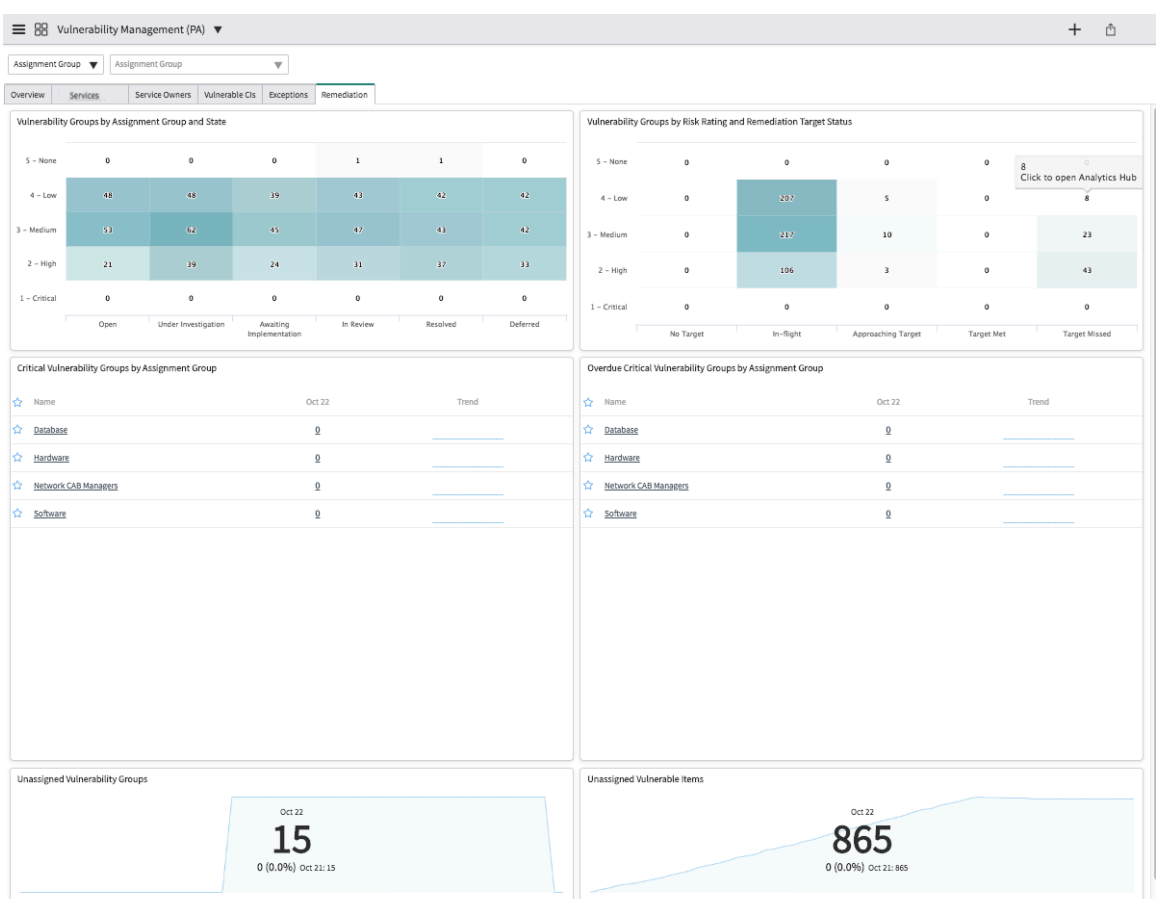
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Onglet Rattrapage

Ce tableau de bord vous aide à comprendre la progression de vos actions de rattrapage et à identifier les équipes d'assistance qui ont le plus besoin d'aide pour les mener à bien.

Dans l'onglet Correction, vous pouvez afficher le rapport sur les éléments vulnérables non affectés en temps réel.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateurs

Indicateurs de Vulnerability Response

Un certain nombre d'indicateurs sont utilisés pour mesurer et suivre la progression de votre rattrapage de vulnérabilité dans l'application Réponse aux vulnérabilités .

L'option de collecte des enregistrements pour les indicateurs est désactivée par défaut pour l'application Réponse aux vulnérabilités . Cette option est désactivée afin que certains rapports puissent être consultés en temps réel. Les informations de tendance utilisées par ces indicateurs sont toujours disponibles si vous préférez activer la collecte manuelle des enregistrements et afficher les enregistrements qui composent les scores.

Vulnérabilités distinctes

Vulnérabilités distinctes avec count_active_vi > 0. L'objectif est de minimiser.

Éléments vulnérables critiques en retard non différés

Il s'agit du décompte sur la source de données Élément vulnérable.Actif, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

% d'éléments vulnérables ayant atteint la cible de remédiation

([[Éléments vulnérables fermés > cible de rattrapage = cible atteinte]] / [[Éléments vulnérables fermés]]) * 100. L'objectif est de maximiser.

Éléments vulnérables non affectés

Tous les éléments vulnérables actifs pour lesquels le groupe d'affectation et les champs Affecté à sont vides. L'objectif est de minimiser.

Éléments vulnérables critiques (services)

Il s'agit du décompte sur la source de données VI actifs (services), qui utilise la table : sn_vul_analytics_business_services_vi. L'objectif est de minimiser.

Éléments hautement vulnérables en retard (services)

Il s'agit du décompte sur la source de données VI actifs (services), qui utilise la table : sn_vul_analytics_business_services_vi. L'objectif est de minimiser.

Tâches de remédiation non affectées

Toutes les tâches de rattrapage actives pour lesquelles le groupe d'affectation et les champs Affecté à sont vides. L'objectif est de minimiser.

Éléments vulnérables critiques

Il s'agit du décompte sur la source de données Élément vulnérable.Actif, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables

Il s'agit du décompte sur la source de données Élément vulnérable.Actif, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Nouveaux éléments vulnérables

Il s'agit du décompte sur la source de données VI.Nouveau, qui utilise la table suivante : sn_vul_vulnerable_item. L'objectif est de minimiser.

Éléments de configuration vulnérables

Il s'agit du décompte distinct sur la source de données VI.Actif, qui utilise la table : sn_vul_vulnerable_item. L'objectif est de minimiser.

Durée cumulée des éléments vulnérables fermés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il s’agit de la somme sur la source de données Élément vulnérable.Fermé, qui utilise la table suivante : sn_vul_vulnerable_item. L’objectif est de minimiser.

Tâches de remédiation non différées

Il s’agit du décompte sur la source de données VG. Actif, qui utilise la table suivante : sn_vul_vulnerability. L’objectif est de minimiser.

Délai moyen de remédiation de l'élément vulnérable

[[Durée cumulée des éléments vulnérables fermés]] / [[Éléments vulnérables fermés]]

Éléments vulnérables critiques en retard (services)

Il s’agit du décompte sur la source de données VI actifs (services), qui utilise la table : sn_vul_analytics_business_services_vi. L’objectif est de minimiser.

Éléments de configuration mis hors service

Il s’agit du décompte distinct sur la source de données VI.Actif, qui utilise la table : sn_vul_vulnerable_item. L’objectif est de minimiser.

Demandes de report

Il s’agit du décompte sur la source de données Demandes de report actif, qui utilise la table : sn_vul_change_approval. L’objectif est de minimiser.

Éléments vulnérables par éléments de configuration

Il s’agit du décompte sur les CI de source de données avec des VI actifs, qui utilise la table : sn_vul_analytics_vi_ci_class. L’objectif est de minimiser.

Éléments vulnérables clôturés

La valeur Éléments vulnérables fermés est mesurée quotidiennement en unité #. L’objectif est de maximiser.

Éléments de configuration sans correspondance

Répertorie les hôtes découverts par les analyseurs de vulnérabilité tiers qui ne correspondent à aucun CI existant dans la CMDB.

Tâches de remédiation critiques en retard non différées

Il s’agit du décompte sur la source de données VG. Actif, qui utilise la table suivante : sn_vul_vulnerability. L’objectif est de minimiser.

Éléments de configuration vulnérables sans groupe de support

Il s’agit du décompte sur la source de données VI.Open qui utilise la table : sn_vul_vulnerable_item. L’objectif est de minimiser.

Tâches de remédiation critiques non différées

Il s’agit du décompte sur la source de données VG. Actif, qui utilise la table suivante : sn_vul_vulnerability. L’objectif est de minimiser.

Éléments vulnérables différés

Il s’agit du décompte sur la source de données Élément vulnérable.Actif, qui utilise la table suivante : sn_vul_vulnerable_item. L’objectif est de minimiser.

Éléments hautement vulnérables (services)

Il s’agit du décompte sur la source de données VI actifs (services), qui utilise la table : sn_vul_analytics_business_services_vi. L’objectif est de minimiser.

Éléments de configuration distincts avec des éléments vulnérables actifs

Il s’agit du décompte distinct sur les CI de source de données avec des VI actifs, qui utilise la table : sn_vul_analytics_vi_ci_class. L’objectif est de minimiser.

Nombre moyen d'éléments vulnérables par élément de configuration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

[[Éléments vulnérables actifs]] / [[CI vulnérables]]. L’objectif est de minimiser.

Tâches de remédiation

Il s’agit du décompte sur la source de données VG. Actif, qui utilise la table suivante : sn_vul_vulnerability. L’objectif est de minimiser.

Éléments vulnérables différés critiques

Il s’agit du décompte sur la source de données Élément vulnérable.Actif, qui utilise la table suivante : sn_vul_vulnerable_item. L’objectif est de minimiser.

Demandes de report (créées)

Il s’agit du décompte sur la source de données Demandes.Fermées, qui utilise la table suivante : sn_vul_change_approval. L’objectif est de minimiser.

Répartitions

Les noms de répartition suivants s’appliquent aux indicateurs sur le tableau de bord :

- Âge
- Âge clôturé
- Groupe d'affectation
- Classe CI
- Gestionnaire CI
- Âge du report
- Motif du report
- Demandeurs d'exceptions
- Vecteur d'attaque de l'exploit
- Un exploit existe
- Niveau de compétence de l'exploit
- Règle de cible de rattrapage
- État de la cible de la remédiation
- État de la cible de rattrapage (fermé)
- Cotes de risque
- Service
- Criticité du service
- Propriétaire de service
- Gravité
- État

Remarque : La personnalisation du calcul de l’âge et de l’âge fermé pour les éléments vulnérables (VI) peut entraîner une forte hausse ou une baisse des rapports d’Analyse des performances (PA) qui incluent ces mesures. Pour plus d’informations sur la personnalisation du calcul de l’âge et de l’âge fermé pour les VI, consultez l’article de la base de connaissances KB1703270 .

Source de répartition

- Groupe d’affectation : s’applique aux rapports VI ou et RT
- Un exploit existe : s’applique aux rapports des VI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vecteur d’attaque de l’exploit : s’applique aux rapports de VI.
- Niveau de compétence de l’exploit : s’applique aux rapports de VI.
- État de la cible de rattrapage : s’applique aux rapports de VI et de RT.
- Cote de risque : s’applique aux rapports VI et RT.
- État : S’applique aux rapports VI et RT.

Visualisations des données

Titre	Type	Description
Vulnérabilités	Score unique	Nombre de vulnérabilités associées à un ou plusieurs éléments vulnérables actifs.
Éléments vulnérables (VI)	Score unique	Nombre d'éléments vulnérables actifs (non fermés).
Éléments de configuration (CI) vulnérables	Score unique	Nombre d’éléments de configuration (CI) associés à un ou plusieurs éléments vulnérables actifs.
Tâches de remédiation	Score unique	Nombre de tâches de rattrapage actives (non fermées).
Éléments vulnérables par cote de risque	Barre	Nombre d'éléments vulnérables actifs regroupés par cote de risque au cours de la période sélectionnée.
Éléments vulnérables par âge et cote de risque	Carte thermique	Nombre d’éléments vulnérables actifs regroupés par cote de risque et par âge (en jours).
Cible de rattrapage de VI atteinte	Score unique	Pourcentage d’éléments vulnérables fermés qui ont atteint leur date cible de rattrapage au cours des trimestres actuels et précédents. Les cibles de rattrapage sont calculées à partir de la dernière date d’ouverture additionnée au nombre de jours (mesurés par incréments de 24 heures).
Délai moyen de rattrapage (MTTR) des VI	Score unique	Le délai moyen de rattrapage (fermeture) d'un élément vulnérable, affiché comme moyenne d'exécution de 30 jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre	Type	Description
		Remarque : La valeur Âge à la fermeture est calculée lors de la collecte des données. La valeur est la différence entre la date de last_opened et la date et l'heure de la tâche de collecte.
Tâches de remédiation critiques proches de l'échéance	Score unique	Nombre de tâches de rattrapage actives approchant de leur date cible de rattrapage. La date cible de rattrapage d'une tâche de rattrapage est fixée à la date d'échéance la plus proche appartenant à un élément vulnérable actif dans le groupe. Les cibles de rattrapage sont calculées à partir de la dernière date d'ouverture additionnée au nombre de jours (mesurés par incréments de 24 heures). Ce rapport exclut les tâches de rattrapage différées.
Éléments vulnérables nouveaux et fermés	Barre	Nombre d'éléments vulnérables nouveaux et fermés sur la période sélectionnée. **Remarque :** La valeur Âge à la fermeture est calculée lors de la collecte des données. La valeur est la différence entre la date de last_opened et la date et l'heure de la tâche de collecte.
Éléments vulnérables fermés par état de la cible de rattrapage	Barre	Nombre d'éléments vulnérables fermés regroupés par état de la cible de rattrapage au cours de la période sélectionnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre	Type	Description
		Remarque : La valeur Âge à la fermeture est calculée lors de la collecte des données. La valeur est la différence entre la date de last_opened et la date et l'heure de la tâche de collecte.
Éléments vulnérables critiques par groupe d'affectation	Liste et ligne 	Nombre d'éléments vulnérables actifs avec une cote de risque critique, regroupés par groupe d'affectation.
Éléments vulnérables critiques en retard par groupe d'affectation	Liste et ligne 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par groupe d'affectation. Les cibles de rattrapage sont calculées à partir de la dernière date d'ouverture additionnée au nombre de jours (mesurés par incréments de 24 heures). Ce rapport exclut les éléments vulnérables différés.

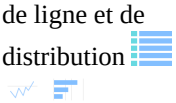
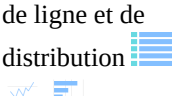
Services d'entreprise

Nom	Type	Description
Éléments vulnérables critiques	Barre de liste, de ligne et de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique, regroupés par service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats.
Éléments vulnérables critiques en retard	Barre de liste, de ligne et de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par service d'entreprise.

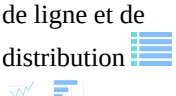
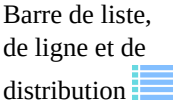
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Services d'entreprise (suite)

Nom	Type	Description
		Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats. Ce rapport exclut les éléments vulnérables différés.
Éléments hautement vulnérables	Barre de liste, de ligne et de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée, regroupés par service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats.
Éléments hautement vulnérables en retard	Barre de liste, de ligne et de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée et dépassant les dates cibles de rattrapage, regroupés par service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats. Ce rapport exclut les éléments vulnérables différés.

Propriétaires de service

Nom	Type	Description
Éléments vulnérables critiques	Barre de liste, de ligne et de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique, regroupés par propriétaire de service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats.
Éléments vulnérables critiques en retard	Barre de liste, de ligne et de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par propriétaire de service d'entreprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétaires de service (suite)

Nom	Type	Description
		Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats. Ce rapport exclut les éléments vulnérables différés.
Éléments hautement vulnérables	Barre de liste, de ligne et de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée, regroupés par propriétaire de service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats.
Éléments hautement vulnérables en retard	Barre de liste, de ligne et de distribution 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée et dépassant les dates cibles de rattrapage, regroupés par propriétaire de service d'entreprise. Affiche une moyenne hebdomadaire de la semaine en cours et de la semaine précédente, la différence entre ces deux semaines (en nombre et en pourcentage) et une tendance. La barre de distribution affiche la différence entre toutes les valeurs sur la page actuelle du tableau de résultats. Ce rapport exclut les éléments vulnérables différés.

CI vulnérables

Nom	Type	Description
Éléments de configuration (CI) vulnérables par classe CI	Barre 	Nombre d'éléments de configuration présentant des vulnérabilités actives, regroupés par classe CI dans la CMDB.
Éléments vulnérables (VI) par classe CI		Nombre de VI actifs répartis par classe CI.
Nombre moyen d'éléments vulnérables par CI	Barre 	Nombre moyen d'éléments vulnérables appartenant à un élément de configuration, regroupés par cote de risque.
Ci sans correspondance	Score unique 	Nombre d'éléments de configuration importés qui ne correspondent à aucun CI existant dans la CMDB.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

CI vulnérables (suite)

Nom	Type	Description
CI vulnérables sans groupe de support	Score unique	Nombre d'éléments de configuration vulnérables auxquels aucun groupe de support n'a été affecté.
CI mis hors service ou volés avec des VI actifs	Score unique	Nombre d'éléments de configuration marqués comme **Mis hors service** ou **Volés** dans la CMDB qui ont des éléments vulnérables actifs.

Exceptions

Nom	Type	Description
Éléments vulnérables différés par motif	Barre	Nombre d'éléments vulnérables reportés regroupés par motif de report.
Demandes de report sur le point d'expirer	Barre	Nombre de demandes de report associées à des tâches de rattrapage ou à des éléments vulnérables sur le point d'être rouverts pour examen. Elles sont regroupées par nombre de jours restants jusqu'à leur réouverture. Si les notifications par e-mail sont définies, un e-mail est envoyé.
Éléments vulnérables différés par gestionnaire d'éléments de configuration (CI)	Barre	Nombre d'éléments vulnérables différés regroupés par le gestionnaire pour l'élément de configuration associé.

Rattrapage

Nom	Type	Description
Tâches de remédiation par cote de risque et par état	Carte thermique	Nombre de tâches de rattrapage actives regroupées par cote de risque et état.
Tâches de remédiation par cote de risque et par état de la cible de remédiation	Carte thermique	Nombre de tâches actives regroupées par cote de risque et par état de la cible de rattrapage. Ce rapport exclut les éléments vulnérables différés.
Tâches de remédiation critiques par groupe d'affectation	Liste et ligne	Nombre de tâches de rattrapage actives avec une cote de risque critique, regroupées par groupe d'affectation. Ce rapport exclut les tâches de rattrapage différées.
Tâches de remédiation critiques en retard par groupe d'affectation	Liste et ligne	Nombre de tâches de rattrapage actives ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupées par groupe d'affectation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rattrapage (suite)

Nom	Type	Description
		Ce rapport exclut les tâches de rattrapage différées.
Tâches de remédiation non affectées	Score unique	Nombre de tâches de rattrapage actives sans délégataire ou groupe d'affectation.
Éléments vulnérables non affectés	Score unique	Nombre d'éléments vulnérables actifs sans délégataire ou groupe d'affectation.

Afficher les Analyse des performances pour Réponse aux vulnérabilités rapports [PA] en temps réel

Pour gérer vos éléments vulnérables (VI) les plus importants et vous aider à les corriger rapidement, affichez les rapports à la demande, en temps réel sur le tableau de bord Gestion de la vulnérabilité (PA). L'application Analyse des performances pour Réponse aux vulnérabilités est disponible avec un abonnement distinct du ServiceNow Store.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pour en savoir plus sur les rapports de Analyse des performances pour Réponse aux vulnérabilités, reportez-vous au tableau de bord Gestion de la vulnérabilité [PA].

Pour plus d'informations sur la configuration et l'installation de l'application Analyse des performances pour Réponse aux vulnérabilités , reportez-vous à la section Installer et configurer l'application Analyse des performances pour Réponse aux vulnérabilités [PA].

S'il n'est pas affiché, pour afficher le tableau de bord, accédez à **Réponse aux vulnérabilités** > **Vue d'ensemble**. En haut du tableau de bord, les onglets de rapport sont affichés.

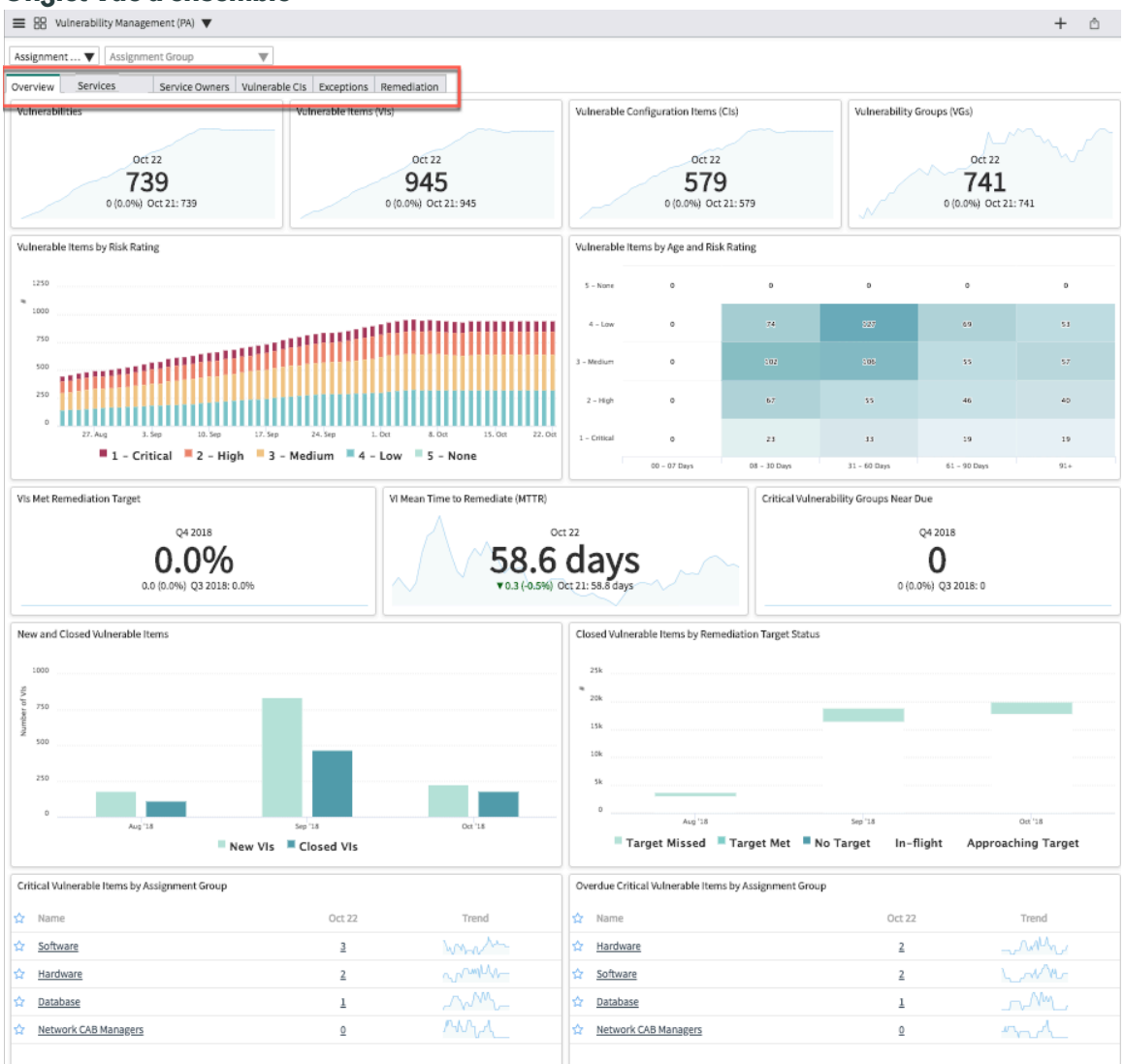
À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord peut également être affiché dans la nouvelle interface utilisateur. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Tableaux de bord dans l'espace de travail du gestionnaire de vulnérabilité et Tableaux de bord dans l'espace de travail Rattrapage informatique.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble



Affichez les rapports suivants sur les onglets du tableau de bord Gestion de la vulnérabilité (PA) en temps réel.

- Onglet Vue d'ensemble
  - Éléments vulnérables critiques par groupe d'affectation
- Onglet CI vulnérables :
  - CI vulnérables sans propriétaires
  - CI mis hors service ou volés avec des VI actifs
- Onglet Exceptions :
  - Éléments vulnérables différés par motif
  - Demandes de report sur le point d'expirer
  - Éléments vulnérables différés par gestionnaire DSI
- Onglet Rattrapage :
  - Éléments vulnérables non affectés

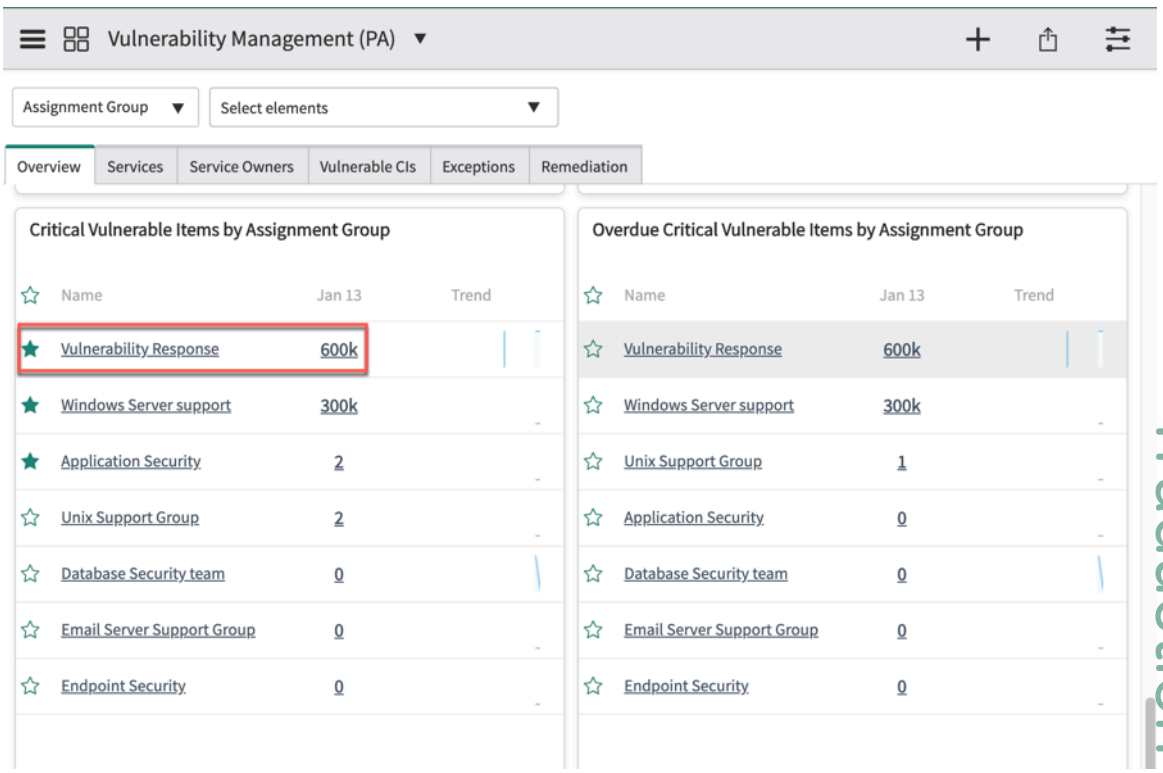
Pour afficher les scores en temps réel, avec l'un des onglets sélectionnés qui contient des rapports en temps réel, procédez comme suit :

Traduction automatique

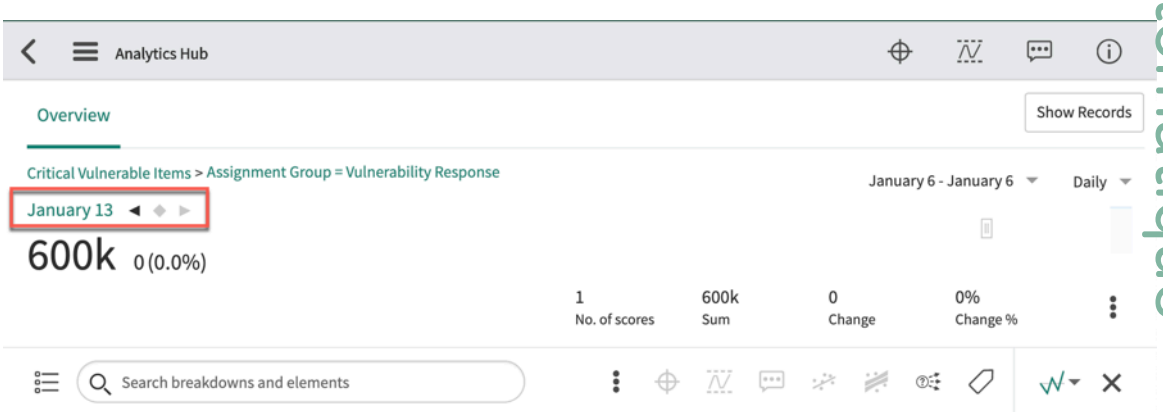
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans le rapport, par exemple, Éléments vulnérables critiques par groupe d'affectation, cliquez sur l'un des liens affichés.



2. Dans l'enregistrement qui s'affiche, cliquez sur la date.

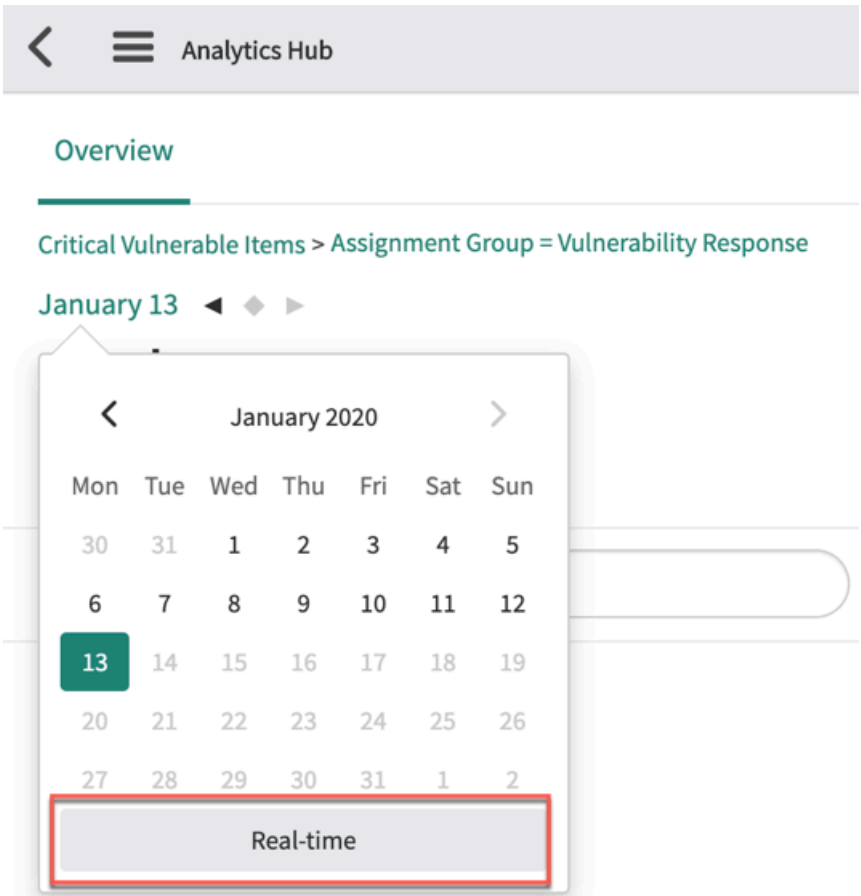


3. Dans le calendrier qui s'affiche, cliquez sur Temps réel.

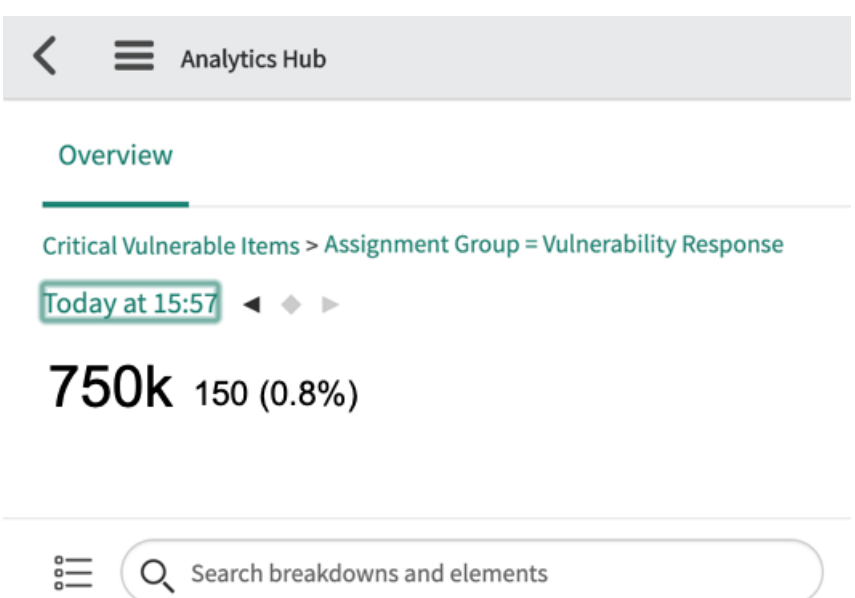
   Si un rapport ne prend pas en charge un score en temps réel, le bouton Temps réel ne s'affiche pas sur la planification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La mise à jour de la valeur peut prendre quelques instants. La date actuelle, les enregistrements, le nombre de nouveaux enregistrements depuis le dernier rapport et le changement en pourcentage par rapport au dernier rapport sont également affichés.



4. **Facultatif :** Pour afficher les enregistrements qui composent le rapport, avec le rapport en temps réel affiché, cliquez sur **Afficher les enregistrements** en haut à droite.
   La liste des enregistrements qui composent la partition s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les Analyse des performances indicateurs pour Réponse aux vulnérabilités [PA]

Affichez des indicateurs automatisés et formulés Analyse des performances représentant les données de vulnérabilité dans votre instance.

Avant de commencer

L'option Collecter les enregistrements pour les indicateurs est inactive par défaut pour l'application Analyse des performances - Pack de contenu Réponse aux vulnérabilités. Cette option est désactivée afin que certains rapports puissent être consultés en temps réel. Les informations de tendance utilisées par ces indicateurs sont toujours disponibles si vous préférez activer la collecte manuelle des enregistrements et afficher les enregistrements qui composent les scores.

Remarque : L'activation de la collecte des enregistrements dans un indicateur peut avoir un impact sur vos performances et allonger considérablement le temps et la mémoire requis pour exécuter le travail de collecte de données.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé) ou pa.viewer

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités comporte à la fois des indicateurs automatisés et des indicateurs formulés.

Termes clés

Indicateur PA

Définit une mesure de performance effectuée à intervalles réguliers d'un service d'entreprise, d'une activité ou d'un comportement organisationnel, par exemple, Éléments vulnérables critiques en retard non différés.

Source de l'indicateur PA

Ensembles de données qui filtrent les enregistrements d'une vue de table ou de base de données, par exemple, VI actif.

Collecter les enregistrements

Lorsqu'elle est activée, elle stocke les enregistrements en mémoire et permet d'accéder au centre d'analyse.

Répartitions

Les répartitions filtrent et regroupent les enregistrements collectés. Les pannes peuvent augmenter l'utilisation de la mémoire, d'autant plus que leur nombre et leur diversité augmentent.

Exclusions de répartition

Les exclusions suppriment certaines répartitions, ce qui peut réduire la consommation de mémoire.

Procédure

1. Pour les indicateurs automatisés, naviguez vers **Analyse des performances** > **Indicateurs** > **Indicateurs automatisés**.
2. Pour les indicateurs formulés, accédez à **Analyse des performances** > **Indicateurs de formule**.

Pour plus d'informations sur les indicateurs, voir Indicateurs d'Analyse des performances .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

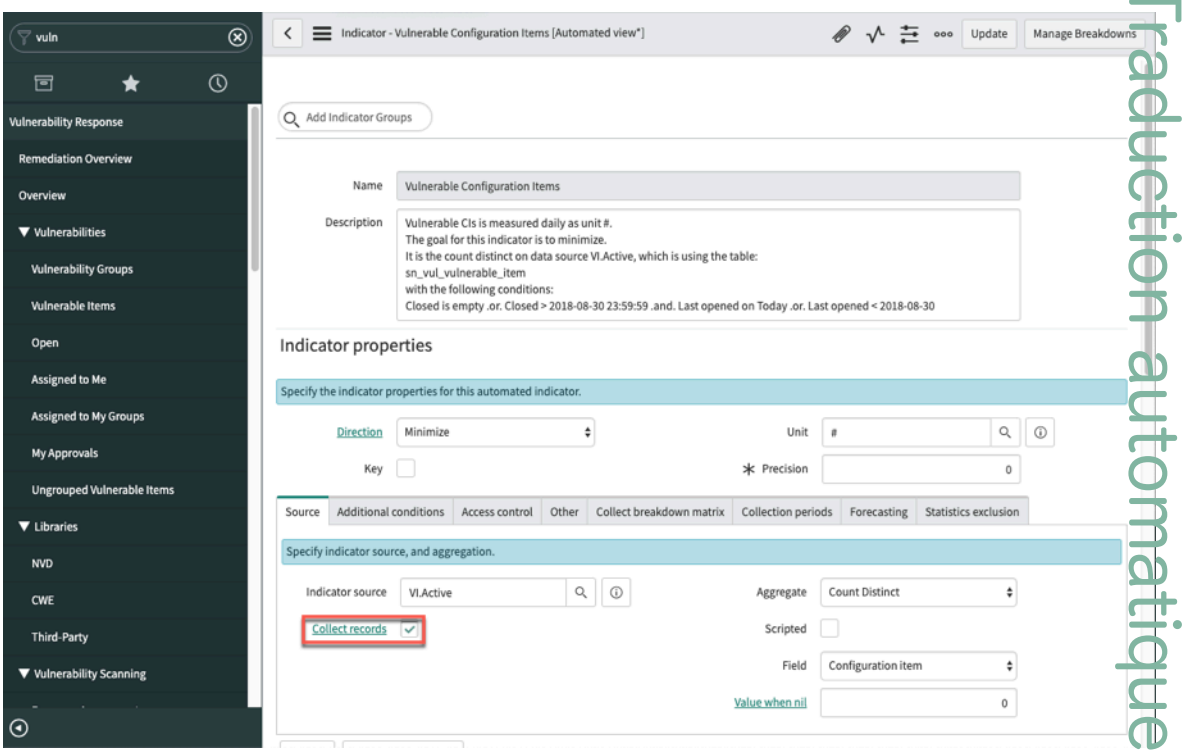
3. Dans les deux cas, recherchez sur **Application** > **Analyse des performances**.

   Remarque : Si elle n'est pas dans votre vue par défaut, ajoutez la colonne **Application** à l'aide de l'icône d'engrenage (icône) dans le coin supérieur gauche de la page. La colonne Application s'affiche alors dans votre menu déroulant Rechercher.

4. **Facultatif :** Pour activer l'option Collecter les enregistrements sur un indicateur Analyse des performances pour Réponse aux vulnérabilités , procédez comme suit :

   a. Une fois la liste des indicateurs automatisés affichée, dans la colonne Nom, cliquez sur l'indicateur pour lequel vous souhaitez activer la collecte des enregistrements.
   L'enregistrement de l'indicateur s'affiche.

   b. Dans la section Propriétés de l'indicateur avec l'onglet Source sélectionné, cochez la case Collecter les enregistrements.



Traduction automatique

   c. Choisissez-en un pour continuer.

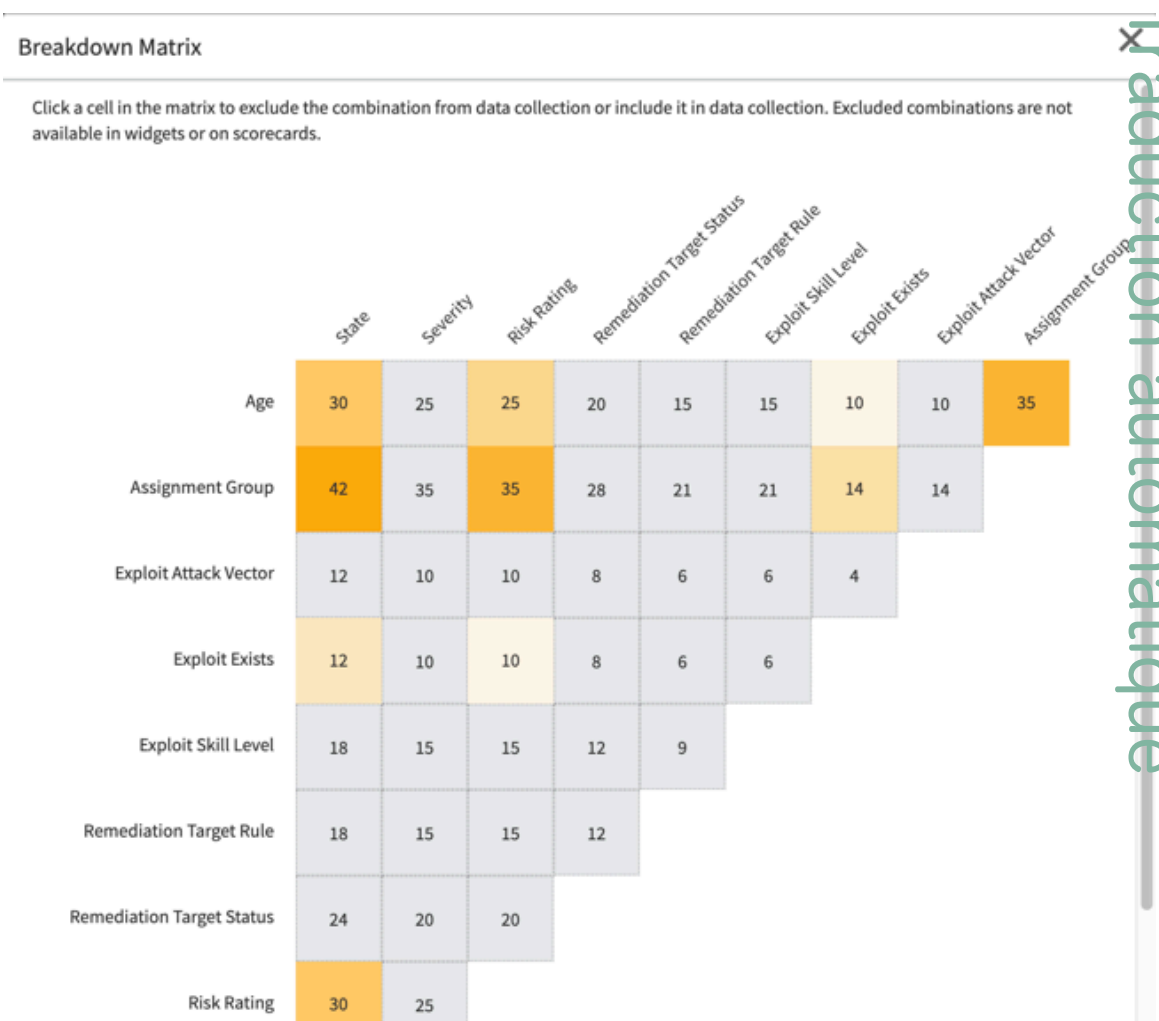
Option	Description
Mettre à jour	Enregistrez vos modifications et revenez à la liste des indicateurs.
Gérer les répartitions **Remarque :** Si vous choisissez de réactiver les répartitions de deuxième niveau, vous risquez d'augmenter considérablement votre consommation de mémoire et de ralentir le travail de collecte de données.	Réactiver les répartitions de second niveau pour les indicateurs répertoriés ou modifier les répartitions pour d'autres indicateurs. (Optional) Pour plus d'informations sur les répartitions d'Analyse des performances, voir Répartitions d'Analyse des performances .

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Par défaut, les exclusions de répartition de second niveau ont été appliquées aux indicateurs suivants : ▪ Éléments de configuration vulnérables ▪ CI mis hors service ▪ VI différés	

d. Cliquez sur **Gérer les répartitions**.

e. Dans le formulaire qui s'affiche, cliquez sur **Configurer la matrice de répartition**.
Le formulaire Matrice de répartition s'affiche. Les combinaisons exclues sont sélectionnées et affichées avec des couleurs, comme le montre la figure suivante.



f. Pour supprimer l'exclusion et réactiver une combinaison exclue, cliquez sur une cellule sélectionnée.

g. Dans l'angle supérieur droit du formulaire, cliquez sur **Fermer** pour renvoyer le formulaire Gérer la répartition.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

h. Cliquez sur la flèche de retour pour revenir à l'enregistrement de l'indicateur.

i. Cliquez sur **Mettre à jour** pour enregistrer vos modifications et revenir à la liste des indicateurs.

Cadre de travail des rapports agrégés

À l'aide de l'infrastructure des rapports agrégés, vous pouvez créer des rapports pour les données qui impliquent des requêtes à la volée complexes et de longue durée afin d'améliorer les performances.

Le cadre de travail des rapports agrégés améliore les performances en :

- en utilisant moins de ressources et en rendant les rapports plus rapidement,
- l'agrégation des données et la réutilisation des agrégations et des répartitions (Grouper par) et
- réduire les requêtes à la base de données

Lorsque vous disposez de plus d'un million d'éléments vulnérables, utilisez le cadre de travail des rapports agrégés fourni dans Réponse aux vulnérabilités commune en même temps que les rapports standard.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur ServiceNow AI Platform (admin) : installer et activer cette Solution d'analyse des performances et génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Analyse des performances Administrateur (pa_admin) : Examinez les agrégations, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.
- Administrateur (sn_vul_cmn.admin) : créer des agrégations.
- VR write(sn_vul_cmn.write) : modifiez les données dans les agrégations et les résultats agrégés.
- VR read (sn_vul_cmn.read) : passez en revue les données dans les agrégations et les résultats agrégés.
- Analyste de vulnérabilité (sn_vul.vulnerability_analyst) : examinez les résultats agrégés.

Information associée

Configurer une agrégation pour les données sources

Exécuter plusieurs agrégations simultanément

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Créer un rapport à l'aide d'une agrégation

Configurer une agrégation pour les données sources

Pour analyser les performances d'une facette spécifique dans un processus business enregistrée dans une ServiceNow table, créez une agrégation spécifique à la facette et créez un rapport pour cette agrégation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul_cmn.admin

Procédure

1. Accédez à la **Tous** > **Rapports agrégés** > **Définitions d'agrégations** > **Tous** et cliquez sur **Nouveau**.
2. Dans le champ **Nom** , donnez un nom descriptif à l'agrégation.
3. Dans le champ **Description** , fournissez une brève description de l'agrégation.
4. Dans l'onglet **Source** , renseignez les champs.

Champs de l'onglet source

Champ	Description
Table	Table à partir de laquelle vous souhaitez extraire les données du rapport. Cette liste déroulante contient uniquement des tables communes App Sec, app-vul, app-vulc, app-vul-container et de vulnérabilité de l'application.
Fonction d'agrégat	Fonction à appliquer à la colonne sélectionnée dans **Champ**. ○ **Nombre** : nombre d'enregistrements. ○ **Somme** : somme totale des valeurs de la colonne sélectionnée dans **Champ**. ○ **Moyenne** : moyenne de toutes les valeurs d'une colonne sélectionnée dans **le champ**. ○ **Maximum** : valeur maximale dans la colonne sélectionnée dans **Champ**. ○ **Minimum** : valeur minimale de la colonne sélectionnée dans le **champ**. ○ **Compte distinct** : valeurs uniques dans la colonne sélectionnée dans le **champ**.
Champ	Colonne à laquelle vous souhaitez appliquer la fonction. **Remarque :** Ce champ n'apparaît pas lorsque vous sélectionnez **Nombre** dans le champ **Fonction d'agrégation** .

5. Dans l'onglet **Conditions supplémentaires** , fournissez la condition dans le champ **Conditions** pour sélectionner un ensemble particulier d'enregistrements pour lequel vous souhaitez obtenir les résultats agrégés.
6. Dans l'onglet **Grouper par** , sélectionnez les colonnes de la table selon lesquelles vous souhaitez regrouper ou empiler les données.
   Vous pouvez sélectionner jusqu'à deux répartitions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous sélectionnez la colonne **de date** dans n'importe quel champ Grouper par, le champ **Tendance par** s'affiche. Vous pouvez obtenir les résultats d'agrégation classés par semaine, jour, minutes, etc. en sélectionnant les options dans le champ **Tendance par** .

7. Dans l'onglet **Calendrier** , sélectionnez ou créez un calendrier d'agrégation, qui définit la fréquence à laquelle vous pouvez exécuter l'agrégation pour extraire les données.
   Pour créer un calendrier d'agrégation, reportez-vous à la section Exécuter plusieurs agrégations simultanément.

   Remarque : Vous ne pouvez pas planifier l'exécution de l'agrégation pour une définition d'agrégation inactive.

8. Cliquez sur **Soumettre** pour créer l'agrégation.
   L'agrégation apparaît dans la liste d'agrégation. À la fréquence prédéfinie, l'agrégation est exécutée et un enregistrement est créé avec une date et une heure d'exécution dans la liste connexe Exécutions planifiées pour chaque exécution.
9. Accédez à la **Tous** > **Résultats agrégés** et ouvrez votre agrégation pour afficher les résultats agrégés et les exécutions planifiées.
   Les résultats agrégés sont répertoriés dans la liste connexe **Résultats agrégés** . Si l'exécution de l'agrégation échoue, consultez la colonne **Notes** de la liste connexe **Exécutions planifiées** pour plus d'informations.
10. **Facultatif :** Sélectionnez **Exécuter maintenant** pour collecter les résultats de l'agrégation, quelle que soit la planification d'agrégation.
    Si vous mettez fin à l'exécution planifiée alors qu'elle est en cours, aucun changement n'est apporté aux résultats agrégés. Vous pouvez également supprimer ou désactiver une agrégation.

Que faire ensuite

Créez un rapport à l'aide de votre agrégation. Pour plus d'informations sur la création d'un rapport à l'aide d'une agrégation, reportez-vous à la section Créer un rapport à l'aide d'une agrégation.

Information associée

- Cadre de travail des rapports agrégés
- Exécuter plusieurs agrégations simultanément
- Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément
- Créer un rapport à l'aide d'une agrégation

Exécuter plusieurs agrégations simultanément

Vous pouvez planifier l'exécution de plusieurs agrégations à l'aide d'un seul calendrier d'agrégation.

Avant de commencer

Rôle requis : sn_vul_cmn.admin

Pourquoi et quand exécuter cette tâche

Supposons que vous souhaitiez exécuter six agrégations en même temps. Créez un calendrier d'agrégation et ajoutez-y toutes les agrégations. Ces agrégations sont exécutées à la fréquence et à l'heure définies.

Procédure

1. Accédez à la **Tous** > **Rapports agrégés** > **Planifier**.
2. Sélectionnez **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Renseignez les champs du formulaire Calendrier d'agrégation.

Champ	Description
Nom de calendrier	Nom du calendrier d'agrégation.
Travail de planification	Exécution de script planifiée qui définit la fréquence à laquelle les agrégations doivent s'exécuter. Vous pouvez créer une tâche planifiée en sélectionnant le bouton **Nouveau** .

4. Sélectionnez **Soumettre**.
   Le calendrier d'agrégation apparaît dans la liste Calendrier d'agrégations.
5. Ouvrez votre calendrier d'agrégation.
6. Sélectionnez **Modifier**, ajoutez les agrégations à la **liste d'agrégation**, puis sélectionnez **Enregistrer**.
   Les agrégations sélectionnées apparaissent dans la liste connexe Agrégations.

   Remarque : Si vous ajoutez une agrégation inactive à une planification, l'exécution planifiée ne commencera pas.

7. Sélectionnez **Mettre à jour**.
   Ces agrégations sont exécutées à la fréquence définie dans le calendrier d'agrégation.

Information associée

Cadre de travail des rapports agrégés

Configurer une agrégation pour les données sources

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Créer un rapport à l'aide d'une agrégation

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Un nouveau processeur ou une tâche en arrière-plan, le processeur de l'infrastructure de génération de rapports agrégés est fourni avec le système de base, qui exécute les travaux planifiés associés à la table de l'infrastructure des rapports agrégés. Cela permet à l'ensemble du sous-système de s'exécuter en arrière-plan et une meilleure utilisation des ressources système lorsqu'elles sont disponibles.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Configuration de la tâche en arrière-plan – Calculateur de résultats d'agrégation courante de Vulnerability Response**.
2. Définissez le nombre d'agrégations que vous souhaitez exécuter simultanément dans le **champ Nombre maximal de threads simultanés** et sélectionnez **Enregistrer**.
   Par défaut, quatre agrégations sont exécutées simultanément.
3. Accédez à la liste des pools de processeurs de tâches en arrière-plan, **sn_sec_cmn_background_job_processor_pool.liste**et sélectionnez **Nouveau** pour créer un processeur de tâches en arrière-plan pour le cadre de travail des rapports agrégés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur la création d'un pool de processeurs de tâches en arrière-plan, consultez Traitement parallèle avancé pour les tâches en arrière-plan dans Vulnerability Response .

Remarque : Le nombre de processeurs de tâches en arrière-plan doit être égal au nombre maximal de threads simultanés fourni dans le formulaire Configuration de la **tâche en arrière-plan – Calculateur de résultats d'agrégation commun de Vulnerability Response** . Voir l'étape 2.

Information associée

Cadre de travail des rapports agrégés

Configurer une agrégation pour les données sources

Exécuter plusieurs agrégations simultanément

Créer un rapport à l'aide d'une agrégation

Créer un rapport à l'aide d'une agrégation

Pour visualiser et analyser les données spécifiques à une agrégation que vous avez créée, générez un rapport en fournissant une condition pour l'agrégation dans le générateur de conditions.

Avant de commencer

Rôle requis : pa_admin

Procédure

1. Accédez à la **Tous** > **Rapports** > **Créer**.
2. Renseignez les champs de l'onglet **Données** .

Champs de l'onglet Données

Champ	Description
Nom du rapport	Le nom du rapport.
Type de source	Type de la source à partir de laquelle les données sont extraites. Sélectionnez **Table**.
Table	Nom de la table pour laquelle l'agrégation est créée. Sélectionnez la table des résultats **agrégés Résultat agrégé [sn_vul_cmn_aggregate_result].**

3. Dans le générateur de conditions, définissez la condition de votre agrégation pour laquelle vous souhaitez générer un rapport.

Condition dans le générateur de conditions

Réf.	Description
Champ	Sélectionnez **l'agrégation**.
Opérateur	Sélectionnez **est**.
Valeur	Nom de l'agrégation.

4. Dans l'onglet **Données** , sélectionnez **Suivant**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans l'onglet **Types** , sélectionnez la façon dont vous souhaitez visualiser les données, puis sélectionnez **Suivant**.
   Pour plus d'informations sur les types de rapports, voir Création de rapports .

   Les visualisations prises en charge sont l'histogramme, le graphique à secteurs et la carte thermique. Vous pouvez modifier les graphiques linéaires et d'autres visualisations de tendances pour utiliser les visualisations prises en charge avec le résultat agrégé afin de représenter les mêmes données. La vue de liste n'est pas prise en charge.

6. Renseignez les champs de l'onglet **Configurer** .

Champ	Description
Grouper par	Regroupe les données en fonction du champ sélectionné. Ici, sélectionnez le champ que vous avez choisi dans le champ **Groupé par 1** de l'onglet #unique_505_Connect_42_group-by de l'agrégation.
Empiler par	Organise les données en couches en fonction du champ sélectionné. Ici, sélectionnez le champ que vous avez choisi dans le champ **Groupé par 2** de l'onglet #unique_505_Connect_42_group-by de l'agrégation. **Remarque :** Seuls les rapports à barres et à barres horizontales utilisent des données empilées. Les autres types de rapports autorisent uniquement le regroupement.
Agrégation	Appliquer une fonction **Minimum** ou **Maximum** à **la valeur**.

7. Dans l'onglet **Style** , renseignez les champs comme il convient et sélectionnez **Exécuter**.
   Pour plus d'informations sur les champs des onglets **Configurer** et **Style** , consultez la vidéo Création d'un rapport .
8. Dans le générateur de conditions, définissez la condition de votre agrégation pour laquelle vous souhaitez générer un rapport et sélectionnez **Exécuter**.

   Le rapport s'affiche.
9. Pour trier les valeurs sur l'axe X, sélectionnez **Ajouter un tri**.

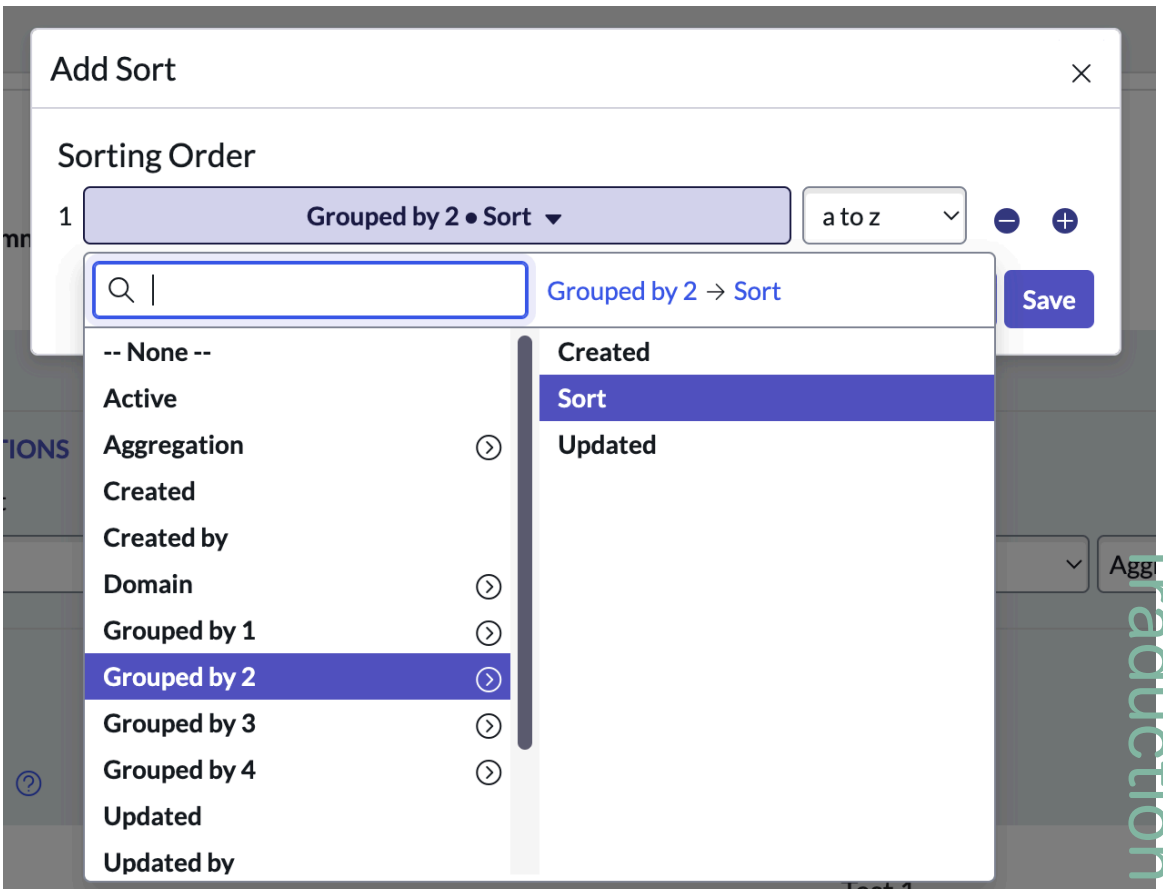
   a. Pour les chaînes, fournissez la condition **Groupé par > a-z ou z-a** pour trier les chaînes dans l'ordre alphabétique.

   b. Pour les valeurs de type nombre entier et date, fournissez la condition **Groupé par.trier > a-z ou z-a** pour trier les valeurs par ordre croissant et décroissant respectivement.

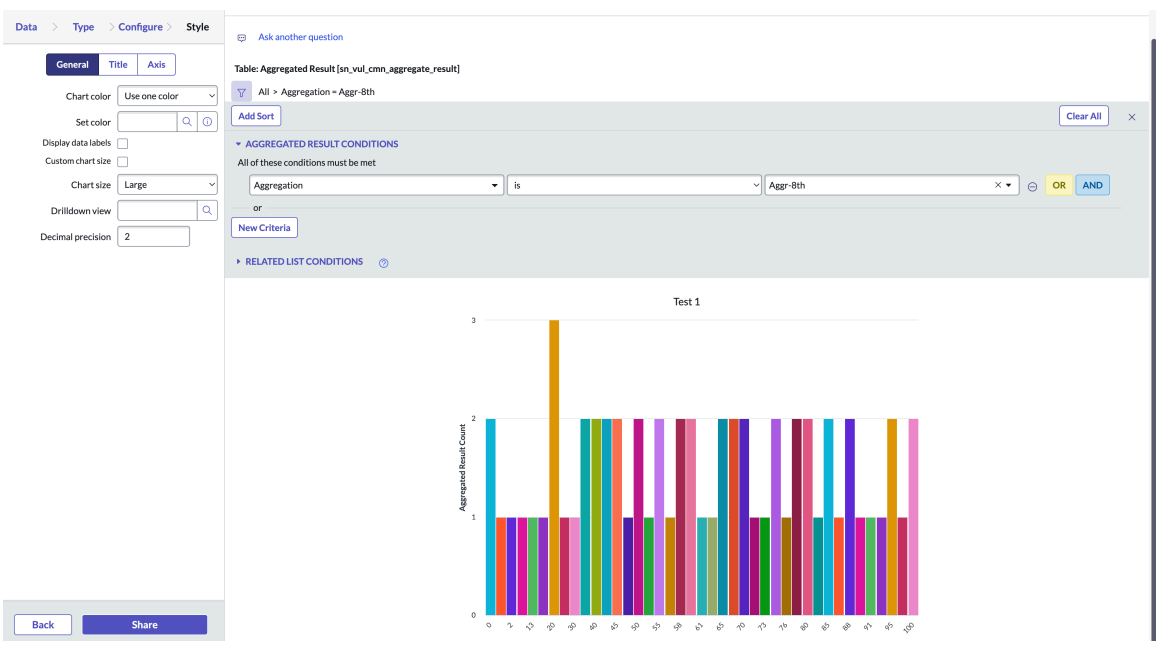
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tri des entiers sur l'axe des X



c. Sélectionnez **Exécuter**.
Les valeurs de nombre entier et de date sont triées sur l'axe des X.



10. Sélectionnez **Enregistrer** pour enregistrer votre rapport.
Le rapport généré pour une agrégation s'affiche dans l'onglet **Résultats** du formulaire **d'agrégation** respectif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. **Facultatif :** Ajouter votre rapport à un tableau de bord.
    Pour plus d'informations sur l'ajout d'un rapport à un tableau de bord, consultez Ajouter un rapport à un tableau de bord réactif .

    Le tableau **de bord Gestion de la vulnérabilité [agrégé],** composé des rapports créés à l'aide de l'infrastructure de génération de rapports mises en cache, est fourni avec le système de base. Pour afficher ce tableau de bord, accédez à **Tous** > **Analyse des performances** > **Tableaux de bord** > **Tous** > **Gestion de la vulnérabilité [agrégé]**. Les agrégations actives correspondant aux rapports de ce tableau de bord sont expédiées avec le système de base.

12. Partagez votre rapport avec d'autres utilisateurs.
    Pour plus d'informations sur le partage de rapports, consultez Distribuer des rapports .

Information associée

Configurer une agrégation pour les données sources

Cadre de travail des rapports agrégés

Exécuter plusieurs agrégations simultanément

Configurer le nombre d'agrégations qui peuvent s'exécuter simultanément

Réponse aux vulnérabilités Informations de référence

Les rubriques suivantes fournissent des liens, des informations de référence, des dépannages et des articles de la base de connaissances, en plus des données de champ sur les formulaires et les enregistrements trouvés dans Réponse aux vulnérabilités.

Vous trouverez ci-dessous des liens vers d'autres ressources qui pourraient vous être utiles, en commençant par un lien vers les liens de la base de connaissances pour l'article Prise en charge et dépannage VR/CC de la base de connaissances HI.

- Liens vers les bases de connaissances pour l'assistance et le dépannage VR/CC
- Pour plus d'informations sur les applications et la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response .
- Vidéos Security Operations
- Formation pour les développeurs
- Documentation pour les développeurs
- Travaillez avec un spécialiste de la mise en œuvre pour atteindre les résultats commerciaux souhaités avec le Customer Success Center .
- Suivez un cours sur la réponse aux vulnérabilités pour développer votre expertise et obtenir un retour sur investissement plus rapide. Pour vous inscrire, consultez Formation et certification ServiceNow .
- Rechercher les composants installés avec une application
- Orchestration de la réponse aux vulnérabilités
- Conseils pour l'écriture d'intégrations
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification d'implémentation pour l'application Réponse aux vulnérabilités

Cette liste de vérification répertorie les étapes nécessaires à une implémentation de base de l'application Réponse aux vulnérabilités sur votre ServiceNow AI Platform® instance. Une fois ces tâches terminées, le système de base est prêt pour l'exploitation et la vérification.

Avant de commencer

Rôles requis : admin pour le téléchargement et l'activation d'applications et l'affectation de rôles, sn_vul.vulnerability_admin pour la configuration Réponse aux vulnérabilités.

Procédure

1. Envisagez de créer et d'imprimer un PDF de cette liste de contrôle afin de pouvoir cocher les tâches au fur et à mesure que vous les terminez.
2. Pour générer un PDF, cliquez sur l'icône **Enregistrer au format PDF** (icône) en haut de la rubrique, puis cliquez sur Rubrique sélectionnée.

Réponse aux vulnérabilités Tâches de liste de vérification d'implémentation de base pour l'administrateur

Élément	Description
☐	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que vous disposez des autorisations et que vous avez téléchargé (**installé**) les applications suivantes à partir de sur ServiceNow® Store votre ServiceNow AI Platform instance : ○ Réponse aux vulnérabilités ○ Réponse aux vulnérabilités Intégration à la base de données de vulnérabilité nationale NIST ○ Qualys Intégration pour Security Operations **a.** Pour vérifier que les applications sont disponibles sur votre instance, accédez à **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous** et recherchez [sn_vul], [sn_vul_nvd] et [sn_vul_qualys]. **b.** Si vous ne parvenez pas à localiser les applications, consultez la rubrique Opérations de sécurité et le ServiceNow Store pour plus d'informations sur l'obtention d'une autorisation et le téléchargement des applications.
☐	En tant qu'utilisateur disposant du rôle administrateur, naviguez dans **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation d'application d'intégration** et activez (**installez**) l'application Réponse aux vulnérabilités ainsi que ses dépendances sur votre ServiceNow AI Platform instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	Remarque : Lors de l'installation de l'application Réponse aux vulnérabilités , vous pouvez installer des données de démonstration. Les données de démonstration sont requises si vous souhaitez exécuter des tests automatisés pour confirmer que votre instance fonctionne après l'installation. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production pour éviter toute corruption et panne de données. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production. L'assistant de configuration est Réponse aux vulnérabilités installé automatiquement en même temps que l'application. L'assistant d'installation est requis pour configurer l'application Réponse aux vulnérabilités . En outre, il est utilisé pour installer et configurer l'application Qualys Integration for Security Operations utilisée dans cet exemple, ainsi que d'autres applications prenant en charge et compatibles avec Réponse aux vulnérabilités. Pour plus d'informations sur l'installation de l'application Réponse aux vulnérabilités , reportez-vous à la section Installer Réponse aux vulnérabilités.
☐	En tant qu'utilisateur disposant du rôle administrateur, dans Assistant de configuration, accédez à **Tous** > **Groupes et utilisateurs de Réponse aux vulnérabilités** et affecter des utilisateurs avec les rôles de profil requis Réponse aux vulnérabilités . **a.** Dans l'Assistant de configuration, affichez les utilisateurs existants et tous les rôles déjà affectés en cliquant sur le lien du **module Administration utilisateurs** . **b.** Dans la liste, cliquez sur un nom d'utilisateur pour ouvrir l'enregistrement et sur la liste connexe **Rôles** . Tous les rôles affectés à cet utilisateur s'affichent. **c.** Revenir à **Groupes et utilisateurs de Réponse aux vulnérabilités** dans l'Assistant de configuration et suivez les invites pour affecter le rôle sn_vul.vulnerability_admin. **Remarque :** Le rôle sn_vul.vulnerability_admin est requis pour poursuivre la configuration. Vous pouvez également poursuivre la configuration en tant qu'utilisateur avec le rôle d'administrateur. (Facultatif) Vous pouvez également affecter les rôles de gestionnaire d'élément de configuration (CI) [sn_vul.ci_manager] et d'approbateur d'exception [sn_vul.exception_approver], mais ces profils ne sont pas requis pour les autres tâches de configuration. Pour plus d'informations sur l'affectation des rôles de personnage à l'aide de l'assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	Pour plus d'informations sur les utilisateurs et l'affectation de rôles aux utilisateurs et aux groupes, voir Administration utilisateurs .
☐	**a.** Accédez à la **Tous** > **Administration** > **Intégrations** et vérifiez que **l'intégration complète CWE 2000** est activée et exécutez la tâche planifiée pour importer des données. **b.** En tant qu'utilisateur disposant du rôle administrateur, accédez à **Applications système** > **Toutes les applications disponibles** et activer (**installer**) l'application Vulnerability Response Integration with NVD. Exécutez les intégrations NVD et CWE dans le cadre de votre configuration initiale et Réponse aux vulnérabilités avant d'importer des données de vulnérabilité dans votre instance avec un produit d'analyse tiers. Consultez Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces et Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE pour plus d'informations sur l'installation, la configuration et l'affichage des bibliothèques NVD et CWE.
☐	En tant qu'utilisateur disposant du rôle administrateur, naviguez dans **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation d'application d'intégration** et activez l'application Qualys Integration for Security Operations. Avant d'installer et d'exécuter un produit de scanner tiers tel Qualys que celui qui dispose d'une bibliothèque, vous devez d'abord installer et exécuter les intégrations NVD et CWE pour ingérer les données de vulnérabilité. Pour plus d'informations, consultez Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.
☐	(Facultatif) En tant qu'utilisateur disposant du rôle administrateur, si vous avez installé des données de démonstration avec l'application Réponse aux vulnérabilités , vous pouvez exécuter la Réponse aux vulnérabilités suite de tests ATF pour vérifier que les applications sont correctement installées. **Remarque :** Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production pour éviter toute corruption et panne de données. Pour plus d'informations, consultez Exécuter la suite de tests Framework de tests automatisés (ATF) pour Réponse aux vulnérabilités. Pour plus d'informations sur les tests automatisés, consultez Infrastructure de tests automatisés (ATF).

3. Poursuivez la configuration des applications à partir de la section Paramètres de Vulnerability Response.

   L'examen de ces paramètres vous aide à comprendre comment Réponse aux vulnérabilités il fonctionne lorsque vous poursuivez la configuration de votre environnement. Pour l'intégration de scanner utilisée dans cet exemple, vous devez modifier les paramètres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les concepts que vous utilisez dans cet exemple de configuration pour le Qualys produit s'appliquent à d'autres applications de scanner.

Vos Qualys informations d'identification sont nécessaires pour configurer l'application. Vérifiez que vous disposez des noms de compte, mots de passe et autres informations de service requises par Qualys les produits afin d'y avoir accès.

Rôles requis : sn_vul.vulnerability_admin ou admin.

Réponse aux vulnérabilités Tâches de liste de vérification d'implémentation de base pour l'administrateur de vulnérabilité

Tâche	Description
☐	Passez en revue les règles d'affectation de vulnérabilité. Les règles d'affectation affectent automatiquement les éléments vulnérables (VI) au groupe d'affectation approprié. Pour en savoir plus, consultez Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Pour plus d'informations sur la configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration, reportez-vous à la section Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration.
☐	Passez en revue les règles de la tâche de rattrapage. Les règles de tâche de rattrapage regroupent automatiquement les éléments vulnérables (VI) à mesure qu'ils sont importés en fonction de certaines conditions. Pour plus d'informations, consultez Réponse aux vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage.
☐	Passez en revue les calculateurs de risque. Les calculateurs de risque notent les éléments vulnérables pour définir leur ordre de priorité. Vous pouvez configurer les calculateurs de manière à incorporer les caractéristiques de l'élément de configuration (CI), de la disponibilité de l'exploitation et de la gravité de la vulnérabilité signalés par votre fournisseur d'évaluation de la vulnérabilité (scanner). Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.
☐	Passez en revue les règles de cibles de rattrapage. Les règles de cibles de rattrapage définissent les chronologies de rattrapage pour les éléments vulnérables et les tâches de rattrapage. Pour plus d'informations, consultez Réponse aux vulnérabilités Règles de cibles de rattrapage.
☐	Dans la section Configuration de l'intégration, examinez les paramètres de l'application Qualys et définissez et planifiez vos importations de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	a. Cliquez sur **Intégrations de scanners**. **b.** Sur la page Applications installées, cliquez sur **Modifier**. **c.** Entrez vos informations d'identification et cliquez sur **Suivant**. **d.** Lisez les descriptions de la configuration de la KnowledgeBase. **e.** Passez en revue la page Configuration de détection d'hôte pour les paramètres d'importation, les règles de recherche de CI et les calendriers d'importation. **f.** Une fois que vous êtes satisfait des paramètres de cette page, cliquez sur **Exécuter maintenant** pour importer des données. Cliquez sur le lien **Afficher les détails** qui s'affiche pour afficher l'état d'exécution de l'intégration de vulnérabilité. **g.** (Facultatif) Continuez à modifier les paramètres de configuration. **h.** Cliquez sur **Terminer** pour terminer l'installation et la configuration dans l'Assistant de configuration. Pour plus d'informations sur la configuration de l'application Qualys , reportez-vous à la section Configurer l'utilisation de l'assistant Qualys Vulnerability Integration de configuration.

Que faire ensuite

Félicitations ! Vous avez correctement installé l'application et l'avez configurée, ainsi qu'une Réponse aux vulnérabilités application de scanner à l'aide de l'assistant de configuration. Le système de base est maintenant prêt à fonctionner.

Pour télécharger, installer et configurer d'autres applications pour Réponse aux vulnérabilités, suivez les mêmes étapes et concepts que ceux de la liste de vérification précédente. Consultez les rubriques spécifiques fournies pour chaque application pour plus d'informations.

Pour en savoir plus sur les applications prises en charge disponibles auprès de , reportez-vous à la ServiceNow Store section Installation et prise en charge des Réponse aux vulnérabilités applications.Réponse aux vulnérabilités

Pour plus d'informations sur l'utilisation Réponse aux vulnérabilités, reportez-vous à la section Explorer l'application Réponse aux vulnérabilités.

Réponse aux vulnérabilités États des tâches de rattrapage

Les intégrations tierces importent des données de détection d'éléments vulnérables qui créent de nouveaux éléments de vulnérabilité (VIT) ou mettent à jour les VIT existants. Les états de détection mettent à jour les états VIT dans la mesure où ils sont ouverts ou fermés.

Pour plus d'informations sur la façon dont l'état d'une détection affecte l'état d'un VIT, reportez-vous à la Détections, tâches de rattrapage et états des éléments vulnérables section .

Avec Change Management pour Réponse aux vulnérabilités, il existe une relation synchronisée entre les champs d'état des tâches de rattrapage et les champs d'état des demandes de changement (CHG) dans le produit Vulnerability Response. Au fur et à mesure qu'une demande de changement progresse dans son cycle de vie, elle modifie automatiquement l'état de toutes les tâches de rattrapage connexes. Une fois qu'une demande de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

changement est implémentée, la tâche de rattrapage est automatiquement résolue. Consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage pour plus d'informations.

Remarque : À partir de la v23.0 de Réponse aux vulnérabilités:

- le workflow **d'approbation de l'état de la tâche de rattrapage** est déconseillé et remplacé par l'approbation de l'état de la tâche de rattrapage de flux dans le concepteur de flux.
- le bouton **Fermer** a été supprimé pour une tâche de rattrapage et la fermeture d'une tâche de rattrapage est pilotée par le scanner.

Le tableau suivant répertorie les états des tâches de rattrapage et les actions que vous pouvez effectuer sur une tâche de rattrapage à l'état respectif :

États des tâches de rattrapage

État	Description
Ouvert	État à la création. À partir de cet état, vous pouvez : **Afficher les VI en double** Identifiez les VIT en double signalés par plusieurs scanners dans le système. Vous pouvez marquer le VIT en double comme Résolu ou Fermé. Les entrées en double ne s'affichent que lorsque la combinaison de vulnérabilités est créée à l'aide des vulnérabilités et expositions communes (CVE). Pour plus d'informations, consultez Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables. **Démarrer l'examen** Affectez cette tâche de rattrapage à une personne ou à un groupe pour qu'il commence à enquêter. **Marquer comme faux positif** Marquez un élément ou un groupe comme faux positif si le scanner signale qu'une vulnérabilité existe dans le système, mais qu'en réalité il n'y a pas de vulnérabilité. **Demande d'exception** Demandez une exception, une date de réouverture (Jusqu'à), un motif et, éventuellement, fournissez des informations supplémentaires. Reporte le rattrapage de l'élément ou du groupe jusqu'à la date à laquelle une exception est demandée. **Résoudre** Marquer comme résolu pour déplacer l'élément ou le groupe vers un état résolu. **Créer un changement** Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. **Diviser la tâche de rattrapage**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tâches de rattrapage (suite)

État	Description
	Pour une tâche de rattrapage comportant plusieurs éléments vulnérables, utilisez un ensemble de conditions pour filtrer un sous-ensemble d'éléments vulnérables et diviser une tâche de rattrapage. Les éléments que vous sélectionnez sont automatiquement déplacés vers une nouvelle tâche de rattrapage. Pour plus d'informations, consultez Fractionner une tâche de rattrapage dans le Espace de travail de remédiation IT. **Différer** Sélectionnez l'état Différé, une date de réouverture, un motif et, éventuellement, fournissez des informations supplémentaires. Diffère l'état de la tâche de rattrapage jusqu'à la date de réouverture. **Supprimer** Confirmez la suppression. Supprime le groupe.
En cours d'examen	Déclenché par le bouton **Démarrer l'examen** . À partir de cet état, vous pouvez : **Créer un incident de sécurité** Pour plus d'informations, consultez Créer un incident de sécurité. **Créer un changement** Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. **Fractionner la tâche** Pour une tâche de rattrapage comportant plusieurs éléments vulnérables, utilisez un ensemble de conditions pour filtrer un sous-ensemble d'éléments vulnérables et diviser une tâche de rattrapage. Les éléments que vous sélectionnez sont automatiquement déplacés vers une nouvelle tâche de rattrapage. Pour plus d'informations, consultez Fractionner une tâche de rattrapage. **Créer une demande de changement** Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage. **En attente d'implémentation** Modifie l'état en En attente d'implémentation. Cet état indique que les tâches de rattrapage ont été renvoyées en dehors d'un Réponse aux vulnérabilités. **Différer** Sélectionnez l'état Différé, une date de réouverture, un motif et, éventuellement, fournissez des informations supplémentaires. Diffère l'état de la tâche de rattrapage jusqu'à la date de réouverture. **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tâches de rattrapage (suite)

État	Description
Différé	Déclenché par le bouton **Demander une exception** . Dans le cadre du workflow d'approbation, l'état Différé est En cours de révision et ne peut pas être fermé tant qu'il n'a pas été approuvé. À partir de cet état, vous pouvez : **Créer un changement** Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. **Fractionner la tâche** Pour une tâche de rattrapage comportant plusieurs éléments vulnérables, utilisez un ensemble de conditions pour filtrer un sous-ensemble d'éléments vulnérables et diviser une tâche de rattrapage. Les éléments que vous sélectionnez sont automatiquement déplacés vers un nouveau VG. Consultez Fractionner une tâche de rattrapage. **Créer un incident de sécurité** Pour plus d'informations, consultez Créer un incident de sécurité. **Rouvrir** Transition vers un état ouvert. **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage. Les informations sur le report s'affichent sous l'onglet **Fermer/ Différer** . À la date de report, le groupe rouvre pour correction.
En attente d'implémentation	Déclenché par le bouton **En attente d'implémentation** . À partir de cet état, vous pouvez : **Créer un incident de sécurité** Pour plus d'informations, consultez Créer un incident de sécurité. **Créer un changement** Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. **Fractionner la tâche** Pour une tâche de rattrapage comportant plusieurs éléments vulnérables, utilisez un ensemble de conditions pour filtrer un sous-ensemble d'éléments vulnérables et diviser une tâche de rattrapage. Les éléments que vous sélectionnez sont automatiquement déplacés vers une nouvelle tâche de rattrapage. Pour plus d'informations, consultez Fractionner une tâche de rattrapage. **Créer une demande de changement**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États des tâches de rattrapage (suite)

État	Description
	Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage. **Différer** Sélectionnez l'état Différé, une date de réouverture, un motif et, éventuellement, fournissez des informations supplémentaires. Diffère l'état de la tâche de rattrapage jusqu'à la date de réouverture. **Résoudre** Ajoutez des notes. L'état devient Résolu. Les notes apparaissent sous l'onglet **Résolution** . **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage.
Résolu	Déclenché à partir du bouton **Résoudre** . À partir de cet état, vous pouvez : **Créer un incident de sécurité** Pour plus d'informations, consultez Créer un incident de sécurité. **Créer un changement** Créez une demande de changement ou associez une tâche de rattrapage à une demande de changement existante. Pour plus d'informations, consultez Créer une demande de changement à partir d'une tâche de rattrapage et Associer une tâche de rattrapage à une demande de changement existante. **Rouvrir** Transition vers un état ouvert. **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage. Les notes apparaissent sous l'onglet **Notes** . Les informations sur la résolution apparaissent sous l'onglet **Résolution** .
Fermé	Déclenché par le scanner. À partir de cet état, vous pouvez : **Créer un incident de sécurité** Pour plus d'informations, consultez Créer un incident de sécurité. **Rouvrir** Transition vers un état ouvert. **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage. Les informations sur la fermeture apparaissent sous l'onglet **Fermer/ Différer** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le propriétaire du rattrapage peut uniquement marquer un élément vulnérable ou une tâche de rattrapage comme résolu. Selon la confirmation de l'analyseur, cet élément résolu ou cette tâche de rattrapage peut être marqué comme Fermé ou Rouvert.
- Le bouton **Supprimer** est disponible pour l'administrateur lorsque plusieurs éléments vulnérables sont créés manuellement et que ceux-ci doivent être fermés ou supprimés.
- Si vous déterminez que les éléments présentent un risque faible, sont en attente d'une fenêtre de changement ou d'un correctif, vous pouvez modifier leur tâche de rattrapage à l'état Différerle rouge pendant une durée définie. Vous pouvez demander une exception à l'aide de l'option **Demande d'exception** .

  Remarque : Lorsque les tâches de rattrapage sont différées ou fermées, vous pouvez spécifier des résolutions pour affiner les raisons de cette opération.

- Lorsqu'un VIT est rouvert, manuellement ou automatiquement, il se produit ce qui suit :
  - L'état VIT devient Ouvert. L'état de la tâche de rattrapage d'origine n'est pas mis à jour.
  - La VIT est réévaluée et placée dans une nouvelle tâche de rattrapage ou dans une tâche de rattrapage existante basée sur les règles de tâche de rattrapage actives.

  Cela préserve son historique tout en permettant un rattrapage supplémentaire.

- Lorsqu'une tâche de rattrapage est créée (automatiquement ou manuellement) ou divisée, ses champs **État**, **Motif etJusqu'à** sont évalués. En cas d'action de division, ces champs sont évalués pour les anciennes et les nouvelles tâches de rattrapage. Lorsqu'un VIT est mis à jour, les champs **État**, Motif et **Jusqu'à de** toutes ses tâches de rattrapage associées sont évalués.
  - Si tous les VIT d'une tâche de rattrapage sont différés et ont le même motif, alors l'état de la tâche de rattrapage passe à **Différé** et le motif des VIT est affecté à la tâche de rattrapage. Si les VIT diffèrent en matière de motif, le motif de la tâche de rattrapage devient **Aucun**.
  - La date de **fin** la plus proche de tous les VIT est mise à jour dans le champ **Jusqu'à** de la tâche de rattrapage.
  - Si vous rouvrez un VIT, l'état de la tâche de rattrapage devient **Ouvert**.

  Cette évaluation est effectuée par la tâche planifiée, qui s'exécute *`Rollup vulnerability item values to vulnerability and group`* toutes les 15 minutes.

Détections, tâches de rattrapage et états des éléments vulnérables

Des intégrations tierces récupèrent les données de détection des éléments vulnérables. Les détections sont des occurrences distinctes de vulnérabilités telles que signalées par les scanners.

Les données de détection sont associées à des éléments vulnérables (VI, VIT) et l'état du VI est mis à jour en fonction de l'état des détections. Si aucun VI n'est trouvé, un nouveau VI est créé. Les détections ne sont ouvertes ou fermées que par les données trouvées directement par un scanner.

Si toutes les détections sont fermées pour un élément vulnérable, cet élément vulnérable est fermé. Sur l'enregistrement du VI, l'état est Fermé/Corrigé. Lorsque tous les VI sont fermés pour une tâche de rattrapage, la tâche de rattrapage est fermée. Sinon, le flux d'état reste le même.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les VI fermés avec un sous-état fixe ou périmé sont rouverts si une nouvelle détection est créée et que les VI peuvent être mis en correspondance avec la nouvelle vulnérabilité.

À partir de la version 20.0 de Réponse aux vulnérabilités, si une détection est périmée et que le VI associé est à l'état Fermé, l'état du VI ne passe pas à l'état Fermé - Périmé. Cela permet d'éviter que le VI ne se rouvre lorsqu'une nouvelle détection est identifiée afin d'éviter de passer par l'ensemble du processus de demande et d'approbation des faux positifs. Pour inverser ce comportement, décochez la case **Ignorer les détections obsolètes pour les VI fermés** dans le formulaire Configuration de fermeture automatique. Pour plus d'informations, consultez Fermer automatiquement les détections obsolètes dans Réponse aux vulnérabilités.

Selon le script include, `DetectionBase`, méthode , `_shouldReOpenVI()`si le VI a été précédemment fermé avec un sous-état fixe, périmé ou CI désactivé, il est rouvert et la détection est mappée au VIT existant.

Par exemple, supposons que la date de fermeture d'un VI est postérieure à la date lastfound d'une détection. Vous vous attendez à ce que ces enregistrements de VI restent fermés. Toutefois, si vous voyez qu'un VI précédemment fermé s'est rouvert, cela signifie que le VI a été fermé par une détection antérieure et que la vulnérabilité a été retrouvée lors d'une analyse ultérieure. Lorsqu'une nouvelle détection correspond au VIT fermé qui présente la même vulnérabilité sur l'élément de configuration du VI, le VI est rouvert.

Tâches de rattrapage et états des éléments vulnérables

Les états des tâches de rattrapage et des éléments vulnérables peuvent s'affecter mutuellement. La plupart du temps, un état de tâche de rattrapage met à jour l'état de l'élément vulnérable, l'état de tâche de priorité le plus élevé étant utilisé pour mettre à jour les éléments vulnérables du groupe.

La priorité des États est la suivante.

Fermé > **Différé** > **Résolu** > **En cours de révision** > **En attente d'implémentation** > **En cours d'examen** > **Ouvert**

- Lorsqu'un groupe d'éléments vulnérables se trouve dans une tâche de rattrapage et qu'ils ne sont pas modifiés au niveau individuel, ils ont le même état que leur tâche de rattrapage.
- Lorsque la tâche de rattrapage passe de l'état Ouvert à l'état En attente d'implémentation, tous les éléments vulnérables de la tâche de rattrapage passent à l'état En attente d'implémentation.
- Lorsque la tâche de rattrapage est différée, l'élément vulnérable l'est également. À partir de la version 16.5, vous pouvez suivre le nombre de reports d'un élément vulnérable, d'un élément vulnérable d'application, d'un élément vulnérable de conteneur ou d'une tâche de rattrapage. La tâche planifiée, `set deferral counts`, s'exécute quotidiennement pour valider les nombres des enregistrements qui sont reportés plusieurs fois dans la colonne Nombre de reports des modules Reports multiples pour VR, AVR et CVR. Tous les décomptes des VI associés à une tâche de rattrapage sont collectés et publiés si une tâche de rattrapage est reportée plusieurs fois.

Éléments vulnérables mis à jour uniquement par les tâches de rattrapage

Les éléments correspondent à l'état de la tâche de rattrapage, s'ils n'ont pas été mis à jour individuellement, à quelques exceptions près :

- Si l'état de la tâche de rattrapage passe à Fermé et sa résolution à Annulé ou Corrigé avec exception, l'élément n'est pas affecté et prend l'état de toute autre tâche de rattrapage qui le contient. Si l'élément vulnérable n'est dans aucune autre tâche de rattrapage, il revient à l'état Ouvert.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si l'état de l'élément vulnérable est Fermé/Corrigé (mis à jour par une analyse ou une importation), lorsque la tâche de rattrapage change d'état, l'élément vulnérable reste à l'état Fermé/Corrigé. Cette condition est vraie, quel que soit l'état de la tâche de rattrapage.

Éléments vulnérables dans des états définis individuellement

Les éléments vulnérables dont l'état est mis à jour sur l'élément, tels que les éléments fermés ou différés individuellement, ne correspondent pas automatiquement à l'état de la tâche de rattrapage. Au lieu de cela, il compare son état à tous les groupes associés pour trouver l'état avec la priorité la plus élevée à appliquer.

Remarque : L'état Fermé/Corrigé est un cas particulier. Pour les éléments vulnérables définis sur l'état Fermé/Corrigé, si tous les éléments vulnérables d'une tâche de rattrapage sont définis sur Fermé/Corrigé, par exemple lorsqu'un scanner constate que toutes les vulnérabilités ont été corrigées, la tâche de rattrapage est automatiquement marquée comme Fermée/Corrigée.

Les tâches de rattrapage contiennent des champs d'affectation vides

Si l'état des VI dans une tâche de rattrapage passe de Résolu à Ouvert, l'état de la tâche de rattrapage est également mis à jour de Résolu à En cours d'examen.

Toutefois, si les champs **Affecté à** et **Groupe d'affectation** de la tâche de rattrapage sont vides, la tâche de rattrapage reste à l'état Résolu et ne passe pas à En cours d'examen.

Le groupe d'affectation des éléments vulnérables n'est pas toujours mis à jour lorsque leur tâche de rattrapage est mise à jour

Si le groupe d'affectation d'un VI à l'état Ouvert est mis à jour manuellement, il n'est pas mis à jour de nouveau lorsque le groupe d'affectation de sa tâche de rattrapage est mis à jour. Ces informations ne sont pas écrasées, car le groupe d'affectation du VI a été mis à jour intentionnellement et peut faire partie d'une autre tâche de rattrapage.

Scénarios de déploiement et de réduction de l'état

Les scénarios de déploiement et de réduction d'état synchronisent automatiquement l'état des tâches de rattrapage (RT) et des éléments vulnérables (VIT), garantissant des mises à jour en temps réel pour les deux. Cette interaction dynamique réduit le suivi manuel, améliore la précision et fournit aux utilisateurs une vue actualisée des progrès, ce qui rend la gestion des vulnérabilités plus efficace et aide les utilisateurs à prendre rapidement des décisions éclairées.

Comportement de déploiement

Lorsque les états des éléments vulnérables (VIT) changent, ces changements peuvent se propager jusqu'au niveau de la tâche de rattrapage (RT). Le tableau suivant récapitule les principaux scénarios de déploiement dans lesquels les changements dans l'état des éléments vulnérables (VIT) peuvent influencer l'état de la tâche de rattrapage (RT) associée, en fonction des conditions de fermeture, des réaffectations et des reports.

Scénarios de déploiement

État VIT	État RT
Ouvrir > en cours d'examen	Reste ouvert
Ouvrir > fermé : faux positif	Reste ouvert

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Scénarios de déploiement (suite)

État VIT	État RT
Ouvrir > en cours de révision	Reste ouvert
Ouvert > différé (tout sous-état)	Ouvert > différé
Ouvert > résolu	Reste ouvert
Ouvert > Fermé-annulé	Reste ouvert
Ouvert > Fermé-Corrigé	Ouvert > Fermé-Corrigé
Ouvert > Fermé-Corrigé avec des exceptions	Ouvert > fermé
Fermé-Corrigé > Ouvert	Reste fermé-fixe
Ouvert > fermé-fixe ; (après l'analyse suivante) > Résolu	Reste ouvert
Ouvert > Fermé-Non valide	Reste ouvert
Ouvert > fermé : périmé	Ouvert > fermé-annulé
Fermé : périmé > ouvert	Reste fermé-annulé
Ouvrir > Résultat de fermeture non valide	Reste ouvert
Ouvert > Fermé-Non valide	Reste ouvert
Ouvert > fermé : CI désactivé	Ouvert > Fermé-annulé
Ouvrir > en attente d'implémentation : correctif planifié	Reste ouvert
Ouvrir > en attente d'implémentation : correctif non planifié	Reste ouvert
Ouvrir > en attente d'implémentation : correctif planifié (date cible manquante)	Reste ouvert
En cours d'examen > CI fermé désactivé	RT1 : en cours d'examen > fermé-annulé RT2 : en cours d'examen > fermé-annulé
Ouvert > résolu ; RT = Résolu ; Réouvre VIT	S'il est affecté, RT : Résolu > en cours d'examen ; Sinon : Ouvert
VIT1 : fermé-fixe VIT2 : En cours d'examen Si VIT2 rouvre et que VIT1 reste résolu.	RT1 : en cours d'examen RT2 : Fermé-Fixe
VIT1 : fermé-périmé VIT2 : CI fermé désactivé	Ouvert > Fermé-annulé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Scénarios de déploiement (suite)

État VIT	État RT
VIT1 : résolu VIT2 : CI fermé désactivé	Reste ouvert
VIT1 : fermé-fixe VIT2 : CI fermé désactivé	Ouvert > Fermé-annulé
VIT1 : fermé-fixe VIT2 : fermé-périmé	Ouvert > Fermé-Corrigé
VIT1 : fermé<tout sous-état> VIT2 : différé	Ouvert> différé Date de fin portée avant en tant que VIT2

Comportement de réduction

Lorsque l'état d'une tâche de rattrapage change, l'état est souvent propagé aux VIT associés, sauf s'il est remplacé par des mises à jour manuelles ou des exceptions spécifiques. Le tableau suivant récapitule les principaux scénarios de restauration dans lesquels les changements apportés à l'état de la tâche de rattrapage (RT) peuvent affecter l'état de l'élément vulnérable associé (VIT), en fonction des règles de priorité et des conditions spéciales.

Scénarios de restauration

État RT	État VIT
Ouvert> en cours d'examen	Ouvert> en cours d'examen
Ouvrir > fermé : faux positif	Ouvrir > fermé : faux positif
Ouvrir > en cours de révision	Ouvrir > en cours de révision
Ouvert > différé (sous-état : motif donné)	Ouvert > différé (sous-état : motif donné)
Ouvert > résolu	Ouvert > résolu
Ouvert > Fermé-annulé	Reste ouvert
Ouvert > Fermé-Corrigé avec des exceptions	Reste ouvert
RT1 : ouvrir > en cours d'examen RT2 : Ouvert	Ouvrir > en cours d'examen
RT1 : > ouverts en cours d'examen > en attente d'implémentation RT2 : en cours d'examen	Ouvert > En cours d'examen > En attente d'implémentation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Scénarios de restauration (suite)

État RT	État VIT
RT1 : en attente d'implémentation > différé RT2 : en attente d'implémentation	En attente d'implémentation > Différé
RT1 : en attente d'implémentation > Fermé-annulé RT2 : en cours d'examen	En attente d'implémentation> En cours d'examen
Ouvert>Fermé-Corrigé avec des exceptions Observations finales : VIT2 reste ouvert	VIT1 : Ouvert > Fermé-Fixe VIT2 : Ouvert
Ouvert>Résolu Observations finales : VIT2 : Ouvert>Résolu	VIT1 : Ouvert > Fermé-Fixe VIT2 : Ouvert
Ouvert>Résolu Observations finales : Réouverture du VIT2 ; VIT1 reste résolu ; RT : résolu > ouvert	VIT1 : Ouvert > Fermé-Fixe VIT2 : Ouvert

État de la tâche de rattrapage pour les éléments vulnérables (VIT) dans plusieurs groupes

Lorsqu'un VIT est dans plusieurs tâches de rattrapage (RT dans les tables suivantes) et que son propre état n'a pas été défini, l'état du groupe de priorité le plus élevé détermine l'état de ce VIT, comme indiqué dans le tableau suivant.

Exemples d'états d'éléments vulnérables

État de la tâche de résolution	État de l'élément vulnérable
RT 1 : **Ouvert** > **En cours d'examen** RT 2 : **En cours**	**En cours d'examen** Lorsque RT 1 est En cours d'examen et que RT 2 est ouvert, l'élément vulnérable passe à En cours d'examen. Après la recherche, entre RT 1 et RT 2, RT 1 a l'état avec la priorité la plus élevée.
RT 1 : **En cours d'examen** RT 2 : **Ouvert** > **En cours d'examen**	**En cours d'examen** Lorsque le RT 2 fait l'objet d'une enquête et que le RT 1 est en cours d'examen, l'élément vulnérable reste à l'état En cours d'examen. Après la recherche, entre RT 1 et RT 2, ils ont l'état avec la même priorité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemples d'états d'éléments vulnérables (suite)

État de la tâche de résolution	État de l'élément vulnérable
RT 1 : **En cours d'examen** RT 2 : **En cours d'examen** > **En attente d'implémentation**	**En attente d'implémentation** Lorsque le RT 2 est en attente d'implémentation et que le RT 1 est en cours d'examen, le VI passe à En attente d'implémentation. Après la recherche, entre RT 1 et RT 2, RT 2 a l'état avec la priorité la plus élevée.
RT 1 : **En cours d'examen** > **Différé** RT 2 : **En attente d'implémentation**	**Différé** Lorsque RT 1 est reporté et que RT 2 est en attente d'implémentation, le VI passe à Différé. Après la recherche, entre RT 1 et RT 2, RT 1 a l'état avec la priorité la plus élevée.

Élément vulnérable dans plusieurs groupes, cas particuliers

État de la tâche de rattrapage	État de l'élément vulnérable
RT 1 : **En cours d'examen** RT 2 : **En attente d'implémentation** > **Fermé (fixe ou annulé)**	**En cours d'examen** Lorsque RT 2 est Fermé/Corrigé ou Fermé/Annulé et que RT 1 est En cours d'examen, l'élément vulnérable passe de En attente d'implémentation (auparavant la priorité la plus élevée) à En cours d'examen (actuellement la priorité la plus élevée).
RT 1 : n'importe quel état RT 2 : n'importe quel état	Si l'état source de l'élément vulnérable est Fixe (mis à jour par une analyse ou une importation), lorsque le groupe change d'état, l'élément vulnérable passe à l'état Fermé/Corrigé. Cette condition est vraie, quels que soient l'état des autres groupes associés. La recherche d'éléments vulnérables pour l'état du groupe ne se produit pas.

Lorsqu'un état de VI est défini individuellement, son état est pris en compte lors de l'évaluation de la priorité, comme pour toute autre tâche de rattrapage. Lorsqu'un VI appartient à plusieurs tâches de rattrapage, le tableau suivant répertorie les mises à jour effectuées.

État de l'élément vulnérable défini individuellement Tickets spéciaux

État de l'élément de vulnérabilité au sein d'un groupe	État final de l'élément vulnérable
État RT 1 : **En cours d'examen** État RT 2 : **En cours d'examen** > **En attente d'implémentation** État de VI d'origine : **En cours d'examen** > **(défini sur le VI)**	**En attente d'implémentation** Lorsque RT 2 est passé à En attente d'implémentation et que RT 1 est resté En cours d'examen, l'élément vulnérable passe à En attente d'implémentation (la priorité la plus élevée).
RT 1 : **En cours d'examen**	**Différé**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État de l'élément vulnérable défini individuellement Tickets spéciaux (suite)

État de l'élément de vulnérabilité au sein d'un groupe	État final de l'élément vulnérable
RT 2 : **En cours d'examen** > **En attente d'implémentation** État de VI d'origine : **Différé** > **(défini sur le VI)**	Lorsque le RT 2 est passé à En attente d'implémentation et que le RT 1 est resté En cours d'examen, le VI reste dans l'état Différé (la priorité la plus élevée).

Le tableau suivant montre que lorsque deux tâches de rattrapage avec des éléments vulnérables communs sont reportées, l'état est différé jusqu'à la dernière date.

Tickets spéciaux d'état différé d'élément vulnérable

État de l'élément de vulnérabilité au sein d'un groupe	État final de l'élément vulnérable
État RT 1 : **En cours de révision (jusqu'au 10 avril)** État RT 2 : **En cours d'examen** > **En cours de révision (jusqu'au 30 avril)** État de VI d'origine : **En cours de révision (jusqu'au 10 avril)** > **(défini sur le VI)**	**Reporté (jusqu'au 30 avril)** Lorsque RT 2 est passé à Différé (jusqu'au 30 avril) et que RT 1 reste Différé (jusqu'au 10 avril), le VI passe de l'état Différé (jusqu'au avril 05) à l'état Différé (jusqu'au 30 avril).
RT 1 : **En cours de révision (jusqu'au 15 juillet)** RT 2 : **En cours d'examen** > **En cours de révision (jusqu'au 10 juillet)** État de VI d'origine : **Différé** > **(jusqu'au 15 juillet)**	**Reporté (jusqu'au 15 juillet)** Lorsque RT 2 est passé en différé (jusqu'au 10 juillet) et que RT 1 reste en différé (15 juillet), le VI reste en différé (jusqu'au 15 juillet).

Paramètres supplémentaires pour la séparation de domaine

Pour une exécution et des résultats précis, les précautions et les paramètres suivants sont requis pour la séparation de domaine dans Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs et Conformité de la configuration.

Ne modifiez pas les logiques métier et les processus dans le domaine global pour éviter tout problème et de sorte que tous les derniers changements soient mis à jour pour chaque mise à niveau. Dupliquez toutes les logiques métier et tous les processus dans chaque domaine séparément et assurez-vous qu'ils sont inactifs dans le domaine global. Dans le cas contraire, les logiques métier et les processus du domaine global ont priorité sur le domaine enfant. Supposons que vous ayez créé une règle de risque dans un domaine enfant et que le domaine global dispose également d'une règle de risque similaire, la règle du domaine global l'emporte sur la règle du domaine enfant.

Réévaluation des calculateurs et des règles

Avant la version 20.0, lorsque vous réappliquez des calculateurs ou des règles, le marqueur de réexécution est défini sur vrai et une règle métier est déclenchée pour exécuter une tâche planifiée qui réapplique les calculateurs et les règles. À partir de la v20.0, vous n'avez pas besoin de dépendre de l'indicateur de réexécution . Lorsque vous cliquez sur le bouton **Réappliquer le calculateur** , une tâche d'arrière-plan est déclenchée pour réappliquer les calculateurs et les règles. Cela vous permet de créer des calculateurs et des règles pour tous les domaines.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres des calculateurs de déploiement

Dans un domaine, un seul calculateur de déploiement doit être actif pour une table. Par exemple, considérez la table Tâche de rattrapage, *sn_vul_vulnerability* avec le calculateur de déploiement, Déploiement de la **tâche de rattrapage** dans le domaine global. Si vous dupliquez ce calculateur cumulatif en modifiant les pondérations pour la même table dans le même domaine, il y aura des divergences dans les calculs cumulatifs. Par conséquent, assurez-vous d'activer un seul calculateur de déploiement s'il existe deux calculateurs de déploiement ou plus pour une table du même domaine.

Champs du formulaire Éléments détectés

Les actifs sont automatiquement mis en correspondance avec les éléments de configuration (CI) lorsqu'ils Base de données de gestion des configurations (CMDB) sont importés à l'aide des règles de recherche de CI. Les enregistrements des CI sans correspondance sont automatiquement créés lors des importations d'intégration de vulnérabilité tierce et inclus dans les éléments détectés. Toutefois, pour les actifs cloud qui ne sont pas présents dans CMDB CI, l'enregistrement est créé dans la classe de ressource cloud.

Champs Éléments détectés

Les informations contenues dans ces enregistrements sont ingérées à partir des enregistrements tiers et classées lors de l'importation.

Ces champs se trouvent sur les enregistrements répertoriés dans la table Éléments détectés [sn_sec_cmn_src_ci].

Pour afficher les données importées dans les champs répertoriés dans les tables suivantes, vous devez avoir, au minimum, le rôle sn_vul.read_all.

Champ	Description
Numéro	Identificateur affecté à l'enregistrement.
Élément de configuration	Élément de configuration importé de l'intégration de source tierce. À partir de la version 12.0, l'élément de configuration est le dernier CI de la liste des CI après filtrage des CI désactivés.
Classe	Classe affectée au CI lors de l'importation par Réponse aux vulnérabilités
Source	Source importée à partir de l'intégration de la source tierce.
Règle de correspondance CI	Règle de correspondance CI utilisée pour créer l'élément.
V18.0 : Type de correspondance pour le DI	Type de correspondance utilisé pour créer l'élément détecté. Les options sont les suivantes : • Créé par VR • Créé par IRE • Correspond à une recherche de CI • Correspond à l'IRE • Mise en correspondance manuelle (à partir de la version 24.0.6 de Réponse aux vulnérabilités, vous pouvez afficher cette option

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	supplémentaire. Cette option est définie automatiquement si vous mettez à jour manuellement un CI sur le formulaire d'élément détecté.) Ces informations ne sont disponibles que pour les données renseignées pour Réponse aux vulnérabilités les versions 18.0 et ultérieures. Sur les données existantes, cette colonne ne contient aucune valeur. **Remarque :** Si vous réappliquez les règles de recherche de CI, certains CI sur les DI peuvent être mis à jour, ce qui entraîne le remplissage de cette colonne.
Autres CI appariés	Liste des autres éléments de configuration correspondant à la règle de recherche de CI.
État	État du CI qui est déterminé lors de l'importation. Les choix possibles sont les suivants : • **En correspondance** : un élément de configuration correspondant a été trouvé dans la CMDB. • **Sans correspondance** : aucune correspondance trouvée dans la CMDB. Un enregistrement d'espace réservé est créé.
Créées	Date de création de l'enregistrement de l'élément détecté.
Mis à jour	Date de mise à jour de l'enregistrement de l'élément détecté.
Mis à jour par	Utilisateur qui a mis à jour les données.
Balise d'hôte	Balises d'hôte affectées à cet élément détecté au cours de l'importation. Vous pouvez avoir jusqu'à 31 balises d'hôte par élément détecté.
Nom de domaine complet	Données associées à ce CI trouvées dans la CMDB.
Adresse MAC	Données associées à ce CI trouvées dans la CMDB.
Système d'exploitation	Système d'exploitation associé à ce CI.
NetBIOS	NetBIOS importé à partir de l'intégration source tierce.
Adresse IP	Données associées à ce CI trouvées dans la CMDB.
Données sources	Dernières données associées à ce CI à partir de la source.
V16 : données sources initiales	Données initiales associées à ce CI à partir de la source.
V16 : Réévaluer le CI	Reçoit les données du scanner. Si des données sont mises à jour, la valeur est définie sur vrai. **Remarque :** Les valeurs des données sources sont recalculées en fonction des dernières données sources. Lorsque des données mises à jour sont récupérées à partir du scanner, les données sources sont mises à jour. La valeur des données sources existantes est déplacée vers le champ de données source initial. Pour réévaluer les éléments détectés, activez les règles de recherche de CI réappliquées sur la tâche planifiée Éléments détectés changés .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
L'agent existe	Indique vrai si l'agent est installé sur l'actif. Si les valeurs hostUID et UUID de la colonne de données sources sont vides, cette valeur est renseignée comme vrai. **Remarque :** Ce champ apparaît à partir de la version 19.0 sur Réponse aux vulnérabilités.

À partir de la version 23.0 du Réponse aux vulnérabilités, la colonne % de conformité des résultats des tests **(CI)** affiche le pourcentage de résultats des tests conformes pour le CI correspondant. Pour obtenir cette valeur, vous devez définir calcTRComplianceForCI sur vrai dans la tâche planifiée **Mettre à jour les mesures de rattrapage** .

Remarque : La valeur **% de conformité des résultats des tests (CI)** est renseignée uniquement pour les éléments détectés dont la valeur est non vide dans les colonnes **Date de la dernière analyse de conformité** de la configuration ou **Date de la dernière analyse de conformité hors infrastructure** .

À partir de la version 18.0 de Réponse aux vulnérabilités, Qualys et Rapid7Tenable pour Réponse aux vulnérabilités les scanners peuvent recevoir les métadonnées supplémentaires suivantes pour les actifs dans le cloud.

Champ	Description
Fournisseur de services dans le cloud	Nom du fournisseur de services dans le cloud qui propose des services de cloud computing. Par exemple, Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).
Région du cloud	Emplacement où la ressource a été hébergée.
Compte dans le cloud	Compte fourni par des fournisseurs de services dans le cloud tels que AWS, GCP, et ainsi de suite pour accéder aux services de cloud computing.
Type de ressource dans le cloud	Types d'actifs présents dans le cloud, tels que l'ordinateur Amazon Elastic Compute Cloud (EC2), les catégories S3, AWS et ainsi de suite.
ID de ressource	Identificateur unique affecté à une ressource dans un environnement de cloud computing. Cet ID est utilisé pour identifier et gérer la ressource.
Nom de la ressource	Nom défini par l'utilisateur utilisé pour identifier et gérer une ressource dans un environnement de cloud computing.
Image	Une image d'ordinateur virtuel ou image serveur est un ordinateur virtuel préconfiguré qui contient un système d'exploitation, des applications et d'autres logiciels. Par exemple, Image d'ordinateur Amazon.

Une nouvelle règle de recherche de CI, « ID de ressource dans le cloud », a été introduite pour correspondre aux CI dans le cloud en fonction des métadonnées dans le cloud.

Réponse aux vulnérabilités Champs du formulaire de vulnérabilité

Les vulnérabilités sont créées automatiquement lorsque les enregistrements sont téléchargés à partir de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou d'intégrations tierces et stockés dans **les bibliothèques** de Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'entrée NVD

Pour afficher les données importées dans les champs répertoriés dans les tables suivantes, vous devez avoir, au minimum, le rôle sn_vul.read_all.

Ces champs se trouvent sur les enregistrements répertoriés dans la table Entrées de la base de données de vulnérabilité nationale [sn_vul_nvd_entry].

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Cote de risque	(Masqué lorsqu'aucun VIT n'est associé à la vulnérabilité) **Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour plus d'informations sur les évaluations de risque, reportez-vous à Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité. **Remarque :** Cette **cote de risque** de base est différente de la cote de **risque** de l'enregistrement de la solution.
Score du risque	(Masqué lorsqu'aucun VIT n'est associé à la vulnérabilité) Quantité calculée de risque que l'élément vulnérable pose à votre environnement. **Remarque :** Ce **score de risque** de base est différent du **score de risque** de l'enregistrement de la solution. Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.
Gravité	Degré de gravité normalisé de cette vulnérabilité. Les cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Pour plus d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Créer une carte de Réponse aux vulnérabilités gravité.
Existence de l'exploit	Oui, si au moins un exploit est associé à cette vulnérabilité.
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter cette vulnérabilité.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour cette vulnérabilité. Disponible lorsque NVD SAM est activé.
VI actifs	(Masqué lorsqu'aucun VIT n'est associé à la vulnérabilité) Nombre d'éléments vulnérables associés à cette vulnérabilité, n'étant pas à l'état Fermé. S'il n'existe aucun VI actif pour cette vulnérabilité, la **cote de risque** et le **score de risque** ne sont pas affichés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Entrée CWE	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux.
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Résumé	Description de la vulnérabilité.
Threat Intelligence (à partir de la Réponse aux vulnérabilités version 20.0)	Renseignements sur les menaces fournis par Qualys. Grâce à ces données, vous pouvez comprendre les motivations, les cibles et les comportements d'attaque d'un acteur malveillant.
Détails des vulnérabilités	
CVSS v2	Données CVSS v2 importées
CVSS v3	Données CVSS v3 importées, non disponibles avant 2015.
Solution privilégiée	(Masqué lorsqu'aucun VIT n'est associé à la vulnérabilité) Solution de remplacement la plus élevée de la chaîne, dérivée des solutions référencées dans la vulnérabilité. S'il existe plus d'un remplacement le plus élevé dans la chaîne, aucune valeur n'est fixée. Toute valeur définie manuellement peut être écrasée lors des importations suivantes. La définition manuelle de cette valeur doit être effectuée sur l'élément vulnérable.
Exploitation CISA (Cet onglet n'est disponible que lorsque l'application CISA est installée.)	
Date d'échéance de CISA	Délai de résolution de la vulnérabilité.
Date d'ajout	Date à laquelle la vulnérabilité a été ajoutée au catalogue CISA.
Produit	Produit sur lequel la vulnérabilité a été identifiée.
Fournisseur/Projet	Fournisseur associé à la vulnérabilité identifiée.
Rançongiciel connu À partir de la v21.0 de Réponse aux vulnérabilités.	Sélectionné lorsque le champ **connu pour être utilisé dans les campagnes de rançongiciels** est ingéré à partir du catalogue des vulnérabilités connues exploitées (KEV) de CISA. Le marqueur est défini au niveau des vulnérabilités et expositions communes (CVE) et déployé jusqu'à l'entrée tierce (TPE).
État du rattrapage (Masqué lorsqu'aucun élément vulnérable n'est associé à la vulnérabilité)	
Exclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
Inclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité.
Liens connexes	
Mettre à jour le statut	Affiche la date et l'heure de la dernière mise à jour. Met à jour les éléments suivants : • État de la tâche de résolution • Score et notation du risque • Des mesures telles que les VIT actifs, le total des VIT de la section État de rattrapage
Listes connexes	
Éléments vulnérables	(Masqué lorsqu'aucun VIT n'est associé à la vulnérabilité) Éléments vulnérables associés à cette vulnérabilité.
Références de vulnérabilité	Informations sur la vulnérabilité provenant de sources externes, citées par NVD.
Exploite	Exploits associés à cette vulnérabilité.
Solutions	(Masqué lorsqu'aucun VIT n'est associé à la vulnérabilité) Toutes les Gestion des solutions pour vulnérabilités solutions d'intégration associées à cette vulnérabilité.
Faiblesses	Données de **faiblesse** importées associées à des vulnérabilités et expositions communes (CVE).
Logiciel vulnérable	(Masqué lorsqu'un logiciel est associé aux CVE) Données CPE (Common Platform Enumeration) importées associées à la vulnérabilité.
Kits de logiciel malveillants de vulnérabilité	Programme malveillant importé de diverses sources d'analyse, pour détecter une vulnérabilité.

Champs d'entrée de vulnérabilité CWE

Ces champs se trouvent sur les enregistrements répertoriés dans la table CWE [sn_vul_cwe].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID CWE	Identificateur de cette entrée de vulnérabilité. Cet identificateur est utilisé à la fois pour les catégories et les faiblesses, et est unique entre les deux ensembles de données.
Nom	Nom descriptif attribué à cet ID CWE.
Probabilité d'exploitation	Probabilité d'exploitation de la faiblesse, à l'échelle qualitative. L'un des suivants : • Inconnu • Faible • Moyen • Élevé
Position dans le top 10 OWASP	Position numérique de cette vulnérabilité dans la liste des 10 premiers de l'OWASP.
SANS à la position 25	Position numérique de cette vulnérabilité dans la liste des 25 premiers SAN.
Classe	Type de faiblesse
Statut	L'un des suivants : • Incomplet • Brouillon • Stable • Déconseillé • Obsolète • Instable
Abstraction	L'un des suivants : • Variante • Classe • Base • Composé
Mis à jour	Dernière mise à jour de l'enregistrement dans l'instance.
Domaines fonctionnels	Liste des domaines fonctionnels affectés. Par exemple, **Traitement des fichiers**. Renseigné uniquement pour les faiblesses 24/862.
Ressources affectées	Liste des ressources affectées. Par exemple, **Fichier** ou **Répertoire**. Renseigné uniquement pour les faiblesses 51/863.
URL	Article de la base de connaissances associé à cette vulnérabilité.
Description	Description de la vulnérabilité.
Exécution de l'intégration	Exécution d'intégration dans laquelle cette CWE a été importée.
Sections	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Informations supplémentaires	Descriptions des concepts logiciels qui expliquent davantage la faiblesse. Comprend: • Description étendue • Détails en arrière-plan • Notes
Méthodes de détection	Détails sur la façon dont vous pouvez détecter cette faiblesse dans une application.
Modes d'introduction	Les phases dans lesquelles la faiblesse est introduite, par exemple, la **mise en œuvre**, l'architecture **et la conception**, etc.
Exemples démonstratifs	Exemples de code de la faiblesse avec les descriptions qui les accompagnent.
Atténuations potentielles	Détails sur la façon de prévenir la faiblesse, y compris la phase du cycle de vie de l'application dans laquelle elle se produit et l'efficacité de l'atténuation.
Listes connexes	
Relations	CWE associés à cette vulnérabilité. Répertorie les relations entre cette CWE et d'autres. Peut inclure parent/enfant, suit/précède, requiredby/requires (pour les faiblesses composites), CanAlsoBe, PeerOf, MemberOf.
Exemples observés	Quelques CVE qui sont représentatives de cette faiblesse.
Conséquences courantes	Conséquences d'un exploit réussi, en termes de portée et d'impact. Par exemple : Champ d'application : Confidentialité Impact : lire les données de l'application
Adhésions	Adhésions CWE avec cette vulnérabilité.
Plateformes applicables	Plateformes associées à cette vulnérabilité.
Entrées de vulnérabilité de l'application	Autres entrées de vulnérabilité de l'application associées à l'une.
Références externes	Informations sur la vulnérabilité provenant de sources externes.

Champs d'entrée de vulnérabilité tierce

Ces champs se trouvent sur les enregistrements répertoriés dans la table Entrées de vulnérabilité tierce [sn_vul_third_party_entry].

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Version 16.0 : CVE	Plusieurs vulnérabilités et expositions courantes (CVE) associées à cette vulnérabilité tierce.
Source	Origine de la vulnérabilité : scanner ou test physique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour plus d'informations sur les cotes de risque, reportez-vous à la section Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité. **Remarque :** Cette **cote de risque** de base est différente de celle de l'enregistrement de solution **Cote de risque**
Score du risque	Quantité calculée de risque que l'élément vulnérable pose à votre environnement, en fonction du score de risque. **Remarque :** Ce **score de risque** de base est différent du **score de risque** de l'enregistrement de la solution. Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.
Gravité	Degré de gravité normalisé de cette vulnérabilité. Les cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Pour plus d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Créer une carte de Réponse aux vulnérabilités gravité.
Existence de l'exploit	Oui, si au moins un exploit est associé à cette vulnérabilité.
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter cette vulnérabilité.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour cette vulnérabilité.
VI actifs	Nombre d'éléments vulnérables associés à cette vulnérabilité, n'étant pas à l'état Fermé.
Catégorie	Classification fournie par l'intégration tierce. Aide à la tâche.
Type de rattrapage	Types d'actions de rattrapage. • Correctif • Changement de configuration • Correctif et changement de configuration • Contre-mesure
Entrée CWE	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux.
PCI	Lorsque la case est cochée, la vulnérabilité est marquée comme présentant un risque important d'exposition des informations de paiement.
Gravité PCI	Niveau de risque d'exposition des informations de paiement. [Qualys uniquement.]
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Résumé	Description de la vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Détails des vulnérabilités	
CVSS v2	Données CVSS v2 importées
CVSS v3	Données CVSS v3 importées, non disponibles avant 2015.
Menace	Description de la menace que représente cette vulnérabilité.
Solution privilégiée	Solution de remplacement la plus élevée de la chaîne, dérivée des solutions référencées dans la vulnérabilité. S'il existe plus d'un remplacement le plus élevé dans la chaîne, aucune valeur n'est fixée. Toute valeur définie manuellement peut être écrasée lors des importations suivantes. La définition manuelle de cette valeur doit être effectuée sur l'élément vulnérable.
Notes de rattrapage	Description de la solution de rattrapage extraite du fournisseur.
État du rattrapage	
Exclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
Inclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité.
Liens connexes	
Mettre à jour le statut	Affiche la date et l'heure de la dernière mise à jour. Met à jour les éléments suivants : • État de la tâche de résolution • Score et notation du risque • Des mesures telles que les VI actifs, le total des VI de la section État de rattrapage
Listes connexes	
Éléments vulnérables	Éléments vulnérables associés à cette vulnérabilité.
Références de vulnérabilité	Informations sur la vulnérabilité provenant de sources externes, citées par NVD.
CVE	Enregistrement CVE (Common Vulnerability Enumeration) associé à cette vulnérabilité.
Catégories	Catégories associées à cette vulnérabilité.
Exploite	Exploits associés à cette vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Kits de logiciel malveillants de vulnérabilité	Kits de logiciels malveillants associés à cette vulnérabilité.
Solutions (Rapid7)	Informations sur les solutions issues des intégrations de solutions Rapid7. Affiché lorsqu'il est disponible.
Cadres de travail de l'exploit	Cadres de travail d'exploitation associés à cette vulnérabilité.
Solutions	Gestion des solutions pour vulnérabilités Solutions associées à cette vulnérabilité.
Exploitation CISA	
CISA existe	L'exploit CISA existe pour la table Entrée de vulnérabilités tierces.
Date d'échéance de CISA	Délai de résolution de la vulnérabilité.

Champs du formulaire de tâche de rattrapage

Grâce aux tâches de rattrapage, l'analyste peut surveiller les progrès et piloter le processus de médiation plus efficacement.

Ces champs se trouvent sur les enregistrements répertoriés dans la table Tâche de rattrapage [sn_vul_vulnerability].

Pour afficher les données importées dans les champs répertoriés dans les tables suivantes, vous devez avoir, au minimum, le rôle sn_vul.read_all.

Champs de tâche de rattrapage

Champ	Description
Numéro	Numéro d'élément vulnérable (VI) généré automatiquement pour cet enregistrement.
Cote de risque	Déploiement des scores de risque de l'élément vulnérable séparés en plages : critique, élevé, moyen, faible et aucun. Pour plus d'informations sur les cotes de risque, reportez-vous à la section Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité. **Remarque :** Cette **cote de risque** de base est différente de la cote de **risque** de l'enregistrement de la solution.
Score du risque	Déploiement des scores des risques de tous les éléments vulnérables associés à cette tâche de rattrapage. Quantité de risque que les éléments vulnérables, collectivement, présentent pour votre environnement. **Remarque :** Ce **score de risque** de base est différent du **score de risque** de l'enregistrement de la solution.
Cible de remédiation	Date à laquelle les éléments vulnérables doivent être corrigés, dès lors qu'ils ont été identifiés pour la première fois. Pour plus d'informations sur les cibles de rattrapage, reportez-vous à la section Réponse aux vulnérabilités Règles de cibles de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

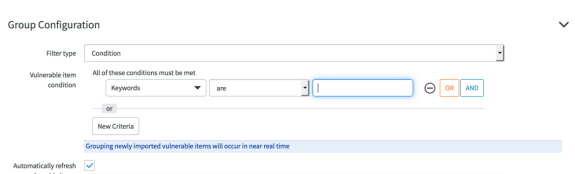
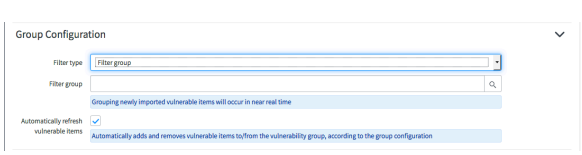
Champs de tâche de rattrapage (suite)

Champ	Description
Statut de la remédiation	État du rattrapage pour la tâche. Elle est déterminée par l'élément vulnérable dont la date d'échéance est la plus proche. Pour les groupes ouverts, les états comprennent : • En cours • Cible presque atteinte • Cible manquée Pour les groupes fermés, les états comprennent : • Pas de cible • Cible atteinte • Cible manquée Pour les dates cibles de rattrapage calculées, si la tâche est fermée, l'état global du rattrapage de tous les éléments vulnérables fermés est affiché dans la tâche. Ceux-ci déterminent si la tâche a atteint sa date ou non. L'état de rattrapage d'une tâche fermée est **Aucune cible** si aucun de ses éléments fermés n'avait de date cible de rattrapage. La **cible est manquée** si l'un de ses éléments fermés n'a pas atteint sa date cible. Elle **est atteinte** si au moins un VI fermé a atteint sa cible et qu'aucun des autres ne l'a manquée.
État	État d'avancement de la tâche. Les États comprennent : • Ouvert • En cours d'examen • En attente d'implémentation • Différé • En cours de révision • Résolu • Fermé Pour en savoir plus sur les états, consultez Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables.
Date de fin pour la réduction du risque	Date d'expiration des contrôles compensatoires appliqués à la tâche de rattrapage. **Remarque :** Ce champ s'affiche uniquement lorsque la valeur est disponible.
Groupe d'affectation	Groupe sélectionné pour travailler sur cette tâche de rattrapage.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cette vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

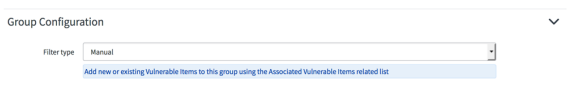
Champs de tâche de rattrapage (suite)

Champ	Description
Créées	Date de création de cette tâche de rattrapage.
Mis à jour	Date de la dernière mise à jour de cette tâche de rattrapage.
Vulnérabilité	Vulnérabilité applicable à la tâche. (Visible lorsque le groupe est formé en fonction d'une vulnérabilité unique.)
Description brève	Brève description de cette tâche de rattrapage.
En cours de révision (visible lorsque le RT est à l'état En cours de révision)	
Demandé par	Personne ayant demandé le report.
Motif souhaité	Motif du report.
État souhaité	État demandé à l'approbateur.
Sous-état souhaité	Le motif demandé à l'approbateur.
Report (visible lorsque la tâche est à l'état Différé)	
Différé par	Personne ayant reporté la tâche.
Différer l'expiration	Date d'expiration du report.
Motif de différer	Motif du report.
Résolution (visible lorsque le RT est à l'état Résolu)	
Résolu par	Personne ayant résolu la tâche de rattrapage.
Date de résolution	Date à laquelle la tâche de rattrapage a été résolue.
Notes de résolution	Informations supplémentaires.
Fermer (visible lorsque le RT est à l'état Fermé)	
Fermé par	Personne ayant résolu la tâche de rattrapage.
Fermé	Date à laquelle la tâche de rattrapage a été fermée.
Fermer les notes	Informations supplémentaires.
Configuration du groupe (visible dans tous les états)	
Type de filtre	Type de filtrage utilisé pour sélectionner les vulnérabilités du groupe : **Condition**  **Remarque :** Actualise une fois par heure. **Groupe de filtres** 

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de tâche de rattrapage (suite)

Champ	Description
	Remarque : Actualise une fois par heure. **Manuel** 
État du rattrapage	
Exclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs au sein de cette tâche. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre total d'éléments vulnérables au sein de cette tâche. Ce nombre exclut les éléments vulnérables différés.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables au sein de cette tâche. Ce nombre exclut les éléments vulnérables différés.
Inclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs au sein de cette tâche.
VI totaux	Nombre total d'éléments vulnérables au sein de cette tâche.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables au sein de cette tâche.
Notes (visibles dans tous les états)	
Description	Description du groupe ou des actions de rattrapage.
Commentaires supplémentaires	Informations supplémentaires.
Activités	Notes système.
Liens connexes	
Analyser à nouveau des éléments vulnérables	Déclenche une nouvelle analyse des éléments vulnérables pour déterminer s'ils sont corrigés.
Mettre à jour l'état	Affiche la date et l'heure de la dernière mise à jour. Répète les éléments suivants à partir des VI dans la tâche : • État de la tâche de résolution • Scores et cotes de risque • Date cible et statut du rattrapage (le cas échéant) • Des mesures telles que les VI actifs, le total des VI de la section État de rattrapage
Listes connexes	
Éléments vulnérables	Éléments vulnérables dans cette tâche.
SLA de tâche	SLA de plateforme associés à cette tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de tâche de rattrapage (suite)

Champ	Description
Solutions privilégiées	Solutions préférées des éléments vulnérables dans cette tâche.
Demandes de changement	Demandes de changement associées à cette tâche.
Approbations demandées	(Visible lorsque la tâche est à l'état En cours de révision.) Liste d'approbateurs. Une fois le report approuvé, la tâche de rattrapage passe à l'état Différé.

Champs de formulaire de configuration du questionnaire

Vous pouvez définir un questionnaire distinct pour une collection distincte de vulnérabilités ou de tâches de rattrapage en filtrant les vulnérabilités ou les tâches de rattrapage respectivement dans la section Configuration du questionnaire VR du formulaire Paramètres pour la gestion des exceptions VR.

Le formulaire Configuration du questionnaire s'affiche lorsque vous sélectionnez le bouton **Nouveau** dans la section Configuration du questionnaire VR du formulaire Paramètres pour la gestion des exceptions VR.

Champs de formulaire de configuration du questionnaire

Champ	Description
Nom	Nom du questionnaire.
Règle d'approbation	Règle d'approbation à laquelle le questionnaire s'applique. • **Demande d'exception pour les groupes de vulnérabilités** • **Demande d'exception pour les éléments vulnérables** • **Faux positif pour les groupes de vulnérabilité** • **Faux positif pour les éléments vulnérables** • **Questionnaire pour les contrôles de compensation des groupes vulnérables** pour les demandes de réduction des risques de la tâche de rattrapage. • **Questionnaire pour les contrôles de compensation des éléments vulnérables** pour les demandes de réduction de risque d'éléments vulnérables.
Description	Brève description de la configuration du questionnaire.
Ordre	Le questionnaire avec l'ordre le plus bas s'affiche pendant les demandes.
Actif	Activé par défaut, ce qui signifie que le questionnaire est en cours d'utilisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire de configuration du questionnaire (suite)

Champ	Description
Table	Table pour laquelle la règle d'approbation s'applique. • Élément vulnérable [sn_vul_vulnerable_item pour les règles d'approbation relatives aux éléments vulnérables. • Tâche de rattrapage [sn_vul_vulnerability] pour les règles d'approbation associées aux tâches de rattrapage.
Condition	Condition pour les enregistrements pour lesquels le questionnaire doit apparaître. Vous pouvez appliquer une condition sur tous les champs d'un élément vulnérable et d'une tâche de rattrapage, à l'exception du **motif**.
Questionnaire	Questionnaire qui s'affiche lorsqu'un propriétaire de rattrapage demande une exception, un faux positif ou une réduction du risque.

Information associée

Configurer la gestion des exceptions pour Réponse aux vulnérabilités

Configurer le questionnaire pour la réduction des risques

Réponse aux vulnérabilités Champs de formulaire d'élément vulnérable

Les éléments vulnérables sont automatiquement créés lors des importations d'intégrations de vulnérabilités tierces.

Champs d'éléments vulnérables

Pour afficher les données importées dans les champs répertoriés dans les tables suivantes, vous devez avoir, au minimum, le rôle sn_vul.read_all.

Ces champs se trouvent sur les enregistrements répertoriés dans la table Éléments vulnérables [sn_vul_vulnerable_item].

Si vous avez activé l'analyse de vulnérabilité NVD SAM, les enregistrements sont comparés au logiciel dans votre Base de données de gestion des configurations (CMDB) et des correspondances sont trouvées avec des logiciels ou des éléments de configuration (CI) vulnérables.

Champ	Description
Sélectionner une balise de sécurité	Balise de sécurité pour ajouter des métadonnées à l'enregistrement ou identifier qui doit avoir accès à cet enregistrement d'incident de sécurité. Ce champ n'apparaît qu'une fois que l'élément vulnérable a été enregistré.
Numéro	Numéro d'élément vulnérable généré automatiquement pour cet enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Scanner qui a trouvé cet élément vulnérable.
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour plus d'informations sur les évaluations de risque, reportez-vous à Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité. **Remarque :** Cette **cote de risque** de base est différente de la **cote de risque** de l'enregistrement de la solution.
Score du risque	Quantité calculée de risque que l'élément vulnérable pose à votre environnement. **Remarque :** Ce **score de risque** de base est différent du score de risque de l'enregistrement de la solution . Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.
Vulnérabilité	ID de la vulnérabilité associée à cet élément vulnérable.
Élément de configuration	Actif affecté.
État	Ce champ est défini par défaut sur **Ouvert**, mais vous pouvez le changer en **En cours d'examen** si la vulnérabilité est prête pour un rattrapage immédiat.
Date de fin pour la réduction du risque	Date à laquelle les contrôles compensatoires appliqués à l'élément vulnérable expirent. **Remarque :** Ce champ est disponible uniquement lorsque la valeur du score de risque d'origine est disponible.
Groupe d'affectation	Groupe sélectionné pour travailler sur cette tâche de rattrapage.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cette vulnérabilité.
Créées	Date à laquelle cet élément vulnérable a été créé dans votre instance.
Dernières ouvertures	Date à laquelle l'élément vulnérable a été ouvert pour la dernière fois dans votre instance. Initialement, il s'agit de la même chose que la date de création de l'élément vulnérable. Cependant, s'il a été fermé puis rouvert, la date de la dernière ouverture contient la date et l'heure de la réouverture.
Mis à jour	Date de la dernière analyse.
Âge	Durée pendant laquelle le VI a été actif depuis la date de sa dernière ouverture. Si le VI est fermé, la valeur du champ Âge est définie sur zéro. Pour plus d'informations sur le champ Âge, reportez-vous à la section Calcul et affichage de l'âge de l'élément vulnérable. Pour plus d'informations sur la personnalisation du calcul de la durée de l'âge, consultez l'article KB1703270 .
Vulnérabilité	
Résumé	Description de la vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Gravité	Degré de gravité normalisé de cette vulnérabilité. Les cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Pour plus d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Créer une carte de Réponse aux vulnérabilités gravité.
Score de vulnérabilité (v3)	Score CVSS v3.
Score de vulnérabilité (v2)	Score CVSS v2.
Existence de l'exploit	Oui, si au moins un exploit est associé aux vulnérabilités associées à cet élément vulnérable.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour les vulnérabilités associées à cet élément vulnérable.
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter les vulnérabilités associées à cet élément vulnérable.
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Menace	Informations pertinentes sur la menace. Extrait de l'enregistrement d'entrée vulnérable. **Remarque :** Tous les changements apportés ici mettent à jour l'enregistrement de l'entrée vulnérable.
Notes de rattrapage	Solution pertinente à la menace, extraite de l'enregistrement d'entrée vulnérable.
Rattrapage Disponible uniquement avec Gestion des solutions pour vulnérabilités.	
Solution privilégiée	Solution préférée importée à partir de l'enregistrement de vulnérabilité. **Remarque :** Les changements manuels apportés ici ne modifient pas l'enregistrement de vulnérabilité et restent inchangés sur l'élément vulnérable lors des importations suivantes.
Résumé	Résumé importé à partir de l'enregistrement de la solution.
Type de solution	Solution potentielle ou privilégiée.
Détection initiale	
Nom DNS	Nom du nom de domaine Nom de service. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il existe.
Nom NetBIOS	Nom du NetBIOS. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il existe.
Adresse IP	Adresse IPv4 ou IPv6. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il existe.
Port	Adresse du port
Protocole	Nom du protocole.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
SSL	Indique si le chiffrement SSL est utilisé ou non.
Détections	
Statut	État de la détection.
Premier trouvé	Date à laquelle la source tierce a trouvé la détection sur cet actif pour la première fois.
Dernier trouvé	Date à laquelle la source tierce a détecté cet actif pour la dernière fois.
Nom DNS	Nom du nom de domaine Nom de service. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il existe.
Nom NetBIOS	Nom du NetBIOS. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il existe.
Adresse IP	Adresse IPv4 ou IPv6. Si aucun CI n'est fourni, ce champ est utilisé pour rechercher un CI correspondant, s'il existe.
Port	Adresse du port
Protocole	Nom du protocole.
SSL	Indique si le chiffrement SSL est utilisé ou non.
Durées trouvées	Nombre de fois où cette vulnérabilité a été détectée sur cet actif par la source tierce.
Exécution de l'intégration	Exécution de l'intégration qui a importé la détection.
Fermer Disponible une fois que l'élément vulnérable a été corrigé et fermé. Les éléments de cette section sont en lecture seule.	
Fermé par	Qui a fermé l'élément vulnérable.
Fermé	Date à laquelle l'élément vulnérable a été fermé.
Fermer les notes	Informations incluses dans la fermeture.
Âge à la fermeture	Période après laquelle l'élément vulnérable a été fermé. Si le VI est rouvert, la valeur du champ Âge fermé est définie sur zéro. Pour plus d'informations sur la fermeture du champ Âge, reportez-vous à la section Calcul et affichage de l'âge de l'élément vulnérable. Pour plus d'informations sur la personnalisation du calcul de la durée d'âge fermé, consultez l'article KB1703270 .
Notes	
Commentaires/ notes de travail supplémentaires	Toute information pertinente. Cochez cette case pour ajouter des commentaires supplémentaires. Réponse aux vulnérabilités À partir de la version 20.0, vous pouvez ajouter des notes de travail dans la section Notes pour un élément vulnérable différé.
Activité	S'affiche uniquement lorsqu'une note de travail a été créée.
Liens connexes	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Calculer le score de risque	Lorsque les calculateurs de **gravité de la vulnérabilité** ou de **score de risque** sont activés, le champ **Score de risque** est mis à jour.

Voici les listes connexes des éléments vulnérables.

Liste connexe	Description
Tâches de remédiation	Tâches associées à cet élément vulnérable.
Affectation des tâches	Tâches associées à cet élément vulnérable.
Adresses IP associées	Disponible si l'application Qualys Vulnerability Integration Vulnerability Integration est installée. Adresses IP trouvées lors de la déduplication.
Services concernés	Services d'entreprise touchés par cet élément vulnérable. Affiché lorsque ces informations sont disponibles dans l'enregistrement cmdb . Ces informations peuvent être saisies manuellement ou à l'aide de l'application ServiceNow® Mappage des services . Voir Mappage des services pour plus d'informations. Si un CI affecté associé à l'élément vulnérable est ajouté ou mis à jour, les informations de cette liste connexe sont automatiquement mises à jour lors de la sauvegarde de l'enregistrement.
Approbations de changement de l'état	État des demandes de changement et autres informations d'approbation associées au VIT.
Tickets Qualys	Qualys Informations d'intégration de ticket associées à cet élément vulnérable.

Champs du formulaire Solution

Les solutions sont créées automatiquement lorsque les enregistrements sont téléchargés à partir d'intégrations de solutions tierces et stockés sous **Solutions** dans Réponse aux vulnérabilités.

Champs d'entrée d'intégration de solution

Les champs importés dans cette table sont en lecture seule.

Champ	Description
Numéro	Identificateur affecté à la solution.
Source	Origine de la solution.
ID source	Identificateur de source pour cette solution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Cote de risque	Sépare le score de **risque** de l'enregistrement de solution en plages allant de Critique à Aucun. Pour plus d'informations sur la **solution Cote de risque**, reportez-vous à Gestion des solutions pour vulnérabilités. **Remarque :** La **cote de risque** de la solution est différente de celle **des enregistrementsd'élément vulnérable**, **d'entrée de vulnérabilité tierce** et de **tâche de rattrapage**.
Score du risque	Calcul pondéré basé sur le **score de risque** et le nombre d'éléments vulnérables avec cette solution **comme solution privilégiée**. Pour en savoir plus sur le score de risque de la solution, reportez-vous à la section Gestion des solutions pour vulnérabilités. **Remarque :** Enregistrement de solution Le **score de risque** est différent **des enregistrementsd'élément vulnérable**, **d'entrée de vulnérabilité tierce** et de **tâches de remédiation**. Disponible lorsque NVD SAM est activé, mais si aucun élément vulnérable (VI) actif n'est associé à une vulnérabilité, le **score de risque** de la solution est défini sur zéro.
Priorité la plus élevée	Indique qu'aucune solution ne la remplace.
Type de solution	Quel genre de solution c'est. Les choix possibles sont les suivants : • Solution de contournement • Atténuation • Correction du fournisseur • Correctif • Déploiement • Droit • Ne corrigera pas • Aucun disponible
Nécessite le redémarrage	Redémarrage nécessaire. Les choix possibles sont les suivants : • Oui • Non • Peut-être
Date de publication	Date à laquelle la vulnérabilité a été publiée par source.
Dernière modification	Date de la dernière modification de la vulnérabilité par la source.
Résumé	Résumé de la correction de la solution.
Bulletin	Bulletin de sécurité associé à la solution.
Catégories de produits	Catégories de produits auxquelles la solution s'applique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Produits	Produits auxquels la solution s’applique.
Détails des solutions	
Description	Si aucun contenu n’est disponible à partir de la source de solution, vous êtes dirigé vers une autre section ou solution pertinente pour plus d’informations.
Liens	Ressources Internet importées associées à la solution.
Détails des vulnérabilités	
Notes de vulnérabilité	Résumé des vulnérabilités corrigées par la solution.
État du rattrapage	
Cibles de solutions privilégiées État du rattrapage pour les éléments vulnérables et leurs éléments de configuration (CI) uniques, pour lesquels il s’agit de la solution privilégiée. **Remarque :** Un CI unique est un CI qui n’est compté qu’une seule fois, quel que soit le nombre de VI auxquels il est associé.	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre d'éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
% des VI rattrapés	Pourcentage complet pour le rattrapage d’éléments vulnérables (VI). S’applique aux éléments vulnérables pour lesquels cette solution est préférée. Ce nombre exclut les VI différés.
CI restants	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les CI des éléments vulnérables différés.
CI totaux	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage. Ce nombre exclut les CI des éléments vulnérables différés.
% des CI rattrapés	Pourcentage complet de CI uniques rattrapés (ce qui signifie que tous les VI pour ce CI et cette solution sont rattrapés). Déterminé par le nombre de CI rattrapés par rapport au total des CI uniques associés à des éléments vulnérables avec la solution privilégiée. Ce nombre exclut les CI des éléments vulnérables différés.
Cibles de solutions préférées (inclut les éléments différés) État du rattrapage pour les éléments vulnérables et leurs CI uniques, y compris les éléments différés, pour lesquels il s’agit de la solution privilégiée.	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est préférée pour le rattrapage.
VI totaux	Nombre d'éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage.
% des VI rattrapés	Pourcentage complet pour le rattrapage d’éléments vulnérables (VI). S’applique aux éléments vulnérables pour lesquels cette solution est préférée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
CI restants	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est préférée pour le rattrapage.
CI totaux	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs et fermés pour lesquels cette solution est préférée pour le rattrapage.
% des CI rattrapés	Pourcentage complet de CI uniques rattrapés (ce qui signifie que tous les VI pour ce CI et cette solution sont rattrapés). Déterminé par le nombre de CI rattrapés par rapport au total des CI uniques associés à des éléments vulnérables avec la solution privilégiée. Ce nombre exclut les CI des éléments vulnérables différés.
Cibles de solutions potentielles État du rattrapage pour les éléments vulnérables et leurs CI uniques, avec une vulnérabilité associée à cette solution.	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est une solution possible pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
CI restants	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est une solution possible pour le rattrapage. Ce nombre exclut les éléments vulnérables différés.
Cibles de solutions potentielles (y compris les éléments différés) État du rattrapage pour les éléments vulnérables et leurs CI uniques, y compris les éléments différés, avec une vulnérabilité qui peut être corrigée par cette solution, y compris les nombres de solutions privilégiées.	
Éléments vulnérables	Nombre d'éléments vulnérables actifs (non fermés) pour lesquels cette solution est une solution possible pour le rattrapage.
CI restants	Nombre de CI uniques associés à un ou plusieurs éléments vulnérables actifs pour lesquels cette solution est une solution possible pour le rattrapage.
Notes	
Notes internes	Champ modifiable fourni pour le spécialiste du rattrapage.
Liens connexes	
Mettre à jour le statut	Date et heure de la dernière mise à jour de l'état du rattrapage. Met à jour les éléments suivants : • État de la tâche de résolution • Score et notation du risque • Mesures de la section État du rattrapage
Listes connexes	
Éléments vulnérables	Éléments vulnérables associés à cette solution en tant que solution privilégiée pour le rattrapage.
Vulnérabilités tierces	Vulnérabilités tierces associées à cette solution.
CVE	Vulnérabilités courantes et vulnérabilités CVE (Common Vulnerability and Exposure) associées à cette solution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Tâches de remédiation	Tâches de rattrapage qui contiennent des éléments vulnérables connexes avec cette solution préférée pour le rattrapage.
Solutions précédentes	Solutions antérieures qui résolvent une ou plusieurs vulnérabilités de cette solution.
Solutions de remplacement	Solutions ultérieures qui résolvent toutes les vulnérabilités de cette solution. Cette liste est vide lorsque la case de **priorité la plus élevée** est cochée.

Configurations de workflow d'approbation pour la demande de désaffectation

Vous pouvez concevoir le workflow d'approbation pour la suppression des affectations des éléments vulnérables (VI, VIT), des tâches de rattrapage, des éléments vulnérables de l'application (AVIT) et des éléments vulnérables de conteneurs (CVIT) pour vous et votre groupe.

VIT, tâche de rattrapage, AVIT et CVIT ont chacun une règle d'approbation par défaut. Chaque règle d'approbation a une configuration d'approbation par défaut. Chaque configuration d'approbation a un niveau d'approbateur par défaut. Les règles d'approbation pour les VIT, la tâche de rattrapage, AVIT et CVIT sont activées par défaut. En tant qu'administrateur, vous pouvez effectuer les actions suivantes en accédant à **Tous** > **Réponse aux vulnérabilités** > **Mes approbations** > **Règles d'approbation** et la sélection de la règle d'approbation appropriée.

- Activer ou désactiver une règle d'approbation.
- Créez et mettez à jour une configuration d'approbation.
- Définissez les conditions pour les éléments vulnérables et les tâches de rattrapage auxquelles s'appliquent les règles d'approbation.
- Créez et mettez à jour plusieurs niveaux d'approbateur.

Le tableau suivant présente les règles d'approbation, les configurations d'approbation et les niveaux d'approbateur par défaut pour un VIT, une tâche de rattrapage, AVIT et CVIT fournis avec le système de base.

Règles d'approbation, configurations d'approbation et niveaux d'approbateur par défaut

Type	Règle d'approbation	Configuration de l'approbation	Niveaux de l'approbateur
VIT ou VI	Demande de modification du champ d'élément vulnérable	Demande de modification du champ d'élément vulnérable	Niveau 1 : Annuler l'affectation de la demande pour VI
Tâche de rattrapage	Demande de modification du champ Groupe de vulnérabilité	Demande de changement du champ de vulnérabilité	Niveau 1 : annuler l'affectation de la demande pour VG
AVIT (traduction dynamique)	Demande de modification du champ d'élément vulnérable d'application	Demande de changement de champ de vulnérabilité de l'application	Annuler l'affectation de l'élément de vulnérabilité de l'application

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles d'approbation, configurations d'approbation et niveaux d'approbateur par défaut (suite)

Type	Règle d'approbation	Configuration de l'approbation	Niveaux de l'approbateur
CVIT	Approbation de la gestion du conteneur	Configuration par défaut de la désaffectation du CVIT	Niveau d'approbation de désaffectation du CVIT : 1

Pour en savoir plus sur l'approbation des demandes de désaffectation, reportez-vous à la section Approuver ou rejeter une demande de désaffectation dans Réponse aux vulnérabilités.

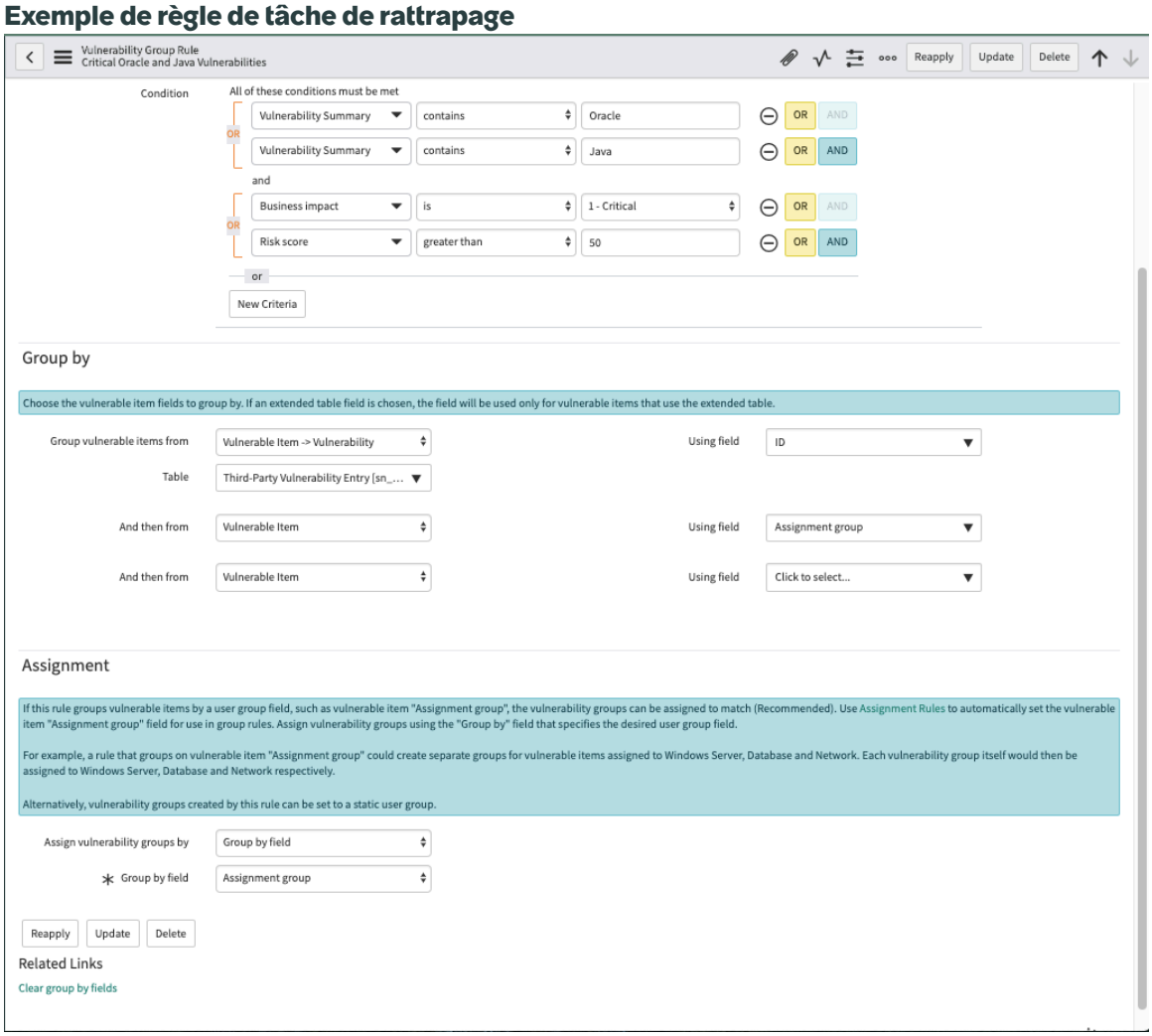
Réponse aux vulnérabilités Exemples de règles de tâches de rattrapage

Exemples de règles de tâche de rattrapage utilisant la vulnérabilité et le risque, ou l'impact, ou l'élément de configuration (CI).

Règle de la tâche de rattrapage pour regrouper les éléments vulnérables Java et Oracle à haut risque

Cet exemple montre une procédure pas à pas de la règle qui regroupe les éléments vulnérables Java et Oracle par vulnérabilité et les affecte à leurs groupes de support respectifs.

Exemple de règle de tâche de rattrapage



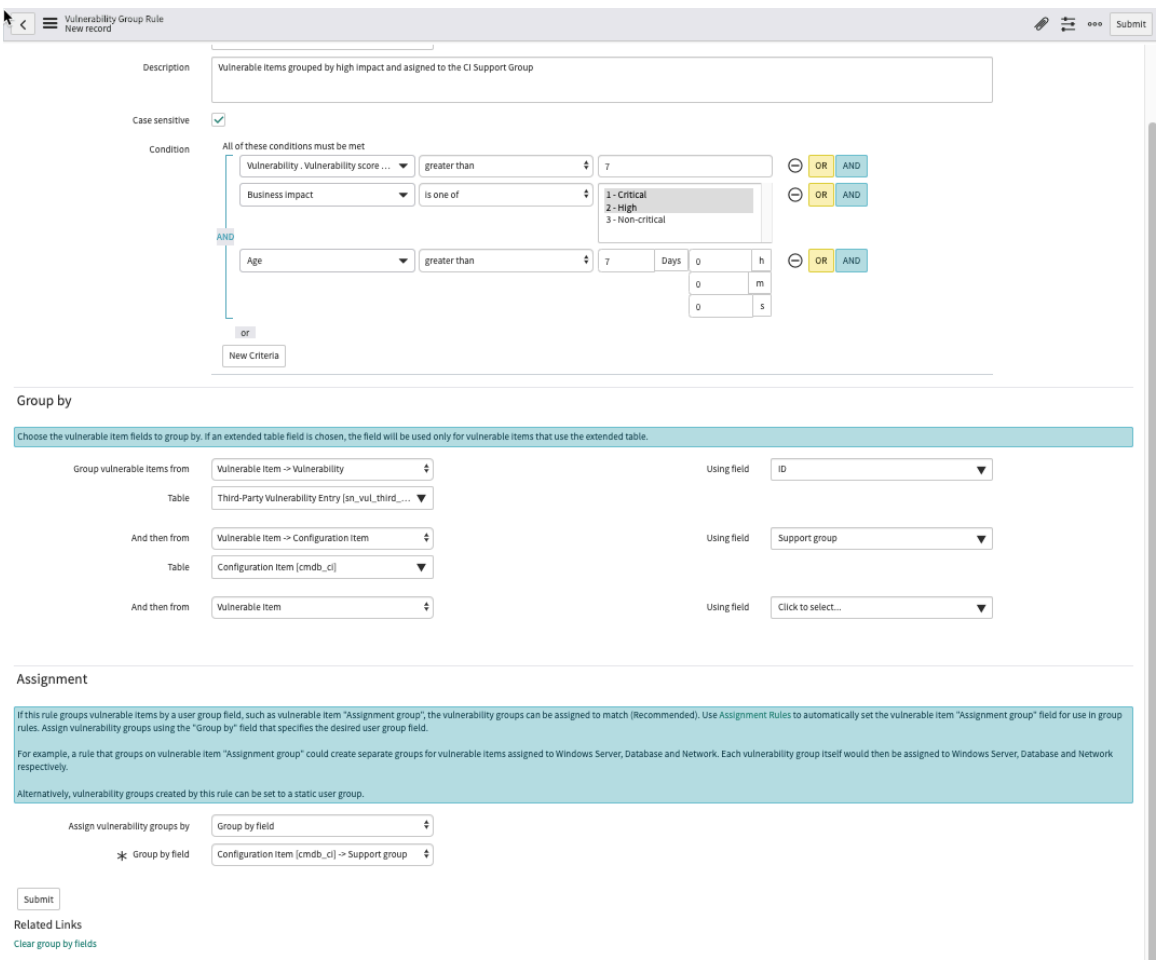
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cliquez avec le bouton droit dans l'en-tête pour **enregistrer**.

Règle de la tâche de rattrapage pour regrouper tous les éléments vulnérables à impact élevé par vulnérabilité et groupe de support de CI

Cet exemple montre les paramètres de champ de formulaire d'une règle de groupe pour les éléments vulnérables à impact élevé qui les affecte au groupe de support CI.

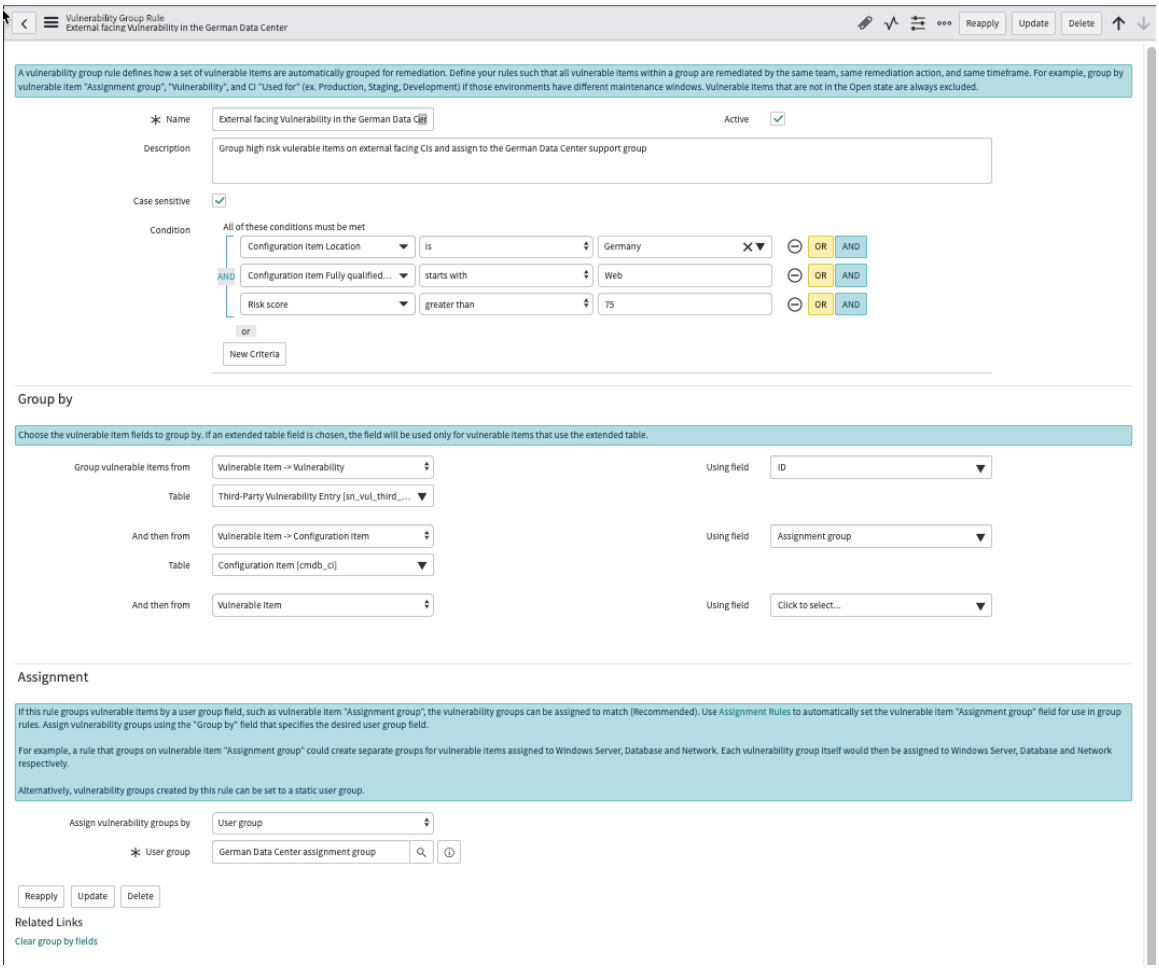


Règle de la tâche de rattrapage pour regrouper toutes les vulnérabilités à haut risque sur un CI orienté vers l'extérieur dans un centre de données allemand

Cet exemple montre les paramètres de champ de formulaire pour une règle de groupe pour les vulnérabilités à haut risque sur les CI orientés vers l'extérieur dans un centre de données allemand. Ils sont affectés au groupe d'affectation du centre de données allemand.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple de calcul de score de risque pour Réponse aux vulnérabilités

Vous pouvez déterminer les calculateurs de score de risque pour générer des scores de risque qui utilisent les données de vulnérabilité et d'actif propres à votre organisation.

Exemple de détermination des scores des calculateurs de règles de risque

L'exemple suivant montre comment les scores des calculateurs de règles de risque sont déterminés.

Supposons qu'un calculateur de règle de risque est configuré avec les champs de cette table :

Champ	Pondération	Répartition du poids
Vulnérabilité.Gravité	50	Par défaut : 20 1 - Critique : 100 2 - Élevé : 80 3 - Moyen : 60 4 - Faible : 40 5 - Aucun : 20

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Pondération	Répartition du poids
Vulnérabilité.Exploit existe	50	Par défaut : 50 Oui : 100 Non : 0

Supposons également que les éléments vulnérables affichés dans cette table sont présents dans le système :

ID	Gravité de la vulnérabilité	Existence d'une exploitation de la vulnérabilité
VIT00001	1 – Critique	1 - Oui
VIT00002	2 - Élevée	1 - Oui
VIT00003	3 : moyen	2 – Non
VIT00004	4 - Faible	2 – Non
VIT00005	5 : aucun	2 – Non

Le calcul du score de risque pour les éléments vulnérables est calculé en fonction de la formule suivante :

`Score de risque = (W(gravité) * FV (gravité). + W(exploitexiste) * FV(exploit existe)) / 100`

où **W** est le poids et **FV** est le pourcentage de poids de la valeur de champ.

Le score de risque résultant pour ces éléments vulnérables est décrit dans ce tableau :

ID	Gravité de la vulnérabilité (50 %)	Existence d'une exploitation de la vulnérabilité (50 %)	Score de risque résultant
VIT00001	1 – Critique (50 % x 100)	1 – Oui (50 % x 100)	100
VIT00002	2 – Élevé (50 % x 80)	1 – Oui (50 % x 100)	90.0
VIT00003	3 – Moyen (50 % x 60)	2 – Non (50 % x 0)	30
VIT00004	4 – Faible (50 % x 40)	2 – Non (50 % x 0)	20
VIT00005	5 : aucun (50 % x 20)	2 – Non (50 % x 0)	10

Remarque : Par VIT00005, étant donné que la valeur de gravité est vide, la pondération par défaut est appliquée.

Si le pourcentage de pondération est modifié pour l'une des valeurs de champ, consultez ce tableau pour connaître les résultats :

Champ	Pondération	Répartition du poids
Vulnérabilité.Gravité	50	• Par défaut : 20 • 1 - Critique : 100 • **2 - Élevé : 70**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Pondération	Répartition du poids
		*Valeur révisée • 3 - Moyen : 60 • 4 - Faible : 40
Vulnérabilité.Exploit existe	50	• Par défaut : 50 • Oui : 100 • Non : 0

Le score de risque pour les éléments vulnérables après réapplication du calculateur est indiqué dans cette table :

ID	Gravité de la vulnérabilité (50 %)	Existence d'une exploitation de la vulnérabilité (50 %)	Score de risque résultant
VIT00001	1 – Critique (50 % x 100)	1 – Oui (50 % x 100)	100
VIT00002	**2 – Élevé (50 % x 70)** *Valeur révisée	1 – Oui (50 % x 100)	**85** *Valeur révisée
VIT00003	3 – Moyen (50 % x 60)	2 – Non (50 % x 0)	30
VIT00004	4 – Faible (50 % x 40)	2 – Non (50 % x 0)	20
VIT00005	5 : aucun (50 % x 20)	2 – Non (50 % x 0)	10

Gestion des erreurs pour les détections

Les erreurs sont consignées lors de la création de détections ou de la création et de la mise à jour des éléments vulnérables lors du traitement des pièces jointes. Si un processus d'intégration de vulnérabilité échoue, les erreurs sont enregistrées dans l'onglet « Journal des intégrations de vulnérabilité ».

Ces erreurs sont consignées dans l'une des catégories suivantes.

Champ	Description
Création de VI	Erreur lors de la création ou de la mise à jour de la détection.
Détection	Erreur lors de la création d'une détection.

Expérience mobile pour Réponse aux vulnérabilités

En tant que propriétaire de rattrapage, vous pouvez accéder à l'application Réponse aux vulnérabilités (VR) sur votre instance ServiceNow AI Platform® avec votre équipement mobile Android ou iOS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Réponse aux vulnérabilités

Pour vous familiariser avec les concepts de Vulnerability Response et comment ce produit peut aider votre organisation, consultez Présentation de Vulnerability Response.

Remarque : Avant d'installer le Application Vulnerability Response Mobile mobile, familiarisez-vous avec le Agent mobile .

Vue d'ensemble

En tant qu'utilisateur disposant du rôle de propriétaire du rattrapage (sn_vul.remediation_owner), il vous permet d'afficher Application Vulnerability Response Mobile et de rechercher les vulnérabilités, les tâches de rattrapage et les affectations sur votre instance directement à partir de votre ServiceNow AI PlatformAndroidiOS appareil mobile.

Vous êtes notifié lorsque des tâches de rattrapage (RT) ou des VI vous ont été affectées ou ont été affectées à vous ou à votre groupe d'affectation. Cette application donne à un propriétaire de rattrapage la possibilité de réaffecter, de modifier des champs et de commencer le rattrapage sans être lié au bureau.

Vous avez accès aux vulnérabilités, aux éléments de vulnérabilité, aux modules et à toutes les solutions. Vous pouvez effectuer les tâches suivantes sur votre équipement mobile :

- Affichez et mettez à jour les tâches de rattrapage.
- Affichez les demandes de changement.
- Réaffectez une tâche de rattrapage ou un élément de vulnérabilité à un autre membre d'un groupe d'affectation.
- Affichez les notifications lorsqu'une tâche de rattrapage critique vous est affectée ou à l'un de vos groupes d'affectation.
- Modifiez un sous-ensemble de champs sur les enregistrements de tâche de rattrapage.
- Recherchez les tâches de rattrapage qui correspondent à des critères de recherche spécifiques.

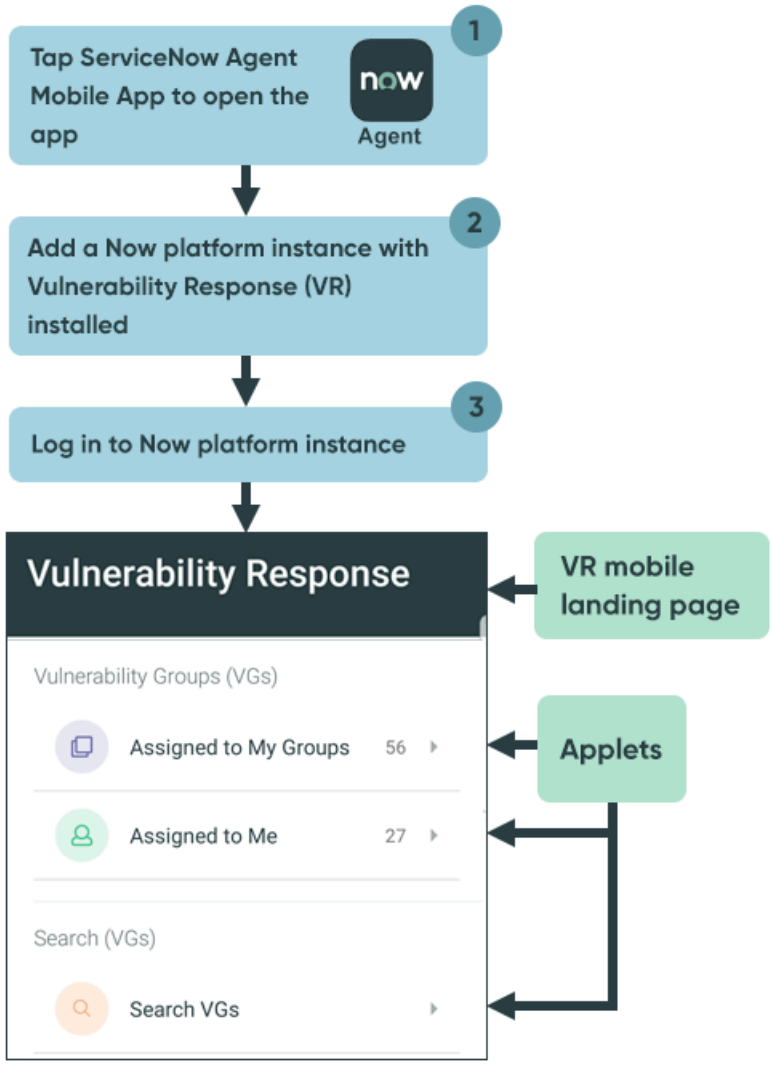
La figure suivante illustre la façon dont vous vous connectez à votre ServiceNow AI Platform instance à partir de votre équipement mobile et l'écran d'accueil qui s'affiche Application Vulnerability Response Mobile après votre connexion.

Pour obtenir des instructions détaillées sur la configuration de votre ServiceNow AI Platform instance et l'installation de , reportez-vous à la Application Vulnerability Response Mobile section Configurer une liste de vérification pour le Application Vulnerability Response Mobile. Pour obtenir des instructions sur la façon de se connecter, reportez-vous à la section Connectez-vous au Application Vulnerability Response Mobile.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application Vulnerability Response Mobile



Traduction automatique

Applications

Les applications sont les ServiceNow composants logiciels tels que Réponse aux incidents de sécurité (SIR), Réponse aux vulnérabilités (VR), Gouvernance, risque et conformité (GRC) et d'autres produits qui fournissent des fonctions et des fonctionnalités spécifiques au sein de ServiceNow votre ServiceNow AI Platform instance. Une fois que vous avez installé les applications principales qui disposent d'applications mobiles sur votre ServiceNow AI Platform instance, ces applications s'affichent sous forme d'icônes sous votre appareil mobile.

Icône Réponse aux vulnérabilités sur un appareil mobile

Dossiers

Chaque ServiceNow® Mobile application contient des dossiers qui séparent les applets par catégories. Dans l'image précédente, les tâches de rattrapage et les recherches (VG) sont les dossiers du Application Vulnerability Response Mobile fichier .

Applets

Les applets sont les différentes options au sein de l'application. Dans l'image précédente, les icônes sous Tâches de rattrapage et Recherche (VG) sont les applets disponibles pour le Application Vulnerability Response Mobile.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consultez les rubriques suivantes pour en savoir plus sur les applets du Application Vulnerability Response Mobile fichier .

Configurer une liste de vérification pour le Application Vulnerability Response Mobile

La liste de vérification suivante comprend les tâches de configuration que vous devez accomplir dans votre ServiceNow AI Platform® instance et sur votre équipement mobile avant d'utiliser le Application Vulnerability Response Mobile.

Avant de commencer
Plus d'informations suivent chaque étape dans la colonne de droite. Temps estimé pour accomplir cette tâche : 15 à 20 minutes.

Rôles requis : admin, sn_vul.remediation_owner

Vous avez correctement configuré votre équipement mobile pour le Application Vulnerability Response Mobile. L'étape suivante consiste à vous connecter Application Vulnerability Response Mobile et à ajouter une ServiceNow AI Platform instance à votre appareil mobile.

Procédure

1. En option, imprimez cette liste de contrôle et utilisez-la pour vous guider dans les tâches nécessaires à l'installation du Application Vulnerability Response Mobile.
2. Vérifiez que chaque élément de la liste est terminé afin de pouvoir vous connecter Application Vulnerability Response Mobile et ajouter une ServiceNow AI Platform instance.

Liste de vérification mobile

Élément	Description
☐	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que l'application Réponse aux vulnérabilités principale est installée sur une ServiceNow AI Platform instance. Il s'agit de l'instance ServiceNow AI Platform que vous affichez sur votre appareil mobile. **Remarque :** L'application Réponse aux vulnérabilités principale et l'instance ServiceNow AI Platform doivent provenir de la même version familiale. **a.** Pour vérifier que l'application principale est installée sur votre instance, accédez à **Modules d'extension** et recherchez Réponse aux vulnérabilités. **b.** Si l'application principale n'est Réponse aux vulnérabilités pas déjà installée, cliquez sur **Installer** pour l'installer. Pour plus d'informations sur l'installation de l'application Réponse aux vulnérabilités principale, reportez-vous à la section Installer Réponse aux vulnérabilités. Pour plus d'informations sur l'obtention de l'application principale sur , l'obtention d'une Réponse aux vulnérabilités autorisation, l'installation des applications principales et l'activation des dépendances, reportez-vous à la section Opérations de sécurité et le ServiceNow Store.ServiceNow Store

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
☐	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que le dispositif Application Vulnerability Response Mobile est installé sur l'instance ServiceNow AI Platform que vous souhaitez afficher sur votre appareil mobile. **Remarque :** L'instance Application Vulnerability Response Mobile et doit ServiceNow AI Platform appartenir à la même version de famille. Le Application Vulnerability Response Mobile et l'application Réponse aux vulnérabilités doit être compatible. Pour plus d'informations sur la compatibilité des applications Vulnerability Response, consultez Vulnerability Response et Configuration Compliance Compatibility Matrix Téléchargez et installez le à partir de Application Vulnerability Response Mobile sur ServiceNow Store votre ServiceNow AI Platform instance. Lorsque vous installez le Application Vulnerability Response Mobile, ses dépendances, com.glide.sg et com.glide.sg.agent_native_client, sont également installées. Pour vérifier que ces dépendances sont installées : **a.** Accédez à la **Tous** > **Modules d'extension**. **b.** Recherchez les ID de module d'extension (com.glide.sg et com.glide.sg.agent_native_client). **c.** S'ils ne sont pas activés, activez ces modules d'extension. Ces modules d'extension sont requis pour le .Application Vulnerability Response Mobile Pour plus d'informations sur l'obtention de l'application Application Vulnerability Response Mobile le , l'obtention ServiceNow Store d'une autorisation, l'installation des applications et l'activation des dépendances, reportez-vous à la section Opérations de sécurité et le ServiceNow Store.
☐	En tant qu'utilisateur disposant du rôle administrateur, vérifiez dans votre ServiceNow AI Platform instance que vous avez affecté les utilisateurs mobiles avec les rôles requis ServiceNow AI Platform . **a.** Pour afficher les rôles affectés à un utilisateur, accédez à **Tous** > **Administration** > **Utilisateurs**. **b.** Sélectionnez le nom d'utilisateur suivi de la liste connexe Rôles. Tous les rôles affectés à cet utilisateur s'affichent. **c.** Vérifiez qu'un utilisateur est affecté ou affectez-lui un rôle itil (IT Infrastructure Library Library). Les utilisateurs disposant du rôle itil peuvent créer, ouvrir, mettre à jour et fermer des demandes de changement et des tâches de rattrapage. Seuls les utilisateurs ayant le rôle itil peuvent se voir affecter des tâches. **d.** Vérifiez qu'un utilisateur est affecté ou affectez-lui le rôle de propriétaire du rattrapage (sn_vul.remediation_owner). Les utilisateurs disposant du rôle sn_vul.remediation_owner peuvent lire les enregistrements de vulnérabilité et de solution. Ce rôle est automatiquement ajouté lorsque vous affectez le rôle itil. **e.** Vérifiez que vous avez créé tous les groupes d'affectation requis et affecté des utilisateurs mobiles à ces groupes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	Remarque : Si vous avez un grand nombre d'utilisateurs pour l'application mobile, vous pouvez également affecter le rôle sn_vul.remediation_owner à un groupe. Chaque utilisateur que vous ajoutez au groupe hérite de ce rôle. Pour plus d'informations sur les règles et les groupes d'affectation, reportez-vous à la section Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Pour plus d'informations sur les utilisateurs et l'affectation de rôles aux utilisateurs et aux groupes, voir Administration utilisateurs .
☐	En tant qu'utilisateur ayant le rôle de propriétaire du rattrapage (sn_vul.remediation_owner), téléchargez l'application Agent la plus récente ServiceNow® sur votre équipement mobile.  L'application Agent la plus récente est disponible sur l'App Store d'Apple iOS et le Google Play Store.
☐	En tant qu'utilisateur disposant du rôle sn_vul.remediation_owner, vérifiez que les notifications sont activées sur votre équipement mobile et dans votre ServiceNow AI Platform instance. Les notifications vous informent lorsque des tâches de rattrapage critiques vous sont affectées ou sont affectées à votre groupe d'affectation. Pour vous aider à corriger en temps opportun, après avoir activé les notifications, cliquez sur une notification dans le Application Vulnerability Response Mobile et accédez directement à l'enregistrement. Pour activer les notifications dans votre ServiceNow AI Platform instance afin qu'elles s'affichent sur votre appareil mobile, procédez comme suit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	a. Vérifiez que vous avez téléchargé et installé sur Application Vulnerability Response Mobile votre ServiceNow AI Platform instance. **b.** Dans Paramètres système de votre ServiceNow AI Platform instance, sous Notifications, vérifiez que vous avez activé **l'application mobile ServiceNow**. Pour plus d'informations sur la définition des notifications, reportez-vous à la section Définir les préférences de notification dans Interface utilisateur principale . ServiceNow AI Platform Les notifications sont également affichées sur l'écran Messages de votre appareil mobile. Vérifiez que les notifications sont également activées dans les paramètres de votre appareil mobile.

Connectez-vous au Application Vulnerability Response Mobile

Ouvrez l'application mobile Vulnerability Response et ajoutez une ServiceNow AI Platform instance avec Vulnerability Response à votre appareil mobile.

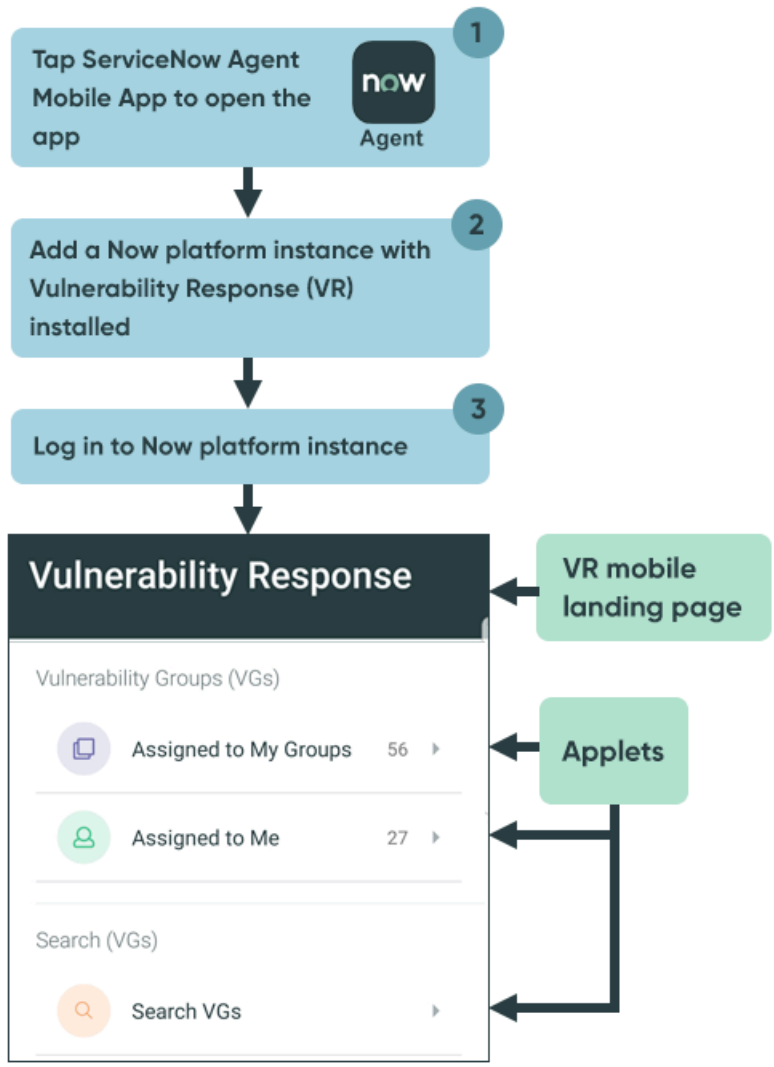
Avant de commencer

Vérifiez que vous avez effectué les étapes de configuration décrites à la section Configurer une liste de vérification pour le Application Vulnerability Response Mobile.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application Vulnerability Response Mobile



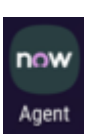
Rôle requis : propriétaire du rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche

Temps pour accomplir cette tâche : 5 à 7 minutes.

Procédure

1. Sur votre équipement mobile, appuyez sur l'application **ServiceNow Agent** .



Si vous n'êtes pas déjà connecté à une ServiceNow AI Platform instance, l'écran Instances s'affiche.

2. Si l'instance ServiceNow AI Platform avec l'application Réponse aux vulnérabilités principale n'est pas déjà ajoutée à votre appareil mobile, procédez comme suit pour l'ajouter.

   a. Sur l'écran Instances qui s'affiche, appuyez sur l'icône (icône Plus).
   Un écran s'affiche et vous invite à saisir et à enregistrer l'adresse d'une ServiceNow AI Platform instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

b. Renseignez les champs.

Nom de champ	Description
Entrez l'adresse de l'instance ou scannez un code QR.	Choisissez-en un pour continuer : ▪ Avant le .service-now.com, saisissez le nom de votre ServiceNow AI Platform instance, par exemple, vrmobilenewyorkagent. ▪ Saisissez une adresse. Cette adresse correspond à l'URL de votre ServiceNow AI Platform instance que vous souhaitez afficher sur votre appareil mobile. ▪ Scannez un code QR.
(Facultatif) Saisir le pseudonyme	entrez un surnom pour cette instance. Si plusieurs instances ont été ajoutées à l'appareil, des surnoms peuvent vous aider à localiser rapidement une ServiceNow AI Platform instance.

c. Appuyez sur **Enregistrer et connectez-vous**

3. Sur l'écran de connexion qui s'affiche ServiceNow , saisissez le nom d'utilisateur et le mot de passe de l'instance ServiceNow AI Platform que vous souhaitez ajouter, puis appuyez sur **Connexion**.
L'écran d'accueil de Vulnerability Response s'affiche. Vous vous êtes connecté avec succès au Application Vulnerability Response Mobile !

4. Une fois connecté, vérifiez que les notifications sont activées dans le Application Vulnerability Response Mobile.

a. Sur l'écran d'accueil en bas, appuyez sur **Notification**.

b. Sur l'écran Notifications, appuyez sur **Activer les notifications** si elles ne sont pas activées.
Les notifications de sont ServiceNow AI Platform affichées sur l'écran Notifications dans le Application Vulnerability Response Mobile.

5. Une fois que vous vous êtes connecté à une instance sur votre équipement mobile, il s'agit de l'instance par défaut ServiceNow AI Platform sur l'appareil.
Si vous souhaitez en afficher un autre ServiceNow AI Platform sur l'appareil, vous devez vous déconnecter de l'instance par défaut. Pour vous déconnecter :

a. Appuyez sur l'icône **Paramètres** .

b. Appuyez sur **Déconnexion**.
L'écran Instances s'affiche avec toutes les ServiceNow AI Platform instances que vous avez ajoutées à l'appareil mobile.

c. Facultatif : Appuyez sur une autre instance pour vous y connecter ou suivez les étapes précédentes pour ajouter une autre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Si l'écran des instances ne s'affiche Application Vulnerability Response Mobile pas après que vous avez appuyé sur l'application **ServiceNow Agent** sur votre appareil, vérifiez que **ServiceNow Agent** est autorisé en tant qu'application de confiance sur votre appareil. Pour autoriser l'accès en tant qu'application de confiance, accédez aux paramètres et à la gestion générale des appareils sur votre appareil et appuyez sur l'option (Faire confiance à l'application, etc.) pour autoriser l'accès.

Si un message d'erreur s'affiche après que vous avez saisi vos informations d'identification sur l'écran de connexion, vérifiez que votre nom d'utilisateur et votre mot de passe pour l'instance ServiceNow AI Platform sont corrects.

Si vous rencontrez des problèmes d'affichage sur l'écran d'accueil, vérifiez votre connexion réseau.

Si vous ne pouvez pas afficher l'écran Instances après avoir appuyé sur l'application **ServiceNow Agent** , essayez de la désinstaller de votre appareil. Vérifiez que vous disposez de la version la plus récente de l'application sur l'App Store d'Apple iOS ou le Google Play Store et essayez de la réinstaller.

Affichez, affectez et modifiez les tâches de rattrapage avec le Application Vulnerability Response Mobile

Affichez, affectez ou modifiez les champs sur les enregistrements de tâche de rattrapage affectés à votre groupe. Parcourez les vulnérabilités, les éléments de vulnérabilité et les enregistrements de solutions et les listes connexes pour afficher les solutions, les mesures de déploiement et les éléments à traiter.

Avant de commencer

Rôle requis : propriétaire du rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche

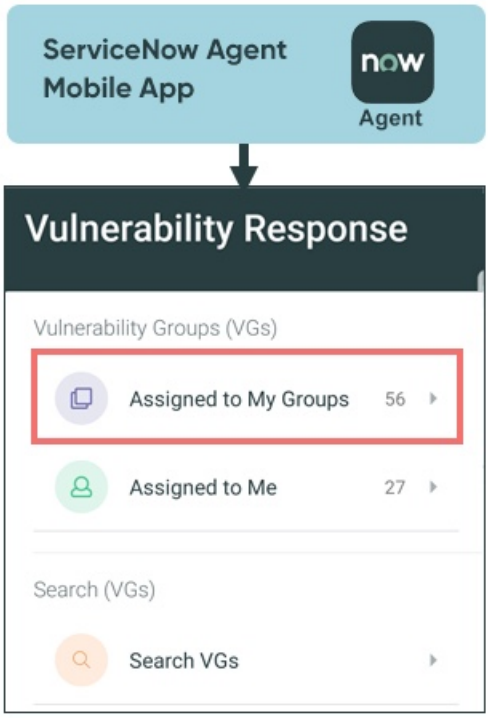
Vous affecter ou réaffecter des enregistrements RT (VUL) à vous-même ou les réaffecter à un autre membre de votre groupe. Vous pouvez également afficher les détails des enregistrements de tâches de rattrapage actifs, des éléments vulnérables (VI), des vulnérabilités NVD et des solutions avant toute modification, affectation ou correction. Temps pour terminer cette tâche : 5 à 10 minutes.

Procédure

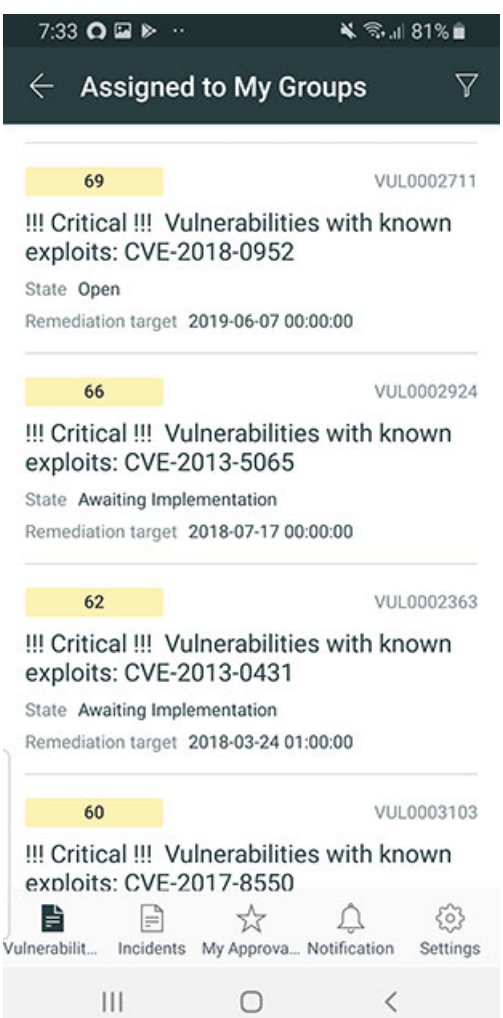
1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Vulnerability Response Mobile.
2. Avec l'écran d'accueil de Vulnerability Response affiché, appuyez sur **Affecté à mes groupes**.
   Si vous quittez le Application Vulnerability Response Mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous aviez affiché.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La liste des enregistrements ouverts affectés à votre groupe s'affiche.



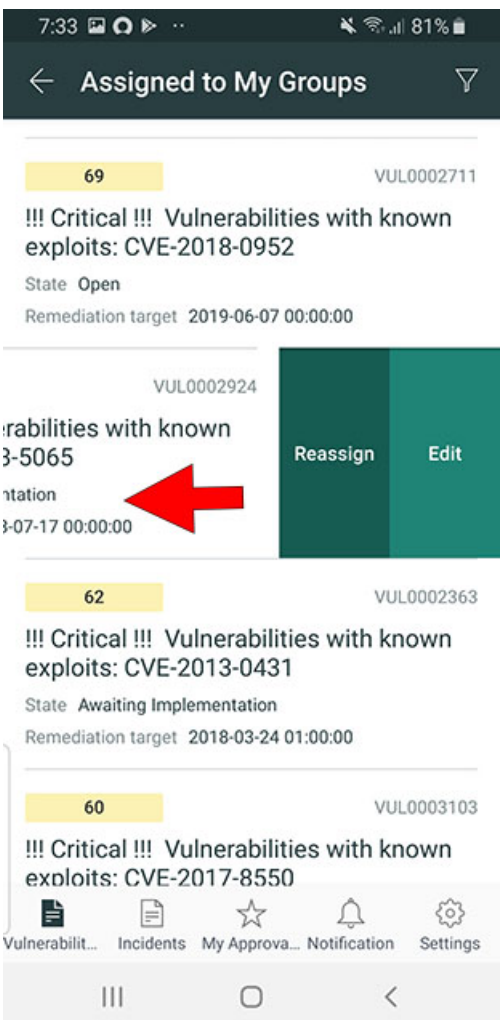
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. **Facultatif :** Reportez-vous à la section Rechercher des tâches de rattrapage avec le Application Vulnerability Response Mobile Rechercher les enregistrements qui correspondent à des critères spécifiques.

4. Alternativement, avec l'icône de filtre (icône affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste.
   Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.

5. Pour réaffecter ou modifier un enregistrement directement à partir de la liste, avec la liste des enregistrements ouverts affichée, faites glisser vers la gauche sur un enregistrement pour ouvrir le menu.



6. Choisissez-en un dans le menu qui s'affiche pour continuer.

Option	Description
M'affecter	Si l'enregistrement RT vous est déjà affecté, cette option ne s'affiche pas. Appuyez sur **Me l'affecter** pour vous attribuer le RT. Votre nom s'affiche dans le champ Affecté à de l'enregistrement. Un message de confirmation de l'affectation s'affiche.

Traduction automatique

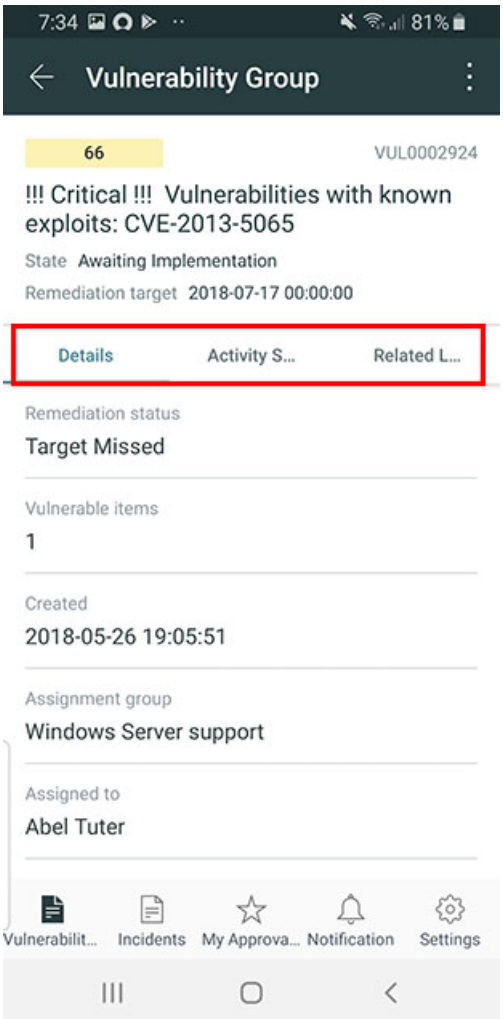
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Réaffecter	Pour réaffecter le RT à un groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Dans la liste, appuyez sur un groupe ou saisissez du texte dans le champ de re–cherche. Pour affecter ou réaffecter le RT à un membre d'un groupe d'affectation : **a.** Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône Envoyer ( ) ou sur **Soumettre** pour enregistrer et soumettre vos modifications.
Modifier	**a.** Appuyez sur **Modifier**. **b.** Développez les champs et sélectionnez une option dans la liste qui s'affiche ou saisissez du texte dans le champ de re–cherche. Appuyez sur l'icône d'envoi (icône) ou sur **Soumettre** pour enregistrer et sou–mettre vos modifications.

7. Alternativement, pour afficher les détails d'un enregistrement de vulnérabilité ouvert et pour afficher plus d'enregistrements associés et de listes connexes, avec l'écran Affecté à mes groupes affiché, appuyez sur un enregistrement de la liste.
8. Sur l'enregistrement de tâche de rattrapage ouvert qui s'affiche, choisissez une option dans la table suivante pour afficher les notes de travail ou les listes connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Onglet Détails	Avec l'onglet Détails sélectionné, examinez les champs de l'enregistrement RT. Appuyez sur l'icône de menu ( ) en haut à droite de l'écran pour afficher les options disponibles. Les options affichées dans ce menu développé varient. Les actions de rattrapage que vous pouvez entreprendre sur vos éléments vulnérables varient et dépendent de la valeur affichée dans le champ État de l'enregistrement. Pour plus d'informations sur le champ État et vos options de rattrapage, reportez-vous à la section Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, choisissez-en un pour continuer. ○ Affichez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Appuyez sur l'icône Plus (icône) pour ajouter une note de travail ou joindre un fichier. ○ Appuyez sur l'icône de menu (icône) en haut à droite de l'écran pour afficher les options de rattrapage disponibles.
Listes connexes	Une fois l'onglet Listes connexes sélectionné, affichez toutes les listes connexes de l'enregistrement RT qui sont renseignées. ○ Appuyez sur **Éléments vulnérables**. Appuyez sur un enregistrement d'élément vulnérable (VI) et accédez à l'enregistrement de solution préféré. Reportez-vous à la figure qui suit la table pour obtenir une carte de navigation et plus de détails. ○ Appuyez sur **Demandes de changement**. Affichez la liste des demandes de changement associées à cet enregistrement. ○ Une fois affiché, appuyez sur l'icône de menu (icône du) en haut à droite d'un écran pour afficher les options de rattrapage disponibles.

L'image suivante illustre le chemin de navigation depuis l'enregistrement de tâche de rattrapage vers l'enregistrement de solution préférée pour la vulnérabilité sélectionnée. Parcourez les enregistrements et les listes connexes pour afficher les solutions, les mesures de déploiement et les éléments à traiter.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chemin de navigation de la tâche de rattrapage via un enregistrement de solution



9. Après examen, modification ou correction, choisissez-en un pour continuer.

Option	Description
Appuyez sur une icône en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ○ Appuyez sur l'icône Réponse aux vulné–rabilités pour revenir à l'écran d'accueil. ○ Si affiché, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ○ Appuyez sur **Notification** pour afficher les notifications de et ServiceNow AI Plat-form de .Application Vulnerability Response Mobile

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	○ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance ServiceNow AI Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle ServiceNow AI Platform .

Afficher, réaffecter et modifier les tâches de rattrapage qui vous sont affectées avec le Application Vulnerability Response Mobile

Affichez, affectez ou modifiez les champs sur les enregistrements de tâches de rattrapage qui vous sont affectés. Parcourez les enregistrements et les listes connexes pour afficher les solutions, les mesures de déploiement et les éléments à traiter.

Avant de commencer

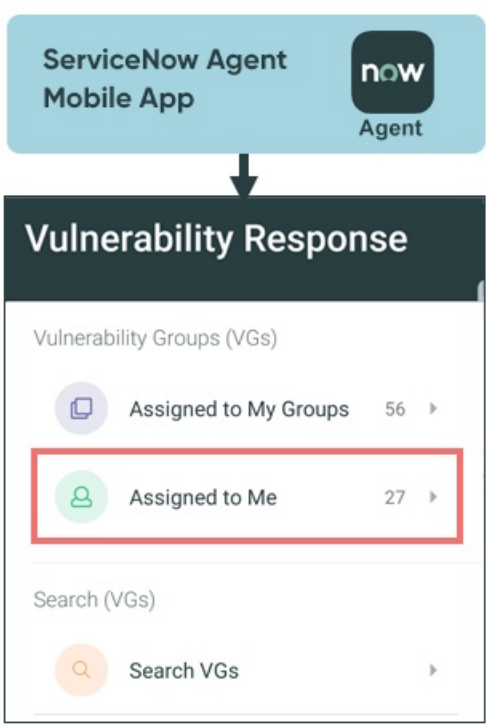
Rôle requis : propriétaire du rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche

Réaffecter ou modifier les enregistrements qui vous sont affectés. Affichez les détails des enregistrements de tâches de rattrapage, des enregistrements d'éléments vulnérables (VI), des vulnérabilités et des solutions actifs avant toute modification, affectation ou correction. Temps pour terminer cette tâche : 5 à 10 minutes.

Procédure

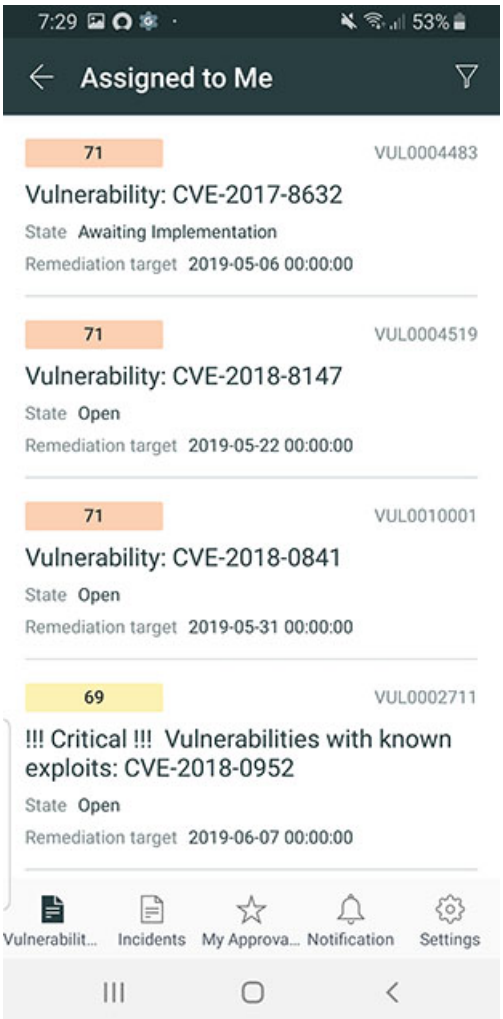
1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Vulnerability Response Mobile.
2. Avec l'écran d'accueil **de Vulnerability Response** affiché, appuyez sur **Affecté à moi**.
   Si vous quittez le Application Vulnerability Response Mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous aviez affiché.



La liste des enregistrements de tâches de rattrapage qui vous sont affectés s'affiche.

Traduction automatique

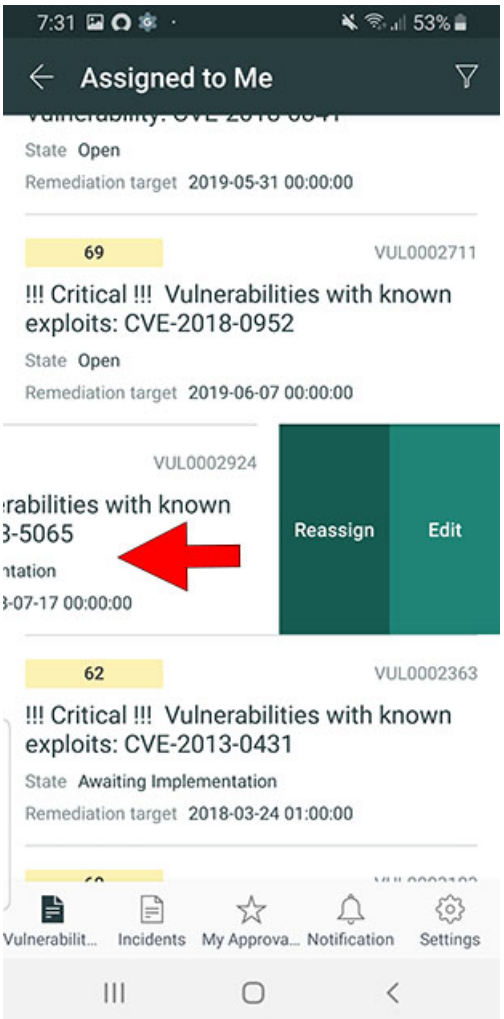
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. **Facultatif :** Reportez-vous à la section Rechercher des tâches de rattrapage avec le Application Vulnerability Response Mobile Rechercher les enregistrements qui correspondent à des critères spécifiques.
4. Alternativement, avec l'icône de filtre (icône affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste.
   Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.
5. Pour réaffecter ou modifier l'enregistrement directement à partir de la liste, avec l'écran Affecté à moi affiché, balayez un enregistrement vers la gauche pour ouvrir le menu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Choisissez-en un pour continuer.

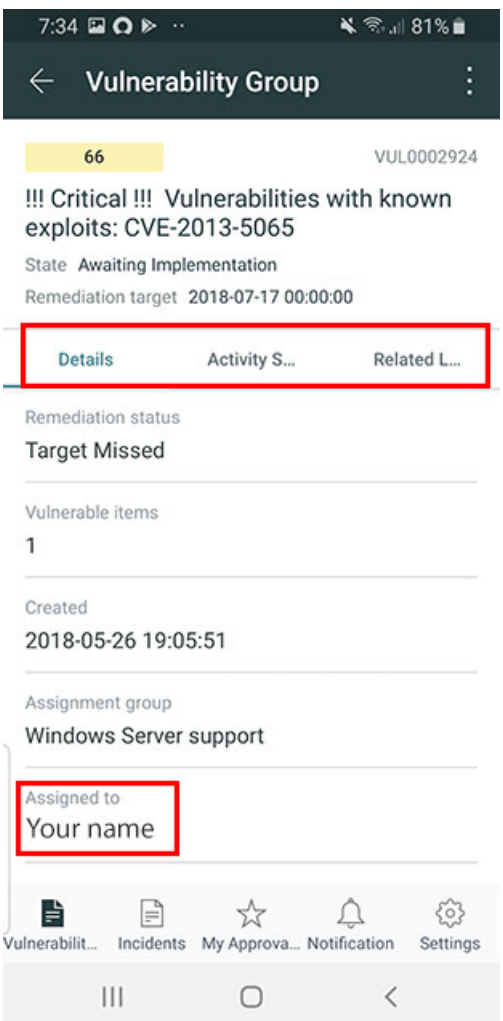
Option	Description
Réaffecter	Pour réaffecter la tâche à un autre groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Pour affecter ou réaffecter le RT à un membre d'un groupe d'affectation : **a.** Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône Envoyer ( ) ou sur **Soumettre** pour enregistrer et soumettre vos modifications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Modifier	**a.** Appuyez sur **Modifier**. **b.** Développez les champs et sélectionnez une option dans la liste qui s'affiche ou saisissez du texte. **c.** Appuyez sur l'icône d'envoi (icône) ou sur **Soumettre** pour enregistrer et soumettre vos modifications.

7. Alternativement, pour afficher les détails d'un enregistrement ouvert et pour afficher plus d'enregistrements associés et de listes connexes, avec l'écran Affecté à moi affiché, appuyez sur un enregistrement de la liste.
8. Sur l'enregistrement de tâche de rattrapage ouvert qui s'affiche, choisissez une option dans la table suivante pour afficher les notes de travail ou les listes connexes.



Option	Description
Onglet Détails	Avec l'onglet Détails sélectionné, examinez les champs de l'enregistrement de tâche de rattrapage. Appuyez sur l'icône de menu ( ) en haut à droite de l'écran pour afficher les options disponibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Les options affichées dans ce menu développé varient. Les actions de rattrapage que vous pouvez entreprendre sur vos éléments vulnérables varient et dépendent de la valeur affichée dans le champ État de l'enregistrement. Pour plus d'informations sur le champ État et vos options de rattrapage, reportez-vous à la section Réponse aux vulnérabilités États de la tâche de rattrapage et des éléments vulnérables.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, choisissez-en un pour continuer. ○ Affichez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône Plus (icône) pour ajouter une note de travail ou joindre un fichier. ○ Appuyez sur l'icône de menu (icône) en haut à droite de l'écran pour afficher les options de rattrapage disponibles.
Onglet Listes connexes	Une fois l'onglet Liste connexe sélectionné, affichez les listes connexes de l'enregistrement qui sont renseignées. ○ Appuyez sur **Demandes de changement**. Affichez la liste des demandes de changement associées à cet enregistrement. ○ Appuyez sur **Éléments vulnérables**. Appuyez sur un enregistrement d'élément vulnérable (VI) et accédez à l'enregistrement de solution préféré. Reportez-vous à la figure qui suit la table pour obtenir une carte de navigation et plus de détails. ○ Une fois affiché, appuyez sur l'icône de menu (icône du) en haut à droite de l'écran pour afficher les options de rattrapage disponibles.

L'image suivante illustre le chemin de navigation depuis l'enregistrement de tâche de rattrapage vers l'enregistrement de solution préférée pour la vulnérabilité sélectionnée. Parcourez les enregistrements et les listes connexes pour afficher les solutions, les mesures de déploiement et les éléments à traiter.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chemin de navigation de RT à travers un enregistrement de solution



9. Choisissez-en un pour continuer.

Option	Description
Appuyez sur une icône en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ○ Appuyez sur l'icône Réponse aux vulné–rabilités pour revenir à l'écran d'accueil. ○ Si affiché, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ○ Appuyez sur **Notification** pour afficher les notifications de et ServiceNow AI Plat-form de .Application Vulnerability Response Mobile

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	○ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance ServiceNow AI Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle ServiceNow AI Platform . Pour vous connecter, appuyez sur **Déconnexion**.

Rechercher des tâches de rattrapage avec le Application Vulnerability Response Mobile

Recherchez les tâches de rattrapage qui correspondent à des critères de recherche spécifiques que vous sélectionnez.

Avant de commencer

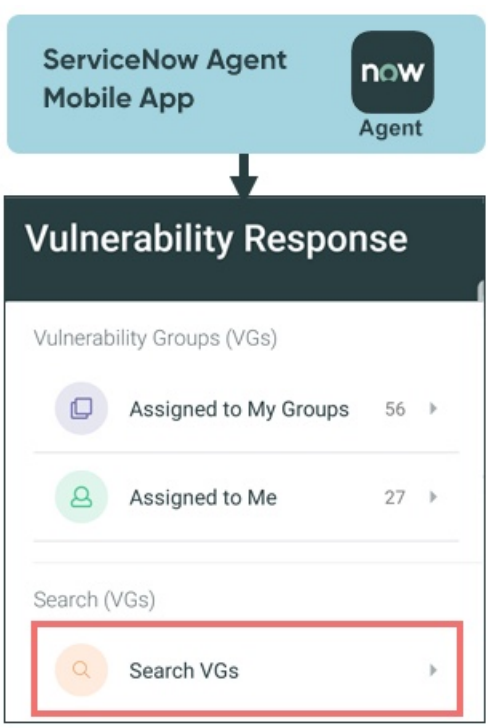
Rôle requis : propriétaire du rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche

Temps pour accomplir cette tâche : 5 à 7 minutes.

Procédure

1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Vulnerability Response Mobile.
2. Une fois l'écran d'accueil de **Vulnerability Response** affiché, appuyez sur **Rechercher des RT.**
   Si vous quittez le Application Vulnerability Response Mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous aviez affiché.



3. Sur l'écran de recherche qui s'affiche, appuyez sur les champs et remplissez le formulaire avec les critères de recherche souhaités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suivez les instructions après la table pour modifier les critères de recherche, effacer les critères de recherche ou soumettre une recherche.

Appuyer sur ce champ	Pour ajouter une entrée sur Android les appareils	Pour ajouter une entrée sur iOS les appareils
Numéro	Appuyez sur l'écran et entrez un numéro RT, par exemple, (VUL0002372) Ce numéro s'affiche en haut à droite de l'enregistrement RT. Appuyez sur l'icône en forme de coche pour ajouter votre entrée et revenir à l'écran Rechercher les RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher les RT.	Saisissez un numéro RT, par exemple : (VUL0002372). Ce numéro s'affiche en haut à droite de l'enregistrement RT. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
Cote de risque	Appuyez sur un ou plusieurs éléments, puis sur l'icône en forme de coche pour ajouter votre entrée et renvoyer l'écran Rechercher les RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher les RT.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments, ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
Statut de la remédiation	Appuyez sur un ou plusieurs éléments, puis sur l'icône en forme de coche pour ajouter votre entrée et renvoyer l'écran Rechercher les RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher les RT.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments, ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
État	Appuyez sur un ou plusieurs éléments, puis sur l'icône en forme de coche pour ajouter votre entrée et renvoyer l'écran Rechercher les RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher les RT.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments, ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appuyer sur ce champ	Pour ajouter une entrée sur Android les appareils	Pour ajouter une entrée sur iOS les appareils
Motif	Appuyez sur un ou plusieurs éléments, puis sur l'icône en forme de coche pour ajouter votre entrée et renvoyer l'écran Rechercher les RT. Appuyez sur l'icône de fermeture (X) pour annuler votre entrée et revenir au champ Rechercher les RT.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments, ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
Groupe d'affectation	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**.	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**.
Affecté à	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**.	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**.
Description brève	Appuyez sur l'écran et saisissez du texte. La fonctionnalité reconnaît les chaînes de texte et les chaînes de texte partielles dans ce champ, mais les caractères génériques (*) ne sont pas acceptés. Aucune majuscule n'est requise. Appuyez sur l'icône en forme de coche pour ajouter votre entrée et revenir à l'écran Rechercher les RT.	Sur l'écran, entrez du texte. La fonctionnalité reconnaît les chaînes de texte et les chaînes de texte partielles dans ce champ, mais les caractères génériques (*) ne sont pas acceptés. Aucune majuscule n'est requise. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer l'entrée et revenir à l'écran Rechercher des RT.
Description	Appuyez sur l'écran et saisissez du texte. La fonctionnalité reconnaît les chaînes de texte et les chaînes de texte partielles dans ce champ, mais les caractères génériques (*) ne sont pas acceptés. Aucune majuscule n'est requise. Appuyez sur l'icône en forme de coche pour ajouter votre entrée et revenir à l'écran Rechercher les RT.	Sur l'écran, entrez du texte. La fonctionnalité reconnaît les chaînes de texte et les chaînes de texte partielles dans ce champ, mais les caractères génériques (*) ne sont pas acceptés. Aucune majuscule n'est requise. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des RT. Dans le champ développé, appuyez sur **Annuler** pour effacer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appuyer sur ce champ	Pour ajouter une entrée sur Android les appareils	Pour ajouter une entrée sur iOS les appareils
		l'entrée et revenir à l'écran SearchRTs.

Pour Android les appareils, avec l'écran Rechercher des RT affiché et tous vos critères saisis, choisissez-en un pour continuer.

Option	Description
Effacer ou modifier les critères de recherche avant d'exécuter une recherche	Pour effacer tous les critères saisis, avec l'écran Rechercher des RT affiché, appuyez sur la flèche arrière pour effacer tous les champs et revenir à l'écran d'accueil de Vulnerability Response. La recherche n'est pas soumise et les critères de recherche sont effacés. Pour modifier un champ, vous pouvez également : ○ Avec l'écran Rechercher RT affiché, appuyez sur un champ avec des critères de recherche pour le développer. ○ Appuyez sur un élément pour le désélectionner. Appuyez sur Tout pour sélectionner tous les éléments. Appuyez à nouveau sur **Tout** pour effacer tous les éléments. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**. ○ Appuyez sur l'icône en forme de coche pour enregistrer les modifications et revenir à l'écran Rechercher les RT.
Soumettre une recherche	Avec l'écran Rechercher RTs affiché avec vos critères de recherche saisis, appuyez sur l'icône d'envoi (icône). Les enregistrements de tâche de rattrapage qui correspondent à vos critères de recherche s'affichent. Une fois la recherche terminée, les critères de recherche ne sont pas enregistrés.

4. Pour iOS les appareils, avec l'écran Rechercher des RT affiché, choisissez-en un pour continuer.

Option	Description
Effacer ou modifier les critères de recherche avant d'exécuter une recherche	Pour effacer tous les critères et revenir à l'écran d'accueil, appuyez sur l'icône de fermeture (X). Les critères de recherche saisis ne sont pas enregistrés. Vous pouvez également modifier un champ :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Avec l'écran Rechercher RT affiché, appuyez sur un champ avec des critères de recherche pour le développer. **b.** Appuyez sur un élément de la liste pour le désélectionner ou appuyez sur **Tout effacer**. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**. **c.** Appuyez sur **Terminé** pour enregistrer les modifications et revenir à l'écran Rechercher des RT.
Soumettre une recherche	Avec l'écran Rechercher RT affiché avec vos critères de recherche saisis, appuyez sur **Rechercher**. Les enregistrements RT qui correspondent à vos critères de recherche s'affichent. Une fois la recherche terminée, les critères de recherche ne sont pas enregistrés.

5. **Facultatif :** Si votre recherche renvoie plusieurs enregistrements, vous pouvez Filtrer les enregistrements avec le Application Vulnerability Response Mobile affiner les résultats de la recherche.

Filtrer les enregistrements avec le Application Vulnerability Response Mobile

Définissez des filtres supplémentaires pour limiter le nombre d'enregistrements qui s'affichent sur un écran. Le filtrage des enregistrements au sein de l'application mobile fonctionne comme avec un créateur de conditions sur ServiceNow AI Platform.

Avant de commencer

Rôle requis : propriétaire du rattrapage (sn_vul.remediation_owner)

Pourquoi et quand exécuter cette tâche

Temps nécessaire pour accomplir cette tâche : 5 minutes.

Procédure

1. Pour affiner les résultats de votre recherche ou pour entrer des critères de filtrage supplémentaires sur toute liste d'enregistrements affichée, appuyez sur l'icône de filtre (icône 
2. Une fois l'écran Filtres affiché, appuyez sur un champ pour le développer.
   Le champ État est un champ courant pour entrer des critères de recherche pour les enregistrements de tâche de rattrapage.
3. Parmi les options affichées, cochez la case ou appuyez sur un élément de votre filtre.
   Pour de nombreux filtres, vous pouvez sélectionner plus d'une option.
4. Appuyez sur l'icône Retour () ou sur **TERMINÉ** pour enregistrer vos modifications dans un champ.
   Les critères que vous avez choisis s'affichent sur l'écran Filtres. Le nombre d'enregistrements qui correspondent à vos critères est également affiché en haut de l'écran. Appuyez sur **RÉINITIALISER** pour supprimer tous les filtres et restaurer le paramètre par défaut.
5. **Facultatif :** Répétez les étapes 1 à 4 avec l'écran Filtres affiché pour continuer à définir vos critères de filtrage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Appuyez sur l'icône d'intersection (icône pour créer les conditions ET.
7. Vous pouvez également appuyer sur l'icône d'intersection (icône pour créer des conditions OR.
8. Une fois que vous avez ajouté tous les critères souhaités, avec l'écran Filtres affiché, appuyez sur **TERMINÉ.**
   À l'écran, seuls les enregistrements qui correspondent à vos critères de filtre sont affichés.

Information associée

Rechercher des tâches de rattrapage avec le Application Vulnerability Response Mobile

Orchestration de la réponse aux vulnérabilités

Avec Orchestration de la réponse aux vulnérabilités les workflows et les activités, vous pouvez interagir avec des systèmes et environnements Windows ou UNIX et les récupérer à l'aide de l'orchestration de workflow. En enrichissant les données, vous pouvez raccourcir le cycle de vie des rattrapages.

Pour plus d'informations sur la modification ou la création de workflows personnalisés, reportez-vous à la section Exploration des flux .

Workflow Analyser la vulnérabilité

Le champ **Réponse aux vulnérabilités** > **Analyser la vulnérabilité** Le workflow analyse à nouveau une tâche de rattrapage.

Avant de commencer
Rôle requis : aucun

Pourquoi et quand exécuter cette tâche
Ce workflow est déclenché par **une nouvelle analyse d'un groupe vulnérable** au cours d'une action **Fermer/Ignorer** .

Les activités du processus de workflow comprennent :

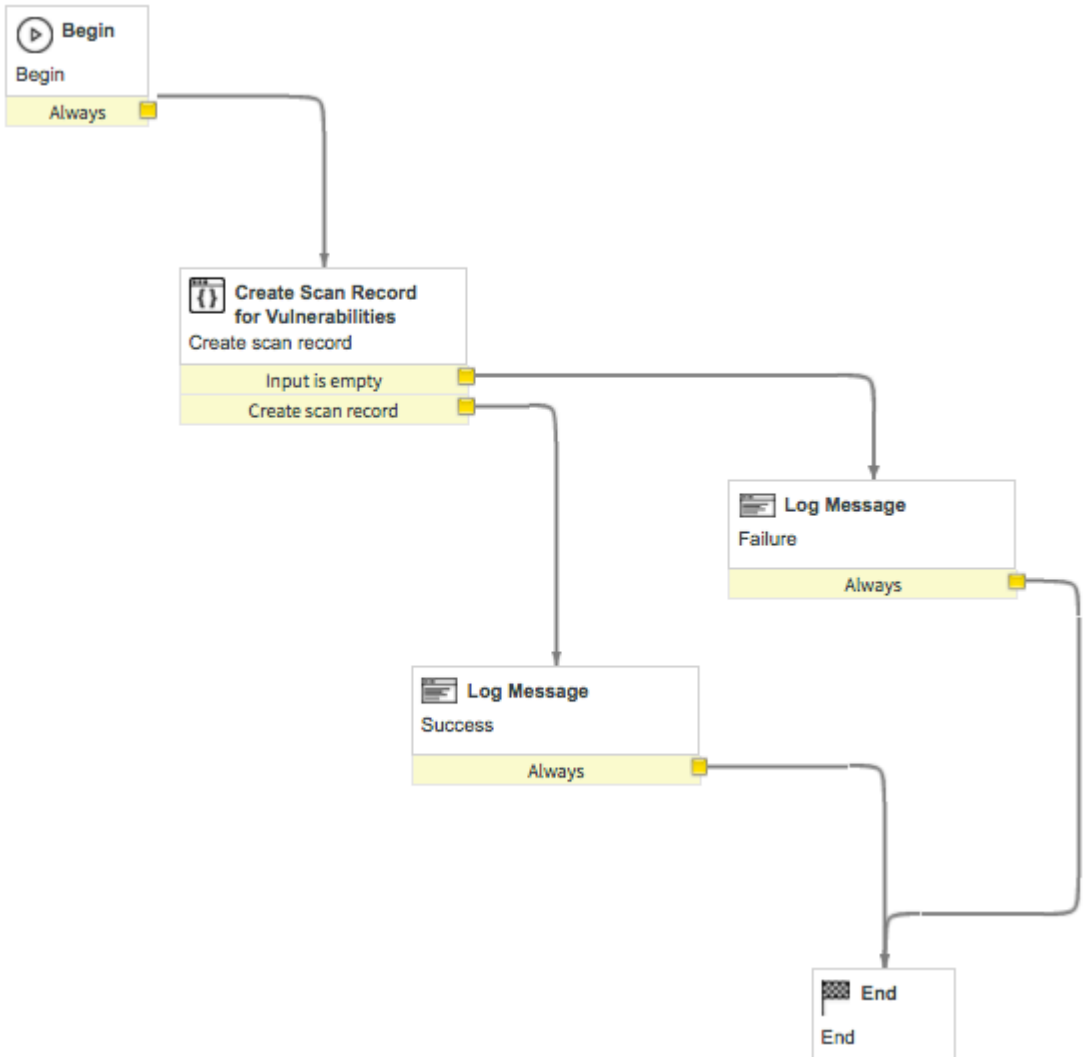
Variables pour créer un enregistrement d'analyse pour l'activité des vulnérabilités

Message du journal

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow Analyser la vulnérabilité



Traduction automatique

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
2. Ouvrez un enregistrement de tâche (VUL).
3. Cliquez sur **Fermer**.
4. Choisissez **Fermé** pour **l'état souhaité**.
5. Choisissez **Corrigé** pour le **Sous-état**.
6. Choisissez **Attendre la confirmation de la prochaine analyse** pour **Fermer maintenant ?**
   Pour la tâche de rattrapage et les éléments vulnérables, **l'état** passe à **En attente de confirmation**, le **sous-état** passe à **Corrigé** et une nouvelle analyse s'exécute.

Workflow Analyser l'élément de vulnérabilité

Le champ**Réponse vulnérable** > **Analyser l'élément de vulnérabilité** Le workflow analyse à nouveau un élément vulnérable.

Avant de commencer

Rôle requis : aucun

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

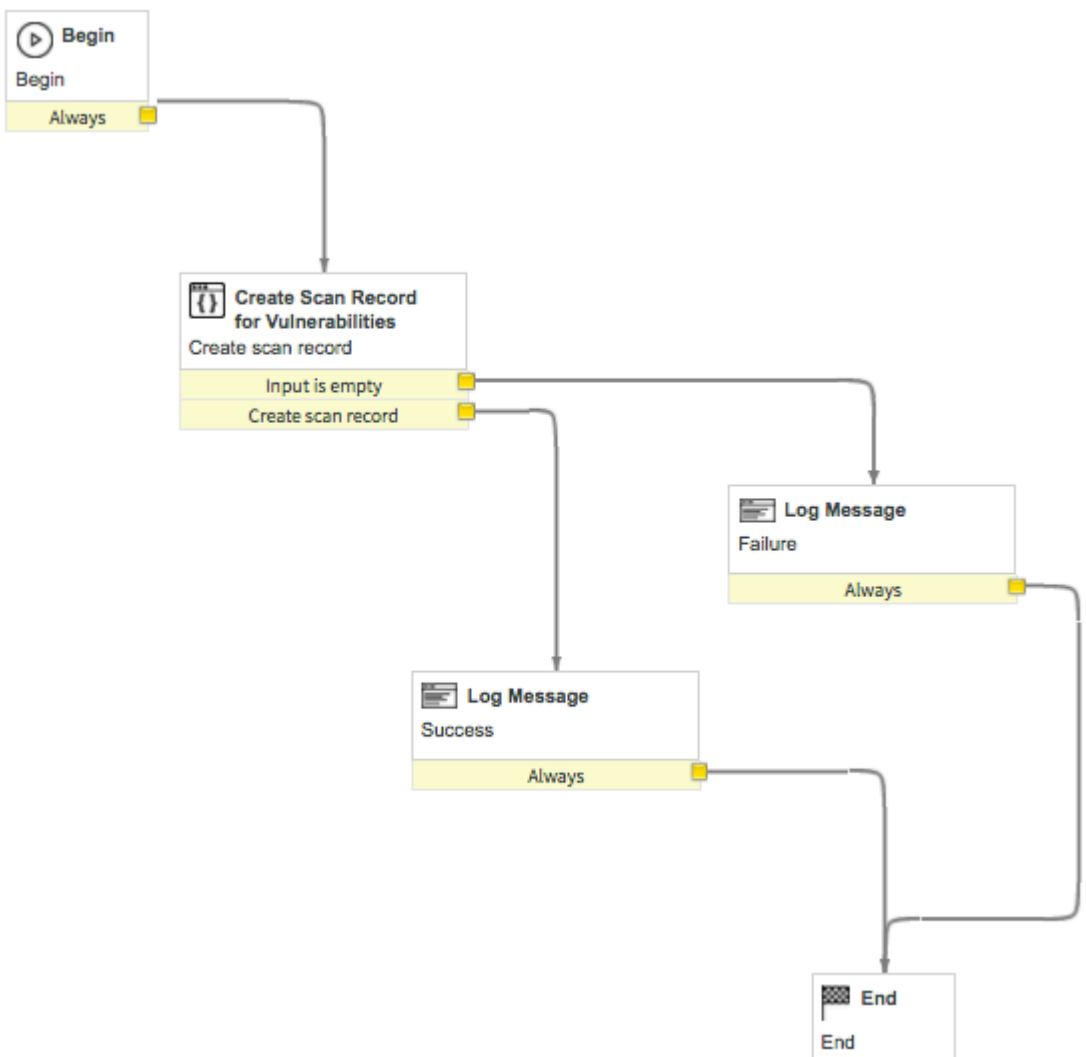
Pourquoi et quand exécuter cette tâche
Ce workflow est déclenché par **une nouvelle analyse d'une vulnérabilité** au cours d'une action **Fermer/Ignorer** .

Les activités du processus de workflow comprennent :

Variables pour créer un enregistrement d'analyse pour l'activité des vulnérabilités

Message du journal

Workflow Analyser la vulnérabilité



Traduction automatique

Procédure

1. Accédez à la **Vulnérabilité** > **Vulnérabilités** > **Éléments vulnérables**.
2. Ouvrez un élément de vulnérabilité.
3. Cliquez sur **Fermer/Ignorer**.
4. Choisissez **Fermé**pour **l'état souhaité**.
5. Choisissez **Corrigé** pour le **Sous-état**.
   L'état du groupe passe à **En attente de confirmation**, le **sous-état** passe à **Corrigé** et une nouvelle analyse s'exécute.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables pour créer un enregistrement d'analyse pour l'activité des vulnérabilités

Les analyses de vulnérabilité pour un ou plusieurs éléments vulnérables peuvent être exécutées à l'aide de l'activité de workflow **Créer un enregistrement d'analyse pour les vulnérabilités** incluse dans le système de base. Lorsque l'entrée est transmise à l'activité, un enregistrement d'analyse est créé.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
taskids [chaîne]	Une chaîne de sysId séparés par des virgules qui définissent les entrées attendues. Ce champ est obligatoire.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
scanResult [booléen]	Renvoie la valeur true si l'entrée n'est pas vide. Un enregistrement d'analyse est créé pour les taskIds.

Réponse aux vulnérabilités des applications

La Réponse aux vulnérabilités des applications fonctionnalité (AVR) de l'application importe les éléments vulnérables de l'application ServiceNow® Réponse aux vulnérabilités (AVIT) et, conformément aux règles, vous permet de corriger les vulnérabilités de l'application. Réponse aux vulnérabilités est disponible par abonnement distinct.

À partir d'AVR v19.0, certains noms de tables et de colonnes clés ont été mis à jour. Par conséquent, vous verrez des références aux noms plus anciens et plus récents dans la documentation. Pour obtenir la liste complète des termes mis à jour, reportez-vous à la section Vue du produit Réponse aux vulnérabilités des applications.

À partir de la version 19.0 de , vous pouvez ingérer des données de vulnérabilité de l'analyse de Réponse aux vulnérabilités la composition logicielle (SCA) et de la nomenclature logicielle (SBOM) pour vous aider à identifier les faiblesses de vos applications logicielles. Pour plus d'informations, consultez Explorer Réponse aux vulnérabilités des applications et Veracode Vulnerability Integration.

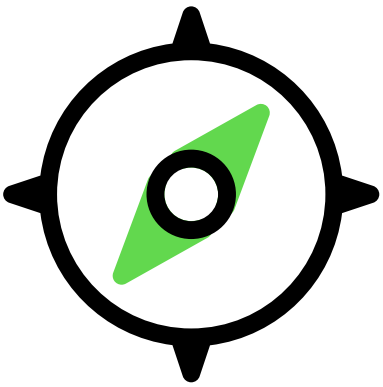
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

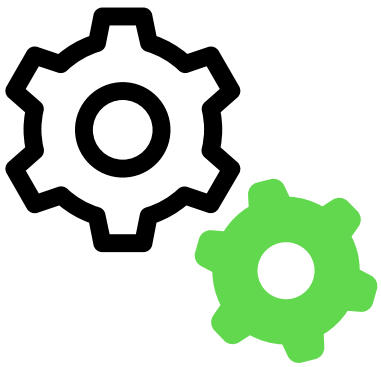
Réponse aux vulnérabilités des applications

Explorer



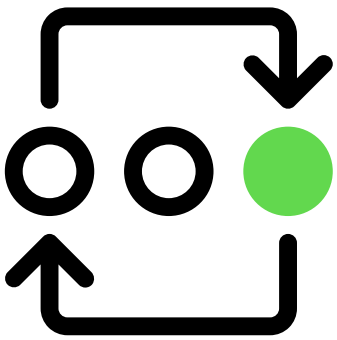
Découvrez les concepts et fonctionnalités d'Application Vulnerability Response.

Configurer



Configurez Application Vulnerability Response.

Intégrer



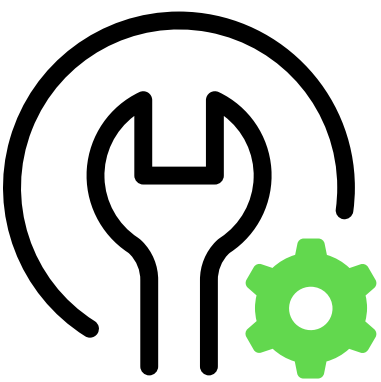
Étendez Application Vulnerability Response en l'intégrant à d'autres applications.

Utiliser les espaces de travail Vulnerability Response



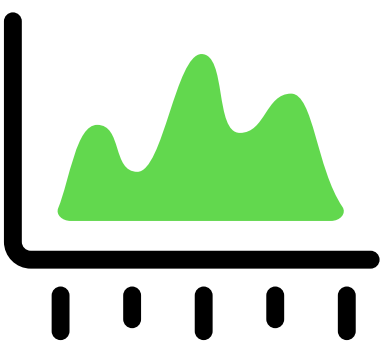
Découvrez comment surveiller, gérer et corriger les AVIT dans les espaces de travail Gestionnaire des vulnérabilités, Rattrapage informatique et Évaluation des vulnérabilités.

Corriger



Découvrez comment corriger des vulnérabilités d'applications.

Analyses et rapports

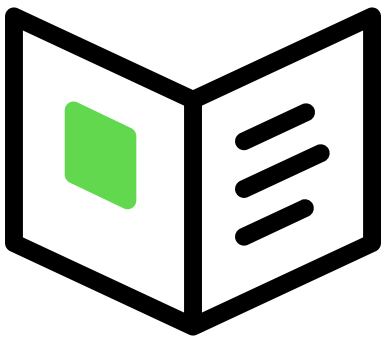


Afficher l'analyse Application Vulnerability Response

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Référence



Obtenez des détails sur les composants d'Application Vulnerability Response tels que les champs, les tables et les propriétés.

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Explorer Réponse aux vulnérabilités des applications

Les vulnérabilités d'application sont des vulnérabilités sur vos applications logicielles personnalisées qui sont analysées tout au long du cycle de vie de développement de l'application.

Vue d'ensemble et Réponse aux vulnérabilités des applications versions disponibles

Réponse aux vulnérabilités des applications (AVR) est la partie de l'application Réponse aux vulnérabilités qui traite les vulnérabilités d'application.

Versions disponibles

Version de mise en production	Notes de publication
Réponse aux vulnérabilités v23.0 Réponse aux vulnérabilités v22.0 Réponse aux vulnérabilités v21.0	Notes de version Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles (suite)

Version de mise en production	Notes de publication
Réponse aux vulnérabilités v20.0 Réponse aux vulnérabilités v19.0 Réponse aux vulnérabilités v18.2	consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Fonctionnement

Les données de vulnérabilité sont importées de sources internes et externes, telles que Common Weakness Enumeration (CWE) ou d'intégrations tierces. Une fois les données importées, elles sont comparées aux données de l'application et Base de données de gestion des configurations (CMDB) traitées dans l'application Réponse aux vulnérabilités des applications . Si une correspondance existe entre les données de vulnérabilité de l'application importées et les données de votre CMDB, un élément vulnérable de l'application (AVIT) est créé.

Le Réponse aux vulnérabilités des applications comprend les fonctionnalités clés suivantes :

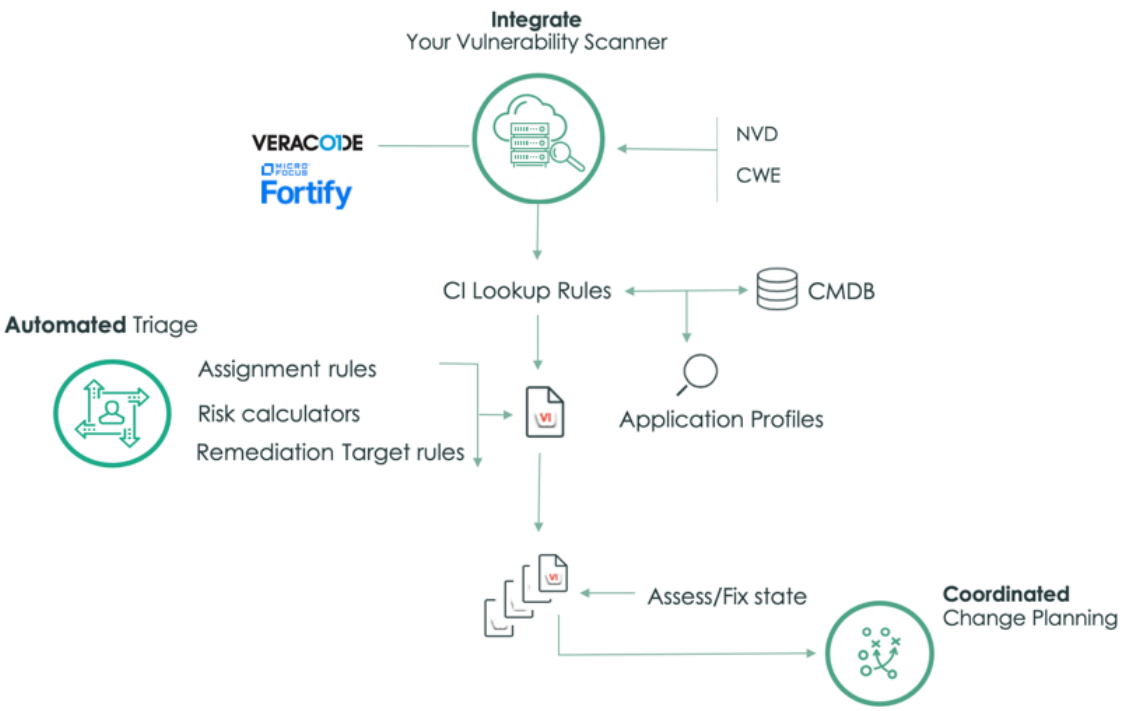
- Intégrez avec des analyseurs tiers pris en charge pour importer des données de vulnérabilité.
- Comparez les données liées à la vulnérabilité des applications et déterminez si des vulnérabilités d'application sont détectées dans une application.
- Classer par ordre de priorité, corriger et gérer les éléments vulnérables de l'application (AVIT). Chaque vulnérabilité d'application représente une entrée de vulnérabilité dans la CWE ou des bibliothèques tierces.
- À partir de la version 18.0 de Réponse aux vulnérabilités, vous pouvez surveiller et corriger les AVIT dans le Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT respectivement. Pour plus d'informations, consultez Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT.
- Corrélez Réponse aux vulnérabilités des applications les données à l'aide de calculateurs et de bibliothèques pour vous aider à effectuer les tâches suivantes.
  - Créez automatiquement des éléments vulnérables **d'application à l'aide des règles de recherche de CI**. Pendant l'importation, des vulnérabilités tierces sont associées à une CWE pour créer un AVIT.
  - Créez des règles d'affectation pour automatiser les affectations d'éléments vulnérables d'applications.
  - Utilisez des groupes de calculateurs pour déterminer l'impact sur l'entreprise, spécifier des conditions variables à l'aide de filtres, appliquer des calculs simples ou utiliser un script.
  - Créez des règles de cibles de rattrapage qui définissent le délai prévu pour le rattrapage des éléments vulnérables d'applications afin de surveiller les activités de rattrapage à venir.
- Associez une vulnérabilité tierce unique à plusieurs entrées CWE et recherchez la CWE primaire pour une vulnérabilité afin de vous aider à déterminer le risque. Pour plus d'informations sur le **CWE principal**, reportez-vous à la section Champs de vulnérabilité de l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Utilisez les enregistrements CWE qui sont téléchargés à partir de la base de données CWE ou importés à partir d'intégrations tierces pour vous aider à décider si vous devez escalader une vulnérabilité. Chaque enregistrement CWE comprend également un article de la base de connaissances associé qui décrit la faiblesse.

À utiliser Réponse aux vulnérabilités des applications pour suivre le flux d'informations, de l'intégration à l'enquête, puis à la résolution.



Types de données de vulnérabilité importées

Réponse aux vulnérabilités des applications prend en charge les types suivants de données de vulnérabilité des applications importées.

Remarque : Avant la version 19.0, les données SAST, SCA, IAST et de test de pénétration n'étaient pas ingérées et peuvent tenir compte des différences entre ce qui est affiché dans Veracode, Fortify et Invicti et ce qui apparaît dans Réponse aux vulnérabilités des applications.

Test dynamique de sécurité des applications (DAST)

Les analyses DAST recherchent les vulnérabilités des applications en envoyant une entrée à vos applications et en surveillant leurs réponses pendant leur exécution. Cette approche pourrait imiter une attaque extérieure. Au cours de l'analyse dynamique, un service en cours d'exécution (URL) est analysé pour rechercher des vulnérabilités. Les résultats de vulnérabilité incluent l'emplacement URL d'une vulnérabilité découverte.

Test statique de sécurité des applications (SAST)

Les analyses SAST examinent le code source des applications au repos et vous aident à trouver des vulnérabilités dans la façon dont vous avez écrit votre code. L'analyse SAST a lieu sur du code source non compilé et existe donc indépendamment de tout service d'application. Les résultats renvoyés comprennent l'emplacement d'un fichier et d'un numéro de ligne d'une vulnérabilité découverte.

Test de sécurité des applications interactives (IAST)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les analyses IAST détectent les vulnérabilités logicielles en interagissant avec le programme pendant son exécution. L'observation humaine, les tests automatisés et les capteurs sont utilisés en combinaison pour interagir avec l'application afin de localiser les vulnérabilités.

Analyse de la composition logicielle (SCA)

À partir de la version 19.0 de , vous pouvez ingérer des vulnérabilités SCA Réponse aux vulnérabilités(Software Composition Analysis). Les données de vulnérabilité SCA vous aident à identifier les faiblesses des logiciels open source utilisés dans vos applications logicielles.

Test de pénétration

Vous configurez les demandes d'évaluation de test de pénétration pour Réponse aux vulnérabilités des applications vous aider à comprendre où se trouvent les faiblesses de votre application et ce que vous pouvez faire pour les corriger.

Nomenclature logicielle

Chargez Nomenclature logicielle des données (SBOM) pour identifier les vulnérabilités dans vos composants open source. Consultez Explorer Nomenclature logicielle pour plus d'informations.

Cas d'utilisation

Certains des cas d'utilisation DAST suivants sont pris en charge :

- Reliez chaque vulnérabilité des résultats de l'analyse à une sorte de cmdb_ci (classe enfant).
- Associez les résultats de l'analyse DAST à une application existante lorsqu'il existe un enregistrement dans l'intégration CMDB De Découverte ou tierce.
- Associez le résultat de l'analyse DAST à une application numérisée nouvellement insérée lorsqu'une nouvelle application n'a pas encore été identifiée et/ou stockée dans la CMDB.
- Stocker les résultats de l'analyse DAST pour une CMDB lorsque vous gérez vos applications dans un produit autre que ServiceNow®.
- Stockez les résultats de l'analyse DAST pour une CMDB si vous l'avez précédemment personnalisé à d'autres fins.
- Créez manuellement une application pour le référentiel de code source.

Certains des cas d'utilisation SAST pris en charge sont pris en charge :

- Reliez chaque vulnérabilité des résultats de l'analyse à une sorte de cmdb_ci (classe enfant).
- Créez manuellement un CI pour le référentiel de code source.
- Stocker les résultats de l'analyse SAST qui sont sans service d'application associé.

Intégrations tierces

Les intégrations tierces prises en charge par Réponse aux vulnérabilités des applications sont disponibles en tant qu'applications distinctes dans le ServiceNow Store. Consultez Intégrer Réponse aux vulnérabilités des applications avec d'autres applications pour plus d'informations.

Fonctionnalités principales

- Une API partagée importe les données DAST, SAST, IAST et SCA ainsi que les résultats des tests d'intrusion manuels. Consultez Test de pénétration.
- Une API distincte est utilisée pour importer des données SBOM. Pour plus d'informations, consultez Explorer Nomenclature logicielle et Veracode Vulnerability Integration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles de recherche de CI

Rechercher automatiquement des correspondances dans les données de l'application Base de données de gestion des configurations (CMDB).

Règles d'affectation

Affectez automatiquement les vulnérabilités des applications en fonction des groupes d'utilisateurs, des champs de groupe d'utilisateurs et des scripts.

Calculateurs de risques

Classer automatiquement par ordre de priorité et évaluer l'impact des AVIT à l'aide de calculateurs, en fonction de n'importe quel critère, à l'aide de filtres de condition.

Mappage de sévérité

Calculez automatiquement les valeurs initiales des champs des éléments vulnérables de l'application. Les entrées de vulnérabilité ont à la fois une gravité source et une gravité normalisée (basée sur le mappage de gravité). La gravité est liée au Common Weakness Enumeration (CWE).

Règles de cibles de rattrapage

Définissez le délai prévu pour le rattrapage d'un élément vulnérable de l'application.

Reporting

Obtenez rapidement un aperçu de votre posture de sécurité, des tendances en matière de rattrapage et des 10 principales applications ou unités business comportant les AVIT les plus critiques.

Le point commun des deux types d'analyses est la version de l'application. Une version de l'application, qui définit une chaîne de **nom** , est le point de connexion permettant de regrouper les résultats de vulnérabilité analysés du côté du scanner. De cette façon, AVR sait à quelle version de l'application appartiennent les résultats lors de l'importation des résultats d'analyse via l'intégration.

Une table enfant d'élément de configuration [cmdb_ci], Applications analysées [sn_vul_app_scanned_application], a été créée dans l'application et dans le Réponse aux vulnérabilités périmètre. Cette table stocke l'abstraction de la version de l'application et fournit un mappage des services par le biais de ses relations CMDB. Elles peuvent être visualisées à partir du **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Applications** module. La vue de liste Applications numérisées contient le **département** et le **groupe de support** ajoutés lors de la configuration.

Éléments vulnérables de l'application (AVIT)

Pour les vulnérabilités d'application, AVR associe une vulnérabilité à une application pour créer l'enregistrement de l'élément vulnérable de l'application (AVIT). En raison des multiples définitions de ce qui constitue une application dans la CMDB, Réponse aux vulnérabilités des applications limite les applications aux applications analysées. Les applications numérisées sont les applications analysées dans votre environnement, identifiées par AVR comme **Nom** et **ID.** Les AVIT sont basés sur le dernier résumé de l'analyse jusqu'à ce qu'il soit confirmé **Corrigé** par le scanner. Si un AVIT n'est plus trouvé, il reste lié au résumé de l'analyse où il a été vu pour la dernière fois.

Les éléments vulnérables de l'application peuvent être affichés à partir de **Tous** > **Réponse aux vulnérabilités de l'application** > **Vulnérabilités** > **Éléments vulnérables** module.

Si une application est supprimée de la CMDB, tous les AVIT associés sont fermés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur les champs du formulaire AVIT, reportez-vous à la section Champs d'élément vulnérable d'application.

Groupes d'utilisateurs et rôles dans Réponse aux vulnérabilités des applications

Souvent, une équipe travaille ensemble pour créer, gérer et superviser la gestion des vulnérabilités des applications. Des rôles stratégiques, ainsi que des rôles opérationnels, sont attribués aux membres de l'équipe. Dans la plupart des organisations, vous pouvez endosser plusieurs rôles et souvent partager des rôles avec d'autres. Réponse aux vulnérabilités des applications utilise trois groupes d'utilisateurs contenant des rôles granulaires : Gestionnaire de sécurité des applications, Champion de la sécurité des applications et Développeur. Consultez la rubrique Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs pour en savoir plus sur ces groupes et rôles.

Réponse aux vulnérabilités des applications États

Réponse aux vulnérabilités des applications offre un modèle d'état pour l'état de vos éléments vulnérables de l'application (AVIT) et vous aide à déterminer quand et comment corriger vos AVIT.

Un élément vulnérable de l'application a plusieurs états possibles, consultez la section États des éléments vulnérables de l'application (AVI) pour plus d'informations.

Réponse aux vulnérabilités applications et CSDM tables

Réponse aux vulnérabilités des applications Les Réponse aux vulnérabilités intégrations et Nomenclature logicielle applications de vulnérabilité tierces gèrent les tables (y contribuent des données). CSDM Ces applications utilisent également des données provenant de CSDM tables générées par d'autres applications. Plusieurs ServiceNow produits bénéficient donc de ces Opérations de sécurité applications et y ajoutent de la valeur. Consultez Réponse aux vulnérabilités applications et CSDM tables pour plus d'informations.

Configurer Réponse aux vulnérabilités des applications

Avant d'exécuter Réponse aux vulnérabilités des applications dans votre ServiceNow AI Platform instance, vous devez la configurer.

Configurer Réponse aux vulnérabilités des applications

Effectuez les étapes de configuration suivantes avant la configuration afin de vous assurer que votre configuration est terminée.

Avant de commencer

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, reportez-vous à la section Installer Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
Vérifiez que l'est Analyse des performances pour Réponse aux vulnérabilités installé et activé pour afficher les Réponse aux vulnérabilités des applications rapports.	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, reportez-vous à la section Installer et configurer l'application Analyse des performances pour Réponse aux vulnérabilités [PA].
Vérifiez que le Veracode Vulnerability Integration est installé, activé et configuré. (N'exécutez pas les intégrations pour l'instant.)	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, reportez-vous à la section Installer l'intégration ServiceNow de Vulnerability Response avec Veracode.
Vérifiez que l'intégration CWE 2000 est en cours d'exécution dans Réponse aux vulnérabilités.	Pour vérifier l'intégration, reportez-vous à la section Vérifiez que la tâche planifiée pour la mise à jour des enregistrements NVD est en cours d'exécution.
[Facultatif] Vérifiez que l'intégration NVD est en cours d'exécution dans Réponse aux vulnérabilités.	Pour vérifier, reportez-vous à la section Vérifiez que la tâche planifiée pour la mise à jour des enregistrements CWE est en cours d'exécution.
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • S'il n'est pas déjà affecté, l'utilisateur disposant du rôle administrateur installe l'application et affecte les utilisateurs aux groupes d'utilisateurs suivants : Responsable de sécurité des applications, Champion de sécurité et Développeur. Pour plus d'informations sur les rôles de groupe, reportez-vous à la section Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs. • Le groupe de gestionnaires App-Sec supervise la configuration et vérifie les résultats attendus. **Remarque :** Réponse aux vulnérabilités des applications configuration n'est pas disponible à partir de la fonctionnalité Assistant de configuration dans Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : groupe d’utilisateurs Gestionnaire de sécurité des applications

Procédure

1. Accédez à la **Security Operations** > **CMDB** > **Règles de recherche**.
   Voir pour Créer une règle de recherche de CI créer ou modifier des règles de recherche de CI pour votre environnement.
2. Accédez à la **Réponse aux vulnérabilités de l'application** > **Administration**.
3. **Sélectionner des règles d’affectation**.
   Reportez-vous à la section Créer ou modifier Réponse aux vulnérabilités des applications des règles d’affectation pour créer ou modifier des règles d’affectation d’application pour votre environnement.
4. Sélectionnez les **calculateurs de vulnérabilité**.
   Consultez la rubrique Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications pour créer ou modifier des calculateurs de vulnérabilité d’application pour votre environnement.
5. Sélectionnez **les règles de cibles de rattrapage**.
   Consultez la rubrique Créer ou modifier des règles de cibles de rattrapage d’applications pour créer ou modifier des cibles de rattrapage d’applications pour votre environnement.
6. **Sélectionnez les cartes de gravité normalisées**.
   Reportez-vous à la section Mapper automatiquement la gravité d’un élément vulnérable d’application pour créer ou modifier des cartes de gravité pour votre environnement.
7. Accédez à l’un ou l’autre des **Intégration de vulnérabilité Veracode** > **Intégrations** ou **Fortify Vulnerability Integration** > **Intégrations**.
8. Ouvrez l’intégration de la liste des applications Veracode ou l’intégration de la liste des applications Fortify On Demand.
9. S’il n’a pas encore été exécuté, sélectionnez **Exécuter maintenant**.

   Remarque : Les autres Veracode intégrations sont Fortify inactives par défaut.

   Pour les états d’exécution de l’intégration, consultez Afficher l’état de l’exécution de l’importation de l’intégration de vulnérabilité de l’application Veracode ou Afficher l’état d’exécution de l’importation Fortify Vulnerability Integration.
10. Une fois l’exécution de l’intégration de liste d’applications Veracode ou Fortify à la demande terminée, accédez à **Réponse aux vulnérabilités de l'application** > **Administration** > **Applications**.
11. Pour chaque application, entrez une valeur pour **Groupe de support** (utilisé par les règles d’affectation) et **pour Département** (utilisé dans la génération de rapports).
    Pour mettre à jour plusieurs entrées, consultez Modifier plusieurs enregistrements dans une liste à l’aide de l’éditeur de liste pour terminer la tâche en bloc.

    Remarque : Pour afficher **l’unité business** mise à jour automatiquement, actualisez la page. Pour en savoir plus sur les champs du formulaire Application numérisée, reportez-vous à la section Champs de l’application analysée.
12. Revenez à la liste Intégrations et activez l’autre Veracode ou Fortify les intégrations.
    Reportez-vous à la section pour Activer Réponse aux vulnérabilités des applications des intégrations définir vos importations d’intégration de données delta.

    Les Veracode intégrations et Fortify sont enchaînées et s’exécuteront consécutivement lorsqu’elles sont activées.
13. **Facultatif :** Accédez à la **Réponse aux vulnérabilités de l'application** > **Administration** > **Règles d'affectation**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. **Facultatif :** Si vous avez choisi **Élément de configuration : Groupe de support** pour le **champ Groupe d'utilisateurs** lors de la création ou de la modification de vos règles d'affectation précédemment, les valeurs que vous avez ajoutées à la vue de liste Applications numérisées peuvent être utilisées dès maintenant.
Vos règles d'affectation sont modifiées.

b. Sélectionnez **Mettre à jour**.

c. Dans la vue de liste Règles d'affectation de vulnérabilité, sélectionnez **Appliquer les changements** pour réappliquer les règles d'affectation à vos AVI.

Résultats

Votre Réponse aux vulnérabilités des applications configuration est maintenant terminée.

Que faire ensuite

Accédez à la **Réponse aux vulnérabilités de l'application** > **Vue d'ensemble** et consultez le tableau de bord Gestion de la vulnérabilité des applications [PA] pour obtenir des informations sur votre posture de sécurité globale.

Vérifiez que la tâche planifiée pour la mise à jour des enregistrements CWE est en cours d'exécution

Utilisez les enregistrements CWE (Common Weakness Enumeration) téléchargés à partir de la base de données CWE comme référence pour décider si une vulnérabilité doit être remontée. Mettez à jour régulièrement les enregistrements des faiblesses courantes de la base de données Common Weakness Enumeration. Vous pouvez également mettre à jour le script par défaut ou écrire vos propres scripts, selon vos besoins.

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires
Chaque enregistrement CWE comprend également un article de la base de connaissances associé qui décrit la faiblesse.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Intégrations**.
2. Sélectionnez la tâche planifiée **Intégration complète CWE 2000** .
3. Vérifiez que la case **Actif** est cochée.

   Remarque : Les paramètres de ce formulaire sont partagés par Réponse aux vulnérabilités et Réponse aux vulnérabilités des applications. La modification des paramètres d'intégration nécessite une coordination avec et une expertise en la ServiceNow matièreRéponse aux vulnérabilités.

4. Si la case est cochée, vous avez terminé.

   Remarque : Si la case n'est pas sélectionnée, cette intégration devra peut-être être configurée dans Réponse aux vulnérabilités. Consultez la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces pour plus d'informations avant de le sélectionner.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Au besoin, consultez Afficher les bibliothèques de vulnérabilités pour afficher les entrées importées.

Le champ **CWE primaire** contient l'entrée CWE. Si plusieurs CWE sont associées à une vulnérabilité, consultez Champs de vulnérabilité de l'application pour en savoir plus sur la façon dont la CWE principale est déterminée.

Vérifiez que la tâche planifiée pour la mise à jour des enregistrements NVD est en cours d'exécution

Identifiez les référentiels que vous souhaitez mettre à jour régulièrement. Vous pouvez exécuter une tâche planifiée pour mettre à jour les enregistrements de la Base de données de vulnérabilité nationale (NVD) tous les soirs ou toutes les semaines. S'il n'est pas déjà en cours d'exécution, vous pouvez activer la tâche

Avant de commencer

Rôles requis : App-Sec Groupe de gestionnaires

L'intégration NVD s'exécute en tant que tâche planifiée tous les lundis à 00:00:00, par défaut.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Intégrations**.
2. Sélectionnez la tâche planifiée **Base de données de vulnérabilité nationale du NIST** .
3. Vérifiez que la case **Actif** est cochée.

   Remarque : Les paramètres de ce formulaire sont partagés par Réponse aux vulnérabilités et Réponse aux vulnérabilités des applications. La modification des paramètres d'intégration nécessite une coordination avec et une expertise en la ServiceNow matièreRéponse aux vulnérabilités.

4. Si la case est cochée, vous avez terminé.

   Remarque : Si la case n'est pas sélectionnée, cette intégration devra peut-être être configurée dans Réponse aux vulnérabilités. Consultez la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces pour plus d'informations avant de le sélectionner.

Au besoin, consultez Afficher les bibliothèques de vulnérabilités pour afficher les entrées importées.

Activer Réponse aux vulnérabilités des applications des intégrations

Activez Réponse aux vulnérabilités des applications les intégrations pour effectuer des mises à jour régulières.

Avant de commencer

Rôle requis : gestionnaire App-Sec

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Intégrations**.
2. Sélectionnez une intégration.
3. Sélectionnez la case à cocher **Activé**.
4. Sélectionnez **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Répétez l'opération au besoin pour chaque intégration.
   Après l'exécution initiale, les intégrations sont enchaînées pour effectuer des importations delta pour les exécutions suivantes.

Définir les Réponse aux vulnérabilités des applications notifications par e-mail

Configurez des notifications par e-mail pour partager des informations utiles sur les mises à jour et les activités importantes, telles que l'approbation et le rejet de demandes de faux positif. La création d'une notification par e-mail implique de spécifier quand l'envoyer, qui la reçoit et ce qu'elle contient.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Modèles d'e-mail**.
2. Sélectionnez **Nouveau**.

   Pour obtenir des instructions détaillées sur la création de notifications par e-mail, reportez-vous à la section Créer une notification par e-mail .

Résultats
À partir de la version 21.0 de , lorsqu'un Réponse aux vulnérabilités destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités ou Espace de travail de remédiation IT en fonction de son rôle.

- Des liens s'ouvrent Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs ayant le rôle sn_vul.app_sec_manager.
- Des liens s'ouvrent Espace de travail de remédiation IT pour les utilisateurs ayant des rôles, sn_vul.app_security_champion ou sn_vul.app_developer.

Si le destinataire ne possède aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Créer ou modifier des notifications de cible de rattrapage dans Réponse aux vulnérabilités des applications

Les administrateurs de vulnérabilité peuvent modifier la notification de cible de rattrapage ou en ajouter de nouvelles, en spécifiant quand envoyer la notification, qui reçoit la notification et quel contenu contient la notification.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Notifications**.
2. Sélectionnez l'enregistrement de notification de la cible de rattrapage ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Pour plus d'informations sur les champs de formulaire, consultez Créer une notification par e-mail .
4. Sélectionnez **Afficher l'aperçu** de la notification pour afficher le message.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
À partir de la version 21.0 de , lorsqu'un Réponse aux vulnérabilités destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités ou Espace de travail de remédiation IT en fonction de son rôle.

- Des liens s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs disposant du rôle sn_vul.app_sec_manager.
- Des liens s'ouvrent Espace de travail de remédiation IT pour les utilisateurs ayant des rôles, sn_vul.app_security_champion ou sn_vul.app_developer.

Si le destinataire ne possède aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Gestion des exceptions dans Réponse aux vulnérabilités des applications

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive publiée en matière de gestion des vulnérabilités ou de sécurité, vous pouvez demander une exception. La gestion des exceptions implique la demande, l'examen, l'approbation ou le rejet d'exceptions à un élément vulnérable de l'application (AVIT) qui ne peuvent pas être corrigées conformément à la politique.

Certaines vulnérabilités peuvent ne pas avoir de correctif, de correctif ou de solution existant. Lorsqu'une exception est approuvée, cela signifie également que vous acceptez un risque, car vous reconnaissez et acceptez les conséquences d'une non-correction de la vulnérabilité.

Remarque :

À partir de la version 21.0 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités des applications des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable de l'application passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable de l'application ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Cycle de vie d'une exception

Définition d'une exception

Une exception est une demande de différer le rattrapage d'un AVI pour une période spécifiée. Par exemple, en tant que développeur, vous pouvez demander une exception si un correctif n'est pas disponible pour un ordinateur.

Demande d'exception

En tant que développeur, vous pouvez demander une exemption pour un AVI en utilisant le processus de gestion des exceptions. Une fois cette demande approuvée par l'analyste de sécurité des applications, l'AVI passe à l'état **Différé** .

Important : Vous pouvez demander des exceptions pour les AVTI et les RT à partir de l'espace de travail du gestionnaire de vulnérabilité et de l'espace de travail de rattrapage informatique respectivement. Pour plus d'informations, consultez Demander des exceptions pour les tâches et les enregistrements de rattrapage dans Espace de travail du gestionnaire de vulnérabilités et Demander une exception dans le Espace de travail de remédiation IT.

Règles d'exception

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 20, vous pouvez créer des règles d'exception afin de différer automatiquement les éléments vulnérables d'application (AVI) existants et nouveaux pour une période spécifique s'ils correspondent aux conditions de la règle. L'utilisation de règles d'exception pour différer automatiquement les AVI minimise le risque de manquer des accords sur les niveaux de service. Les règles peuvent vous aider à gérer plusieurs éléments, car vous éliminez les interventions manuelles. Voir Créer une règle d'exception.

Demande d'extension pour une règle d'exception

À partir de la version 20, vous pouvez soumettre une demande d'extension de la date de **fin** de report d'une règle d'exception. Vous pouvez demander l'extension d'une règle si vous constatez qu'un grand nombre d'enregistrements créés par la règle ne sont pas résolus dans sa date **Différé jusqu'à** , c'est-à-dire la date à laquelle la tâche de rattrapage cesse d'accepter les nouveaux AVI. L'extension met à jour la règle d'exception afin de prolonger automatiquement la date de report de votre règle existante. Vous pouvez saisir des dates jusqu'à un an à partir de la date actuelle, et vous devez inclure un motif pour l'extension. Une demande d'extension nécessite l'approbation à deux niveaux de groupes d'approbation distincts.

Approbation d'une demande d'exception

Les AVIT qui ne peuvent pas être corrigés immédiatement sont examinés par des analystes de sécurité des applications, évalués pour le risque et approuvés pour le report jusqu'à ce qu'ils puissent être corrigés. L'approbation d'une demande d'exception peut être un flux à deux niveaux. Si seul l'approbateur de premier niveau est présent, l'exception peut être demandée et approuvée. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Consultez Ajouter un approbateur d'exception pour Réponse aux vulnérabilités des applications pour plus d'informations.

Important : Vous pouvez approuver ou rejeter les demandes d'exception dans l'espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Approuver ou rejeter les demandes dans le Espace de travail du gestionnaire de vulnérabilités.

Remarque :

Une fois qu'une demande d'exception pour un AVIT est approuvée, vous pouvez effectuer les actions suivantes :

- Rouvrir
- Obtenir plus de détails

Suivi d'une demande d'exception

Après avoir levé l'exception, vous pouvez suivre son état à l'aide de l'onglet **Approbations de changement d'état** de l'AVIT.

Expiration d'une demande d'exception et demande d'une extension d'une règle d'exception

Lorsqu'une demande d'exception pour un AVI particulier expire, l'AVI impacté revient à son état **Ouvert** .

Toutefois, à partir de la version 20, vous pouvez soumettre une demande d'extension de la date de **fin de** report sur la règle d'exception.

Configurer la gestion des exceptions pour Réponse aux vulnérabilités des applications

Limitez la durée d'une exception demandée et ajoutez un questionnaire à la demande d'exception ou de faux positif à l'aide du module. Par défaut, une exception est demandée à l'aide du ServiceNow® Réponse aux vulnérabilités des applications module. Vous pouvez également demander une exception à l'aide de l'intégration GRC : Gestion de la politique et de la conformité .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vul.app_manage_exception_configuration

Pourquoi et quand exécuter cette tâche
Si Réponse aux vulnérabilités cette option est activée, vous pouvez limiter la durée pendant laquelle une exception peut être demandée. De même, si le GRC : Gestion de la politique et de la conformité module est installé, vous pouvez sélectionner GRC : Gestion de la politique et de la conformité sur l'écran de configuration. L'activation de cette option vous permet de demander une exception qui spécifie l'objectif de politique et de contrôle à partir de GRC.

Si vous ajoutez un questionnaire, il est envoyé à la personne qui émet la demande d'exception ou de faux positif. Vous pouvez utiliser le questionnaire par défaut ou en créer un en fonction de vos besoins.

Il est utile que l'approbateur d'exceptions comprenne la raison de la demande d'exception.

Procédure
1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Configuration de gestion de l'exception, sélectionnez la façon dont vous souhaitez gérer une exception en sélectionnant une option dans la liste Gérer les exceptions à l'aide.

   Remarque : À partir de la Réponse aux vulnérabilités version 17.1, vous pouvez sélectionner soit Réponse aux vulnérabilités ou GRC : Gestion de la politique et de la conformité. Vous devez activer le module d'extension GRC à utiliser GRC : Gestion de la politique et de la conformité pour demander une exception. La modification de la configuration n'a pas d'impact sur les données existantes.

3. Renseignez les champs du formulaire en fonction de l'option que vous avez sélectionnée.
   - Si vous avez sélectionné l'option Réponse aux vulnérabilités , renseignez les champs du formulaire.

Paramètres pour le formulaire de gestion des exceptions VR

Champ	Description
Durée	Période pour laquelle une exception peut être demandée.
Unité	Unité de temps pour la période spécifiée.
Activer le questionnaire pour demander une exception	Option permettant d'ajouter un questionnaire à la demande d'exception en cours d'émission.
Questionnaire pour demander une exception	Option permettant d'afficher le questionnaire que vous avez sélectionné pour demander une exception. Le questionnaire d'exceptions s'affiche par défaut.
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Option permettant d'afficher le questionnaire que vous avez sélectionné pour le marquer comme faux positif. Le questionnaire pour la demande de faux positif s'affiche par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si vous avez sélectionné l'option GRC : Gestion de la politique et de la conformité , renseignez les champs du formulaire.

Paramètres pour le formulaire de gestion des exceptions VR

Champ	Description
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Option permettant d'afficher le questionnaire que vous avez sélectionné pour marquer comme faux positif. Le questionnaire pour la demande de faux positif s'affiche par défaut.

4. Sélectionnez **Enregistrer**.

Configurer les règles d'approbation pour la gestion des exceptions

Réponse aux vulnérabilités des applications À partir de la version 15.0, utilisez le concepteur de flux pour approuver les demandes d'exception pour la gestion des exceptions, les règles d'exception et la gestion des faux positifs. Si vous déployez Réponse aux vulnérabilités des applications (AVR) pour la première fois, le concepteur de flux est activé par défaut.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Si vous êtes un utilisateur VR existant, l'option par défaut est le workflow.
Si vous avez déployé Réponse aux vulnérabilités des applications la version 15.0 ou ultérieure, la valeur de la propriété *sn_vul.flow_designer_activation* système est définie sur vrai. Cela signifie que Flow Designer est activé par défaut.

Si vous utilisez déjà une version Réponse aux vulnérabilités des applications antérieure à la version 15.0, la valeur de cette propriété système est définie sur faux. Vous pouvez activer le concepteur de flux en changeant la valeur en vrai.

Remarque : Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer. Pour une comparaison détaillée entre le workflow et Flow Designer, reportez-vous à la section Comparaison du workflow de gestion des exceptions et du concepteur de flux.

Pour utiliser Flow Designer, créez des règles à l'aide du module Règles d'approbation. À l'aide de ce module, vous pouvez configurer des règles d'approbation pour chacun des workflows de gestion des exceptions suivants.

- Demande d'exception pour les tâches de rattrapage
- Demande d'exception pour les éléments vulnérables de l'application
- Règle d'exception
- Faux positif pour les tâches de remédiation
- Faux positif pour les éléments vulnérables de l'application

Remarque : Vous pouvez également définir des conditions contenant plusieurs niveaux d'approbation dans une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Règles d'approbation**.
2. Sur la page Règles d’approbation, sélectionnez le groupe pour lequel vous souhaitez définir la règle d’approbation.
3. Remplissez les champs du formulaire.

Formulaire Règle d'approbation

Champ	Description
Nom	Nom de configuration de l’approbation.
Table	Table sur laquelle la règle est appliquée.
Application	La valeur par défaut est Réponse aux vulnérabilités.
Type de règle	Spécifie le type de règle. Par exemple, gestion des exceptions, faux positifs ou règle d’exception.
Actif	Activé par défaut, ce qui signifie que la règle d’approbation est utilisée.
Description	Brève description des règles d’approbation.
Expirationde l’approbation (jours) À partir de la version 21.0 de Réponse aux vulnérabilités des applications	Date jusqu’à laquelle l’approbateur peut approuver la demande.
Notification de l'approbateur (jours) À partir de la version 21.0 de Réponse aux vulnérabilités des applications	Date après laquelle l’approbateur est notifié pour effectuer des actions.

4. Sélectionnez **Mettre à jour**.
   Dans l’onglet Configurations d’approbation, deux niveaux d’approbateurs sont configurés par défaut. Vous pouvez sélectionner une règle pour définir les conditions en fonction de différents cas d’utilisation au sein d’une règle.

> **Remarque :** Dans chaque page de configuration, vous pouvez créer plusieurs niveaux d’approbation.

Example:
En fonction de différents cas d’utilisation, vous pouvez définir différents processus d’approbation pour les mêmes vulnérabilités trouvées dans différents éléments de configuration.

Différer le rattrapage dans Réponse aux vulnérabilités des applications

À partir de la version 20.0, vous pouvez différer le rattrapage avec l’état **En attente d’implémentation** disponible pour les éléments vulnérables de l’application (AVI) et les tâches de rattrapage au fur et à mesure de leur cycle de vie. Vous pouvez uniquement faire passer manuellement des enregistrements à cet état en sélectionnant **En attente d’implémentation** dans AVI et les enregistrements de tâche de rattrapage à l’état **En cours d’examen** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation

En tant que spécialiste du rattrapage, vous pouvez déplacer un enregistrement dans **En attente d'implémentation** pour informer votre équipe que vos recherches et votre travail sur une tâche sont terminés. Vous pouvez choisir cette mise à jour si vous constatez qu'un correctif est prêt à être implémenté, mais qu'il n'est pas disponible. Un correctif logiciel est un exemple de correctif non disponible. Si la fenêtre de maintenance d'un correctif n'est pas disponible à la fin de vos recherches, vous pouvez déplacer la tâche vers **En attente d'implémentation** jusqu'à ce que le correctif puisse être déployé.

Champs obligatoires

Il existe deux champs obligatoires et modifiables dans les enregistrements AVI et de tâche de rattrapage qui sont à l'état En attente d'implémentation :

Date de l'engagement de rattrapage

Date de rattrapage prévue.

Plan de rattrapage

Description du plan de rattrapage pour le rattrapage. Ce texte s'affiche dans les notes de l'enregistrement.

Champs et propriétés système

Il existe deux propriétés système qui sont définies sur vrai par défaut pour le modal qui s'affiche lorsque vous faites passer un enregistrement en **attente d'implémentation**. S'ils sont laissés dans leurs paramètres par défaut :

sn_vul.remediation_fields

Définit la **date de l'engagement de rattrapage** et **le plan de rattrapage** comme champs obligatoires. Si la valeur est définie sur faux, ces champs sont facultatifs.

sn_vul.awaiting_implementation

Affiche le modal avec la **date d'engagement de rattrapage** et les champs **Plan de rattrapage** après **avoir sélectionné En attente d'implémentation** sur un enregistrement. Si la valeur est définie sur faux, vous pouvez changer l'état d'un AVI en attente d'implémentation sans invite pour saisir une date d'engagement ou un plan.

Module de la date de l'engagement de rattrapage non respecté

Affichez tous les AVI qui n'ont pas respecté leur date d'engagement de **rattrapage dans le module Date d'engagement de rattrapage non respectée** . Naviguer **Réponse aux vulnérabilités de l'application** > **Éléments vulnérables** > **Date de l'engagement de rattrapage non respectée** pour afficher la liste.

Restauration de l'état des tâches de rattrapage vers les AVI

Le bouton d'action d'interface utilisateur permettant la transition d'un enregistrement en **attente d'implémentation** n'est visible que sur les enregistrements d'élément vulnérable et de tâche de rattrapage de l'application à l'état **En cours d'examen** . Pour la restauration de l'état, dans le modal qui s'affiche lorsque vous sélectionnez **En attente d'implémentation** sur une tâche de rattrapage, vous pouvez **remplacer les AVI existants**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Sélectionnez **Remplacer les AVI existants**.	Sélectionnez cette option pour remplacer les dates d'engagement de rattrapage et les plans de rattrapage tous les AVI existants dans la tâche déjà à l'état **En attente d'implémentation** . Si elle est sélectionnée, cette fonctionnalité enregistre la date et les données de plan de la tâche de rattrapage vers les AVI.
Laisser désactiver **les AVI existants** .	Laissez l'option désactivée pour conserver intacts la date et les valeurs du plan pour tous les AVI existants sur la tâche déjà à l'état **En attente d'implémentation** . En cas de désactivation, les AVI déjà **en attente d'implémentation** conservent leurs données de date et de plan existantes et ne sont pas impactés par la restauration de l'état.

Restaurer des exemples

Supposons que vous souhaitiez faire passer une tâche de rattrapage de **Ouverte** à **En attente d'implémentation** afin de pouvoir mettre à jour la date d'engagement de la tâche et les informations de plan pour une fenêtre de maintenance des correctifs logiciels. Supposons que cette tâche comporte un AVI à l'état **En attente d'implémentation** et que vous souhaitez mettre à jour sa date d'engagement et ses informations de plan pour qu'elles correspondent à la tâche de rattrapage.

Pour remplacer la date des AVI et les données du plan afin qu'elles correspondent à la tâche de rattrapage, cochez la case pour **remplacer les AVI existants lorsque vous** y êtes invité. Les valeurs de date et de plan de l'AVI deviennent les valeurs de plan et de date que vous saisissez pour la tâche dans l'invite lorsque vous sélectionnez **En attente d'implémentation**.

Si vous ne sélectionnez pas l'option de remplacement dans ce cas et qu'il y a un AVI **en attente de mise en œuvre**, la date d'origine et les données de plan sur l'AVI restent intactes. Les valeurs de plan et de date que vous saisissez pour la tâche dans l'invite lorsque vous sélectionnez **En attente d'implémentation** ne sont pas utilisées sur les AVI déjà à l'état **En attente d'implémentation** de la tâche.

Si un AVI sur une tâche est **en état Résolu** ou **Fermé-corrigé** et que vous transférez la tâche en **attente d'implémentation**, la sélection de **Remplacer les AVI existants** ne modifie pas les AVI de **Fermé-fixe** et **Résolu** à **En attente d'implémentation** en raison d'une priorité d'état plus élevée.

Si le remplacement n'est pas sélectionné lors du déplacement de la tâche vers **En attente d'implémentation** et qu'il y a déjà un AVI **en attente d'implémentation** et que vous déplacez la tâche vers **Ouvert** ou **En cours d'examen**, l'AVI reste en **attente d'implémentation**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter un approbateur d'exception pour Réponse aux vulnérabilités des applications

Ajoutez des utilisateurs aux groupes d'approbateurs afin de pouvoir demander une exception.

Avant de commencer

Rôle requis : sn_vul.app_exception_approver

Pourquoi et quand exécuter cette tâche

Une demande d'exception pour un élément vulnérable de l'application est approuvée à l'aide du flux d'approbation à deux niveaux par défaut. La demande peut être approuvée par deux niveaux d'approbateurs. L'ajout d'utilisateurs au groupe de premier niveau est obligatoire. Si aucun utilisateur ne se trouve dans le deuxième niveau, la demande est approuvée après l'approbation de premier niveau.

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Groupes**.
2. Dans la colonne Nom, recherchez **Exception**, puis cliquez sur **Approbateur d'exception d'application : niveau 1**.

   Remarque : À partir de la Réponse aux vulnérabilités des applications version 12.8.1, vous pouvez utiliser les propriétés système fournies dans le système de base pour les approbations d'exception via workflow dans la table Propriétés système [sys_properties]. Ainsi, lorsqu'une demande d'exception ou de faux positif est émise via le workflow, elle est envoyée pour approbation aux ID de groupe définis dans la propriété système. Accédez à la **Tous** > **Propriétés système** et sélectionnez `sn_vul.app_exception_approver_L1`, `sn_vul.app_exception_approver_L2`ou `sn_vul.app_false_positive_approver_group` pour modifier la valeur de la propriété.

3. Dans le formulaire Approbateur d'exception d'application de groupe : niveau 1, cliquez sur la liste connexe Membres du groupe.
4. Cliquez sur **Nouveau** pour créer une liste.
5. Remplissez les champs du formulaire.

Formulaire d'utilisateur

Champ	Description
ID d'utilisateur	Identificateur unique pour l'utilisateur.
Prénom	Prénom de l'utilisateur.
Nom de famille	Nom de famille de l'utilisateur.
Titre	Fonction de l'utilisateur. Saisissez un titre ou une description de poste, ou sélectionnez-en un dans la liste.
Département	Département de l'utilisateur.
Mot de passe	Mot de passe affecté à l'utilisateur. Ce mot de passe peut être permanent ou temporaire.
Mot de passe à réinitialiser	Option permettant à l'utilisateur de réinitialiser le mot de passe pour garantir la sécurité.
Verrouillé	Option permettant de verrouiller l'utilisateur hors de l'instance et de mettre fin à toutes les sessions actives de l'utilisateur. Le système empêche les utilisateurs ayant le rôle admin de se verrouiller.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Option pour rendre cet utilisateur actif. Vous seul pouvez voir un utilisateur inactif dans les zones suivantes : ○ Listes d'utilisateurs ○ Liste de sélection sur les champs de référence (icône de loupe) ○ Liste de saisie semi-automatique qui s'affiche lorsque vous tapez dans un champ de référence
Accès au service Web uniquement	Option permettant de désigner cet utilisateur comme utilisateur non interactif.
Utilisateur d'intégration interne	Option permettant de désigner cet utilisateur comme utilisateur d'intégration interne.
E-mail	Adresse e-mail de l'utilisateur.
Langue	Langue préférée de l'utilisateur.
Intégration du calendrier	Calendrier utilisé pour gérer le calendrier de travail. Par exemple, Outlook.
Fuseau horaire	Fuseau horaire de l'emplacement de cet utilisateur.
Format de date	Format préféré de l'utilisateur pour les dates.
Tél. professionnel	Téléphone professionnel de l'utilisateur.
Tél. mobile	Téléphone mobile de l'utilisateur.
Photo	Photo que vous pouvez télécharger en cliquant sur **Cliquez pour ajouter...**.

6. Cliquez sur **Envoyer**.
7. **Facultatif :** Répétez les étapes 1 à 5 pour créer un approbateur d'exception d'application : niveau 2. L'approbateur doit accéder à **Application Vulnerability Response** > **Mes approbations et approuver les demandes** .

Demander et approuver une exception dans Réponse aux vulnérabilités des applications

Vous pouvez demander de différer le rattrapage d'un élément vulnérable applicatif et d'une tâche de rattrapage pour une période spécifiée.

Par exemple, en tant que développeur, vous pouvez demander une exception si un correctif n'est pas disponible pour un ordinateur. Les approbateurs disposant d'un accès peuvent approuver les demandes provenant d'autres utilisateurs.

Vous pouvez également créer des règles d'exception et demander une extension d'exception pour une règle d'exception. Par défaut, deux niveaux d'approbation sont requis pour les reports, les règles d'exception et les demandes d'extension d'exception.

Pour demander ou approuver une exception, consultez :

- Demander une exception pour un élément vulnérable de l'application
- Demander une exception pour les vulnérabilités d'applications à l'aide de GRC : Gestion de la politique et de la conformité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Approuver les règles d’exception et les demandes d’extension de règle d’exception dans Réponse aux vulnérabilités des applications
- Demander une extension pour une règle d’exception dans Réponse aux vulnérabilités des applications

Remarque :

Des notifications par e-mail sont envoyées à chaque étape de la gestion des exceptions, fournissant l’état et d’autres détails d’une demande. Par exemple, lorsqu’une exception est demandée, le demandeur reçoit un e-mail confirmant que la demande est soumise. L’approbateur reçoit également un e-mail indiquant qu’une exception a été demandée.

À partir de la version 21.0 de , vous pouvez configurer les délais d’approbation Réponse aux vulnérabilités des applications des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l’approbateur et le demandeur après un nombre de jours défini. Lorsqu’une demande est émise, l’élément vulnérable de l’application passe à l’état En cours de révision et un enregistrement de changement d’état est créé. Si l’approbateur ne répond pas dans le délai configuré, l’élément vulnérable de l’application ou la tâche de rattrapage revient à l’état Ouvert. L’état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d’approbation pour la gestion des exceptions.

Demander une exception pour un élément vulnérable de l’application

Demander une exception pour un élément vulnérable de l’application qui ne peut pas être corrigé immédiatement. Par exemple, en tant que développeur, vous pouvez demander une exception si un correctif n’est pas disponible pour un ordinateur.

Important : Vous pouvez demander des exceptions pour un élément vulnérable de l’application et une tâche de rattrapage à partir de l’espace de travail du gestionnaire de vulnérabilité et de l’espace de travail de rattrapage informatique. Pour plus d'informations, consultez Demander des exceptions pour les tâches et les enregistrements de rattrapage dans Espace de travail du gestionnaire de vulnérabilités et Demander une exception dans le Espace de travail de remédiation IT.

Avant de commencer

Rôle requis : Groupe de développeurs

Procédure

1. Accédez à la **Réponse aux vulnérabilités de l'application** > **Éléments vulnérables de l'application** > **Tous** et sélectionnez l’élément pour lequel vous souhaitez demander une exception. L’élément sélectionné doit être à l’état Ouvert ou En cours d’examen.

   Remarque :

   À partir de la version 21.0 de Réponse aux vulnérabilités des applications, l’état précédent d’un élément vulnérable d’application est stocké dans le champ **backup_state** .

2. Sur le formulaire Élément vulnérable de l’application, cliquez sur **Demande d’exception**.

   Remarque : Selon qu’il Réponse aux vulnérabilités est sélectionné ou GRC : Gestion de la politique et de la conformité dans le **Réponse aux vulnérabilités de l'application** > **Gestion des exceptions** , le formulaire de demande d’exception change. Si GRC : Gestion de la politique et de la conformité, reportez-vous à la section Demander une exception pour les vulnérabilités d’applications à l’aide de GRC : Gestion de la politique et de la conformité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Si Réponse aux vulnérabilités est sélectionné dans l'écran Gestion des exceptions, renseignez les champs du formulaire Demande d'exception.

Formulaire de demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée sélectionnée dans le **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Gestion des exceptions** écran. Lorsque la demande d'exception expire, le groupe revient à son état **Ouvert** . **Remarque :** À partir de la version 18.0 de (AVR), un élément vulnérable d'application Réponse aux vulnérabilités des applications différé peut être fermé et rouvert par un scanner. Si l'élément se rouvre avant l'expiration de la fenêtre d'exception, l'état de l'AVIT revient à l'état Différé, ce qui respecte la fenêtre d'exception active. Pour activer cette fonctionnalité, définissez la valeur de la propriété système sn_vul.auto_defer_avit_in_active_exception_window sur vrai. De plus, la date de fin différée persiste même après la fermeture de l'AVIT ou l'expiration de l'exception. Le rôle requis est sn_vul.app_manage_exception_configuration pour la lecture et l'écriture.
Motif	Sélectionnez le **motif**. Les choix possibles sont les suivants : ○ Risque accepté ○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Contrôle d'atténuation en place ○ Autre Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à Définir le mappage du motif de la politique.
Informations supplémentaires	Détails liés au motif pour lequel cette demande est effectuée. Ce champ obligatoire doit être mis à jour par le propriétaire du rattrapage.

4. Cliquez sur **Demander l'approbation** pour soumettre la demande d'exception.
L'état de l'élément de vulnérabilité de l'application passe à En cours de révision. Utilisez l'onglet **Approbation du changement d'état** pour suivre l'état de la demande d'exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander une exception pour les vulnérabilités d'applications à l'aide de GRC : Gestion de la politique et de la conformité

Demandez des exceptions à la politique à l'aide de l'aptitude de GRC gestion des exceptions de politique de l'application à partir de Réponse aux vulnérabilités des applications.Gestion de la politique et de la conformité

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions de politique, vous devez télécharger l'application à partir GRC : Gestion de la politique et de la conformité du ServiceNow Store.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions dans l'interface utilisateur classique :

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Éléments vulnérables de l'application** (ou **Tâches de remédiation**)>**Toutes**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.
   L'élément ou le groupe sélectionné doit être dans l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Sur le formulaire sélectionné, cliquez sur **Demande d'exception**.
3. Si GRC : Gestion de la politique et de la conformité est sélectionné dans l'écran Gestion des exceptions, renseignez les champs du formulaire Demande d'exception.

Formulaire de demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date actuelle. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert. **Remarque :** Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale de l'exception (jours)** que vous définissez pour la politique dans Politique et conformité. Pour plus d'informations, consultez Créer une politique .
Motif	Motif de la demande d'exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Justification	Détails liés au motif pour lequel cette demande est effectuée. Ce champ obligatoire doit être renseigné par le propriétaire du rattrapage.

a. Cliquez sur **Demander l'approbation** pour soumettre la demande d'exception.
L'état des éléments vulnérables passe à En cours de révision et une exception de politique est créée.
Utilisez l'onglet **Approbation du changement d'état** pour suivre l'état de la demande d'exception.

b. Cliquez sur la liste connexe Exceptions de politique pour afficher l'exception de politique.

c. Cliquez sur le numéro d'exception de politique.

d. Dans le champ **Approbateur** , sélectionnez son nom.

e. Cliquez sur l'onglet Source et sélectionnez un objectif de contrôle dans le champ **Objectif de contrôle** .

f. Cliquez sur l'onglet Évaluation des risques et sélectionnez l'évaluation du risque dans le champ **Évaluation du risque** .

g. Enregistrez le formulaire.

h. Cliquez sur l'onglet Contrôles impactés, puis sur Ajouter pour ajouter les contrôles.

i. Enregistrez le formulaire.

Remarque : Vous pouvez effectuer un examen de conformité en cliquant sur **Demander un examen de conformité**.

j. Le formulaire d'approbation est envoyé à l'approbateur.

k. En tant qu'approbateur, vous pouvez approuver la demande en cliquant sur **Approuver** ou demander une approbation supplémentaire en cliquant sur **Demander une approbation supplémentaire**.
L'état de l'enregistrement devient Différé. Le motif indiqué est celui que vous avez sélectionné lors de l'émission de la demande d'exception. L'onglet Report fournit des notes supplémentaires sur l'enregistrement.

Remarque : Si la demande est rejetée, l'enregistrement revient à son état précédent.

4. Cliquez sur **Envoyer**.
Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez Configuration facultative de Policy and Compliance Management .

Demander une exception pour une tâche de rattrapage d'application

Demandez une exception pour différer une tâche de rattrapage d'application pendant une période spécifiée si elle ne peut pas être résolue immédiatement.

Avant de commencer

Vous pouvez demander des exceptions aux espaces de Réponse aux vulnérabilités travail.
Consultez Demander une exception dans le Espace de travail de remédiation IT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Rôles requis : sn_vul.remediation_owner, sn_vul.app_security_champion ou sn_vul_container.remediation_owner.

Vous pouvez également demander des exceptions pour les tâches de rattrapage d'applications dans l'environnement classique.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Tâches de rattrapage** > **Tous**.
2. Sélectionnez le groupe pour lequel vous souhaitez demander une exception.
   La tâche sélectionnée doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Sur l'enregistrement de tâche de rattrapage de l'application, sélectionnez **Demande d'exception**.
4. Remplissez les champs du formulaire.

Formulaire de demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée d'exception définie dans la configuration.
Motif	Justification de la demande d'exception.
Informations supplémentaires	Détails liés au motif pour lequel cette demande est effectuée. Ce champ doit être mis à jour par le propriétaire du rattrapage.

5. Cliquez sur **Demander l'approbation**.

Approuver les règles d'exception et les demandes d'extension de règle d'exception dans Réponse aux vulnérabilités des applications

Approuvez les demandes d'exception pour les éléments vulnérables de l'application qui ne peuvent pas être corrigés immédiatement. Vous devez évaluer ces demandes pour connaître le risque, puis approuver leur report jusqu'à ce qu'elles puissent être corrigées.

Avant de commencer

Rôle requis : sn_vul.app_exception_approver

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir le mappage du motif de la politique

Vous pouvez définir les choix de motifs pour qu'ils soient accessibles à tout utilisateur qui demande une exception.

Avant de commencer

L'application GRC : Policy and Compliance Management doit être installée. Cette application est disponible auprès de avec ServiceNow® Store un abonnement séparé.

Pour plus d'informations sur la configuration système requise et la compatibilité des familles, consultez la liste des applications sur le site Web ServiceNow Store .

Rôles requis : sn_vul.compliance.manager et sn_vul.vulnerability_admin

Procédure

1. Accédez à la **Tous** > **Politique et Conformité** > **Exceptions de politique** > **Registre d'intégration**.

   Remarque : Vous pouvez sélectionner un motif parmi les choix de motifs disponibles dans la table Choix de motifs ou ajouter un nouveau motif.

2. Cliquez sur le registre d'intégration de votre application, par exemple, **Application Vulnerability Response**, **Vulnerability Response**...
3. Pour ajouter un choix de motif existant, procédez comme suit :
   a. Dans la liste Choix des motifs, cliquez sur **Nouveau**.
   b. Cliquez sur l'icône de loupe pour sélectionner un motif.
4. Pour ajouter de nouveaux choix de motifs à la table Choix de motifs, procédez comme suit :
   a. Dans la liste Choix des motifs, cliquez sur **Nouveau**.
   b. Cliquez sur l'icône de loupe.
   c. Cliquez sur **Nouveau**.
   d. Remplissez les champs du formulaire.

Formulaire Liste de choix de motifs

Champ	Description
Étiquette	Étiquette unique pour ce choix.
Valeur	Valeur unique pour ce choix. Cette valeur est mappée dans la table Mappages de motif d'exception de politique pour les applications respectives. Pour accéder à cette table, saisissez sn_vul_policy_reason_mapping. LIST dans le navigateur de filtre.
Ordre	Ordre pour ce choix. Les motifs sont classés en fonction de ce nombre.
Par défaut	Option pour indiquer que ce choix de motif sera disponible chaque fois qu'une exception de politique sur demande est demandée. Si le registre d'intégration ne contient pas de choix

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	spécifiques à l'application, tous les choix de motifs pour lesquels le champ **Par défaut** est sélectionné seront disponibles.
Actif	Option permettant d'afficher le choix dans la liste des choix de motifs.

5. Cliquez sur **Envoyer**.

Demander une extension pour une règle d'exception dans Réponse aux vulnérabilités des applications

Demandez une extension pour une règle d'exception différée avant qu'elle n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôles requis : Gestionnaire de sécurité des applications sn_vul.app_sec_manager, Champion de sécurité sn_vul.app_security_champion.

Pourquoi et quand exécuter cette tâche

Sur un enregistrement de règle d'extension, vous pouvez demander une extension pour la date **Différé jusqu'au** uniquement si la règle est dans l'état **Approuvé** . Vous pouvez demander cette extension d'une règle si vous constatez qu'un grand nombre d'enregistrements créés par la règle ne sont pas résolus dans sa date **Différé jusqu'à** , c'est-à-dire la date à laquelle la tâche de rattrapage cesse d'accepter les nouveaux AVI. L'extension met à jour la règle d'exception afin de prolonger automatiquement la date de report de votre règle existante.

Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Règles d'exception**.
2. Sélectionnez une règle d'exception approuvée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle la règle d'exception doit être prolongée.
Motif	Entrez le motif du report de la règle d'exception. Les choix sont les suivants : ○ Risque accepté ○ En attente de fenêtre de maintenance ○ Correctif non disponible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les champs Différé jusqu'à, Motif et Informations supplémentaires sont mis à jour sur la règle d'exception et les tâches de rattrapage associées et les éléments vulnérables de l'application. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une règle d'exception différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Demander une extension pour une tâche de rattrapage différée dans Réponse aux vulnérabilités des applications

Demander une extension pour une tâche de rattrapage différée (VUL) avant qu'elle n'atteigne sa date d'échéance différée. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Tâches de remédiation**.
2. Ouvrez une tâche de rattrapage différée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'état de report expire et la tâche de rattrapage est réactivée.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Une fois la demande approuvée, les changements apportés à la tâche de rattrapage sont également transférés aux éléments vulnérables de l'application, qui font partie de la tâche de rattrapage. Toutefois, les éléments vulnérables de l'application doivent être à l'état Différé et leur valeur actuelle jusqu'à ce que les données précèdent la date de fin de mise à jour. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une tâche de rattrapage différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Demander une extension pour un élément vulnérable d'application différé dans Réponse aux vulnérabilités des applications

Demandez une extension pour un élément vulnérable d'application différé avant qu'il n'atteigne sa date d'échéance différée. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Éléments vulnérables**.
2. Ouvrez un élément vulnérable d'application différé.
3. Sélectionnez **Demande d'extension**.

   Remarque : Le bouton Demande d'extension n'est visible que lorsque l'état de l'élément vulnérable de l'application est Différé.

4. Renseignez les champs du formulaire comme il convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'élément vulnérable d'application différé doit être prolongé pour correction.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants : ○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Un e-mail est déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Si une règle d'exception différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

6. Une fois la demande approuvée, les notes Jusqu'à, Motif et Report sont mises à jour.

Créer, supprimer et annuler une règle d'exception pour Réponse aux vulnérabilités des applications

Créez une règle pour demander automatiquement une exception pour les éléments vulnérables de l'application (AVI) qui répondent à des conditions spécifiques.

Avant de commencer

Par exemple, vous pouvez créer une règle avec une condition basée sur une vulnérabilité connue ou critique spécifique que vous savez ne pas pouvoir corriger immédiatement. Avec cette règle, vous pouvez différer automatiquement les AVI nouveaux et existants s'ils correspondent à la condition de règle approuvée.

- La règle d'exception s'applique à partir de la date de **début de validité** jusqu'à la date de **fin de validité** que vous saisissez dans l'enregistrement de règle.
- La tâche de rattrapage (AVUL) est créée une fois que la règle est approuvée pour les AVI correspondants à l'état **Différé** .
- La méthode de regroupement pour cette AVUL est connue sous le nom de règles d'exception.
- Vous ne pouvez pas fermer, rouvrir ou supprimer cet AVUL. Les AVI nouveaux et rouverts sont différés et ajoutés à cette AVUL à partir de la date de **début de validité** jusqu'à l'expiration du groupe à la date de **fin de validité** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de la règle d'exception. Ces e-mails fournissent l'état et d'autres détails d'une demande. Par exemple, lorsqu'une règle d'exception est demandée, le demandeur reçoit un e-mail confirmant l'envoi de la demande.

Si la règle est rejetée, vous pouvez la rouvrir à l'état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Rôles requis : responsable SEC de l'application sn_vul.app_sec_manager et champion de sécurité sn_vul.app_security_champion.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Règles d'exception**.
2. Sur la page Nouvel enregistrement de règle d'exception, sélectionnez **Nouveau**.
3. Renseignez les champs.

Champ	Description
Nom	Nom de la règle d'exception.
État	Lecture seule : brouillon
Début de validité	Date à partir de laquelle cette règle est active pour différer les AVI.
Ordre d'exécution	Ordre unique pour chaque règle d'exception Une valeur inférieure précède une valeur élevée.
Date de fin de validité	Date à laquelle la tâche de rattrapage n'accepte plus de nouveaux AVI.
Reporté jusqu'à	Date jusqu'au report des tâches de rattrapage et des AVI. À cette date, les AVUL sont fermés et tous les AVI sortent des tâches et sont rouverts. Les règles de groupe sont réappliquées à ces AVI.
Motif	Raison de la création de cette règle d'exception.
Groupe d'affectation	Groupe auquel la tâche de rattrapage est affectée pour le suivi des AVI différés.
Informations supplémentaires	Informations supplémentaires que le demandeur souhaite fournir à l'approbateur. Ces informations sont renseignées dans le champ Description de la tâche de rattrapage.
Condition	Conditions de filtre pour spécifier quels AVI correspondent à cette règle.
Exécuter sur les données existantes	Option qui vous permet d'exécuter cette règle sur des données existantes la première fois que cette règle est exécutée. Si vous laissez cette option désactivée, votre règle s'exécute quotidiennement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	par la tâche *Associate existing AVIs with Auto Exception Rule* planifiée en commençant par de nouvelles données. Si vous activez l'option Exécuter sur les données existantes, une tâche planifiée s'exécute une fois sur les données existantes à la date de **début de validité** .

4. Ajoutez le groupe d'affectation lorsque vous créez la règle.
5. Choisissez-en un.

Option	Description
Enregistrer la règle	Enregistrez vos changements et la règle s'affiche dans la liste des règles d'exception [sn_vul_auto_-exception_rule]. Tant que vous n'avez pas soumis la règle d'exception pour approbation, elle reste à l'état **Brouillon** .
Soumettre la règle	Si vous soumettez la règle, l'état de la de–mande devient **En cours de révision**. Une approbation de règle d'exception nécessite deux niveaux d'approbation, l'un de l'ap–probateur d'exception d'application de ni–veau 1 et l'autre de l'approbateur d'excep–tion d'application de niveau 2.

Une fois la règle approuvée, elle passe à l'état **Approuvé** . Votre règle évalue les AVI avec la *Associate existing AVIs with Auto Exception Rule scheduled* tâche. Si vous avez sélectionné **Exécuter sur les données existantes**, les AVI existants sont évalués. Une tâche de rattrapage est automatiquement créée pour la règle, et tous les AVI correspondants qui remplissent ses conditions sont associés à la tâche.

La tâche planifiée exécute la règle d'exception une seule fois sur les données existantes. La règle ne s'exécute pas à nouveau sur les données existantes même si aucun AVI n'est trouvé. Elle évalue uniquement les nouvelles données, car les AVI existants correspondant à la règle ont déjà été reportés.

6. Pour supprimer une règle, sélectionnez **Supprimer** dans l'enregistrement de la règle d'exception.
   Le message suivant s'affiche : Si vous supprimez la règle, la tâche de rattrapage associée sera supprimée et les éléments vulnérables associés seront rouverts. Les règles de tâche de rattrapage seront ensuite appliquées aux AVI individuels et la règle d'exception sera supprimée.
7. Sélectionnez**Conserver la règle** pour arrêter ou **Supprimer la règle** pour continuer.
8. Pour désactiver une règle tout en la conservant dans la liste des règles d'exception, sélectionnez **Annuler**.
   Le message suivant s'affiche : Si vous annulez cette règle, la tâche de rattrapage associée sera supprimée et les éléments vulnérables associés seront rouverts. Les règles de tâche de rattrapage seront ensuite appliquées aux éléments vulnérables individuels et la règle d'exception passera à l'état de brouillon.
9. Sélectionnez**Conserver la règle** pour l'arrêter ou **Annuler** pour passer la règle à **l'état Brouillon** et la désactiver.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Vue d'ensemble des tâches de rattrapage et des règles de tâche

Configurez les tâches de rattrapage (AVUL) pour aider les analystes et les spécialistes du rattrapage à organiser les éléments vulnérables de l'application (AVI) et à les analyser en bloc. Les critères selon lesquels les tâches de rattrapage sont formées sont configurés de sorte que les AVI sont automatiquement affectés aux tâches de rattrapage. Les tâches de rattrapage vous permettent de surveiller la progression et de piloter le processus de rattrapage plus efficacement.

Suivi du nombre de reports pour les éléments vulnérables et les tâches de rattrapage de l'application

Suivez le nombre de reports d'un élément vulnérable, d'un élément vulnérable d'application, d'un élément vulnérable de conteneur ou d'une tâche de rattrapage. La *`set deferral counts`* tâche planifiée s'exécute quotidiennement pour valider les nombres des enregistrements qui sont différés plusieurs fois dans la colonne Nombre de reports. Les enregistrements sont affichés dans les modules Reports multiples pour VR, AVR et CVR.

Comprendre les règles de tâche de rattrapage

Les règles de tâche de rattrapage vous permettent de définir comment les éléments vulnérables d'application sont automatiquement regroupés et affectés. Règle par défaut **Vulnerability** est incluse dans le système de base qui rassemble les AVI en fonction de leurs vulnérabilités. Toutefois, vous pouvez effectuer un regroupement par tout autre ensemble de valeurs dans des colonnes accessibles à partir de l'AVI. Ces valeurs peuvent inclure l'élément de configuration (CI), l'entrée de vulnérabilité et autres.

Il existe des règles de tâche pour Application Vulnerability Response qui sont incluses dans l'application Réponse aux vulnérabilités disponible lorsque vous l'activez.

Vous pouvez créer plusieurs conditions avec le générateur de conditions. Dans la section Grouper par, une autre ligne s'affiche après avoir défini une paire de champs. Vous pouvez avoir jusqu'à six sélections **Grouper par** . Vous pouvez également automatiser l'affectation des groupes. Voir Affecter automatiquement des éléments vulnérables d'applications Réponse aux vulnérabilités des applications et Filtrage au sein de Réponse aux vulnérabilités pour plus d'informations.

Par exemple, vous pouvez regrouper les éléments vulnérables de votre application par élément de configuration ou par modèle de produit. Vous pouvez avoir une règle de tâche unique pour les vulnérabilités de faible gravité ou les CI à faible risque. Vous pouvez avoir une autre règle de tâche pour les serveurs critiques et les vulnérabilités qui exposent l'entreprise à plus de risques. Consultez la rubrique Créer, modifier et supprimer des règles de tâche de rattrapage Réponse aux vulnérabilités des applications pour plus d'informations sur les options qui s'offrent à vous.

Un ensemble différent de règles peut être utilisé pour les éléments vulnérables de l'application qui exposent l'entreprise à davantage de risques. Le nom de la tâche de rattrapage est ajouté à la règle de tâche de rattrapage **Grouper par** valeurs pour faire la brève description du nouvel enregistrement.

Lorsqu'un nouvel élément vulnérable d'application est créé, importé ou rouvert après avoir été fermé, les règles sont évaluées par rapport à celui-ci. Un AVI n'est évalué qu'une seule fois, automatiquement, à moins qu'il ne soit rouvert après avoir été fermé ou que les règles ne soient réappliquées manuellement.

Le processus suivant est utilisé pour chaque AVI nouveau ou rouvert :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour chaque règle de tâche de rattrapage, l'AVI est comparé au filtre de règle de tâche de rattrapage.

- Pour chaque règle où la condition de la règle de tâche de rattrapage est vérifiée, la règle extrait les données des sélections **Grouper par** sur l'AVI. Il génère un nom de groupe et un champ. Dans ce cas, **risque élevé : QID-32342 :** *`résumé de QID-3242`* (Nom : ID de vulnérabilité : résumé de la vulnérabilité).

  Remarque : Le champ Description brève est limité à 160 caractères. Les résumés de vulnérabilité plus longs sont tronqués.

  La règle vérifie s'il existe une tâche de rattrapage **ouverte** correspondante affectée au même groupe d'affectation que l'AVI.

  - Si la tâche est trouvée, l'AVI est ajouté à la tâche existante à l'état **ouvert** .
  - Si aucune tâche à l'état **Ouvert** n'est trouvée, la règle crée une tâche **à risque élevé : QID-32342** , l'affecte au même groupe d'affectation que l'AVI et place l'AVI dans la tâche de rattrapage.

Plusieurs règles de tâche de rattrapage peuvent être définies pour regrouper différents types de vulnérabilités. Étant donné que chaque vulnérabilité est comparée aux conditions de la règle de tâche de rattrapage avant de la placer dans une tâche de rattrapage, trop de règles peuvent avoir un impact sur les performances. Configurez vos règles de tâche afin que les conditions vous aident à éviter de créer des tâches de rattrapage en double.

Par défaut, les règles de tâche de rattrapage utilisent le groupe d'affectation défini par les **règles d'affectation** sur l'AVI lors du regroupement des éléments et affecte la tâche de rattrapage pour correspondre aux AVI.

Dans le cadre de la règle de tâche par défaut, l'affectation de ces tâches de rattrapage est contrôlée par les règles du module **Règles d'affectation** . Pour plus d'informations sur les règles d'affectation, reportez-vous à Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Lorsqu'une règle de tâche est supprimée de la vue de formulaire ou de liste, vous avez la possibilité de supprimer toutes les tâches **ouvertes** créées par cette règle. Les tâches dont l'état **n'est pas Ouvert** sont exclues.

Réapplication des règles de tâche de rattrapage

Lorsque vous souhaitez modifier une règle de tâche de rattrapage, utilisez le bouton **Réappliquer** sur la page de règle de tâche de rattrapage pour réexécuter la règle modifiée sur toutes les tâches de rattrapage **ouvertes** actives créées par cette règle. Elle supprime et recrée automatiquement les tâches de rattrapage en fonction de la règle modifiée.

La réapplication vérifie uniquement les tâches de rattrapage existantes.

Une fois que vous avez sélectionné **Réappliquer**, le message suivant s'affiche : La réapplication de cette règle de tâche de rattrapage supprimera et recréera les tâches de rattrapage pour cette règle. Les tâches de rattrapage qui ne sont pas à l'état Ouvert ne sont pas supprimées.

Créer des tâches de rattrapage et ajouter manuellement des AVI

Vous créez une tâche de rattrapage d'application (AVUL) à partir d'un autre enregistrement de tâche de rattrapage d'application et ajoutez manuellement des éléments vulnérables

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'application (AVIT). Consultez Créer manuellement une tâche de rattrapage d'application dans Réponse aux vulnérabilités des applications pour plus d'informations.

Règles de tâche de rattrapage et création et mise à jour AVI

Si un CI ou un modèle de produit d'une analyse est associé à une vulnérabilité connue, un AVI est créé. Une fois créé, l'AVI est évalué par rapport aux conditions des règles de tâche de rattrapage pour une correspondance. S'il y a une correspondance avec une tâche de rattrapage existante, l'AVI est ajouté. Si aucune tâche de rattrapage correspondante n'est trouvée, une tâche de rattrapage est créée pour l'AVI.

Si une propriété capturée dans les conditions de filtrage de la tâche de rattrapage est mise à jour ou modifiée sur un AVI, l'AVI mis à jour est également évalué par rapport aux règles de la tâche de rattrapage pour une correspondance. S'il y a une correspondance avec une tâche de rattrapage existante, l'AVI est ajouté. Si aucune tâche de rattrapage correspondante n'est trouvée, une tâche est créée pour l'AVI.

Déploiement et généralisation de l'état

Si vous mettez à jour une tâche de rattrapage sur Ouvert, ou d'Ouvert sur En cours d'examen, le nouvel état s'applique à tous les AVI associés. La réduction de l'état se produit immédiatement après le changement de l'état.

Le déploiement de l'état des AVI vers la tâche de rattrapage se produit uniquement si tous les AVI de la tâche sont à l'état **Différé** ou **Fermé - fixe** . Le déploiement est effectué avec la tâche planifiée, qui s'exécute toutes les `Rollup application vulnerable item values to vulnerability and group` 15 minutes. L'état n'est pas déployé tant que la tâche ne s'exécute pas. Pour qu'un état se répète entre les AVI et la tâche de rattrapage, tous les AVI doivent être dans le même état.

Créer, modifier et supprimer des règles de tâche de rattrapage Réponse aux vulnérabilités des applications

Vous pouvez créer des règles pour regrouper automatiquement les éléments vulnérables de l'application (AVI) en tâches de rattrapage (AVUL) en fonction des conditions de filtre. Ces règles regroupent automatiquement les AVI à mesure qu'ils sont importés ou créés manuellement.

Avant de commencer

Si vous créez une règle, elle ne s'applique pas aux données existantes. Une fois que vous l'avez soumise, elle est exécutée sur de nouvelles importations.

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Règles de la tâche de rattrapage**.
2. Ouvrez la règle ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire ou modifiez-les.

Règle de la tâche de rattrapage

Champ	Description
Nom	Nom de la règle de tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Indique si la tâche est active.
Description	Description de la règle.
Sensible à la casse	Détermine si une condition est sensible à la casse ou non. **Remarque :** La valeur par défaut est insensible à la casse.
Condition	Conditions de filtre facultatives pour la règle. Par défaut (case **sensible à la casse** non cochée), le texte de recherche que vous saisissez dans le générateur de conditions sur les enregistrements de règles de tâche et les formulaires n'est pas sensible à la casse. Vous pouvez activer les recherches sensibles à la casse sur les enregistrements de tâches et les formulaires. Voici un exemple de condition : **Vulnérabilité** > **est** > **VULNENT123451** (une vulnérabilité importée connue). Tous les AVI qui présentent cette vulnérabilité correspondent à cette condition.
Grouper par (jusqu'à six ensembles de conditions sont disponibles)	
Regrouper les éléments vulnérables de l'application à partir de	Table que la règle utilise pour regrouper les AVI. Sélectionnez les éléments de l'arborescence : ○ Élément vulnérable de l'application [sn_vuln_vulnerable_item] ○ Élément vulnérable d'application Élément de configuration [cmdb_ci] ○ Élément vulnérable de l'application Vulnérabilité de l'application [sn_vul_third_party_entry] ○ Modèle de produit d'élément vulnérable d'application **Remarque :** Si vous choisissez une table étendue, le **champ Utilisation** n'est appliqué qu'aux éléments vulnérables de l'application qui utilisent cette table étendue.
Utilisation du champ	Champ de la table que la règle utilise pour regrouper les AVI. Sélectionnez les conditions dans l'arborescence. **Remarque :** Vous pouvez créer des conditions de groupement par afin que tous les AVI qui partagent des données ne soient pas affectés à la même tâche de rattrapage. Par exemple, si vous sélectionnez Groupe d'affectation et Adresse IP comme champs Utilisation, et que plusieurs AVI correspondent à la condition de filtrage initiale **Vulnérabilité**, ces AVI peuvent être affectés à des groupes d'affectation distincts pour le rattrapage à l'aide des nombreuses options disponibles dans la section Grouper par. Les conditions Grouper par vous donnent la possibilité de créer des tâches de rattrapage distinctes qui peuvent être affectées à différents groupes, même s'ils partagent certaines données.
Affectation	
Affecter la tâche de rattrapage par	Lors de l'affectation automatique des tâches de rattrapage, le choix Affectation est utilisé en plus des choix **Grouper par** pour regrouper les éléments vulnérables. De nouvelles tâches sont créées, selon les besoins,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	afin que chaque AVI soit placé dans une tâche avec un groupe d'affectation correspondant défini. Pour automatiser l'affectation des tâches créées en fonction de cette règle, choisissez l'une des options disponibles. ○ Regrouper par champ : si vous avez sélectionné un champ de groupe d'utilisateurs dans les valeurs **de champ Utilisation** de la section **Grouper par**, elles apparaissent dans le menu déroulant. ○ Groupe d'utilisateurs : utilisez la liste de recherche pour sélectionner un groupe d'utilisateurs statique.

Si vous supprimez une règle à partir de la vue de formulaire ou de liste, vous avez la possibilité de supprimer toutes les tâches de rattrapage **ouvertes** créées par cette règle. Les groupes dont l'état n'est pas **Ouvert** sont exclus.

4. Sélectionnez **Soumettre pour les** nouvelles règles.
   Une fois que vous avez sélectionné **Soumettre**, votre règle s'affiche dans la liste Règles de la tâche de rattrapage [sn_vul_grouping_rule]. Les situations suivantes déclenchent votre règle.
   - Lorsque de nouveaux AVI sont créés.
   - Lorsque vous sélectionnez **Réappliquer**. Vous sélectionnez **Réappliquer** pour évaluer les règles de tâche sur les tâches de rattrapage existantes uniquement.
   - Lorsque les AVI sont mis à jour, par vous ou par le système.

     Si un AVI est mis à jour, les règles de tâches sont évaluées pour déterminer les correspondances avec les tâches de rattrapage existantes. Voici quelques mises à jour courantes qui lancent une vérification des règles :
     - Lorsque l'état passe de Fermé à Ouvert, ou de Fermé à En cours d'examen.
     - L'élément de configuration (CI) est modifié.
     - La vulnérabilité est changée.

   Le système vérifie toutes les règles de tâche pour voir s'ils correspondent à l'AVI mis à jour. Si les conditions d'une règle correspondent aux conditions d'une tâche de rattrapage, les AVI correspondants lui sont affectés.

   Si aucune correspondance n'est trouvée, une nouvelle tâche de rattrapage est créée.

   Pour plus d'informations sur le déploiement de l'état des AVI vers les tâches de rattrapage et sur la réduction de l'état des tâches de rattrapage vers les AVI, reportez-vous à la section Réponse aux vulnérabilités des applications Vue d'ensemble des tâches de rattrapage et des règles de tâche.

   Pour obtenir un exemple de règle de tâche de rattrapage, reportez-vous à la section Réponse aux vulnérabilités des applications Exemples de règles de tâches de rattrapage.

5. Pour supprimer une règle de tâche, sélectionnez-la dans la liste Règles de tâche de rattrapage, puis sélectionnez **Supprimer**.
   Le message suivant s'affiche : La règle de tâche de rattrapage sélectionnée a créé n tâches de rattrapage. Parmi les tâches de rattrapage, n sont à l'état Ouvert.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Case à cocher désactivée (par défaut).	Supprimez uniquement la règle. Les tâches dont l'état **n'est pas Ouvert** sont exclues.
Case à cocher sélectionnée.	Incluez les tâches de rattrapage dans l'état **Ouvert** lorsque vous supprimez la règle de tâche de rattrapage. Supprimez la règle et toutes les tâches de rattrapage à l'état **ouvert** .

6. Choisissez une option et sélectionnez **Supprimer**.

Créer manuellement une tâche de rattrapage d'application dans Réponse aux vulnérabilités des applications

Créez une tâche de rattrapage d'application (AVUL) à partir d'un autre enregistrement de tâche de rattrapage d'application et ajoutez manuellement des éléments vulnérables d'application (AVIT).

Avant de commencer

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Tâches de remédiation** > **Tous**.
2. Dans l'angle supérieur droit de la page, sélectionnez **Nouveau**.
3. Dans l'onglet Configuration du groupe, pour Méthode de regroupement, sélectionnez **Manuel**.
4. Sélectionnez **Soumettre**.
5. Localisez votre nouvel enregistrement de tâche (AVUL) sur la table Tâches de remédiation d'applications [sn_vul_app_vulnerability].
   L'enregistrement est créé à l'état **Ouvert** .
6. Ouvrez l'enregistrement et ajoutez des éléments vulnérables d'application nouveaux ou existants à ce groupe à l'aide de la liste connexe des éléments vulnérables d'application (**Modifier** ou **Ajouter**).
7. Sélectionnez **Mettre à jour** pour enregistrer l'enregistrement ou d'autres actions d'interface utilisateur pour faire passer l'enregistrement à un autre état.

Créer des règles de fermeture automatique

Utilisez les règles de fermeture automatique pour fermer automatiquement les anciens AVIT en fonction des conditions de filtre que vous avez définies.

Avant de commencer

Rôle requis : sn_vul.app_manage_auto_close_rules

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Règles de fermeture automatique**.
   Le système de base fournit les règles de fermeture automatique suivantes :

   Vulnérabilités d'applications analysées en dernier Les vulnérabilités qui n'ont pas été signalées au cours des 90 derniers jours passent à l'état **Périmé.**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Sélectionnez **Nouveau** pour créer une nouvelle règle de fermeture automatique.
3. Renseignez les champs du formulaire.

Champ	Valeur
Nom	Nom de la règle de fermeture automatique.
Actif	Option permettant d'activer la règle. Si elle est activée, elle ferme automatiquement toutes les détections correspondant à ses critères de filtre.
Ordre d'exécution	Valeur unique pour l'exécution de la règle de fermeture automatique. Cette valeur détermine l'ordre d'exécution. La valeur par défaut est 100.
Type d'intégration	Intégration de vulnérabilité de l'application
Description	Description de la règle de fermeture automatique.
Condition	Conditions de filtre utilisées pour identifier les détections qui doivent être fermées.

4. Sélectionnez **Soumettre**.

La tâche **planifiée du processeur de règles de fermeture automatique** s'exécute tous les soirs. Il identifie les AVIT en fonction des conditions spécifiées et fait passer ceux qui correspondent à l'état **Périmé.** Dans les cas où il y a des AVIT avec des statuts « Fermé » et « Périmé », l'AVIT est fermé avec le sous-état défini sur **Fixe**.

Configurer les tests de pénétration

Vous pouvez configurer la durée du sprint et l'effort estimé pour les types d'évaluation des tests de pénétration. Cela fournit la fonctionnalité de planification pour les propriétaires d'applications, ce qui les aide à déterminer un délai provisoire pour leurs demandes d'évaluation de test de pénétration.

Avant de commencer

Rôle requis : Hacker éthique

Pourquoi et quand exécuter cette tâche

La configuration des paramètres d'évaluation du test de pénétration pour l'équipe de piratage éthique permet également de déterminer le groupe et le point de contact qui reçoivent la demande d'évaluation de test de pénétration.

À partir de la version 19.0 de Réponse aux vulnérabilités, si vous utilisez le Veracode Vulnerability Integration, les tests d'évaluation de pénétration dans le Veracode Vulnerability Integration sont des conclusions manuelles de Veracode. Ils ne sont pas liés à des demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les évaluations de tests de pénétration de , reportez-vous à Veracode la Veracode Vulnerability Integration section .

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Configuration du test de pénétration**.
2. Utilisez la première section pour configurer le groupe d'affectation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Remplissez les champs du formulaire.

Formulaire de configuration du test de pénétration

Champ	Description
Groupe d'utilisateurs de l'équipe de test de pénétration	Groupe auquel la demande d'évaluation de test de pénétration est affectée.
Délégataire par défaut des demandes d'évaluation de test de pénétration	Point de contact pour la demande d'évaluation de test de pénétration.

4. Sélectionnez **Mettre à jour**.
5. Utilisez la deuxième section pour configurer les sprints.
   Pour plus de détails, voir Configurer les sprints pour le test de pénétration.
6. Utilisez la troisième section pour configurer les types d'évaluation.
   Pour plus de détails, voir Configurer les types d'évaluation pour les tests de pénétration.

Configurer les sprints pour le test de pénétration

Configurez la durée et la capacité du sprint pour l'équipe de piratage éthique afin qu'elle puisse gérer la capacité de sprint pour les évaluations de tests de pénétration.

Avant de commencer

Rôle requis : Piratage éthique

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Configuration du test de pénétration**.
2. Sélectionnez l'option **Configurer** pour Configurer les sprints.
3. Remplissez les champs du formulaire.

Formulaire Configuration du sprint

Champ	Description
Durée du sprint (jours)	Nombre de jours dans un sprint.
Date de début	Date de début de la durée du sprint.
Nombre de sprints	Nombre de sprints pouvant être générés, en fonction des dates de début et de fin de la plage de sprint.
Date de fin	Date de fin de la durée du sprint.
Capacité de sprint	
Capacité de sprint (h)	Capacité d'un sprint en heures.

4. **Sélectionnez Générer des sprints**.
   Pour afficher les sprints créés, sélectionnez **Afficher les sprints**.

> **Remarque :** Une fois les sprints générés et en cours, si vous sélectionnez **Générer des sprints** pour la même durée, le sprint actuel se termine comme d'habitude. Les sprints restants sont recalculés en fonction de la configuration de sprint mise à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les types d'évaluation pour les tests de pénétration

Configurer l'effort estimé pour chaque type d'évaluation de test de pénétration. Cela vous permet de gérer la capacité de chaque sprint, en estimant l'effort requis pour chaque type d'évaluation.

Avant de commencer

Rôle requis : Piratage éthique

Pourquoi et quand exécuter cette tâche

Chaque sprint est affecté à une demande de test de pénétration. En fonction de l'effort estimé pour le type d'évaluation, les heures sont ajustées pour refléter le solde des heures du sprint.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Configuration du test de pénétration**.
2. À partir de la version 19.0 sur , sélectionnez **Configurer** pour afficher les types d'évaluation, la taille de l'application Réponse aux vulnérabilités et l'effort estimé.
3. **Facultatif :** Sélectionnez un enregistrement de type d'évaluation pour mettre à jour les champs selon vos besoins ou créer de nouveaux enregistrements.

   (Optional) Les valeurs de taille de l'application vous offrent plus d'options pour vous aider à estimer plus précisément le temps et l'effort du test. Vous pouvez modifier les heures de ces enregistrements ou sélectionner **Nouveau** pour créer vos propres combinaisons.

   Vous pouvez modifier le type d'évaluation et la taille de l'application sur les valeurs des enregistrements de demande de test de pénétration existants afin de pouvoir planifier des tests en fonction de la capacité de sprint. Par exemple, si vous remplissez une demande de test, il est possible que vous ne voyiez pas le nombre de sprints que vous avez configurés, car certains sprints sont déjà pris à des fins de test. Si les heures d'effort estimées d'un sprint correspondent à la combinaison requise pour le type et la taille d'un test, elles ne sont pas disponibles pour les nouvelles demandes.

   Vous pouvez voir les sprints qui sont affectés aux demandes de test sur les enregistrements de la liste des sprints de test de pénétration à l'adresse **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Configuration du test de pénétration** > **Configurer les sprints**. Consultez Configurer les sprints pour le test de pénétration pour plus d'informations sur la configuration des sprints.

   Les valeurs de base pour le type d'évaluation, la taille de l'application et l'effort estimé sont les suivantes :

Formulaire de configuration de type d'évaluation de test de pénétration

Type d'évaluation	Taille de l'application	Efforts estimés (h)
Test ciblé	Petit	20
Test ciblé	Moyen	30
Test ciblé	Grand	40
Test ciblé	Standard	40
Re-tester	Petit	10
Re-tester	Moyen	15

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type d'évaluation	Taille de l'application	Efforts estimés (h)
Re-tester	Grand	20
Re-tester	Standard	20
Test de pénétration complet	Petit	60
Test de pénétration complet	Moyen	70
Test de pénétration complet	Grand	80
Test de pénétration complet	Standard	80

4. Sélectionnez Mettre à jour pour enregistrer vos changements ou Soumettre pour un nouvel enregistrement.
5. Avant la version 19.0, sélectionnez l'option **Configurer** pour Configurer les types d'évaluation.
6. Mettez à jour les valeurs des types d'évaluation selon vos besoins.
   Les valeurs de base sont les suivantes :

Formulaire de configuration de type d'évaluation de test de pénétration

Type d'évaluation	Efforts estimés (h)
Test ciblé	40
Re-tester	20
Test de pénétration complet	80

7. Enregistrez les changements.

Intégrer Réponse aux vulnérabilités des applications avec d'autres applications

Réponse aux vulnérabilités inclut la prise en charge des intégrations tierces.

Intégrations tierces

Les intégrations de vulnérabilité des applications permettent d'enrichir les données de vulnérabilité des applications sur votre instance en récupérant les données des systèmes externes et des fournisseurs. Consultez les rubriques générales suivantes pour en savoir plus sur les intégrations prises en charge :

- Fortify Vulnerability Integration
- GitHub Application Intégrations de vulnérabilités
- Invicti Vulnerability Integration
- Veracode Vulnerability Integration
- Intégration de Réponse aux vulnérabilités avec Black Duck
- Ingestion manuelle des vulnérabilités pour Application Vulnerability Response
- Intégration Atlassian Jira

Important : Dans l'espace de travail du gestionnaire de vulnérabilités, vous pouvez créer manuellement un problème Agile à l'aide de l'action de liste et de l'action de formulaire pour suivre le rattrapage des AVIT et des RT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Les intégrations multisources ne sont pas prises en charge dans Réponse aux vulnérabilités des applications. Les intégrations tierces sont traitées séparément. Si plusieurs applications d'intégration tierces sont utilisées dans votre environnement, il n'y a pas de déduplication d'élément vulnérable d'application (AVI) entre les intégrations.

Le tableau suivant fournit une liste des intégrations créées par ServiceNow® et des Réponse aux vulnérabilités des applications partenaires pour importer des vulnérabilités et créer des éléments vulnérables.

Vulnerability Response : intégrations d'infrastructure

Fournisseur	Produit du fournisseur	Résumé de l'intégration	Lien vers la boutique en ligne	Fonctionnalités principales	Généré par
Veracode	Analyse dynamique Veracode	Importer le test, les politiques, les résultats Importer les résultats DAST Importer les résultats SAST Importer les résultats SCA			ServiceNow®
Qualys ÉTAIT					ServiceNow®
					ServiceNow®
					Partenaire
					ServiceNow®
					ServiceNow®
					Partenaire
					Partenaire
					Partenaire
					Partenaire
					Partenaire
					Partenaire
					Partenaire
					Partenaire
					Partenaire
					Partenaire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vulnerability Response : intégrations d'infrastructure (suite)

Fournisseur	Produit du fournisseur	Résumé de l'intégration	Lien vers la boutique en ligne	Fonctionnalités principales	Généré par
					Partenaire
					Partenaire
					Partenaire
					Partenaire
					Partenaire

Réponse aux vulnérabilités applications et CSDM tables

Réponse aux vulnérabilités des applications Les Réponse aux vulnérabilités intégrations et Nomenclature logicielle applications de vulnérabilité tierces gèrent les tables (y contribuent des données). CSDM Ces applications utilisent également des données provenant de CSDM tables générées par d'autres applications. Plusieurs ServiceNow produits bénéficient donc de ces Opérations de sécurité applications et y ajoutent de la valeur. Consultez Réponse aux vulnérabilités applications et CSDM tables pour plus d'informations.

Remarques supplémentaires sur les intégrations

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités des applications mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Les intégrations de vulnérabilité pour Réponse aux vulnérabilités des applications sont configurées pour s'exécuter sur une base planifiée. Toutefois, vous pouvez les exécuter manuellement si nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_vul.app_read_integrations

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Intégrations**.
2. Ouvrez l'enregistrement de l'intégration que vous souhaitez exécuter.
3. Cliquez sur **Exécuter maintenant**.

Intégration de Réponse aux vulnérabilités avec Black Duck

L'intégration Réponse aux vulnérabilités utilise Intégration de Réponse aux vulnérabilités avec Black Duck les données importées de l'outil Black Duck Software Composition Analysis (SCA) pour vous aider à déterminer l'impact et la priorité des failles dans votre code.

Vue d'ensemble de l'intégration

Avec le Intégration de Réponse aux vulnérabilités avec Black Duck, vous pouvez collecter SCA et mettre ces données à la disposition du ServiceNow AI Platform. À partir de la version 22.0.5 de , vous pouvez importer des données de Réponse aux vulnérabilités vulnérabilités SCA dans votre instance afin d'identifier les vulnérabilités dans vos applications logicielles. Pour plus d'informations, consultez Explorer Nomenclature logicielle.

Une API partagée ingère les données SCA.

Remarque : Chaque enregistrement d'intégration a un utilisateur run-as configuré. La valeur par défaut pour cet utilisateur est Système VR. Ne changez pas cette valeur.

Chaque jour, les travaux planifiés appellent automatiquement les intégrations dans l'ordre dans lequel elles sont répertoriées. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Versions disponibles

Versions disponibles de l'intégration Black Duck

Version de mise en production	Notes de publication
Intégration de Réponse aux vulnérabilités avec Black Duck 1.0.5	Notes de version Réponse aux vulnérabilités des applications

Groupe d'utilisateurs et rôles

Le Intégration de Réponse aux vulnérabilités avec Black Duck est installé par un utilisateur disposant du rôle administrateur et configuré par un membre du groupe Gestionnaire App-Sec. Pour en savoir plus, voir Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs.

Pour les états d'exécution de l'intégration, consultez Afficher l'état d'exécution de l'importation Intégration de Réponse aux vulnérabilités avec Black Duck

Pour afficher les données dans les vulnérabilités tierces, reportez-vous à la section Afficher les bibliothèques de vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préparer les tâches de pré-intégration pour Intégration de Réponse aux vulnérabilités avec Black Duck

Planifiez et exécutez les tâches de pré-intégration afin que votre Intégration de Réponse aux vulnérabilités avec Black Duck intégration réussisse. Cela Intégration de Réponse aux vulnérabilités avec Black Duck suppose que vous connaissez l'application et les API Black Duck Software Composition Analysis (SCA).

Avant de commencer

Avant d'installer et de configurer le Intégration de Réponse aux vulnérabilités avec Black Duck, vous devez exécuter et installer l'intégration CWE (Common Weakness Enumeration), qui est également utilisée par Réponse aux vulnérabilités des applications. L'intégration CWE est installée avec par Réponse aux vulnérabilités défaut.

Remarque : Bien que les données de la base de données de vulnérabilité NIST (NVD) ne soient pas nécessaires pour installer l'intégration de vulnérabilité de l'application Black Duck, il serait utile de les avoir. Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.

Chaque enregistrement d'intégration a un utilisateur run-as configuré. La valeur par défaut pour cet utilisateur est VR. Système. Ne changez pas cette valeur.

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration, apportez les changements de configuration nécessaires en fonction de vos besoins.

Validez le dimensionnement de votre instance par le nombre d'éléments vulnérables d'application que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service client et assistance.

Le nécessite une URL d'API et un jeton d'API Intégration de Réponse aux vulnérabilités avec Black Duck .

Procédure

Créez le jeton d'API et les informations d'identification de clé.

a. Connectez-vous à la plateforme Black Duck.

b. Accédez au menu du compte utilisateur et sélectionnez **Informations d'identification d'API**.

c. Sélectionnez **Générer les informations d'identification d'API**.

d. Enregistrez vos informations d'identification pour une utilisation ultérieure.

Installez le ServiceNow Intégration de Réponse aux vulnérabilités avec Black Duck

Avant d'exécuter l'intégration sur votre instance, vous devez effectuer les étapes d'installation et de configuration afin que l'outil Black Duck Software Composition Analysis (SCA) s'intègre correctement à Réponse aux vulnérabilités des applications.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Vous devez effectuer ces tâches de configuration pour que l'outil Analyse de la composition logicielle (SCA) de Black Duck s'intègre correctement à Réponse aux vulnérabilités des applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, reportez-vous à la section Installer Réponse aux vulnérabilités.
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • S'il n'est pas déjà affecté, l'utilisateur disposant du rôle administrateur installe l'application et affecte des utilisateurs au groupe Gestionnaire App-Sec. Pour en savoir plus sur les rôles de groupe, reportez-vous à la section Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs. • Le groupe de gestionnaires App-Sec supervise la configuration et vérifie les résultats attendus.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Cet outil SCA est disponible sous forme d'abonnement séparé.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer le Intégration de Réponse aux vulnérabilités avec Black Duck .
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez Vulnerability Response Integration with the Black Duck.
4. Sélectionnez la vignette de l'application.
   Les détails de l'application que vous installez s'affichent.

   Remarque : pensez à lire les sections Autres exigences et Dépendances, le cas échéant.

5. Sélectionnez **Demander une application** et saisissez vos Now Support informations d'identification de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez **Obtenir**.
7. Entrez le nom et la raison de l'instance, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demande**.
   Vous recevrez un e-mail avec les instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Configurez le Intégration de Réponse aux vulnérabilités avec Black Duck pour votre environnement. Reportez-vous à la rubrique Configurez la Intégration de Réponse aux vulnérabilités avec Black Duck..

Configurez la Intégration de Réponse aux vulnérabilités avec Black Duck.

Avant d'exécuter sur Intégration de Réponse aux vulnérabilités avec Black Duck votre instance, vous devez effectuer les étapes d'installation et de configuration afin que l'outil Black Duck Software Composition Analysis (SCA) s'intègre correctement à l'application Réponse aux vulnérabilités des applications .

Avant de commencer

Rôle requis : groupe d'utilisateurs Gestionnaire de sécurité des applications

Pourquoi et quand exécuter cette tâche

est Intégration de Réponse aux vulnérabilités avec Black Duck disponible sous forme d'abonnement distinct.

Procédure

1. Accédez à la **Tous** > **Intégration de Vulnérabilité Blackduck** > **Configuration**.
2. Sélectionnez le type d'authentification de base.
   L'authentification de base nécessite un Serveur MID pour les instances locales. Vous pouvez générer le jeton d'API requis pour l'authentification de base à partir de votre compte Black Duck.
3. Remplissez les champs du formulaire.
   Authentification de base

Champ	Description
URL D'API	URL de l'API Black Duck pour les instances d'entreprise ou locales. L'instance locale est l'URL de votre point de terminaison Black Duck.
Jeton d'API	Jeton que vous avez généré depuis votre console Black Duck.
Serveur MID	Serveur MID qui est requise pour les instances locales pour l'authentification de base.
Inclure SCA	Vulnérabilités des analyses Analyse de la composition logicielle (SCA) qui sont incluses par défaut. Les analyses SCA identifient les vulnérabilités des composants open source.
Sélectionner l'option pour gérer les faux positifs dans ServiceNow	ServiceNow Option pour gérer les faux positifs. Laissez cette option activée si vous souhaitez trier les éléments vulnérables de l'application (AVI)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	importés avec l'état **Source** marqué comme **Faux positif** ou **Faux positif potentiel**. Les AVI avec ces états **sources** qui sont normalement mappés à un état **Fermé** dans votre instance sont mappés à **Ouvert**. Vous pouvez demander un **faux positif** à partir de l'enregistrement AVI. ○ Désactivez l'une des options ou les deux si vous souhaitez conserver les états **Source** qui ont été importés à partir de votre scanner. ○ Si elle est désactivée, les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVI.
Instance d'intégration	Instance que vous utilisez pour importer les données.

4. Sélectionnez **Enregistrer et tester les informations d'identification**.
5. Exécutez **l'intégration de la liste des projets Black Duck** avant d'exécuter d'autres intégrations.
   Les autres intégrations Black Duck, telles que l'intégration de la liste des applications Black Duck et l'intégration des éléments vulnérables de l'application Black Duck, dépendent du projet actuel et des données d'application que vous avez importées de l'intégration de la liste des projets.

Afficher l'état d'exécution de l'importation Intégration de Réponse aux vulnérabilités avec Black Duck

Vérifiez le succès de vos exécutions d'intégration, localisez les problèmes et confirmez vos décisions de rattrapage en consultant la liste connexe Exécutions d'intégration de vulnérabilité.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Intégration de Vulnérabilité Blackduck** > **Intégrations**.
2. Sélectionnez une intégration.
3. Sélectionnez la liste connexe Exécutions d'intégration de vulnérabilité.
4. Vérifiez que toutes les importations ont réussi.
   Dépannage:

   Les causes les plus courantes d'un échec d'exécution sont les suivantes :

   ○ Interruption du réseau.

   ○ Un problème dans le transfert de données qui entraîne des données corrompues lors d'une transformation.

   Si l'une de ces conditions est réunie, sélectionnez **Exécuter maintenant** et réexécutez l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Affichez les référentiels importés en naviguant vers la liste des intégrations et en sélectionnant l'enregistrement d'intégration Black Duck.
6. Sélectionnez la liste connexe Exécutions d'intégration de vulnérabilité et ouvrez un enregistrement.

Transformation des données pour le Intégration de Réponse aux vulnérabilités avec Black Duck

Une fois que vous avez identifié les données que vous souhaitez importer, les données sont récupérées à partir du Intégration de Réponse aux vulnérabilités avec Black Duck, traitées via un ensemble de sources de données et transformées dans votre instance.

Intégration de Réponse aux vulnérabilités avec Black Duck

Les données de l'API sont d'abord chargées dans la table d'importation d'éléments AppVul de Black Duck [sn_vul_blackduck_appvul_item_import], et la transformation d'élément AppVul de Black Duck est utilisée pour transformer les informations importées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation** et recherchez **Black Duck AppVul Item Transform**. La table suivante répertorie les champs de carte de transformation par intégration.

Champs de carte de transformation d'élément AppVul de canard noir

Champ source	Champ cible	Description
app_id	source_app_id	ID d'application.
ID du problème	source_avit_id	ID AVIT.
app_name	app_name	Nom de l'application.
version	app_version	Version d'application.
build_id	source_scan_id	ID de build de l'application.
account_id	account_id	ID de compte.
sandbox_id	sandbox_id	ID de bac à sable.
last_update_time	last_scan_date	Heure de la dernière mise à jour.
app_name + last_scan_date	scan_summary_name	Synthèse de l'analyse.
life_cycle_stage	source_sdlc_status	État SDLC source.
niveau	source_severity	Gravité de la source.
category_name	catégorie	Catégorie.
source_severity	source_severity	Gravité de la source.
category_id + « CWE- » + cweId	source_entry_id	ID d'entrée source.
source_vulnerability_summary	source_vulnerability_summary	Résumé de la vulnérabilité source.
source_recommendation	source_recommendation	Recommandation de la source.
description	description	Description de la source.
description	source_vulnerability_explanation	Explication de vulnérabilité source.
mitigation_status_desc	source_mitigation_status	État de l'atténuation de la source.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de carte de transformation d'élément AppVul de canard noir (suite)

Champ source	Champ cible	Description
remediation_status	source_remediation_status	État du rattrapage de la source.
ligne	line_number	Ligne sur laquelle se trouve la faille.
module	application_module	Module d'application.
Fichier source	source_notes	Notes sources.
affects_policy_compliance	complies_with_policy	Les valeurs peuvent être Oui ou Non selon que les informations source sont vraies ou fausses.
Chemin d'accès au fichier source + fichier source	emplacement	Le mappage d'emplacement est une faille statique.
URL	emplacement	Mappage de l'emplacement d'une faille dynamique.
scope, type, exploitLevel	source_additional_info	Champ de valeur de nom renseigné avec les valeurs de la source pour les défauts statiques.

La table suivante répertorie les scripts de transformation exécutés au cours du processus de transformation.

Cible et objectif du script de carte de transformation de Canard noir

Script de carte de transformation de Canard noir

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a créé une transformation).	Script utilisé pour traiter l'enregistrement et mettre à jour le nombre d'entités créées, mises à jour ou inchangées, ainsi que celles qui sont importées dans le cadre de cette intégration. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation)	Script utilisé pour définir le comportement des enregistrements qui ne sont pas valides et doivent être ignorés. Également utilisé pour définir l'objet global pour le traitement d'enregistrement. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Mappage de l'état de l'intégration de Black Duck

Le tableau suivant répertorie les états sources de l'intégration de vulnérabilité Black Duck et leurs états cibles dans votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États sources de Black Duck et leurs états correspondants ServiceNow AI Platform

États sources de Black Duck	Description des états sources	État cible dans ServiceNow AI Platform
Nouveau	La vulnérabilité affecte la version de ce composant.	Ouvert
Requiert une revue	Il n'est pas possible de déterminer si une vulnérabilité affecte cette version de composant.	Ouvert
Rattrapage requis	Une correction est requise pour cette version.	Ouvert
Remédiation terminée	Le rattrapage de cette vulnérabilité est terminé.	Fermé
Atténué	La vulnérabilité a été atténuée.	Fermé
Patché	La vulnérabilité a été corrigée.	Fermé
Ignoré	La vulnérabilité a été ignorée.	Fermé

Importer les informations de projet à partir de l'instance d'intégration Black Duck

Importez les informations de projet à partir de l'instance d'intégration Black Duck pour vous assurer que les intégrations de vulnérabilité s'exécutent séquentiellement. Une intégration réussie vous aide à identifier et à ingérer les éléments vulnérables de l'application (AVI).

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

Vous pouvez importer toutes les informations du projet dans la table des Intégration de Réponse aux vulnérabilités avec Black Duck projets [sn_vul_blackduck_project] Black Duck. Tous les attributs requis, par exemple, le GUID du projet, qui sont nécessaires pour interroger différentes versions du projet, sont capturés dans la table des projets [sn_vul_blackduck_project] Black Duck.

Procédure

1. Accédez à la **Tous** > **Intégration de Vulnérabilité Blackduck** > **Intégrations**.
2. Sélectionnez une intégration.
   Par exemple, vous pouvez sélectionner l'intégration de la **liste des projets Black Duck.**
3. Sélectionnez **Exécuter maintenant**.

   Remarque : Chacun Intégration de Réponse aux vulnérabilités avec Black Duck est destiné à fournir la récupération de données la plus complète. L'exécution de ces intégrations dans le désordre peut entraîner des données incomplètes et nécessite une ServiceNow expertise en Application Vulnerability Response.

   Une fois l'importation terminée, vous pouvez voir les détails du projet dans la table des projets [sn_vul_blackduck_project] Black Duck.
4. Pour les états d'exécution de l'intégration, reportez-vous à la section Afficher l'état d'exécution de l'importation Intégration de Réponse aux vulnérabilités avec Black Duck.
5. **Facultatif :** Si vous souhaitez modifier d'autres paramètres d'intégration, vous devez accéder à l'instance d'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importez Intégration de Réponse aux vulnérabilités avec Black Duck les versions de projet dans la table Applications détectées

Importez les versions de projet de l'intégration de Vulnerability Response avec Black Duck dans la table Applications détectées [sn_vul_release] afin que les intégrations de vulnérabilité de Black Duck s'exécutent séquentiellement. Une intégration réussie vous aide à identifier et à ingérer les éléments vulnérables de l'application (AVI).

Avant de commencer
Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche
Vous pouvez ajouter et afficher toutes les différentes versions des projets (voir les détails dans la table des projets Black Duck) qui ont été importées à partir de la Intégration de Réponse aux vulnérabilités avec Black Duck table Applications détectées [sn_vul_release].

Procédure

1. Accédez à la **Tous** > **Intégration de Vulnérabilité Blackduck** > **Intégrations** .
2. Sélectionnez une intégration.
   Par exemple, vous pouvez sélectionner l'intégration de la **liste des applications Black Duck**.
3. Sélectionnez **Exécuter maintenant**.

   Remarque : Chaque version de projet des intégrations est destinée à fournir la récupération de données la plus complète. L'exécution de ces intégrations dans le désordre peut entraîner des données incomplètes et nécessite une expertise de ServiceNow et d'Application Vulnerability Response.

   Une fois l'importation terminée, vous pouvez voir les différentes versions d'un projet dans la table Applications détectées [sn_vul_release]. Si vous utilisez des règles de recherche de CI, ces applications détectées sont liées à la table d'éléments de configuration [cmdb_ci].
4. Consultez l'état des exécutions de votre intégration.
   Pour plus d'informations, consultez Afficher l'état d'exécution de l'importation Intégration de Réponse aux vulnérabilités avec Black Duck.

Importer les éléments vulnérables d'applications à partir de Intégration de Réponse aux vulnérabilités avec Black Duck

Importez les éléments vulnérables de l'application (AVI) de l'intégration de Vulnerability Response avec Black Duck afin que l'intégration s'exécute séquentiellement. Une intégration réussie vous aide à identifier et à ingérer les AVI.

Avant de commencer
Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche
Vous pouvez afficher les résultats de l'analyse Intégration de Réponse aux vulnérabilités avec Black Duckà partir du , insérer des AVI dans votre instance et enrichir vos données de vulnérabilité tierces. Par défaut, si l'enregistrement de scanner est à l'état Fermé, les AVI ne sont pas créés. Vous pouvez contrôler les AVI existants à l'aide de la propriété sn_vul_create_closed.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité de Black Duck** > **Intégrations**.
2. Sélectionnez une intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, vous pouvez sélectionner **l'intégration des éléments vulnérables de l'application Black Duck**.

3. Sélectionnez **Exécuter maintenant**.

> **Remarque :** Le Intégration de Réponse aux vulnérabilités avec Black Duck est destiné à vous fournir la récupération de données la plus complète. L'exécution de ces intégrations dans le désordre peut entraîner des données incomplètes, ainsi que des exigences ServiceNow et Réponse aux vulnérabilités des applications une expertise.

Après avoir importé toutes les vulnérabilités SCA à partir du Intégration de Réponse aux vulnérabilités avec Black Duck, vous pouvez afficher les AVI et les données de vulnérabilité tierces.

Définir les heures d'importation pour le Intégration de Réponse aux vulnérabilités avec Black Duck

Définissez l'heure de début des Intégration de Réponse aux vulnérabilités avec Black Duck importations. Vous pouvez définir les intégrations à l'avance afin d'obtenir de meilleures performances et des exécutions d'importation plus rapides.

Avant de commencer
Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche
Après l'importation initiale, les intégrations de vulnérabilité Black Duck effectuent une importation complète à chaque exécution.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité de Black Duck** > **Intégrations**.
2. Sélectionnez une intégration.
3. Définissez la nouvelle **heure de début**.
   L'heure est calculée en heures en heure locale. L'heure par défaut pour les importations d'intégration de liste d'applications Black Duck est 00:00:00. Les autres intégrations sont **sur demande** et sont enchaînées, ce qui signifie qu'elles suivent une séquence à exécuter après l'intégration de la liste des applications Black Duck. La modification de **l'heure de début** nécessite de l'avancée ServiceNow et Gestion de la vulnérabilité des applications de l'expertise.
4. Sélectionnez **Mettre à jour**.
   La nouvelle heure est utilisée pour la prochaine importation planifiée.

Inclure les éléments vulnérables de l'application Black Duck fermés

Incluez les éléments vulnérables de l'application (AVI) fermés lors des importations d'intégration des éléments vulnérables Black Duck, car ils ne sont pas créés par défaut lors des importations d'intégration. Si vous voulez les créer, vous devez modifier la propriété système.

Avant de commencer
Assurez-vous que le est installé et en cours d'exécution Intégration de Réponse aux vulnérabilités avec Black Duck .

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans le filtre de navigation, saisissez `sys_properties.list`.
2. Dans le champ **Nom** de la liste, saisissez `sn_vul.create_closed`.
3. Double-cliquez sur le champ **Valeur** et définissez-le sur **Vrai**
4. Enregistrez en sélectionnant l'icône de coche verte .
   Les enregistrements à l'état Fermé dans la prochaine importation de Black Duck sont créés en tant qu'AVI dans Réponse aux vulnérabilités des applications.

Fortify Vulnerability Integration

Utilise Fortify Vulnerability Integration les Fortify données importées du produit pour vous aider à déterminer l'impact et la priorité des failles dans votre code.

Fortify Vulnerability Integration

Le Fortify produit collecte les données du scanner et les met à la disposition du ServiceNow AI Platform®. Il s'intègre facilement à la ServiceNow® Réponse aux vulnérabilités des applications fonctionnalité de cartographie des Réponse aux vulnérabilités vulnérabilités tierces, enrichissant ainsi les données de votre instance.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Chaque jour, les travaux planifiés appellent automatiquement les intégrations. Une fois que toutes les intégrations sont activées, elles sont enchaînées pour s'exécuter dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Versions disponibles

Version de mise en production	Notes de publication
Intégration de Vulnerability Response avec Fortify v2.4 Fortify v2.3 Fortify v2.2 Fortify v2.1	Notes de version Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Fortify Vulnerability Integration

Pour afficher le Fortify Vulnerability Integration, accédez à **Intégration de vulnérabilité Fortify** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base. Ces intégrations ne sont pas toutes actives par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après l'exécution initiale, chaque jour, des travaux planifiés sont enchaînés pour exécuter les intégrations automatiquement dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Fortify Intégrations de vulnérabilité

Intégration	Description
Fortify Intégration de la liste des applications sur demande	Récupère les données du scanner d'application (vulnérabilités Fortify , métadonnées) et enrichit vos données d'application tierce. Cette intégration est définie pour s'exécuter quotidiennement à 00:00:00. Elle est active par défaut.
Fortify Intégration de la synthèse de l'analyse sur demande	Récupère les enregistrements d'analyse à partir de Fortify. Cette intégration est enchaînée pour s'exécuter après l'intégration de la liste des applications sur demande lorsqu'elle Fortify est activée. Il est inactif, par défaut.
Fortify Intégration d'élément vulnérable d'application sur demande	Récupère les résultats de l'analyse à partir de Fortify, insère les AVIT et enrichit vos données de vulnérabilité tierces. Si l'enregistrement de scanner est à l'état **Fermé** , les AVIT ne sont pas créés. Les AVIT existants sont toujours à jour. À partir de la version 2.3, affichez des détails tels que les temps de traitement totaux, les temps moyens des processus avant et après l'exécution de l'intégration, ainsi que des rapports sur les enregistrements d'exécution de l'intégration pour l'intégration des éléments vulnérables de l'application. Cette intégration est enchaînée pour s'exécuter après l'intégration du résumé de l'analyse à la demande lorsqu'elle Fortify est activée. Il est inactif, par défaut.

Pour les états d'exécution de l'intégration, Afficher l'état d'exécution de l'importation Fortify Vulnerability Integration reportez-vous à la section .

Pour afficher les données dans les vulnérabilités tierces, reportez-vous à la section Afficher les bibliothèques de vulnérabilités.

Préparation pour le Fortify Vulnerability Integration

Pour réussir, Fortify Vulnerability Integration il faut planifier et exécuter des tâches de pré-intégration. Préparez-vous à l'intégration en effectuant ces tâches. Cela Fortify Vulnerability Integration suppose que vous connaissez le produit et l'API Fortify .

Avant de commencer

L'intégration CWE (Common Weakness Enumeration) est également utilisée par Réponse aux vulnérabilités des applications et doit être en cours d'exécution avant l'installation et la configuration de .Fortify Vulnerability Integration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les données de la base de données de vulnérabilité NIST (NVD) ne sont pas nécessaires pour installer le Fortify Vulnerability Integration, mais elles fournissent un enrichissement et seraient utiles.

Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Rôle requis : gestionnaire App-Sec

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration, apportez tout changement de configuration nécessaire en fonction de vos besoins.

Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables d'applications que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service client et assistance.

Cela Fortify Vulnerability Integration nécessite une clé API, un secret API et une URL racine API, disponibles sur votre Fortify compte à la demande.

Procédure

Pour créer une clé secrète d'API :

a. Connectez-vous à votre Fortify portail sur demande.

b. Accédez à la **Tous** > **Administration** > **Paramètre** > **API**.

c. Ajoutez ServiceNow en tant qu'application.

d. Cliquez sur **Nouveau secret** pour générer un secret API.

e. Enregistrez votre secret API pour une utilisation ultérieure.

Installer l'intégration ServiceNow® de Vulnerability Response avec Fortify

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit s'intègre Fortify correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	abonnements > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe de gestionnaires App-Sec. Pour en savoir plus sur les rôles de groupe, Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs reportez-vous à la section . • Le groupe de gestionnaires App-Sec supervise la configuration et vérifie les résultats attendus.

Rôle requis : gestionnaire App-Sec

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer le Fortify Vulnerability Integration .
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez Vulnerability Response Integration with Fortify application.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Configurez le Fortify Vulnerability Integration pour votre environnement. Consultez Configurez la Fortify Vulnerability Integration..

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurez la Fortify Vulnerability Integration.

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées pour que le produit s'intègre Fortify correctement à la Réponse aux vulnérabilités des applications fonctionnalité de Réponse aux vulnérabilités. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer
Rôles requis : Gestionnaire App-Sec

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que l'intégration à Fortify l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer l'intégration ServiceNow de Vulnerability Response avec Fortify reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe de gestionnaires App-Sec. • Le gestionnaire App-Sec supervise la configuration et vérifie les résultats attendus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
Pour le Fortify Vulnerability Integration, préparez votre **ID API** et votre **clé API** .	Contact Fortify pour obtenir **l'ID** API et la **clé API**.

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer les intégrations de vulnérabilité de l'application Fortify .
2. Accédez au ServiceNow Store.
3. Dans , recherchez l'intégration avec Fortify l'application.ServiceNow StoreRéponse aux vulnérabilités
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre application est automatiquement installée sur votre instance.
11. Une fois l'installation terminée, accédez à **Intégration de vulnérabilité Fortify** > **Configuration de FoD**.
12. Remplissez les champs du formulaire.

Formulaire de configuration de Fortify sur demande

Champ	Description
URL racine de l'API	URL d'instance Fortify de l'utilisateur.
Clé API	Identificateur unique envoyé à l'API Fortify .
Secret API	Secret client fourni par Fortify.
Inclure DAST	Option permettant d'inclure les vulnérabilités à partir des analyses DAST. Les analyses DAST identifient les vulnérabilités dans le comportement de votre application globale.
Inclure SAST	Option permettant d'inclure les vulnérabilités à partir des analyses SAST. Les analyses SAST identifient les vulnérabilités dans le code.
Exceptions de triage et faux positifs dans ServiceNow (à partir de la version 20.0 de Vulnerability Response)	Sélectionnez des options pour gérer automatiquement la gestion des exceptions et des faux positifs pour les AVI avec ServiceNow des workflows lors de l'importation. Ces options

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	sont activées par défaut. Pour un exemple de cas d'utilisation, reportez-vous à la section Gestion du mappage d'état pour les reports et les faux positifs dans Réponse aux vulnérabilités des applications. **Gérer les exceptions dans ServiceNow** Laissez cette option activée si vous souhaitez trier les AVI importés marqués pour l'état **Différé** . Les AVI avec des états **Source** qui sont normalement mappés à un état **Différé** dans votre instance sont plutôt mappés à **Ouvert**. Vous **demandez une exception** à partir de l'enregistrement AVI. **Gérer les faux positifs dans ServiceNow** Laissez cette option activée si vous souhaitez trier les AVI importés dont l'état **Source** est marqué comme **Faux positif** ou **Faux positif potentiel**. Les AVI avec ces états **sources** qui sont normalement mappés à un état **Fermé** dans votre instance sont mappés à **Ouvert**. Vous demandez un **faux positif** à partir de l'enregistrement AVI. ○ Désactivez l'une des cases à cocher ou les deux si vous souhaitez conserver les états **Source** importés de votre scanner. ○ Ces AVI sont mappés aux états cibles et aux états des motifs cibles au fur et à mesure de leur importation, mais ne sont pas triés par les workflows d'exception et de faux positifs. Les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVI.
Triage dans ServiceNow (avant la version 20.0 de Vulnerability Response)	Gérez le triage de la vulnérabilité de votre application dans l'instance ServiceNow : ○ Cochez la case pour trier les AVI dans ServiceNow. Si cette option est sélectionnée, les AVI sont importés à l'état Ouvert. Vous pouvez ensuite demander une exception ou marquer l'AVI comme faux positif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Pour conserver l'état source, c'est-à-dire l'état importé à partir du scanner, assurez-vous que la case n'est pas cochée. **Remarque :** Les options **Marquer comme faux positif** et **Demander une exception** ne sont disponibles que pour les AVI triés dans ServiceNow.

13. Sélectionnez **Enregistrer et tester les informations d'identification**.

Que faire ensuite

Si votre environnement nécessite des importations séparées par domaine, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

Lors de l'installation initiale, voir Configurer Réponse aux vulnérabilités des applications pour plus d'instructions.

Après l'installation initiale, pour les modifications, reportez-vous à Fortify Vulnerability Integration Modification et activités.

Afficher l'état d'exécution de l'importation Fortify Vulnerability Integration

Utilisez la liste connexe **Exécutions d'intégration de vulnérabilité** pour vérifier le succès de vos exécutions d'intégration, localiser les problèmes et éclairer vos décisions de correction.

Avant de commencer

Pour afficher l'état de l'exécution de l'importation Fortify :

- Les Réponse aux vulnérabilités applications et Fortify Vulnerability Integration doivent être installées et configurées.
- Les Fortify Vulnerability Integration importations doivent être planifiées et en cours d'exécution.

Rôle requis : gestionnaire App-Sec

Pourquoi et quand exécuter cette tâche

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités des applications mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Fortify** > **Intégrations**.
2. Sélectionnez une intégration.
3. Cliquez sur la liste connexe **Exécutions d'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.
5. À partir de la version 2.3, affichez des détails tels que les temps de traitement totaux, les temps moyens des processus avant et après l'exécution de l'intégration, ainsi que des rapports sur les enregistrements d'exécution de l'intégration pour les intégrations d'éléments vulnérables d'application.

Fortify Vulnerability Integration Modification et activités

Configurez des modifications facultatives spécifiques au Fortify Vulnerability Integration.

Remarque : La modification d'autres paramètres, autres que ceux répertoriés ici, nécessite une Fortify Vulnerability Integration expertise avancée ServiceNow et Réponse aux vulnérabilités des applications dépasse le cadre de la documentation du produit.

Effectuer une importation manuelle Fortify de vulnérabilité de l'application

Si votre importation initiale a échoué, ou si vous ne souhaitez pas attendre l'importation initiale planifiée, vous pouvez effectuer une importation de données complète indépendamment de la tâche planifiée quotidienne.

Avant de commencer

Rôle requis : gestionnaire App-Sec

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Fortify** > **Intégrations**.
2. Choisissez une intégration, par exemple, Application Fortify List Integration.
3. Sélectionnez **Exécuter maintenant**.

Remarque : Pour une récupération complète des données, exécutez les intégrations de vulnérabilité de l'application Fortify dans l'ordre.

Importer des données à l'aide du Fortify Vulnerability Integration

Importez des données à partir du scanner Fortify pour mapper les éléments vulnérables de l'application (AVI), enrichissant ainsi les données de votre instance.

Avant de commencer

Rôle requis : gestionnaire App-Sec

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Après l'importation initiale, Fortify les intégrations de vulnérabilité effectuent une importation delta à chaque exécution, récupérant ainsi les dernières données. Consultez la section Effectuer une importation manuelle Fortify de vulnérabilité de l'application pour plus d'informations sur les importations complètes.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Fortify** > **Intégrations**.
2. Choisissez une intégration.
3. Remplissez les champs du formulaire.

Champ	Description
Nom	Nom de l'exécution de l'intégration.
Actif	Option permettant d'activer une intégration.
Exécuter	Fréquence d'exécution de l'intégration.
Heure	
Application	Application contenant cet enregistrement.
Intégration source	Intégration source pour cette intégration.
Instance source	Instance source pour cette intégration.
Intégration suivante	Intégration suivante dans la séquence, à exécuter après l'exécution de l'intégration actuelle.
Heure de début	Date et heure de début de la dernière exécution réussie de l'intégration. L'heure est calculée comme étant Heures en heure locale. L'heure par défaut pour l'exécution initiale est 00:00:00.
Détails de l'intégration	
Script d'intégration	Include de script qui étend le `VulnerabilityIntegrationBase` à exécuter lorsque l'intégration s'exécute. Ce script définit comment récupérer les données à partir d'un système tiers.
Script de l'instanciateur d'intégration	Script qui définit le mode de construction de l'include de script sélectionné pour le script d'intégration.
Stratégie de processeur de rapport	Stratégie que vous souhaitez utiliser pour gérer les données renvoyées par le script d'intégration lors de l'exécution de l'intégration.

4. Sélectionnez **Exécuter maintenant** pour exécuter l'intégration.

Inclure les éléments vulnérables de l'application Fortify sur demande fermés

Par défaut, les éléments vulnérables de l'application (AVIT) **fermés** ne sont pas créés lors Fortify des importations d'intégration d'éléments vulnérables. Si vous souhaitez les créer, vous devez modifier une propriété système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Doit Fortify Vulnerability Integration être installé et en cours d'exécution.

Rôle requis : gestionnaire App-Sec

Procédure

1. Dans la zone de texte du **navigateur de filtre** de navigation de gauche, tapez `sys_properties.list`.
2. Dans **la zone** de recherche Nom de la liste, saisissez `sn_vul.create_closed`.
3. Double-cliquer sur le champ **Valeur** et définir sur **Vrai**
4. Cliquez sur coche verte pour enregistrer.
   Les enregistrements à l'état **Fermé** dans l'importation suivante Fortify sont créés en tant qu'AVIT dans Réponse aux vulnérabilités des applications.

GitHub Application Intégrations de vulnérabilités

L'importation GitHub Application Intégrations de vulnérabilités de données de test statique de sécurité des applications (SAST) et d'analyse de la composition logicielle (SCA) pour vous aider à afficher les alertes de vulnérabilité dans les référentiels de votre GitHub environnement.

GitHub Application Intégrations de vulnérabilités

Le collecte GitHub Application Intégrations de vulnérabilités les données du scanner et les met à la disposition du ServiceNow AI Platform®. Il s'intègre facilement à la ServiceNow® Réponse aux vulnérabilités des applications fonctionnalité de mappage des Réponse aux vulnérabilités vulnérabilités et GitHub des alertes tierces dans votre instance.

L'environnement GitHub prend en charge plusieurs organisations. Ces organisations, sur site ou en entreprise, peuvent contenir différents départements, tels que l'ingénierie, la qualité, la documentation, etc. Chaque organisation, à son tour, peut prendre en charge plusieurs référentiels. Après avoir importé vos données d'application avec l'intégration de référentiel GitHub , vous pouvez importer des données de vulnérabilité et d'alerte à partir de ces référentiels. Les données importées sont traitées comme une application dans l'application Réponse aux vulnérabilités des applications . Lorsque les scanners détectent des vulnérabilités et génèrent des alertes pour les référentiels, des vulnérabilités sont créées dans Réponse aux vulnérabilités des applications.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Versions disponibles

Version de mise en production	Notes de publication
GitHub Application Intégrations de vulnérabilités v1.2, v1.1, 1.0	Notes de version Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de GitHub

Intégration	Description
GitHub Intégration du référentiel	À partir de la version 1.1, importez toutes les données d'application pour vos GitHub comptes sur site et dans le cloud (entreprise). L'intégration importe les applications à partir des référentiels que vous avez configurés pour une organisation (sur site) ou à partir de votre environnement d'entreprise (cloud). Exécutez cette intégration avant d'exécuter les autres GitHub intégrations, car elles dépendent des données d'application actuelles importées à partir de l'intégration des référentiels.
GitHub Intégration CodeScan	Récupère les alertes de vulnérabilité d'analyse de code des référentiels pour détecter les vulnérabilités de sécurité et les erreurs de GitHub codage. Les données importées sont mappées aux résultats SAST dans votre instance.
GitHub Intégration de Dependabot	Récupère les alertes Dependabot pour les dépendances avec des vulnérabilités connues à partir des référentiels. Les données importées sont mappées aux résultats SCA dans votre instance.
GitHub Analyse secrète	Récupère les secrets du code de votre organisation ainsi que les résultats des tests de sécurité des applications. Les données sont mappées aux résultats SCA dans votre instance.
GitHub Emplacement de l'analyse secrète	Récupère l'emplacement et les numéros de ligne des secrets analysés dans le code de votre organisation pour aider vos développeurs à y remédier.

Chargement de SBOM fichiers à ServiceNow AI Platform® partir de vos GitHub référentiels

Déterminez si SBOM les fichiers générés dans vos pipelines CI/CD (intégration continue et livraison/déploiement continus) ont été mis en file d'attente avec succès dans votre ServiceNow AI Platform® instance.

- Protégez vos environnements contre les composants potentiellement dangereux pendant les cycles de développement logiciel avec GitHub les actions que vous initiez à partir de votre GitHub environnement.
- Obtenez toutes les actions requises GitHub pour SBOM le chargement dans GitHub Marketplace.

Les SBOM applications sont requises pour charger SBOM des fichiers. Consultez Explorer Nomenclature logicielle pour plus d'informations.

Affichage des données importées

Les données d'application importées à partir de l'intégration des référentiels GitHub sont affichées dans la table Applications détectées [sn_vul_app_release]. Exécutez d'abord cette intégration.

L'intégration des référentiels importe les balises et les rubriques que vous avez configurées pour un référentiel dans votre GitHub compte à partir du menu Paramètres. Toutes les propriétés personnalisées se trouvent dans le menu sous votre référentiel. Les valeurs que vous définissez pour les propriétés sont importées sous forme de paires clé-valeur. Pour en savoir plus sur l'endroit où afficher ces informations dans votre instance, reportez-vous à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la section Afficher le statut d'exécution de l'importation et les données du GitHub Application Intégrations de vulnérabilités référentiel importé.

Les données importées (résultats) à partir de l'intégration GitHub Dependabot sont affichées sur les tables suivantes.

- Applications détectées [sn_vul_app_release].
- Synthèses de numérisation de vulnérabilité de l'application [sn_vul_app_vul_scan_summary].
- Éléments vulnérables de l'application [sn_vul_app_vulnerable_item].
- Forfaits [sn_vul_app_package].

Les données importées à partir de GitHub CodeScan Integration sont affichées dans les tables suivantes.

- Applications détectées [sn_vul_app_release].
- Synthèses de numérisation de vulnérabilité de l'application [sn_vul_app_vul_scan_summary].
- Entrées de vulnérabilité de l'application [sn_vul_app_vul_entry].
- Éléments vulnérables de l'application [sn_vul_app_vulnerable_item].

Préparation pour le GitHub Application Intégrations de vulnérabilités

Préparez-vous à l'intégration en effectuant ces tâches. Cela GitHub Application Intégrations de vulnérabilités suppose que vous connaissez le produit et l'API GitHub.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Rôles requis :

- administrateur pour télécharger, installer et activer des applications et affecter des rôles.
- Administrateur GitHub pour obtenir les informations d'identification et générer des jetons dans la console GitHub.
- administrateur pour configurer les connexions et les enregistrements d'alias dans votre instance.

Tâches de configuration

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration (suite)

Tâches de configuration	Description
Vérifiez que le GitHub Application Intégrations de vulnérabilités est installé et activé.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installez le ServiceNow GitHub Application Intégrations de vulnérabilités reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • S'il n'est pas déjà affecté, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe d'utilisateurs Gestionnaire de sécurité des applications. • Le gestionnaire App-Sec supervise la configuration et vérifie les résultats attendus. • sn_vul_github_config_integration est hérité par le groupe d'utilisateurs Gestionnaire de sécurité des applications. Ce rôle contient les rôles connection_admin et oauth_admin.
Obtenez vos informations d'identification GitHub et votre compte.	Les informations de compte sont requises sur les enregistrements que vous créez pour l'authentification. Consultez pour Création d'informations d'identification OAuth 2.0 pour GitHub les applications : JWT pour la GitHub Application Intégrations de vulnérabilités plus d'informations sur les détails dont vous avez besoin et la configuration des enregistrements requis pour l'authentification OAuth.
Vérifiez que vous importez des données de Common Weakness Enumeration (CWE).	L'intégration de Common Weakness Enumeration (CWE) est également utilisée par Réponse aux vulnérabilités des applications l'intégration des vulnérabilités GitHub et doit être en cours d'exécution avant l'installation et la configuration de GitHub Vulnerability Integration. Il est installé avec Réponse aux vulnérabilités, par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration (suite)

Tâches de configuration	Description
	Remarque : Les données de la base de données de vulnérabilité NIST (NVD) ne sont pas nécessaires pour installer GitHub Vulnerability Integration, mais elles fournissent un enrichissement et seraient utiles. Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.

Création d'informations d'identification OAuth 2.0 pour GitHub les applications : JWT pour la GitHub Application Intégrations de vulnérabilités

Pour intégrer vos GitHub applications à l'aide du jeton de porteur JWT pour le GitHub Application Intégrations de vulnérabilités fichier .

Rôles requis :

- sn_vul.app_sec_manager et administrateur pour les enregistrements de votre ServiceNow AI Platform.
- Aucun rôle d'instance requis pour les tâches de votre GitHub compte.
- Pour plus d'informations sur le contexte des étapes de cette configuration, consultez la rubrique Protocole OAuth 2.0 .

Créer et configurer l'application GitHub pour le GitHub Application Intégrations de vulnérabilités

Créez une application personnalisée GitHub à partir de votre GitHub compte pour activer l'authentification OAuth 2.0 avec votre GitHub Application Intégrations de vulnérabilités instance dans votre instance.

Avant de commencer

Rôle requis : aucun rôle d'instance requis

Pourquoi et quand exécuter cette tâche

Suivez ces étapes à partir de votre GitHub compte. Reportez-vous à Bâtiment GitHub Applications sur le site Developer pour obtenir des instructions sur la création et la configuration d'applications GitHub personnalisées.

Procédure

1. À partir de votre GitHub compte, créez votre GitHub application en accédant à **Paramètres du développeur** > **Applications GitHub**.
2. Dans le champ URL de la **page d'accueil** , saisissez `https://<nom-instance>.service-now.com`.
3. Dans le champ **URL de rappel d'autorisation utilisateur** , saisissez `https://<nom-instance>.service-now.com/oauth_redirect.do`.
4. Dans la section **Identification et autorisation des utilisateurs** , désélectionnez le champ **Faire expirer les jetons d'autorisation de l'utilisateur** .
5. Dans la section **Webhook** , sélectionnez le champ **Actif** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans le champ **URL Webhook** , saisissez `https://instance-name>.service-now.com/`.
7. Laissez les champs restants vides (par défaut).
8. Dans la section **Autorisations du référentiel** , configurez les paramètres suivants.

Analyse du code	Lecture seule
Contenus	Lecture seule
Propriétés personnalisées	Lecture seule
Alertes Dependabot	Lecture seule
Métadonnées	Lecture seule

Remarque : Si vous utilisez déjà une application GitHub et que vous mettez à jour l'une des autorisations, vous devez passer en revue et accepter ces autorisations pour votre application GitHub. Vous pouvez accéder à votre application, puis sélectionner **Configurer > Examiner la demande > Accepter de nouvelles autorisations**.

9. Laissez les autorisations restantes sur `Aucun accès` (par défaut).
10. Dans la section **S'abonner aux événements** , sélectionnez l'option **Règle de protection du déploiement** .
11. Cliquez avec le bouton droit de la souris sur l'en-tête pour enregistrer les modifications.
12. Installez l'application nouvellement créée GitHub sur les comptes de votre choix.
    a. Dans la page des paramètres GitHub Apps, sélectionnez votre application.
    b. Dans la barre latérale gauche, sélectionnez **Installer l'application**.
    c. Sélectionnez **Installer** en regard du compte d'organisation ou personnel contenant le référentiel approprié.
    d. Installez l'application sur tous les référentiels ou sélectionnez des référentiels.
    Pour plus d'informations, consultez Installation des applications GitHub .
13. Après l'installation, sélectionnez les paramètres (icône d'engrenage) de votre application et notez ou notez les informations suivantes.

    Ces détails sont requis lorsque vous créez le registre d'application dans votre ServiceNow AI Platform instance.

    - ID d'application
    - ID client
    - Secret client.
    - Notez le jeton dans l'URL. Il s'agit de l'ID de jeton que vous saisissez dans l'URL du jeton de votre instance.
14. Faites défiler la page vers le bas et générez une nouvelle clé privée et enregistrez-la sur votre ordinateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Générer le certificat JKS pour le GitHub Application Intégrations de vulnérabilités

Générez un certificat JKS pour l'authentification JWT pour le GitHub Application Intégrations de vulnérabilités fichier .

Avant de commencer

Vous devez noter le mot de passe que vous utilisez pour générer le fichier .jks (mot de passe KeyStore).

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Créez un certificat signé par une autorité de certification à l'aide de la clé privée de l'application GitHub :

```
openssl req -new -x509 -key <file-name>.pem -out <certificate-name>.pem -days 1095
```

2. Entrez les détails requis.
3. Créez le fichier PKCS 12 à l'aide de la clé privée de l'application et du certificat signé par l'autorité GitHub de certification :

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey <file-name>.pem -certfile
 <certificate-name>.pem -out <PKCS-12-file-name>.p12
```

4. Fournir le mot de passe d'exportation.
5. Créez le fichier JKS :

```
keytool -importkeystore -srckeystore <PKCS-12-file-name>.p12 -srcstoretype pkcs12
 -destkeystore <JKS-certificate-filename>.jks -deststoretype JKS
```

6. Fournissez les mots de passe de magasin de clés de destination et source.

Joindre le certificat de magasin de GitHub clés Java à votre instance pour le GitHub Application Intégrations de vulnérabilités

Activez l'authentification par jeton JWT Bearer Grant en joignant le certificat valide GitHub Java KeyStore (JKS) à votre instance.

Avant de commencer

Un certificat Java KeyStore valide.

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Certificats**.
2. Sélectionnez **Nouveau**.
3. Remplissez les champs du formulaire.

Champs du formulaire Certificat X.509

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement de façon unique. Par exemple, Mon certificat d'application GitHub pour AVR.
Notification à l'expiration	Option permettant de spécifier les utilisateurs à notifier lorsque le certificat expire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Avertissement avant l'expiration (en jours)	Nombre de jours pour envoyer une notification avant l'expiration du certificat.
Actif	Option permettant d'activer le certificat.
Type	Option permettant de sélectionner le type de certificat. Sélectionnez **Magasin de clés Java**.
Échéance en jours	Nombre de jours jusqu'à l'expiration du certificat.
Mot de passe de magasin de clés	Mot de passe associé au certificat (indice : mot de passe KeyStore de destination précédemment créé).
Description brève	Résumé du certificat.

4. Sélectionnez l'icône Pièces jointes et joignez un certificat JKS.
5. Sélectionnez **Valider les banques/certificats**.
   Un message de key_store valide s'affiche pour les fichiers de certificat valides.

Créer une clé de signature JWT pour le GitHub certificat JKS pour le GitHub Application Intégrations de vulnérabilités

Créez une clé de signature JSON Web Token (JWT) à affecter à votre GitHub certificat Java KeyStore.

Avant de commencer

Rôles requis :

- administrateur
- sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Clés JWT**.
2. Sélectionnez **Nouveau**.
3. Remplissez les champs du formulaire.

Champs du formulaire Clés JWT

Champ	Description
Nom	Nom permettant d'identifier de façon unique la clé de signature JWT. Par exemple, Mon application GitHub Clé JWT pour AVR.
Magasin de clés de signature	Sélectionnez le certificat JKS valide que vous avez joint dans la tâche précédente.
ID de clé	Laissez ce champ vide.
Algorithme de signature	Laissez cette valeur sur RSA 256.
Signature avec le mot de passe de clé	Mot de passe associé à la clé de signature. Il s'agit du mot de passe que vous avez utilisé pour générer le fichier JKS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Option permettant d'activer la clé.

4. Cliquez avec le bouton droit n'importe où dans l'en-tête gris de la page et sélectionnez **Enregistrer**.

Créer un fournisseur JWT pour votre GitHub clé de signature pour le GitHub Application Intégrations de vulnérabilités

Ajoutez un fournisseur de jeton Web JSON (JWT) à votre ServiceNow instance pour GitHub.

Avant de commencer

Rôles requis :

- administrateur
- sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Fournisseurs JWT**.
2. Sélectionnez **Nouveau**.
3. Remplissez les champs du formulaire.

Champs du formulaire Fournisseur JWT

Champ	Description
Nom	Nom permettant d'identifier de façon unique le fournisseur JWT. Par exemple, Mon application GitHub Fournisseur JWT pour AVR.
Intervalle d'expiration (s)	Nombre en secondes pour définir la durée de vie des jetons de fournisseur JWT. Vous pouvez conserver ce paramètre par défaut.
Configuration de la signature	Sélectionnez la clé JWT que vous avez créée lors des étapes précédentes.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
5. Saisissez **l'ID**GitHub de votre application pour la valeur de la réclamation **ISS**, dans la liste connexe Réclamations standard.
   Il s'agit de l'ID de l'application GitHub dans votre GitHub console que vous avez créée aux étapes précédentes.
6. Laissez **les valeurs aud** et **sub** vides (par défaut).
7. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

Inscrivez-vous GitHub en tant que fournisseur OAuth (JWT) pour GitHub Application Intégrations de vulnérabilités

Utilisez les informations générées pendant GitHub la configuration du compte d'application pour vous inscrire GitHub en tant que fournisseur OAuth et permettre à l'instance de demander des jetons OAuth 2.0.

Avant de commencer

Rôles requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- administrateur
- sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application**.
2. Sélectionnez **Nouveau**.
   Le message Quel type d'application OAuth ? s'affiche.
3. Sélectionnez **Se connecter à un fournisseur OAuth tiers**.
4. Remplissez les champs du formulaire.

Champs du formulaire Registre d'application

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement de façon unique. Par exemple, saisissez `Mon fournisseur d'applications GitHub pour AVR`.
ID client	ID client de votre GitHub application. L'ID client provient de l'application GitHub de votre GitHub console que vous avez créée aux étapes précédentes. Cet ID disponible dans la section **À propos** de votre GitHub configuration d'application dans GitHub.
Accessible	Laissez ce paramètre dans sa valeur actuelle.
Secret client	Secret client de votre GitHub application. Le secret client provient de l'application GitHub de votre GitHub console que vous avez créée aux étapes précédentes. Cet ID disponible dans la section **À propos** de votre GitHub configuration d'application dans GitHub.
Actif	Option permettant d'activer la clé. Laissez cette option sélectionnée.
URL d'autorisation	Cette URL est générée automatiquement.
URL de jeton	Emplacement du point de terminaison du jeton que l'instance utilise pour récupérer et actualiser les jetons. Entrez le jeton à partir de l'URL dans votre GitHub application. Il s'agit du jeton affiché dans l'URL une fois votre application installée dans GitHub. Dans la section Installer l'application de votre configuration d'application GitHub dans GitHub, sélectionnez l'engrenage. Le jeton s'affiche dans l'URL de la page Web. ○ Pour le cloud : https://api.github.com/app/installations/49374672/access_tokens . ID d'installation : 9374672. ○ Pour les sites : https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3 .
Script de l'API OAuth	Option qui vous permet de référencer un include de script OAuthUtil modifié. Sélectionnez **OAuthGitHubJWTHandler**.
Type d'accord par défaut	Type de subvention associé au registre d'application. **Sélectionnez Support JWT**.

5. Laissez les autres champs de formulaire par défaut.
6. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
7. Faites défiler l'écran jusqu'à la liste connexe **Profils des entités OAuth** , sélectionnez-la et ouvrez le profil par défaut qui a été créé dans la liste.

Traduction automatique

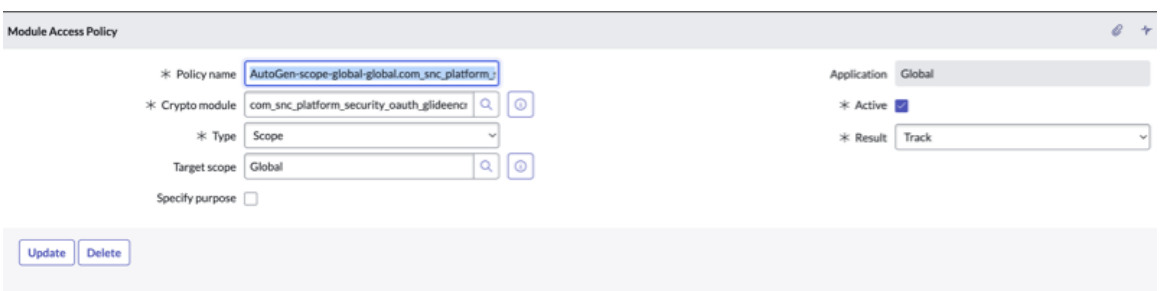
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Renseignez le champ **Fournisseur JWT** avec le fournisseur JWT précédemment créé et enregistrez le formulaire.
9. Revenez au fichier de registre d'application et enregistrez-le.
10. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > **Tous**.
11. Sélectionnez la politique afin qu'com_snc_platform_security_oauth_glideencrypter s'affiche en tant que valeur du **champ Module de chiffrement** et que OAuthGitHubJWTHandler soit l'include de script dans le champ **de script Cible** .

    Dans l'image suivante, le com_snc_platform_security_oauth_glideencrypter est sélectionné comme valeur pour le champ **Module de chiffrement** . Le champ **Table Script** affiche la table Script Include [sys_script_include] et la valeur du champ **Script cible** est OAuthGitHubJWTHandler.



12. Sélectionnez **Mettre à jour**.



    Comme illustré dans l'image précédente, la valeur du champ **Nom de la politique** change et les champs Table **de script** et **Script cible** ne sont plus affichés.

13. Vérifiez que le champ **Résultat** est défini sur Suivre et enregistrez vos modifications.

Créer des informations d'identification et des connexions pour le GitHub Application Intégrations de vulnérabilités

Créez un enregistrement d'informations d'identification auprès du fournisseur d'application GitHub précédemment créé pour autoriser des actions.

Avant de commencer

Rôles requis :

- administrateur
- sn_vul.app_sec_manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Informations d'identification et connexions** > **Informations d'identification**.
2. Sélectionnez **Nouveau**.
3. Sélectionnez **Informations d'identification OAuth 2.0**.
4. Sélectionnez **Nouveau** et renseignez les champs.

Champ	Description
Nom	Nom unique pour l'enregistrement.
Concerne	Sélectionnez les informations d'identification OAuth 2.0 dans la liste.
Profil de l'entité OAuth	Sélectionnez l'icône de recherche et localisez le profil d'entité que vous avez créé lors des étapes précédentes.
Autres champs	Laissez ces champs dans leurs valeurs par défaut.

5. Cliquez avec le bouton droit n'importe où dans l'en-tête de la page et sélectionnez **Enregistrer**.
   La liste des informations d'identification s'affiche.
6. Ouvrez l'enregistrement que vous venez de créer et sélectionnez le lien connexe **Obtenir un jeton OAuth** .
   Un message s'affiche, indiquant que le jeton OAuth a été importé avec succès.
7. Accédez à la **Informations d'identification et connexions** > **Connexions**.
8. Sélectionnez **Nouveau**.
9. Sélectionnez **Connexion HTTP(s)**.
10. Sélectionnez **Nouveau** et renseignez les champs.

Champ	Description
Nom	Nom de l'enregistrement.
Application	Lecture seule.
Alias parent (facultatif)	Sélectionnez l'icône de recherche et choisissez-en une dans la liste.
Type	Connexion et informations d'identification.
Type de connexion	HTTP.
Prendre en charge plusieurs connexions actives (facultatif)	Désactivé.
Politique des nouveaux essais par défaut	Politique des nouveaux essais HTTP par défaut
Modèle de configuration	À laisser vide.

11. Sélectionnez **Soumettre**.
    La liste Alias de connexion et d'informations d'identification s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

12. Ouvrez votre enregistrement, puis dans l'onglet de liste connexe Connexions, sélectionnez **Nouveau** et renseignez les champs de l'enregistrement Connexion HTTP.

Champ	Description
Nom	Nom de l'enregistrement.
Actif	Activé.
Informations d'identification	Sélectionnez l'enregistrement d'informations d'identification que vous avez créé lors des étapes précédentes.
Alias de connexion	Votre enregistrement s'affiche.
Générateur d'URL	Désactivé.
URL de connexion	Il s'agit de l'URL de base : https://api.github.com pour Enterprise. Sur site, il s'agit de l'URL de votre point de terminaison GitHub.
Utiliser Serveur MID (facultatif)	Serveur MID est requis pour les messages sur site. Il est facultatif pour Enterprise.
Délai de connexion	Saisissez une valeur.

13. Sélectionnez **Soumettre**.
La liste Alias de connexion et d'informations d'identification s'affiche. Vous êtes maintenant prêt à effectuer les étapes vers Configurez la GitHub Application Intégrations de vulnérabilités.. Dans le champ Connexion, entrez les informations d'identification que vous avez créées au cours des étapes précédentes.

Installez le ServiceNow® GitHub Application Intégrations de vulnérabilités

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que l'intégration s'intègre GitHub Application Intégrations de vulnérabilités correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Rôle requis : admin

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer le GitHub Application Intégrations de vulnérabilités .
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez une GitHub Application Intégrations de vulnérabilités application.
4. Sélectionnez la vignette de l'application.
Vous obtenez des informations détaillées sur l'application que vous allez installer.

Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez **Demander une application** et saisissez vos Now Support informations d'identification de connexion.
6. Sélectionnez **Obtenir**.
7. Entrez le **nom et** la **raison d'être de l'instance**, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demande**.
   Vous recevez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer**.
    Votre application est automatiquement installée sur votre instance.

Configurez la GitHub Application Intégrations de vulnérabilités.

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées pour que le produit GitHub s'intègre correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Rôles requis :

- Groupe d'utilisateurs du gestionnaire de sécurité des applications
- sn_vul.app_sec_manager requis pour la configuration OAuth

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité de GitHub** > **Configuration**.
2. Choisissez **Authentification de base** ou **OAuth** comme type d'authentification.
   - L'authentification de base nécessite un serveur MID pour les instances sur site. Générez le jeton d'API requis pour l'authentification de base à partir de votre GitHub compte.
   - OAuth nécessite la configuration de l'application, des informations d'identification et de la connexion OAuth décrites à la section Création d'informations d'identification OAuth 2.0 pour GitHub les applications : JWT pour la GitHub Application Intégrations de vulnérabilités.
3. Renseignez les champs en fonction du type que vous choisissez.
   Authentification de base

Champ	Description
URL D'API	L'URL d'API appropriée GitHub pour l'entreprise ou sur site. L'URL par défaut est https://api.github.com . L'URL de votre GitHub point de terminaison est On-premise.
Jeton d'API	Jeton que vous avez généré à partir de votre GitHub console.
Type d'API	Sélectionner un élément : **Organisation** Choisissez cette option si vous souhaitez importer des données pour une organisation spécifique par nom.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	L’environnement GitHub prend en charge plusieurs organisations. Chaque organisation peut prendre en charge plusieurs référentiels. Si vous saisissez une organisation, seules les données de cette organisation sont importées. **Entreprise** L’environnement Enterprise prend en charge plusieurs organisations. Choisissez cette option si vous souhaitez importer des données de vulnérabilité de toutes les organisations de votre environnement d’entreprise (cloud).
Nom de l'organisation	Nom de votre GitHub référentiel. Seules les données de l’organisation que vous saisissez sont importées.
Serveur MID	Pour les instances sur site pour l’authentification de base, un Serveur MID est requis.
Sélectionnez des options pour gérer la gestion des exceptions et les faux positifs.	Sélectionnez des options pour gérer la gestion des exceptions et des faux positifs pour les éléments vulnérables d’applications (AVI) avec ServiceNow des workflows automatiquement lors de l’importation. **Gérer les exceptions dans ServiceNow** Laissez cette option activée si vous souhaitez trier les AVI importés marqués pour l’état **Différé** . Les AVI avec des états **Source** qui sont normalement mappés à un état **Différé** dans votre instance sont plutôt mappés à **Ouvert**. Vous **demandez une exception** à partir de l’enregistrement AVI. **Gérer les faux positifs dans ServiceNow** Laissez cette option activée si vous souhaitez trier les AVI importés dont l’état **Source** est marqué comme **Faux positif** ou **Faux positif potentiel**. Les AVI avec ces états **sources** qui sont normalement mappés à un état **Fermé** dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	votre instance sont mappés à **Ouvert**. Vous demandez un **faux positif** à partir de l'enregistrement AVI. ○ Désactivez l'une des cases à cocher ou les deux si vous souhaitez conserver les états **Source** importés de votre scanner. ○ Si elle est désactivée, les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVI.
Instance d'intégration	Instance dans laquelle vous importez des données.

OAuth

Champ	Description
URL D'API	L'URL d'API appropriée GitHub pour l'entreprise ou sur site. L'URL par défaut est https://api.github.com . L'URL de votre GitHub point de terminaison est On-premise.
Connexion	La connexion que vous avez créée décrite dans .Création d'informations d'identification OAuth 2.0 pour GitHub les applications : JWT pour la GitHub Application Intégrations de vulnérabilités
Type d'API	Sélectionner un élément : **Organisation** Choisissez cette option si vous souhaitez importer des données pour une organisation spécifique par nom. L'environnement GitHub prend en charge plusieurs organisations. Chaque organisation peut prendre en charge plusieurs référentiels. Si vous saisissez une organisation, seules les données de cette organisation sont importées. **Entreprise** L'environnement Enterprise prend en charge plusieurs organisations. Choisissez cette option si vous souhaitez importer des données de vulnérabilité de toutes les organisations de votre environnement d'entreprise (cloud).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : GitHub Les applications ne prennent pas en charge les API au niveau de l'entreprise.
Nom de l'organisation	Nom de l'organisation de vos GitHub référentiels. Seules les données provenant des référentiels de l'organisation que vous saisissez sont importées.
Sélectionnez des options pour gérer la gestion des exceptions et les faux positifs.	Sélectionnez des options pour gérer la gestion des exceptions et des faux positifs pour les éléments vulnérables d'applications (AVI) avec ServiceNow des workflows automatiquement lors de l'importation. **Gérer les exceptions dans ServiceNow** Laissez cette option activée si vous souhaitez trier les AVI importés marqués pour l'état **Différé** . Les AVI avec des états **Source** qui sont normalement mappés à un état **Différé** dans votre instance sont plutôt mappés à **Ouvert**. Vous **demandez une exception** à partir de l'enregistrement AVI. **Gérer les faux positifs dans ServiceNow** Laissez cette option activée si vous souhaitez trier les AVI importés dont l'état **Source** est marqué comme **Faux positif** ou **Faux positif potentiel**. Les AVI avec ces états **sources** qui sont normalement mappés à un état **Fermé** dans votre instance sont mappés à **Ouvert**. Vous demandez un **faux positif** à partir de l'enregistrement AVI. ○ Désactivez l'une des cases à cocher ou les deux si vous souhaitez conserver les états **Source** importés de votre scanner. ○ Si elle est désactivée, les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Enregistrer et tester les informations d'identification**.
5. Exécutez l'intégration des référentiels GitHub avant d'exécuter les autres intégrations.
   Les autres GitHub intégrations dépendent des données d'application actuelles importées à partir de l'intégration des référentiels. Les données de l'intégration des référentiels sont stockées dans la table Applications détectées [sn_vul_app_release]. Consultez Afficher le statut d'exécution de l'importation et les données du GitHub Application Intégrations de vulnérabilités référentiel importé pour plus d'informations.

Afficher le statut d'exécution de l'importation et les données du GitHub Application Intégrations de vulnérabilités référentiel importé

Utilisez la liste connexe **Exécutions d'intégration de vulnérabilité** pour vérifier le succès de vos exécutions d'intégration, localiser les problèmes et éclairer vos décisions de correction.

Avant de commencer

Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité GitHub** > **Intégrations**.
2. Sélectionnez une intégration.
3. Sélectionnez la liste connexe **Exécutions d'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.

   Trouble?

   Les causes les plus courantes d'un échec d'exécution sont les suivantes :
   - Interruption du réseau.
   - Un problème dans le transfert des données entraînant des données corrompues pendant la transformation.

   Si l'une de ces conditions est réunie, sélectionnez **Exécuter maintenant** et réexécutez l'intégration.
5. Pour afficher les référentiels importés, revenez à la liste des intégrations et sélectionnez l'enregistrement d'intégration du GitHub référentiel.
6. Sélectionnez la liste connexe **Exécutions d'intégration de vulnérabilité** et ouvrez un enregistrement.
   Le nombre de référentiels que vous avez importés avec une exécution d'intégration s'affiche dans la colonne Éléments importés.

   Toutes les balises et rubriques que vous avez configurées pour un référentiel dans votre GitHub compte à partir du menu Paramètres sont importées. Toutes les propriétés personnalisées importées se trouvent dans le menu sous votre référentiel.

   Les balises, rubriques et propriétés personnalisées sont importées dans votre instance uniquement si elles sont configurées dans votre GitHub compte.

   Si elles sont importées, ces GitHub informations s'affichent dans votre instance dans la colonne Informations supplémentaires de la source de la table Applications détectées [sn_vul_app_release] et dans la section Informations supplémentaires de la source. de l'enregistrement d'une application détectée. Les propriétés personnalisées sont affichées sous forme de paires clé-valeur, et les balises et les rubriques sont affichées sous forme de tableaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les GitHub Application Intégrations de vulnérabilités jeux d'importation

Afficher les détails des informations sur l'importation pour le GitHub Application Intégrations de vulnérabilités.

Avant de commencer
Rôle requis : sn_vul.app_sec_manager

Procédure

1. Accédez au **Intégration de vulnérabilité GitHub** > **Tables de jeux d'importation**.
2. Sélectionnez un enregistrement pour une intégration.
3. Sélectionnez un lien connexe pour afficher les informations suivantes :
   - Ensembles de données à importer
   - Cartes de transformation
   - Historique de transformation

Invicti Vulnerability Integration

Utilise Invicti Vulnerability Integration les données d'application importées du produit Invicti pour vous aider à déterminer l'impact et la priorité des failles dans votre code.

Invicti Vulnerability Integration

Le collecte Invicti Vulnerability Integration les données du scanner et les met à la disposition du ServiceNow AI Platform®. Il s'intègre facilement à la ServiceNow® Réponse aux vulnérabilités des applications fonctionnalité de mappage des informations de Réponse aux vulnérabilités vulnérabilité des applications tierces importées dans votre instance.

L'intégration importe les types de données analysés suivants.

- Test dynamique de sécurité des applications (DAST)
- Test de sécurité des applications interactives (IAST)

Pour plus d'informations sur DAST et IAST, reportez-vous à la section Explorer Réponse aux vulnérabilités des applications.

Versions disponibles

Version de mise en production	Notes de publication
Invicti Vulnerability Integration v1.1 Invicti Vulnerability Integration 1.0	Notes de version Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations

Les intégrations suivantes sont incluses dans le système de base. Les intégrations sont enchaînées de sorte qu'une fois qu'une intégration s'est terminée avec succès, l'intégration suivante est lancée. Les intégrations s'exécutent dans l'ordre indiqué dans le tableau suivant.

Après l'exécution initiale, chaque jour, des travaux planifiés sont enchaînés pour exécuter ces intégrations automatiquement dans l'ordre. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Intégrations de vulnérabilité de l'application Invicti

Intégration	Description
Application de la liste des demandes Invicti	Importe les applications analysées par Invicti dans la table Applications détectées [sn_vul_app_release] ou la table Application analysée [sn_vul_app_scanned_application] en fonction de la façon dont la `sn_vul.use_product_model` propriété système est définie pour les enregistrements de règle de recherche de CI. • Si la propriété du modèle de produit est définie sur vrai, une application est insérée dans la table de version de l'application détectée. • Si la propriété du modèle de produit est définie sur false, une application est insérée dans la table Application numérisée. Vous pouvez choisir d'activer des règles de recherche avec des éléments de configuration (CI) comme cibles de recherche en modifiant la propriété système. Si vous la modifiez, vous devez également activer les règles de recherche de CI pour correspondre à la cible de recherche. Pour en savoir plus, consultez : • Configurez la Invicti Vulnerability Integration. • Créer une règle de recherche de CI • Réapplication des règles de recherche de CI dans Réponse aux vulnérabilités des applications
Intégration de la liste des analyses Invicti	Cette intégration est lancée une fois l'intégration de la liste des applications terminée. Cette intégration importe des données sur la date et l'heure d'exécution d'une analyse.
Intégration d'élément vulnérable de l'application Invicti	Cette intégration est lancée une fois l'intégration de la liste des analyses terminée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de vulnérabilité de l'application Invicti (suite)

Intégration	Description
	À partir de la version 1.1, affichez des détails tels que les temps de traitement totaux, les temps moyens des processus avant et après l'exécution de l'intégration, ainsi que des rapports sur les enregistrements d'exécution de l'intégration pour l'intégration des éléments vulnérables de l'application. Chaque vulnérabilité dans Invicti a un type, par exemple, **DirectoryListing**. Ce type est mappé en tant qu'ID unique dans votre instance et affiché dans le cadre de la valeur du champ Vulnérabilité de l'enregistrement de l'élément vulnérable de l'application (AVI) : **Invicti-DirectoryListing**. Pour plus d'informations sur le mappage, reportez-vous à la section Invicti Vulnerability Integration Mappage de l'état.

La limite supérieure d'éléments par page pour les trois intégrations est de 200.

Préparez-vous pour le Invicti Vulnerability Integration

Une intégration réussie nécessite la planification et l'exécution de tâches préalables à l'intégration. Préparez-vous à l'intégration en effectuant ces tâches. Cela Invicti Vulnerability Integration suppose que vous connaissez le produit et l'API Invicti.

L'intégration Common Weakness Enumeration (CWE) est également utilisée par Réponse aux vulnérabilités des applications l'intégration des vulnérabilités Invicti et doit être en cours d'exécution avant l'installation et la configuration.

Remarque : Les données de la base de données de vulnérabilité NIST (NVD) ne sont pas nécessaires pour installer l'intégration, mais elles permettent un enrichissement des vulnérabilités et sont utiles.

Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Remarque : Avant d'exécuter l'intégration, apportez tout changement de configuration nécessaire en fonction de vos besoins.

Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables d'applications que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service client et assistance. Le rôle administrateur est requis pour installer et configurer des applications sur votre ServiceNow AI Platform instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Obtenez vos informations d'identification API et votre jeton API sur votre console Invicti. Consultez les informations disponibles sur le site Web des produits Invicti à l'adresse API Overview .

Installer l'intégration ServiceNow® de Vulnerability Response avec Invicti

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que l'application s'intègre Invicti Vulnerability Integration correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer
Rôle requis : admin

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer le Invicti Vulnerability Integration .
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez l'application Invicti Vulnerability Integration .
4. Sélectionnez la vignette de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

5. Sélectionnez **Demander une application** et saisissez vos Now Support informations d'identification de connexion.
6. Sélectionnez **Obtenir**.
7. Entrez le **nom et** la **raison d'être de l'instance**, puis sélectionnez **Valider l'instance**.
8. Sélectionnez **Demande**.
   Vous recevez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.
10. Localisez l'application, sélectionnez-la, puis sélectionnez **Installer** pour l'activer.
    Votre application est automatiquement installée sur votre instance.

Configurez la Invicti Vulnerability Integration.

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que l'fonctionne Invicti Vulnerability Integration correctement avec la Réponse aux vulnérabilités des applications fonctionnalité de Réponse aux vulnérabilités.

Avant de commencer
Rôles requis :

- administrateur pour installer et activer les applications
- Groupe d'utilisateurs du gestionnaire de sécurité des applications pour configurer l'intégration

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que le Invicti Vulnerability Integration est installé et activé.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer l'intégration ServiceNow de Vulnerability Response avec Invicti reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe de gestionnaires App-Sec. • Le gestionnaire App-Sec supervise la configuration et vérifie les résultats attendus.
Pour l'intégration des vulnérabilités Inviciti, préparez votre **ID d'utilisateur** et votre **jeton d'API** .	Contactez votre administrateur Invicti pour obtenir **l'identifiant d'utilisateur** et le **jeton d'API** si vous ne les connaissez pas. Pour plus d'informations, consultez le site Web des produits Invicti à la section Présentation de l'API .

Traduction automatique

Procédure

1. Accédez à la **Tous** > **Invicti** > **Configuration Invicti**.
2. Remplissez les champs.

Champ	Description
URL D'API	URL d'instance Invicti de l'utilisateur. Voici les informations que vous avez obtenues de Préparez-vous pour le Invicti Vulnerability Integration.
ID d'utilisateur	ID d'utilisateur unique.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Jeton d'API	Jeton d’API que vous avez généré à partir de votre console Invicti. Voici les informations que vous avez obtenues de Préparez-vous pour le Invicti Vulnerability Integration.
Choisissez le type d’analyse. Vous devez en sélectionner au moins un.	
Importer DAST	Option permettant d’inclure les vulnérabilités à partir des analyses DAST. Les analyses DAST détectent dynamiquement les vulnérabilités d’une application pendant son exécution. Cette approche pourrait imiter une attaque extérieure.
Importer IAST	Option permettant d’inclure les vulnérabilités à partir des analyses IAST. Les analyses IAST détectent les vulnérabilités logicielles en interagissant avec le programme pendant son exécution. L’observation humaine, les tests automatisés et les capteurs sont utilisés en combinaison pour interagir avec l’application afin de localiser les vulnérabilités.
Format de date	Paramètre qui convertit l’heure de début au format pris en charge par l’API Invicti utilisée par l’intégration des éléments vulnérables de l’application Invicti. Ce paramètre doit correspondre au format que vous avez défini ou sélectionné dans votre compte Invicti, par exemple, **jj/MM/aaaa**. Vérifiez que les formats de date et d’heure de votre console Invicti correspondent à ceux que vous saisissez pour le format de date dans votre ServiceNow AI Platform instance. Pour modifier ce format dans votre console Invicti : **a.** Connectez-vous à Connexion Invicti . **b.** Sélectionnez **Nom d’utilisateur** en haut à droite. **c.** Accédez à la **Paramètres utilisateur** > **Format de date et d'heure**. **Remarque :** Des échecs d’importation peuvent se produire si vous saisissez un format de date non valide dans votre ServiceNow AI Platform instance. Si vous entrez un format valide dans votre instance qui diffère du format de date de votre console Invicti, Invicti renverra une charge utile vide.
Gérer les exceptions dans ServiceNow	Sélectionner un élément :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Activé (sélectionné) Les éléments vulnérables de l'application (AVIT) d'Invicti avec des états tels que **Présent** et **RisqueAccepté** qui peuvent être différés dans votre instance sont plutôt mappés pour **être** ouverts automatiquement. **Désactivé (non sélectionné)** Les états sources pour les éléments vulnérables de l'application (AVIT) importés à partir d'Invicti sont conservés. Vous devez gérer les exceptions pour ces AVIT (les reporter) à partir des dossiers AVIT. Pour plus d'informations sur les états sources et les champs cibles Invicti, reportez-vous à la section Invicti Vulnerability Integration Mappage de l'état.
Gérer les faux positifs dans ServiceNow	Sélectionner un élément : **Activé (sélectionné)** Les AVIT avec des états de Invicti tels que **Présent** et **Faux positif** qui peuvent passer à **Fermé** dans votre instance sont plutôt mappés pour **Ouvrir** automatiquement. **Désactivé (non sélectionné)** Les États AVIT importés d'Invicti sont préservés. Vous devez gérer les faux positifs ou les faux positifs potentiels pour ces AVIT à partir des enregistrements AVIT.

Traduction automatique

3. Sélectionnez **Enregistrer et tester les informations d'identification**.
4. **Facultatif :** Modifiez vos règles de recherche afin qu'elles soient basées sur des éléments de configuration.

   (Optional) Par défaut, la propriété système **sn_vul.use_product_model** est activée (définie sur vrai) pour vos règles de recherche répertoriées dans la table [sn_sec_cmn_ci_lookup_rule] en fonction du modèle de produit. Lorsque cette règle est activée :

   - Cette règle identifie les correspondances entre les données importées et les données de votre Base de données de gestion des configurations (CMDB) en fonction du modèle de produit.
   - Les enregistrements sont créés ou mis à jour dans la table Applications détectées [sn_vul_app_release].
   - Lorsque vous créez ou modifiez vos règles de recherche pour Invicti, le **modèle de produit** s'affiche dans le champ **Cible de recherche** du formulaire de règle.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour modifier vos règles afin qu'elles soient basées sur des éléments de configuration, vous devez désactiver manuellement (définir sur faux) la propriété système **sn_vul.use_product_model** .

a. Accédez à la **Tous** > **Propriétés système** et localisez l'enregistrement **sn_vul.use_product_model** et définissez la valeur sur faux.

b. Sélectionnez **Mettre à jour**.

c. Accédez à la **Tous** > **Security Operations** > **CMDB** > **Règles de recherche**.

d. Localisez les règles Nom de l'application et ID d'application source qui ont la cible de recherche comme **élément de configuration**.

e. Cochez la case Actif pour ces règles.

f. Sélectionnez **Mettre à jour**.
Lorsque vous créez ou modifiez vos règles de recherche pour Invicti, notez que **l'élément de configuration** s'affiche dans le champ **Cible** de recherche du formulaire de règle. Les enregistrements sont créés ou mis à jour dans la table Applications numérisées [sn_vul_app_scanned_application].

Affichage du statut et des enregistrements d'exécution de l'importation Invicti Vulnerability Integration

Utilisez la liste connexe **Exécutions d'intégration de vulnérabilité** pour vérifier le succès de vos exécutions d'intégration, localiser les problèmes et éclairer vos décisions de correction.

Affichage de l'état des importations, des jeux d'importation et des enregistrements

Pour afficher l'état de vos importations, en tant qu'utilisateur du groupe d'utilisateurs Gestionnaire de sécurité des applications, accédez à **Tous** > **Intégration de vulnérabilité Invicti** > **Intégrations** et sélectionnez un enregistrement d'intégration. Sélectionnez la liste connexe **Exécutions d'intégration de vulnérabilité** .

À partir de la version 1.1, affichez des détails tels que les temps de traitement totaux, les temps moyens des processus avant et après l'exécution de l'intégration, ainsi que des rapports sur les enregistrements d'exécution de l'intégration pour l'intégration des éléments vulnérables de l'application.

Pour afficher les jeux d'importation, accédez à **Tous** > **Intégration de vulnérabilité Invicti** > **Intégrations** > **Tables de jeux d'importation** et sélectionnez une intégration.

L'intégration de la liste des applications crée ou met à jour des enregistrements en fonction de la cible de recherche :

- Modèle de produit : Table Applications détectées [sn_vul_app_release]
- Élément de configuration : Table Applications numérisées [sn_vul_app_scanned_application]

L'intégration de la liste d'analyse crée ou met à jour des enregistrements dans la table Applications numérisées [sn_vul_app_scan_summary].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'intégration des éléments vulnérables de l'application crée ou met à jour des enregistrements dans la table Éléments vulnérables de l'application [sn_vul_app_vulnerable_item] et CWE [sn_vul_cwe].

Remarque : Chaque vulnérabilité dans Invicti a un « type », par exemple, ProductDirectoryListing. Ce type est importé, mappé en tant qu'ID unique dans votre instance et affiché dans le cadre de la valeur du champ Vulnérabilité de l'enregistrement de l'élément vulnérable de l'application (AVIT). Dans cet exemple, la valeur est Invicti-ProductDirectoryListing, et cette valeur est également affichée comme ID unique sur l'enregistrement d'entrée de vulnérabilité de l'application. Les AVIT Invicti prennent en charge plusieurs entrées de Common Weakness Enumeration (CWE), de sorte que les CWE ne sont pas utilisés comme ID uniques. Les CWE sont également affichés dans l'enregistrement AVIT.

Pour les AVIT Invicti, s'il existe des types en double dans Invicti pour une vulnérabilité, le mot « personnalisé » est inséré dans la valeur, par exemple, Invicti-custom-ProductDirectoryListing. Si vous créez un type personnalisé pour les vulnérabilités, l'ID de vulnérabilité peut être Invicti-Custom-<title of vulnerability>.

Nouveaux champs : pour le type d'analyse = Invicti, les paramètres affectés et les champs personnalisés peuvent inclure des données qui peuvent vous aider à comprendre la vulnérabilité et à y remédier. S'il n'y a pas de données, ces champs ne sont pas affichés sur l'AVIT.

Invicti Vulnerability Integration Mappage de l'état

Les états sources suivants de et Invicti Vulnerability Integration leurs états cibles dans votre instance sont répertoriés dans le tableau suivant.

États d'origine des Invicti et leurs états correspondants ServiceNow AI Platform

États sources des Invicti	Description des états sources	État cible dans ServiceNow AI Platform
Présent	Le problème est identifié.	Ouvert
Présent, RisqueAccepté, Relancé	Le problème a été pris en compte et est marqué comme une vulnérabilité à faible risque.	Différé
Présent, faux positif	Le problème a été examiné et est marqué comme n'étant pas une véritable vulnérabilité.	Fermé
CorrigéNon confirmé, Corrigé Non confirmé	Le problème a été résolu mais n'a pas été confirmé par Invicti Enterprise.	Résolu
Fixe (confirmé), FixedConfirmed, FixedConfirmed, AcceptedRisk, FixedConfirmed, Faux positif	Le problème a été résolu et confirmé par Invicti Enterprise et aucune autre action n'est requise.	Fermé
Corrigé (impossible de tester à nouveau)	Le problème a été identifié, mais Invicti ne peut pas effectuer un nouveau test pour confirmer s'il a été résolu ou non.	Résolu
Ranimé	Le problème a été résolu lors des analyses précédentes, mais a été retrouvé.	Ouvert
Différé, Ignoré	Le problème a été ignoré par l'utilisateur. Dans Invicti	Risque accepté

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États d'origine des Invicti et leurs états correspondants ServiceNow AI Platform (suite)

États sources des Invicti	Description des états sources	État cible dans ServiceNow AI Platform
	Enterprise, pour ignorer un problème, un utilisateur met à jour son état sur « Risque accepté ».	

Mappage de version de l'application

Champ source	Champ cible dans ServiceNow AI Platform
ID	source_app_id
CreatedAt	app_creation_date
UpdatedAt	app_updation_date
Nom	app_name
URL racine	Source_additional_info
Description	description
Balises	Balises

Mappage de vulnérabilité

Champ source	Champ cible dans ServiceNow AI Platform
Type	Nom de catégorie
Détail de la vulnérabilité	Résumé
Impact	Menace
Références de la source	Références Web
Recommandation source	Solution
Type	source_entry_id/ID
Gravité	source_severity
Classification["Cwe"]	Liste CWE
CvssVectorString	Champs CVVS v3

Mappage de la synthèse de l'analyse

Champ source	Champ cible
Source	Source
Nombre total de vulnérabilités	Detected_flaw_count
Date de lancement	Date de l'analyse dynamique
id	source_scan_id

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de l'élément vulnérable de l'application (AVIT)

Champ source	Champ cible dans ServiceNow AI Platform
Type	Type d'analyse
ID du site web	ID d'application source
ID	ID AVIT source
Date de la dernière consultation	Dernier trouvé
Date du premier observé	Premier trouvé
Date de la dernière mise à jour	Date de la dernière analyse
paramètres	Paramètre affecté
URL	URL affectée
Gravité	Gravité de la source
URL	Lien source
Détail de la vulnérabilité	Résumé de la vulnérabilité source
Références externes	Références de la source
Références Remedy + Remedy	Recommandation source
État	État du rattrapage de la source
Impact	Explication de la vulnérabilité source

Veracode Vulnerability Integration

L'intégration Réponse aux vulnérabilités à Veracode l'application utilise des données importées à partir du produit pour vous aider à déterminer l'impact et la priorité des failles Veracode dans votre code.

Veracode Vulnerability Integration

Le Veracode produit collecte les données des tests dynamiques de sécurité des applications (DAST), des tests de sécurité des applications statiques (SAST) et des scanners manuels et met ces données à la disposition du ServiceNow AI Platform®. Il s'intègre facilement à la Réponse aux vulnérabilités des applications fonctionnalité de cartographie des Réponse aux vulnérabilités vulnérabilités tierces, enrichissant ainsi les données de votre instance.

À partir de la version 19.0 de , vous pouvez importer des vulnérabilités de l'analyse de Réponse aux vulnérabilités la composition logicielle (SCA) et Nomenclature logicielle des données de vulnérabilité (SBOM) pour vous aider à identifier les faiblesses de vos applications logicielles. Pour plus d'informations, consultez Explorer Nomenclature logicielle.

Une API partagée ingère les données DAST, SAST, SCA et les résultats des tests de pénétration manuels.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Chaque jour, les travaux planifiés appellent automatiquement les intégrations dans l'ordre dans lequel elles sont répertoriées. Vous pouvez également exécuter manuellement des travaux planifiés individuels. Les travaux planifiés simplifient le cycle de vie du rattrapage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

des vulnérabilités en maintenant l'instance synchronisée avec d'autres systèmes de gestion des vulnérabilités.

Obtenir plus de détails de Veracode

À partir de la version 4.2, sélectionnez **Obtenir plus de détails** sur les éléments vulnérables de l'application (AVIT) qui ont Veracode comme source dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item] ou à partir des vues de listes dans les espaces de travail Réponse aux vulnérabilités pour afficher les données suivantes Veracode .

- Les détails de la demande source HTTP et de la réponse source pour les analyses de Test dynamique de sécurité des applications (DAST) sont affichés dans la liste connexe Demande/réponse HTTP.
- Les recommandations de solutions de Veracode sont affichées dans la liste connexe Résultats.
- La demande source HTTP, la réponse source et les recommandations sont affichées dans l'onglet Détails dans les espaces de travail Réponse Réponse aux vulnérabilités aux vulnérabilités.
- La colonne Description est prise en charge dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item].

Versions disponibles

Version de mise en production	Notes de publication
Veracode v4.3 Veracode v4.2 Veracode v4.1	Notes de version Réponse aux vulnérabilités des applications Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Groupe d'utilisateurs et rôles

Le Veracode Vulnerability Integration système est installé par un administrateur système [administrateur] et configuré par un membre du groupe Gestionnaire App-Sec. Consultez Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs pour plus d'informations.

Veracode Vulnerability Integration

Pour afficher les intégrations de Veracode vulnérabilité, accédez à **Tous** > **Intégration de vulnérabilité Veracode** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Vulnerability Integration

Intégration	Description
À partir de la version 4.1 : Veracode Lier les projets Intégration	Cette intégration est activée par défaut. Récupère tous les projets associés pour chaque application à partir de Veracode. Les applications peuvent avoir plusieurs projets dans l'application Veracode . Les données importées à partir de cette intégration sont affichées dans les enregistrements suivants : • **La date de la dernière analyse SCA**, **la date de création de l'application** et **la date de mise à jour de l'application** sont répertoriées sur les enregistrements dans **les applications détectées**. • Sur les enregistrements de synthèse de l'analyse de vulnérabilité de l'application et les éléments vulnérables de l'application (AVIT), **l'état SDLC source** (cycle de vie du développement logiciel) s'affiche. • **L'exploitabilité de la source** est affichée sur les enregistrements d'éléments vulnérables de l'application (AVI).
Veracode Intégration de la liste des applications (JSON)	Cette intégration est désactivée par défaut. Récupère les données du scanner d'application (vulnérabilités Veracode , métadonnées) et enrichit vos données d'application. Récupère les enregistrements d'analyse Veracode via une API basée sur JSON.
Veracode Intégration de la liste des applications (XML)	Cette intégration est désactivée par défaut. La version XML de cette intégration a été désactivée (déconseillée). Récupère les données du scanner d'application (vulnérabilités Veracode , métadonnées) et enrichit vos données d'application. Cette intégration est définie pour s'exécuter quotidiennement à 00:00:00. **Remarque :** Une API basée sur JSON est Veracode utilisée pour récupérer la liste des applications. Cette API importe la « date de dernière vérification de conformité de politique » pour ces applications, ce qui indique la date de la dernière analyse de ces applications par Veracode.
Veracode Nomenclature logicielle (SBOM) Intégration	La version 4.3 du Veracode Vulnerability Integration comprend les améliorations suivantes avec Veracode SBOM les fichiers : • Si vous avez installé SBOM Response, vous avez la possibilité d'inclure les vulnérabilités trouvées par Veracode pour les fichiers SBOM que vous chargez. • Veracode est mappé au champ **Source** pour les enregistrements dans la table Nomenclature [sn_sbom_doc] pour les Veracode fichiers SBOM. Cette intégration est activée par défaut. À partir de la version 4.2, importe les Nomenclature logicielle fichiers aux formats CycloneDX et SPDX générés par Veracode et les met en file d'attente pour les analyser dans votre instance. Vous devez avoir installé les Nomenclature logicielle applications pour importer ces données et les afficher.
Veracode Intégration de la synthèse	Cette intégration est désactivée par défaut. Récupère les enregistrements d'analyse Veracode via une API basée sur JSON. Cette intégration remplace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Vulnerability Integration (suite)

Intégration	Description
de l'analyse (JSON)	l'intégration d'API basée sur XML. Il est enchaîné et suit l'intégration de la liste des applications lorsqu'il Veracode est activé.
Veracode Synthèse de l'analyse (XML)	Cette intégration est désactivée par défaut. La version XML de cette intégration a été désactivée (déconseillée). Récupère les enregistrements d'analyse à partir de Veracode. Cette intégration est enchaînée et suit l'intégration de la liste d'applications lorsqu'elle Veracode est activée. **Remarque :** Suit automatiquement l'intégration de la Veracode liste des applications lorsqu'elle est activée. Avec la « dernière date de vérification de conformité de politique » pour les applications de Veracode, cette intégration récupère uniquement les données des applications qui ont été analysées après la « delta_start_time » de cette intégration.
Veracode Intégration JSON d'élément vulnérable d'application	À partir de la version 4.2, affichez des détails tels que les temps de traitement totaux, les temps moyens des processus avant et après l'exécution de l'intégration, ainsi que des rapports sur les enregistrements d'exécution de l'intégration pour les intégrations d'éléments vulnérables de l'application. Cette intégration est désactivée par défaut. Récupère les résultats de l'analyse contenant plus de données de vulnérabilité que l'intégration basée sur XML à partir de Veracode. Il insère des AVI et enrichit vos données de vulnérabilité tierces.
Veracode Intégration d'éléments vulnérables d'application (XML)	À partir de la version 4.2, affichez des détails tels que les temps de traitement totaux, les temps moyens des processus avant et après l'exécution de l'intégration, ainsi que des rapports sur les enregistrements d'exécution de l'intégration pour les intégrations d'éléments vulnérables de l'application. Cette intégration est désactivée par défaut. Récupère les résultats de l'analyse à partir de Veracode, insère des éléments vulnérables de l'application (AVIT) et enrichit vos données de vulnérabilité tierces. Par défaut, si l'enregistrement du scanner est à l'état **Fermé** , les AVIT ne sont pas créés. Les AVIT existants sont toujours à jour. Cette intégration est enchaînée et suit l'intégration du résumé de l'analyse lorsqu'elle Veracode est activée. L'API basée sur XML est déconseillée pour l'intégration JSON du résumé de l'analyse Veracode . **Remarque :** Suit automatiquement l'intégration du résumé de l'analyse Veracode . Avec la « dernière date de vérification de conformité de politique » pour les applications de Veracode, cette intégration récupère uniquement les données des applications qui ont été analysées après la « delta_start_time » de cette intégration.
Veracode Catégories Intégration	Cette intégration est désactivée par défaut. Récupère les données de catégories améliorées à partir de Veracode.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Vulnerability Integration (suite)

Intégration	Description
Veracode Intégration CWE	Cette intégration est activée par défaut. Récupère des données CWE (Common Weakness Enumeration) spécifiques pour obtenir des informations sur les menaces et des Veracode recommandations de correction. Ces données sont renseignées et mises à jour dans les enregistrements Entrée de vulnérabilité de l'application. Cette intégration CWE fonctionne indépendamment de la tâche planifiée pour l'intégration complète CWE 2000 que vous activez pour l'application Réponse aux vulnérabilités . Vos données ne sont pas dupliquées si vous avez activé l'intégration Veracode CWE et l'intégration complète CWE 2000.
Veracode Intégration DevOps	Cette intégration est désactivée par défaut. L'intégration est visible sur la liste Intégrations de vulnérabilité de l'application dans Réponse aux vulnérabilités des applications. Si vous disposez d'une licence DevOps Change Velocity, cette fonctionnalité est structurée de manière à ce que les utilisateurs DevOps n'aient pas besoin d'une licence SecOps pour afficher les détails récapitulatifs des analyses de vulnérabilité tierces. Il n'y a aucun impact ni changement à Réponse aux vulnérabilités des applications.

Pour les états d'exécution de l'intégration, Afficher l'état de l'exécution de l'importation de l'intégration de vulnérabilité de l'application Veracode reportez-vous à la section .

Pour afficher les données dans les vulnérabilités tierces, reportez-vous à la section Afficher les bibliothèques de vulnérabilités.

Préparation pour le Veracode Vulnerability Integration

Pour réussir, Veracode Vulnerability Integration il faut planifier et exécuter des tâches de pré-intégration. Préparez-vous à l'intégration en effectuant ces tâches. Cela Veracode Vulnerability Integration suppose que vous connaissez le produit et l'API Veracode .

Avant de commencer

L'intégration CWE (Common Weakness Enumeration) est également utilisée par Réponse aux vulnérabilités des applications et doit être en cours d'exécution avant l'installation et la configuration de .Veracode Vulnerability Integration Il est installé avec Réponse aux vulnérabilités, par défaut.

Remarque : Les données de la base de données de vulnérabilité NIST (NVD) ne sont pas nécessaires pour installer l'intégration de vulnérabilité de l'application Veracode , mais elles constituent un enrichissement et seraient utiles. Pour plus d'informations sur NVD, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.

Il existe un utilisateur d'exécution en tant que configuré pour chaque enregistrement d'intégration. La valeur par défaut pour cet utilisateur est **VR. système**. Ne modifiez en aucun cas cette valeur.

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

Remarque : Avant d'exécuter l'intégration, apportez les changements de configuration nécessaires en fonction de vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Validez le dimensionnement de votre instance en fonction du nombre d'éléments vulnérables d'applications que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, contactez Service client et assistance.

Nécessite Veracode Vulnerability Integration un ID API et une clé API.

Procédure

Pour créer l'ID API et les informations d'identification de clé :

a. Connectez-vous à la Veracode plateforme.

b. Accédez au menu du compte utilisateur et sélectionnez **Informations d'identification d'API**.

c. Cliquez sur **Générer les informations d'identification de l'API**.

d. Enregistrez vos informations d'identification pour une utilisation ultérieure.

Installer l'intégration ServiceNow® de Vulnerability Response avec Veracode

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit s'intègre Veracode correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si ce n'est pas déjà fait, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe de gestionnaires App-Sec. Pour en savoir plus sur les rôles de groupe, Réponse aux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	vulnérabilités des applications Groupes et rôles d'utilisateurs reportez-vous à la section . • Le groupe de gestionnaires App-Sec supervise la configuration et vérifie les résultats attendus.

Rôle requis : admin

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer le Veracode Vulnerability Integration .
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez Vulnerability Response Integration with Veracode application.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Envisagez de lire les sections **Autres exigences** et **dépendances** , le cas échéant.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Saisissez le **Nom de l'instance** et le **Motif de l'instance**, puis cliquez sur **Valider l'instance**.
8. Cliquez sur **Demander**.
   Vous recevrez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Configurez le Veracode Vulnerability Integration pour votre environnement. Consultez Configurez la Veracode Vulnerability Integration..

Configurez la Veracode Vulnerability Integration.

Avant d'exécuter l'intégration sur votre instance, les étapes d'installation et de configuration doivent être terminées afin que le produit s'intègre Veracode correctement à Réponse aux vulnérabilités des applications. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
Vérifiez que l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que l'intégration à Veracode l'application Réponse aux vulnérabilités est installée et activée.	Pour vérifier que cette application est activée, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer l'intégration ServiceNow de Vulnerability Response avec Veracode reportez-vous à la section .
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • S'il n'est pas déjà affecté, l'administrateur système [admin] installe l'application et affecte les utilisateurs au groupe d'utilisateurs Gestionnaire de sécurité des applications. • Le gestionnaire App-Sec supervise la configuration et vérifie les résultats attendus.
Pour l'intégration de vulnérabilité Veracode de l'application, préparez votre **ID API** et votre **clé API** .	Contact Veracode pour obtenir**l'ID** API et la **clé API**. Consultez Préparation pour le Veracode Vulnerability Integration. À partir de la version 4.0, si vous utilisez le Veracode Vulnerability Integration, les tests d'évaluation de pénétration dans le Veracode Vulnerability Integration sont des conclusions manuelles de Veracode. Ces résultats ne sont pas liés à des demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les demandes de test de pénétration dans , reportez-vous à Réponse aux vulnérabilités des applications la section Configurer les tests de pénétration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : groupe d'utilisateurs Gestionnaire de sécurité des applications

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Veracode** > **Configuration**.
2. Renseignez les champs **ID API** et **Clé API** .
3. Choisissez vos résultats de test.

Option	Description
Version 4.0 :	**a.** Sélectionnez les types **de données DAST** ou **SAST** à inclure dans l'importation. **Remarque :** Vous pouvez choisir l'un ou l'autre, ou les deux, mais vous devez en sélectionner au moins un. **b.** Sélectionnez **SCA** pour importer les vulnérabilités de l'analyse de la composition logicielle (SCA). **c.** Sélectionnez **Inclure manuel** pour importer les résultats des tests de pénétration manuels à partir de Veracode. Des AVIT sont créés pour ces résultats.
Version 3.0	Sélectionnez les types **de données DAST** ou **SAST** à inclure dans l'importation. **Remarque :** Vous pouvez choisir l'un ou l'autre, ou les deux, mais vous devez en sélectionner au moins un.
Version 1.0 :	Les résultats des tests dynamiques de sécurité des applications sont sélectionnés par défaut.

4. Ajoutez le niveau Veracode **de gravité** pour filtrer vos données importées.
   Cette valeur est importée de Veracode. Vous pouvez ajouter plusieurs valeurs au champ. Si elle est renseignée, l'importation rassemble uniquement les données qui correspondent aux niveaux de gravité que vous avez ajoutés.
5. Enregistrez et validez vos choix.

Option	Description
Version 3.0 :	Cliquez sur **Enregistrer et tester les informations d'identification**. **Remarque :** La configuration est terminée avec succès à moins qu'un message d'erreur ne s'affiche. Si un message d'erreur s'affiche pendant la configuration, saisissez à nouveau vos données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Version 1.0 :	Cliquez sur **Enregistrer**. Vérifiez la réussite de la configuration en cliquant sur **Tester les informations d'identification**. **Remarque :** La configuration est terminée avec succès à moins qu'un message d'erreur ne s'affiche. Si un message d'erreur s'affiche pendant la configuration, saisissez à nouveau vos données.

6. Sélectionnez la façon dont vous souhaitez gérer les exceptions et les faux positifs pour les AVIT lors de l'importation.
   Les options permettant de gérer les AVIT lors de l'importation avec les ServiceNow workflows Gestion des exceptions et Faux positifs sont activées par défaut. Les workflows sont déclenchés en fonction de la façon dont les états **sources** sur les AVIT sont mappés dans votre instance. Pour un exemple de cas d'utilisation, reportez-vous à la section Gestion du mappage d'état pour les reports et les faux positifs dans Réponse aux vulnérabilités des applications.

Activé	**Gérer les exceptions dans ServiceNow** Laissez cette option activée si vous souhaitez trier les AVIT importés marqués pour l'état **Différé** . Les AVIT avec des états **Source** qui sont normalement mappés à un état **Différé** dans votre instance sont plutôt mappés à **Ouvert**. Vous **demandez une exception** à partir de l'enregistrement AVI. **Gérer les faux positifs dans ServiceNow** Laissez cette option activée si vous souhaitez trier les AVIT importés dont l'état **Source** est marqué comme **Faux positif** ou **Faux positif potentiel**. Les AVIT avec ces états **sources** qui sont normalement mappés à un état **Fermé** dans votre instance sont mappés à **Ouvert**. Vous demandez un **faux positif** à partir de l'enregistrement AVIT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactivé	Désactivez l'une des cases à cocher ou les deux si vous souhaitez conserver les états **Source** importés de votre scanner. Ces AVIT sont mappés aux états **Cible** et **Motif cible** au fur et à mesure de leur importation, mais ne sont pas triés par les workflows d'exception et de faux positif. Les actions **Demande d'exception** et **Faux positif** ne sont pas visibles sur les AVIT.

7. À partir de la version 4.3, choisissez ou vérifiez les paramètres des paramètres suivants.

Paramètre	Description
Région de l'API	Sélectionnez une région dans la liste.
Délai d'attente de l'API	La valeur par défaut est 30 000. Vous préférez peut-être laisser ce champ dans son paramètre par défaut.
Inclure les vulnérabilités SBOM	Sélectionnez cette option pour inclure toute vulnérabilité ingérée par les Veracode intégrations dans les Veracode SBOM fichiers que vous chargez. Laissez le champ vide afin que Veracode les vulnérabilités ne soient pas analysées sur Veracode SBOM les fichiers.

8. Sélectionnez **Enregistrer et tester les informations d'identification**.

Que faire ensuite

Si votre environnement nécessite des importations séparées par domaine, reportez-vous à la section Créer des importations séparées par domaine pour une intégration.

Lors de l'installation initiale, reportez-vous à pour plus d'instructions Configurer Réponse aux vulnérabilités des applications .

Après l'installation initiale, pour les modifications, reportez-vous à Veracode Vulnerability Integration Modifications et activités.

Afficher l'état de l'exécution de l'importation de l'intégration de vulnérabilité de l'application Veracode

Utilisez la liste connexe **Exécutions d'intégration de vulnérabilité** pour vérifier le succès de vos exécutions d'intégration, localiser les problèmes et éclairer vos décisions de correction.

Avant de commencer

Pour afficher l'état de l'exécution de l'importation Veracode Vulnerability Integration :

- Réponse aux vulnérabilités des applications et le Veracode Vulnerability Integration doit être installé et configuré.
- Les Veracode Vulnerability Integration importations doivent être planifiées et en cours d'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités des applications mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à **Tous** > **Intégration de vulnérabilité Veracode** > **Intégrations**.
2. Sélectionnez une intégration.
3. Cliquez sur la liste connexe **Exécutions d'intégration de vulnérabilité** .
4. Vérifiez que toutes les importations ont réussi.

   Trouble?

   Les causes les plus courantes d'un échec d'exécution sont les suivantes :

   - Interruption du réseau.
   - Un problème dans le transfert des données entraînant des données corrompues pendant la transformation.

   Si vous rencontrez l'une de ces conditions, cliquez sur **Exécuter maintenant** et réexécutez l'intégration.
5. À partir de la version 4.2, affichez des détails tels que les temps de traitement totaux, les temps moyens des processus avant et après l'exécution de l'intégration, ainsi que des rapports sur les enregistrements d'exécution de l'intégration pour les intégrations d'éléments vulnérables d'applications.
   Pour plus d'informations sur l'affichage des détails supplémentaires importés par Veracode, voir Obtenir plus de détails dans Veracode Vulnerability Integration.

Afficher les Veracode résumés de l'analyse

Affichez les détails des informations de synthèse de l'analyse pour l'intégration de vulnérabilité Veracode .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Procédure

1. Accédez à la table Synthèses de l'analyse de vulnérabilité de l'application [sn_vul_app_vul_scan_summary_list].
2. Sélectionnez un enregistrement pour une Veracode analyse.
3. À partir des Réponse aux vulnérabilités versions 19.0 et 4.0 de l'intégration de vulnérabilité Veracode, utilisez l'icône Personnaliser la liste (icône Engrenage) pour afficher les colonnes suivantes.
   - Taille de l'analyse statique
   - Nombre de bibliothèques tierces
   - Nombre de bibliothèques tierces vulnérables
   - Nombre de failles tierce par gravité
   - Nombre de problèmes de bibliothèques tierces
   - Nombre de problèmes de licences tierces
   - Nombre de failles mixtes
   - Nombre de failles atténuées
   - Nombre de failles non atténuées
   - Nombre de failles statiques par gravité
   - Nombre de nouvelles failles par gravité
   - Nombre de failles non atténuées par gravité
   - Nombre total de failles par gravité
   - Dernière évaluation de l'analyse SCA
   - Date de la dernière analyse SCA
   - Date de publication de l'analyse
   - Balises

Transformation des données pour l'intégration Veracode de vulnérabilité

Une fois que vous avez identifié les données que vous souhaitez importer, les données sont récupérées à partir de l'application Veracode , traitées via un ensemble de sources de données et transformées dans votre instance.

Veracode Intégration d'élément vulnérable d'application

Les données de l'API sont d'abord chargées dans la Veracode table d'importation d'éléments AppVul [sn_vul_veracode_appvul_item_import], puis AppVul Veracode Item Transform est utilisée pour transformer les informations importées.

Pour accéder à cette carte de transformation, accédez à Transformation de *`System Import Sets > Transform Maps`* l'élément AppVul et recherchez celle-ci Veracode . La table suivante répertorie les champs de carte de transformation par intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Champs de carte de transformation d'élément AppVul

Champ source	Champ cible	Description
app_id	source_app_id	ID d'application.
ID du problème	source_avit_id	ID AVIT.
app_name	app_name	Nom de l'application.
version	app_version	Version d'application.
build_id	source_scan_id	ID de build de l'application.
account_id	account_id	ID de compte.
sandbox_id	sandbox_id	ID de bac à sable.
last_update_time	last_scan_date	Heure de la dernière mise à jour.
app_name + last_scan_date	scan_summary_name	Synthèse de l'analyse.
life_cycle_stage	source_sdlc_status	État SDLC source.
niveau	source_severity	Gravité de la source.
category_name	catégorie	Catégorie.
source_severity	source_severity	Gravité de la source.
category_id + « CWE- » + cweId	source_entry_id	ID d'entrée source.
source_vulnerability_summary	source_vulnerability_summary	Résumé de la vulnérabilité source.
source_recommendation	source_recommendation	Recommandation de la source.
description	description	Description de la source.
description	source_vulnerability_explanation	Explication de vulnérabilité source.
mitigation_status_desc	source_mitigation_status	État de l'atténuation de la source.
remediation_status	source_remediation_status	État du rattrapage de la source.
ligne	line_number	Ligne sur laquelle se trouve la faille.
module	application_module	Module d'application.
Fichier source	source_notes	Notes sources.
affects_policy_compliance	complies_with_policy	Les valeurs peuvent être Oui ou Non selon que les informations source sont vraies ou fausses.
Chemin d'accès au fichier source + fichier source	emplacement	Cartographie des emplacements en cas de `static` défaut.
URL	emplacement	Cartographie des emplacements en cas de `dynamic` défaut.
scope, type, exploitLevel	source_additional_info	Champ de valeur de nom renseigné avec les valeurs de la source en cas de défauts statiques.

Les scripts de transformation suivants sont exécutés au cours du processus de transformation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Veracode Minutage et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onComplete (lorsqu'un jeu d'importation a terminé la transformation)	Script utilisé pour traiter la source de données et mettre à jour le nombre d'AVIT créés, mis à jour ou inchangés, et ceux importés dans le cadre de cette intégration à partir de Veracode. Ce script est destiné à un usage interne et ne doit pas être modifié ou supprimé.

Veracode Vulnerability Integration Modifications et activités

Configurez des modifications facultatives spécifiques au Veracode Vulnerability Integration.

Affichage des données supplémentaires importées par le Veracode Vulnerability Integration

Remarque : La modification d'autres paramètres, autres que ceux répertoriés ici, nécessite une Veracode Vulnerability Integration expertise avancée ServiceNow et Réponse aux vulnérabilités des applications dépasse le cadre de la documentation du produit.

Obtenir plus de détails de Veracode

À partir de la version 4.2, sélectionnez **Obtenir plus de détails** sur les éléments vulnérables de l'application (AVIT) qui ont Veracode comme source dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item] ou à partir des vues de listes dans les espaces de travail Réponse aux vulnérabilités pour afficher les données suivantes Veracode .

- Les détails de la demande source HTTP et de la réponse source pour les analyses de Test dynamique de sécurité des applications (DAST) sont affichés dans la liste connexe Demande/réponse HTTP.
- Les recommandations de solutions de Veracode sont affichées dans la liste connexe Résultats.
- La demande source HTTP, la réponse source et les recommandations sont affichées dans l'onglet Détails dans les espaces de travail Réponse Réponse aux vulnérabilités aux vulnérabilités.
- La colonne Description est prise en charge dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item].

Modifier les Veracode paramètres d'instance d'intégration

Après l'installation initiale, vous pouvez modifier les Veracode paramètres des intégrations dans l'instance d'intégration Veracode .

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

Vous pouvez modifier les paramètres d'une intégration à partir de son instance pour déterminer le type de données que vous ingérez. Pour certains de ces paramètres, vous pouvez également modifier ces paramètres à partir de la page de configuration de l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Intégrations**.
2. Sélectionnez **Vulnérabilité de l'application Veracode** dans la colonne Instance source de l'intégration Veracode que vous souhaitez modifier.
3. Sélectionnez l'onglet **Paramètres de l'instance d'intégration** et double-cliquez sur un champ dans la colonne Valeur pour modifier les valeurs.

   À partir des versions 19.0 et Réponse aux vulnérabilités 4.0 de , Veracode Vulnerability Integration vous pouvez configurer les paramètres suivants pour les Veracode intégrations.

   Importer manuellement

   Entrez vrai pour importer les résultats des tests de pénétration manuels à partir de Veracode. Vous pouvez également modifier cette valeur à partir de la page de configuration de l'intégration.

   Les tests d'évaluation de la pénétration dans le Veracode Vulnerability Integration sont des résultats manuels de Veracode. Ces résultats ne sont pas liés à des demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les demandes de test de pénétration dans , reportez-vous à Réponse aux vulnérabilités des applications la section Configurer les tests de pénétration.

   import_sca

   Entrez vrai pour importer les vulnérabilités de l'analyse de la composition logicielle (SCA). Vous pouvez également modifier cette valeur à partir de la page de configuration de l'intégration.

   état

   Entrez Ouvert ou Fermé pour importer les résultats pour les états souhaités. Si vous laissez ce champ vide, les résultats de l'intégration importent pour les états Ouvert et Fermé.

   policy_sandbox

   Entrez une politique ou un bac à sable pour importer les enregistrements qui correspondent à une politique ou à un bac à sable. Ces enregistrements peuvent être liés à la façon dont les applications sont testées dans votre environnement.

   policy_rule_passed

   Entrez vrai ou faux pour importer des enregistrements qui ont satisfait à une règle de politique. Ces enregistrements peuvent être liés à la façon dont les applications sont testées dans votre environnement.

4. Sélectionnez **Mettre à jour** pour enregistrer vos changements.

Effectuer une importation manuelle Veracode de vulnérabilité de l'application

Si votre importation initiale a échoué, ou si vous ne souhaitez pas attendre l'importation initiale planifiée, vous pouvez effectuer une importation de données complète indépendamment de la tâche planifiée quotidienne.

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Veracode** > **Intégrations**.
2. Choisissez et l'intégration, par exemple, l'intégration de la liste des Veracode applications.
3. Cliquez sur **Exécuter maintenant**.

   Remarque : Chacune des intégrations de vulnérabilité des Veracode applications est destinée à fournir la récupération de données la plus complète. Les exécuter dans le désordre nécessite ServiceNow une Réponse aux vulnérabilités des applications expertise et peut entraîner des données incomplètes.

   Une fois l'importation terminée, les importations planifiées reprennent.
4. Pour les états d'exécution de l'intégration, Afficher l'état de l'exécution de l'importation de l'intégration de vulnérabilité de l'application Veracode reportez-vous à la section .
5. Si vous souhaitez modifier d'autres paramètres d'intégration, vous devez accéder à l'instance d'intégration.

Définir Veracode Vulnerability Integration les heures d'importation

Pour plus de commodité, vous pouvez réinitialiser l'heure de début du Veracode Vulnerability Integration fichier .

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

Après l'importation initiale, les Veracode intégrations de vulnérabilité effectuent une importation complète à chaque exécution. Voir Effectuer une importation manuelle Veracode de vulnérabilité de l'application pour plus d'informations sur l'exécution d'importations.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Veracode** > **Intégrations**.
2. Choisissez une intégration.
3. Définissez la nouvelle **heure de début**.
   L'heure est calculée en heures en heure locale. L'heure par défaut pour les importations d'intégration de liste d'applications Veracode est 00:00:00. Les autres intégrations sont **sur demande** et enchaînées pour s'exécuter après l'intégration de la Veracode liste des applications. La modification de **l'heure de début** pour l'un ou l'autre de ces éléments nécessite une expertise et Gestion de la vulnérabilité des applications une expertise avancéesServiceNow.
4. Cliquez sur **Mettre à jour**.
   La nouvelle heure est utilisée pour la prochaine importation planifiée.

Inclure les éléments vulnérables des applications Veracode fermées

Par défaut, les éléments vulnérables de l'application (AVI) **fermés** ne sont pas créés lors Veracode des importations d'intégration d'éléments vulnérables. Si vous souhaitez les créer, vous devez modifier une propriété système.

Avant de commencer

Doit Veracode Vulnerability Integration être installé et en cours d'exécution.

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans la zone de texte du **navigateur de filtre** de navigation de gauche, tapez `sys_properties.list`.
2. Dans **la zone** de recherche Nom de la liste, saisissez `sn_vul.create_closed`.
3. Double-cliquer sur le champ **Valeur** et définir sur **Vrai**
4. Cliquez sur coche verte pour enregistrer.
   Les enregistrements à l'état **Fermé** dans l'importation suivante Veracode sont créés en tant qu'AVI dans Réponse aux vulnérabilités des applications.

Ingestion manuelle des vulnérabilités pour Application Vulnerability Response

Les professionnels de la sécurité et les testeurs d'applications peuvent créer et gérer les conclusions du test de pénétration des applications dans l'espace de travail des tests de pénétration.

Les formulaires de test de pénétration sont disponibles dans l'espace de travail Test de pénétration pour documenter les vulnérabilités identifiées dans les applications d'entreprise principales.

Les professionnels de la sécurité et les testeurs d'applications peuvent importer manuellement les résultats à partir de sources et de plateformes externes à l'aide des modèles fournis au format Excel ou CSV. Tous les résultats de vulnérabilité sont disponibles dans l'espace de travail des tests de pénétration.

Pour accéder au modèle et le télécharger pour le chargement dans l'espace de travail Test de pénétration, accédez à **Tous** > **Ingestion manuelle des AVIT** > **Interface utilisateur, charger le fichier**.

Un nouveau formulaire de test de pénétration est créé pour chaque chargement de fichier pour l'application respective. Tous les résultats de vulnérabilité de ce chargement sont associés au même formulaire de test de pénétration. Le nom de l'application doit correspondre aux enregistrements dans l'une des tables :

- Table de l'application
- Table d'application d'entreprise
- Table de l'application numérisée

Le Nom de l'application est un champ obligatoire présent dans le modèle permettant d'identifier les vulnérabilités présentes au sein d'une application, associées à un formulaire de test de pénétration. Tout enregistrement sans nom d'application ne sera pas traité et ignoré lors de la création de la vulnérabilité.

Remarque : Les champs obligatoires du modèle sont nécessaires pour traiter les conclusions du test de pénétration. Il est nécessaire de s'assurer que tous les champs du modèle sont intacts afin d'éviter tout problème lors du traitement des résultats du test de pénétration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs obligatoires dans le cadre du modèle pour la création des résultats du test de pénétration

Nom de colonne	Obligatoire	Description	Options disponibles/ Nombre maximal de caractères dans les chaînes
Cote de risque	Obligatoire	Gravité de l'élément vulnérable de l'application	Critique Élevé Moyenne Faible Aucun (par défaut)
Demandé par	Obligatoire	Demandé par	151
Catégorie CWE	Obligatoire (remplir une seule colonne)	CWE ID	255
ID de la vulnérabilité	Obligatoire (remplir une seule colonne)	ID de la vulnérabilité	255
Application	Obligatoire	Nom de l'application	255
Objet de l'application	Obligatoire	Objet de l'application	4 000
Types de données sensibles	Obligatoire	Types de listes de données sensibles accessibles à partir des applications	40
Liste des programmes de conformité	Obligatoire	Liste des programmes de conformité	4 000
Détails des piles de technologies	Obligatoire	Détails des piles de technologies	4 000
Équipe d'application	Obligatoire	Nom de l'équipe d'application ; Groupe responsable du développement et de la maintenance des applications logicielles	100
URL à tester	Obligatoire	URL à tester	4 000
Étapes à reproduire	Obligatoire	Étapes à reproduire	1 000
Détails techniques	Obligatoire	Détails techniques	1 000
Affecté à	Obligatoire	Affecté à (personne responsable de la réalisation des tests de pénétration et de la génération des résultats de sécurité)	151

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs obligatoires dans le cadre du modèle pour la création des résultats du test de pénétration (suite)

Nom de colonne	Obligatoire	Description	Options disponibles/ Nombre maximal de caractères dans les chaînes
Groupe d'affectation	Obligatoire	Groupe d'affectation (groupe responsable de la réalisation des tests de pénétration et de la génération des résultats de sécurité)	151

Télécharger les vulnérabilités d'applications à l'aide d'un fichier de modèle

Utilisez un fichier de modèle pour charger les vulnérabilités de l'application. Pour accéder au modèle et le télécharger, accédez à **Tous** > **Ingestion manuelle des AVIT** > **Interface utilisateur, charger le fichier**.

Avant de commencer

Rôle requis : Hacker éthique **sn_vul.app_pen_tester**

Procédure

1. Accédez à la **Tous** > **Ingestion manuelle des AVIT** > **Interface utilisateur, charger le fichier**.
2. Sélectionnez les liens Excel ou CSV et téléchargez le modèle dans le format respectif.
3. Dans le modèle, saisissez les données de vulnérabilité dans les enregistrements.
   Pour obtenir des instructions sur la façon de renseigner les données dans le modèle, consultez la feuille « exemples » dans le modèle.
4. Sélectionnez Importer le fichier et chargez le modèle mis à jour.
5. Sélectionnez Soumettre.

   La page Files d'attente push d'intégration de vulnérabilité s'affiche. Vous pouvez suivre l'état et afficher les notes de journal associées aux soumissions.

Remarque : Pour toute erreur qui se produit :

- Un **fichier journal d'erreurs** est joint directement à l'enregistrement de **file d'attente push** associé.
- Des détails supplémentaires sur **les erreurs** se trouvent également dans la section **Notes du journal** du même enregistrement de file d'attente push.
- Cette approche garantit qu'Ethical Hackers peut facilement surveiller et résoudre les problèmes liés à leurs soumissions sans avoir besoin d'accéder à des détails d'intégration plus profonds au niveau du système.

Vérifier l'exécution de l'intégration

Si l'exécution de l'intégration réussit, passez en revue le nombre de détections individuelles et les conclusions du test de pénétration créées ou mises à jour.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Ingestion manuelle des AVIT** > **Intégrations**.
2. Sélectionnez le nom de l'intégration en fonction du type de fichier téléchargé.
3. Sélectionnez l'onglet Exécutions d'intégration de vulnérabilité.
4. Sélectionnez le numéro d'exécution de l'intégration.
5. Sélectionnez l'onglet Éléments.
   Passez en revue les informations de l'onglet Éléments.

Résultats

Onglet Éléments

Onglet/champ	Description
Onglet Éléments	Affiche le nombre total d'AVIT importés.
Nouveaux éléments	Affiche le nombre d'éléments vulnérables de l'application créés à partir de l'exécution de cette intégration.
Éléments importés	Affiche la somme de tous les champs dans cette section.
Éléments en double	Affiche les éléments en double. Ce champ n'est plus renseigné.
Éléments inchangés	Affiche les éléments vulnérables de l'application trouvés pendant l'exécution de l'intégration qui existent dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Remarque : Après avoir confirmé la réussite de l'exécution de l'intégration, suivez l'état de la soumission en accédant à l'enregistrement File **d'attente push** . L'enregistrement de file d'attente push fournit les détails suivants :

- **Notes de journal** : Contient des informations sur le traitement des enregistrements.
- **Fichiers d'erreur** : contient les détails de l'erreur qui se sont produits pendant le push.

Vérifier l'état du chargement

Vérifiez si l'exécution de l'intégration de vulnérabilité a réussi, partiellement réussi ou échoué.

Avant de commencer

Rôle requis : sn_vul.app_pen_tester

Procédure

1. Accédez à la **Tous** > **Ingestion manuelle des AVIT** > **Historique des fichiers chargés**.
2. **Examiner l'état du chargement** : dans la table **Files d'attente push de l'intégration de vulnérabilité de l'application** , examinez la colonne Créé pour l'horodatage du chargement et la colonne État pour l'état du chargement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. **Facultatif : Vérifier la réussite** : dans le champ Notes, affichez le massage de la réussite pour vous assurer que tous les enregistrements ont été traités avec succès.
4. **Gestion des erreurs (échec/réussite partielle)**
   - Pour les chargements à l'état « Échec » ou « Réussite partielle », un fichier journal d'erreurs est généré.
   - Les utilisateurs administrateurs peuvent afficher ce fichier pour comprendre les raisons de l'échec du chargement.
   - Les utilisateurs disposant du rôle app_pen_tester peuvent afficher les enregistrements de file d'attente push et les détails des erreurs associées.
   - Le fichier journal d'erreurs contient uniquement les résultats dont le traitement a échoué, fournissant des informations spécifiques pour la correction et la réingestion.
5. **Directives de réingestion** :
   - La ré-ingestion réussie des résultats traités créera des enregistrements en double.
   - Pour éviter les doublons, réingérez uniquement les résultats répertoriés dans le fichier journal d'erreurs.

Rattrapage des Réponse aux vulnérabilités des applications vulnérabilités

La surveillance du rattrapage est un processus qui commence par l'examen de l'état et se termine par la fermeture des éléments vulnérables de l'application (AVIT). Réponse aux vulnérabilités des applications offre des outils et des procédures pour rendre ce processus plus productif et efficace.

Réponse aux vulnérabilités des applications Processus de rattrapage

Le rattrapage des éléments vulnérables d'applications est effectué manuellement.

Une vue d'ensemble du processus :

- Connectez-vous à votre instance Réponse aux vulnérabilités des applications.
- Vérifiez que vos règles (Recherche de CI, Affectation) pour les éléments vulnérables de l'application fonctionnent comme prévu. Pour plus d'informations sur la révision des règles de recherche de CI, reportez-vous à la section Identifier automatiquement les applications dans Réponse aux vulnérabilités des applications. Pour en savoir plus sur les règles d'affectation, reportez-vous à la section Affecter automatiquement des éléments vulnérables d'applications Réponse aux vulnérabilités des applications.
- Validez que vos cibles de rattrapage sont correctes. Consultez Automatiser le suivi de la cible de rattrapage dans Réponse aux vulnérabilités des applications pour en savoir plus sur le fonctionnement des règles de cibles de rattrapage et sur la manière de les réviser. Afficher l'état de la cible de rattrapage d'un élément vulnérable d'application

  Remarque : Les règles de cibles de rattrapage appartiennent aux AVIT. Ces règles sont exécutées lorsque l'AVIT est importé.

- Examinez les tableaux de bord ou les rapports. Par exemple, consultez les tableaux de bord qui montrent l'ancienneté des AVIT par états.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Lorsque l'application Analyse des performances pour Réponse aux vulnérabilités (com.snc.vulnerability.analytics) est activée, les utilisateurs dotés de certains rôles peuvent afficher les données d'intérêt pour les membres des groupes Gestionnaire de sécurité des applications et Champion de sécurité.

Pour les gestionnaires de sécurité des applications, Analyse des performances pour Réponse aux vulnérabilités contient la vue d'ensemble Réponse aux vulnérabilités des applications , qui peut vous aider à surveiller les zones de préoccupation. Consultez les solutions d'analyse et de reporting pour le tableau de bord Application Vulnerability Response et Application Vulnerability Management [PA].

À partir de la version 13.0 de l'application Réponse aux vulnérabilités : Pour les champions de sécurité, Analyse des performances pour Réponse aux vulnérabilités contient le tableau de bord Mes vulnérabilités d'applications, qui peut vous aider à surveiller vos zones de préoccupation. Voir le tableau de bord Mes vulnérabilités d'application.

À partir de la version 13.0 de l'application Réponse aux vulnérabilités : Pour limiter la quantité de données collectées pour les rapports ou les listes connexes, reportez-vous à la section Définir les classifications de service pour Réponse aux vulnérabilités la génération de rapports et les listes connexes.

- Examinez l'état des AVIT, par ordre de priorité, en recherchant ce qui a changé.
- Révisez le risque pour les AVIT, au besoin. Consultez Créer un calculateur de vulnérabilité de l'application pour plus d'informations.
- Réaffectez l'AVIT à un groupe d'affectation pour y remédier, si nécessaire.
- Les nouvelles analyses sont déclenchées automatiquement par le calendrier d'importation tiers.
- Après une nouvelle analyse, si l'état est **Fixe**, les AVIT sont automatiquement fermés pendant l'importation.
- Après l'analyse, si l'état n'est pas **Fixe**, l'AVIT est rouvert.

Obtenir plus de détails de Veracode

Sélectionnez **Obtenir plus de détails** sur les éléments vulnérables de l'application (AVIT) qui ont Veracode comme source dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item] ou à partir des vues de listes dans les espaces de travail Réponse aux vulnérabilités pour afficher les données suivantes Veracode .

- Les détails de la demande source HTTP et de la réponse source pour les analyses de Test dynamique de sécurité des applications (DAST) sont affichés dans la liste connexe Demande/réponse HTTP.
- Les recommandations de solutions de Veracode sont affichées dans la liste connexe Résultats.
- La demande source HTTP, la réponse source et les recommandations sont affichées dans l'onglet Détails dans les espaces de travail Réponse Réponse aux vulnérabilités aux vulnérabilités.
- La colonne Description est prise en charge dans la table Élément vulnérable de l'application [sn_vul_app_vulnerable_item].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les bibliothèques de vulnérabilités

Vous pouvez afficher les données de vulnérabilité importées à partir de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou de tiers pour décider s'il y a lieu d'escalader une tâche de rattrapage.

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > pour **les bibliothèques**.

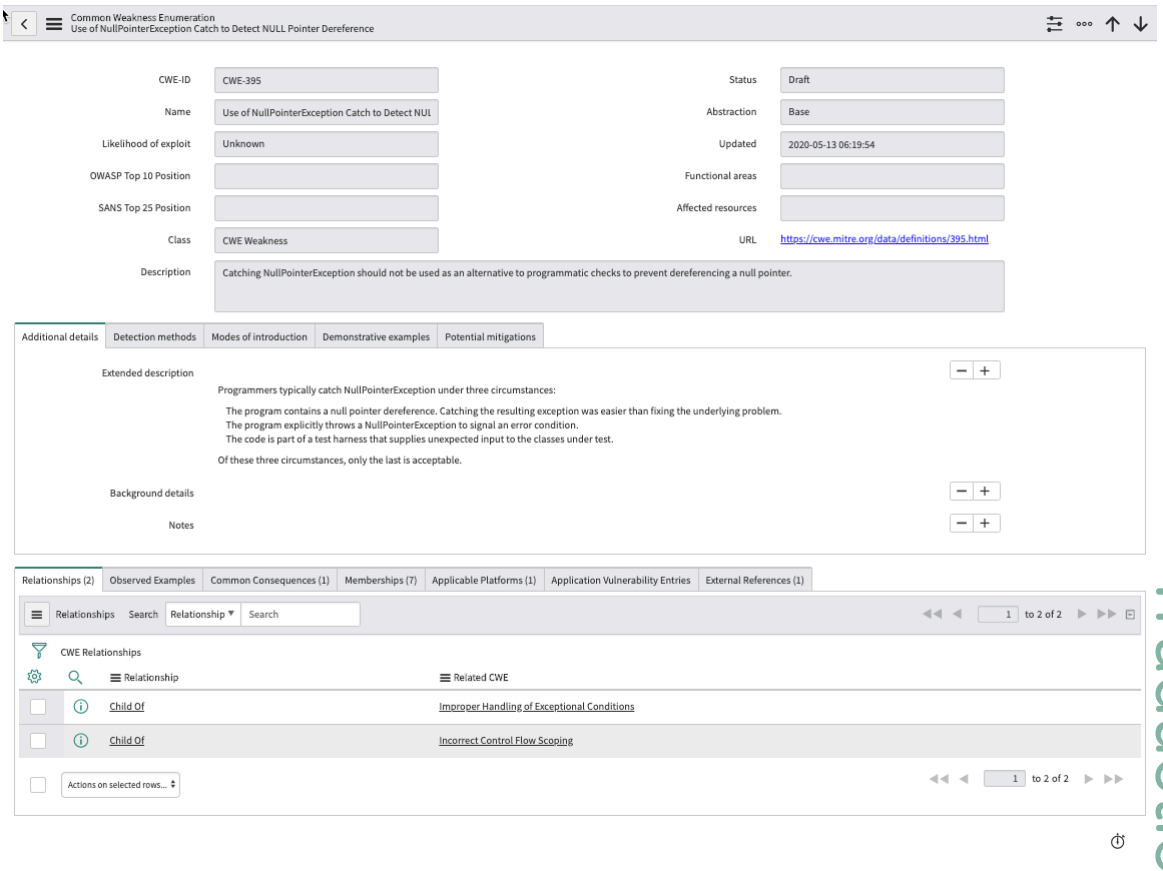
   Les bibliothèques suivantes sont disponibles :

Bibliothèques	Description
NVD	Liste des vulnérabilités trouvées par NVD et comprend des listes de vérification de sécurité, des failles logicielles liées à la sécurité, des erreurs de configuration, des noms de produits et des mesures d'impact, y compris les exploits.
CWE	Liste des types de faiblesses logicielles développés par la communauté. Chaque enregistrement CWE comprend également un article de la base de connaissances associé qui décrit la faiblesse. Vous ne pouvez pas escalader une vulnérabilité à partir de l'écran Common Weakness Enumerations, à titre de référence uniquement.
Tiers	Liste des vulnérabilités tierces importées dans votre instance. Contient une liste des références, des éléments vulnérables, des exploits, des CWE et des CVE connexes.

2. Choisissez une bibliothèque pour afficher les vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pour plus d'informations sur des champs spécifiques, reportez-vous à la section Champs de vulnérabilité de l'application.

Champs de vulnérabilité de l'application

Les vulnérabilités sont créées automatiquement lorsque les enregistrements sont téléchargés à partir de la base de données de vulnérabilité nationale (NVD), de Common Weakness Enumeration (CWE) ou d'intégrations tierces. NVD et CWE sont stockés dans **Bibliothèques** dans Réponse aux vulnérabilités ou sous **Vulnérabilités** dans Réponse aux vulnérabilités des applications.

Champs d'entrée de vulnérabilité CWE

Les champs de cette table sont en lecture seule.

Champ	Description
ID CWE	Identificateur de cette entrée de vulnérabilité. Cet identificateur est utilisé à la fois pour les catégories et les faiblesses, et est unique entre les deux ensembles de données.
Nom	Nom descriptif attribué à cet ID CWE.
Probabilité d'exploitation	Probabilité d'exploitation de la faiblesse, à l'échelle qualitative. L'un des suivants : • Faible • Moyen • Élevé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Position dans le top 10 OWASP	Position numérique de cette vulnérabilité dans la liste des 10 premiers de l'OWASP.
SANS à la position 25	Position numérique de cette vulnérabilité dans la liste des 25 premiers SAN.
Classe	Type de faiblesse
Statut	L'un des suivants : • Incomplet • Brouillon • Stable • Déconseillé • Obsolète • Instable
Abstraction	L'un des suivants : • Variante • Classe • Base • Composé
Mis à jour	Dernière mise à jour de l'enregistrement dans l'instance.
Domaines fonctionnels	Liste des domaines fonctionnels affectés. Par exemple, **Traitement des fichiers**. Renseigné uniquement pour les faiblesses 24/862.
Ressources affectées	Liste des ressources affectées. Par exemple, **Fichier** ou **Répertoire**. Renseigné uniquement pour les faiblesses 51/863.
URL	Article de la base de connaissances associé à cette vulnérabilité.
Description	Description de la vulnérabilité.
Exécution de l'intégration	Exécution d'intégration dans laquelle cette CWE a été importée.
Sections	
Informations supplémentaires	Descriptions des concepts logiciels qui expliquent davantage la faiblesse. Comprend: • Description étendue • Détails en arrière-plan • Notes
Méthodes de détection	Détails sur la façon dont vous pouvez détecter cette faiblesse dans une application.
Modes d'introduction	Les phases dans lesquelles la faiblesse est introduite, par exemple, la **mise en œuvre**, **l'architecture et la conception**, etc.
Exemples démonstratifs	Exemples de code de la faiblesse avec les descriptions qui les accompagnent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Atténuations potentielles	Des détails sur la façon de prévenir la faiblesse, y compris la phase du cycle de vie de l'application dans laquelle elle se produit et l'efficacité de l'atténuation.
Listes connexes	
Relations	CWE associés à cette vulnérabilité. Répertorie les relations entre cette CWE et d'autres. Peut inclure parent/enfant, suit/précède, requiredby/requires (pour les faiblesses composites), CanAlsoBe, PeerOf, MemberOf.
Exemples observés	Quelques CVE qui sont représentatives de cette faiblesse.
Conséquences courantes	Conséquences d'un exploit réussi, en termes de portée et d'impact. Par exemple : Champ d'application : Confidentialité Impact : lire les données de l'application
Adhésions	Adhésions CWE avec cette vulnérabilité.
Plateformes applicables	Plateformes associées à cette vulnérabilité.
Entrées de vulnérabilité de l'application	Autres entrées de vulnérabilité de l'application associées à l'une.
Références externes	Informations sur la vulnérabilité provenant de sources externes.

Champs d'entrée de vulnérabilité de l'application

Les champs de cette table sont en lecture seule.

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Source	Origine de la vulnérabilité : scanner ou test physique.
Gravité	Degré de gravité normalisé de cette vulnérabilité. Les cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Pour plus d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Mapper automatiquement la gravité d'un élément vulnérable d'application.
Version 13.0 : CWE primaire Version 12.1 : entrée CWE	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux. S'il existe plusieurs CWE associées à la vulnérabilité, la CWE principale est déterminée comme suit : • La CWE est-elle mappée au top 10 OWASP ? Si tel est le cas, utilisez ce CWE. Sinon, continuez. • La CWE est-elle mappée au top 25 des SAN ? Si tel est le cas, utilisez ce CWE. Sinon, continuez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	• La CWE a-t-elle la gravité la plus élevée ? Si c'est le cas, utilisez ce CWE. Sinon, continuez. • Sélectionnez la plus récente de toutes les CWE. La dernière CWE est celle avec la dernière valeur de champ **Mis à jour** dans l'enregistrement CWE.
Nom de catégorie	Classification fournie par l'intégration tierce. Aide à la tâche.
Détails des vulnérabilités	
Menace	Description de la menace que représente cette vulnérabilité.
Description de l'atténuation	Description des mesures qui pourraient être prises pour atténuer la vulnérabilité.
Liste connexe	
Version 13.0 : CWE	Liste des CWE associés à cette vulnérabilité. Non applicable pour le Veracode Vulnerability Integration.

Champs d'entrée NVD

Les champs importés dans cette table sont en lecture seule.

Remarque :

Les données NVD ne sont pas utilisées et Réponse aux vulnérabilités des applications les entrées représentent Réponse aux vulnérabilités uniquement les données.

Les CWE, qui sont utilisés dans Réponse aux vulnérabilités des applications, peuvent pointer vers des entrées NVD, comme exemples de faiblesse, et sont fournis ici à titre informatif uniquement.

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Cote de risque	(Masqué lorsqu'aucun élément vulnérable (VI) n'est Réponse aux vulnérabilités associé à la vulnérabilité) **Score de risque** quantifié séparant les VI en critiques, élevés, moyens, faibles et nuls.
Score du risque	(Masqué lorsqu'aucun élément vulnérable n'est associé à la vulnérabilité) Quantité calculée de risque que l'élément vulnérable pose à votre environnement.
Gravité	Degré normalisé de gravité de cette vulnérabilité dans Réponse aux vulnérabilités. Les cartes de gravité sont fournies pour NVD et avec ServiceNow des intégrations tierces. Réponse aux vulnérabilités des applications **La gravité** est dérivée de **la gravité source** importée et non de NVD. Pour en savoir plus sur le Réponse

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	aux vulnérabilités des applications mappage de sévérité, reportez-vous à la section Mapper automatiquement la gravité d'un élément vulnérable d'application.
Existence de l'exploit	Oui, si au moins un exploit est associé à cette vulnérabilité.
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter cette vulnérabilité.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour cette vulnérabilité.
VI actifs	(Masqué lorsqu'aucun élément vulnérable n'est associé à la vulnérabilité) Nombre d'éléments vulnérables associés à cette vulnérabilité, n'étant pas à l'état Fermé. Si aucun AVI actif n'est actif pour cette vulnérabilité, la **cote de risque** et le **score de risque** ne s'affichent pas.
Entrée CWE	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux selon la NVD.
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Résumé	Description de la vulnérabilité.
Détails des vulnérabilités	
CVSS v2	Données CVSS v2 importées
CVSS v3	Données CVSS v3 importées, non disponibles avant 2015.
Solution privilégiée	(Masqué lorsqu'aucun élément vulnérable n'est associé à la vulnérabilité) Solution de remplacement la plus élevée de la chaîne, dérivée des solutions référencées dans la vulnérabilité. S'il existe plus d'un remplacement le plus élevé dans la chaîne, aucune valeur n'est fixée. Toute valeur définie manuellement peut être écrasée lors des importations suivantes. La définition manuelle de cette valeur doit être effectuée sur l'élément vulnérable.
État du rattrapage (Masqué lorsqu'aucun élément vulnérable n'est associé à la vulnérabilité)	
Exclut les éléments différés	
Éléments vulnérables	Nombre d'éléments vulnérables actifs de l'application avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité. Ce nombre exclut les éléments vulnérables différés.
Inclut les éléments différés	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Éléments vulnérables	Nombre d'éléments vulnérables actifs avec cette vulnérabilité.
VI totaux	Nombre total d'éléments vulnérables avec cette vulnérabilité.
%VI rattrapés	Pourcentage complet pour le rattrapage des éléments vulnérables avec cette vulnérabilité.
Liens connexes	
Avant la version 13.0 : Forcer l'importation de la vulnérabilité logicielle **Remarque :** Supprimé dans la version v13.0	(Déconseillé) Recalcule le mappage du produit sur la base des informations de NVD. Met à jour la bibliothèque de logiciels vulnérables. Gestion des actifs logiciels ITSM
Mettre à jour le statut	Affiche la date et l'heure de la dernière mise à jour. Met à jour les éléments suivants : • État de la tâche de résolution • Score et notation du risque • Des mesures telles que les VI actifs, le total des VI de la section État de rattrapage
Listes connexes	
Éléments vulnérables	(Masqué lorsqu'aucun élément vulnérable n'est associé à la vulnérabilité) Éléments vulnérables associés à cette vulnérabilité.
Références de vulnérabilité	Informations sur la vulnérabilité provenant de sources externes, citées par NVD.
Exploite	Exploits associés à cette vulnérabilité.
Solutions	(Masqué lorsqu'aucun élément vulnérable n'est associé à la vulnérabilité) Toutes les Gestion des solutions pour vulnérabilités solutions d'intégration associées à cette vulnérabilité.
Version 13.0 : Faiblesses	Données de faiblesse CWE importées associées à des vulnérabilités et expositions communes (CVE).
Version 13.0 : Logiciel vulnérable	(Masqué lorsqu'aucun élément vulnérable n'est associé à la vulnérabilité) Données CPE (Common Platform Enumeration) importées associées à la vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identifier automatiquement les applications dans Réponse aux vulnérabilités des applications

Lorsque les données sont importées à partir d'une intégration tierce, Réponse aux vulnérabilités des applications utilise automatiquement les données de l'application pour rechercher des correspondances dans le Base de données de gestion des configurations (CMDB). Pour ce faire, il utilise les **règles de recherche de CI**. Ces règles identifient les applications pour l'enregistrement de l'élément vulnérable de l'application (AVI) afin de faciliter le rattrapage.

Au fur et à mesure que les applications sont importées, une recherche est effectuée sur l'application numérisée [sn_vul_app_scanned _application] ne pouvant pasutiliser source_app_id et app_name pour trouver des correspondances avec les applications provenant d'importations antérieures. Lorsqu'une correspondance d'ID d'application est trouvée, ses valeurs sont utilisées dans les champs **Application** et **Version de l'application** dans l'enregistrement de l'élément vulnérable de l'application.

Si aucune correspondance n'est trouvée ou si le champ ID de l'application est vide, les règles utilisent les autres informations de l'application pour tenter d'identifier correctement l'application. Si aucune correspondance n'est toujours trouvée, un enregistrement d'application analysé d'espace réservé est créé avec uniquement les champs **Nom de l'application** et **ID de l'application** .

Les règles de recherche **d'ID d'application source** et de **nom d'application** sont fournies avec , Veracode Vulnerability Integration par défaut.

Remarque : Les règles Réponse aux vulnérabilités des applications de recherche de CI par défaut ne sont disponibles que pour l'intégration de vulnérabilité Veracode .

Lors d'une tentative de correspondance, les règles de recherche sont évaluées en fonction de la valeur **d'ordre** la plus faible en premier. Elles s'arrêtent lorsqu'une règle renvoie un seul CI comme correspondance.

Remarque : Si une règle est créée de telle sorte qu'elle renvoie plusieurs CI, seule la première correspondance est utilisée.

Pour faciliter la recherche de problèmes correspondants, lorsqu'une correspondance est trouvée, la règle de recherche de CI utilisée pour la trouver est ajoutée au champ de **règle de correspondance de CI** pour les applications numérisées. Cliquez sur l'icône Mettre à jour la liste personnalisée en haut de la vue de liste Applications numérisées pour l'ajouter à la vue.

Remarque : Une fois supprimées, les règles ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Les règles de recherche de CI peuvent être séparées par domaine et sont spécifiques à la source. Si elle est prise en charge, chaque source peut avoir plusieurs déploiements. Par exemple, l'intégration de vulnérabilité Veracode peut avoir plusieurs déploiements de l'intégration de vulnérabilité Veracode . Chaque déploiement a son propre ensemble de règles de recherche de CI.

Remarque : Les règles de recherche de CI sont partagées par tous les déploiements de l'intégration de vulnérabilité. Si une règle est supprimée ou modifiée, la suppression ou les changements affectent tous les déploiements de l'intégration de vulnérabilité.

L'importation de données de vulnérabilité peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer la correspondance dans peut entraîner de longs délais de CMDB traitement. Pour éviter toute dégradation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

potentielle des ressources ou toute complication des performances, testez toutes les règles de recherche de CI écrites sur mesure ou les modifications apportées aux **règles de recherche de CI prédéfinies**. Consultez Empêcher les enregistrements dupliqués ou orphelins après l'exécution des règles de recherche de CI d'Application Vulnerability Response pour plus d'informations sur la prévention des enregistrements orphelins en double, la suppression des données et le nettoyage des données.

Information associée

Gestion des configurations et CMDB

Créer une règle de recherche de CI

Le module **Règles de recherche de CI** contient des règles qui définissent les champs qui ont des données correspondantes dans le Base de données de gestion des configurations (CMDB). Ces règles sont utilisées pour identifier les applications et les versions d'application et les ajouter à l'enregistrement de l'élément vulnérable de l'application (AVI) pour faciliter le rattrapage.

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

La création de règles de recherche de CI nécessite une expertise et Gestion de la vulnérabilité des applications une expertise avancéesServiceNow. Plutôt que de modifier l'une des règles de recherche existantes, envisagez de la copier et de modifier la copie. Lorsque vous êtes satisfait que la nouvelle règle fait ce que vous voulez, désactivez l'original.

Remarque : Une fois supprimées, les règles ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lorsque vous en créez de nouvelles.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **CMDB** > **Règles de recherche de CI**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de règle de recherche de CI

Champ	Description
Nom	Nom de la règle.
Méthode de recherche	Méthode utilisée pour l'appariement. Les choix possibles sont les suivants : ○ **Script** : script prédéfini ou personnalisé. ○ **Correspondance de champ** : recherchez sur une table ou un champ dans la CMDB.
Type	Type utilisé avec la **méthode de recherche** de script.
Ordre	Ordre de priorité de la règle. Les correspondances avec l'ordre le plus bas sont évaluées en premier.
Actif	Cochez la case indiquant si la règle est active ou désactivée.
Source	Source utilisée comme entrée dans cette règle. Une fois choisis, des filtres de condition apparaissent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

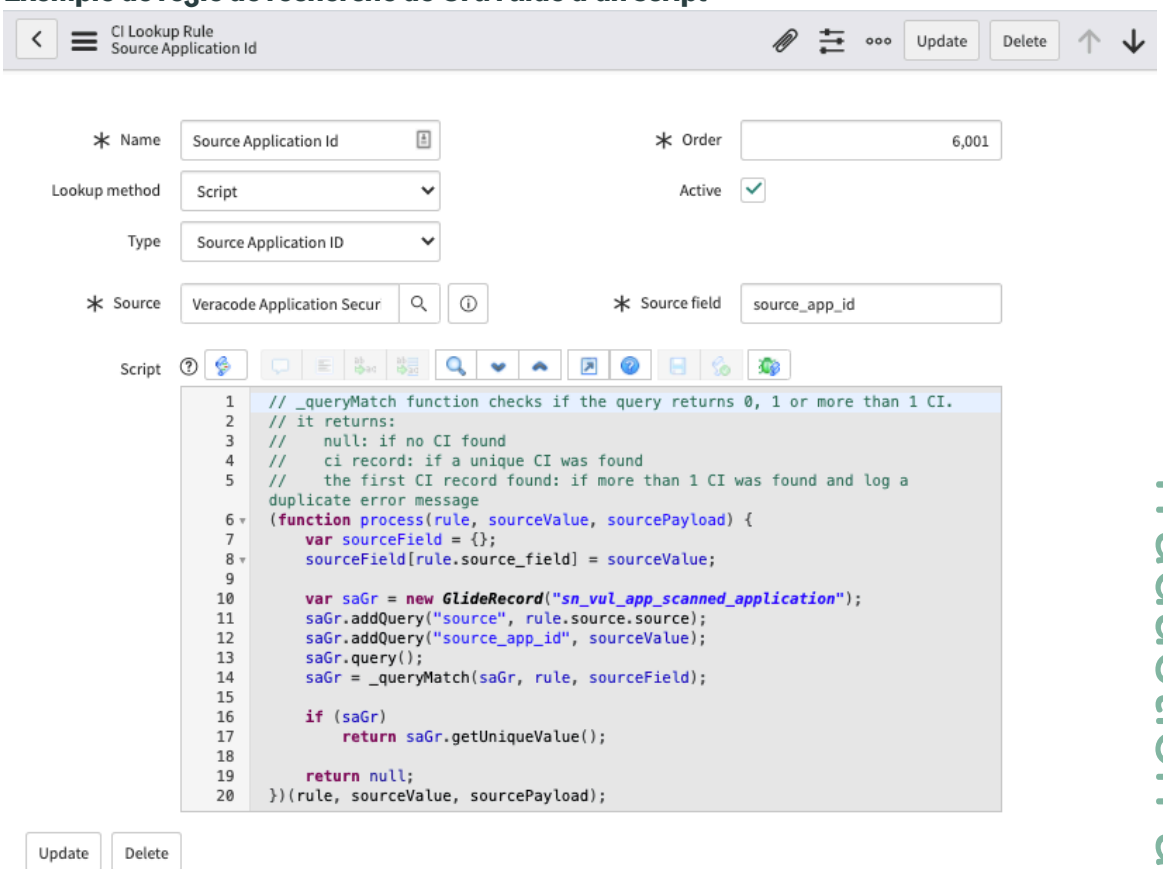
Champ	Description
Champ source	Champ source utilisé comme entrée dans cette règle. Les champs doivent être une chaîne ou un numéro.
Description	Texte décrivant la règle.
V19.0 : Cible de recherche	Approche de recherche que vous souhaitez suivre. Sélectionner à partir de : ◦ Élément de configuration ◦ Modèle de produit
Script	Un exemple de script modifiable, basé sur le **type**, s'affiche. Implémentez le script personnalisé en fonction des commentaires inclus dans le modèle de la fonction par défaut. **Remarque :** La fonction de processus comporte trois paramètres : `rule`, `sourceValue`, et `sourcePayload`
Rechercher sur la table CI	Table à rechercher dans la CMDB. Utilisé avec **la méthode de recherche** de correspondance de champ.
V19.0 : Rechercher sur la table des produits	Si vous choisissez la cible de **recherche Modèle de** produit, la valeur par défaut est Modèle d'application.
Rechercher sur le champ CI	Champ qui contient des informations pouvant être utilisées pour localiser un CI. Utilisé avec la **méthode de recherche** de correspondance de champ. Ce champ peut se trouver sur l'enregistrement du CI ou sur un enregistrement connexe, tel qu'une carte réseau.
V19.0 : Rechercher sur le champ Modèle de produit	Si vous choisissez la cible de **recherche** du modèle de produit, la valeur par défaut est Nom.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Envoyer**.

Exemple de règle de recherche de CI à l'aide d'un script



Information associée

Champs d'élément vulnérable d'application

Réapplication des règles de recherche de CI dans Réponse aux vulnérabilités des applications

Vous pouvez réappliquer vos règles de recherche d'éléments de configuration (CI) pour mettre à jour les CI existants (applications analysées et modèles de produits) sur les enregistrements d'application détectés.

Réapplication d'une règle de recherche

Vous pouvez « Réappliquer des règles de recherche » pour les éléments sélectionnés ou filtrés dans la table des applications détectées.

Si aucun filtre n'est appliqué, l'option Réappliquer est désactivée. Après avoir postulé à nouveau, les utilisateurs peuvent recevoir une URL de tâche en arrière-plan ou un message d'erreur si l'intégration est en cours d'exécution.

Pour réappliquer les règles aux applications détectées existantes, accédez à **Tous** > **Security Operations** > **CMDB** > **Règles de recherche**.

Remarque : À partir de la version 25.0.3 de , une nouvelle règle de Réponse aux vulnérabilités des applications fermeture automatique « CI désactivé » est introduite pour fermer les éléments vulnérables et les détections associés aux CI désactivés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définition de la cible de recherche

Par défaut, la *sn_vul.use_product_model* propriété système est activée (définie sur **vrai**). Selon la façon dont la propriété système est définie sur les enregistrements de règle de recherche de CI, les enregistrements d'application détectés sont mis à jour de la manière suivante :

- Si le champ Valeur est défini sur **vrai**, le modèle de produit est la cible de recherche des règles de recherche de CI et les applications détectées sont mises à jour avec les modèles de produit.
- Si le champ Valeur est défini sur **faux**, l'élément de configuration (applications analysées) est la cible de recherche et les applications détectées sont mises à jour avec les éléments de configuration (applications analysées).

Pour modifier la *sn_vul.use_product_model* propriété système afin que les éléments de configuration soient utilisés comme cible :

1. En tant qu'utilisateur disposant du rôle sn_vul.app_sec_manager, accédez à **Tous** > **Propriétés système** > **Tous**
2. Localisez *sn_vul.use_product_model*.
3. Ouvrez l'enregistrement.
4. Définissez le champ Type sur **faux**.
5. Sélectionnez **Mettre à jour**.

Si vous réinitialisez cette propriété système, vous devez modifier vos règles afin que les cibles de recherche correspondent au paramètre de propriété système. Par exemple, si vous réinitialisez la propriété système de sorte que vous utilisez l'élément de configuration comme cible, localisez les règles qui ont la cible de recherche comme élément de configuration.

1. Cochez la case Actif de ces règles et sélectionnez **Mettre à jour**.
2. Localisez les règles qui utilisent le modèle de produit comme cible et désactivez-les en désélectionnant la case à cocher Actif et en sélectionnant **Mettre à jour**.

Si vous créez une règle de recherche, vous devez définir la cible de recherche de la règle sur le formulaire de règle. Consultez Créer une règle de recherche de CI pour plus d'informations.

Empêcher les enregistrements dupliqués ou orphelins après l'exécution des règles de recherche de CI d'Application Vulnerability Response

Prenez des mesures pour empêcher les enregistrements en double ou orphelins résultant de la mise en correspondance (éléments de configuration (CI) dans le CMDB.

L'importation de données de vulnérabilité peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer des correspondances dans la CMDB peut entraîner de longs délais de traitement. Un test et un débogage approfondis des scripts de traitement dans les règles permettent d'atténuer le risque de problèmes ultérieurs dans le processus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Empêcher les enregistrements dupliqués ou orphelins

- Utilisez de petits sous-ensembles de données spécifiques à la règle de recherche de CI testée.
  - Définissez toutes les **règles de recherche de CI**, autres que celle en cours de test, sur **Inactives**.
  - Analysez les applications et les éléments de configuration (CI) importés pour vous assurer que vous observez le comportement attendu et que la correspondance se produit correctement.
- Examinez les états des CI tels que **Mis hors service**.
- Supprimer les données de test. Une fois que vous commencez à observer le comportement correct ou attendu dans la correspondance de CI, recommencez. Cela peut être fait par :
  - Suppression des données utilisées pour le test : (voir la section **Suppression des données des tables**)
    - Applications numérisées
    - Éléments vulnérables de l'application (AVI)
  - Réexécutez manuellement les intégrations.

.

Suppression des données des tables

Parfois, vous avez importé des données et vous vous rendez compte que quelque chose ne va pas. Si cela se produit dans un environnement de développement ou de performance, vous pouvez vous retirer d'un meilleur environnement, mais ce n'est pas toujours une option.

Remarque : L'exécution de ces actions nécessite une expertise avancée ServiceNow .

Il existe quatre options pour supprimer des données des tables :

- Utilisation de **Supprimer tous les enregistrements dans laconfiguration de table**.
- Configurez le **nettoyeur de table** en accédant à **Purges automatiques** (sys_auto_flush.list) et en créant un nouvel enregistrement **Purge automatique** .
- Tronquez la table gs.truncateTable à l'aide d'un script en arrière-plan.

  Remarque : Ne jamais utiliser `truncateTable` dans un environnement de production. Consultez votre représentant du support avant d'effectuer des suppressions importantes dans des environnements de production ou partagés.

- Créez une demande dans HI pour que les données soient supprimées.

Affecter automatiquement des éléments vulnérables d'applications Réponse aux vulnérabilités des applications

Affectez automatiquement les vulnérabilités d'application en fonction des balises d'application, ou de l'un des groupes d'affectation dans l'élément de configuration [cmdb_ci] ou des groupes d'affectation de plateforme, afin de réduire le délai moyen d'affectation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affectation automatique des éléments vulnérables de l'application

Il existe trois façons différentes d'affecter des AVI à l'aide de **l'affectation à l'aide de** :

Remarque : La fonctionnalité de recommandation d'affectation dans Réponse aux vulnérabilités n'est pas disponible pour Réponse aux vulnérabilités des applications.

- Groupe d'utilisateurs : cette option vous permet de sélectionner n'importe quel groupe d'utilisateurs existant ServiceNow AI Platform® .
- Champ du groupe d'utilisateurs : cette option vous permet de choisir n'importe quel champ de groupe d'affectation disponible à l'aide de la table cmdb_ci. Par défaut, les trois champs de groupe suivants s'affichent dans le menu Liste sous **Champ Groupe d'utilisateurs**.
  - Aucune : n'indique aucune valeur par défaut pour ce champ obligatoire
  - Élément de configuration : groupe d'approbation
  - Élément de configuration : groupe d'affectation
  - Élément de configuration : groupe de support
- Script : cette option vous permet de définir les conditions à l'aide d'un script. Cette option nécessite un codage ou une expertise avancée ServiceNow .

Exécutez d'abord les règles de priorité élevée (éléments nécessitant une gestion spéciale, lorsque le risque est critique ou qu'un AVI doit être géré par la conformité réglementaire). Ensuite, exécutez vos règles générales, où aucune manipulation spéciale n'est requise, et vous savez qui doit en être responsable. Enfin, créez une règle par défaut pour affecter des AVI au groupe qui déterminera à quel groupe d'affectation ils doivent appartenir. Ce groupe pourrait ajouter une autre règle pour couvrir ses décisions. Cette règle par défaut s'exécute en dernier.

Processus d'évaluation des règles d'affectation

Lorsqu'un nouvel AVI est créé, importé ou rouvert après avoir été fermé, les règles d'affectation sont évaluées en fonction de celui-ci. Un AVI n'est évalué qu'une seule fois, sauf s'il est rouvert après avoir été fermé. Vous pouvez réappliquer manuellement des règles après des changements.

Le processus suivant est utilisé pour chaque AVI nouveau, mis à jour ou rouvert :

- Pour chaque règle d'affectation de vulnérabilité, l'AVI est comparé au filtre d'affectation, en commençant par la règle d'ordre le plus bas.
- Lorsque la condition est remplie, l'AVI se voit attribuer un groupe d'affectation. La recherche s'arrête.
- Lorsque les conditions ne trouvent pas de correspondance parmi toutes les autres règles, l'AVI est affecté au groupe d'affectation par défaut, s'il existe une règle par défaut.

Remarque : S'il n'y a pas de règle par défaut, l'AVI reste non affecté.

Le type d'affectation, qu'il soit **manuel** ou **règleet règle d'affectation** , est disponible dans la zone de sélection Mise en page du formulaire de l'élément vulnérable de l'application (AVI). Tout AVI initialement affecté par une règle, mais réaffecté manuellement par la suite, contient une référence à la règle d'origine. Utilisez les informations de **règle d'affectation** et de **type d'affectation** pour identifier les tickets pour lesquels les règles d'affectation n'ont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pas trouvé de correspondance appropriée pour le destinataire prévu. Ou quelles règles ont connu le plus de réaffectations.

Remarque : Les règles d'affectation ne réévaluent pas les affectations créées manuellement.

Réapplication des règles d'affectation

Lorsque vous modifiez une règle d'affectation, utilisez le bouton **Appliquer les modifications** dans la vue de liste Règles d'affectation pour réexécuter toutes les règles modifiées sur tous les AVI ouverts actifs (à l'exception de ceux qui ont été affectés manuellement).

Remarque :

Si la tâche planifiée ne s'est `Reapply all vulnerability assignment rules` pas exécutée avant la première fois que vous utilisez **Appliquer des changements**, elle exécute toutes les règles d'affectation sur tous les AVI ouverts, à l'exception des AVI qui ont été affectés manuellement. Ensuite, toutes les utilisations ultérieures de **l'application Appliquer les modifications** réexécutent uniquement les règles modifiées et les règles dépendantes. Les changements apportés à une règle peuvent faire en sorte qu'un AVI correspondant à une règle différente non modifiée.

La tâche planifiée [`Reapply all assignment rules`] est inactive, par défaut. Lorsqu'elle est activée, elle applique toutes les règles à tous les AVI ouverts, à l'exception de ceux affectés manuellement. Il peut s'exécuter **quotidiennement**, **hebdomadairement**, **mensuellement**, **périodiquement**, **une fois** ou **sur demande**. En fonction du nombre d'AVI actifs que vous avez dans votre environnement, n'oubliez pas de définir le champ **Exécuter** correctement après l'exécution initiale pour éviter tout impact sur les performances.

Créer ou modifier Réponse aux vulnérabilités des applications des règles d'affectation

Vous pouvez créer des règles pour affecter automatiquement des éléments vulnérables d'application (AVI) en fonction des conditions de filtre. Ces règles affectent les AVI au fur et à mesure de leur importation ou de leur création manuelle.

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

Les règles d'affectation vous permettent de définir la condition d'affectation et l'ordre d'exécution. Une fois qu'un AVI correspond à une condition de règle, la recherche d'affectation s'arrête. Consultez Filtrage au sein de Gestion de la vulnérabilité des applications pour plus d'informations.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Règles d'affectation**.
2. Cliquez sur **Nouveau**.
3. S'il s'agit **d'un nouveau**, renseignez les champs du formulaire comme il convient.

Règle d'affectation de vulnérabilité de l'application

Champ	Description
Nom	Nom de la règle de groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Indique si la règle d'affectation est active.
Ordre d'exécution	Ordre dans lequel les règles sont évaluées. Les règles de priorité élevée, les éléments qui nécessitent une gestion spéciale, où le risque est critique ou un AVI doit être traité par la conformité réglementaire, à exécuter en premier. Ensuite, exécutez vos règles générales, où aucune manipulation spéciale n'est requise, et vous savez qui devrait en être responsable. Enfin, créez une règle par défaut pour affecter des AVI au groupe qui déterminera à quel groupe d'affectation ils doivent appartenir. Ce groupe pourrait ajouter une autre règle pour couvrir ses décisions. Cette règle par défaut s'exécute en dernier.
Description	Description de la règle d'affectation.
Condition	
Champs de condition	Conditions à remplir.
Nouveau critère	Ajoute d'autres champs de filtre de condition à choisir.
Affecter à l'aide de	Pour automatiser l'affectation des groupes créés en fonction de cette règle, choisissez l'une des options disponibles. ◦ Groupe d'utilisateurs : sélectionnez un groupe d'utilisateurs dans la table de recherche. ◦ Champ de groupe d'utilisateurs : sélectionnez un champ de groupe d'utilisateurs dans le menu Liste. ◦ Script : créez ou modifiez un script. **Remarque :** La création ou la modification d'un script nécessite une ServiceNow expertise.

4. Cliquez sur **Envoyer**.
   Les règles nouvelles ou mises à jour sont évaluées lors de l'importation suivante.

Suppression des affectations des éléments vulnérables et des tâches de Réponse aux vulnérabilités des applications rattrapage

Vous pouvez effacer les champs **Affecté à** et **Groupe d'affectation** des Réponse aux vulnérabilités des applications éléments vulnérables directement à partir des enregistrements d'élément vulnérable et de tâche de rattrapage de l'application que vous déterminez comme susceptibles d'être incorrectement affectés à vous ou à vos groupes.

Vue d'ensemble du workflow

Si vous déterminez que Réponse aux vulnérabilités des applications les éléments vulnérables (AVIT) et les tâches de rattrapage (AVUL) ne se trouvent pas dans votre périmètre pour le rattrapage, ou si vous pensez que des enregistrements vous ont été incorrectement affectés ou ont été affectés à vos groupes, vous pouvez vous supprimer ou supprimer vos groupes des champs **Affecté à** et **Groupe d'affectation** des enregistrements AVIT et AVUL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le workflow de désaffectation est pris en charge dans les vues classique et de l'espace de travail pour les AVIT et les AVUL.

Vous avez la possibilité d'envoyer des demandes pour effacer les champs d'affectation pour approbation. Consultez Approuver ou rejeter une demande de désaffectation dans Réponse aux vulnérabilités pour plus d'informations.

- Le bouton **Annuler l'affectation** s'affiche sur les enregistrements AVIT et AVUL dans tout état autre que Fermé ou Résolu.
- Une fois la demande d'effacement des champs approuvée, tous les champs **Affecté à** et **Groupe d'affectation** sur les AVIT qui sont associés à une AVUL et qui ont le même groupe d'affectation sont également désaffectés. Si un élément vulnérable d'application a un groupe d'affectation différent de celui de sa tâche de rattrapage associée, il n'est pas désaffecté. Dans la plupart des cas, ces éléments d'application vulnérables ont été affectés manuellement. Consultez Suppression des affectations des éléments vulnérables et des tâches de rattrapage pour plus d'informations.
- Tous les enregistrements que vous mettez à jour avec l'action d'interface utilisateur ou manuellement sont affichés dans le module Non affecté pour Réponse aux vulnérabilités des applications.
- Vous pouvez effacer les champs d'affectation de plusieurs AVIT d'une liste. Une fois que vous avez sélectionné les AVIT et sélectionné **Modifier en bloc**, dans la boîte de dialogue qui s'affiche, cochez la case **Annuler l'affectation** .

Consultez la rubrique Supprimer les affectations des éléments vulnérables et des tâches de rattrapage pour plus d'informations sur les étapes permettant d'effacer les champs d'affectation.

Propriétés système et notifications d'approbation

Si un propriétaire de rattrapage sélectionne **Annuler l'affectation** sur un enregistrement, par défaut, la propriété système sn_vul.unassign_vr.approval_required déclenche le flux d'approbation et crée un enregistrement d'approbation de changement d'état à l'état Révision, et la demande est acheminée pour approbation. La demande s'affiche dans la liste Mes approbations pour les utilisateurs disposant du sn_vul_.unassign_approver.

Remarque : En tant qu'administrateur de vulnérabilité [sn_vul.vulnerability_admin], vous pouvez définir la *`sn_vul.unassign_vr.approval_required`* propriété système sur **false** pour désactiver le processus d'approbation.

En outre, vous pouvez modifier la valeur de la *`sn_vul.default_assignment_group`* propriété système de sorte qu'un groupe spécifique est affecté si les champs d'affectation sont effacés. Par exemple, si un utilisateur clique sur **Annuler l'affectation** d'un enregistrement et que vous souhaitez le rediriger vers un groupe spécifique pour révision, vous pouvez ajouter l'ID système du groupe de votre choix dans le champ de valeur de la propriété système.

Remarque : Si vous modifiez cette valeur, les notifications pour tous les VIT, AVIT et CVIT qui ne sont pas affectés sont envoyées au groupe que vous spécifiez.

Pour plus d'informations sur la modification des propriétés système, reportez-vous à la section Suppression des affectations des éléments vulnérables et des tâches de rattrapage .

Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications

Les calculateurs de vulnérabilité de l'application automatisent le calcul des valeurs de risque initiales pour les champs des éléments vulnérables de l'application (AVI). Les calculs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de risque offrent un aperçu de la hiérarchisation du rattrapage. La condition de chaque calculateur est évaluée dans l'ordre, et le premier calculateur correspondant est utilisé.

Calculateurs de vulnérabilité de l'application

Le Réponse aux vulnérabilités des applications système de base comprend deux calculateurs de vulnérabilité qui définissent le **score de risque** de base sur l'élément vulnérable de l'application.

- **Calculateur de risque de base**
- **Calculateur Advanced Risk**

Les calculateurs de vulnérabilité de l'application peuvent être créés pour hiérarchiser et évaluer l'impact des AVI en fonction de n'importe quel critère à l'aide de filtres de condition. Qu'il s'agisse de l'impact de la vulnérabilité sur l'entreprise, de la classe de l'élément de configuration (CI) ou de l'âge de l'AVI, vous pouvez créer des calculateurs de vulnérabilité supplémentaires pour définir d'autres champs sur les AVI. Vous pouvez également personnaliser les calculateurs de vulnérabilité existants. Une calculatrice peut être rédigée pour refléter n'importe quel ensemble de priorités. Consultez Filtrage au sein de Gestion de la vulnérabilité des applications pour plus d'informations.

Les AVI contiennent la valeur du **score de risque** dérivée des calculateurs de risque.

Remarque : Un AVI affiche la **gravité de la source** , mais pas la gravité normalisée. La gravité normalisée est utilisée par les calculateurs pour obtenir la valeur du **score de risque** , mais n'est pas affichée sur les AVI.

Chaque calculateur contient une liste de règles du calculateur, avec une condition déterminant quand l'appliquer. Lorsque le calculateur est exécuté, la condition de chaque règle est évaluée dans l'ordre et la première règle correspondante est utilisée.

Tous les calculateurs de vulnérabilité activés définissent les champs sélectionnés chaque fois qu'un AVI est créé, lorsqu'un CI associé ou une vulnérabilité change.

Le calculateur de **risque de base** calcule le **score de risque** pour les AVI en utilisant la gravité de vulnérabilité normalisée.

Remarque : Un seul calculateur par champ cible (**score de risque**) peut être actif à la fois.

Le **risque de base** est activé par défaut. Le **calculateur Advanced Risk** est désactivé par défaut.

Règles du calculateur de vulnérabilité de l'application

Le **calculateur de risque de base** du système de base contient des règles qui affectent à chaque niveau de gravité (Aucun à Critique) une valeur (0-100) pour le **score de risque** en fonction de la gravité. Un score de **risque de 100** est automatiquement affecté à la gravité inconnue. Ces valeurs peuvent être ajustées et, comme pour **le calculateur Advanced Risk**, de nouvelles règles de calcul ou de nouvelles règles de risque peuvent être créées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 23.0 de , chaque fois que le score de Réponse aux vulnérabilités des applications risque est mis à jour sur un AVIT, la section **Notes** est mise à jour avec les détails suivants :

- Nom du groupe de calculateurs
- Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre crochets. Pour modifier ou afficher la base de la règle du calculateur, sélectionnez une règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. **Si Modèle** est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si **Script** est sélectionné, vous pouvez ajouter ou mettre à jour le script existant. La propriété `sn_sec_cmn.risk_score_changes_add_worknotes` système permet de renseigner la section Notes de travail. À partir de la version 25.0.3 de Réponse aux vulnérabilités des applications, la propriété `sn_sec_cmn.risk_score_changes_add_worknotes` système est inactive par défaut. Si vous l'activez, vous pouvez alors seulement voir tous les changements liés au score de risque d'un élément vulnérable d'application dans la section Notes de travail. En outre, les notes de travail ne sont mises à jour qu'en cas de changement du score de risque.

Le **calculateur Advanced Risk du** système de base contient une règle de calcul de vulnérabilité spécialisée appelée **Règle de risque par défaut**. Il calcule le **score de risque** en fonction de plusieurs valeurs :

- Gravité de la vulnérabilité
- 10 premiers OWASP
- SANS Top 25

Vous pouvez personnaliser les critères de la règle de risque par défaut. Pour plus d'informations, consultez Définir des champs et des poids pour la règle de risque.

Vous pouvez ajuster les valeurs à utiliser dans la **règle de risque par défaut** et le poids à donner à chacune de ces valeurs. Les poids sont utilisés pour ajuster le nombre de chaque élément lors de la définition du **score de risque**.

Chaque règle a un paramètre **d'ordre** . Cependant, la première à correspondre aux conditions met à jour le champ de **score de risque** dans l'AVI. Les règles de calculateur non scriptées ont généralement un impact moindre sur les performances que les règles de calculateur scriptées.

Poids du score de risque de vulnérabilité

Toutes les vulnérabilités se voient attribuer un score de risque et une cote de risque en fonction de facteurs tels que la gravité, la criticité, les informations sur l'exploitation, et ainsi de suite. La règle `Update Risk Rating from Risk Score` métier de la table des éléments vulnérables est responsable du calcul de la cote de risque. Chaque fois que le score de risque change, la cote de risque est calculée et renseignée pour les éléments vulnérables. Avant la version 17.1 de l'application Réponse aux vulnérabilités (VR), les cotes de risque suivantes étaient fournies dans le cadre du script include VulnerabilityUtils, qui étaient codées en dur.

Valeur (cote de risque)	Poids (score de risque)
1	90–100

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur (cote de risque)	Poids (score de risque)
2	70–89
3	40–69
4	1–39
5	0

À partir de la version 18.0 de Réponse aux vulnérabilités,

- Les types de cote de risque sont expédiés dans la table de base sous forme de avr_risk_rating. Ces types sont transmis dans le cadre de la règle métier sur chaque table où la cote de risque est calculée.
- Le script a été modifié afin que vous puissiez interroger les entrées dans les valeurs de la table Poids du score de risque pour le calcul de la cote de risque.
- Ajoutez des entrées supplémentaires pour un type existant ou créez-en un nouveau. Lorsque vous créez un nouveau type, assurez-vous d'ajouter les étiquettes pour la nouvelle cote de risque et de modifier les scripts et les règles métier associés. Vous devez également ajouter un nouveau style pour le nouveau score de risque.
- Modifiez le script pour interroger les enregistrements dans la table de base.

Vous pouvez accéder à la table des pondérations des scores de risque en saisissant sn_sec_cmn_risk_score_weight dans le navigateur de filtre.

En outre, le score de risque est automatiquement recalculé dans les scénarios suivants :

- Lorsqu'un élément de configuration (CI) passe d'un mode non accessible sur Internet à un élément accessible sur Internet.
- Lorsque les vulnérabilités et expositions communes (CVE) ou les entrées tierces (TPE) associées sur les éléments de vulnérabilité (VI) sont liées à une vulnérabilité d'exploitation connue (KEV) CVE.

Définir des champs et des poids pour la règle de risque

Personnalisez les paramètres et les pondérations de la règle de risque afin de pouvoir générer des scores de risque qui utilisent les données de vulnérabilité et d'actif propres à votre organisation. En sélectionnant les champs qui sont inclus dans la règle de risque, vous pouvez définir un cadre de travail de notation des risques efficace.

Avant de commencer

Rôle requis : sn_vul.app_manage_risk_score_configuration

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Calculateurs de vulnérabilités**.
2. Sur la page Calculateurs de vulnérabilité, cliquez sur **Calculateur de risque avancé**.
3. Accédez à la **Page Calculateur de vulnérabilité** > **Onglet Règles du calculateur de vulnérabilité** > **Règle sur les risques par défaut**.
4. **Facultatif :** Dans la section Critères du calculateur de risque de la page Règle de risque de vulnérabilité, définissez le poids de chaque critère en fonction de son importance dans le calcul du score de risque global.
5. Pour désactiver la règle, vous devez décocher la case **Actif** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Pour ajouter des champs de règles de risque aux critères du calculateur de risque, cliquez sur **Ajouter des critères**.
7. Remplissez les champs du formulaire.

Formulaire de champ de règle de risque

Champ	Description
Choisir la table de référence	Table que vous utilisez pour définir la pondération du score de risque. Vous pouvez sélectionner l'une des options suivantes : ○ **Élément vulnérable de l'application** : ajoutez des champs qui peuvent être remontés pas à pas à partir de l'élément vulnérable (VI). ○ **Élément vulnérable de l'application : élément de configuration** : ajoutez des champs parcourables par point qui font partie des extensions de table de base, telles que la table Matériel. Ces champs ne font pas partie de la table de base (cmdb_ci). ○ **Élément vulnérable de l'application : vulnérabilité** : ajoutez des champs parcourables par point qui font partie des tables qui étendent la table de base, par exemple, Entrée tierce. Ces champs ne font pas partie de la table de base Entrée de vulnérabilité. ○ **Table de référence de l'élément vulnérable de l'application** : ajoutez des champs qui font partie des tables connexes (m2m) ou des tables qui ont une référence à l'élément vulnérable. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du VI. ○ **Table de référence d'élément de configuration** : ajoutez des champs qui font partie des tables connexes (m2m) de cmdb_ci ou des tables qui ont une référence à cmdb_ci. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du VI. ○ **Table de référence de vulnérabilité** : ajoutez des champs qui font partie des tables connexes (m2m) des sn_vul_entry ou des tables qui ont une référence à sn_vul_entry. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du VI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **Conditions personnalisées** : utilisez cette option pour affecter des poids à la règle en évaluant la condition. Par exemple, le filtre orienté vers Internet détermine si un élément de configuration (CI) est externe ou interne.
Table	Champ qui s'affiche uniquement lorsque l'une des options suivantes est sélectionnée dans la table Choisir une référence : ○ **Élément vulnérable de l'application -> Élément de configuration** ○ **Élément vulnérable de l'application -> vulnérabilité** ○ **Table de référence des éléments vulnérables de l'application** ○ **Table de référence de l'élément de configuration** ○ **Table de référence de vulnérabilité**
Champ	Champ à utiliser pour le calcul du score de risque pour cette règle.
Agrégation	Champ qui s'affiche uniquement lorsqu'une table de référence est sélectionnée dans la table Choisir une référence. Sélectionnez la valeur minimale ou maximale à prendre en compte pour les calculs lorsque le champ est sélectionné dans les tables connexes (m2m).
Pondération	Pondération de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
Définir la pondération de la valeur	Composant permettant d'attribuer des poids à chaque valeur de champ. Pour les champs numériques, les valeurs de champ peuvent être définies comme une plage (par exemple, 1 à 5). Les pondérations doivent être un nombre entier compris entre 0 et 100. **Remarque :** Ce champ n'apparaît pas si l'option Conditions personnalisées est sélectionnée dans la table Choisir une référence.
Table de condition	Champ qui s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans la table Choisir la référence. Sélectionnez une condition dans la liste.
Nom de champ	Champ qui s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	table Choisir la référence. Entrez un nom pour les critères de risque.
Condition	Champ qui s'affiche uniquement lorsque l'option Conditions personnalisées est sélectionnée dans la table Choisir la référence. Prévisualisez les éléments de cette table qui correspondent aux conditions définies.

8. Cliquez sur **Envoyer**.
9. Sur la page Règle, activez et réappliquez la règle pour réévaluer le score de risque des éléments vulnérables actifs.

Example:
Ajoutez la gravité de la source comme critère pour une règle de risque.

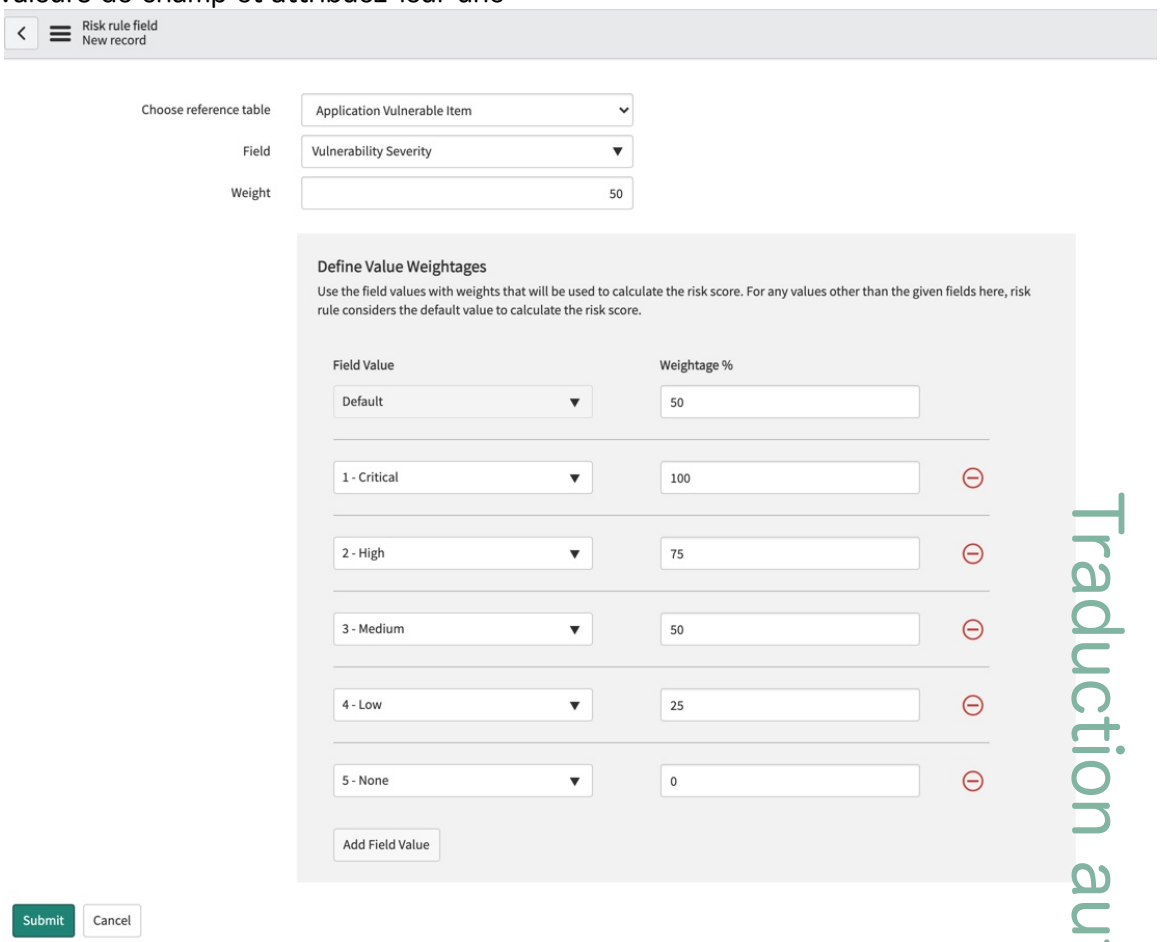
Cas d'utilisation : les fournisseurs tiers, comme Qualys et Tenable, fournissent leurs propres scores. Ces scores sont renseignés dans le champ Gravité de la **source** de la table sn_vul_entry. Utilisez ce champ pour les calculs de score de risque. Pour utiliser ce score afin de calculer le score de risque, procédez comme suit :

1. Accédez à la page Règle de risque.
2. Pour désactiver la règle, décochez la case **Actif** .
3. Pour ajouter des champs de règles de risque aux critères du calculateur de risque, cliquez sur **Ajouter des critères**.
4. Dans la liste Choisir la table de référence, sélectionnez **Élément vulnérable d'application**.
5. Dans la liste Champ, sélectionnez **Vulnérabilité.Gravité**.
6. Dans le champ **Poids** , entrez l'importance relative de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Dans la section Définir la pondération de la valeur, ajoutez des valeurs de champ et attribuez-leur une pondération.



8. Cliquez sur **Envoyer**.

Information associée

Calculateurs de Vulnerability Response et règles du calculateur de vulnérabilité

Créer un calculateur de vulnérabilité de l'application

Un calculateur de vulnérabilité d'application est une formule prédéfinie permettant de calculer un champ cible lorsque certains critères sont remplis. Les calculateurs, qui calculent le **score de risque** de l'élément vulnérable de l'application (AVI), peuvent contenir **des règles de risque**. Les calculs de risque offrent un aperçu de la hiérarchisation des mesures correctives.

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Remarque : Vous pouvez constater une dégradation des performances lors de l'exécution de calculateurs de vulnérabilité d'application contenant des scripts.

Organisez vos règles pour exécuter d'abord les règles les plus simples. N'exécutez des scripts que sur les éléments qui ne peuvent pas être traités avec une condition et une valeur de modèle ou une règle de risque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Calculateurs de vulnérabilités**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Formulaire du calculateur de vulnérabilité

Champ	Description
Nom	Le nom du calculateur de vulnérabilité de l'application.
Table	Rempli automatiquement avec le nom de la table AVI.
Application	Rempli automatiquement avec Réponse aux vulnérabilités.
Champ cible	Champ à calculer.
Description	Description textuelle du calculateur.
Actif	Allumez ou désactivez la calculatrice.

4. Cliquez avec le bouton droit dans l'en-tête pour **enregistrer**.
   La section **Règles du calculateur de vulnérabilité** s'affiche.
5. Créez une règle pour le calculateur en cliquant sur **Nouveau**.

> **Remarque :** Pour le formulaire **Nouvelles règles de risque** (disponible uniquement lorsque le **champ cible** est **Score de risque**), reportez-vous à l'étape 10.

6. Renseignez les champs comme il convient.

Formulaire Règle du calculateur de vulnérabilité

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur de vulnérabilité. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Rempli automatiquement avec le parent de calculateur.
Actif	Par défaut, la case **Actif** est sélectionnée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Vue avancée	Lorsque cette option est sélectionnée, les conditions de script et les valeurs de script peuvent être sélectionnées à partir du **type de condition** et du **type de valeur**.

7. Renseignez les champs de l'onglet **Quand cette condition est remplie** , le cas échéant.

Quand cette condition est remplie pour l'onglet

Champ	Description
Type de condition	Disponible lorsque vous sélectionnez la **vue Avancée**. Les choix sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Filtre : utilise des conditions de filtre. ◦ Groupe de filtres : voir Créer et définir des groupes de filtres pour définir les critères du calculateur. ◦ Script : condition de script utilisée pour déterminer quand appliquer ce calculateur. **Remarque :** Avant d'écrire des scripts pour déterminer quand appliquer les calculateurs, revenez à la liste **des calculateurs de vulnérabilité de l'application** . Explorez les enregistrements du calculateur de vulnérabilité fournis avec le système de base.
Condition	Définit les conditions de filtre de base pour déterminer s'il faut utiliser le calculateur ou non. La sélection des types **de conditions de groupe de filtres** ou de **script** masque ce champ.

8. Cliquez sur l'onglet **Définir ces valeurs** et renseignez les champs du formulaire comme il convient.

Onglet Définir ces champs

Champ	Description
Type de valeur	Disponible lorsque vous sélectionnez la **vue Avancée**. Les choix sont les suivants : ◦ Modèle : définissez les valeurs à définir sur chaque champ. ◦ Script : utilisé pour définir les valeurs de chaque champ.
Valeurs de script	Disponible si vous avez sélectionné le type de valeur **Script** . Définit les valeurs auxquelles appliquer les calculs.
Modèle	Sélectionnez les champs et les valeurs que vous souhaitez utiliser pour le calculateur. La sélection du type de valeur **de script** masque ce champ.

9. Lorsque vous avez terminé toutes les entrées, cliquez sur **Soumettre**.

Remarque : Lorsque vous modifiez un calculateur existant et que vous souhaitez mettre à jour tous les scores existants, vous pouvez utiliser le bouton **Réappliquer le calculateur** . Il passe en revue tous les AVI actifs, et si ce calculateur est utilisé pour définir sa valeur, il recalcule la valeur de ces AVI. Étant donné que la réapplication d'un calculateur peut prendre beaucoup de temps, une tâche planifiée le gère.

10. Pour le formulaire **Nouvelles règles de risque** , renseignez les champs comme il convient.

Définissez chaque poids en fonction du pourcentage du résultat qui doit provenir de cette valeur. Pour toutes les données que votre scanner ne fournit pas, ou pour les données qui ne doivent pas faire partie du score de risque, définissez le poids sur zéro.

Traduction automatique

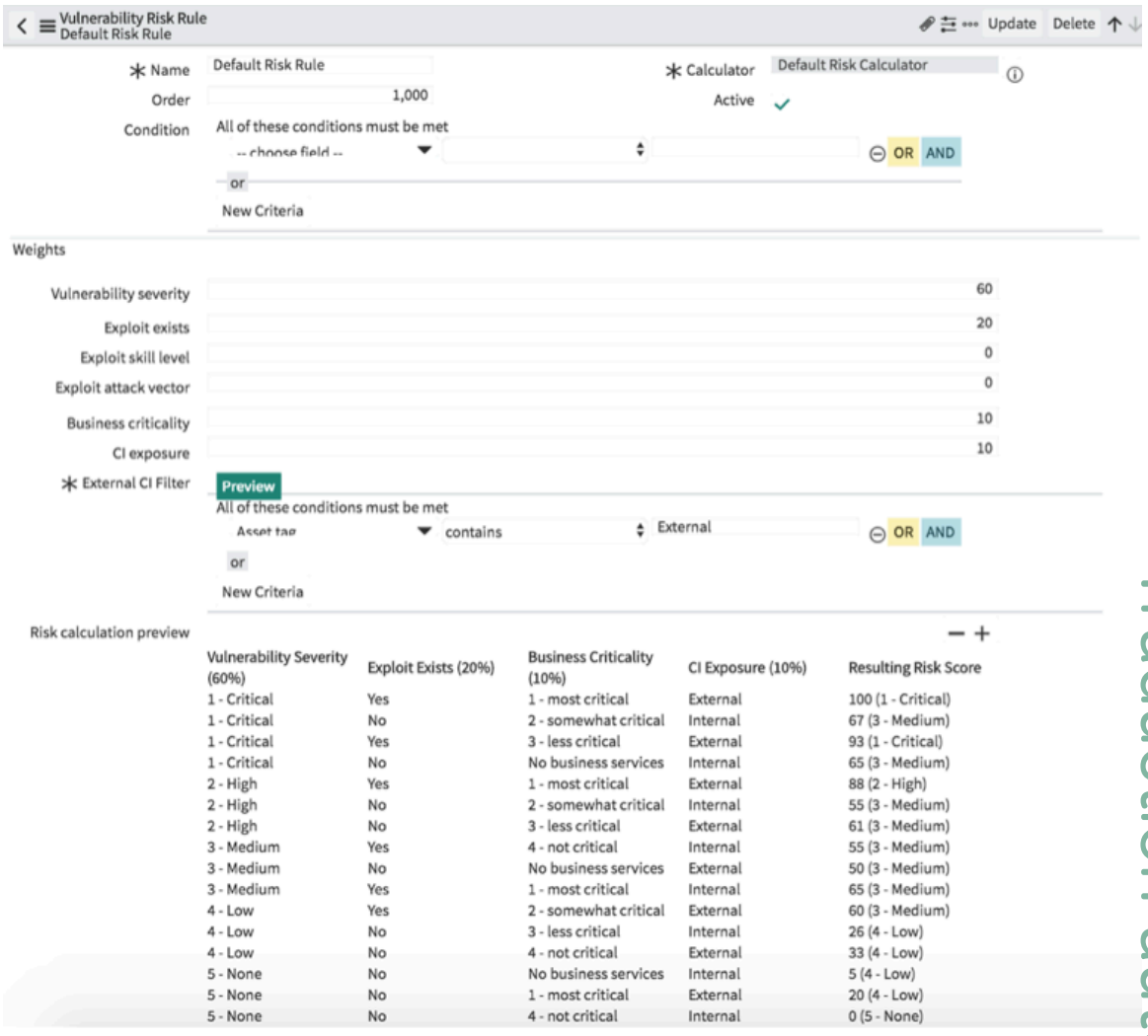
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous mettez à jour les pondérations, les scénarios affichent les pondérations restantes, ainsi que les résultats du **score de risque** prévus.

Champ	Description
Nom	Nom de la règle du calculateur.
Ordre	Ordre dans lequel exécuter le calculateur. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Calculateur	Rempli automatiquement avec le parent de calculateur.
Actif	Par défaut, la case **Actif** est sélectionnée, ce qui signifie que la règle du calculateur est active. Si vous décochez cette case, cette règle ne s'applique pas aux nouveaux éléments vulnérables créés dans le système.
Condition	Définit les conditions de filtre de base permettant de déterminer s'il faut utiliser le calculateur. La sélection des types **de conditions de groupe de filtres** ou de **script** masque ce champ.
Pondérations	
Gravité de la vulnérabilité	Pourcentage du résultat qui provient de la gravité.
10 premiers OWASP	Pourcentage du résultat qui provient de la présence de la vulnérabilité dans la liste des 10 premiers OWASP. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.
SANS Top 25	Pourcentage du résultat qui provient de la présence de la vulnérabilité dans la liste des 25 premiers SANS. Si ces informations ne sont pas présentes dans vos vulnérabilités, définissez le poids sur zéro.
Exécution totale	Pourcentages totaux calculés automatiquement. Lorsque cette valeur atteint 100, l'aperçu du scénario affiche des exemples de scores de risque dans différents scénarios.
Scénarios d'exemple	Lorsque tous les poids totalisent 100 %, les scénarios de score de risque s'affichent, fournissant un aperçu du score de risque dans certains des scénarios possibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Cliquez sur **Envoyer**.

Mapper automatiquement la gravité d'un élément vulnérable d'application

Réponse aux vulnérabilités des applications Le mappage de gravité transforme les champs de gravité de source tierce en champs reconnaissables dans Réponse aux vulnérabilités.

Avant de commencer

Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités des applications Des intégrations tierces telles que Fournir des mappages de gravité lors de l'installation Veracode Vulnerability Integration . Ces cartes peuvent être ajustées en modifiant les champs dans les cartes existantes.

La création ou la modification d'une carte de gravité est destinée uniquement aux mappages tiers personnalisés ou non standard dans votre environnement et nécessite Réponse aux vulnérabilités des applications une ServiceNow expertise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Mappage de gravité normalisé**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Mappage de champs

Champ	Description
Source	Nom de la source pour le mappage de gravité.
Valeur de la source	Valeur de gravité source.
Valeur cible	Valeur de gravité cible. Les choix possibles sont les suivants : ○ 1 - Critique ○ 2 - Élevée ○ 3 : moyen ○ 4 - Faible ○ 5 : aucun

4. Répétez l'étape 3 pour chaque niveau de gravité de la source.
5. Cliquez sur **Envoyer**.

Filtrage au sein de Gestion de la vulnérabilité des applications

Les calculateurs et les règles d'affectation utilisent des conditions lors de l'importation, créées à l'aide du **générateur de conditions**. Les changements apportés à leurs critères peuvent affecter les performances, car chaque enregistrement est évalué à l'aide de ces filtres.

Les règles et calculateurs fournis avec le système de base sont optimisés pour les performances. L'édition ou la création de règles ou de calculateurs prend soin et peut nécessiter les deux ServiceNow et Réponse aux vulnérabilités des applications une expertise. Cela dit, quelques conseils sont disponibles.

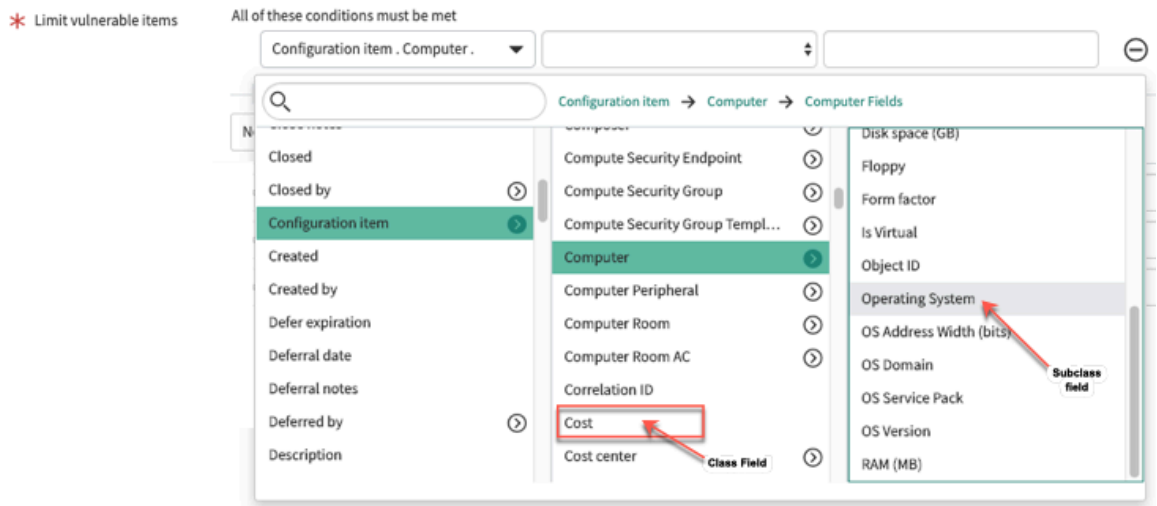
Éviter le filtrage basé sur les champs de sous-classe

Certaines tables prennent en charge l'extension. La table CI CMDB [cmdb_ci] en est un exemple. Des tables comme cmdb_ci_hardware et cmdb_ci_computer étendre cette table. Si vous filtrez en fonction d'un champ qui ne figure pas dans la table parente, la construction et l'évaluation de ce filtre peuvent s'avérer coûteuses.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Menu déroulant Filtre de condition



Par exemple, le filtrage sur **Élément de configuration** > **Coût** ne nuirait pas aux performances, car **le coût** est un champ de classe et non un champ de sous-classe de **l'élément de configuration**.



Élément de configuration > **Ordinateur**, cependant, est une sous-classe nécessitant une remontée pas à pas vers un autre champ, dans ce cas, **le système d'exploitation**. Ce processus peut prendre plusieurs millisecondes, ce qui s'accumule rapidement, lorsque des millions d'éléments vulnérables sont importés, et affecte les performances.



Remarque : L'utilisation de la condition [contains] s'apparente à une recherche par caractères génériques et peut avoir un impact sur les performances. L'utilisation de [est], dans la mesure du possible, est plus efficace.

Automatiser le suivi de la cible de rattrapage dans Réponse aux vulnérabilités des applications

Les règles de cibles de rattrapage d'applications définissent le délai prévu pour le rattrapage des éléments vulnérables d'applications (AVI), en fournissant un délai pour le rattrapage de la vulnérabilité elle-même. Par exemple, si un élément vulnérable d'application contient une cote de risque critique, la vulnérabilité de cet élément doit être corrigée dans les 15 jours.

Les gestionnaires App-Sec peuvent créer des règles de cibles de rattrapage d'applications en définissant :

- La cible de rattrapage.
- La cible de rappel.

Les gestionnaires App-Sec peuvent voir la date cible de rattrapage dans le formulaire AVI et les vues de listes, mais les dates ne sont pas mises à jour pour les AVI à l'état **Différé**, **Résolu** ou **Fermé** .

La **date cible de rattrapage** est codée par couleur sur la vue de liste AVI sous forme de points, comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les AVI qui n'ont pas encore atteint leur date de notification sont affichés en vert.
- Les AVI approchant de la date cible de rattrapage sont affichés en orange.
- Les AVI dépassant la date cible de rattrapage sont affichés en rouge.

Règles par défaut

Réponse aux vulnérabilités des applications est livré avec trois règles par défaut qui sont inactives par défaut :

- Règle de cote de risque critique : une cible de rattrapage avec une cote de risque critique **de 1** , une cible de rattrapage de 15 jours et un rappel de **7** jours avant la date cible.
- Règle de cote de risque moyen à élevé : une cible de rattrapage avec une cote de risque **2-élevé** ou **3-moyen** , une cible de rattrapage de 30 jours et un rappel de **7** jours avant la date cible.
- Règle de cote de risque moins critique : une cible de rattrapage avec une cote de risque **faible de 4-Faible** , une cible de rattrapage de 45 jours et un rappel de **7** jours avant la date cible.

Les règles de cibles de rattrapage peuvent être désactivées ou supprimées

Lorsqu'une règle est désactivée, les dates cibles de rattrapage actuelles pour les AVI auxquels elle s'applique sont effacées. Si un AVI satisfait à une règle active, cette règle est appliquée, sinon l'AVI n'a pas de règle ou de date cible, et son état est **Aucune cible**.

Lorsque des règles sont supprimées, la date **cible de rattrapage** et les champs connexes des AVI fermés sont conservés. La date **cible de rattrapage** et les champs connexes des AVI non fermés sont effacés et toutes les règles dépendantes sont réappliquées.

Scénario de règle de rattrapage

Lorsque plusieurs règles cibles de rattrapage sont appliquées au même AVI, la règle la plus restrictive s'applique.

Par exemple, si un AVI répond à la condition de deux règles de cibles de rattrapage d'applications :

Scénario : AVI ouvert pour la dernière fois le 03/01/2018 à 10:00:00.

- Règle de cible de rattrapage d'application 1 : Dernière ouverture le 03/07/2018 ; la cible de rattrapage est de 15 jours depuis sa dernière ouverture ; La date cible de rattrapage calculée est le 16/03/2018 10:00:00.
- Règle 2 de cible de rattrapage d'application : Dernière ouverture le 10/03/2018 ; la cible de rattrapage est de 10 jours à compter de sa dernière ouverture ; La date cible de rattrapage calculée est le 11/03/2018 10:00:00.

Dans ce scénario, la règle de cible de rattrapage d'application 2 s'applique à l'AVI, car elle a la date la plus restrictive. 10 jours depuis la première identification de l'AVI contre 15 jours.

Remarque : Les cibles de rattrapage de l'application sont calculées à partir de la **dernière date d'ouverture** additionnée au nombre de jours (mesurés par incréments de 24 heures). Vous pouvez ajouter ce champ au formulaire AVI à partir de la zone de sélection Mise en page. Il s'agit de la date à laquelle l'AVI a été ouvert pour la dernière fois dans votre instance.

À partir de la version 17.1, les cibles de rattrapage sont calculées à partir **de la cible à partir du (date).** La valeur par défaut reste **Date de la dernière ouverture**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Une fois que la règle de cible de rattrapage de l'application est définie, les dates cibles de rattrapage sont calculées par la `Evaluate remediation targets` tâche planifiée ou le bouton **Appliquer les changements** dans la vue de liste Règles de cibles de rattrapage.

À propos de la tâche planifiée Évaluer les cibles de rattrapage

`Evaluate remediation targets` s'exécute une fois à 4:00:00 tous les jours.

`Evaluate remediation targets` itère toutes les règles de vulnérabilité actives, en commençant par celles dont la date cible de rattrapage est la plus précoce. Il examine tous les AVI qui :

- ne sont pas à l'état **Fermé**, **Différé** ou **Résolu** .
- N'ont pas de date cible de rattrapage.
- Avoir une date cible de rattrapage ultérieure à la date de la règle de cible de rattrapage de l'application.

`Evaluate remediation targets` Ajoute une date cible de rattrapage, s'il n'en existe pas, ou si cette règle contient une date antérieure à celle de l'enregistrement, elle met à jour la date cible existante. Enfin, il met à jour les champs **Date cible de rattrapage** et **État du rattrapage** dans le formulaire AVI. Pour les règles inactives, **l'option Évaluer les cibles de rattrapage** efface les champs de rattrapage sur l'AVI.

Réapplication des règles de cibles de rattrapage

Lorsque vous modifiez une règle de cible de rattrapage, utilisez le bouton **Appliquer les changements** de la page de liste des règles de cibles de rattrapage pour réexécuter toutes les règles modifiées sur tous les AVI ouverts actifs, à l'exception de ceux dont l'état est **Fermé**, **Différé** ou **Résolu** .

Remarque :

Si la tâche planifiée est en cours d'exécution `Evaluate remediation targets` , vous ne pouvez pas lancer un processus de nouvelle demande. Toutefois, si un processus de réapplication est déjà en cours d'exécution et que la tâche planifiée est déclenchée, ils s'exécutent en parallèle.

Les processus de réapplication sont Réponse aux vulnérabilitésRéponse aux vulnérabilités des applications indépendants et peuvent s'exécuter en parallèle.

Créer ou modifier des règles de cibles de rattrapage d'applications

Favorisez le rattrapage des vulnérabilités à haut risque en temps opportun en configurant une règle de cible de rattrapage au niveau de l'élément vulnérable de l'application (AVI).

Avant de commencer
Rôle requis : App-Sec Groupe de gestionnaires

Remarque : Le système de base est livré avec trois règles de cible de rattrapage.

- Règle de cote de risque critique
- Règle de cote de risque moins critique
- Règle d'évaluation RIsk moyenne à élevée

Ces règles sont inactives par défaut. Si vous choisissez d'en modifier un plutôt que d'en créer un nouveau, n'oubliez pas de cocher la case**Actif** avant d'enregistrer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Administration** > **Règles de cibles de remédiation**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom de la règle.
Cible (jours)	Spécifiez le nombre de jours pendant lesquels les AVI doivent être corrigés, depuis leur dernière ouverture.
V17.1 : (date) de la cible	Date à partir de laquelle les SLA cibles sont calculés. Vous pouvez spécifier uniquement les champs de date ou le type de date et d'heure. La valeur par défaut est Dernière date d'ouverture. Pour personnaliser les valeurs de ce champ, consultez KB1642413 .
Actif	Par défaut, la case **Actif** est cochée, ce qui signifie que la règle de cible de rattrapage est active. Si cette case n'est pas cochée, cette règle ne s'applique pas aux nouveaux AVI créés dans le système.
Notifier (jours avant l'échéance)	Nombre de jours avant le délai de rattrapage ciblé pour la définition d'un rappel. La date de notification calculée à l'aide de cette valeur est utilisée pour afficher l'état du rattrapage et le code couleur. Si la date est antérieure à la date de notification, l'état du rattrapage est « En cours ». S'il a dépassé la date de notification et est antérieur à la date cible de rattrapage, l'état indique que la cible approche. **Remarque :** Si ce champ est défini sur 0, seule une notification **de cible manquée** est définie.
La règle s'applique à	À l'aide du filtre de condition, sélectionnez les critères d'application de la règle aux AVI. Pour éviter l'impact sur les performances, testez vos conditions à l'échelle de la production. Les tests vous permettent de déterminer la durée d'exécution de la tâche **Évaluer les cibles de rattrapage** , compte tenu des conditions et de la taille de votre Base de données de gestion des configurations (CMDB).
Mettre à jour l'historique	
Activités	Non utilisé lors de la création initiale d'une règle. Ensuite, les notes de travail du système sont consignées ici.

4. Cliquez sur **Envoyer**.
   Cette règle entre en vigueur lors de la prochaine exécution de la tâche planifiée, `Evaluate remediation targets`. Il en va de même lorsqu'une règle existante est mise à jour ou lors de l'utilisation du bouton **Appliquer les changements** dans la vue de liste Règles de cibles de rattrapage. Il en va de même lorsqu'une règle existante est mise à jour. Pour plus d'informations sur la tâche planifiée et **Appliquer des changements** , Automatiser le suivi de la cible de rattrapage dans Réponse aux vulnérabilités des applications reportez-vous à la section .

Afficher l'état de la cible de rattrapage d'un élément vulnérable d'application

Lorsqu'un élément vulnérable de l'application (AVI) a presque atteint (ou dépassé) sa date cible de rattrapage, telle que définie par une règle de cible de rattrapage, l'enregistrement AVI est mis à jour avec un état. Ces informations peuvent vous aider à surveiller de manière proactive les activités de rattrapage à venir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : App-Sec Groupe de gestionnaires

Pourquoi et quand exécuter cette tâche
La tâche planifiée **Évaluer les cibles de rattrapage** s'exécute une fois par jour pour comparer la date actuelle à la date de rattrapage de l'élément vulnérable spécifiée dans la règle de cible de rattrapage associée. Lorsque la date actuelle tombe dans le nombre de jours avant l'échéance du rattrapage, un état de rattrapage est ajouté à l'enregistrement d'élément vulnérable.

Procédure

Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Éléments vulnérables**.
Si la date de rattrapage de l'AVI se situe dans la plage des conditions définies dans la règle de cible de rattrapage, vérifiez les colonnes État de la cible de rattrapage, visibles dans la vue de liste Éléments vulnérables. Si la date cible de rattrapage est passée pour un AVI, une annotation s'affiche sur le formulaire AVI.

Remarque : Pour afficher le nombre d'AVI qui **approchent** de la cible, **en cours**et dépassent la**cible**, consultez le tableau de bord Gestion de la vulnérabilité des applications [PA].

Information associée

Créer ou modifier des règles de cibles de rattrapage d'applications

Fermer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage d'application peut être fermé immédiatement sans analyse supplémentaire, vous pouvez utiliser la fonction **Fermer** . À partir de la version 23.0 de , le bouton **Fermer** a été supprimé pour une tâche de rattrapage d'applicationsRéponse aux vulnérabilités.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Dans les espaces de Réponse aux vulnérabilités travail, une tâche de rattrapage passe par les mêmes états que dans les versions précédentes de Réponse aux vulnérabilités. Lorsque tous les éléments vulnérables (VIT) d'une tâche de rattrapage sont fermés, la tâche de rattrapage passe à l'état Inactif.

Important : Vous pouvez déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement les tâches de rattrapage des états Fermé ou Différé .

Procédure

1. Ouvrez l'enregistrement pour lequel vous souhaitez demander une révision.
2. Sélectionnez le bouton **Fermer** .
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
État	Sélectionnez l'état Fermé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Motif	Entrez le motif de la fermeture du problème.
Informations supplémentaires	Entrez toute autre information pertinente.

4. Sélectionnez **Soumettre**.
   La tâche de rattrapage est marquée comme **fermée**.

Gestion des changements pour Application Vulnerability Response

Créez des demandes de changement à partir des tâches de rattrapage dans l'application Réponse aux vulnérabilités de l'application pour accélérer votre enquête sur les vulnérabilités de l'application (AVIT) qui nécessitent une intervention manuelle.

Créez des demandes de changement avec des informations préremplies pour les applications numérisées qui sont classées comme éléments de configuration (CI) afin de vous aider à accélérer votre enquête sur les vulnérabilités d'applications (AVIT) qui nécessitent une intervention manuelle.

- Le workflow de demande de changement dans Réponse aux vulnérabilités des applications est similaire à celui pris en charge dans Réponse aux vulnérabilités.
- Pour plus d'informations sur le workflow de Réponse aux vulnérabilités demande de changement, reportez-vous à la section Change Management pour Réponse aux vulnérabilités.

Créer une demande de changement pour la tâche de rattrapage d'applications

En tant que gestionnaire App-sec ou champion de sécurité, vous pouvez créer des demandes de changement à partir de tâches de rattrapage dans l'application Application Vulnerability Response.

Avant de commencer

Rôles requis :

Depuis l'espace de travail du gestionnaire de vulnérabilité : sn_vul.app_sec_manager.

Depuis l'espace de travail du propriétaire ITRem : sn_vul.app_sec_champion ou sn_vul.app_developer, et rôle itil.

Pourquoi et quand exécuter cette tâche

Pour créer une demande de changement à partir de l'environnement classique, suivez les étapes ci-dessous.

Vous pouvez créer, approuver, implémenter, examiner et fermer des demandes de changement directement à partir d'une tâche de rattrapage. Vous pouvez créer trois types de demandes de changement avec des informations pré-remplies à partir d'une tâche de rattrapage :

- Standard. Un changement pré-autorisé à risque faible, relativement commun et qui suit une procédure ou une instruction de travail spécifique.
- Normal. Les demandes de changement normal suivent un processus prescriptif qui requiert deux niveaux d'approbation avant leur implémentation, revue et fermeture.
- Urgence. Un changement pour résoudre un incident majeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les demandes de changement ne sont prises en charge pour Application Vulnerability Response que si l'application détectée est associée à un élément de configuration (CI), ce qui se produit uniquement lorsque vous définissez « Modèle de produit » sur « Faux » dans la propriété système Utiliser le modèle de produit [sn_vul.use_product_model].

Procédure

1. Pour créer une demande de changement complète à partir d'un enregistrement de tâche de rattrapage existant, accédez à **Tous** > **Réponse aux vulnérabilités de l'application** > **Tâches de remédiation** > **Affecté à mes groupes**.
   La liste des tâches de rattrapage affectées à votre groupe d'affectation s'affiche.
2. **Facultatif :** Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Aperçu du rattrapage** pour afficher le tableau de bord Vue d'ensemble du rattrapage et localiser une VUL qui vous est affectée ou qui est affectée à votre groupe d'affectation.
3. Sinon, dans la colonne Nombre, cliquez sur une tâche de rattrapage pour ouvrir l'enregistrement et afficher les détails.
   L'enregistrement s'affiche.
4. Une fois l'enregistrement APP-VUL affiché pour lequel vous souhaitez créer la demande de changement, cliquez sur **Créer un changement** dans la partie supérieure droite de l'enregistrement.
   Le formulaire Créer une demande de changement s'affiche.
5. Renseignez les champs.

   a. Dans la liste de choix du champ S'applique à, choisissez-en un pour continuer.

Option	Description
Tous les éléments vulnérables actifs de l'application dans ce groupe	Si cette option est sélectionnée, tous les éléments vulnérables d'application actifs de cette tâche de rattrapage dont l'état n'est pas Fermé sont ajoutés automatiquement à la demande de changement une fois que vous avez cliqué sur **Créer un changement**.
Tous les éléments vulnérables d'applications dans ce groupe correspondant à un ensemble de conditions	S'il est sélectionné, le générateur de conditions s'affiche comme illustré dans la deuxième figure ci-dessous. Entrez des critères de filtre pour identifier les éléments vulnérables que vous souhaitez pour la nouvelle demande de changement. Un exemple de filtre peut inclure uniquement les éléments vulnérables qui correspondent à des critères de recherche spécifiques : **L'état est Ouvert** et le **score de risque est supérieur à 75**. Une fois que vous avez entré vos conditions, un message s'affiche avec le nombre d'AVIT qui correspondent à vos critères (10). Un lien (**Afficher l'aperçu des éléments correspondants**) permettant de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	prévisualiser les éléments correspondants s'affiche. Si aucun élément ne correspond à vos conditions de filtre, un message s'affiche sous le générateur de conditions pour vous demander d'ajuster votre filtre. Une fois que vous avez cliqué sur **Créer un changement**, tous les éléments vulnérables d'applications qui correspondent à ce filtre de condition sont déplacés vers une nouvelle tâche de rattrapage. Cette demande de changement est associée à la nouvelle tâche de rattrapage.

Créer un formulaire de demande de changement pour les éléments vulnérables de l'application dans une tâche qui correspond à un ensemble de conditions

b. **Facultatif :** S'il est affiché sur le formulaire, cliquez sur le lien **Prévisualiser les éléments correspondants** pour obtenir une liste des AVIT qui correspondent à vos critères de filtre. L'aperçu de la liste des tâches de rattrapage s'affiche. Vous pouvez sélectionner des éléments dans cette liste d'aperçu et y effectuer des actions d'interface utilisateur, mais ces actions sont également effectuées sur APP-VUL. Par exemple, si vous supprimez un VI de la liste d'aperçu, cet AVIT est également supprimé de APP-VUL.

c. Une fois que vous avez terminé votre aperçu, fermez la fenêtre du navigateur pour renvoyer le formulaire de demande de changement.

d. Pour la case à cocher Ajouter des CI au CR, choisissez-en un pour continuer.

Option	Description
Case à cocher Ajouter des CI au CR sélectionnée	Sélectionné par défaut. Si la case à cocher est sélectionnée, tous les éléments de configuration (CI) qui appartiennent aux éléments vulnérables actifs dans cette tâche de rattrapage sont ajoutés à cette demande de changement. L'APP-VUL passe automatiquement à l'état En attente d'implémentation .
Case Ajouter des CI au CR décochée	Décochez la case si vous ne souhaitez pas que les CI des éléments vulnérables d'application actifs de cette tâche de rattrapage soient ajoutés à la nouvelle demande de changement. Lorsqu'elle est désactivée, l'état de la demande de changement n'est pas synchronisé avec APP-VUL et l'APP-VUL reste dans son état actuel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Dans la liste de choix du champ Type de changement, choisissez-en un pour continuer.

Type de changement	Description
Urgence	Un changement pour résoudre un incident majeur.
Normal	Type de changement utilisé pour implémenter un changement apporté à un service qui n'est ni standard ni urgent.
Standard	Demande de changement préautorisée et à faible risque fréquemment implémentée. Les demandes de changement standard approuvées peuvent être prédéfinies dans un catalogue de modèles pour améliorer l'accès et le processus de demande d'un changement standard. Si cette option est sélectionnée, deux champs s'affichent. Sélectionnez-en un dans chaque liste de choix pour remplir ces champs : ▪ Catégorie de changement : sélectionnez une catégorie pour le changement dans votre catalogue existant, par exemple, Matériel, Changements standard du serveur, Logiciel. Dans cet exemple, l'option Appliquer des correctifs aux changements standard est sélectionnée. ▪ Modèle de changement : sélectionnez un modèle disponible pour les demandes de changement avec des tâches de prise en charge prédéfinies à partir de votre catalogue. Dans cet exemple, le modèle du cycle d'application de correctif mensuel Microsoft est sélectionné. Pour en savoir plus sur les catégories de demandes de changement ITSM, les modèles et les types de changements, consultez Types de changements .

La fonctionnalité lit automatiquement les types de demandes de changement que vous configurez dans votre catalogue dans Gestion des changements ITSM. Par exemple, si vous changez le nom de vos demandes de changement standard dans ITSM de Standard à Préapprouvé, votre nouveau nom s'affiche automatiquement dans la liste de choix Type de changement de l'onglet Créer une demande de changement à partir de comme illustré dans la figure suivante.

Les champs de la section Aperçu de la demande de changement du formulaire sont pré-remplis avec des informations provenant de APP-VUL. Si nécessaire, ces valeurs de champ peuvent être modifiées. Par exemple, examinez les valeurs dans les champs de la figure suivante :

Date de fin prévue

Cette date (10/10/2019) est la même que celle affichée dans le champ Date cible de rattrapage de APP-VUL. Cette valeur est dérivée de la date cible de rattrapage la plus précoce à partir des éléments vulnérables d'application qui appartiennent à APP-VUL. Si vous créez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

une demande de changement pour un problème critique qui nécessite une date de rattrapage antérieure, vous préférez peut-être modifier cette valeur et la valeur dans le champ Priorité.

Justification

Ce champ affiche le nombre de CI ajoutés au CHG. Si vous souhaitez ajouter des informations supplémentaires, vous préférerez peut-être modifier ce texte. Par exemple, vous préférerez peut-être ajouter une note dans ce champ sur le filtre que vous avez utilisé pour créer la nouvelle APP-VUL, par exemple, un score de risque supérieur à 75. Ce texte peut vous aider à localiser votre nouvelle demande de changement et tâche de rattrapage.

Plan d'implémentation

Ce champ affiche la solution préférée pour la vulnérabilité.

Groupe d'affectation et Affecté à

Modifiez ces champs pour modifier le groupe d'affectation ou réaffecter cette demande de changement à un utilisateur de l'un de vos groupes d'affectation.

6. Continuez à prévisualiser et modifiez les champs au besoin.
7. Pour enregistrer vos changements et rester sur cette page, dans la bannière grise en haut du formulaire, cliquez avec le bouton droit de la souris et sélectionnez **Insérer et rester**.
8. Une fois vos modifications terminées, choisissez-en une pour continuer.

Option	Description
Créer un changement	Votre demande de changement est créée et la nouvelle demande de changement s'affiche dans l'état Nouveau . En haut, des messages indiquent que la demande de changement a été créée avec succès, compte tenu du nombre d'éléments vulnérables de l'application ajoutés. Si la synchronisation de l'état est activée et que la VUL n'est pas déjà dans l'état En cours d'examen, la VUL est automatiquement déplacée dans l'état En cours d'examen et une note de travail est publiée.
Annuler	La demande de changement n'est pas créée et l'APP-VUL s'affiche.

Remarque :

Pour une tâche de rattrapage à l'état Ouvert avec le groupe d'affectation et les champs Affecté à non affecté (vide), l'utilisateur connecté actuel est automatiquement affecté à la tâche une fois que vous avez cliqué sur **Créer un changement**. En outre, la case Ajouter des CI au CR doit être cochée. En haut de la VUL, un message de confirmation bleu s'affiche qui indique cette affectation.

Que faire ensuite

Surveillez la demande de changement et les tâches de changement pour vérifier qu'elles sont terminées et que la demande de changement est implémentée. Une fois ce CHG implémenté et passé à l'état de révision , si la synchronisation d'état est activée, l'APP-VUL passe automatiquement à l'état Résolu.

Associer une tâche de rattrapage à une demande de changement existante

En tant que gestionnaire Appsec ou champion de sécurité, évitez de créer des demandes de changement en double (CHG) lorsque vous travaillez à résoudre vos tâches de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

rattrapage en associant une tâche de rattrapage (APP-VUL) à une demande de changement déjà disponible dans votre instance.

Avant de commencer
Rôles requis :

Depuis l'espace de travail du gestionnaire de vulnérabilité : sn_vul.app_sec_manager.

Depuis l'espace de travail du propriétaire ITRem : sn_vul.app_sec_champion ou sn_vul.app_developer, et rôle itil.

Pourquoi et quand exécuter cette tâche
En tant que propriétaire de rattrapage, vous pouvez associer les tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe d'affectation aux demandes de changement existantes directement à partir des enregistrements de tâche de rattrapage. L'image suivante illustre le flux de base pour associer une demande de changement à une vulnérabilité d'application (VG) existante.

Remarque : Vous pouvez associer une demande de changement existante à une APP-VUL dans n'importe quel état (Ouvert, En cours d'examen, En attente d'implémentation, Fermé et Différé). Lorsque vous associez une demande de changement à une VUL existante, seuls les VI actifs sont ajoutés à la demande de changement.

Avant de commencer, afin d'éviter de créer des demandes de changement en double, vous pouvez préférer afficher toutes les demandes de changement existantes déjà associées à APP-VUL. Pour suivre facilement le nombre de demandes de changement liées à une APP-VUL spécifique, consultez la colonne Nombre de CR sur la liste des tâches de remédiation. Si elle n'est pas affichée, cliquez sur l'icône des paramètres () en haut à droite. Déplacez la colonne Nombre de CR de Disponible à Sélectionné et cliquez sur **OK**.

Pour remplir automatiquement la nouvelle colonne, pour les clients ayant des données existantes dans cette table, exécutez le travail planifié : Remplir la nouvelle colonne Nombre de CR.

Procédure

1. Pour associer une tâche de rattrapage à une demande de changement existante, accédez à **Tous** > **Réponse aux vulnérabilités de l'application** > **Tâches de remédiation**.
2. Localisez la tâche de rattrapage avec laquelle vous travaillez.
3. **Facultatif :** Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Aperçu du rattrapage** pour afficher le tableau de bord Vue d'ensemble du rattrapage et localiser une APP-VUL qui vous est affectée ou qui est affectée à votre groupe d'affectation.
4. Dans la colonne Numéro, cliquez sur un enregistrement APP-VUL pour l'ouvrir.
   L'enregistrement APP-VUL s'affiche.
5. Une fois l'enregistrement ouvert affiché, s'il ne l'est pas déjà, accédez à la liste connexe Demandes de changement et sélectionnez-la.
   Toutes les demandes de changement associées à APP-VUL sont affichées avec le bouton **Ajouter** . Dans la figure suivante, aucune demande de changement n'est déjà associée à cette APP-VUL.
6. Pour associer l'APP-VUL à un CHG existant, cliquez sur **Ajouter**.
   Le formulaire Ajouter une demande de changement existante à une tâche de rattrapage s'affiche.
7. Dans le formulaire, cliquez sur l'icône de recherche.
   Une vue de liste des demandes de changement existantes s'affiche dans une nouvelle fenêtre, comme illustré dans la figure suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Sélectionnez un élément dans la liste affichée ou cliquez sur le filtre () et entrez des conditions pour limiter les résultats de votre recherche.
9. Pour la case à cocher Ajouter des CI au CR, choisissez-en un pour continuer.

Remarque : Cette case à cocher s'affiche uniquement pour les demandes de changement existantes dans l'état Nouveau .

Option	Description
Case à cocher Ajouter des CI au CR sélectionnée	Sélectionné par défaut. Si la case à cocher est sélectionnée, tous les éléments de configuration (CI) qui appartiennent aux éléments vulnérables actifs dans cette tâche de rattrapage sont ajoutés à cette demande de changement. Lorsque cette option est sélectionnée, l'état de la demande de changement est synchronisé avec APP-VUL. Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.
Case Ajouter des CI au CR décochée	Décochez la case si vous ne souhaitez pas que les CI des éléments vulnérables actifs de cette tâche de rattrapage soient ajoutés à la nouvelle demande de changement. Lorsqu'elle est désactivée, l'état de la demande de changement n'est pas synchronisé avec APP-VUL et l'APP-VUL reste dans son état actuel.

10. Une fois le numéro de demande de changement que vous souhaitez afficher dans le champ Rechercher une demande de changement, cliquez sur **Envoyer**.
L'APP-VUL s'affiche. En haut de l'enregistrement, le message bleu de confirmation s'affiche et indique que la demande de changement que vous avez sélectionnée est correctement associée à APP-VUL.

Remarque : Pour une APP-VUL à l'état Ouvert avec le groupe d'affectation et les champs Affecté à non affectés (vides), l'utilisateur connecté actuel est automatiquement affecté à APP-VUL après avoir cliqué sur **Ajouter**. En outre, la case Ajouter des CI au CR doit être cochée. En haut de l'APP-VUL, un message de confirmation bleu s'affiche et indique que l'utilisateur actuel est affecté.

Que faire ensuite

Examinez l'enregistrement APP-VUL. Dans la colonne Demande de changement de la liste connexe Demandes de changement, cliquez sur le lien du nouveau CHG pour afficher l'enregistrement CR. Dans l'enregistrement CHG ouvert, vous pouvez surveiller l'état de la demande de changement. Les éléments de configuration (CI) affectés et les tâches de rattrapage sont affichés dans les listes connexes CI affectés et tâches de rattrapage.

Test de pénétration

Les tests de pénétration dans Réponse aux vulnérabilités des applications permettent aux propriétaires d'applications d'évaluer la posture de sécurité de leur application. Il s'agit du test manuel d'une application par l'équipe de piratage éthique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles requis

Les tests de pénétration nécessitent les rôles suivants :

Gestionnaire de sécurité des applications : contient les gestionnaires de la sécurité et les propriétaires d'applications qui gèrent les demandes d'évaluation des tests de pénétration. Il contient les rôles granulaires suivants :

- sn_vul.app_manage_pen_test_request
- sn_vul.app_lecture_tout
- cmdb_read

Hacker éthique : contient les membres de l'équipe de piratage éthique qui effectuent des tests de pénétration des applications. Il comprend les rôles granulaires suivants :

- sn_vul.app_update_assignment_group
- sn_vul.app_update_assigned_to
- sn_vul.app_gérer_les AVIT manuels
- sn_vul.app_manage_pen_test_request_config
- itil
- sn_vul.app_lecture_tout
- sn_vul.app_manage_pen_test_request
- sn_vul.app_update_state

Pour en savoir plus sur ces rôles, reportez-vous à la section Réponse aux vulnérabilités des applications Groupes et rôles d'utilisateurs.

À partir de la version 19.0 de Réponse aux vulnérabilités, si vous utilisez le Veracode Vulnerability Integration, les tests d'évaluation de pénétration dans le Veracode Vulnerability Integration sont des conclusions manuelles de Veracode. Ils ne sont pas liés à des demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les évaluations de tests de pénétration de , reportez-vous à Veracode la Veracode Vulnerability Integration section .

Cycle de vie du test de pénétration

En tant que propriétaire d'application, vous pouvez demander à l'équipe de piratage éthique d'évaluer votre application par un test de pénétration. L'équipe de piratage éthique donne suite à cette demande et crée les conclusions du test de pénétration. Ces résultats sont des éléments vulnérables de l'application (AVI) créés manuellement.

Le workflow des tests de pénétration couvre le cycle de vie du test de pénétration, depuis le lancement de la demande de test jusqu'à la résolution des conclusions de l'équipe de piratage éthique.

Demande d'évaluation de test de pénétration

À partir de la version 19.0, vous pouvez créer de nouvelles demandes ou copier des demandes existantes sur **Tous** > **Demandes d'évaluation de test de pénétration** > **Tous**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant la version 19.0, en tant que propriétaire de l'application, vous pouviez demander une évaluation de test de pénétration pour votre application à l'aide du catalogue de services ITSM.

Examen de la demande d'évaluation du test de pénétration

L'équipe de piratage éthique examine et évalue l'application et le périmètre de la demande d'évaluation du test de pénétration, et les ajoute au backlog existant.

Préparation d'un environnement

L'équipe de piratage éthique envoie ensuite une demande au propriétaire de l'application pour qu'il lui fournisse un environnement pour commencer les tests. Une fois que l'environnement est prêt, le propriétaire de l'application informe l'équipe de piratage éthique.

Pour plus d'informations sur la configuration des demandes de test, reportez-vous à la section Configurer les tests de pénétration.

Test et rapport des conclusions du test de pénétration

L'équipe de piratage éthique teste l'application et rend compte des résultats au propriétaire de l'application. L'équipe de piratage éthique définit également les accords sur les niveaux de service (SLA) pour les conclusions du test de pénétration en utilisant la date cible de rattrapage. Ces résultats sont les AVI créés manuellement. Le propriétaire de l'application examine à son tour les AVI créés par l'équipe de piratage éthique. Ils planifient les correctifs et les affectent à l'équipe d'application.

Remarque : Les règles de cibles de rattrapage ne s'appliquent pas aux conclusions du test de pénétration.

L'équipe de piratage éthique peut créer une bibliothèque d'entrées de vulnérabilité d'application (AVE) et les réutiliser lors de la génération de rapports sur les AVI. Ils peuvent également suivre l'état des conclusions du test de pénétration.

Corriger et valider les conclusions du test de pénétration

Une fois les résultats du test de pénétration corrigés et résolus par l'équipe d'application, les correctifs sont validés manuellement et fermés par l'équipe de piratage éthique.

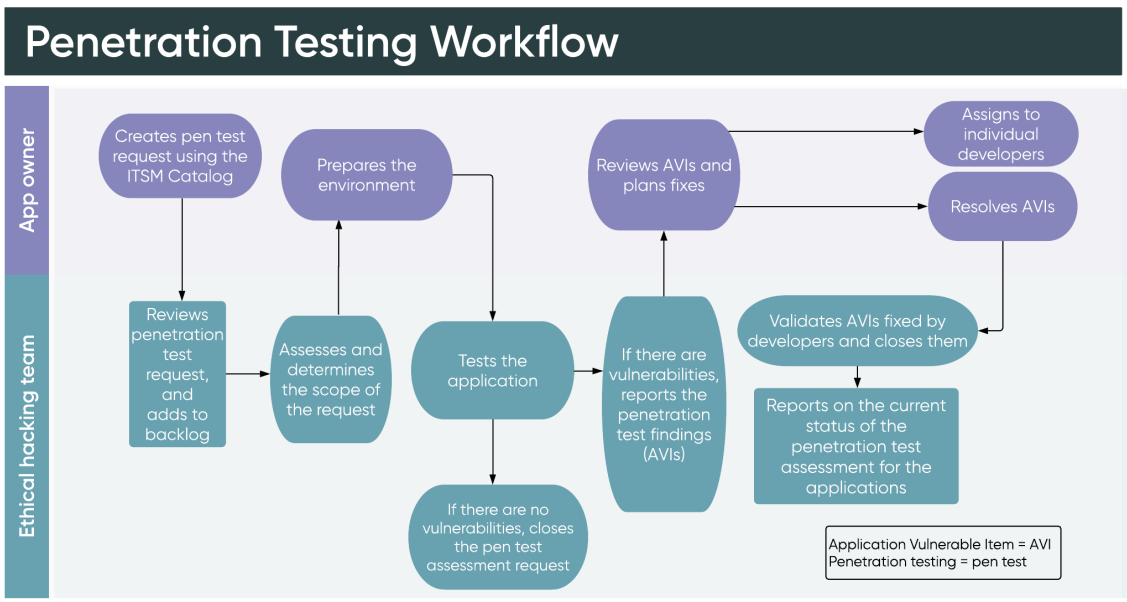
Rapports Gestion de la vulnérabilité des applications

Utilisez les rapports disponibles sur le tableau de Gestion de la vulnérabilité des applications bord PA pour suivre les conclusions du test de pénétration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cycle de vie du test de pénétration



Créer une demande d'évaluation de test de pénétration à partir de demandes existantes (v19.0)

À partir de la version 19.0, vous créez des demandes d'évaluation de test de pénétration directement à partir de la liste des demandes existantes. Vous pouvez également copier des demandes existantes à l'état Fermé sur cette liste pour créer des demandes.

Avant de commencer

Rôle requis : gestionnaire App-Sec

Pourquoi et quand exécuter cette tâche

À partir de la version 19.0 de Réponse aux vulnérabilités, si vous utilisez le Veracode Vulnerability Integration, les tests d'évaluation de pénétration dans le Veracode Vulnerability Integration sont des conclusions manuelles de Veracode. Ils ne sont pas liés à des demandes d'évaluation de test de pénétration que vous configurez dans Réponse aux vulnérabilités des applications. Pour plus d'informations sur les évaluations de tests de pénétration de , reportez-vous à Veracode la Veracode Vulnerability Integration section .

Procédure

1. Accédez à la **Tous** > **Demandes d'évaluation de test de pénétration** > **Tous**.
2. **Facultatif :** Vous pouvez également créer une demande en répliquant les demandes fermées. Toutes les valeurs de la demande d'origine sont conservées dans le nouveau formulaire. Les éléments vulnérables de l'application (AVI) actifs sont automatiquement copiés dans la nouvelle demande. Sélectionnez **Copier et créer une demande** à partir d'enregistrements à l'état Fermé.
3. Sélectionnez Nouveau et remplissez les champs.

Formulaire de demande d'évaluation de test de pénétration

Champ	Description
Numéro	Identificateur unique généré pour la demande d'évaluation de test de pénétration.
État	Sélectionnez une valeur en fonction de l'état de la demande.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Demandé par	Personne demandant l'évaluation de la demande.
Groupe d'affectation	Groupe sélectionné pour travailler sur les résultats du test de pénétration. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec. Pour configurer les groupes, reportez-vous à la section Configurer les tests de pénétration.
Application	Sélectionnez une application à l'aide de l'option de recherche.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur les résultats du test de pénétration. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec.
Type de demande	Sélectionnez une option dans : ○ Service Web (connu sous le nom d'API avant la version v16.1) ○ Application Web ○ Client lourd ○ Mobile (si vous sélectionnez **Mobile**, l'onglet Mobile s'affiche au bas du formulaire avec des champs supplémentaires)
Sprint	Affiche les sprints avec la bande passante disponible pour prendre en charge la demande d'évaluation en fonction du champ de type d'évaluation sélectionné. Consultez Configurer les sprints pour le test de pénétration et Configurer les types d'évaluation pour les tests de pénétration pour plus d'informations sur la modification de la capacité de sprint et du champ d'application du test.
v19.0 : Taille de l'application	Sélectionnez la taille de l'application que vous souhaitez tester. ○ Petit ○ Moyenne ○ Grand ○ Standard (sélectionnez cette option si vous n'êtes pas sûr de la taille) Découvrez plus Configurer les tests de pénétration d'informations sur la modification de la capacité de sprint et le périmètre de test avec la taille de l'application et la capacité de sprint.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Créées	Date et heure de création de la demande.
Type d'évaluation	Sélectionnez le type d’évaluation dans : ○ Test de pénétration complet ○ Test ciblé ○ Retester Pour plus d’informations sur les combinaisons de test et le champ d’application du test, reportez-vous à la section Configurer les types d’évaluation pour les tests de pénétration.
Mis à jour	Date et heure de la dernière mise à jour de la demande.
Date de la démo	Date à laquelle cette application peut être démontrée.
Déploiement du produit planifié le	Date planifiée de déploiement de cette application en production.
Version/mise en production de l'application planifiée pour le déploiement	Version de l’application planifiée pour le déploiement en production.
v19.0 : onglet Application appartenant à un fournisseur tiers ou à une société commune Si vous sélectionnez Oui pour ce champ, l’onglet Informations sur le fournisseur/la société commune s’affiche. Renseignez les champs supplémentaires.	
Existe-t-il une clause qui nous permet d’effectuer un test de pénétration ?	Le terme « Clause » peut faire référence à des normes de test qui incluent tout accord existant entre deux ou plusieurs parties que vous souhaitez ajouter. Si vous sélectionnez **Oui**, ajoutez la clause.
La clause citant l’autorisation d’effectuer un test de pénétration	
Nom juridique complet et adresse du fournisseur	
Système de détection des intrusions	
Contact technique du fournisseur	
Les informations enregistrées ont-elles été examinées à partir d’une activité malveillante ?	
Application hébergée par un autre fournisseur tiers ?	
Contact du fournisseur qui signera le test de pénétration	
Onglet Détails de l’application	
Objet de l'application	Description de la fonctionnalité de l’application.
Détails des piles de technologies	Pile technologique complète, du front-end au back-end, des bases de données et d’autres technologies clés.
S’agit-il d’une application tierce ?	Confirme si cette application appartient à un fournisseur tiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Types de listes de données sensibles accessibles à partir de l'application	Types de données sensibles accessibles à partir de l’application. Par exemple, les données PII, les données PHI et les données financières telles que les numéros de carte de crédit.
Type d'authentification	Spécifie si cette application utilise l’authentification LDAP, sa propre authentification native ou d’autres formes d’authentification.
L'application a-t-elle un impact sur un programme de conformité ?	Spécifie si cette application a un impact sur des programmes de conformité tels que PCI.
Contacts de l'équipe d'application	Les membres de l’équipe d’application doivent être contactés par l’équipe de piratage éthique pour toute question.
Liste des programmes de conformité	
Interfaces ou applications tierces associées	
Adresse IP	
Nombre approximatif d’utilisateurs en production ?	
Existe-t-il un script automatisé ?	
La version de production de cette application est orientée vers l’extérieur ?	
v 19.0 : Impact sur l’entreprise	
Dommage financier	Sélectionnez-en un dans la liste.
Non-conformité	Sélectionnez-en un dans la liste.
Atteinte à la réputation	Sélectionnez-en un dans la liste.
Violation de la confidentialité	Sélectionnez-en un dans la liste.
Onglet Détails du test	
URL à tester	URL qui doivent être incluses dans le test de pénétration.
URL à exclure	URL qui doivent être exclues des tests de pénétration.
Cette application a-t-elle été testée précédemment ?	Spécifie si cette application a déjà été testée de pénétration.
Motif du nouveau test	Raison de demander une réévaluation par test de pénétration si l’application a été testée plus tôt.
Quand l’application a-t-elle été testée ?	Délai du test de pénétration de l’application.
Détails du compte de test	Détails du compte de test qui peuvent être utilisés par l’équipe de piratage éthique pour les tests de pénétration.
Rôles d'application	Rôles pris en charge par l’application pour ses utilisateurs.
Rôles les plus utilisés	Rôles les plus couramment utilisés dans l’application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Onglet Commentaires supplémentaires	
Notes de travail	

4. Sélectionnez **Enregistrer** pour enregistrer vos modifications ou **Soumettre** pour lancer la demande.

Créer une demande d'évaluation de test de pénétration (avant la version 19.0)

Lancez une demande d'évaluation de test de pénétration pour vos applications Web ou API. Ces demandes sont soumises à l'équipe de piratage éthique, qui procède ensuite au test de ces applications et rapporte manuellement les résultats du test de pénétration.

Avant de commencer

Rôle requis : gestionnaire App-Sec

Pourquoi et quand exécuter cette tâche

Le propriétaire de l'application émet une demande d'évaluation de test de pénétration pour analyser manuellement son application ou ses API. L'équipe de piratage éthique teste l'application et crée manuellement les résultats du test de pénétration. Ces résultats sont des éléments vulnérables de l'application (AVI) créés manuellement.

Le groupe d'affectation par défaut pour le résultat du test de pénétration est le groupe configuré dans le champ « Équipe d'application » de la demande d'évaluation de test de pénétration associée. Le type d'affectation du résultat du test de pénétration est manuel. Les règles d'affectation ne peuvent pas remplacer l'affectation de ces conclusions du test de pénétration.

À partir de la version 19.0, vous pouvez créer des demandes d'évaluation de test de pénétration directement à partir de la table Demandes d'évaluation de test de pénétration [sn_vul_pen_test_assessment_request_list]. Consultez Créer une demande d'évaluation de test de pénétration à partir de demandes existantes (v19.0) pour plus d'informations.

Procédure

1. Avant la version 19.0, accédez à **Tous** > **Libre-service** > **Catalogue de services** > **Services** > **Demande d'évaluation de test de pénétration**.
2. **Facultatif :** Vous pouvez également créer une demande en répliquant les demandes fermées. Toutes les valeurs de la demande d'origine sont conservées. Les éléments vulnérables de l'application (AVI) actifs sont automatiquement copiés dans la nouvelle demande.
3. Remplissez les champs du formulaire.

Formulaire de demande d'évaluation de test de pénétration

Champ	Description
Numéro	Identificateur unique généré pour la demande d'évaluation de test de pénétration.
Demandé par	Personne demandant l'évaluation de la demande.
Demande d'évaluation parente	Demande d'évaluation de test de pénétration d'origine utilisée pour créer la demande enfant. Il est créé à l'aide d'une demande d'évaluation fermée. Visible uniquement sur le formulaire de demande d'évaluation de l'enfant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Sélectionnez une application à l'aide de l'option de recherche.
Type de demande	Sélectionnez une option dans : ○ Service Web (connu sous le nom d'API avant la version v16.1) ○ Application Web ○ Client lourd ○ Mobile (si vous sélectionnez Mobile, l'onglet Mobile s'affiche au bas du formulaire avec des champs supplémentaires)
v19.0 : Taille de l'application	Sélectionnez la taille de l'application que vous souhaitez tester. ○ Petit ○ Moyenne ○ Grand ○ Standard (sélectionnez cette option si vous n'êtes pas sûr de la taille)
Type d'évaluation	Sélectionnez le type d'évaluation dans : ○ Test de pénétration complet ○ Test ciblé ○ Retester Pour plus de détails, voir Configurer les types d'évaluation pour les tests de pénétration.
Objet de l'application	Description de la fonctionnalité de l'application.
Détails des piles de technologies	Pile technologique complète, du front-end au back-end, en passant par les bases de données et autres technologies clés.
S'agit-il d'une application tierce ?	Confirme si cette application appartient à un fournisseur tiers.
Types de listes de données sensibles accessibles à partir de l'application	Types de données sensibles accessibles à partir de l'application. Par exemple, les données PII, les données PHI et les données financières telles que les numéros de carte de crédit.
Type d'authentification	Spécifie si cette application utilise l'authentification LDAP, sa propre authentification native ou d'autres formes d'authentification.
L'application a-t-elle un impact sur un programme de conformité ?	Spécifie si cette application a un impact sur des programmes de conformité tels que PCI.
Contacts de l'équipe d'application	Les membres de l'équipe d'application doivent être contactés par l'équipe de piratage éthique pour toute question.
Date de la démo	Date à laquelle cette application peut être démontrée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Déploiement du produit planifié le	Date planifiée de déploiement de cette application en production.
Version/mise en production de l'application planifiée pour le déploiement	Version de l'application planifiée pour le déploiement en production.
v19.0 : application appartenant à un fournisseur tiers ou à une société commune	Si vous sélectionnez Oui pour ce champ, l'onglet Informations sur le fournisseur/la société commune s'affiche avec des champs supplémentaires. Le terme « clause » peut faire référence à des normes de test qui incluent tout accord existant entre deux ou plusieurs parties.
État	Sélectionnez une valeur en fonction de l'état de la demande.
Groupe d'affectation	Groupe sélectionné pour travailler sur les résultats du test de pénétration. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur les résultats du test de pénétration. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec.
Sprint	Affiche les sprints avec la bande passante disponible pour prendre en charge la demande d'évaluation en fonction du champ de type d'évaluation sélectionné.
Créées	Date et heure de création de la demande.
Date de début du test	Date et heure de début du test.
Mis à jour	Date et heure de la dernière mise à jour de la demande.
Détails du test	
URL à tester	URL qui doivent être incluses dans le test de pénétration.
URL à exclure	URL qui doivent être exclues des tests de pénétration.
Cette application a-t-elle été testée précédemment ?	Spécifie si cette application a déjà été testée de pénétration.
Motif du nouveau test	Raison de demander une réévaluation par test de pénétration si l'application a été testée plus tôt.
Quand l'application a-t-elle été testée ?	Délai du test de pénétration de l'application.
Détails du compte de test	Détails du compte de test qui peuvent être utilisés par l'équipe de piratage éthique pour les tests de pénétration.
Rôles d'application	Rôles pris en charge par l'application pour ses utilisateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Rôles les plus utilisés	Rôles les plus couramment utilisés dans l'application.

4. Sélectionnez **Soumettre**.
   Une notification par e-mail est envoyée à l'équipe de piratage éthique indiquant que la demande a été créée pour l'application concernée.

Répliquer une demande de test de pénétration à l'état Fermé

Créez une demande d'évaluation de test de pénétration en répliquant une demande à l'état Fermé. Les éléments vulnérables de l'application (AVI) actifs sont copiés dans la nouvelle demande.

Avant de commencer
Rôle requis : équipe d'application

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Demandes d'évaluation de test de pénétration** > **Tous**.
2. Sélectionnez une demande à l'état Fermé.
3. Sélectionnez **Copier et Créer une demande**.
   Une nouvelle demande est créée et les AVI actifs sont copiés dans cette demande avec les données mises à jour. Pour afficher l'état d'origine des AVI à partir de la demande parente, accédez à l'onglet **Instantané des conclusions du test de pénétration** .

Créer des résultats de tests de pénétration basés sur les demandes d'évaluation (avant la version 19.0)

Créez les conclusions du test de pénétration en fonction de la demande d'évaluation du test de pénétration. Ces résultats sont des éléments de vulnérabilité de l'application (AVI) créés manuellement.

Avant de commencer
Rôle requis : Hacker éthique

Procédure

1. Accédez à la **Tous** > **Libre-service** > **Catalogue de services** > **Services** > **Demandes d'évaluation de test de pénétration**.
2. Pour créer un AVI pour une demande d'évaluation de test de pénétration, sélectionnez la demande pertinente.
3. Dans la section Éléments vulnérables de l'application, sélectionnez **Nouveau**.
4. Remplissez les champs du formulaire.

Formulaire d'élément vulnérable d'application (vue de test de pénétration)

Champ	Description
Numéro	Identificateur AVI généré automatiquement pour cet enregistrement.
Demande d'évaluation	Demande d'évaluation de test de pénétration à laquelle cet AVI est associé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Vulnérabilité	Vulnérabilité sélectionnée dans la table Entrées de vulnérabilité à l'aide de l'option de recherche.
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour plus d'informations sur les évaluations de risque, reportez-vous à Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications. À partir de la version 16.1, la valeur par défaut est la même que la gravité de la vulnérabilité.
Impacte un programme de conformité ?	Confirme s'il y a un impact sur un programme de conformité. Les choix sont Oui et Non.
Liste des programmes de conformité impactés	Ce champ s'affiche lorsque la valeur du champ « Impacte tout programme de conformité » est définie sur `Yes`. Répertorie les programmes de conformité impactés.
Publication/version fixe planifiée	Publication avant le moment où les conclusions du test de pénétration doivent être résolues.
État	La valeur par défaut est **Ouvert** lorsque l'AVI est créé. Consultez États des éléments vulnérables de l'application (AVI) pour plus d'informations sur la façon dont les états sont mappés.
Groupe d'affectation	Groupe sélectionné pour travailler sur cet AVI. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cet AVI. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec.
Cible de remédiation	Date à laquelle les AVI doivent être corrigés, dès lors qu'ils ont été identifiés pour la première fois. Ce champ s'affiche uniquement le cas échéant. Pour plus d'informations sur les cibles de rattrapage, reportez-vous à la section Automatiser le suivi de la cible de rattrapage dans Réponse aux vulnérabilités des applications.
Créées	Horodatage de création de l'élément vulnérable de l'application (AVI).
Mis à jour	Horodatage de la mise à jour de l'élément vulnérable de l'application (AVI).
Ouvert par	Utilisateur qui a créé ce résultat du test de pénétration.
Contact de l'équipe de sécurité	Point de contact dans l'équipe de piratage éthique.
Description brève	Brève explication des conclusions du test de pénétration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Détails	
Détails techniques	Détails techniques du résultat du test de pénétration.
Impact	Évaluation de l'impact du résultat du test de pénétration.
Étapes à reproduire	Documentez les étapes de reproduction et d'examen des résultats du test de pénétration.
Recommandation	Enregistrez les actions recommandées dans ce champ.
Notes	
Notes de travail	Ajoutez des notes pour communiquer des informations sur les transitions d'états et d'autres mises à jour de champs.
V16.1 : URL affectées	Plus d'informations relatives aux URL affectées.
V16.1 : Paramètres affectés	Informations supplémentaires relatives aux paramètres affectés.
V16.1 : Fonctionnalités affectées	Autres informations relatives aux fonctionnalités affectées.

5. Pour enregistrer le formulaire, sélectionnez **Soumettre**.

Créer une entrée de vulnérabilité de l'application

Créez une entrée de vulnérabilité de l'application pour la vulnérabilité spécifiée pour le résultat du test de pénétration. Les vulnérabilités d'application sont des vulnérabilités sur les applications logicielles personnalisées.

Avant de commencer

Rôle requis : Hacker éthique

Pourquoi et quand exécuter cette tâche

Réponse aux vulnérabilités des applications associe une vulnérabilité à une application pour créer le résultat du test de pénétration. Ces résultats sont des éléments vulnérables de l'application (AVI) créés manuellement. Vous pouvez réutiliser une entrée existante ou en créer une manuellement pour chaque vulnérabilité pendant le test de pénétration.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Bibliothèques** > **Tiers**.
2. Sur la page Entrées de vulnérabilité de l'application, sélectionnez **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire d'entrée de vulnérabilité de l'application (vue de test de pénétration)

Champ	Description
ID	Identificateur de cette entrée de vulnérabilité.
Gravité	Degré de gravité normalisé de cette vulnérabilité. Les cartes de gravité sont fournies pour NVD et avec les intégrations tierces ServiceNow. Pour plus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'informations sur la création ou l'ajustement de cartes de gravité, reportez-vous à la section Mapper automatiquement la gravité d'un élément vulnérable d'application.
CVE primaire	Référence à l'élément Common Weakness Enumeration dans lequel cette vulnérabilité s'intègre le mieux.
Nom de catégorie	Classification fournie par l'intégration tierce. Aide à la tâche.
Détails des vulnérabilités	
Vecteur d'attaque	Vecteur d'attaque le plus vulnérable pour cette vulnérabilité.
Complexité de l'attaque	Mesure qui décrit les conditions indépendantes de la volonté de l'attaquant qui doivent exister pour exploiter la vulnérabilité.
Champ d'application	Mesure permettant de mesurer la capacité d'une vulnérabilité logicielle à avoir un impact sur les ressources au-delà de ses moyens.
Intégrité	Mesure permettant de mesurer l'impact sur l'intégrité d'une vulnérabilité exploitée avec succès.
Vecteur CVSS	Cadre de travail ouvert pour capturer les caractéristiques et la gravité des vulnérabilités logicielles.
Privilèges requis	Niveau de privilèges qu'un attaquant doit posséder avant d'exploiter avec succès la vulnérabilité.
Interaction de l'utilisateur	Condition d'interaction humaine pour exploiter avec succès une vulnérabilité.
Confidentialité	Impact sur la confidentialité des ressources d'informations en raison d'une vulnérabilité exploitée avec succès. Ces ressources sont gérées par un composant logiciel.
Disponibilité	Impact sur la disponibilité du composant impacté résultant d'une vulnérabilité exploitée avec succès.
Score de base CVSS	Représentation numérique (0-10) de la gravité d'une entrée de vulnérabilité d'application.
Menace	Description de la menace que représente cette vulnérabilité.
Description de l'atténuation	Description des étapes visant à atténuer la vulnérabilité.

4. Pour enregistrer le formulaire, sélectionnez **Soumettre**.

Remarque : Les AVE sont créés dans la table Entrée de vulnérabilité de l'application (sn_vul_app_vul_entry). La table Entrée de vulnérabilité de l'application est un enfant de la table Entrée de vulnérabilité (`sn_vul_entry`). Par conséquent, les AVE créés sont également ajoutés à la table Entrée de vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Espace de travail Test de pénétration

L'espace de travail des tests de pénétration dans Application Vulnerability Response aide les clients à demander une demande d'évaluation de test de pénétration et à la suivre à l'aide du workflow. Elle permet aux propriétaires d'applications d'évaluer la posture de sécurité de leur application. Il s'agit du test manuel d'une application par l'équipe de piratage éthique.

Rôles requis

Les tests de pénétration nécessitent les rôles suivants :

sn_vul.app_pen_tester : Représente un testeur d'intrusion qui est responsable de créer les conclusions du test d'intrusion dans le cadre du test d'intrusion de l'application.

sn_vul.app_pen_test_requester : sélectionner l'enregistrement pour l'action : sn_vul.app_pen_test_requester.

Cycle de vie des tests de pénétration

En tant que propriétaire d'application, vous pouvez demander à l'équipe de piratage éthique d'évaluer votre application par un test de pénétration. L'équipe de piratage éthique donne suite à cette demande et crée les conclusions du test de pénétration. Ces résultats sont des éléments vulnérables de l'application (AVI) créés manuellement.

Le workflow des tests de pénétration couvre le cycle de vie du test de pénétration, depuis le lancement de la demande de test jusqu'à la résolution des conclusions de l'équipe de piratage éthique.

Créer une nouvelle demande d'évaluation de test de pénétration

Lancez une demande d'évaluation de test de pénétration pour vos applications Web, applications mobiles ou API. Ces demandes sont soumises à l'équipe de piratage éthique, qui procède ensuite au test de ces applications et rapporte manuellement les résultats du test de pénétration.

Avant de commencer
Rôle requis : gestionnaire App-Sec

Procédure

1. Accédez à la **Espace de travail Test de pénétration**.
2. Sur le formulaire **de demande d'évaluation de test d'intégration** , renseignez les champs.
3. Sélectionnez **Soumettre**.
   Une notification par e-mail est envoyée à l'équipe de piratage éthique indiquant que la demande a été créée pour l'application concernée.
4. Une fois le formulaire soumis, l'équipe de piratage éthique peut **commencer à définir le champ d'application**.
5. Après la définition du champ d'application, le propriétaire de l'application prépare l'environnement de tests et l'équipe de piratage éthique peut **commencer les tests**.
6. Si vous devez vérifier les détails de la demande, vous pouvez marquer la phase de test en suspens en sélectionnant le bouton **Mettre en attente** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Une fois le test terminé, vous pouvez afficher les AVIT sous l'onglet Résultats du test de pénétration.

Remarque : Vous pouvez dupliquer une demande à partir d'une demande existante. Une fois dupliqués, les AVIT joints à la demande parente sont déplacés (et non copiés) vers la demande dupliquée.

Créer les conclusions d'un test de pénétration basés sur un questionnaire d'évaluation

Créer les conclusions du test de pénétration en alignant les tests sur les normes reconnues du questionnaire MASVS dans le workflow des tests de pénétration. Ces résultats sont des éléments de vulnérabilité d'application (AVI) créés manuellement.

Avant de commencer
Rôle requis : Gestionnaire App-sec

Procédure

1. Accédez à la **Conclusions du test de pénétration** onglet.
2. Sélectionnez le questionnaire publié en fonction de votre application.
3. Examinez les tests et marquez la phase de test comme terminée.
4. Une fois l'étape ci-dessus terminée, fermez la demande.

Remarque : Les étapes précédentes peuvent être effectuées par un membre de l'équipe de piratage éthique.

Publier le questionnaire d'évaluation

Pour tester une application mobile, il existe certaines normes développées par la communauté OAS pour aider les testeurs à identifier les bogues dans leurs produits. Accédez à l'espace de travail d'évaluation pour créer le questionnaire de votre choix. Publiez-les pour pouvoir les afficher dans le formulaire de demande d'évaluation.

Avant de commencer
Rôle requis : sn_vul.app_pen_test_requester

Rôles requis pour le test de pénétration Demandeur et Testeur :

sn_vul.app_manage_pen_test_request :

contient : sn_smart_asmt.assessment_reader sn_smart_asmt :assessment_admin sn_smart_asmt.actor.

sn_vul.app_pen_tester

contient : sn_smart_asmt.assessment_reader sn_smart_asmt :actor.

Remarque : Dans le cadre de la fonctionnalité du moteur d'évaluation intelligent, nous avons ajouté les rôles ci-dessus. Ces rôles sont essentiels pour que le demandeur et le testeur de test de pénétration puissent afficher et soumettre les questionnaires.

Procédure

1. Accédez à la **Espace de travail d'évaluation**.
2. Chaque questionnaire contient des lignes directrices. Examinez les questionnaires et, si nécessaire, modifiez-les pour répondre aux besoins de votre organisation en matière de tests, après quoi vous pourrez terminer les tests.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le questionnaire suit par défaut les normes MASVS. Pour plus d'informations, visitez :

3. Publiez les questionnaires et sélectionnez le questionnaire publié dans la liste sous la section Détails du test du formulaire de demande d'évaluation de test d'intégration.

   Remarque : Publiez le questionnaire pour pouvoir l'afficher sur le formulaire Demande d'évaluation de test de pénétration.

4. Le profil qui effectue le test peut alors marquer les tests comme réussis, échoués ou non applicables sous l'onglet Évaluation du formulaire de demande de test de pénétration.

Utiliser un questionnaire d'évaluation

Après la création du questionnaire d'évaluation, vous pouvez utiliser ces questionnaires à des fins de test.

Avant de commencer
Rôle requis : sn_vul.app_pen_tester

Procédure

1. Accédez à la **Demande de test de pénétration** forme.
2. Suivez les directives mentionnées sur le formulaire.
3. Sélectionnez une **demande de test de pénétration**.
4. Accédez à **l'onglet Évaluation**.
5. Ouvrez l'onglet, répondez au questionnaire et **soumettez**.

   Remarque : Le profil affecté à la demande de test de pénétration peut l'envoyer.

Tableau de bord des tests de pénétration

Obtenez une vue d'ensemble de vos demandes de test de pénétration et des résultats manuels sur votre tableau de bord de test de pénétration personnel. Vous pouvez afficher la progression de votre équipe dans l'espace de travail du test de pénétration. Le tableau de bord vous fournit une vue d'ensemble des résultats du test de pénétration, affichez et hiérarchisez les tests qui requièrent votre attention, suivez les résultats des tests et affichez les affectations.

Le responsable des tests d'intrusion / responsable de l'équipe de piratage éthique peut identifier et analyser les mesures clés, telles que la surveillance des demandes de test de pénétration, et afficher la progression globale de son équipe dans l'espace de travail du test de pénétration. Le responsable du test d'intrusion / responsable de l'équipe de piratage éthique peut également visualiser les informations suivantes :

- Vue d'ensemble des résultats manuels classés par état et par type d'évaluation pour éclairer la prise de décision stratégique.
- Répartition des tests de pénétration affectés entre les personnes pour une meilleure planification de la capacité
- Classez les conclusions en retard par ordre de priorité en fonction de leur progression afin d'améliorer l'efficacité de la résolution.
- Comprendre le paysage des résultats des tests d'intrusion basés sur la distribution critique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants du tableau de bord de pénétration

Analysez visuellement les progrès et les données de votre équipe et favorisez les résultats commerciaux à l'aide des composants de votre tableau de bord personnel.

Indicateurs d'éléments importants

Affichez la mise en production d'urgence non affectée, les tests ayant une date de vue d'ensemble antérieure, les tests non affectés et toute validation critique en attente.

- **Mise en production d'urgence non affectée** : indique le nombre total de demandes de test de pénétration non affectées pour le type d'évaluation « Mise en production d'urgence ».
- **Tests en retard** : indique le nombre total de tests après la date d'échéance.
- **Tests non affectés** : indique le nombre total de tests non affectés à l'équipe.
- **En attente de validation critique** : indique le nombre total d'AVIT pour toutes les demandes ayant l'état « En attente de validation ».

Remarque : Sélectionnez chaque tuile pour afficher la liste des éléments et effectuer les tâches requises.

Demandes de test de pénétration

Affichez les demandes de test par état, les tests en retard et les tests par approbations de mise en production.

- **Demandes de test par état** : indique le nombre de demandes de test dans ces différents états du cycle de test de pénétration. Vous pouvez afficher et accéder à la liste des demandes de test dans différents états en cliquant sur chaque vignette colorée. Vous pouvez également afficher l'état de ces tests pour les six mois suivants en sélectionnant le mois dans la liste déroulante de filtres située en haut à droite de l'onglet. Les différents états de la demande de test sont les suivants :
  - Ouvert : nombre de demandes de test ouvertes.
  - Définition du champ d'application en cours :
  - Définition du champ d'application terminée :
  - Préparation de l'environnement :
  - Environnement prêt pour le test :
  - Test en cours :
  - Test de pénétration complet :
  - Programmes de bug bounty : incitent les pirates éthiques à trouver et à signaler les vulnérabilités de sécurité.
  - Test ciblé :
  - Intérêt de la direction : Rendre compte de l'engagement et du soutien de la haute direction à l'égard des projets essentiels au sein de l'organisation.
  - Examens ponctuels : évaluez des projets spécifiques en dehors des cycles de développement et de publication réguliers pour évaluer les performances et mettre en œuvre des améliorations.
  - Mise en production d'urgence : prend en charge les mises en production d'urgence requises pour les mises à jour logicielles rapides afin de résoudre des problèmes critiques tels que les vulnérabilités de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Tests en retard :** indique le test en attente à partir d'une certaine période. Vous pouvez sélectionner la chronologie pour laquelle vous souhaitez afficher les tests à échéance. Les options déroulantes sont les suivantes : **Échu hier**, **Échu cette semaine**, **Échu la semaine dernière**, **Échu le mois dernier** et **Échu avant le mois dernier**.
- **Tests par approbations de mise en production** : indique les états d'approbation des tests terminés prêts à être mis en production. Vérifie également que toutes les vérifications nécessaires sont effectuées avant de déployer de nouveaux logiciels. Vous pouvez également afficher l'état de ces tests pour les six mois suivants en sélectionnant le mois dans la liste déroulante de filtres située en haut à droite de l'onglet.

Conclusions

Indique le nombre de conclusions de test de pénétration ouvert (AVIT) rapportées ainsi que le nombre d'AVIT en attente de validation. Vous pouvez afficher et accéder à la liste des résultats dans différents états en sélectionnant chaque vignette colorée. Les données suivantes peuvent être affichées dans cette section :

- **Conclusions ouvertes (AVIT) par cote de risque**
- **En attente de validation des conclusions (AVIT)**

Vue d'ensemble de l'équipe

Indique les tests affectés aux membres de l'équipe pour la période de six mois suivante. Les différents états sont les suivants :

- **Définition du champ d'application en cours**
- **Ouvert**
- **Définition du champ d'application terminée**
- **Environnement prêt pour le test**
- **Test en cours d'exécution**
- **Préparation de l'environnement**

Platform Analytics et Reporting pour Réponse aux vulnérabilités des applications

Platform Analytics et Reporting contiennent du contenu préemballé Platform Analytics à utiliser avec d'autres ServiceNow AI Platform produits. Cela Solution d'analyse des performances et génération de rapports présente des mesures importantes pour analyser votre processus de gestion de la vulnérabilité des applications.

Vue d'ensemble

Le pack de contenu Performance Analytics pour Vulnerability Response est disponible sous forme d'abonnement ServiceNow® Store distinct. L'application n'est pas automatiquement installée avec l'application Vulnerability Response. Le pack de contenu Application Vulnerability Response fait partie du pack de contenu Performance Analytics pour Vulnerability Response.

Pour plus d'informations sur l'installation, l'installation et la configuration de votre application Performance Analytics pour Vulnerability Response, voir Installer et configurer l'application Performance Analytics pour Vulnerability Response [PA].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Termes clés

Analyse des performances (PA)

Solution qui crée des tableaux de bord de gestion, des rapports sur les KPI et les mesures, et répond aux questions commerciales clés pour aider à améliorer la qualité et à réduire les coûts.

Élément vulnérable de l'application (AVI)

Une vulnérabilité de l'application signalée par un scanner de vulnérabilité tiers présent sur un élément de configuration (CI).

Indicateur PA

Définit une mesure de performance effectuée à intervalles réguliers d'une activité ou d'un comportement organisationnel, par exemple, 10 principales applications comportant les éléments vulnérables les plus critiques.

Source de l'indicateur PA

Ensembles de données qui filtrent les enregistrements d'une vue de table ou de base de données, par exemple, AVI actif.

- Le tableau de bord Mes vulnérabilités d'application suit le volume, les performances et la progression des vulnérabilités d'application, de l'analyse/détection initiale au confinement ou à la correction.
- Consultez les taux de réalisation des objectifs de rattrapage et déterminez efficacement quels éléments vulnérables de l'application (AVI) présentent le plus de risque pour votre organisation.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur ServiceNow AI Platform (admin) : installer et activer cette solution d'analyse et de génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Administrateur Analyse des performances (pa_admin) : passer en revue les indicateurs, les répartitions, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.

Les tableaux de bord suivants fournissent une vue graphique de l'activité AVI pour aider à déterminer les plans de rattrapage et la progression de l'état. Vous pouvez vous concentrer sur les KPI associés aux applications critiques affectées et aux vulnérabilités à haute visibilité.

- Le tableau de bord Gestion de la vulnérabilité des applications (PA) communique les KPI pour le risque et la prévalence de la vulnérabilité, les applications affectées, les tendances de rattrapage et la progression du rattrapage. La valeur par défaut des tendances est de trois mois, mais peut être changée en 7 jours, un mois, 3 mois, 6 mois, Cumul annuel, 1 année ou Tout.
- Le tableau de bord Mes vulnérabilités d'application suit le volume, les performances et la progression des vulnérabilités d'application, de l'analyse/détection initiale au confinement ou à la correction.

Remarque : Le tableau de bord Mes vulnérabilités d'applications est un sous-ensemble du tableau de bord de vue d'ensemble et n'est disponible que lorsqu'un membre du groupe d'utilisateurs Champion de sécurité se connecte à une instance. Pour plus d'informations sur le tableau de bord Mes vulnérabilités d'application, consultez Tableau de bord Mes vulnérabilités d'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion de la vulnérabilité des applications Tableau de bord (PA)

Suivez le volume, les performances et la progression des vulnérabilités des applications, de l'analyse initiale et de la détection au confinement ou à la correction.

Cas d'utilisation

Utilisateur	Utilisation du tableau de bord
Responsables des vulnérabilités	À l'aide du tableau de bord, la gestion des vulnérabilités peut déterminer quels éléments vulnérables de l'application Gestion de la vulnérabilité des applications (AVI) présentent le plus de risque pour leurs organisations. Ces tableaux de bord fournissent une vue graphique de l'activité AVI pour les aider à déterminer les plans de rattrapage et la progression de l'état. Concentrez-vous sur les KPI associés aux applications affectées critiques et aux vulnérabilités à haute visibilité.

Onglets Rôles, Configuration et Tableau de bord requis ServiceNow AI Platform

Le tableau de bord Gestion de la vulnérabilité des applications (PA) est inclus dans le pack de contenu Performance Analytics pour Vulnerability Response. Le pack de contenu Performance Analytics pour Vulnerability Response n'est pas automatiquement installé avec l'application Réponse aux vulnérabilités . Il est disponible sous forme d'abonnement ServiceNow® Store séparé.

Pour plus d'informations sur l'installation, l'installation et la configuration de votre application Performance Analytics pour Vulnerability Response, voir Installer et configurer l'application Performance Analytics pour Vulnerability Response [PA].

Pour afficher le tableau de bord, en tant qu'utilisateur affecté à des groupes d'utilisateurs Champion de sécurité, Gestionnaire de sécurité des applications ou Développeur, accédez à **Réponse aux vulnérabilités de l'application** > **Vue d'ensemble**.

Remarque : Le tableau de bord Mes vulnérabilités d'applications est un sous-ensemble du tableau de bord de vue d'ensemble et n'est disponible que lorsqu'un membre du groupe d'utilisateurs Champion de sécurité se connecte à une instance. Pour en savoir plus sur le tableau de bord Mes vulnérabilités d'application, reportez-vous à la section Tableau de bord Mes vulnérabilités d'applications.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités des applications bord peut également être affiché dans la nouvelle interface utilisateur. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône**Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Page Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités et Page Tableaux de bord dans Espace de travail de remédiation IT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le tableau de bord de vue d'ensemble communique les KPI pour le risque et la prévalence de la vulnérabilité, les applications affectées, les tendances de rattrapage et la progression du rattrapage. La valeur par défaut des tendances est de trois mois, mais peut être changée en 7 jours, un mois, 3 mois, 6 mois, Cumul annuel, 1 année ou Tout.

Répartissez les données du Gestion de la vulnérabilité des applications tableau de bord par **type d'analyse**, **application** ou **unité business**. Chacun de ces choix dispose d'un filtre supplémentaire, **Sélectionner des éléments**, pour affiner vos sélections. À partir de la Réponse aux vulnérabilités des applications version 15.0, les applications d'entreprise et CI ont été ajoutées aux choix pour le filtre **d'application** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

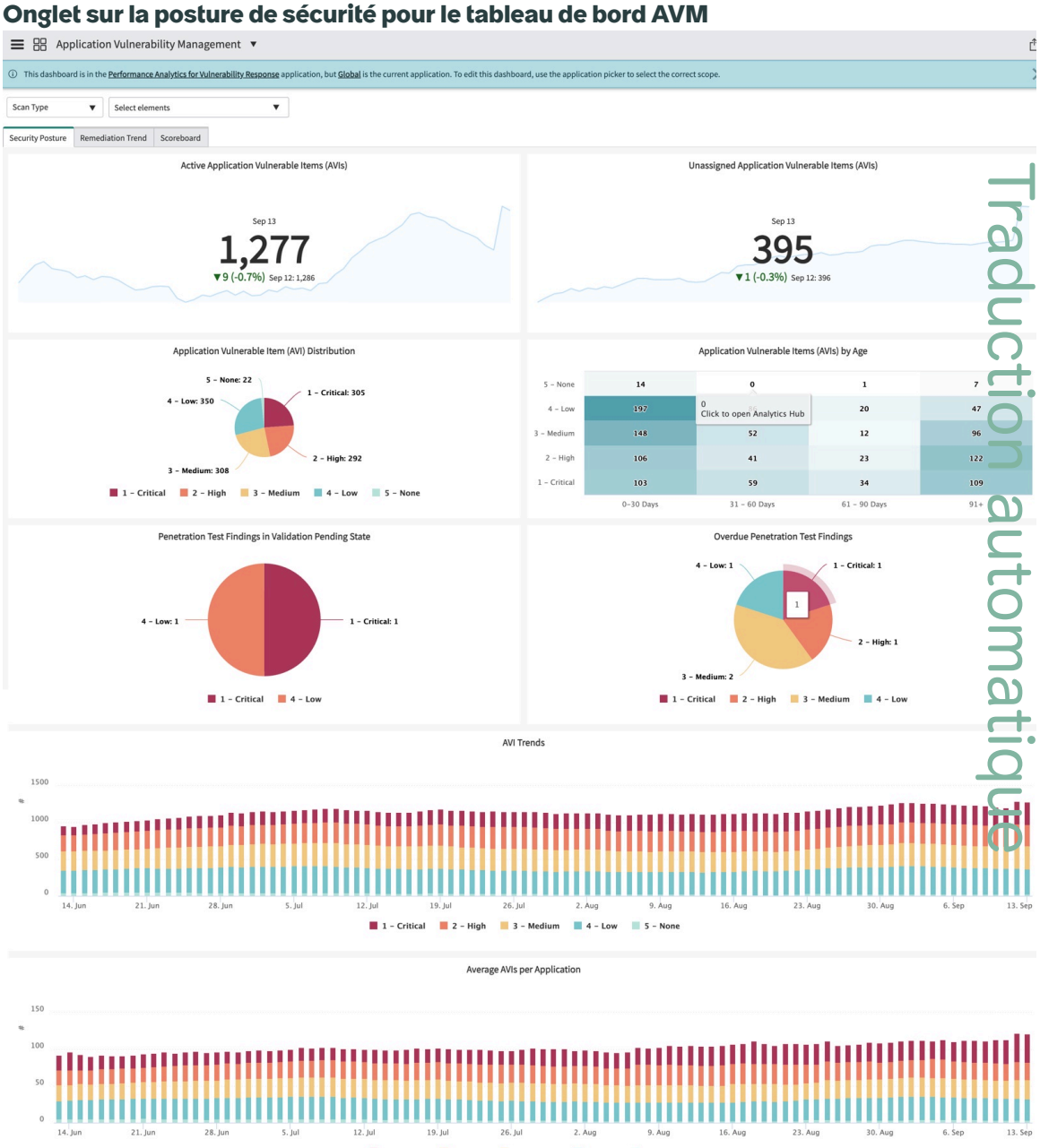
Onglet Posture de sécurité

L'onglet Posture de sécurité vous aide à comprendre votre posture de sécurité et la progression de vos actions de correction.

À partir de la version 15.0, vous pouvez afficher les rapports de conclusions du test de Réponse aux vulnérabilités des applications pénétration. Les conclusions du test de pénétration sont des éléments vulnérables de l'application (AVI) créés manuellement en fonction des demandes d'évaluation du test de pénétration.

Remarque : Le type d'analyse pour ces widgets est manuel.

Onglet sur la posture de sécurité pour le tableau de bord AVM



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

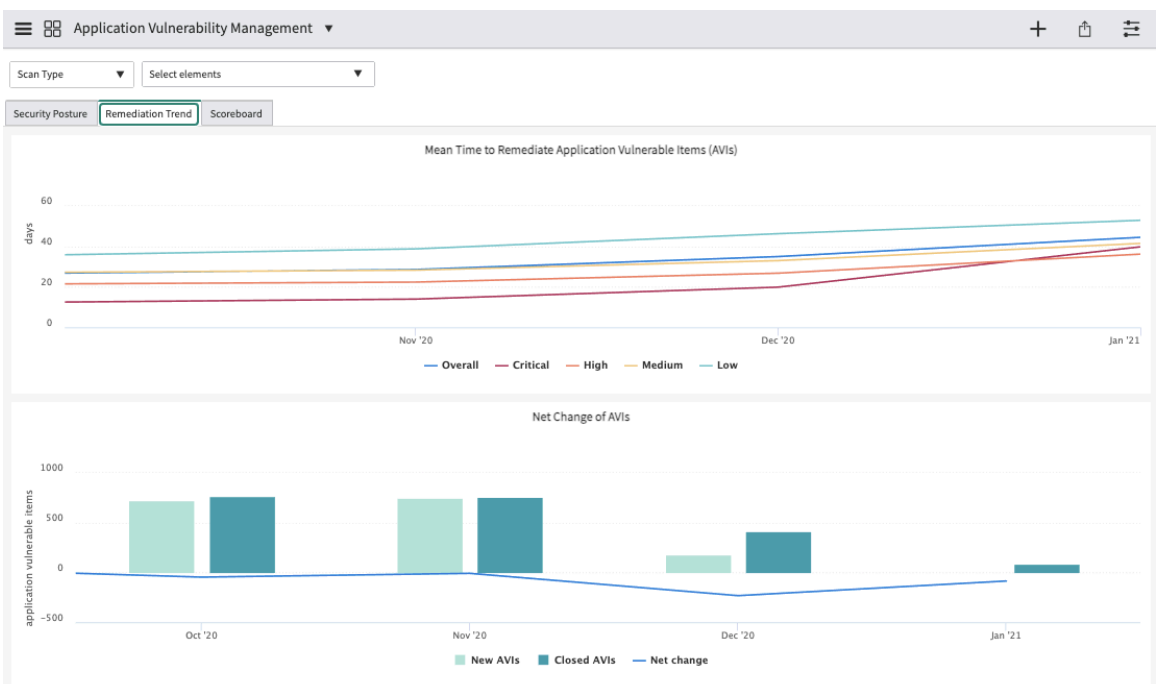
Onglet Exceptions

Ce tableau de bord vous aide à comprendre où votre organisation prend des risques en raison de reports potentiellement excessifs et à reconsidérer les options de rattrapage.

Vous pouvez afficher les éléments vulnérables d'application différés par motif, les demandes de report arrivant à expiration pour les AVI, les exceptions pour les éléments vulnérables critiques de l'application par groupe d'affectation, les demandes d'exception AVI par demandeur.

Onglet Tendance de rattrapage

L'onglet Tendance de rattrapage vous aide à comprendre la progression de vos actions de rattrapage.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

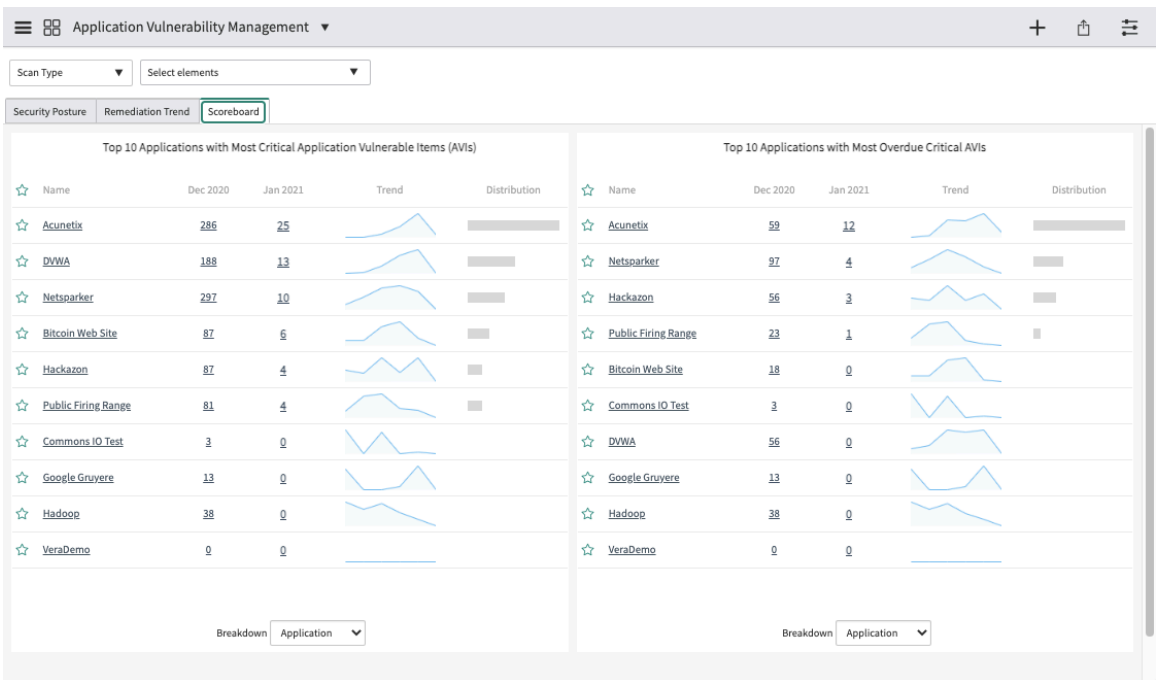
Onglet Tableau d'affichage

L'onglet Tableau d'affichage vous aide à comprendre la progression de vos actions de rattrapage et à identifier les AVI qui ont le plus besoin d'aide pour les mener à bien.

Éléments de type d'analyse :

- Dynamique : utiliser uniquement les mesures d'importation de données dynamiques
- Statique : utiliser uniquement les mesures d'importation de données statiques

Vous pouvez choisir l'un ou l'autre ou les deux.



Indicateurs

Délai moyen de remédiation des AVI bas

[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 4 - faible]]/[[Éléments vulnérables de l'application fermée > cote de risque = 4 - faible]]. L'objectif est de minimiser.

Versions de l'application

Il s'agit du nombre distinct sur les applications d'AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables de l'application

Il s'agit du nombre d'éléments vulnérables de l'application AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Nombre moyen d'AVI par application

[Éléments vulnérables de l'application actifs]] / [[Versions de l'application]]. L'objectif est de minimiser.

VI non affectés

Il s'agit du décompte sur la source de l'indicateur AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Délai moyen de rattrapage des AVI

[[Durée cumulée des éléments vulnérables de l'application fermée]] / [[Éléments vulnérables de l'application fermée]]. L'objectif est de minimiser.

Délai moyen de remédiation des AVI élevés

[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 2 - élevé]]/[[Éléments vulnérables de l'application fermée > cote de risque = 2 - élevé]]. L'objectif est de minimiser.

Éléments vulnérables d'application clôturés

Il s'agit du décompte sur la source de l'indicateur AVI. Fermé, qui utilise la table : sn_vul_app_vulnerable_item. L'objectif est de maximiser.

Délai moyen de rattrapage des AVI critiques

[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 1 - critique]]/[[Éléments vulnérables de l'application fermée > cote de risque = 1 - critique]]. L'objectif est de minimiser.

Nouveaux éléments vulnérables de l'application

Il s'agit du décompte sur la source de l'indicateur AVI. Nouveau, qui utilise la table : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Délai moyen de remédiation des AVI moyens

[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 3 - moyen]]/[[Éléments vulnérables de l'application fermée > cote de risque = 3 - moyen]]. L'objectif est de minimiser.

Changement net des éléments vulnérables

[[Nouveaux éléments vulnérables de l'application]] - [[Éléments vulnérables de l'application fermés]]. L'objectif est de minimiser.

Durée cumulée des éléments vulnérables de l'application fermés

Il s'agit du décompte sur la source de l'indicateur AVI. Fermé, qui utilise la table : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables d'application critiques en retard

Il s'agit du décompte sur la source de données AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables d'application critiques

Il s'agit du décompte sur la source de l'indicateur Applications avec des AVI actifs, qui utilise la table : sn_vul_analytics_app_ci_dept_bu. L'objectif est de minimiser.

Répartitions

- Âge
- Âge clôturé
- Application
- Unité business
- Cotes de risque
- Type d'analyse

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : La personnalisation du calcul de l'âge et de l'âge fermé pour les éléments vulnérables de l'application (AVI) peut entraîner une forte hausse ou une baisse des rapports d'Analyse des performances (PA) qui incluent ces mesures. Pour plus d'informations sur la personnalisation du calcul de l'âge et de l'âge fermé pour les AVI, consultez l'article de la base de connaissances KB1703270 .

Visualisations des données

Posture de Security

Nom	Type	Description
V15.0 : Conclusions du test de pénétration en attente de validation	Graphique à	Conclusions du test de pénétration à l'état Résolu, mais avec validation en attente, regroupés par cote de risque.
V15.0 : Conclusions du test de pénétration en retard	Graphique à	Conclusions du test de pénétration critique qui n'ont pas respecté leur date cible de rattrapage, regroupées par cote de risque.
Éléments vulnérables de l'application (AVI) actifs	Score unique	Nombre d'éléments vulnérables de l'application (AVI) actifs (non fermés).
Éléments vulnérables de l'application (AVI) non affectés	Score unique	Nombre d'éléments vulnérables d'applications (AVI) actifs sans groupe d'affectation.
Distribution de l'élément vulnérable de l'application (AVI)	Graphique à	Distribution de tous les éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque.
Éléments vulnérables de l'application (AVI) par âge	Carte thermique	Nombre d'éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque et par âge (en jours). **Remarque :** La personnalisation du calcul de l'âge et de l'âge fermé pour les éléments vulnérables de l'application (AVI) peut entraîner une forte hausse ou une baisse des rapports d'Analyse des performances (PA) qui incluent ces mesures. Pour plus d'informations sur la personnalisation du calcul de l'âge et de l'âge fermé pour les AVI, consultez l'article de la base de connaissances KB1703270 .
Tendances AVI	tendance	Tendance des éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Posture de Security (suite)

Nom	Type	Description
Nombre moyen d'AVI par application	tendance	Tendance des éléments vulnérables de l'application (AVI) moyens par application, regroupés par cote de risque.

Tendance des rattrapages

Nom	Type	Description
Délai moyen de remédiation des éléments vulnérables de l’application (AVI)	Ligne	Tendance du délai moyen de remédiation pour les éléments vulnérables de l'application (AVI) par cote de risque.
Changement net des AVI	tendance	Tendance des nouveaux éléments vulnérables de l'application (AVI) détectés par rapport à ceux fermés par mois.

Tableau d'affichage

Nom	Type	Description
10 principales applications ayant les éléments vulnérables d'application (AVI) les plus critiques	Carte de score et barre de distribution	Applications ayant le plus d'éléments vulnérables d'application (AVI) critiques.
10 principales applications ayant les éléments vulnérables d’application (AVI) critiques les plus en retard	Carte de score et barre de distribution	Applications ayant le plus d’éléments vulnérables d’application (AVI) actifs dont la date cible de rattrapage est dépassée.

Tableau de bord Mes vulnérabilités d’applications

Ce tableau de bord présente des mesures importantes pour analyser votre processus de gestion de la vulnérabilité des applications, comme l’affichage des taux de réalisation des cibles de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles requis ServiceNow AI Platform et affichage du tableau de bord

Remarque :

- Ce tableau de bord fait partie du pack de contenu Application Vulnerability Response. Le pack de contenu Application Vulnerability Response fait partie du pack de contenu Performance Analytics pour Vulnerability Response.
- Le pack de contenu Performance Analytics pour Vulnerability Response est disponible sous forme d'abonnement ServiceNow® Store distinct.
- Le pack de contenu Performance Analytics pour Vulnerability Response n'est pas automatiquement installé avec l'application Vulnerability Response.

Le tableau de bord Mes vulnérabilités d'application n'est disponible que lorsqu'un membre du groupe d'utilisateurs Champion de sécurité se connecte à une instance. Pour plus d'informations sur le tableau de bord de vue d'ensemble, voir Tableau de bord Gestion de la vulnérabilité des applications [PA].

Pour afficher le tableau de bord, accédez à **Réponse aux vulnérabilités de l'application** > **Mes vulnérabilités d'applications**.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités des applications bord peut également être affiché dans la nouvelle interface utilisateur. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône**Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Page Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités et Page Tableaux de bord dans Espace de travail de remédiation IT.

Affichez les rapports qui affichent des données de tendance dans le temps. Consultez régulièrement les tendances des mesures importantes pour analyser vos processus business globaux et identifier les domaines d'amélioration.

Le tableau de bord des vulnérabilités de mes applications est inclus dans le pack de contenu Performance Analytics pour Vulnerability Response. Le pack de contenu Performance Analytics pour Vulnerability Response n'est pas automatiquement installé avec l'application Réponse aux vulnérabilités . Il est disponible sous forme d'abonnement ServiceNow® Store séparé.

Cas d'utilisation

Utilisateur	Utilisation du tableau de bord
Spécialistes informatiques, responsables du rattrapage ou analystes qui corrigent les vulnérabilités qui leur sont affectées ou qui sont affectées à un groupe auquel ils appartiennent.	Un champion de sécurité utilise le tableau de bord Mes vulnérabilités d'applications pour suivre le volume, les performances et la progression du rattrapage des vulnérabilités d'application. Déterminez efficacement quels éléments vulnérables de l'application (AVI) présentent le plus de risque pour votre organisation. Ces tableaux de bord fournissent une vue graphique de l'activité AVI pour aider

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur	Utilisation du tableau de bord
	à déterminer les plans de rattrapage et la progression de l'état. Vous pouvez vous concentrer sur les KPI associés aux applications critiques affectées et aux vulnérabilités à haute visibilité. Obtenez rapidement un aperçu de votre exposition aux vulnérabilités et de votre posture de sécurité. Suivez le suivi de l'analyse initiale et de la détection au confinement ou à la correction.

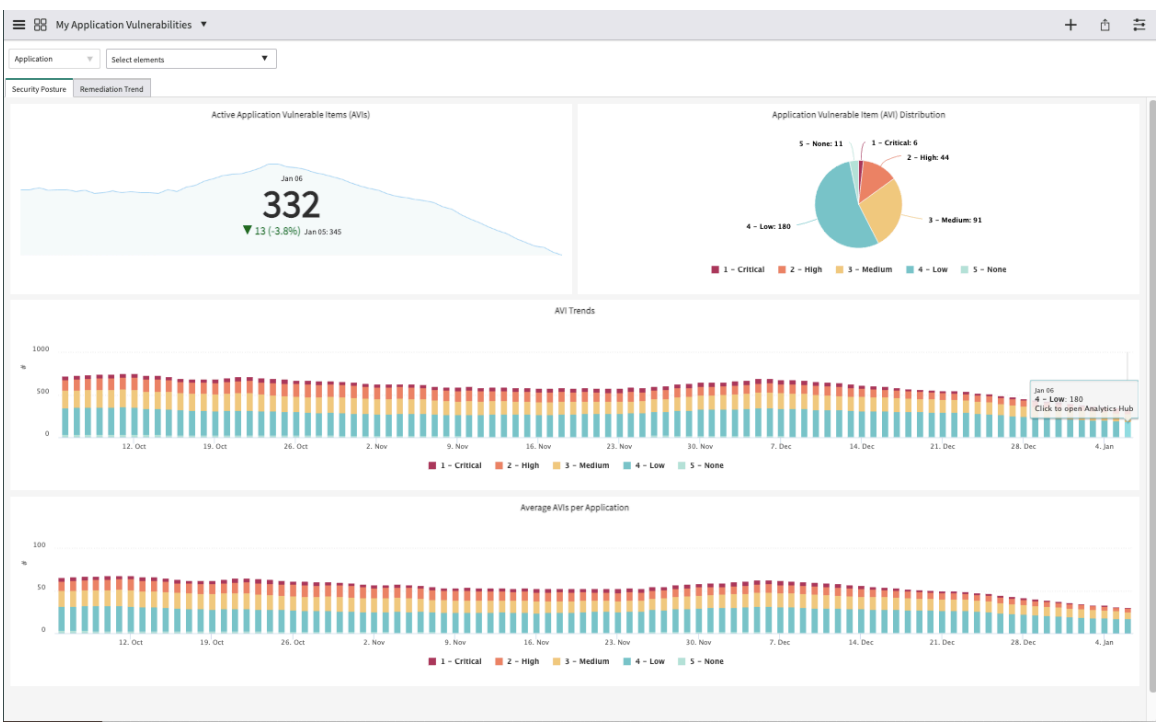
Onglets du tableau de bord Mes vulnérabilités d'applications [PA]

Le tableau de bord Mes vulnérabilités d'application communique les KPI pour le risque et la prévalence de la vulnérabilité, les applications affectées, les tendances et la progression du rattrapage. La valeur par défaut des tendances est de trois mois, mais peut être changée en 7 jours, un mois, 3 mois, 6 mois, Cumul annuel, 1 année ou Tout.

Les données sont réparties dans le tableau de bord par **application**. Utilisez la liste **Sélectionner des éléments** pour affiner vos sélections.

Onglet Posture de sécurité

L'onglet Posture de sécurité vous aide à comprendre votre posture de sécurité et la progression de vos actions de correction. Répartissez les données du tableau de bord Gestion de la vulnérabilité des applications par **type d'analyse, application** ou **unité business**. Chacun de ces choix dispose d'un filtre supplémentaire, **Sélectionner des éléments**, pour affiner vos sélections.

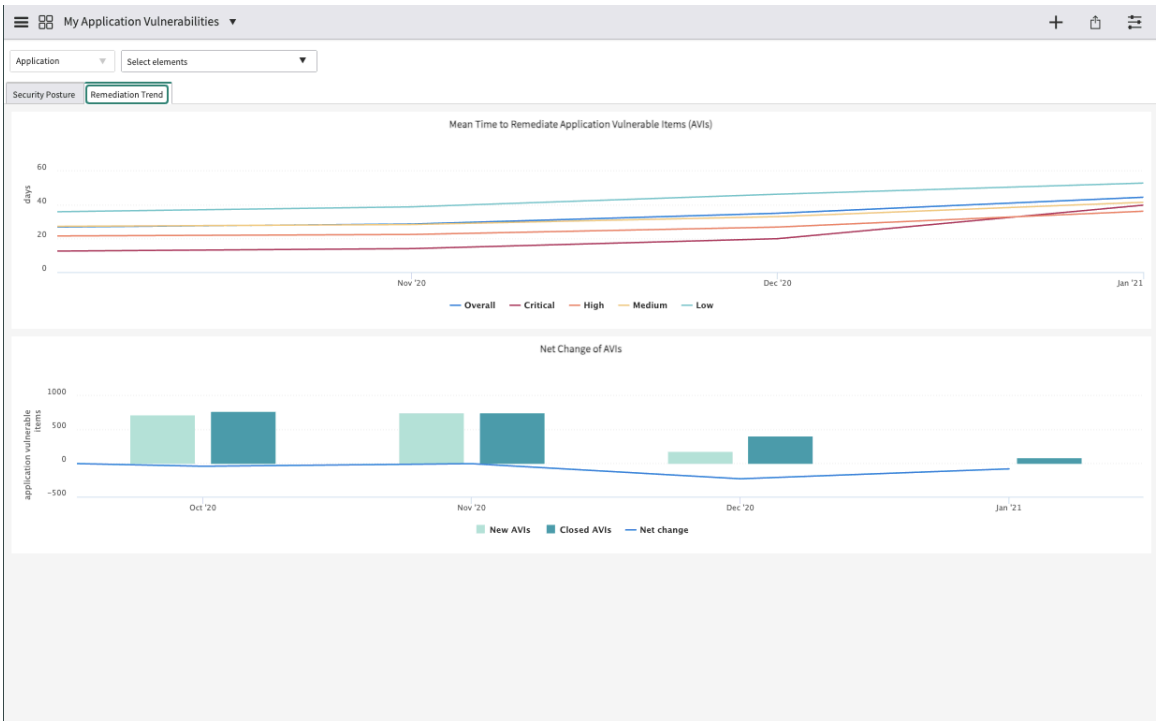


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Tendance de rattrapage

L’onglet Tendance de rattrapage vous aide à comprendre la progression de vos actions de rattrapage.



Indicateurs

Délai moyen de remédiation des AVI bas

[[Durée cumulée des éléments vulnérables de l’application fermée > cote de risque = 4 - faible]]/[[Éléments vulnérables de l’application fermée > cote de risque = 4 - faible]]. L’objectif est de minimiser.

Versions de l'application

Il s’agit du nombre distinct sur les applications d’AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L’objectif est de minimiser.

Éléments vulnérables de l'application

Il s’agit du nombre d’éléments vulnérables de l’application AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L’objectif est de minimiser.

Nombre moyen d'AVI par application

[Éléments vulnérables de l’application actifs]] / [[Versions de l’application]]. L’objectif est de minimiser.

VI non affectés

Il s’agit du décompte sur la source de l’indicateur AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L’objectif est de minimiser.

Délai moyen de rattrapage des AVI

[[Durée cumulée des éléments vulnérables de l’application fermée]] / [[Éléments vulnérables de l’application fermée]]. L’objectif est de minimiser.

Délai moyen de remédiation des AVI élevés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 2 - élevé]]/[[Éléments vulnérables de l'application fermée > cote de risque = 2 - élevé]]. L'objectif est de minimiser.

Éléments vulnérables d'application clôturés

Il s'agit du décompte sur la source de l'indicateur AVI. Fermé, qui utilise la table : sn_vul_app_vulnerable_item. L'objectif est de maximiser.

Délai moyen de rattrapage des AVI critiques

[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 1 - critique]]/[[Éléments vulnérables de l'application fermée > cote de risque = 1 - critique]]. L'objectif est de minimiser.

Nouveaux éléments vulnérables de l'application

Il s'agit du décompte sur la source de l'indicateur AVI. Nouveau, qui utilise la table : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Délai moyen de remédiation des AVI moyens

[[Durée cumulée des éléments vulnérables de l'application fermée > cote de risque = 3 - moyen]]/[[Éléments vulnérables de l'application fermée > cote de risque = 3 - moyen]]. L'objectif est de minimiser.

Changement net des éléments vulnérables

[[Nouveaux éléments vulnérables de l'application]] - [[Éléments vulnérables de l'application fermés]]. L'objectif est de minimiser.

Durée cumulée des éléments vulnérables de l'application fermés

Il s'agit du décompte sur la source de l'indicateur AVI. Fermé, qui utilise la table : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables d'application critiques en retard

Il s'agit du décompte sur la source de données AVI. Actif, qui utilise la table suivante : sn_vul_app_vulnerable_item. L'objectif est de minimiser.

Éléments vulnérables d'application critiques

Il s'agit du décompte sur la source de l'indicateur Applications avec des AVI actifs, qui utilise la table : sn_vul_analytics_app_ci_dept_bu. L'objectif est de minimiser.

Répartitions

- Âge
- Âge clôturé
- Application
- Unité business
- Cotes de risque
- Type d'analyse

Remarque : La personnalisation du calcul de l'âge et de l'âge fermé pour les éléments vulnérables de l'application (AVI) peut entraîner une forte hausse ou une baisse des rapports d'Analyse des performances (PA) qui incluent ces mesures. Pour plus d'informations sur la personnalisation du calcul de l'âge et de l'âge fermé pour les AVI, consultez l'article de la base de connaissances KB1703270 .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations des données

Posture de Security

Nom	Type	Description
Éléments vulnérables de l'application (AVI) actifs	Score unique	Nombre d'éléments vulnérables de l'application (AVI) actifs (non fermés).
Distribution de l'élément vulnérable de l'application (AVI)	Graphique à	Distribution de tous les éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque.
Tendances AVI	tendance	Tendance des éléments vulnérables de l'application (AVI) actifs, regroupés par cote de risque.
Nombre moyen d'AVI par application	tendance	Tendance des éléments vulnérables de l'application (AVI) moyens par application, regroupés par cote de risque.

Tendance des rattrapages

Nom	Type	Description
Délai moyen de remédiation des éléments vulnérables de l'application (AVI)	Ligne	Tendance du délai moyen de remédiation pour les éléments vulnérables de l'application (AVI) par cote de risque.
Changement net des AVI	tendance	Tendance des nouveaux éléments vulnérables de l'application (AVI) détectés par rapport à ceux fermés par mois.

Cadre de travail des rapports agrégés pour Réponse aux vulnérabilités des applications

À l'aide de l'infrastructure des rapports agrégés, vous pouvez créer des rapports pour les données qui impliquent des requêtes à la volée complexes et de longue durée pour de meilleures performances.

Le cadre de travail des rapports agrégés améliore les performances en :

- en utilisant moins de ressources et en rendant les rapports plus rapidement,
- l'agrégation des données et la réutilisation des agrégations et des répartitions (Grouper par) et
- réduire les requêtes à la base de données

Lorsque vous avez plus d'un million d'éléments vulnérables d'application (AVIT), utilisez le cadre de travail des rapports agrégés en même temps que les rapports standard.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Administrateur ServiceNow AI Platform (admin) : installer et activer cette Solution d'analyse des performances et génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Analyse des performances Administrateur (pa_admin) : Examinez les agrégations, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.
- Administrateur (sn_vul_cmn.admin) : créer des agrégations.
- VR write(sn_vul_cmn.write) : modifiez les données dans les agrégations et les résultats agrégés.
- VR read (sn_vul_cmn.read) : passez en revue les données dans les agrégations et les résultats agrégés.
- Analyste de vulnérabilité (sn_vul.vulnerability_analyst) : examinez les résultats agrégés.

Information associée

Configurer une agrégation pour les données sources

Exécuter plusieurs agrégations simultanément

Configurer le nombre d’agrégations qui peuvent s’exécuter simultanément

Créer un rapport à l’aide d’une agrégation

Références de Réponse aux vulnérabilités des applications

Rubriques de référence contenant des informations sur les tables, les rôles et les propriétés installés avec l’application Réponse aux vulnérabilités des applications .

Pour en savoir plus, consultez :

- Réponse aux vulnérabilités des applications Groupes et rôles d’utilisateurs
- Composants installés avec Réponse aux vulnérabilités des applications
- États des éléments vulnérables de l’application (AVI)
- Champs de l’application analysée
- Champs d’élément vulnérable d’application
- Champs de vulnérabilité de l’application
- États des tests de pénétration

Réponse aux vulnérabilités des applications Groupes et rôles d’utilisateurs

Avant de pouvoir corriger les vulnérabilités avec Réponse aux vulnérabilités des applications (AVR), vous devez affecter des utilisateurs à des groupes d’utilisateurs.

Les rôles définissent ce que vous et vos groupes pouvez voir et effectuer dans Réponse aux vulnérabilités des applications, Analyse des performances pour Réponse aux vulnérabilités ainsi que dans les intégrations tierces avec Réponse aux vulnérabilités des applications.

Groupes d'utilisateurs

Les groupes d’utilisateurs par défaut suivants prennent en charge Réponse aux vulnérabilités des applications:

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Gestionnaire de sécurité des applications : contient les gestionnaires de sécurité. À partir de la version 15.0, il contiendra également les propriétaires d'applications Réponse aux vulnérabilités des applications qui géreront les demandes d'évaluation des tests de pénétration.
- Champion de sécurité : contient des liaisons entre le groupe de développement et les gestionnaires de sécurité.
- Développeur : contient les contributeurs individuels.
- V15.0 : Hacker éthique : contient les membres de l'équipe de piratage éthique qui effectuent des tests de pénétration des applications.

Le rôle d'administrateur système [admin] est requis pour affecter des utilisateurs aux groupes d'utilisateurs Réponse aux vulnérabilités des applications par défaut, à l'aide du module Administration utilisateurs,

Remarque :

L'affectation d'utilisateurs AVR aux Réponse aux vulnérabilités des applications groupes d'utilisateurs pour Réponse aux vulnérabilités des applications n'est pas disponible dans la fonctionnalité de l'Assistant Réponse aux vulnérabilités de configuration. Seuls les Réponse aux vulnérabilités rôles y sont affectés.

La table suivante répertorie les groupes d'utilisateurs disponibles Réponse aux vulnérabilités des applications et les rôles qui leur sont associés. Utilisez cette table pour déterminer quels utilisateurs doivent être affectés à quels groupes.

Groupe d'utilisateurs	Rôles dans ce groupe
Champion de la sécurité Les membres de ce groupe peuvent : • Lecture et écriture des éléments vulnérables de l'application (AVI) qui vous sont affectés. • Affectez un AVI, qui vous est affecté, à une autre personne ou à un autre groupe. • V20.0 : Créer, mettre à jour, supprimer et annuler (désactiver) des règles d'exception.	• sn_vul.app_read_assigned • sn_vul.app_écriture_affectée • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_manage_auto_exception_rule
Gestionnaire de sécurité des applications Les membres de ce groupe peuvent : • V20.0 : Créer, mettre à jour, supprimer et annuler (désactiver) des règles d'exception. • Lecture, écriture, suppression et toutes les opérations sur les règles de tâche de rattrapage d'application. • Lecture et écriture de tous les AVI.	• sn_vul.app_manage_auto_exception_rule • sn_vul.app_manage_group_rules • sn_vul.app_lecture_tout • sn_vul.app_écrire_tout • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_configure_integrations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupe d'utilisateurs	Rôles dans ce groupe
• Configurez AVR en créant et en gérant des règles, des calculateurs et des cartes de gravité. • Configurez les intégrations. • Supprimer les AVI. • Affecter AVI à des individus ou à des groupes. • Gérer les applications. • Permet l'accès au module d'application. • Planifier, configurer, exécuter l'intégration. • Lire et exécuter des intégrations. • Afficher les tableaux de bord et les rapports AVR Analyse des performances . • V15.0 : Gérez les demandes d'évaluation des tests de pénétration.	**Remarque :** Par défaut, ce rôle contient des rôles granulaires pour la configuration d'intégration tierce. Pour définir ou modifier un groupe d'utilisateurs App-Sec Manager par intégrations uniques ou spécifiques, reportez-vous à la section Réponse aux vulnérabilités Profils et rôles granulaires. • sn_vul.app_manage_assignment_rules • sn_vul.app_manage_remediation_target_rules • sn_vul.app_manage_risk_score_configurations • sn_vul.app_manage_applications • sn_vul.app_manage_app_vul_permissions • sn_vul.app_manage_normalized_severity • Version 13.0 : sn_vul.app_manage_app_sc • Version 12.0 uniquement : sn_vul.app_read_application_release [Supprimé dans la version 12.1. Ne pas utiliser] • sn_sec_int.admin • Version 13.0 : pa_power_user • pa_viewer **Remarque :** Réponse aux vulnérabilités À partir de la version 13.0, pa_viewer est inclus dans pa_power_user et n'est plus nécessaire en soi. • V15.0 : sn_vul.app_manage_pen_test_request • V15.0 : sn_vul.app_update_state • V15.0 : cmdb_read
Développeur Les membres de ce groupe peuvent : • Lire et écrire les enregistrements AVR qui vous sont affectés. • Affectez un AVI, qui vous est affecté, à une autre personne ou à un autre groupe.	• sn_vul.app_read_assigned • sn_vul.app_écriture_affectée • sn_vul.app_update_assignment_group • sn_vul.app_update_assigned_to • sn_vul.app_pa_sc_view

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupe d'utilisateurs	Rôles dans ce groupe
V15.0 : Hacker éthique Les membres de ce groupe peuvent : • Configurez le groupe d'affectation et le délégataire par défaut pour les demandes d'évaluation de test de pénétration. • Gérer les résultats du test de pénétration. • Gérez les demandes d'évaluation de test de pénétration. • Affichez les éléments vulnérables de l'application. • Mettez à jour l'affectation des éléments vulnérables de l'application.	• V15.0 : sn_vul.app_update_state • V15.0 : sn_vul.app_manage_pen_test_request • V15.0 : ITIL • V15.0 : sn_vul.app_read_all • V15.0 : sn_vul.app_manage_pen_test_request_config • V15.0 : sn_vul.app_manage_manual_avits • V15.0 : sn_vul.app_update_assigned_to • V15.0 : sn_vul.app_update_assignment_group

Affecter des utilisateurs à des groupes d'utilisateurs dans Réponse aux vulnérabilités des applications

Affectez des utilisateurs à des groupes à l'aide du module Administration utilisateurs de votre instance.

Avant de commencer

Rôle requis : admin

Procédure

Pour affecter un utilisateur ou le supprimer d'un groupe :

a. Accédez à la **Administration** > **Groupes**.

b. Recherchez et ouvrez le groupe approprié, par exemple, **Gestionnaire de sécurité des applications**.
L'enregistrement du groupe s'affiche.

c. Sélectionnez l'onglet **Membres de groupe**.
Les membres actuels du groupe s'affichent.

d. Cliquez sur **Modifier**.
Le formulaire Modifier les membres s'affiche.

e. Dans la liste **Collection** , sélectionnez les utilisateurs à ajouter ou supprimer du groupe.

f. Une fois que tous les utilisateurs ont été ajoutés à la **liste des membres du groupe** ou supprimés, cliquez sur **Enregistrer**.
Vous revenez à l'onglet **Membres du groupe** .

g. Cliquez sur **Mettre à jour** pour enregistrer vos modifications et revenir à la liste des groupes.

Information associée

Composants installés avec Réponse aux vulnérabilités des applications

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants installés avec Réponse aux vulnérabilités des applications

Plusieurs types de composants sont installés avec l'activation de la fonctionnalité, notamment les tables, les rôles d'utilisateur et les Réponse aux vulnérabilités des applications travaux planifiés.

À partir de la version 24.0.6 de Réponse aux vulnérabilités des applications, les propriétés système les plus fréquemment utilisées sont désormais accessibles dans l'application Réponse aux vulnérabilités des applications . Pour afficher ces propriétés système, accédez à **Tous**Réponse aux vulnérabilités des applications**Propriétés**.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Rôles installés

Les rôles granulaires sont Réponse aux vulnérabilités des applications affectés par défaut à des groupes d'utilisateurs spécifiques.

Remarque : L'utilisation de rôles granulaires en dehors de ces groupes d'utilisateurs nécessite du codage et une expertise avancée Réponse aux vulnérabilités des applicationsServiceNow .

Titre du rôle [name]	Description	Contient des rôles
V20.0 : sn_vul.app_manage_auto_exception_rule	Créer, mettre à jour, supprimer et annuler (désactiver) des règles d'exception.	sn_vul.app_read_auto_exception_rule
sn_vul.app_manage_group_rules	Lecture, écriture, suppression et toutes les opérations sur les règles de tâche de rattrapage d'application.	• sn_vul.app_lecture_tout • sn_vul.app_read_group_rules
V20.0 : sn_vul.app_exception_approver	Approuve les règles d'exception et les demandes d'extension de règle d'exception. À partir de la version 20.0, le rôle granulaire, sn_vul.app_read_all, a été supprimé pour ce rôle afin que vous puissiez accéder aux éléments vulnérables de l'application et aux tâches de rattrapage qui vous sont affectées, à vous et à votre groupe, au lieu de tous les éléments vulnérables de l'application et des tâches de rattrapage.	• sn_vul.app_read_auto_exception • sn_vul.view_manager_workspace
sn_vul.app_approbateur_faux_positif	Approuve ou rejette les demandes de faux positifs.	sn_vul.view_manager_workspace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
sn_vul.app_read_assigned	Affichez les éléments vulnérables de l'application (AVI) qui vous sont affectés à la fois dans l'interface utilisateur classique et Espace de travail de remédiation IT dans . **Important :** À partir de la version 24.0 de Réponse aux vulnérabilités, le rôle sn_vul.app_read_assigned a le privilège d'accéder Espace de travail de remédiation IT au .	sn_vul.view_rem_workspace
sn_vul.app_lecture_tout	Affichez tous les AVI et les informations connexes dans l'interface utilisateur classique ou Espace de travail du gestionnaire de vulnérabilités. **Important :** À partir de la version 24.0 de Réponse aux vulnérabilités, le rôle sn_vul.app_read_all a le privilège d'accéder Espace de travail du gestionnaire de vulnérabilités au .	sn_vul.view_manager_workspace
sn_vul.app_écriture_affectée	Mettre à jour les AVI qui vous sont affectés.	
sn_vul.app_écrire_tout	Mettre à jour tous les AVI et les informations connexes.	
sn_vul.app_update_assignment_group	Mettre à jour le groupe d'affectation AVI.	**Remarque :** En cas d'utilisation en dehors du groupe d'utilisateurs par défaut, sn_vul.app_write_all ou sn_vul.app_write_assigned.
sn_vul.app_update_assigned_to	Mettre à jour le délégataire AVI.	**Remarque :** En cas d'utilisation en dehors du groupe d'utilisateurs par défaut, sn_vul.app_write_all ou sn_vul.app_write_assigned.
sn_vul.app_configure_integrations	Configurez des intégrations tierces.	sn_vul.app_lecture_tout sn_vul.app_read_integrations sn_sec_int.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
		sn_vul_veracode.configure_integra sn_vul.configure_nvd_administratio **Remarque :** Pour définir ou mo un groupe d'utilisateurs App-Sec Ma par intégrations uniques ou spécifiqu reportez-vous à la section Réponse a vulnérabilités Profils et rôles granula
sn_vul.app_read_integrations	Affichez toutes les intégrations tierces.	
sn_vul_veracode.configure_integration	Définir, mettre à jour et supprimer les intégrations Veracode.	
sn_vul.app_manage_assignment_rules	Définir, mettre à jour et supprimer des règles d'affectation AVI.	sn_vul.app_lecture_tout sn_vul.app_read_assignment_rules
sn_vul.app_read_assignment_rules	Affichez les règles d'affectation.	
sn_vul.app_manage_remediation_target_rules	Définir, mettre à jour et supprimer les règles de cibles de rattrapage AVI.	sn_vul.app_lecture_tout sn_vul.app_read_remediation_targ
sn_vul.app_manage_risk_score_configurations	Définir, mettre à jour et supprimer les calculateurs AVR et les règles de risque.	sn_vul.app_lecture_tout sn_vul.app_read_risk_score_config sn_sec_cmn.calc.write
sn_vul.app_read_risk_score_configuration	Afficher les calculateurs AVR et les règles de risque.	
sn_vul.app_manage_applications	Affichez, mettez à jour et supprimez des enregistrements d'application.	
sn_vul.app_manage_app_sc	Donne au champion de la sécurité la possibilité de s'ajouter ou de se supprimer de la liste connexe Applications numérisées.	
sn_vul.app_pa_sc_view	Fournit une vue pertinente pour le champion de sécurité spécifique.	
sn_vul.app_manage_app_vul_permissions	[Interne] Utilisé par sn_vul.app_manage_applications.	
sn_vul.app_manage_normalized_severity	Mettez à jour le mappage sur la gravité normalisée.	sn_vul.app_read_normalized_severity

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
sn_vul.app_read_normalized_severity [Supprimé dans la version 12.1. Ne pas utiliser.]	Afficher les enregistrements de gravité normalisée.	
sn_vul.app_read_application_release	Afficher les enregistrements de version de l'application.	
sn_sec_int.admin	Permet d'accéder aux intégrations.	
pa_power_user	Permet d'accéder aux rapports	pa_viewer
sn_vul.app_sec_manager	Classe par ordre de priorité et gère les éléments vulnérables de l'application.	
sn_vul.app_développeur	Développeur responsable de la correction des vulnérabilités de l'application.	
sn_vul.app_créer_surveiller_rubrique	Créez des rubriques de surveillance pour les vulnérabilités de l'application.	
sn_vul.app_read_watch_topic	Lisez les rubriques de surveillance pour connaître les vulnérabilités des applications.	
sn_vul.app_modifier_regarder_rubrique	Modifier les rubriques de surveillance pour les vulnérabilités de l'application.	
sn_vul_blackduck.configure_integration	Configurez des intégrations tierces.	sn_vul_blackduck.configure_integration

Travaux planifiés installés

Pour Réponse aux vulnérabilités les travaux planifiés partagés, Composants installés avec Réponse aux vulnérabilités reportez-vous à la section .

Tâche planifiée	Description
Associer des AVI existants à la règle d'exception automatique	Évalue les éléments vulnérables de l'application pour déterminer s'ils correspondent aux règles d'exception.
Renseigner l'entrée et le CVE M2M	Rend les enregistrements existants cohérents avec plusieurs enregistrements CWE. Exécuter une fois après la mise à niveau pour renseigner puis désactiver.
Resynchroniser la CWE primaire	Pour les calculs CWE primaires personnalisés. Exécuter une fois après la mise à niveau pour resynchroniser puis désactiver.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Pour déployer les valeurs d'éléments vulnérables d'applications vers la vulnérabilité et le groupe	Calcule les vulnérabilités et les déploiements de groupes pour les éléments vulnérables de l'application. **Remarque :** À partir de la version 23.0 de Réponse aux vulnérabilités des applications, la tâche planifiée est améliorée pour créer des tâches en arrière-plan avec des options de multithreading. Cette mise à niveau implique de segmenter la tâche en plusieurs tâches enfants plus petites, qui sont exécutées en parallèle ou simultanément. Cette modification permet de traiter plusieurs enregistrements simultanément, ce qui accélère considérablement la tâche globale.
Intégration de la liste des projets Black Duck	Extrait et ingère les données dans la table des projets Black Duck.
Intégration de la liste des applications Black Duck	Importe les applications dans la table des applications détectées pour toutes les versions de projet disponibles avec l'intégration de Black Duck dans la table des projets.
Intégration d'élément vulnérable de l'application Black Duck	Ingère des éléments vulnérables dans l'application ServiceNow en fonction des vulnérabilités détectées par les analyseurs pour chaque application détectée dans le système.

Tables installées

Table	Description
Version de l'application [sn_vul_app_release]	Contient des informations sur la version de l'application.
Version 13.0 : Champions de sécurité des applications [sn_vul_app_m2m_app_sc]	Contient les enregistrements de groupe du Réponse aux vulnérabilités des applications champion de sécurité.
Entrée de vulnérabilité de l'application [sn_vul_app_vul_entry]	Contient les entrées de vulnérabilité de l'application.
Intégration de vulnérabilité de l'application [sn_vul_app_integration]	Contient Réponse aux vulnérabilités des applications les enregistrements d'intégration.
Emplacement de numérisation de vulnérabilité de l'application [sn_vul_app_vul_scan_location]	Contient des informations sur l'emplacement de l'analyse tierce.
Synthèse de numérisation de vulnérabilité de l'application	Contient des informations sur la synthèse de l'analyse tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vul_app_vul_scan_summary]	
Élément vulnérable de l'application [sn_vul_app_vulnerable_item]	Contient des enregistrements AVI. À partir de la version 19.0, les colonnes suivantes sont ajoutées pour la nomenclature logicielle : • sn_sbm_config_rule • sn_sbom_component • vex_justification • vex_detail • vex_response • vex_state • sca_type (SBOM-SCA)
Application numérisée [sn_vul_app_scanned_application]	Contient des informations sur l'application.
Mappage d'états [sn_vul_app_state_map]	Contient le mappage de l'état des intégrations tierces vers les états des éléments vulnérables de l'application (AVI).
CWE de vulnérabilité [sn_vul_m2m_entry_cwe]	Relie les données CVE aux entrées vulnérables de l'application.
Manifeste de tâche de rattrapage d'application sn_vul_app_rt_manifest	Toutes les mises à jour sur la tâche de rattrapage sont effectuées à l'aide de cette table de manifeste par travaux planifiés.
Tâche de rattrapage d'application sn_vul_app_vulnerability	Contient des tâches de rattrapage d'applications.
Élément de tâche de rattrapage d'application sn_vul_app_m2m_vul_group_item	Table M2M entre les tâches AVI et de rattrapage d'application.
Version 21.0 : Éléments vulnérables de l'application sn_vul_app_vulnerable_item	Contient des enregistrements AVI.
Version 21.0 : Package [sn_vul_app_package]	Contient les détails du package d'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Version 21.0 : Licences sn_vul_app_license	Contient les licences d'application.
Version 21.0 : Tâches de remédiation d'applications sn_vul_app_vulnerability	Contient des tâches de rattrapage d'applications.
sn_vul_blackduck_config	Contient les détails de la configuration de l'intégration de Black Duck.
sn_vul_blackduck_project	Contient des détails sur les projets provenant de Black Duck.
sn_vul_blackduck_project_import	Table de jeu d'importation pour l'ingestion de projet Black Duck.
sn_vul_blackduck_app_import	Table de jeu d'importation pour l'ingestion d'application Black Duck.
sn_vul_blackduck_avit_import	Table de jeux d'importation pour l'ingestion AVIT de Black Duck.

États des éléments vulnérables de l'application (AVI)

Réponse aux vulnérabilités des applications offre un modèle d'état pour l'état des éléments vulnérables de votre application (AVI), à un moment donné. Savoir comment chaque état est lié et s'affecte les uns les autres vous aide à déterminer quand et comment corriger vos AVI.

États des éléments vulnérables d'applications

Comprendre le fonctionnement des états permet de créer ou de modifier des règles d'éléments vulnérables de l'application (AVI). Les AVI ont plusieurs états possibles qui sont mappés à partir de l'état Rattrapage importé à partir de l'intégration tierce. Dans un AVI, le champ **État** est en lecture seule.

Réponse aux vulnérabilités des applications Diagramme de flux d'états

État	Description
Ouvert	État à la création. À partir de cet état, vous pouvez : **V16 : obtenir plus de détails** Obtenez les informations suivantes sur un AVI importé de Fortify : • Résumé de la vulnérabilité • Explication de vulnérabilité • Recommandation • Références • Demande • Réponse **V16 : Marquer comme faux positif**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	Marquez un élément comme faux positif si le scanner signale qu'il existe une vulnérabilité dans le système, mais qu'il n'y a en réalité aucune vulnérabilité. **V16 : demande d'exception** Demandez une exception, une date de réouverture (Jusqu'à), un motif et, éventuellement, fournissez des informations supplémentaires. Reporte le rattrapage de l'élément jusqu'à la date à laquelle une exception est demandée. **V15 : fermer** Sélectionnez l'état Fermé, un motif dans la boîte de dialogue Fermer l'élément vulnérable et fournissez des informations supplémentaires. Ferme l'AVI. **V15 : résoudre** Marquez un AVI ouvert comme Résolu pour le faire passer à l'état Résolu. Vous devez ajouter des notes de résolution dans la boîte de dialogue Résoudre l'élément vulnérable de l'application.
Différé	**V15 :** Cette opération est déclenchée par l'option **Demande d'exception** . Dans le cadre du workflow d'approbation, l'état Différé est en cours de révision et ne peut pas être fermé tant qu'il n'a pas été approuvé. À partir de cet état, vous pouvez : **V16 : obtenir plus de détails** Obtenez les informations suivantes sur un AVI importé de Fortify : • Résumé de la vulnérabilité • Explication de vulnérabilité • Recommandation • Références • Demande • Réponse **Rouvrir** Fait passer un AVI fermé ou résolu à un état ouvert.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	Fermer Sélectionnez l'état Fermé, un motif et fournissez des informations supplémentaires. Ferme l'AVI.
En cours d'examen	Sélectionnez cette option dans la liste **État** . À partir de cet état, vous pouvez : **V20.0** Transférez manuellement une tâche de rattrapage ou un enregistrement AVI en **attente d'implémentation**. **V16 : obtenir plus de détails** Obtenez les informations suivantes sur un AVI importé de Fortify : • Résumé de la vulnérabilité • Explication de vulnérabilité • Recommandation • Références • Demande • Réponse **V16 : Marquer comme faux positif** Marquez un élément comme faux positif si le scanner signale qu'il existe une vulnérabilité dans le système, mais qu'il n'y a en réalité aucune vulnérabilité. **V16 : demande d'exception** Demandez une exception, une date de réouverture (Jusqu'à), un motif et, éventuellement, fournissez des informations supplémentaires. Reporte le rattrapage de l'élément jusqu'à la date à laquelle une exception est demandée. **V15 : fermer** Sélectionnez l'état Fermé, un motif dans la boîte de dialogue Fermer l'élément vulnérable et fournissez des informations supplémentaires. Ferme l'AVI. **V15 : résoudre** Marquez un AVI ouvert comme Résolu pour le faire passer à l'état Résolu. Vous devez ajouter des notes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	de résolution dans la boîte de dialogue Résoudre l'élément vulnérable de l'application.
En attente d'implémentation	Vous pouvez uniquement faire passer manuellement des enregistrements à cet état en sélectionnant En attente d'implémentation dans AVI et les enregistrements de tâche de rattrapage à l'état En cours d'examen. À partir de cet état, vous pouvez : **Ouvert** Replace l'AVI à un état ouvert. **En cours d'examen** Obtenez plus d'informations pour la résolution. Transitions vers En cours d'examen. **Résoudre** Marquez un AVI ouvert comme Résolu pour le faire passer à l'état Résolu. Vous devez ajouter des notes de résolution dans la boîte de dialogue Résoudre l'élément vulnérable de l'application. **Fermer** Sélectionnez l'état Fermé, un motif dans la boîte de dialogue Fermer l'élément vulnérable et fournissez des informations supplémentaires. Ferme l'AVI. Dans cet état, faites passer un enregistrement en En attente d'implémentation lorsque vos recherches et votre travail sur une tâche sont terminés et bien qu'un correctif soit prêt à être implémenté, il n'est pas encore disponible. Définissez la **date d'engagement de rattrapage** et les champs **Plan de rattrapage** . Après l'implémentation, vous résolvez ou fermez les enregistrements.
Résolu	Déclenché à partir du bouton Résoudre. À partir de cet état, vous pouvez : **V16 : obtenir plus de détails**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Diagramme de flux d'états (suite)

État	Description
	Obtenez les informations suivantes sur un AVI importé de Fortify : • Résumé de la vulnérabilité • Explication de vulnérabilité • Recommandation • Références • Demande • Réponse **Rouvrir** Revient à un état **ouvert** . **Fermer** Sélectionnez l'état **Fermé** , un motif et fournissez des informations supplémentaires. Ferme le groupe. Les notes et les informations sur la résolution s'affichent sous l'onglet **Notes** .
Fermé	Déclenché à partir du bouton Fermer. À partir de cet état, vous pouvez : Rouvrir : revient à un état ouvert.

Remarque : Consultez la section Intégration d'Application Vulnerability Response avec d'autres applications pour comprendre les différentes intégrations qui ont alimenté l'AVI.

États de la tâche de rattrapage d'application

De la création à la fermeture d'une tâche de rattrapage d'application, la tâche de rattrapage d'application passe par différents états au cours de l'ensemble du processus de rattrapage.

La priorité des États est la suivante :

Fermé > **Différé** > **Résolu** > **En cours de révision** > **En attente d'implémentation** > **En cours d'examen** > **Ouvert**

La transition d'état se produit lorsque vous effectuez diverses actions telles que Différer, Ouvrir, Fermer, etc.

Les actions que vous pouvez effectuer sur une tâche de rattrapage d'application à un état spécifique sont similaires à celles d'une tâche de rattrapage d'hôte. Par conséquent, pour plus d'informations, consultez le Réponse aux vulnérabilités États des tâches de rattrapage et Scénarios de déploiement et de réduction de l'état dans la Réponse aux vulnérabilités documentation.

Remarque : À partir de la version 23.0 de Réponse aux vulnérabilités, le bouton **Fermer** a été supprimé pour garantir que la fermeture de la tâche de rattrapage est pilotée par le scanner.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités des applications Exemples de règles de tâches de rattrapage

Exemple de règle de tâche de rattrapage utilisant le Créateur de conditions.

Une règle de tâche de rattrapage utilisant la vulnérabilité, le modèle de produit, l'adresse IP et le groupe d'affectation

1. Dans le générateur de conditions d'un nouvel enregistrement, définissez la condition sur **Vulnérabilité** > **est** et entrez une vulnérabilité connue.

   Les vulnérabilités sont importées à partir des intégrations Base de données de vulnérabilité nationale (NVD) et Common Weakness Enumeration (CWE), comme décrit dans .Configurer Réponse aux vulnérabilités des applications

2. Dans la section Grouper par, sélectionnez **Élément vulnérable d'application** pour le champ **Regrouper les éléments vulnérables d'application** .
3. Dans le champ Utilisation, sélectionnez **Groupe d'affectation**.

   Utilisez les règles d'affectation pour définir automatiquement le champ **Groupe d'affectation** à utiliser dans votre règle de tâche de rattrapage. Vous pouvez utiliser une règle fournie avec l'application ou configurer vos propres règles d'affectation. Consultez Affecter automatiquement des éléments vulnérables d'applications Réponse aux vulnérabilités des applications pour plus d'informations.

4. Sélectionnez une autre condition, par exemple, l'élément de configuration d'élément vulnérable d'application dans le champ **Élément vulnérable d'application depuis** et l'adresse IP ou le modèle de produit dans le champ **Utilisation** .
5. Dans la section Affectation, pour Affecter la tâche de rattrapage champ par champ, sélectionnez **Grouper par champ**.
6. Dans le champ Grouper par, sélectionnez **Groupe d'affectation**.

   Comme décrit dans cette section, cette sélection affecte des éléments vulnérables à différents groupes en fonction des conditions définies dans la section Grouper par. Bien que les AVI partagent la vulnérabilité, ils sont affectés à différents groupes en fonction du modèle de produit CI ou de l'adresse IP.

7. Sélectionnez **Soumettre** pour enregistrer votre règle.

Champs de l'application analysée

Les applications sont stockées pendant l'importation sous **Administration** > **Applications détectées** in Réponse aux vulnérabilités des applications.

Champs de l'application analysée

sauf indication contraire, les champs importés dans cette table sont en lecture seule. **Les entrées de département** et **de groupe de support** peuvent être ajoutées ou modifiées manuellement par un gestionnaire App-Sec.

Champ	Description
Nom	Nom importé de l'application.
Version	Version importée de l'application, le cas échéant.
Statut opérationnel	Statut opérationnel importé de l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Département	Département importé auquel appartient l'application. S'il est vide, il peut être ajouté manuellement.
Unité business	Unité business importée à laquelle appartient le département. Lorsque le champ **Département** est renseigné, il est automatiquement renseigné avec l'unité business à laquelle le département appartient. Sinon, il est laissé vide et en lecture seule.
Groupe de support	Groupe de support importé auquel appartient l'application. S'il est vide, il peut être ajouté manuellement.
Description	Description importée de l'application.
Date de dernière vérification de conformité de politique	Date à laquelle l'application a été analysée pour la dernière fois par Veracode pour vérifier sa conformité aux politiques. Il est utilisé dans les intégrations enchaînées de l'intégration de liste d'applications, où la prise en charge de l'ingestion delta pour les applications est disponible, en comparant cette date à l'heure de début delta des intégrations respectives. **Remarque :** Les données sont récupérées lorsque les applications sont extraites de Veracode, dont la valeur « Date de dernière vérification de conformité de politique » est supérieure ou égale à l'« Heure de début » (delta_start_time) des intégrations enchaînées.
Liste connexe (visible uniquement par un gestionnaire App-Sec ou un champion de sécurité)	
Champion de sécurité	Répertorie les applications associées à un champion de sécurité. Les gestionnaires App-Sec peuvent ajouter ou supprimer des membres de la liste.

Champs d'élément vulnérable d'application

Les éléments vulnérables de l'application (AVIT) sont automatiquement créés lors des importations d'intégration de vulnérabilité tierces.

Champs d'élément vulnérable d'application

À l'exception des champs **Groupe d'affectation**, **Affecté à** et **Notes**, tous les autres champs de l'AVIT sont en lecture seule.

Champ	Description
Numéro	Identificateur AVIT généré automatiquement pour cet enregistrement.
Type d'analyse	Type de scanner qui a trouvé cet AVIT. Les choix possibles sont les suivants : • Dynamique • Statique • SCA
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun. Pour en savoir plus sur les cotes de risque, reportez-vous à la section Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications.
Score du risque	Quantité calculée de risque que l'AVI pose à votre environnement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour plus d'informations, consultez Calculer automatiquement le risque dans Réponse aux vulnérabilités des applications.
Date de l'engagement de rattrapage	Date à laquelle les AVIT doivent être corrigés après leur passage dans **l'état En cours d'examen**. Ce champ s'affiche uniquement si l'AVIT est **en cours d'examen**.
Cible de remédiation	Date à laquelle les AVIT doivent être assainis, depuis leur première identification. S'affiche uniquement le cas échéant. Pour plus d'informations sur les cibles de rattrapage, reportez-vous à la section Automatiser le suivi de la cible de rattrapage dans Réponse aux vulnérabilités des applications.
Statut de la remédiation	État du rattrapage pour l'AVIT. Il est déterminé par l'AVIT avec la date d'échéance la plus proche, le cas échéant. Les États comprennent : • En cours • Cible presque atteinte • Cible passée
Nom de catégorie	Nom de la catégorie de vulnérabilité.
Vulnérabilité	ID de la vulnérabilité associée à l'élément vulnérable de cette application.
Version de l'application	Version de l'application.
Module d'application	Application affectée dans l'analyse DAST. Masqué pour les analyses SAST.
Emplacement Version 14.0 : SAST	DAST : Emplacement URL de la vulnérabilité dans l'application. SAST : chemin d'accès au fichier et numéro de ligne de la vulnérabilité dans l'application.
État	Ce champ est défini par défaut sur **Ouvert** lors de sa création. Consultez États des éléments vulnérables de l'application (AVI) pour plus d'informations sur la façon dont les états sont mappés.
Motif	[Visible uniquement lorsque l'AIV est à l'état **Fermé** .] Explication de l'état.
Groupe d'affectation	Groupe sélectionné pour travailler sur cet AVIT. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cet AVI. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec
Premier trouvé	Date à laquelle la source tierce a trouvé l'élément vulnérable de l'application pour la première fois.
Dernier trouvé	Date à laquelle la source tierce a trouvé l'élément vulnérable de l'application pour la dernière fois.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Fermé	[Visible uniquement lorsque l'AVIT est à l'état **Fermé** .] Date à laquelle l'AVI a été fermé.
Fermé par	[Visible uniquement lorsque l'AVIT est à l'état **Fermé** .] Entité qui a fermé l'AVIT.
Résumé	Description importée de la vulnérabilité.
Résultats Données en lecture seule importées d'une intégration tierce.	
ID AVIT source	Identificateur importé pour l'AVIT source.
Gravité de la source	Gravité importée à partir de l'application source.
Date de correction de la cible source	Date importée à laquelle la source s'attend à ce que l'AVIT soit corrigé.
État de l'atténuation de la source	État d'atténuation importé à partir de l'application source.
État du rattrapage de la source	État de rattrapage importé à partir de l'application source.
État du résultat de la source	[Visible uniquement lorsque le champ est renseigné] État du problème importé à partir de l'application source.
État SDLC	État du cycle de vie du développement logiciel importé.
Conforme à la politique	Statut de conformité importé. Si l'état n'est pas fourni, ce champ est défini sur **Non applicable**.
Lien source	URL de l'AVIT source.
Notes sources	Notes importées à partir de la source.
Résumé de la vulnérabilité	Résumé importé à partir de la source.
Explication de vulnérabilité	Explication importée à partir de la source.
Recommandation	Recommandation importée à partir de la source.
Références	Références importées à partir de la source.
Demande/réponse HTTP (visible uniquement pour les analyses DAST)	
Demande source	Demande HTTP
Réponse source	Réponse HTTP
Notes	
Plan de rattrapage	Détails sur la façon dont les AVIT seront corrigés. Le plan doit être mis en œuvre d'ici la **date de l'engagement de rattrapage**. Ce champ s'affiche uniquement si l'AVIT est **en cours d'examen**.
Commentaires/ notes de travail supplémentaires	Toute information pertinente. Sélectionnez la zone de texte pour les notes de travail afin d'ajouter des informations. Réponse aux vulnérabilités À partir de la version 20.0, vous pouvez ajouter des notes de travail dans la section Notes pour un élément vulnérable d'application différé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculs de l’âge pour un AVIT :

- La colonne Âge de la liste AVIT affiche la durée (format : Jours HH :MM :SS) pendant laquelle un AVIT est actif. La valeur Âge est de zéro pour un AVIT fermé.
- La colonne Âge fermé de la liste AVIT affiche la durée (format : Jours HH :MM :SS) pendant laquelle un AVI est actif avant sa fermeture. Pour les AVIT autres qu’à l’état Fermé, la valeur Âge fermé est égale à zéro.

Pour plus d’informations sur la personnalisation du calcul de l’âge et des durées d’âge fermé, consultez l’article KB1703270 .

États des tests de pénétration

Les propriétaires d’applications peuvent demander une évaluation de test de pénétration pour leurs applications et surveiller la progression de l’équipe de piratage éthique jusqu’à ce que la demande soit résolue.

La demande d’évaluation de test de pénétration passe par les états de transition suivants jusqu’à ce qu’elle soit résolue.

Étapes de la demande d’évaluation de test de pénétration

Champ	Description
États des tests de pénétration	
Ouvert	État lorsque la demande d’évaluation est créée par le propriétaire de l’application.
Définition du champ d'application	L’équipe de piratage éthique évalue la demande et le périmètre de l’application.
Préparation de l'environnement	Le propriétaire de l’application crée un environnement avec des rôles et d’autres informations et les fournit à l’équipe de piratage éthique pour test.
Test en cours	L’équipe de piratage éthique teste manuellement l’application pour identifier les conclusions du test de pénétration.
V16.1 : Test en cours	L’équipe de piratage éthique indique que des tests sont actuellement en cours. Si cet état est sélectionné, l’option **Test en suspens** devient disponible sur le formulaire.
V16.1 : Test en suspens	ce champ n’est affiché que lorsque l’état Test en cours est sélectionné. L’équipe de piratage éthique contrôle les accords sur les niveaux de service (SLA) des demandes d’évaluation de test de pénétration en sélectionnant cet état, si nécessaire. Cela garantit que les SLA précis sont signalés.
V16.1 : Test en cours de révision	L’équipe de piratage éthique indique que les tests sont terminés et en cours d’examen par un expert en la matière.
Fermé	L’équipe de piratage éthique ferme les demandes d’évaluation de test de pénétration après que les résultats du test de pénétration ont été rapportés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étapes de la demande d'évaluation de test de pénétration (suite)

Champ	Description
	Remarque : À partir de la version 16.1, vous pouvez utiliser l'option **Copier et créer une demande** sur le formulaire pour répliquer la demande à l'état Fermé et créer une nouvelle demande. Pour plus de détails, voir Répliquer une demande de test de pénétration à l'état Fermé.
V16.1 : annulé	Le propriétaire de l'application annule la demande d'évaluation du test de pénétration.
V16.1 : Brouillon	Le propriétaire de l'application crée une demande et l'enregistre en tant que brouillon avant de soumettre la demande.
États des éléments vulnérables d'applications	
Ouvert	Lorsque l'équipe de piratage éthique identifie et crée les conclusions du test de pénétration, son statut est Ouvert.
Résolu	Lorsque l'équipe d'application résout les conclusions du test de pénétration, leur état passe à Résolu. **Remarque :** Si le résultat du test de pénétration a été résolu mais doit encore être validé par l'équipe de piratage éthique, le sous-état est `Validation Pending`.
Fermé	L'équipe de piratage éthique valide que les résultats du test de pénétration ont été résolus et passe l'état à Fermé.

Gestion du mappage d'état pour les reports et les faux positifs dans Réponse aux vulnérabilités des applications

Vous pouvez gérer la façon dont les états **de la source** sur les éléments vulnérables de l'application (AVI) importés par le Veracode Vulnerability Integration et Fortify Vulnerability Integration sont mappés dans votre instance après l'importation.

À partir de la version 20.0 de , vous disposez de plus d'options Réponse aux vulnérabilités pour trier vos AVI importés avec ServiceNow des workflows.

Lorsque vous Configurez la Fortify Vulnerability Integration. ou le Configurez la Veracode Vulnerability Integration., les pages de configuration de l'intégration vous offrent deux options pour vous aider à gérer les exceptions et les faux positifs dans votre instance.

- Gérer les exceptions dans ServiceNow
- Gérer les faux positifs dans ServiceNow

Rôle requis : gestionnaire de sécurité des applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation pour la gestion des exceptions

Les AVI sont importés à partir de ces intégrations avec les états **sources** . Lors de l'importation, ces états sont mappés aux états **Cible** et Motif de la **cible** dans votre instance, car dans certains cas, il n'y a pas de correspondance exacte entre les états sources de votre scanner et les états utilisés par votre instance.

Par exemple, les états sources tels que **Ne corrigera pas**, **Rattrapage différé**, **Risque accepté** et **Risque atténué** sont Fortify Vulnerability Integration mappés à l'état **Différé** avec un sous-état **Risque accepté** ou **Contrôle d'atténuation en place dans** votre instance.

Sur les pages de configuration de ces intégrations, vous disposez des options suivantes :

Option	Case à cocher sélectionnée	Description
Gérer les exceptions dans ServiceNow	Y (par défaut)	Si vous laissez cette option sélectionnée, vous devez demander des exceptions à partir des enregistrements AVI. Les AVI importés marqués pour l'état **Différé** sont triés avec le ServiceNow workflow Gestion des exceptions. Les AVI avec des états **sources** qui sont normalement mappés à un état **Différé** sont mappés à **l'état de triage cible** dans l'état **Ouvert** .
	N	Si vous désactivez la case à cocher, vous conservez les états **Source** importés de votre scanner. Ces AVI sont mappés à **l'état Ciblecomme Différé** et à un état **de motif Cible** dans votre instance. Ils ne sont pas triés par le workflow d'exception, car ils ne sont pas mappés à l'état **de triage cible** et aux états de **motif de triage cible** . L'action d'interface utilisateur **Demander une exception** n'est pas disponible sur l'enregistrement AVI, car

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Case à cocher sélectionnée	Description
		l'enregistrement est déjà à l'état **Cible différée** .

Cas d'utilisation du faux positif

Pour les faux positifs provenant de par Veracode Vulnerability Integration exemple, les états source tels que **Faux positif** ou **Faux positif potentiel** sont mappés à l'état **Cible fermée** avec un sous-état **Faux positif**.

Option	Case à cocher sélectionnée	Description
Gérer les faux positifs dans ServiceNow	Y (par défaut)	Si vous laissez cette option sélectionnée, vous devez demander un **faux positif** à partir des enregistrements AVI. Les AVI importés marqués pour l'état **Faux positif** ou **Faux positif potentiel** sont triés avec le ServiceNow workflow Gestion des exceptions. Les AVI avec des états **sources** qui sont normalement mappés à un **état ciblefermé** sont mappés à un état **de triage cible** dans **Ouvert**. L'action d'interface utilisateur **Faux positif** est disponible sur l'enregistrement AVI.
	N	Si vous désactivez la case à cocher, vous conservez les états **Source** importés de votre scanner. Ces AVI sont mappés à **l'état Cible** en tant que **Fermé** et à l'état Motif **cible** en **Faux positif** dans votre instance. Ils ne sont pas triés par workflow de faux positif. L'action d'interface utilisateur **Faux positif** n'est pas disponible sur l'enregistrement AVI, car

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Case à cocher sélectionnée	Description
		l'enregistrement est déjà à l'état **Cible fermée** .

Références de Réponse aux vulnérabilités des applications

Les termes suivants sont utilisés dans .Réponse aux vulnérabilités des applications

Éléments vulnérables d'applications (AVI)

Appariements des entrées de vulnérabilité et des applications potentiellement vulnérables dans votre environnement d'entreprise.

Règles d'affectation

Règles utilisées pour affecter des AVI en fonction de vos critères définis.

Common Platform Enumeration (CPE)

Schéma de dénomination structuré NVD du NIST pour les systèmes, logiciels et progiciels de technologie de l'information.

Vulnérabilités et expositions communes (CVE)

Dictionnaire des vulnérabilités et des expositions en matière de sécurité de l'information connues du public.

Common Weakness Enumeration (CWE)

Liste des types de faiblesses logicielles développés par la communauté.

Intégrations

Travaux planifiés qui extraient les données de rapport de CWE ou d'un système tiers, tel que Veracode, pour récupérer des données de vulnérabilité.

> **Remarque :** Si l'intégration de la base de données des vulnérabilités nationale du Réponse aux vulnérabilités NIST dans est activée et configurée, l'enrichissement CVE est disponible pour les CWE, mais pas obligatoire. Pour en savoir plus sur l'intégration de la base de données des vulnérabilités nationale du NIST, reportez-vous à la section Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces.

Base de données de vulnérabilité nationale (NVD)

Référentiel gouvernemental des États-Unis sur les données de gestion des vulnérabilités basées sur des normes représentées à l'aide du protocole d'automatisation du contenu de sécurité (SCAP).

Règles de cibles de rattrapage

Règles utilisées pour affecter des AVI à des dates cibles pour le rattrapage en fonction des critères définis.

Calculateurs de vulnérabilités

Calculateurs utilisés pour classer par ordre de priorité et catégoriser les vulnérabilités d'applications en fonction des critères que vous avez définis.

Exemple de règle d'exception pour Réponse aux vulnérabilités des applications

Exemple de règle basée sur une vulnérabilité connue pour une règle d'exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Un nom unique pour vous aider à identifier son objectif et à localiser facilement la règle, par exemple, Veracode-1 cwe-22 exception.
État	Lecture seule : brouillon
Début de validité	Date à laquelle cette règle est active pour différer les AVI.
Ordre d'exécution	Ordre unique pour chaque règle d'exception Une valeur inférieure précède une valeur élevée.
Date de fin de validité	Date à laquelle la tâche de rattrapage arrête d'accepter de nouveaux VI.
Reporté jusqu'à	Date à laquelle les tâches de rattrapage et les AVI sont reportés. À cette date, l'AVUL est fermé, tous les AVI sortent de la tâche et sont rouverts. Les règles de groupe sont réappliquées à ces AVI.
Motif	Raison de la création de cette règle d'exception. Sélectionnez-en un dans la liste, par exemple **Correctif non disponible**.
Groupe d'affectation	Groupe affecté au suivi des VI différés, par exemple, le gestionnaire APP Sec.
Informations supplémentaires	Informations supplémentaires que le demandeur souhaite fournir à l'approbateur. Ces informations sont renseignées dans le champ Description de la tâche de rattrapage. Dans cet exemple, Différer les AVI avec la vulnérabilité – Veracode-1-22.
Condition	Conditions de filtre pour spécifier quels AVI correspondent à cette règle. Pour cet exemple, la vulnérabilité est Veracode-1-22.
Exécuter sur les données existantes	Option qui vous permet d'exécuter cette règle sur des données existantes la première fois que cette règle est exécutée. Si vous laissez cette option désactivée, votre règle s'exécute quotidiennement par la tâche *`Associate existing AVIs with Auto Exception Rule`* planifiée en commençant par de nouvelles données. Si vous activez l'option Exécuter sur les données existantes, une tâche planifiée s'exécute une fois sur les données existantes à la date de **début de validité** .

Vue du produit Réponse aux vulnérabilités des applications

Le produit Application Vulnerability Response (AVR) ingère les faiblesses et les vulnérabilités détectées par vos outils de test de sécurité des applications et fournit un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

guichet unique pour comprendre la posture de sécurité de toutes les applications de votre environnement.

AVR vous permet de réduire les risques avec les workflows de rattrapage. L'objectif de cette vue de produit est de vous aider à comprendre comment les entités clés d'AVR utilisent le cadre de travail CSDM principal.

Terminologie mise à jour

À partir d'AVR v19.0, les noms de tables et de colonnes clés suivants ont été mis à jour. Par conséquent, vous verrez des références aux noms plus anciens et plus récents dans la documentation.

Mise à jour de la liste des termes, des noms de tables et de champs pour AVR

Avant AVR v19.0	À partir d'AVR v19.0
Règles de recherche de CI	Règles de recherche
Formulaire de règle de recherche de CI	Formulaire de règle de recherche
Règle de correspondance CI	Règle de correspondance
Rechercher sur la table	Rechercher sur la table CI
Rechercher sur le champ	Rechercher sur le champ CI
Version de l'application	Applications détectées
Table de version de l'application	Table des applications détectées
Criticité opérationnelle	Criticité opérationnelle source

Prérequis

Installez les dernières versions des applications suivantes :

- Security Support Common
- Réponse aux vulnérabilités
- Cadre de travail d'intégration de sécurité
- Orchestration du support de sécurité
- Intégrations de scanners telles que Veracode et Fortify

AVR et CSDM 4.0

Avant AVR v19.0, lorsque des vulnérabilités d'application étaient ingérées, l'application pour laquelle les vulnérabilités étaient ingérées était recherchée à l'aide des règles de recherche de CI, par rapport aux applications numérisées (sn_vul_app_scanned_application). Si l'enregistrement du nom d'application n'était pas là, une entrée était effectuée.

À partir d'AVR v19.0, pour s'aligner sur le cadre de travail CSDM 4.0, les tables Modèle de produit sont utilisées à la place de la table Applications numérisées. Si l'application possède la version, la recherche s'effectue par rapport à la table Modèle logiciel. S'il n'y a pas de version, la recherche s'effectue par rapport à la table Modèle d'application. Le modèle d'application et le modèle logiciel sont tous deux des tables enfants de la table Modèle de produit, qui est la table de base dans CMDB. La capture d'écran suivante explique le modèle de produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété système

Pour utiliser le processus de recherche basé sur un modèle de produit CSDM 4.0, définissez la propriété *sn_vul.use_product_model* système sur *true*.

Considérations relatives aux propriétés système

Nom de la propriété système	Valeur de la propriété système	Valeur de la cible de recherche	Considérations
sn_vul.use_product_model	vrai	Sélectionner la valeur **Modèle de produit**	Les nouveaux utilisateurs doivent sélectionner la valeur **Modèle de produit** pour utiliser les règles de recherche de modèle de produit du cadre de travail CSDM 4.0.
	Faux	Sélectionner la valeur **Élément de configuration**	Les utilisateurs existants peuvent continuer à utiliser le processus de recherche de CI et les **règles de recherche de CI** existantes.

Remarque : Pour définir la valeur cible de recherche, accédez à la page **Règle de recherche** > **[règle de recherche d'intégration AVR]** > champ **Cible de recherche** .

Règles de recherche dans AVR

Dans le cadre de travail CSDM 4.0, les règles de recherche basées sur des modèles de produits sont utilisées à la place des règles de recherche de CI pour créer des entrées dans les classes de modèles de produits respectives. De même pour les scripts, vous pouvez définir les règles de recherche dans le cadre du modèle CSDM 4.0.

À partir d'AVR v19.0, lors de la création d'une règle de recherche, vous devez définir si vous souhaitez utiliser l'approche de l'élément de configuration ou du modèle de produit à l'aide du champ **Rechercher la cible** . Pour plus d'informations, consultez Créer une règle de recherche de CI.

Applications détectées

Accédez à la **Tous** > **Applications détectées**. La table Applications détectées affiche les applications ingérées à partir des analyseurs. Si la propriété *sn_vul.use_product_model* système est définie sur *true*, vous pouvez voir les modèles de produits correspondants pour les applications.

Considérations relatives à l'AVR

Présence d'enregistrements de modèles de CI ou de produits en double

Vérifiez que la propriété *sn_vul.use_product_model* système a été correctement configurée pour le processus de recherche. Assurez-vous de sélectionner **l'élément de configuration** ou le **modèle de produit** comme cible de recherche lors de la configuration du formulaire de règle de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

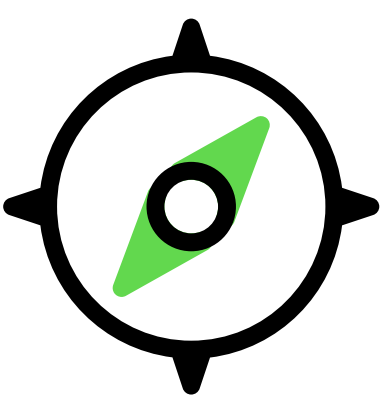
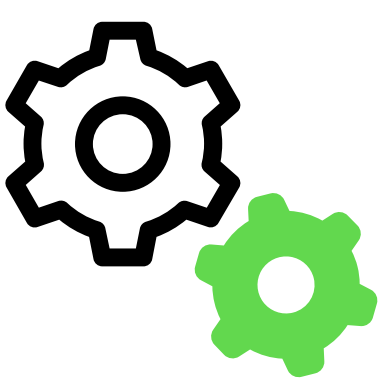
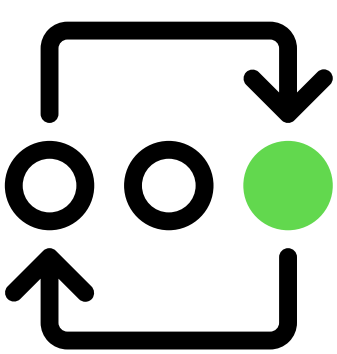
Réponse aux vulnérabilités pour conteneurs

L'application ServiceNow® Réponse aux vulnérabilités pour conteneurs importe les éléments vulnérables du conteneur (CVIT) et, en fonction des règles, vous permet de corriger les vulnérabilités du conteneur. Les données de vulnérabilité proviennent de sources internes et externes, telles que la base de données de vulnérabilité nationale (NVD) ou des intégrations tierces.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Réponse aux vulnérabilités pour conteneurs

Explorer	Configurer	Intégrer
		
Découvrez les concepts et fonctionnalités de Container Vulnerability Response.	Configurez Container Vulnerability Response.	Étendez Container Vulnerability Response en l'intégrant à d'autres applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

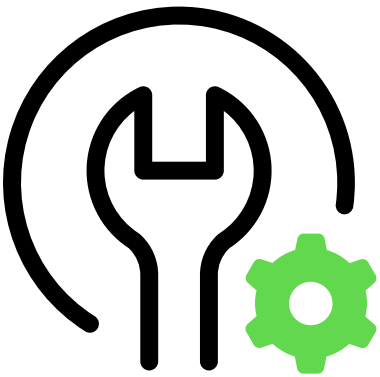
Réponse aux vulnérabilités pour conteneurs (suite)

Utiliser les espaces de travail Vulnerability Response



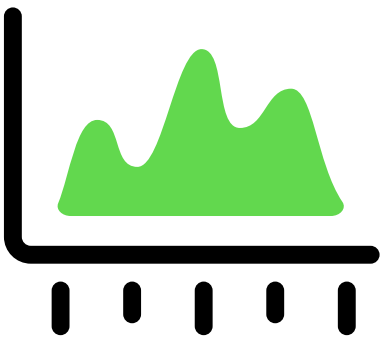
Découvrez comment surveiller, gérer et corriger les CVIT dans les espaces de travail Gestionnaire des vulnérabilités, Rattrapage informatique et Évaluation des vulnérabilités.

Corriger



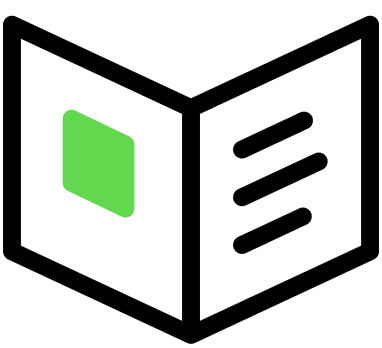
Découvrez comment corriger les vulnérabilités des conteneurs.

Analyses et rapports



Afficher l'analyse de Container Vulnerability Response

Référence



Obtenez des détails sur les composants de Container Vulnerability Response tels que les champs, les tables et les propriétés.

Traduction automatique

Avantages

L'application Réponse aux vulnérabilités pour conteneurs offre les avantages suivants :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- S’intègre à des produits de sécurité de conteneurs tiers, tels que Prisma Cloud Compute de Palo Alto Networks.
- Importe les données de vulnérabilité des images déployées pour l’exécution et enrichit les données de vulnérabilité avec des informations contextuelles d’exécution (hôtes, grappes Kubernetes, services et espaces de noms).
- Fournit une liste des références créées à partir des vulnérabilités vers les entités Kubernetes pertinentes lors de l’utilisation Base de données de gestion des configurations (CMDB)ServiceNow de Découverte Kubernetes.
- Offre un tableau de bord de génération de rapports complet, fournissant des informations sur les tendances en matière de vulnérabilité et de rattrapage.

Fonctionnalités principales

L’application Réponse aux vulnérabilités pour conteneurs gère les vulnérabilités détectées dans les conteneurs. Il fournit les fonctionnalités suivantes :

- Pointez vers l’image Docker source à partir de CVIT au lieu de conteneurs en cours d’exécution.
- Configurez la granularité des CVIT à suivre au niveau de l’image, de la grappe Kubernetes, de l’espace de noms ou du service.
- Suivez les nouvelles versions d’images pour identifier les vulnérabilités corrigées. Toutes les vulnérabilités signalées dans les anciennes versions sont automatiquement résolues lorsque ServiceNow de nouvelles versions d’image sont déployées au moment de l’exécution.
- Suivez les CVIT dans les images de base séparément des images d’application pour permettre un rattrapage indépendant.
- Émettez des demandes d’exception ou des demandes de faux positifs, qui peuvent être examinées par le biais d’un processus d’approbateur à plusieurs niveaux.
- Définissez des règles d’exception pour différer automatiquement les CVIT.

Cas d'utilisation

Les conteneurs sont un excellent moyen de déployer et de faire évoluer des applications sur plusieurs environnements avec moins de frais généraux et une portabilité accrue. Cependant, les vulnérabilités dans les images de conteneurs peuvent présenter un risque pour l’hôte sous-jacent et, en fin de compte, pour l’infrastructure où les conteneurs ont été lancés à partir de ces images. Bien qu’il existe de nombreux produits de sécurité des conteneurs qui analysent les images des conteneurs pour détecter les vulnérabilités, il existe quelques considérations et problèmes associés à la correction des vulnérabilités. Réponse aux vulnérabilités pour conteneurs peut aider à résoudre divers problèmes ou cas d’utilisation impliqués dans le rattrapage des vulnérabilités d’image de conteneur. Explorez des façons de tirer parti du Réponse aux vulnérabilités pour conteneurs module :

Contexte d'exécution

Les vulnérabilités des images de conteneurs peuvent être découvertes en analysant l’image aux étapes suivantes du cycle de vie de l’application.

- Étape 1 : lorsque les images sont en cours de construction dans le pipeline CI/CD.
- Étape 2 : Lorsque les images sont publiées dans le registre
- Étape 3 : lorsque les images sont déployées pour l’exécution.

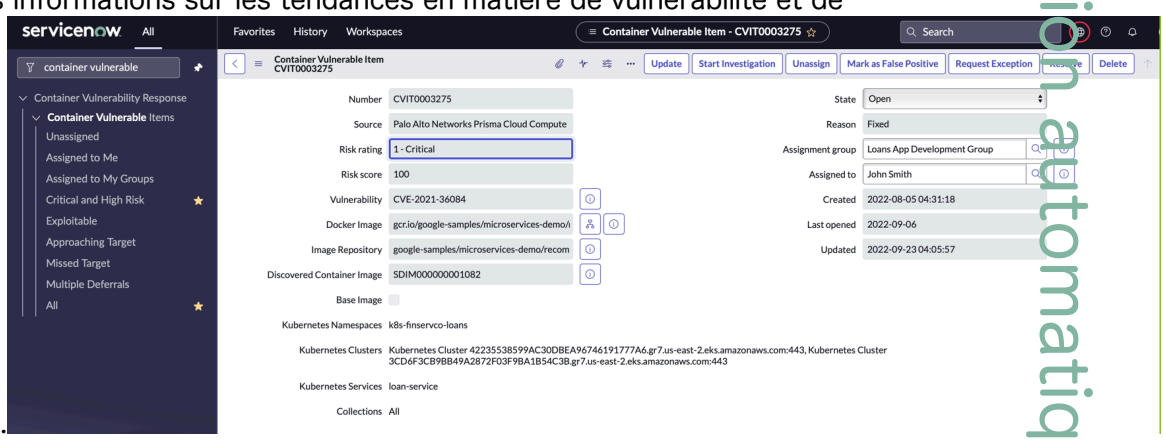
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

S’il est important d’identifier les vulnérabilités le plus tôt possible à l’étape 1 et à l’étape 2, il est tout aussi important d’effectuer une analyse des images déployées dans un environnement d’exécution. Il offre les avantages suivants :

- identifiant toutes les nouvelles vulnérabilités et expositions courantes (CVE) publiées.
- Fournir une visibilité précise de la situation vis-à-vis du risque des applications déployées.
- Classer par ordre de priorité les vulnérabilités qui doivent être résolues. Le contexte d’exécution en termes de services d’application ou de services d’entreprise affectés en raison d’une vulnérabilité peut aider à établir des priorités.

Réponse aux vulnérabilités pour conteneurs s’intègre aux produits de sécurité des conteneurs tels que Prisma Cloud Compute pour extraire les données de Palo Alto Networks vulnérabilité des images déployées dans l’exécution et enrichit les données de vulnérabilité avec les informations contextuelles d’exécution telles que les hôtes, les grappes Kubernetes, les services et les espaces de noms où ces images de conteneur sont déployées. Les clients qui utilisent la ServiceNow découverte Kubernetes peuvent voir les références créées à partir des vulnérabilités vers les entités Kubernetes pertinentes dans leur Base de données de gestion des configurations (CMDB). En plus d’enrichir les métadonnées, ServiceNow propose également un tableau de bord de reporting complet pour fournir des informations sur les tendances en matière de vulnérabilité et de rattrapage.



Traduction automatique

Identifier la propriété

Conditions préalables

- **Métadonnées et références Kubernetes** : pour Réponse aux vulnérabilités pour conteneurs renseigner les métadonnées Kubernetes (espace de noms, grappe, etc.) et les références aux Base de données de gestion des configurations (CMDB) entrées, vous devez implémenter la découverte Kubernetes à partir de Information Technology Operations Management (ITOM). La découverte Kubernetes remplit l’image Docker, les conteneurs Docker en cours d’exécution, les pods, les grappes Kubernetes, etc., dans le CMDB. Réponse aux vulnérabilités pour conteneurs identifie l’image Docker en CMDB fonction de l’ID de l’image, puis identifie les entités Kubernetes connexes et remplit les références à ces entités à partir des éléments vulnérables.

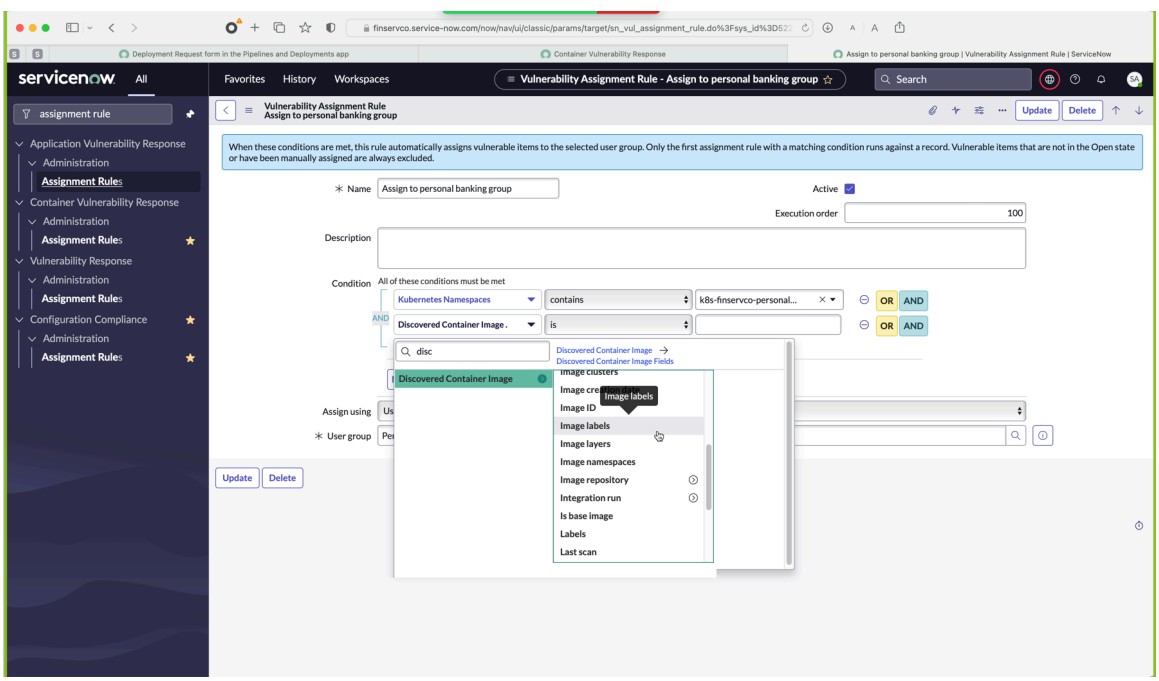
- **Métadonnées dans le cloud et étiquettes d’image Docker** : Réponse aux vulnérabilités pour conteneurs remplit également les étiquettes d’image Docker, les ID de compte dans le cloud, les régions où une image est déployée.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ces données sont conservées dans l'enregistrement « Image du conteneur détecté » associé à l'élément vulnérable. Il n'existe aucune condition préalable pour renseigner ces données. Réponse aux vulnérabilités pour conteneurs utilise les données renvoyées par les produits de sécurité des conteneurs (par exemple, Palo Alto Prisma Cloud Compute) pour renseigner ces entrées.

La propriété de la correction d'une vulnérabilité dans une image de conteneur peut varier d'une organisation à l'autre. Ces informations peuvent être saisies à différents endroits. Certaines organisations utilisent des étiquettes d'image Docker comme moyen d'identifier les équipes d'application qui possèdent une certaine image de conteneur, tandis que d'autres organisations peuvent utiliser l'espace de noms Kubernetes ou le compte cloud où une image de conteneur est déployée pour identifier le bon propriétaire.

Réponse aux vulnérabilités pour conteneurs fournit les éléments de modèle de données nécessaires pour pouvoir capturer et utiliser les étiquettes d'image Docker, les métadonnées de grappe/service/espace de noms Kubernetes ou les métadonnées du compte dans le cloud (ID de compte dans le cloud, région, fournisseur, etc.) dans le module « Règles d'affectation » et affecter automatiquement les vulnérabilités à la bonne équipe d'application en fonction des métadonnées de l'image ou de l'environnement d'exécution.



Suivre les vulnérabilités dans les images de base

Conditions préalables

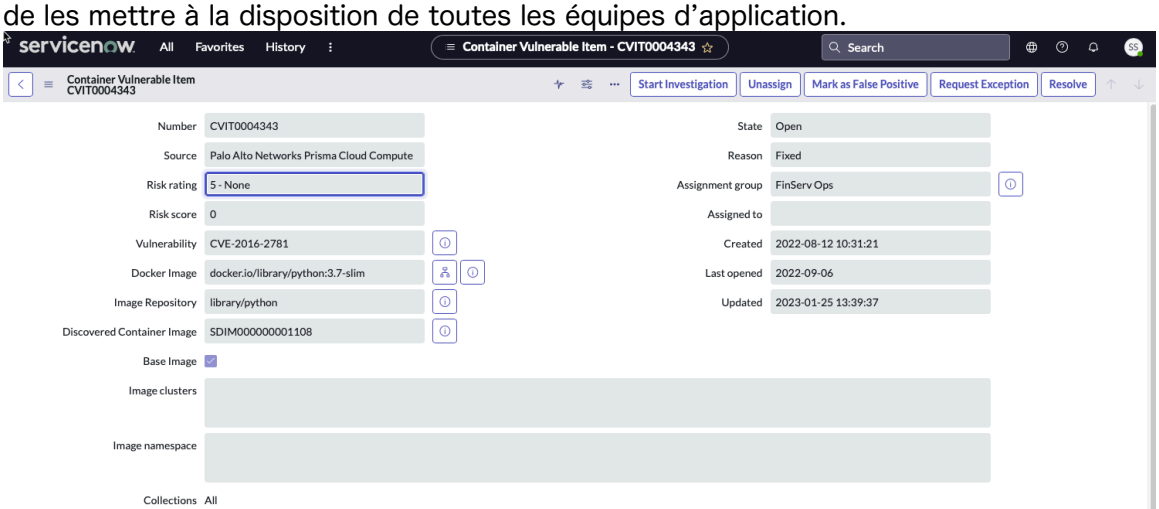
Pour que la propriété « Image de base » soit renseignée dans Réponse aux vulnérabilités pour conteneurs, les images de base doivent être configurées explicitement dans la Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute console. Pour plus d'informations sur la configuration des images de base dans Prisma Cloud, consultez https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin- compute/vulnerability_management/base_images.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités pour conteneurs Permet de créer des enregistrements de vulnérabilité distincts pour une couche de base afin qu'ils puissent être affectés à une autre équipe.

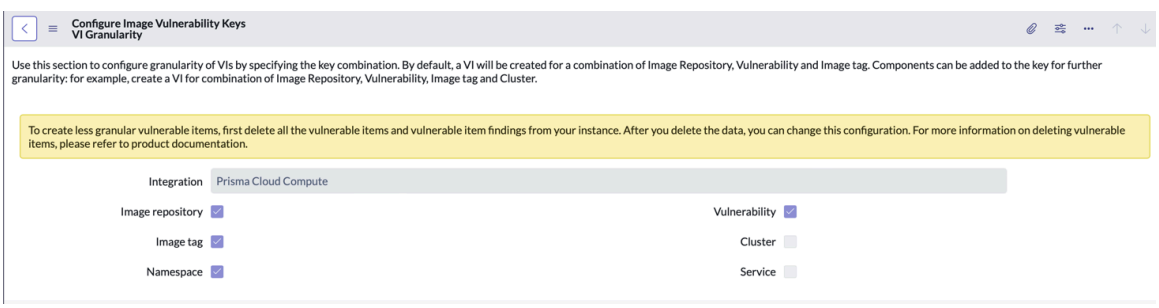
Suivez les vulnérabilités identifiées dans une image de système d'exploitation de base telle qu'Alpine à partir des vulnérabilités détectées dans d'autres couches de l'image du conteneur. De nombreuses organisations ont des équipes dédiées qui sont chargées d'appliquer des correctifs aux images du système d'exploitation de base et de les mettre à la disposition de toutes les équipes d'application.



Définir la granularité pour les éléments vulnérables

Conditions préalables

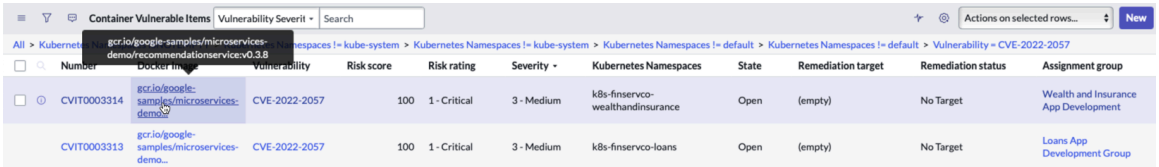
Configurez la granularité des CVIT en accédant à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Configurer la granularité VI**.



Par défaut, un élément vulnérable est créé pour chaque combinaison unique de CVE et de la version de l'image Docker (référence + balise). Toutefois, quelques images Docker peuvent être déployées dans plusieurs espaces de noms Kubernetes et chaque espace de noms peut appartenir à différentes unités ou équipes commerciales. Chaque équipe peut suivre sa propre cadence pour déployer de nouvelles versions d'images de conteneurs afin de corriger les vulnérabilités. Pour prendre en charge ce scénario, Réponse aux vulnérabilités pour conteneurs vous permet de définir la granularité des éléments vulnérables : indique si un élément vulnérable doit être créé pour chaque espace de noms/grappe/service Kubernetes, même pour chaque combinaison unique de version d'image Docker et de vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Dans l'exemple, vous pouvez voir deux éléments vulnérables créés pour la même combinaison d'image Docker et de CVE. L'un pour l'espace de noms Kubernetes 'k8s-finservco-loans' et l'autre pour 'k8s-finservco-wealthandinsurance'.

Identifier les services impactés à l'aide de l'identification des services basée sur les balises

Conditions préalables

- Identifiez les différents services dans votre application et définissez les balises/paires clé-valeur qui représentent ces services.
- Déployez des images Docker et des pods Kubernetes avec ces balises ou étiquettes.
- Déployer Découverte Kubernetes ITOM Définissez les « Services basés sur les balises » avec les balises ou les étiquettes appropriées.
- Déployer Découverte Kubernetes ITOM
- Définissez les « Services basés sur les balises » avec les balises ou les paires clé-valeur appropriées.
- Importer des données de vulnérabilité à l'aide ServiceNow de Réponse aux vulnérabilités pour conteneurs

Le calcul du risque pour les éléments vulnérables peut être effectué en examinant le CI (image Docker) et la criticité des services associés dans CMDB. Toutefois, pour faciliter l'identification des services impactés, Réponse aux vulnérabilités pour conteneurs propose une identification des services basée sur les balises.

Lorsque des pods ou des entités Kubernetes sont publiés avec des clé-valeurs ou des étiquettes correspondant aux clé-valeurs définies dans tout « Service basé sur les balises » dans ServiceNow, Réponse aux vulnérabilités pour conteneurs il établit automatiquement la relation entre une image Docker et le service d'application impacté, et utilise la criticité de ce service d'application dans le calcul des risques.

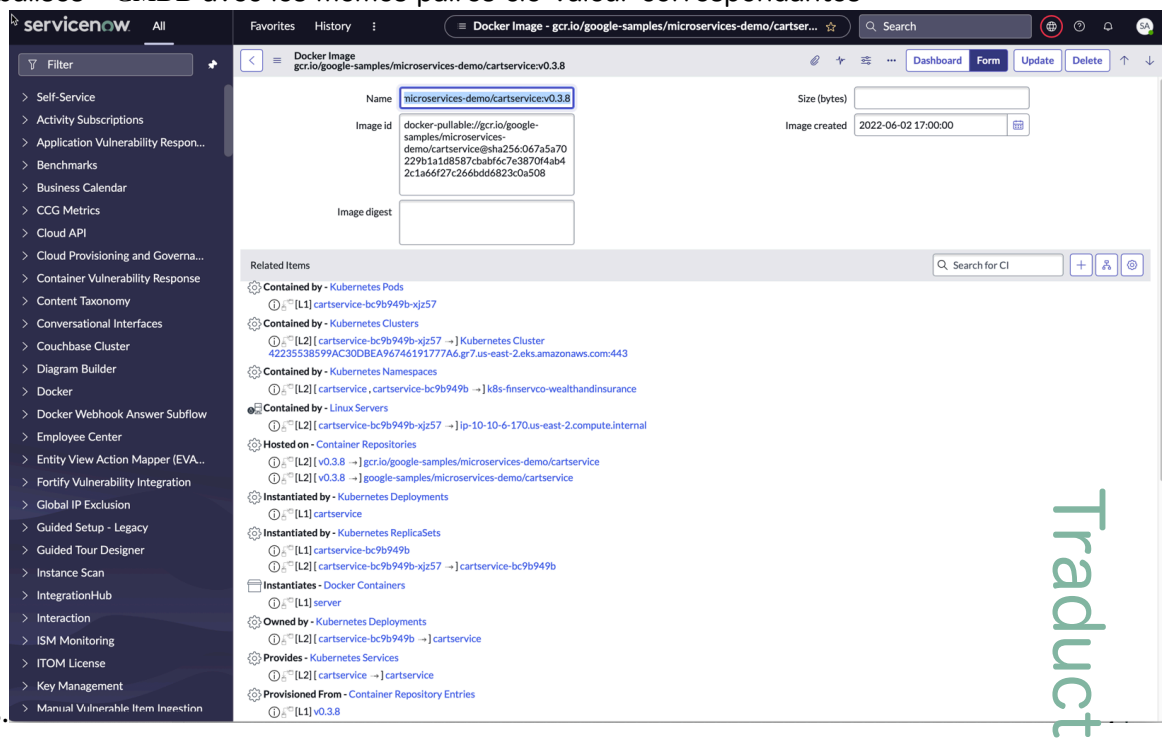
Le flux est le suivant :

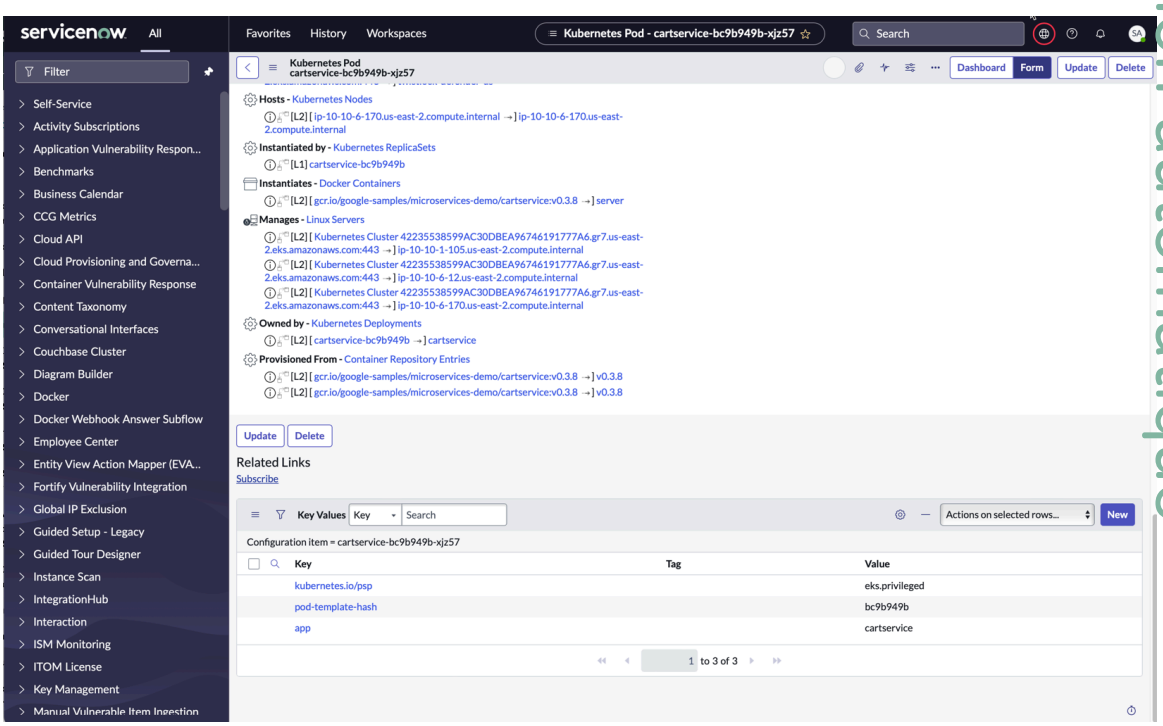
1. Réponse aux vulnérabilités pour conteneurs Importe les données de vulnérabilité à partir du produit de sécurité de conteneur.
2. Pour chaque élément vulnérable de conteneur, Réponse aux vulnérabilités pour conteneurs remplit l'image Docker à partir de CMDB laquelle présente la vulnérabilité.
3. Réponse aux vulnérabilités pour conteneurs examine ensuite les étiquettes d'image Docker ou les étiquettes/clés-valeurs publiées avec les pods Kubernetes où cette image est déployée. Cette image est disponible dans CMDB si la découverte Kubernetes est en cours d'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Réponse aux vulnérabilités pour conteneurs recherche ensuite « Services basés sur les balises » CMDB avec les mêmes paires clé-valeur correspondantes définies.

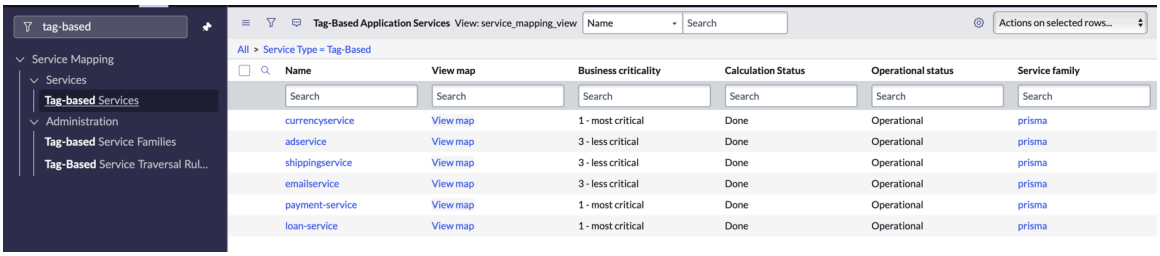


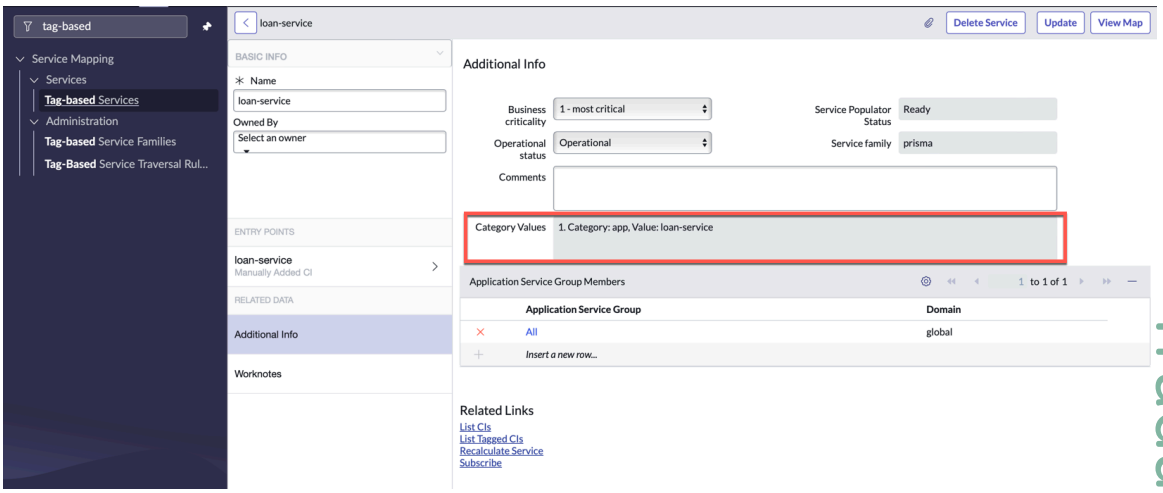


5. Réponse aux vulnérabilités pour conteneurs utilise la « criticité opérationnelle » du « service basé sur les balises » correspondant (le cas échéant) pour calculer le risque d'un élément vulnérable de conteneur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

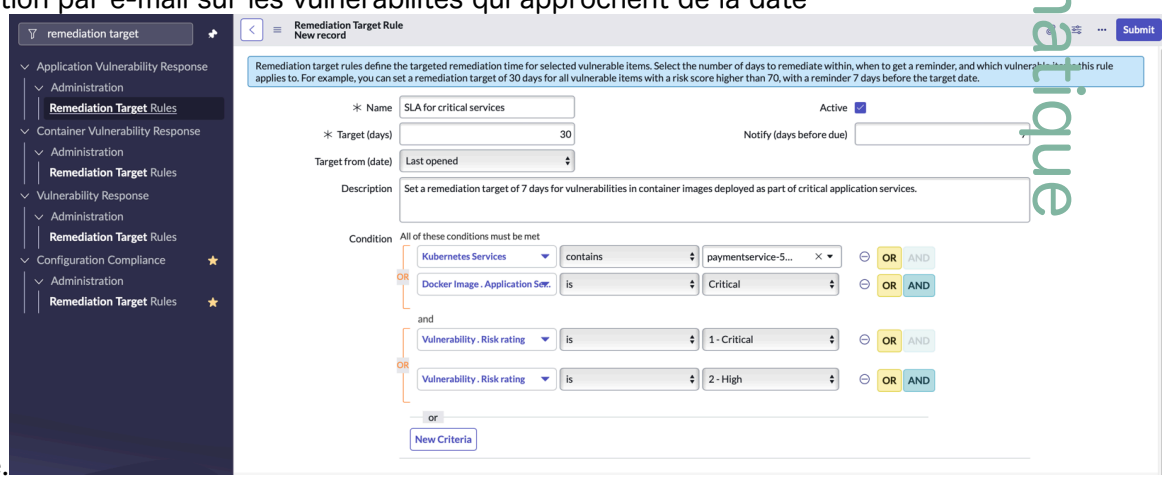




Suivi des vulnérabilités

Définition des cibles de rattrapage

ServiceNow permet aux responsables des vulnérabilités de définir des « règles de cibles de rattrapage » pour pouvoir définir des accords sur les niveaux de service (SLA) destinés à corriger les vulnérabilités trouvées dans les images des conteneurs. La date cible de rattrapage peut être définie en fonction d'une condition ou d'un critère sur les métadonnées d'image ou les informations de vulnérabilité. Les propriétaires de rattrapage reçoivent une communication par e-mail sur les vulnérabilités qui approchent de la date d'échéance.



Identification des vulnérabilités corrigées

Contrairement aux vulnérabilités d'hôte qui peuvent être corrigées en appliquant un correctif sur un hôte, les vulnérabilités des conteneurs ne peuvent pas être corrigées. De nouvelles versions d'images de conteneurs doivent être créées et déployées pour remplacer les anciennes versions. Les nouvelles versions ont un identifiant différent (ID d'image) par rapport aux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

versions précédentes, ce qui rend difficile le suivi des vulnérabilités qui ont déjà été corrigées.

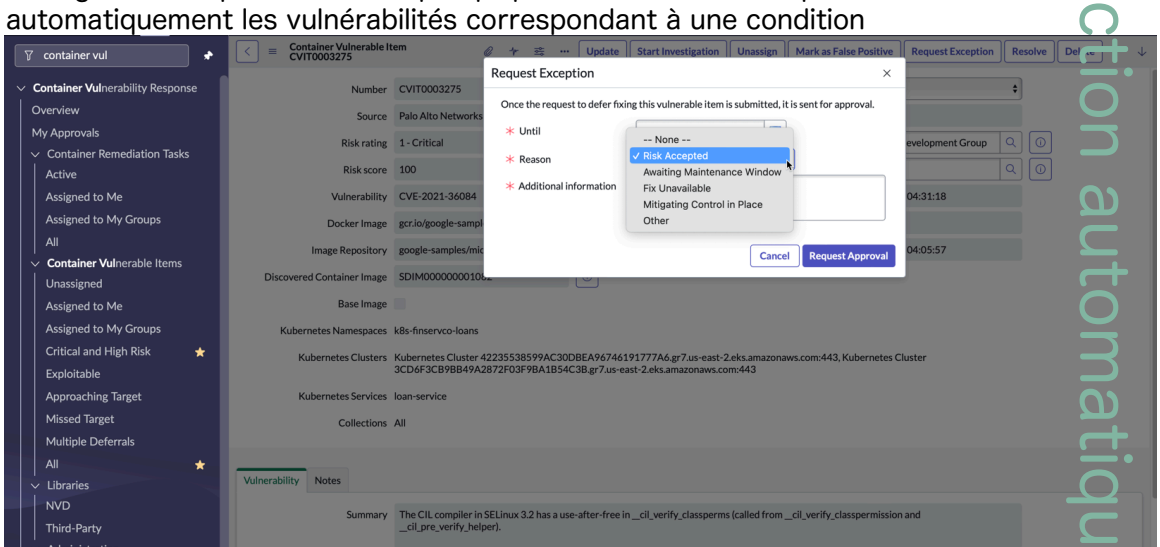
ServiceNow Identifie les vulnérabilités qui ont été signalées dans les versions précédentes des images de conteneur mais résolues dans la dernière version de l'image et déplace automatiquement ces vulnérabilités vers l'état « Fermé/Corrigé » afin que les équipes de sécurité aient toujours une visibilité précise sur la dernière situation vis-à-vis du risque.

Gérer les exceptions

Les équipes d'application ou les propriétaires de rattrapage pour les vulnérabilités peuvent avoir besoin de la possibilité de demander une exception pour les raisons suivantes.

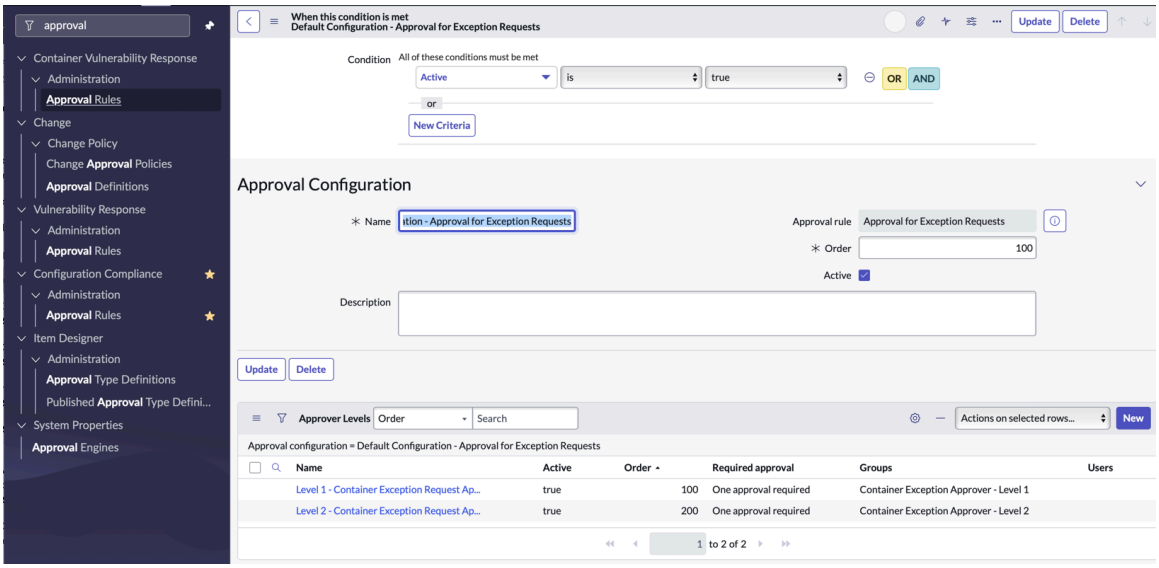
- Un contrôle d'atténuation est déjà en place
- Risque accepté
- En attente d'une fenêtre de maintenance pour pousser le correctif.

ServiceNow Permet aux administrateurs de sécurité de définir plusieurs niveaux d'approbateurs pour les demandes d'exception. Vous pouvez également définir des règles d'exception automatique qui peuvent être utilisées pour différer automatiquement les vulnérabilités correspondant à une condition donnée.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Nouveautés

Pour en savoir plus sur les nouveautés et les changements dans Zurich, consultez les notes de Zurich publication.

Premiers pas

- Pour obtenir une vue d'ensemble de Opérations de sécurité dans votre ServiceNow AI Platform instance, consultez Présentation des opérations de sécurité.
- Pour en savoir plus sur toutes les Opérations de sécurité applications disponibles au téléchargement à partir de , ServiceNow Store consultez Opérations de sécurité et ServiceNow Store.

Explorer Réponse aux vulnérabilités pour conteneurs

L'application Réponse aux vulnérabilités pour conteneurs importe les éléments vulnérables de conteneur (CVIT). Selon les règles, la fonctionnalité vous permet de corriger les vulnérabilités des conteneurs. Réponse aux vulnérabilités pour conteneurs est disponible via un abonnement séparé.

Contrairement aux applications traditionnelles, les conteneurs regroupent tous les codes sources des applications ainsi que leurs dépendances dans un fichier binaire appelé image de conteneur. L'image est publiée dans un registre pour fournir une option permettant d'exécuter cette image en tant qu'application ou instance de conteneur sur n'importe quelle plateforme. Les étapes d'un cycle de vie de pré-déploiement de conteneur sont les suivantes :

1. Composer l'image du conteneur : l'image du conteneur est composée et pointe vers un code source ou une bibliothèque dépendante.
2. Créer l'image du conteneur
3. Publier l'image du conteneur : le fichier d'image du conteneur est publié dans un registre. Chaque image a son propre ID unique basé sur le contenu de l'image. Ces images sont extraites du registre vers l'environnement d'exécution en mode post-déploiement. Les images s'exécutent ensuite en tant qu'instances de conteneur sur l'hôte dans l'environnement de production.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyse des images du conteneur

Une image de conteneur peut être analysée pour détecter les vulnérabilités avant ou après le déploiement. Si les images de conteneurs sont analysées pendant la phase de pré-déploiement, vous risquez de recevoir de nombreuses alertes de vulnérabilité, qui peuvent ne pas nécessiter votre attention immédiate. Cependant, l'analyse des vulnérabilités pendant la phase post-déploiement offre des avantages supérieurs, tels que les suivants :

- Fournir une visibilité sur le risque associé aux applications déployées.
- Fournir une vue ciblée uniquement sur les images dans l'environnement de production.
- Identifier et classer par ordre de priorité les vulnérabilités qui doivent être traitées immédiatement.
- Regroupement et affectation des vulnérabilités en fonction des métadonnées de l'image. Par exemple, un référentiel d'images, une étiquette d'image et d'autres attributs associés à l'image du conteneur peuvent être utilisés pour les règles de regroupement et d'affectation.

Chaque image de conteneur comporte les composants clés suivants :

- Référentiel de conteneurs ou d'images : représente l'image de Docker avec un référentiel ou un nom donné. Il héberge toutes les versions de l'image.
- Image de Docker : représente une version spécifique de l'image de Docker de la version.
- Conteneur Docker : représente une instance en cours d'exécution de l'image Docker. Chaque version a un ID unique et comporte plusieurs instances des conteneurs en cours d'exécution dans l'environnement de production.

Réponse aux vulnérabilités pour conteneurs modules

Le Réponse aux vulnérabilités pour conteneurs module fournit des détails sur les points suivants :

Éléments vulnérables de conteneurs

Les éléments vulnérables de conteneur (CVIT) sont regroupés et répertoriés en fonction de leur affectation, de leur criticité, de leur exploitabilité et de leur état de rattrapage.

Bibliothèques

Accédez à la base de données de vulnérabilité nationale (NVD) et aux bibliothèques tierces. Alors que la bibliothèque NVD fournit des informations limitées à l'ID de l'élément de vulnérabilité, la bibliothèque tierce fournit la plupart des détails sur un élément de vulnérabilité. Les informations de l'écran NVD ne sont renseignées que lorsque l'intégration NVD est déclenchée.

Administration

Le module Administration fournit des informations sur les règles d'affectation des éléments vulnérables, les règles de cible de rattrapage et les intégrations de vulnérabilité des conteneurs. En outre, vous pouvez également configurer la durée après laquelle un élément vulnérable doit être fermé automatiquement. Vous pouvez utiliser la section Configurer la granularité VI pour configurer la granularité des CVIT en spécifiant les combinaisons de clés. Par défaut, une CVIT est créée pour une combinaison d'un référentiel d'images, d'une balise d'image et d'une vulnérabilité. Vous pouvez ajouter des composants supplémentaires à la clé pour une granularité supplémentaire. Par exemple, vous pouvez créer une CVIT pour une combinaison de référentiel d'images, de balise d'image, de vulnérabilité et de cluster.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles

Version de mise en production	Notes de publication
Réponse aux vulnérabilités pour conteneurs v2.1 Réponse aux vulnérabilités pour conteneurs v2.06 Réponse aux vulnérabilités pour conteneurs v2.0.4	Notes de version de Container Vulnerability Response Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response .

Réponse aux vulnérabilités pour conteneurs États de la tâche de rattrapage et des éléments vulnérables du conteneur

Avec l'application Réponse aux vulnérabilités pour conteneurs , vous pouvez utiliser le modèle d'état pour voir l'état d'une tâche de rattrapage, à un moment donné. Savoir comment chaque état est lié et s'affecte les uns les autres vous aide à déterminer quand et comment corriger vos éléments vulnérables de conteneur (CVIT).

États des tâches de rattrapage

Les cas d'utilisation complexes peuvent parfois entraîner un élément vulnérable de conteneur dans un état différent de celui de sa tâche de rattrapage. Comprendre le fonctionnement des états permet d'expliquer ce comportement et peut aider à créer des tâches de rattrapage et à créer ou modifier des règles de tâche de rattrapage.

Les tâches de rattrapage ont de nombreux états possibles, comme illustré dans le diagramme suivant.

Flux d'état de Vulnerability Response de conteneur

Remarque :

- Les éléments vulnérables du conteneur ne peuvent pas être fermés manuellement.
- Chaque formulaire de tâche contient des boutons **Suivre** et **Mettre à jour** standard pour ServiceNow les tâches.

Tâche de rattrapage et ordre de priorité d'état et de CVIT

Les états des tâches de rattrapage et des éléments vulnérables peuvent s'affecter mutuellement. La plupart du temps, un état de tâche de rattrapage met à jour l'état de l'élément vulnérable, l'état de tâche de priorité le plus élevé étant utilisé pour mettre à jour les éléments vulnérables du groupe.

De la création à la fermeture d'une tâche de rattrapage de conteneur, celle-ci passe par différents états au cours de l'ensemble du processus de rattrapage.

La priorité des États est la suivante :

Fermé > **Différé** > **Résolu** > **En cours de révision** > **En attente d'implémentation** > **En cours d'examen** > **Ouvert**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La transition d'état se produit lorsque vous effectuez diverses actions telles que Différer, Ouvrir, Fermer, etc.

Les actions que vous pouvez effectuer sur une tâche de rattrapage de conteneur à un état spécifique sont similaires à celles d'une tâche de rattrapage d'hôte. Par conséquent, pour plus d'informations, consultez le Réponse aux vulnérabilités États des tâches de rattrapage et Scénarios de déploiement et de réduction de l'état dans la Réponse aux vulnérabilités documentation.

Configurer Réponse aux vulnérabilités pour conteneurs

Avant d'exécuter Réponse aux vulnérabilités pour conteneurs dans votre ServiceNow AI Platform instance, vous devez la configurer.

Installer Vulnerability Response et Configuration Compliance pour conteneurs

Avant d'exécuter l'application dans votre ServiceNow AI Platform instance, vous devez obtenir une Vulnerability Response et Configuration Compliance pour conteneurs autorisation et télécharger l'application à partir du ServiceNow Store. Installez l'application sur votre ServiceNow AI Platform instance et effectuez quelques étapes d'installation dans l'assistant de configuration.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Tâches de configuration	Description
Vérifiez que l'application est installée et activée.	Pour vérifier qu'il est activé, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Si l'application n'est pas installée et activée, Installer Réponse aux vulnérabilités reportez-vous à la section .
Vérifiez que les rôles requis ServiceNow sont affectés à votre instance.	Le rôle administrateur est requis pour l'installation. S'il n'est pas déjà affecté, l'administrateur système [admin] affecte également le rôle d'administrateur de vulnérabilité, sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)].

Rôle requis : admin

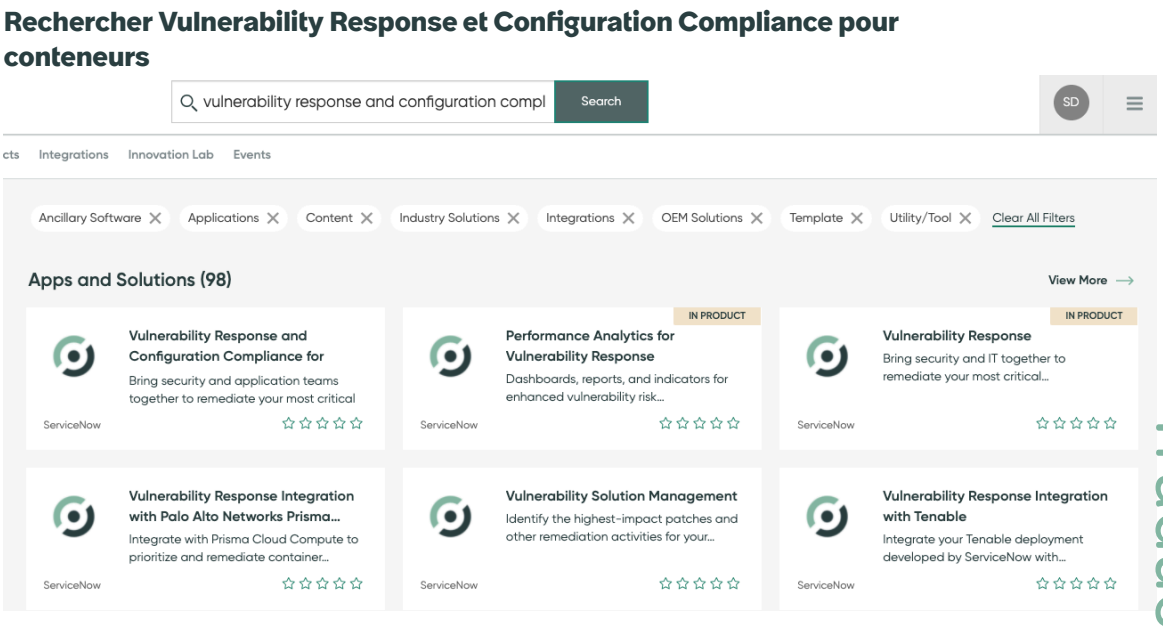
Procédure

1. Pour obtenir une autorisation et télécharger l'application Vulnerability Response et Configuration Compliance pour conteneurs , accédez au ServiceNow Store.
2. En haut à droite de la page, cliquez sur **Se connecter**.

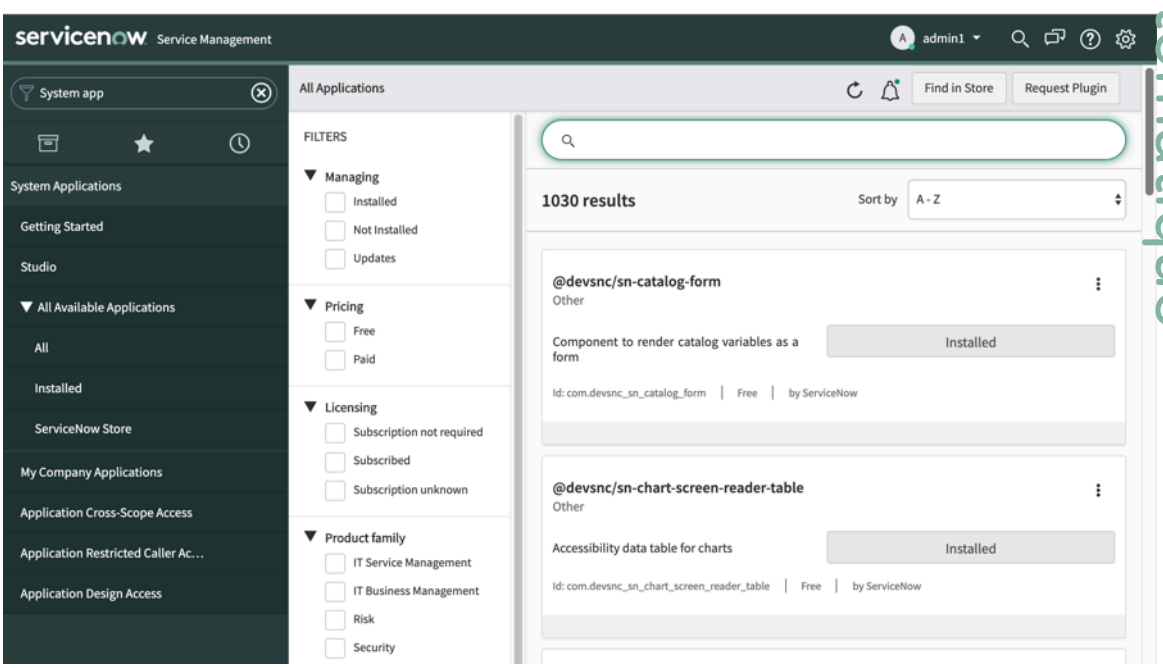
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la barre de recherche, tapez Vulnerability Response et Configuration Compliance pour conteneurs.
4. Sous Applications et solutions, cliquez sur la Vulnerability Response et Configuration Compliance pour conteneurs vignette.



5. Cliquez sur **Demander l'installation**.
6. Connectez-vous à l'instance ServiceNow AI Platform sur laquelle vous souhaitez installer l'application Vulnerability Response et Configuration Compliance pour conteneurs .
7. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous**.



8. Dans les applications répertoriées, localisez l'application Vulnerability Response et Configuration Compliance pour conteneurs , sélectionnez une version dans la liste, puis cliquez sur **Installer**.
   La boîte de dialogue d'installation de l'application s'affiche. Toutes les dépendances installées s'affichent.
9. Cliquez sur **Fermer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir les Réponse aux vulnérabilités pour conteneurs notifications par e-mail

Configurez des notifications par e-mail pour partager des informations utiles sur les mises à jour et les activités importantes, telles que l'approbation et le rejet de demandes de faux positif. La création d'une notification par e-mail implique de spécifier quand l'envoyer, qui la reçoit et ce qu'elle contient.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Modèles d'e-mail**.
2. Sélectionnez **Nouveau**.

   Pour obtenir des instructions détaillées sur la création de notifications par e-mail, reportez-vous à la section Créer une notification par e-mail .

Résultats
À partir de la version 21.0 de , lorsqu'un Réponse aux vulnérabilités destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités ou Espace de travail de remédiation IT en fonction de son rôle.

- Des liens s'ouvrent pour les Espace de travail du gestionnaire de vulnérabilités utilisateurs disposant des rôles sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin.
- Des liens s'ouvrent dans le pour les utilisateurs disposant de Espace de travail de remédiation IT rôles, sn_vul_container.remediation_owner.

Si le destinataire ne possède aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Créer ou modifier des notifications de cible de rattrapage

Les administrateurs de vulnérabilité peuvent modifier la notification de cible de rattrapage ou en ajouter de nouvelles, en spécifiant quand envoyer la notification, qui reçoit la notification et quel contenu contient la notification.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Notifications**.
2. Sélectionnez l'enregistrement de notification de la cible de rattrapage ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Pour plus d'informations sur les champs de formulaire, consultez Créer une notification par e-mail .
4. Sélectionnez **Afficher l'aperçu** de la notification pour afficher le message.

Résultats
À partir de la version 21.0 de , lorsqu'un Réponse aux vulnérabilités destinataire clique sur les liens d'une notification par e-mail, les enregistrements s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités ou Espace de travail de remédiation IT en fonction de son rôle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Des liens s'ouvrent Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs disposant des rôles sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin.
- Des liens s'ouvrent pour les utilisateurs dotés de Espace de travail de remédiation IT rôles, sn_vul_container.remediation_owner.

Si le destinataire ne possède aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Configurer la gestion des exceptions pour Réponse aux vulnérabilités pour conteneurs

Limitez la durée d'une exception demandée et ajoutez un questionnaire à la demande d'exception ou de faux positif à l'aide du Réponse aux vulnérabilités pour conteneurs module. Par défaut, une exception est demandée à l'aide du ServiceNow® Réponse aux vulnérabilités pour conteneurs module. Vous pouvez également demander une exception à l'aide de l'intégration GRC : Gestion de la politique et de la conformité .

Avant de commencer

Rôle requis : sn_vul_container.manage_exception_configuration

Pourquoi et quand exécuter cette tâche

Si Réponse aux vulnérabilités pour conteneurs cette option est activée, vous pouvez limiter la durée pendant laquelle une exception peut être demandée. De même, si le GRC : Gestion de la politique et de la conformité module est installé, vous pouvez sélectionner GRC : Gestion de la politique et de la conformité sur l'écran de configuration. L'activation de cette option vous permet de demander une exception qui spécifie l'objectif de politique et de contrôle à partir de GRC.

Si vous ajoutez un questionnaire, il est envoyé à la personne qui émet la demande d'exception ou de faux positif. Vous pouvez utiliser le questionnaire par défaut ou en créer un en fonction de vos besoins. .

Il est utile que l'approbateur d'exceptions comprenne la raison de la demande d'exception.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Configuration **de gestion de l'exception** , sélectionnez la façon dont vous souhaitez gérer une exception en sélectionnant une option dans la liste **Gérer les exceptions à l'aide** . Vous pouvez sélectionner soit Réponse aux vulnérabilités ou GRC : Gestion de la politique et de la conformité.
3. Si vous avez sélectionné l'option Réponse aux vulnérabilités , saisissez les informations suivantes :

Réponse aux vulnérabilités champs

Champ	Description
Durée	Période pour laquelle une exception peut être demandée.
Unité	Unité de temps pour la période spécifiée.
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Activer le questionnaire pour demander une exception	Option permettant d’ajouter un questionnaire à la demande d’exception en cours d’émission.
Questionnaire pour demander une exception	Affiche le questionnaire que vous avez sélectionné pour demander une exception. Le questionnaire d’exceptions s’affiche par défaut.

Remarque : Lorsque vous sélectionnez GRC : Gestion de la politique et de la conformité, les champs Durée et Unité disparaissent en tant que Gouvernance, risque et conformité gestionnaires de ce flux.

4. Sélectionnez **Enregistrer**.

Configurer les règles d’approbation pour la gestion des exceptions

Réponse aux vulnérabilités À partir de la version 15.0, utilisez le concepteur de flux pour approuver les demandes d’exception pour la gestion des exceptions, les règles d’exception et la gestion des faux positifs. Si vous déployez Réponse aux vulnérabilités (VR) pour la première fois, Flow Designer est activé par défaut.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Pour utiliser Flow Designer, créez des règles à l’aide du module Règles d’approbation. À l’aide de ce module, vous pouvez configurer des règles d’approbation pour chacun des workflows de gestion des exceptions suivants.

- Demande d’exception pour les tâches de rattrapage
- Demande d’exception pour les éléments vulnérables du conteneur
- Règle d'exception
- Faux positif pour les tâches de remédiation
- Faux positif pour les éléments vulnérables du conteneur

Vous pouvez également définir des conditions contenant plusieurs niveaux d’approbation dans une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d’approbation correspondant.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles d'approbation**.
2. Sur la page Règles d’approbation, sélectionnez le groupe pour lequel vous souhaitez définir la règle d’approbation.
3. Remplissez les champs du formulaire.

Formulaire Règle d'approbation

Champ	Description
Nom	Nom de configuration de l’approbation.
Table	Table sur laquelle la règle est appliquée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	La valeur par défaut est Réponse aux vulnérabilités.
Type de règle	Spécifie le type de règle. Par exemple, gestion des exceptions, faux positifs ou règle d'exception.
Actif	Activé par défaut, ce qui signifie que la règle d'approbation est utilisée.
Description	Brève description des règles d'approbation.
Expirationde l'approbation (jours) À partir de la v2.5 de Réponse aux vulnérabilités pour conteneurs	Date jusqu'à laquelle l'approbateur peut approuver la demande.
Notification de l'approbateur (jours) À partir de la v2.5 de Réponse aux vulnérabilités pour conteneurs	Date après laquelle l'approbateur est notifié pour effectuer des actions.

4. Sélectionnez **Mettre à jour**.
   Dans l'onglet Configurations d'approbation, deux niveaux d'approbateurs sont configurés par défaut. Vous pouvez sélectionner une règle pour définir les conditions en fonction de différents cas d'utilisation au sein d'une règle. Pour plus d'informations, consultez Créer des configurations pour une règle d'approbation.

   Remarque : Dans chaque page de configuration, vous pouvez créer plusieurs niveaux d'approbation. Pour plus d'informations, consultez Créer des niveaux d'approbation pour la gestion des exceptions.

Example:
En fonction de différents cas d'utilisation, vous pouvez définir différents processus d'approbation pour les mêmes vulnérabilités trouvées dans différents éléments de configuration.

Tests de démarrage rapide pour Réponse aux vulnérabilités pour conteneurs

Validez que Réponse aux vulnérabilités pour conteneurs fonctionne toujours après avoir apporté un changement de configuration telle que l'application d'une mise à niveau ou le développement d'une application. Copiez et personnalisez ces tests de démarrage rapide à effectuer lorsque vous utilisez des données spécifiques à votre instance.

La propriété d'exécution de test est désactivée par défaut pour empêcher l'exécution de tests sur un système de production. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production. Pour Exécuter la suite de tests Framework de tests automatisés (ATF) pour Réponse aux vulnérabilités plus d'informations sur la configuration et l'exécution de la suite de tests pour Réponse aux vulnérabilités pour conteneurs.

Les tests de démarrage rapide Réponse aux vulnérabilités pour conteneurs nécessitent l'activation de l'application Réponse aux vulnérabilités pour conteneurs (sn_vul_container).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux vulnérabilités pour conteneurs

Test	Description	Version de mise en production
CVR : Règles d'affectation	Déterminez si un exemple d'ensemble de règles d'affectation peut affecter automatiquement des éléments vulnérables de conteneur à un groupe d'affectation à des fins de correction.	Vancouver
CVR : Règle d'exception	Testez les règles d'exception	Vancouver
CVR : Flux Marquer comme faux positif	Vérifiez si le flux Marquer comme faux positif fonctionne sur l'élément vulnérable de conteneur.	Vancouver
CVR : Règles de cibles de remédiation	Créez une règle de cible de rattrapage.	Vancouver
CVR : Flux de demande d'exception	Vérifiez si le flux de demande d'exception fonctionne comme prévu.	Vancouver
VR : Calculateurs de vulnérabilité	Testez les calculateurs de vulnérabilité du conteneur.	Vancouver

Information associée

Tests de démarrage rapide

Exécuter la suite de tests Framework de tests automatisés (ATF) pour Réponse aux vulnérabilités pour conteneurs

Exécutez la suite de tests Framework de tests automatisés (ATF) après avoir installé ou mis à niveau l'application Réponse aux vulnérabilités pour conteneurs .

Avant de commencer

Confirmez que l'installation a réussi et que votre instance fonctionne comme prévu.

La propriété d'exécution de test est désactivée par défaut pour empêcher l'exécution de tests sur un système de production. Exécutez des tests uniquement sur les instances de développement, de test et autres instances de non-production. Si des données de démonstration ou des comptes de démonstration sont créés, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production.

- Pour activer le test, procédez comme suit :
  1. Accédez à la **Tous** > **Framework de tests automatisés (ATF)** > **Administration** > **Propriétés**.
  2. Si elle n'est pas cochée, cochez la case **Activer l'exécution du test/de la suite de** tests.
  3. Cliquez sur **Enregistrer**.
  4. Si le champ d'application n'est pas défini sur **Conteneur Vulnerability Response** dans l'en-tête, ou s'il n'est pas affiché dans l'en-tête, cliquez sur l'icône des paramètres.
  5. Dans la fenêtre Paramètres système, cliquez sur **Développeur**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Si elle n'est pas sélectionnée, cliquez sur **Afficher le sélecteur d'application dans l'en-tête** et fermez la fenêtre.
7. Dans la liste qui s'affiche en regard de Administrateur système, cliquez sur **Conteneur Vulnerability Response** pour le champ.

Rôle requis : admin ou atf_test_admin

Procédure

1. Accédez à la **Tous** > **Framework de tests automatisés (ATF)** > **Tests**.
2. Dans la liste Package, recherchez **Réponse aux vulnérabilités et Configuration Compliance pour les conteneurs**.
3. Sélectionnez un test pour ouvrir l'enregistrement.
4. Dans l'enregistrement ouvert, cochez la case **Actif** .
5. Dans la liste connexe à Étapes de test, sélectionnez vrai dans la colonne Actif.
6. Cliquez sur **Mettre à jour**.
7. Ouvrez à nouveau le test et cliquez sur **Activer l'exécution des tests et de la suite de tests ici**.
8. Activez les propriétés de test/suite de tests et les propriétés de débogage des tests.
9. Cliquez sur **Enregistrer**.
10. Si le bouton Exécuter le test ne s'affiche pas, **actualisez** votre écran, ouvrez à nouveau l'enregistrement et cliquez sur **Exécuter le test** pour démarrer le test.
    Après quelques instants, la boîte de dialogue Exécuter le test indique un test réussi. Cliquez sur **Accéder au résultat pour plus d'informations** .

Que faire ensuite

Félicitations ! Vous pouvez poursuivre votre configuration de Réponse aux vulnérabilités pour conteneurs.

Pour plus d'informations sur les tests automatisés et Réponse aux vulnérabilités pour conteneurs les tests automatisés, les suites de tests et la création de tests automatisés, consultez Infrastructure de tests automatisés (ATF).

Intégrer Réponse aux vulnérabilités pour conteneurs avec d'autres applications

Étendre les options en Réponse aux vulnérabilités pour conteneurs les intégrant à d'autres applications.

Réponse aux vulnérabilités pour conteneurs s'intègre aux produits de sécurité des conteneurs pour extraire les données de vulnérabilité des images qui sont déployées pour l'exécution. Il enrichit ensuite les données de vulnérabilité avec les informations contextuelles d'exécution telles que les hôtes, les clusters Kubernetes, les services et les espaces de noms où ces images de conteneur sont déployées. Avec la découverte Kubernetes de ServiceNow, vous pouvez voir les références créées à partir des vulnérabilités vers les entités Kubernetes pertinentes dans votre Base de données de gestion des configurations (CMDB). En plus d'enrichir les métadonnées, ServiceNow propose également un tableau de bord de génération de rapports complet pour fournir des informations sur les tendances en matière de vulnérabilité et de rattrapage.

Réponse aux vulnérabilités pour conteneurs fournit des intégrations avec les applications suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Intégration Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute
- Présentation de l'intégration Atlassian Jira avec Réponse aux vulnérabilités
- Présentation de l'intégration de vulnérabilité Tenable

- **Important :** Dans l'espace de travail du gestionnaire de vulnérabilités, vous pouvez créer manuellement un problème Agile à l'aide de l'action de liste et de l'action de formulaire pour suivre le rattrapage des CVIT et des RT.

Remarques supplémentaires sur les intégrations

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 2.1.2 de Réponse aux vulnérabilités pour conteneurs, des horodatages (pulsations) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Intégration Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

L'intégration Prisma Cloud Compute vous permet d'analyser les images de conteneurs pour détecter les vulnérabilités.

À partir de la version 23.0 de , Réponse aux vulnérabilités vous pouvez utiliser les Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute dans l'application Réponse aux vulnérabilités pour conteneurs pour importer les vulnérabilités sur les hôtes en cours d'exécution. Les API hôtes Prisma permettent de récupérer des informations complètes sur les vulnérabilités d'un hôte spécifique et fournissent également un instantané des vulnérabilités de l'hôte à un moment précis. Cette API permet une synchronisation régulière entre Prisma et l'instance ServiceNow. Comme Prisma est proposé à la fois en tant que logiciel en tant que service (SaaS) et en tant que solution sur site, l'utilisation d'un serveur MID est nécessaire pour appeler les API Prisma à partir de l'instance ServiceNow.

À partir de la version 16.1 de , Réponse aux vulnérabilités vous pouvez utiliser le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute dans l'application Réponse aux vulnérabilités pour conteneurs pour importer des données de vulnérabilité d'image de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

conteneur pour les conteneurs déployés. Vous pouvez ensuite afficher les rapports sur les vulnérabilités et les éléments vulnérables sur les tableaux de Réponse aux vulnérabilités bord. Ces vulnérabilités peuvent ensuite être classées par ordre de priorité et corrigées.

Si le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute produit et votre ServiceNow AI Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID. Pour plus d'informations, consultez Configuration système requise pour le Serveur MID .

Affichage des intégrations

Vous pouvez afficher les intégrations qui font partie du Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute. Pour afficher les intégrations, accédez à **Tous** > **Intégration des calculs dans le cloud Prisma** > **Intégrations**.

Les intégrations suivantes sont disponibles.

Séquence d'exécution	Planifier	Intégration	Description
1	Quotidien	Intégration des images de base de calcul dans le cloud Prisma	Récupère les vulnérabilités pour les images de base à partir de l'API Prisma et signale séparément les vulnérabilités des images de base. Il crée également des résultats d'images et des éléments vulnérables, qui pointent vers les images de base.
2	Quotidien	Intégration des vulnérabilités de calcul dans le cloud Prisma	Récupère les vulnérabilités du conteneur. Crée des résultats, des éléments vulnérables de conteneur (CVIT) et des images de conteneurs détectés.
3	Sur demande	Nombres de conteneurs de calcul dans le cloud Prisma Intégration des nombres	Récupère les nombres de conteneurs pour chaque image autre que de base.
4	Quotidien	Intégration du registre de calcul dans le cloud Prisma	Récupère les résultats d'images statiques obtenus à partir de l'analyse du registre Prisma et les ingère dans Réponse aux vulnérabilités pour conteneurs.

Configuration d'image de base dans Prisma

Dans la console Prisma, vous pouvez configurer le registre, puis configurer les images de base à partir de ces registres. Si une vulnérabilité est présente dans l'image de base, lorsque vous exécutez l'intégration des images de base de calcul dans le cloud Prisma, la case Image **de base** est cochée, indiquant que les vulnérabilités sont présentes dans l'image de base.

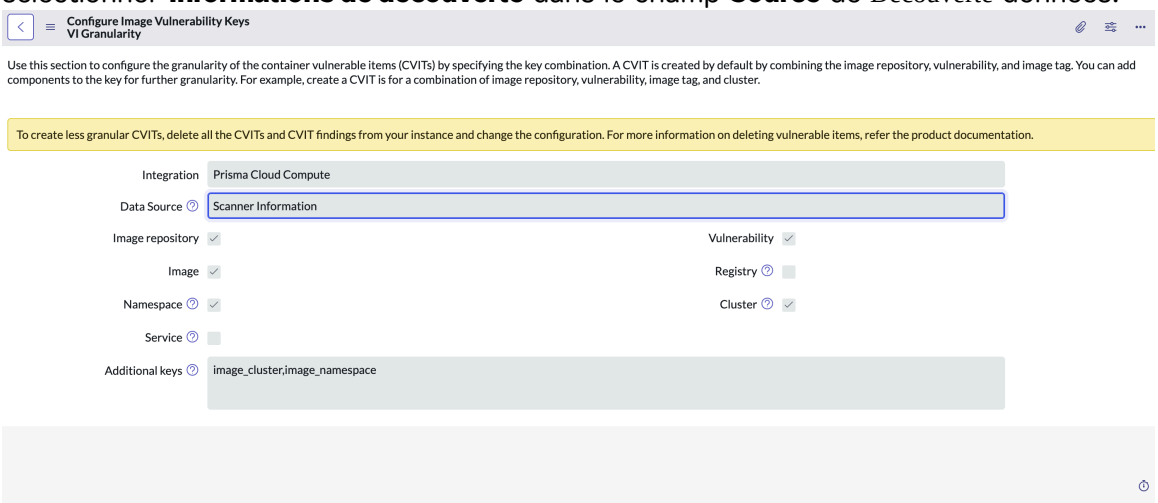
Configurer la granularité VI basée sur le CVR

Pour configurer la granularité des CVIT, accédez à **Tous** > **Intégration des calculs dans le cloud Prisma** > **Configurer la granularité VI en fonction du CVR** et spécifiez les combinaisons de touches. Par défaut, une CVIT est créée pour une combinaison de référentiel d'images, d'image et de vulnérabilité. Vous pouvez ajouter des composants supplémentaires à la clé pour une granularité supplémentaire. Par exemple, vous pouvez créer une CVIT pour une combinaison de référentiel d'images, d'image, de vulnérabilité et de cluster.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 2.12.1 de Réponse aux vulnérabilités pour conteneurs, vous pouvez également configurer la granularité des éléments vulnérables de conteneur (CVIT) à l'aide des informations du registre et des sources de données. Les informations relatives à l'espace de noms et à la grappe sont reçues à la fois du scanner et Découverte de . Si vous souhaitez obtenir ces informations uniquement à partir de , vous pouvez sélectionner **Informations de découverte** dans le champ **Source** de Découverte données.



Selon la source de données choisie, vous pouvez afficher des images ou des informations Kubernetes liées à un enregistrement CVIT.



Si les **informations du scanner** sont sélectionnées, l'enregistrement CVIT affiche **les champs de grappes d'images** et **d'espace de noms d'images** .

Si Informations **sur la découverte** est sélectionnée, l'enregistrement CVIT affiche **les grappes Kubernetes et les** champs d'espace de **noms Kubernetes** .

Processus d'intégration Prisma

Lors de l'exécution Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute , il vérifie s'il existe une vulnérabilité et une exposition communes (CVE) dans la table Base de données de vulnérabilité nationale (NVD). Si elles sont déjà présentes, les informations existantes sont utilisées. Toutefois, si le CVE n'est pas trouvé, des enregistrements d'espace réservé sont générés dans la table NVD. Lors de la création de ces enregistrements NVD d'espace réservé, seuls le CVE et son nom sont initialement renseignés. D'autres détails ne sont pas renseignés en supposant que l'intégration NVD les renseigne ultérieurement. Si le paramètre *update_nvd* d'instance d'intégration est défini sur vrai, les enregistrements NVD de l'espace réservé sont mis à jour. Par défaut, le paramètre d'instance est défini sur false. Toutefois, au moins jusqu'à ce que l'intégration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

NVD s'exécute et renseigne ces détails, une certaine compréhension des CVE, tels que sa gravité ou d'autres détails sur le problème est nécessaire. Pour répondre à cette exigence, les champs **Exploit existent** et les **notes de rattrapage** sont renseignées avec les détails obtenus à partir de Prisma. De plus, cette configuration est personnalisable, ce qui vous permet de spécifier tous les autres champs que vous souhaitez renseigner dans l'entrée NVD en fonction des informations fournies par Prisma.

Préparation pour le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

Vous pouvez vous préparer en effectuant des Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute tâches de configuration.

Avant de commencer

Pour installer et configurer l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute , vous pouvez imprimer la liste de vérification suivante. Vérifiez que les éléments énumérés sont terminés avant d'installer l'application et importez les données de vulnérabilité dans votre ServiceNow AI Platform® instance.

Liste de vérification de la préparation de l'intégration

Tâche	Description
☐	Vérifiez que vous disposez des ensembles d'informations suivants : • URL de base de l'API • Nom d'utilisateur et mot de passe. Ces informations d'identification sont utilisées pour extraire les vulnérabilités de l'intégration Prisma Cloud Compute. Pour plus d'informations, voir https://pan.dev/compute/api/ **Remarque :** Serveur MID est facultatif. Les informations d'identification de l'utilisateur utilisées pour l'intégration de Prisma Cloud Compute ont besoin d'une autorisation pour surveiller les images. Consultez le code suivant : `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Si elle n'est pas déjà installée et activée, installez l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour plus d'informations sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration requiert la version 16.1 ou Réponse aux vulnérabilités ultérieure.
☐	Obtenez les autorisations et téléchargez l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute sur votre ServiceNow AI Platform® instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
☐	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance ou si vous avez besoin d'aide, contactez ServiceNow l'assistance technique.
☐	Vérifiez que vous disposez des groupes ou utilisateurs suivants pour gérer les intégrations et corriger les éléments vulnérables : **administrateur** Installez l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute. S'il n'est pas affecté, l'administrateur affecte le rôle d'administrateur de vulnérabilité du conteneur (sn_vul_container.vulnerability_admin) et d'autres rôles. **sn_vul_container.vulnerability_admin** Termine la configuration de l'intégration des calculs dans le cloud Prisma. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités pour conteneurs (CVR) et à ses enregistrements. Cet administrateur configure les intégrations et les règles dans Réponse aux vulnérabilités pour conteneurs. **Groupe de réponse aux vulnérabilités** Par défaut, le groupe Vulnerability Response est disponible. Les utilisateurs affectés au groupe Réponse aux vulnérabilités héritent de sn_vul.read_all sn_vul_container.read_all. **Groupe propriétaire du rattrapage de conteneur** Par défaut, le groupe propriétaire du rattrapage de conteneurs est disponible. Les utilisateurs affectés à ce groupe héritent du sn_vul_container.remediation_owner. Le propriétaire de rattrapage de conteneur corrige les vulnérabilités des conteneurs qui lui sont affectées ou qui sont affectées à un groupe auquel il appartient. **Analyste de vulnérabilité** Les utilisateurs affectés au groupe d'analystes de vulnérabilité de conteneur héritent de sn_vul.vulnerability_analyst. L'analyste de vulnérabilité surveille le rattrapage de tous les éléments vulnérables. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance. Pour plus d'informations, consultez Créer un groupe d'utilisateurs .
☐	Installez l'intégration Réponse aux vulnérabilités avec NVD et exécutez l'API d'intégration de la base de données des vulnérabilités nationale du NIST (CVE UNIQUEMENT).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous êtes prêt à Configurer l’application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute.

Installer Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

Avant d’exécuter l’intégration sur votre instance, effectuez les étapes d’installation et de configuration afin que le produit Prisma Cloud Compute s’intègre correctement à Réponse aux vulnérabilités et Réponse aux vulnérabilités pour conteneurs. Cette application est disponible sous forme d’abonnement distinct.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l’installation. Ces tâches d’installation sont nécessaires pour une installation et une configuration fluides.

Remarque : Ce processus s’applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n’est pas nécessaire d’obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Rôle requis : admin

Procédure

1. Connectez-vous à l’instance sur laquelle vous souhaitez installer le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute .
2. Accédez au ServiceNow Store.
3. Dans , ServiceNow Store recherchez une Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute application.
4. Cliquez sur la miniature de l'application.
   Vous obtenez des informations détaillées sur l'application que vous allez installer.

   Remarque : Lisez les sections **Autres exigences** et **dépendances** , au besoin.

5. Cliquez sur **Demander l'application** et saisissez vos identifiants de connexion Now Support.
6. Cliquez sur **Télécharger**.
7. Mettez à jour le **nom de l’instance** et la **raison d’être des champs Instance** , puis cliquez sur **Valider l’instance**.
8. Cliquez sur **Demander**.
   Vous recevez un e-mail contenant des instructions d'installation détaillées.
9. Accédez à la **Applications système** > **Applications**.
10. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.

Résultats

Votre application est automatiquement installée sur votre instance.

Que faire ensuite

Configurez le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute pour votre environnement. Consultez Configurer l’application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

Installez et configurez l'application Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute . Importez des données à partir de Prisma Cloud Compute. Vous pouvez utiliser les données importées pour classer par ordre de priorité et corriger les vulnérabilités de vos images et hôtes Docker.

Avant de commencer

Rôle requis : admin

Procédure

1. Ouvrez l'e-mail que vous avez reçu au sujet de ServiceNow l'intégration.
2. Connectez-vous à votre instance en tant qu'administrateur.
3. Suivez les instructions dans l'e-mail pour obtenir le Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute.
4. Accédez à la **Tous** > **Intégration des calculs dans le cloud Prisma** > **Administration** > **Configuration**.
   Renseignez les champs du formulaire Configuration de calcul dans le cloud Prisma. Pour plus d'informations, consultez Formulaire Configuration des calculs dans le cloud Prisma.
5. Dans la liste Projets, sélectionnez **Tous les projets** ou **Projets spécifiques** pour configurer respectivement tous les projets ou les projets sélectionnés.
   Si vous sélectionnez **Projets spécifiques**, vous pouvez sélectionner les projets dans la liste Disponibles.
6. Pour terminer la configuration, sélectionnez **Terminer** ou **Enregistrer et tester les informations d'identification**.
   - Si vous avez configuré un projet, sélectionnez **Terminer**.
   - Si vous n'avez pas configuré de projet, sélectionnez **Enregistrer et tester les informations d'identification**
7. Affichez l'instance nouvellement créée en accédant à **Intégration des calculs dans le cloud Prisma** > **Administration** > **Instances d'intégration**.
8. Affichez les projets que vous avez configurés précédemment en sélectionnant **Paramètres d'instance d'intégration**.
9. Exécutez l'instance d'intégration nouvellement créée pour importer les données suivantes :
   - Images Docker : répertorie les images Docker, qui sont créées à l'aide d'un moteur Identification et réconciliation (IRE). Chaque image Docker fournit également des informations sur la relation entre les référentiels et les versions installées.
   - Images du conteneur détectées : le module Images du conteneur détectées fournit des informations sur l'ID de l'image, l'image Docker et le référentiel d'images. Il stocke également les informations de la couche et les associe à l'image découverte. Vous pouvez également afficher les projets et le nombre de conteneurs ici. Pour une image de conteneur détectée, vous pouvez afficher les métadonnées dans le cloud telles que le fournisseur dans le cloud, la région du cloud, l'ID de compte dans le cloud et les ID de ressources dans le cloud.
   - Packages d'images de conteneurs : fournit des informations sur les packages où se trouvent les vulnérabilités. Les détails du package binaire sont également fournis sous forme de valeurs séparées par des virgules.
   - Couches d'images du conteneur : cet écran affiche l'enregistrement de chaque couche d'image.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Conclusions d'images de conteneurs : cet écran affiche la liste des conclusions ainsi que des informations sur les vulnérabilités associées, la couche d'images, l'image de Docker, le référentiel d'images et l'image détectée. Actuellement, les informations de vulnérabilité sont limitées à l'ID. Les informations supplémentaires sont renseignées lorsque l'intégration de la base de données de vulnérabilité nationale (**NVD)** est déclenchée.
- Éléments vulnérables de conteneurs : chaque résultat a une vulnérabilité correspondante. Les CVIT sont ensuite créés en fonction de la granularité.

10. Configurer la granularité d'un élément vulnérable.

a. Accédez à la **Tous** > **Intégration des calculs dans le cloud Prisma** > **Configurer les clés de vulnérabilité de l'image**

b. Configurez la granularité des CVIT en cochant les cases requises.
Les éléments vulnérables sont créés en fonction des clés sélectionnées lors de l'importation suivante.

> **Remarque :** Par défaut, une CVIT est créée pour une combinaison de référentiel d'images, de vulnérabilité et de balise d'image. Vous pouvez ajouter des composants à la clé pour plus de granularité. Par exemple, vous pouvez créer une CVIT pour une combinaison de référentiel d'images, vulnérabilité, balise d'image et grappe. Une fois les éléments vulnérables ou les conclusions d'éléments vulnérables créés, les cases ne sont plus modifiables.

Explorer l'intégration de vulnérabilité du Wiz conteneur

Importez les données de vulnérabilité du conteneur avec l'intégration de vulnérabilité du Wiz conteneur incluse dans l'intégration Wiz Réponse aux vulnérabilités .

Wiz Vue d'ensemble de l'intégration de vulnérabilité du conteneur

L'intégration Wiz de vulnérabilité de conteneur importe les vulnérabilités d'image de conteneur identifiées par le scanner de Wiz vulnérabilité. Importez des données pour vous aider à identifier, classer par ordre de priorité et affecter des vulnérabilités de conteneurs à corriger avec les workflows automatisés de l'instance de plateforme IA ServiceNow.

Les résultats sont mappés aux éléments vulnérables de conteneur (CVIT) pour prendre en charge les workflows de triage, de hiérarchisation des risques et de rattrapage ciblé pour les charges de travail basées sur des conteneurs.

Pour plus d'informations sur les autres intégrations incluses dans les étapes d'intégration et d'installation Wiz Réponse aux vulnérabilités et de configuration, reportez-vous à la section Présentation de Wiz Réponse aux vulnérabilités l'intégration.

Rattrapage des vulnérabilités des conteneurs

La surveillance du rattrapage est un processus qui commence par l'état d'examen et se termine par la fermeture des éléments vulnérables de conteneur (CVIT). Réponse aux vulnérabilités pour conteneurs offre des outils et des procédures pour rendre ce processus plus productif et efficace.

Réponse aux vulnérabilités pour conteneurs Règles du calculateur

Les calculateurs de vulnérabilité automatisent le calcul des valeurs initiales pour les champs des éléments vulnérables du conteneur. La condition de chaque calculateur est évaluée dans l'ordre, et le premier calculateur correspondant est utilisé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher et créer des calculateurs de vulnérabilité, accédez à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Calculateurs de vulnérabilités**.

Le Réponse aux vulnérabilités pour conteneurs système de base comprend deux calculateurs de vulnérabilité qui définissent le score de risque de base sur l'élément vulnérable du conteneur. Les groupes de calculateurs suivants sont disponibles dans le système de base :

- Gravité de la vulnérabilité : calcule le score du risque pour les éléments vulnérables en utilisant la gravité de vulnérabilité normalisée.
- Calculateur de risque par défaut : il est basé sur la règle de risque.

Remarque : À partir de la version 2.10 de Réponse aux vulnérabilités pour conteneurs, en cas de :

- **Règle du calculateur de risque par défaut** : chaque fois que le score de risque d'un élément vulnérable de conteneur (CVIT) change, les détails suivants sont documentés dans la section Notes du CVIT :
  - Nom du groupe de calculateurs
  - Nom du calculateur
  - Valeurs de champ dont la pondération est supérieure à 1 et dont la contribution au score de risque est supérieure à 1.
  - Score de risque final
- **Règle de risque de gravité** de la vulnérabilité : chaque fois que le score de risque est mis à jour sur une CVIT, la section **Notes** est mise à jour avec les détails suivants :
  - Nom du groupe de calculateurs
  - Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre crochets. Pour modifier ou afficher la base de la règle du calculateur, sélectionnez une règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. **Si Modèle** est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si **Script** est sélectionné, vous pouvez ajouter ou mettre à jour le script existant. La propriété `sn_sec_cmn.risk_score_changes_add_worknotes` système permet de renseigner la section des notes de travail. À partir de la version 2.12.2 de Réponse aux vulnérabilités pour conteneurs, la propriété `sn_sec_cmn.risk_score_changes_add_worknotes` système est inactive par défaut. Si vous l'activez, vous pouvez alors voir tous les changements liés au score de risque d'un élément vulnérable de conteneur dans la section Notes de travail. En outre, les notes de travail ne sont mises à jour qu'en cas de changement du score de risque.

Poids du score de risque de vulnérabilité

Toutes les vulnérabilités se voient attribuer un score de risque et une cote de risque en fonction de facteurs tels que la gravité, la criticité, les informations sur l'exploitation, et ainsi de suite. La règle `Update Risk Rating from Risk Score` métier sur la table des éléments vulnérables du conteneur est responsable du calcul de la cote de risque. Chaque fois que le score de risque change, la cote de risque est calculée et renseignée sur les éléments vulnérables du conteneur. Avant la version 17.1 de l'application Réponse aux vulnérabilités (VR), les cotes de risque suivantes étaient fournies dans le cadre du script include VulnerabilityUtils, qui étaient codées en dur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur (cote de risque)	Poids (score de risque)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

À partir de la version 18.0 de Réponse aux vulnérabilités,

- Les types de cote de risque sont expédiés dans la table de base Poids du score de risque [sn_sec_cmn_risk_scorew_weights] comme cvr_risk_rating. Ces types sont transmis dans le cadre des règles métier ou des includes de script sur chaque table où la cote de risque est calculée.
- Le script a été modifié afin que vous puissiez interroger les entrées dans les valeurs de la table Poids du score de risque pour le calcul de la cote de risque.
- Ajoutez des entrées supplémentaires pour un type existant ou créez-en un nouveau. Lorsque vous créez un nouveau type, assurez-vous d'ajouter les étiquettes pour la nouvelle cote de risque et de modifier les scripts et les règles métier associés. Vous devez également ajouter un nouveau style pour le nouveau score de risque.
- Modifiez le script pour interroger les enregistrements dans la table de base.

Vous pouvez accéder à la table des pondérations des scores de risque en saisissant sn_sec_cmn_risk_score_weight dans le navigateur de filtre.

En outre, le score de risque est automatiquement recalculé dans les scénarios suivants :

- Lorsqu'un élément de configuration (CI) passe d'un mode non accessible sur Internet à un élément accessible sur Internet.
- Lorsque les vulnérabilités et expositions communes (CVE) ou les entrées tierces (TPE) associées sur les éléments de vulnérabilité (VI) sont liées à une vulnérabilité d'exploitation connue (KEV) CVE.

Pour plus d'informations, consultez Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.

Réponse aux vulnérabilités pour conteneurs Règles d'affectation

Définissez les critères selon lesquels les éléments vulnérables de conteneur sont automatiquement affectés à un groupe d'affectation pour le rattrapage.

Pour créer et afficher des règles d'affectation pour les éléments vulnérables de conteneur, accédez à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles d'affectation**. Lorsque vous créez une règle d'affectation, vous pouvez définir les conditions. Lorsque ces conditions sont remplies, la règle affecte automatiquement les éléments vulnérables de conteneur au groupe d'utilisateurs sélectionné. Seule la première règle d'affectation avec une condition correspondante s'exécute sur un enregistrement. Pour en savoir plus sur les règles d'affectation, reportez-vous à la section Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation .

Rôles requis : sn_vul_container.manage_assignment_rules pour définir et mettre à jour les règles et sn_vul_container.container_reapply pour réappliquer les règles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 2.13, des champs pour les informations du scanner ont été ajoutés aux enregistrements de la table Image de conteneur détectée [sn_vul_container_image]. Vous pouvez utiliser les valeurs suivantes comme conditions lorsque vous créez ou mettez à jour vos règles d'affectation pour les éléments vulnérables d'image de conteneur (CVIT) afin de vous aider à suivre la propriété dans vos environnements de conteneur.

- ID de comptes dans le cloud
- Espaces de noms d'images
- Registre
- Hôtes
- Étiquettes
- Statut (statut du fournisseur pour une vulnérabilité résolue)

Remarque : Cette valeur de la table Recherche d'image de conteneur [sn_vul_container_image_findings] fait référence à la version dans laquelle une vulnérabilité a été résolue, par exemple, Corrigée dans la version 6.2.1. Cette valeur est importée à partir de .Intégration Vulnerability Response integration with Palo Alto Networks Prisma Cloud Compute

Remarque : Les éléments vulnérables de conteneur (CVIT) qui ne sont pas à l'état Ouvert ou qui ont été affectés manuellement sont toujours exclus des règles d'affectation. Si vous ajoutez des valeurs pour ces champs de scanner à vos règles d'affectation et que vous réexécutez vos règles, les éléments vulnérables ne sont pas réaffectés, sauf si le type d'affectation est Règle. Les éléments de type manuel ne sont pas pris en compte par les règles d'affectation.

Important : En tant qu'administrateur et analyste des vulnérabilités, vous pouvez obtenir les dernières affectations pour les CVIT sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités. Cette méthode est plus efficace que la réapplication des règles d'affectation pour tous les CVIT dans l'interface classique utilisateur, ce qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Réponse aux vulnérabilités pour conteneurs Règles de cibles de rattrapage

Les règles de cibles de rattrapage définissent le délai prévu pour le rattrapage d'un élément vulnérable de conteneur (CVIT). Ces règles sont similaires à la façon dont les SLA fournissent un délai pour corriger la vulnérabilité elle-même.

Pour créer et afficher des règles de cibles de rattrapage pour les vulnérabilités de conteneur, accédez à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles de cibles de remédiation**.

Les règles de cibles de rattrapage définissent le temps de rattrapage cible pour les éléments vulnérables de conteneur (CVIT) sélectionnés. Définissez une date limite pour le rattrapage de la vulnérabilité en sélectionnant le nombre de jours pour le rattrapage. Définissez un rappel pour le rattrapage et définissez les éléments vulnérables du conteneur auxquels la règle s'applique. Vous pouvez définir une cible de rattrapage pour les jours pendant lesquels elle doit être corrigée, ainsi qu'un rappel avant d'approcher de la date cible. Pour plus d'informations, consultez Réponse aux vulnérabilités Règles de cibles de rattrapage.

Important : En tant qu'administrateur et analyste de vulnérabilité, vous pouvez obtenir la dernière date cible de rattrapage pour les CVIT sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités. Cette méthode est plus efficace que l'exécution des règles de cibles de rattrapage pour tous les CVIT dans l'interface classique utilisateur, qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des exceptions dans Réponse aux vulnérabilités pour conteneurs

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive publiée en matière de gestion des vulnérabilités ou de sécurité, vous pouvez demander une exception. La gestion des exceptions implique de demander, de réviser, d'approuver ou de rejeter les exceptions à un élément vulnérable de conteneur (CVIT) qui ne peuvent pas être corrigées conformément à la politique.

Certaines vulnérabilités de conteneur (CVIT) peuvent ne pas avoir de correctif, de correctif ou de solution existant. Lorsqu'une exception est approuvée, cela signifie également que vous acceptez un risque, car vous reconnaissez et acceptez les conséquences d'une non-correction de la vulnérabilité.

Cycle de vie d'une exception

Définition d'une exception

Une exception est une demande de différer le rattrapage d'une CVIT ou d'un RT pour une période spécifiée. Par exemple, en tant que propriétaire de rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour une machine.

Demande d'exception

En tant que propriétaire du rattrapage, vous pouvez demander une exemption pour un CVIT ou un RT à l'aide du processus de gestion des exceptions. Une fois que l'approbateur d'exception a approuvé cette demande, le CVIT ou le RT passe à un état **Différé** .

Approbation d'une demande d'exception

Les CVIT ou les RT qui ne peuvent pas être corrigés immédiatement sont examinés par des analystes de vulnérabilité, évalués pour le risque et approuvés pour le report jusqu'à ce qu'ils puissent être corrigés. L'approbation d'une demande d'exception peut être un workflow à deux niveaux. Si seul l'approbateur de premier niveau est présent, l'exception peut être demandée et approuvée. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Consultez Ajouter un approbateur d'exception pour plus d'informations.

Remarque :

À partir de la version 15.0, si vous déployez l'application VR pour la première fois, le concepteur de Réponse aux vulnérabilités flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et les faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Une fois qu'une demande d'exception pour une CVIT ou une RT est approuvée, vous pouvez effectuer les actions suivantes :

- Rouvrir
- Supprimer
- Mettre à jour les champs Affectation à ou **Groupes d'affectation**

Suivi d'une demande d'exception

Après avoir déclenché l'exception, vous pouvez suivre son état à l'aide de l'onglet **Approbations de changement d'état** du CVIT ou du RT. Si une action est effectuée sur un RT, vous ne pouvez pas suivre l'état des CVIT individuels dans ce RT.

Expiration d'une demande d'exception

Lorsqu'une demande d'exception pour une CVIT ou une RT particulière expire, la CVIT ou la RT impactée revient à son état **Ouvert** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si une seule CVIT ou tous les CVIT d'un RT réussissent lors de l'analyse suivante, les CVIT et, le cas échéant, le champ **État** RT passent à **Fermé** avec le sous-état **Corrigé**.

Configurer les règles d'approbation

Affichez et configurez les règles d'approbation en accédant à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles d'approbation**. Demandez une exception pour les CVIT qui ne peuvent pas être corrigés ou différés immédiatement, en identifiant les vulnérabilités, les éléments de configuration (CI) ou les CVIT impactés. Automatisez le processus de report de la CVIT. Différez les CVIT correspondants en fonction de ces règles lorsque le système identifie ces CVIT.

Les règles d'approbation suivantes sont expédiées par défaut :

- Approbation des demandes d'exception : une configuration par défaut avec deux niveaux d'approbation est fournie dans le système de base. Chaque fois qu'il existe une demande d'exception sur un élément vulnérable, la demande d'approbation est envoyée aux utilisateurs ou groupes présents au niveau 1. Une fois approuvé par les approbateurs de niveau 1, il est envoyé aux approbateurs de niveau 2.

  Remarque : Vous pouvez modifier les niveaux par défaut et les modifier au besoin. À partir de Réponse aux vulnérabilités pour conteneurs la version 2.0.6, vous pouvez utiliser les propriétés système fournies dans le système de base pour les approbations d'exception via workflow dans la table Propriétés système [sys_properties]. Ainsi, lorsqu'une demande d'exception ou de faux positif est émise via le workflow, elle est envoyée pour approbation aux ID de groupe définis dans la propriété système. Accédez à la **Tous** > **Propriétés système** et sélectionnez *`sn_vul_container.container_exception_approver_L1`*, *`sn_vul_container.container_exception_approver_L2`*ou *`sn_vul_container.container_false_positive_approver_group`* pour modifier la valeur de la propriété.

- Approbation des règles d'exception : il n'a pas de configuration mais deux niveaux d'approbation.
- Approbation des faux positifs : il a une configuration avec un niveau d'approbation.

Remarque : À partir de la version 2.5 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités pour conteneurs des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable du conteneur passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable du conteneur ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Demander et approuver une exception dans Réponse aux vulnérabilités pour conteneurs

Vous pouvez demander à différer le rattrapage d'un élément vulnérable de conteneur (CVIT) pour une période spécifiée. Par exemple, en tant que développeur, vous pouvez demander une exception si un correctif n'est pas disponible pour un ordinateur. Les approbateurs disposant d'un accès peuvent approuver les demandes provenant d'autres utilisateurs.

Pour demander ou approuver une exception, consultez :

- Demander une exception pour un élément vulnérable de conteneur
- Demander une exception pour les vulnérabilités des conteneurs à l'aide de GRC : Gestion de la politique et de la conformité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Des notifications par e-mail sont envoyées à chaque étape de la gestion des exceptions, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'une exception est demandée, le demandeur reçoit un e-mail confirmant que la demande est soumise. L'approbateur reçoit également un e-mail indiquant qu'une exception a été demandée. À partir de la version 2.5 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités pour conteneurs des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable du conteneur passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable du conteneur ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Demander une exception pour un élément vulnérable de conteneur

Demander une exception pour un élément vulnérable de conteneur (CVIT) qui ne peut pas être corrigé immédiatement. Par exemple, en tant que propriétaire de rattrapage, vous pouvez demander une exception si un correctif n'est pas disponible pour un ordinateur.

Avant de commencer

Rôle requis : Groupe de développeurs

Pourquoi et quand exécuter cette tâche

Vous pouvez demander une exception pour plusieurs CVIT simultanément à l'aide de la fonction de modification en bloc du Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Demander une exception en bloc dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Réponse aux vulnérabilités du conteneur** > **Éléments vulnérables de conteneurs** > **Tous**.
2. Sélectionnez l'élément pour lequel vous souhaitez demander une exception.
   L'élément sélectionné doit être à l'état Ouvert ou En cours d'examen.
3. Sur le formulaire Élément vulnérable de conteneur, cliquez sur **Demande d'exception**.

4. a. Remplissez les champs du formulaire.

Formulaire de demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée sélectionnée dans le **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Gestion des exceptions** écran. Lorsque la demande d'exception expire, le groupe revient à son état Ouvert.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : À partir de la version 1.2 de , si un élément vulnérable a été différé pour correction à l'aide de la fonctionnalité de gestion des Réponse aux vulnérabilités pour conteneurs exceptions, s'il est rouvert par le scanner, la date de report définie sur la vulnérabilité persistera. Pour activer cette fonctionnalité, définissez la valeur de la propriété `sn_vul.container.auto_defer_cvit_in_active_e` système sur vrai. En outre, la date de fin de report persiste même après la fermeture de la CVIT ou l'expiration de l'exception. Le rôle requis est sn_vul_container.manage_exception_configuration pour la lecture et l'écriture.
Motif	Raison de l'exception. Les choix sont les suivants : ▪ Risque accepté ▪ En attente de fenêtre de maintenance ▪ Correctif non disponible ▪ Contrôle d'atténuation en place ▪ Autre Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir un mappage de motif de politique.
Informations supplémentaires	Détails liés au motif pour lequel cette demande est effectuée. Ce champ doit être mis à jour par le propriétaire du rattrapage.

b. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**.
L'état de l'élément vulnérable du conteneur bascule sur En cours de révision. Utilisez l'onglet **Approbation du changement d'état** pour suivre l'état de la demande d'exception.

Demander une exception pour une tâche de rattrapage de conteneur

Demandez une exception pour différer une tâche de rattrapage de conteneur pendant une période spécifiée si elle ne peut pas être résolue immédiatement.

Avant de commencer

Vous pouvez demander des exceptions aux espaces de Réponse aux vulnérabilités travail.
Consultez Demander une exception dans le Espace de travail de remédiation IT.

Rôle requis :

sn_vul.remediation_owner, sn_vul.app_security_champion ou sn_vul_container.remediation_owner.

Vous pouvez également demander des exceptions pour les tâches de rattrapage de conteneurs dans l'environnement classique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Tâches de rattrapage** > **Tous**.
2. Sélectionnez le groupe pour lequel vous souhaitez demander une exception.
   La tâche sélectionnée doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Sur l'enregistrement de tâche de rattrapage de conteneur, sélectionnez **Demande d'exception**.
4. Remplissez les champs du formulaire.

Formulaire de demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée d'exception définie dans la configuration.
Motif	Justification de la demande d'exception.
Informations supplémentaires	Détails liés au motif pour lequel cette demande est effectuée. Ce champ doit être mis à jour par le propriétaire du rattrapage.

5. Cliquez sur **Demander l'approbation**.

Demander une exception pour les vulnérabilités des conteneurs à l'aide de GRC : Gestion de la politique et de la conformité

Demandez des exceptions à la politique à l'aide de l'aptitude de GRC gestion des exceptions de politique de l'application à partir de Réponse aux vulnérabilités pour conteneurs.Gestion de la politique et de la conformité

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions de politique, vous devez télécharger l'application à partir GRC : Gestion de la politique et de la conformité du ServiceNow Store.

Rôle requis : sn_vul.remediation_owner

Vous pouvez également demander des exceptions dans l'interface utilisateur classique :

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Éléments vulnérables de conteneurs** (ou **Tâches de remédiation**)>**Toutes**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.
   L'élément ou le groupe sélectionné doit être dans l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Sur le formulaire sélectionné, cliquez sur **Demande d'exception**.

   Remarque : S'il GRC : Gestion de la politique et de la conformité est sélectionné dans l'écran Gestion des exceptions, renseignez les champs du formulaire Demande d'exception. Pour plus d'informations sur les champs de formulaire, consultez Formulaire de demande d'exception.

   a. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**.
   L'état des éléments vulnérables passe à En cours de révision et une exception de politique est créée.
   Utilisez l'onglet **Approbation du changement d'état** pour suivre l'état de la demande d'exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

b. Pour afficher l'exception de politique, cliquez sur la liste connexe Exceptions de politique.

c. Cliquez sur le numéro d'exception de politique.

d. Dans le champ **Approbateur** , sélectionnez son nom.

e. Cliquez sur l'onglet Source et sélectionnez un objectif de contrôle dans le champ **Objectif de contrôle** .

f. Cliquez sur l'onglet Évaluation des risques et sélectionnez l'évaluation du risque dans le champ **Évaluation du risque** .

g. Enregistrez le formulaire.

h. Cliquez sur l'onglet **Contrôles impactés** .

i. Ajoutez les commandes en cliquant sur **Ajouter**.

j. Enregistrez le formulaire.

Remarque : Vous pouvez effectuer un examen de conformité en cliquant sur **Demander un examen de conformité**.

Le formulaire d'approbation est envoyé à l'approbateur.

L'approbateur peut approuver la demande en cliquant sur **Approuver** ou demander une approbation supplémentaire en cliquant sur **Demander une approbation supplémentaire**.

L'état de l'enregistrement devient Différé. Le motif indiqué est celui que vous avez sélectionné lors de l'émission de la demande d'exception. L'onglet **Report** fournit des notes supplémentaires sur l'enregistrement.

Remarque : Si la demande est rejetée, l'enregistrement revient à son état précédent.

3. Cliquez sur **Envoyer**.
Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez Configuration facultative de Policy and Compliance Management .

Définir un mappage de motif de politique

Définissez les choix de motifs pour qu'ils soient disponibles pour tout utilisateur qui demande une exception.

Avant de commencer

Rôle requis : sn_vul.compliance.manager et sn_vul_container.manage_exception_configuration

Procédure

1. Accédez à la **Tous** > **Politique et Conformité** > **Exceptions de politique** > **Registre d'intégration**.

Remarque : Vous pouvez sélectionner un motif parmi les choix de motifs disponibles dans la table Choix de motifs ou ajouter un nouveau motif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Cliquez sur le registre d'intégration Container Vulnerability Response - CVIT.
3. Dans la liste Choix des motifs, cliquez sur **Nouveau**.
4. Cliquez sur l'icône de loupe.
5. Ajoutez un choix de motif existant pour en créer un nouveau.
   - Si vous souhaitez ajouter un choix de motif existant, sélectionnez un motif.
   - Si vous souhaitez ajouter un nouveau choix de motif à la table Choix de motifs, cliquez sur **Nouveau** et remplissez les champs du formulaire.

Formulaire Liste de choix de motifs

Champ	Description
Étiquette	Étiquette unique pour ce choix.
Valeur	Valeur unique pour ce choix. Cette valeur est mappée dans la table de mappage de motif de politique pour les applications respectives. Pour accéder à cette table, saisissez `sn_vul_policy_reason_mapping.LIST` dans le navigateur de filtre.
Ordre	Ordre pour ce choix. Les motifs sont classés en fonction de ce nombre.
Par défaut	Option pour indiquer que ce choix de motif sera disponible chaque fois qu'une exception de politique sur demande est demandée. Si le registre d'intégration ne contient pas de choix spécifiques à l'application, tous les choix de motifs pour lesquels le champ **Par défaut** est sélectionné seront disponibles.
Actif	Option permettant d'afficher le choix dans la liste des choix de motifs.

6. Cliquez sur **Envoyer**.

Résultats
Le choix de la raison est ajouté. Le choix du motif sera disponible dans le champ **Motif** du formulaire de demande d'exception de politique pour l'application sélectionnée.

Approuver une demande d'exception dans Réponse aux vulnérabilités pour conteneurs

Approuvez les demandes d'exception pour les éléments vulnérables du conteneur ou les tâches de rattrapage qui ne peuvent pas être corrigées immédiatement. Vous devez évaluer ces demandes pour connaître le risque, puis approuver leur report jusqu'à ce qu'elles puissent être corrigées.

Avant de commencer
Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche
Vous pouvez approuver les demandes d'exception et de faux positifs dans le .Espace de travail du gestionnaire de vulnérabilités

Vous pouvez également approuver les demandes d'exception dans l'environnement classique :

Procédure
1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Différer un élément vulnérable de conteneur dans Réponse aux vulnérabilités pour conteneurs

Si vous déterminez que le problème associé à un élément vulnérable de conteneur (CVIT) présente un risque faible et peut être immédiatement différé sans analyse supplémentaire, vous pouvez utiliser la fonctionnalité **Différer** .

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l'application Réponse aux vulnérabilités . Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pourquoi et quand exécuter cette tâche

Une tâche planifiée s'exécute tous les jours pour rechercher les éléments vulnérables différés qui ont atteint leur date de réouverture. Le jour où le report de la CVIT doit expirer, l'enregistrement est rouvert.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Éléments vulnérables de conteneurs**.
2. Ouvrez un élément vulnérable.
3. Cliquez sur **Demande d'exception**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Jusqu'à	Sélectionnez la date à laquelle l'état Différé expire et la tâche de rattrapage est réactivée. **Remarque :** À partir de la version 18.0 de , si un élément vulnérable de Réponse aux vulnérabilités pour conteneurs conteneur différé (CVIT) est fermé et rouvert par un scanner avant l'expiration de la fenêtre d'exception, l'état de la CVIT revient à l'état différé en respectant la fenêtre d'exception active. Pour activer cette fonctionnalité, définissez la valeur de la propriété `sn_vul.container.auto_defer_cvit_in_active_ex` système sur vrai. En outre, la date de fin différée persiste même après la fermeture de l'élément vulnérable ou l'expiration de l'exception. Le rôle requis est sn_vul_container.manage_exception_configuration pour la lecture et l'écriture. Une fois l'enregistrement envoyé, si les notifications par e-mail sont définies,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	les Réponse aux vulnérabilités pour conteneurs membres du groupe reçoivent un e-mail indiquant que la date d'expiration est dans moins d'une semaine. Lorsque la date de report expire, l'élément vulnérable est redéfini sur Ouvert et une deuxième notification par e-mail est envoyée.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants : ○ En attente de fenêtre de maintenance ○ Faux positif ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Cliquez sur **Envoyer**.
   Le groupe est marqué **En cours de révision**. Un lien connexe **Rouvrir** s'affiche. La date et le motif de réouverture apparaissent dans les notes de travail sous l'onglet **Approbations de changement de l'état** .

   Réponse aux vulnérabilités pour conteneurs À partir de la version 2.3, vous pouvez ajouter des informations pertinentes dans le champ Notes de travail de la section Notes pour un élément vulnérable de conteneur différé.

Demander une extension pour un élément vulnérable de conteneur différé

Demandez une extension pour un élément vulnérable de conteneur différé avant qu'il n'atteigne sa date d'échéance différée. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Éléments vulnérables de conteneurs**.
2. Ouvrez un élément vulnérable de conteneur différé.
3. Sélectionnez **Demande d'extension**.

> **Remarque :** Le bouton Demande d'extension n'est visible que lorsque l'état de l'élément vulnérable du conteneur est Différé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle l'élément vulnérable de conteneur différé doit être prolongé pour correction.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants : ○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
Un e-mail est déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Si un élément vulnérable de conteneur différé est prolongé à nouveau, le nombre de reports d'extension augmente dans le back-end.

6. Une fois la demande approuvée, les notes Jusqu'à, Motif et Report sont mises à jour.

Utiliser une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Vous pouvez demander une exception pour les éléments vulnérables de conteneur (CVIT) qui ne peuvent pas être corrigés ou différés immédiatement. En automatisant le processus de report de VI, vous pouvez différer les CVIT correspondants en fonction de la règle lorsque le système les identifie.

Vous pouvez effectuer les tâches suivantes pour une règle d'exception :

- Créer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- Approuver une demande de règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- Activer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- Rouvrez une règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- Mettre à jour une règle d'exception approuvée dans Réponse aux vulnérabilités pour conteneurs
- Supprimer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs
- Différer un élément vulnérable de conteneur dans Réponse aux vulnérabilités pour conteneurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 2.5 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités pour conteneurs des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable du conteneur passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable du conteneur ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Créer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Créez une règle pour demander automatiquement une exception pour une condition spécifique pour un groupe d'éléments vulnérables de conteneurs (CVIT), telle qu'une règle avec une condition basée sur la gravité de vulnérabilité de ces CVIT. Avec cette règle, vous pouvez différer automatiquement les CVIT nouveaux et existants s'ils correspondent à la condition de règle approuvée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

La règle s'applique à partir de la date de début de validité jusqu'à la date de fin de validité. La tâche de rattrapage (VUL) est créée lorsque la règle est approuvée. La méthode de regroupement pour cette VUL est connue sous le nom de règles d'exception. La VUL est créée à l'état Différé. Vous ne pouvez pas fermer, rouvrir ou supprimer cette VUL. Les CVIT nouveaux et rouverts sont différés et ajoutés à cette VUL à partir de la date « Valide à partir de » jusqu'à l'expiration du groupe à la date « Valide jusqu'à ».

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de la règle d'exception. Ces e-mails fournissent l'état et d'autres détails d'une demande. Par exemple, lorsqu'une règle d'exception est demandée, le demandeur reçoit un e-mail confirmant l'envoi de la demande.

Remarque : Si la règle est rejetée, vous pouvez la rouvrir à l'état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles d'exception**.
2. Sur la page Nouvel enregistrement de règle d'exception, cliquez sur **Nouveau** pour créer une règle.
3. Renseignez les champs du formulaire Règle d'exception.

   Remarque : Pour plus d'informations sur les champs de formulaire, consultez Formulaire Règle d'exception.

4. Ajoutez le groupe d'affectation lorsque vous créez la règle.
5. Envoyez le formulaire pour approbation.
   L'état de la demande est défini sur En cours de révision. Tant que vous n'avez pas soumis la règle d'exception, elle reste à l'état Brouillon.
6. Pour afficher et créer un groupe chargé de gérer les règles d'exception :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tous** > **Administration utilisateurs** > **Groupes**.

b. Dans une règle d'exception, cliquez sur l'onglet **Approbations demandées** pour afficher l'état de la demande.
Une tâche planifiée est exécutée quotidiennement pour appliquer les règles d'exception sur les données existantes. Tous les éléments vulnérables qui correspondent à la condition sont passés à l'état Différé. Si une règle d'exception approuvée est supprimée, tous les éléments vulnérables différés reviennent à leur état précédent. Pour plus d'informations, consultez Utiliser une règle d'exception.

Approuver une demande de règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Évaluez les demandes de règle d'exception des utilisateurs afin de pouvoir approuver ou rejeter ces demandes.

Avant de commencer
Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche
Approbateur d'exceptions Les membres du groupe d'utilisateurs de niveau 1 peuvent approuver les demandes de règle d'exception de niveau 1. De même, les membres du groupe d'utilisateurs de niveau 2 de l'approbateur d'exceptions peuvent approuver les demandes de règle d'exception de niveau 2. Les deux groupes d'utilisateurs héritent du rôle d'approbateur d'exceptions par défaut.

Remarque :

Si vous déployez l'application VR pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow. Pour configurer des règles d'approbation pour la gestion des exceptions et les faux positifs, reportez-vous à la section Configurer les règles d'approbation pour la gestion des exceptions.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec et expliquez pourquoi vous avez approuvé ou rejeté la demande.
Une fois qu'une règle d'exception est approuvée, une tâche de rattrapage (RT) est créée par défaut dans l'état Différé. À partir de la date de début de validité, cette règle s'exécute sur tous les CVIT créés, ainsi que sur ceux qui sont passés de l'état Fermé à l'état Ouvert. Les CVIT qui correspondent aux conditions définies sont ajoutés au RT et différés pour la période spécifiée.

Remarque : Si la règle est rejetée, vous pouvez la rouvrir à l'état Brouillon, la mettre à jour, puis la soumettre à nouveau pour approbation.

Activer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Une règle est activée à sa date de début de validité. Après l'activation, il automatise le processus d'exception pour les éléments vulnérables de conteneur (CVIT).

La règle d'exception suit le cycle de vie suivant :

1. Les nouveaux CVIT que vous créez ou rouvrez et qui remplissent la condition spécifiée sont reportés. Si vous activez l'option Exécuter sur les données existantes lorsque vous exécutez la règle d'exception pour la première fois, tous les CVIT actifs et non

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

différés qui remplissent la condition de règle d'exception sont déplacés vers la tâche de rattrapage (RT) nouvellement créée et son état devient Différé.

2. Si une CVIT nouvellement créée correspond à la condition de la règle d'exception, elle est déplacée vers la RT différée qui est associée à la règle et la règle de groupe n'est pas exécutée sur celle-ci.
3. À la date de début de validité, les CVIT existants sont ajoutés si vous activez l'option Exécuter sur les données existantes.
4. Le RT cesse d'accepter de nouveaux CVIT lorsque la règle expire à la date « Valide jusqu'à ». Le RT existe jusqu'à la date « Différé jusqu'à ».
5. La règle d'exception expire à la date « Fin de validité ».

Rouvrez une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Rouvrez une règle d'exception qui a été rejetée, mais que vous souhaitez soumettre à nouveau. La réouverture de la règle la fait passer à l'état Brouillon.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Vous pouvez ensuite mettre à jour et soumettre à nouveau la règle pour approbation.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles d'exception**.
2. Recherchez la règle que vous souhaitez rouvrir, puis cliquez sur **Rouvrir**.
3. Mettez à jour le formulaire et soumettez-le à nouveau pour approbation.

Mettre à jour une règle d'exception approuvée dans Réponse aux vulnérabilités pour conteneurs

Annulez une règle approuvée pour pouvoir la mettre à jour. Par exemple, avant de pouvoir modifier des dates ou ajouter une condition à une règle approuvée, vous devez l'annuler afin que la tâche de rattrapage (VUL) soit supprimée et que les éléments vulnérables de conteneurs (CVIT) passent à l'état Ouvert.

Avant de commencer
Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
Les règles de groupe sont réappliquées à ces CVIT. Soumettez la règle après avoir apporté les changements afin qu'elle repasse par le processus d'approbation.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles d'exception**.
2. Ouvrez la règle d'exception que vous souhaitez annuler, puis cliquez sur **Annuler**.
3. Dans la boîte de dialogue Annuler la règle, cliquez sur **Annuler la règle**.
   La règle revient à l'état Brouillon et la VUL associée est supprimée. Les CVIT associés sont rouverts et des règles de groupe sont appliquées aux CVIT individuels.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supprimer une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Supprimez une règle d'exception qui n'est plus requise. Par exemple, vous pouvez supprimer une règle si vous ne souhaitez pas différer un élément vulnérable de conteneur (CVIT) pendant l'ingestion.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

La suppression d'une règle annule la tâche de rattrapage associée (VUL). Les CVIT associés sont rouverts et des règles de groupe sont appliquées aux CVIT individuels.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles d'exception**.
2. Ouvrez la règle d'exception que vous souhaitez supprimer et cliquez sur **Supprimer**.
3. Dans la boîte de dialogue Supprimer la règle, cliquez sur **Supprimer la règle** pour supprimer la règle sélectionnée.
   La tâche de rattrapage associée est également supprimée. Les CVIT associés sont rouverts et des règles de groupe sont appliquées aux CVIT individuels.

Demander une extension pour une tâche de rattrapage différée dans Réponse aux vulnérabilités pour conteneurs

Demander une extension pour une tâche de rattrapage différée (VUL) avant qu'elle n'atteigne sa date d'échéance différée. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Tâches de remédiation**.
2. Ouvrez une tâche de rattrapage différée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'état Différer expire et l'élément vulnérable de conteneur est réactivé.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Une fois la demande approuvée, les changements apportés à la tâche de rattrapage sont également reportés sur les éléments vulnérables du conteneur, qui font partie de la tâche de rattrapage. Toutefois, les éléments vulnérables du conteneur doivent être à l'état Différé et Leur date actuelle jusqu'à ce que les données précèdent la date de fin de mise à jour. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une tâche de rattrapage différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Demander une extension pour une règle d'exception dans Réponse aux vulnérabilités pour conteneurs

Demandez une extension pour une règle d'exception différée avant qu'elle n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer
Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche
Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Règles d'exception**.
2. Sélectionnez une règle d'exception différée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle la règle d'exception doit être prolongée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Motif	Entrez le motif du report de la règle d'exception. Les choix sont les suivants : ○ Risque accepté ○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les champs Différé jusqu'à, Motif et Informations supplémentaires sont mis à jour sur la règle d'exception et les éléments vulnérables du conteneur. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Le bouton Demande d'extension n'est pas disponible pour les tâches de rattrapage créées dans le cadre d'une règle d'exception.
- Si une règle d'exception différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Marquage et approbation d'un élément de vulnérabilité de conteneur faux positif

Les éléments vulnérables de conteneurs (CVIT) et les tâches de rattrapage (VUL) peuvent être marqués comme des faux positifs. Les approbateurs avec un accès en écriture peuvent approuver de telles demandes provenant d'autres utilisateurs.

- Marquer comme faux positif dans Réponse aux vulnérabilités pour conteneurs
- Approuver un faux positif

Remarque :

Des notifications par e-mail sont envoyées à chaque étape du workflow de faux positif, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'une CVIT ou une tâche de rattrapage est marquée comme faux positif, le demandeur reçoit un e-mail de confirmation. Simultanément, l'approbateur reçoit un e-mail indiquant qu'une CVIT ou une tâche de rattrapage a été marquée comme faux positif. À partir de la version 2.5 de , vous pouvez configurer les délais d'approbation Réponse aux vulnérabilités pour conteneurs des faux positifs et des exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, l'élément vulnérable du conteneur passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, l'élément vulnérable du conteneur ou la tâche de rattrapage revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez Configurer les règles d'approbation pour la gestion des exceptions.

Important : En tant qu'analyste de vulnérabilité et responsable du rattrapage, vous pouvez demander et approuver des faux positifs à partir de l'espace de travail du gestionnaire de vulnérabilité et de l'espace de travail de rattrapage informatique respectivement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Marquer comme faux positif dans Réponse aux vulnérabilités pour conteneurs

Marquez un élément vulnérable de conteneur (CVIT) ou une tâche de rattrapage comme un faux positif si l'avertissement donné par le scanner n'est pas réellement un problème. Par exemple, si une CVIT a été mise hors service, mais que le scanner soulève toujours un problème à ce sujet, marquez-la comme faux positif.

Important : En tant qu'analyste de vulnérabilité et responsable du rattrapage, vous pouvez demander des faux positifs à partir de l'espace de travail du gestionnaire de vulnérabilité et de l'espace de travail de rattrapage informatique respectivement.

Avant de commencer

Rôle requis : propriétaire du rattrapage

Procédure

1. Accédez à la **Tous** > **Container Vulnerability Response (ou Tâches de remédiation)** > **Tous**.
2. Ouvrez la CVIT que vous souhaitez marquer comme faux positif et cliquez sur **Marquer comme faux positif**.
   Le CVIT doit être à l'état **Ouvert** .
3. Sur le formulaire Faux positif, saisissez les détails dans **Informations supplémentaires** et cliquez sur **Demander l'approbation**.
   La demande est envoyée pour approbation et l'état de la CVIT devient **En cours de révision**. Le demandeur et l'approbateur sont tous deux informés par e-mail.

Approuver un faux positif

En tant qu'approbateur de faux positif, vous pouvez approuver les demandes de faux positif d'autres utilisateurs.

Important : Vous pouvez approuver ou rejeter les demandes de faux positif dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis : false_positive_approver

Vous pouvez également approuver des demandes d'exception et de faux positifs dans l'environnement classique :

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Remarque : Un faux positif peut être limité dans le temps. Seul l'approbateur peut définir la date de fin.

Tâches de rattrapage de Container Vulnerability Response et vue d'ensemble des règles de tâche

Configurez les tâches de rattrapage (CVUL) pour aider les analystes et les spécialistes du rattrapage à organiser les éléments vulnérables de conteneur (CVIT) et à les analyser en bloc. Les critères selon lesquels les tâches de rattrapage sont formées sont configurés de sorte que les CVIT sont automatiquement affectés aux tâches de rattrapage. Les tâches de rattrapage vous permettent de surveiller la progression et de piloter le processus de rattrapage plus efficacement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suppression des affectations des éléments vulnérables et des tâches de rattrapage de conteneur

À partir de la version 2.13, vous pouvez effacer les champs **Affecté à** et **Groupe d'affectation** sur les éléments vulnérables de conteneur (CVIT) directement à partir des enregistrements CVIT et de tâches de rattrapage que vous déterminez comme susceptibles d'être incorrectement affectés à vous ou à vos groupes.

Voir Suppression des affectations des éléments vulnérables et des tâches de rattrapage de conteneur et Supprimer les affectations des éléments vulnérables et des tâches de rattrapage pour plus d'informations.

Suivi du nombre de reports pour les éléments vulnérables et les tâches de rattrapage des conteneurs

Suivez le nombre de reports d'un élément vulnérable, d'un élément vulnérable d'application, d'un élément vulnérable de conteneur ou d'une tâche de rattrapage. La tâche planifiée Définir les nombres de reports s'exécute quotidiennement pour valider les nombres d'enregistrements qui sont différés plusieurs fois dans la colonne Nombre de reports. Les enregistrements sont affichés dans les modules Reports multiples pour VR, AVR et CVR.

Comprendre les règles de tâche de rattrapage

Les règles de tâche de rattrapage vous permettent de définir comment les éléments vulnérables de conteneur sont automatiquement regroupés et affectés. Une **vulnérabilité** de règle par défaut est incluse dans le système de base qui rassemble les CVIT en fonction de leurs vulnérabilités. Toutefois, vous pouvez regrouper par tout autre ensemble de valeurs dans des colonnes accessibles à partir de la CVIT. Ces valeurs peuvent inclure l'élément de configuration (CI), l'entrée de vulnérabilité et autres.

Il existe des règles de tâche pour Container Vulnerability Response qui sont incluses dans l'application Vulnerability Response disponible lorsque vous l'activez.

Vous pouvez créer plusieurs conditions avec le générateur de conditions. Dans la section Grouper par, une autre ligne s'affiche après avoir défini une paire de champs. Vous pouvez avoir jusqu'à six sélections **Grouper par** . Vous pouvez également automatiser l'affectation des groupes.

Par exemple, vous pouvez regrouper vos éléments vulnérables de conteneur par élément de configuration ou par modèle de produit. Vous pouvez avoir une règle de tâche unique pour les vulnérabilités de faible gravité ou les CI à faible risque. Vous pouvez avoir une autre règle de tâche pour les serveurs critiques et les vulnérabilités qui exposent l'entreprise à plus de risques. Consultez la rubrique Créer, modifier et supprimer des règles de tâche de rattrapage de Container Vulnerability Response pour plus d'informations sur les options qui s'offrent à vous.

Un autre ensemble de règles peut être utilisé pour les éléments vulnérables de conteneurs qui exposent l'entreprise à davantage de risques. Le nom de la tâche de rattrapage est ajouté à la règle de tâche de rattrapage **Grouper par** valeurs pour faire la brève description du nouvel enregistrement.

Lorsqu'un nouvel élément vulnérable de conteneur est créé, importé ou rouvert après avoir été fermé, les règles sont évaluées par rapport à celui-ci. Une CVIT n'est évaluée qu'une seule fois, automatiquement, sauf si elle est rouverte après avoir été fermée ou si les règles sont réappliquées manuellement.

Le processus suivant est utilisé pour chaque CVIT nouveau ou rouvert :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour chaque règle de tâche de rattrapage, la CVIT est comparée au filtre de règle de tâche de rattrapage.
- Pour chaque règle dans laquelle la condition de la règle de tâche de rattrapage est vérifiée, la règle extrait les données des sélections **Grouper par** sur la CVIT. Il génère un nom de groupe et un champ. Dans ce cas, **risque élevé : QID-32342 : résumé de QID-3242** (Nom : ID de vulnérabilité : résumé de la vulnérabilité).

> **Remarque :** Le champ Description brève est limité à 160 caractères. Les résumés de vulnérabilité plus longs sont tronqués.

La règle vérifie s'il existe une tâche de rattrapage **ouverte** correspondante affectée au même groupe d'affectation que la CVIT.

- Si la tâche est trouvée, le CVIT est ajouté à la tâche existante à l'état **ouvert** .
- Si aucune tâche à l'état **Ouvert** n'est trouvée, la règle crée une tâche **à risque élevé : QID-32342** , l'affecte au même groupe d'affectation que la CVIT et place la CVIT dans la tâche de rattrapage.

Plusieurs règles de tâche de rattrapage peuvent être définies pour regrouper différents types de vulnérabilités. Étant donné que chaque vulnérabilité est comparée aux conditions de la règle de tâche de rattrapage avant de la placer dans une tâche de rattrapage, trop de règles peuvent avoir un impact sur les performances. Configurez vos règles de tâche afin que les conditions vous aident à éviter de créer des tâches de rattrapage en double.

Par défaut, les règles de tâche de rattrapage utilisent le groupe d'affectation défini par les **règles d'affectation** sur la CVIT lors du regroupement des éléments et affecte la tâche de rattrapage pour correspondre aux CVIT.

Dans le cadre de la règle de tâche par défaut, l'affectation de ces tâches de rattrapage est contrôlée par les règles du module **Règles d'affectation** . Pour plus d'informations sur les règles d'affectation, consultez Vue d'ensemble des règles d'affectation de Vulnerability Response.

Lorsqu'une règle de tâche est supprimée de la vue de formulaire ou de liste, vous avez la possibilité de supprimer toutes les tâches ouvertes créées par cette règle. Les tâches dont l'état **n'est pas Ouvert** sont exclues.

Réapplication des règles de tâche de rattrapage

Lorsque vous souhaitez modifier une règle de tâche de rattrapage, utilisez le bouton **Réappliquer** sur la page de règle de tâche de rattrapage pour réexécuter la règle modifiée sur toutes les tâches de rattrapage **ouvertes** actives créées par cette règle. Elle supprime et recrée automatiquement les tâches de rattrapage en fonction de la règle modifiée.

La réapplication vérifie uniquement les tâches de rattrapage existantes.

Une fois que vous avez sélectionné **Réappliquer**, le message suivant s'affiche : La réapplication de cette règle de tâche de rattrapage supprimera et recréera les tâches de rattrapage pour cette règle. Les tâches de rattrapage qui ne sont pas à l'état ouvert ne sont pas supprimées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : En tant qu'administrateur et analyste des vulnérabilités, vous pouvez évaluer les règles de tâche de rattrapage pour les éléments vulnérables sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités. Cette méthode est plus efficace que la réapplication des règles de tâche de rattrapage dans l'interface utilisateur classique, qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Règles de tâche de rattrapage et création et mise à jour de CVIT

Si un CI d'une analyse est associé à une vulnérabilité connue, une CVIT est créée. Une fois créé, le CVIT est évalué par rapport aux conditions des règles de tâche de rattrapage pour une correspondance. S'il y a une correspondance avec une tâche de rattrapage existante, la CVIT est ajoutée. Si aucune tâche de rattrapage correspondante n'est trouvée, une tâche est créée pour la CVIT.

Si une propriété capturée dans les conditions de filtrage de la tâche de rattrapage est mise à jour ou modifiée sur une CVIT, l'AVI mis à jour est également évaluée par rapport aux règles de tâche de rattrapage pour une correspondance. S'il y a une correspondance avec une tâche de rattrapage existante, la CVIT est ajoutée. Si aucune tâche de rattrapage correspondante n'est trouvée, une tâche est créée pour la CVIT.

Déploiement et généralisation de l'état

Si vous mettez à jour une tâche de rattrapage sur Ouvert, ou d'Ouvert sur En cours d'examen, le nouvel état est étendu à tous les CVIT associés. La réduction de l'état se produit immédiatement après le changement de l'état.

Le déploiement de l'état des CVIT vers la tâche de rattrapage se produit uniquement si tous les CVIT de la tâche sont à l'état **Différé** ou **Fermé - fixe** . Le déploiement est effectué avec les valeurs des éléments vulnérables du conteneur de déploiement sur Vulnerability et une tâche planifiée par groupe, qui s'exécute toutes les 15 minutes. L'état n'est pas déployé tant que la tâche ne s'exécute pas. Pour qu'un état se déploie entre les CVIT et la tâche de rattrapage, tous les CVIT doivent être dans le même état.

Créer, modifier et supprimer des règles de tâche de rattrapage de Container Vulnerability Response

Vous pouvez créer des règles pour regrouper automatiquement les éléments vulnérables de conteneur (CVIT) en tâches de rattrapage (CVUL) en fonction des conditions de filtre. Ces règles regroupent automatiquement les CVIT à mesure qu'ils sont importés ou créés manuellement.

Avant de commencer

Si vous créez une règle, elle ne s'applique pas aux données existantes. Une fois que vous l'avez soumise, elle est exécutée sur de nouvelles importations.

Rôle requis : gestionnaire App-Sec

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles de la tâche de rattrapage.**.
2. Ouvrez la règle ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire ou modifiez-les.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règle de la tâche de rattrapage

Champ	Description
Nom	Nom de la règle de tâche.
Actif	Indique si la tâche est active.
Description	Description de la règle.
Sensible à la casse	Détermine si une condition est sensible à la casse ou non. **Remarque :** La valeur par défaut est insensible à la casse.
Condition	Conditions de filtre facultatives pour la règle. Par défaut (case **sensible à la casse** non cochée), le texte de recherche que vous saisissez dans le générateur de conditions sur les enregistrements de règles de tâche et les formulaires n'est pas sensible à la casse. Vous pouvez activer les recherches sensibles à la casse sur les enregistrements de tâches et les formulaires. Voici un exemple de condition : **Vulnérabilité** > **est** > **VULNENT123451** (une vulnérabilité importée connue). Toute CVIT présentant cette vulnérabilité correspond à cette condition.
Grouper par (jusqu'à six ensembles de conditions sont disponibles)	
Regrouper les éléments vulnérables de conteneurs à partir de	Table que la règle utilise pour regrouper les CVIT. Sélectionnez les éléments de l'arborescence : ○ Élément vulnérable de conteneur [sn_vuln_vulnerable_item] ○ Élément vulnérable de conteneur : image de Docker ○ Élément vulnérable de conteneur : vulnérabilité du conteneur **Remarque :** Si vous choisissez une table étendue, le **champ Utilisation** n'est appliqué qu'aux éléments vulnérables de l'application qui utilisent cette table étendue.
Utilisation du champ	Champ de la table que la règle utilise pour regrouper les CVIT. Sélectionnez les conditions dans l'arborescence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Affectation	
Affecter la tâche de rattrapage par	Lors de l'affectation automatique des tâches de rattrapage, le choix Affectation est utilisé en plus des choix **Grouper par** pour regrouper les éléments vulnérables. De nouvelles tâches sont créées, selon les besoins, afin que chaque CVIT soit placé dans une tâche avec un groupe d'affectation correspondant défini. Pour automatiser l'affectation des tâches créées en fonction de cette règle, choisissez l'une des options disponibles. ○ Regrouper par champ : si vous avez sélectionné un champ de groupe d'utilisateurs dans les valeurs **de champ Utilisation** de la section **Grouper par** , elles apparaissent dans le menu déroulant. ○ Groupe d'utilisateurs : utilisez la liste de recherche pour sélectionner un groupe d'utilisateurs statique.

Remarque : Si vous supprimez une règle à partir de la vue de formulaire ou de liste, vous avez la possibilité de supprimer toutes les tâches de rattrapage ouvertes créées par cette règle. Les groupes dont l'état n'est pas Ouvert sont exclus.

4. Sélectionnez **Soumettre pour les** nouvelles règles.
   Une fois que vous avez sélectionné **Soumettre**, votre règle s'affiche dans la liste Règles de la tâche de rattrapage [sn_vul_grouping_rule]. Les situations suivantes déclenchent votre règle.
   - Lorsque de nouveaux CVIT sont créés.
   - Lorsque vous sélectionnez **Réappliquer**. Vous sélectionnez **Réappliquer** pour évaluer les règles de tâche sur les tâches de rattrapage existantes uniquement.
   - Lorsque les CVIT sont mis à jour, soit par vous, soit par le système.

     Si un CVIT est mis à jour, les règles de tâche sont évaluées pour déterminer les correspondances avec les tâches de rattrapage existantes. Voici quelques mises à jour courantes qui lancent une vérification des règles :
     - Lorsque l'état passe de Fermé à Ouvert, ou de Fermé à En cours d'examen.
     - L'élément de configuration (CI) est modifié.
     - La vulnérabilité est changée.

   Le système vérifie toutes les règles de tâche pour voir si elles correspondent à la CVIT mise à jour. Si les conditions d'une règle correspondent aux conditions d'une tâche de rattrapage, les CVIT correspondants lui sont affectés.

   Si aucune correspondance n'est trouvée, une nouvelle tâche de rattrapage est créée.

   Pour plus d'informations sur le déploiement de l'état des CVIT vers les tâches de rattrapage et sur le déploiement de l'état des tâches de rattrapage vers les CVIT,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

consultez Vue d'ensemble des tâches de rattrapage et des règles de tâche de Container Vulnerability Response.

Pour obtenir un exemple de règle de tâche de rattrapage, consultez Exemples de règles de tâche de rattrapage Application Vulnerability Response.

5. Pour supprimer une règle de tâche, sélectionnez-la dans la liste Règles de tâche de rattrapage, puis sélectionnez Supprimer.
   Le message suivant s'affiche : La règle de tâche de rattrapage sélectionnée a créé n tâches de rattrapage. Parmi les tâches de rattrapage, n sont à l'état Ouvert.

Option	Description
Case à cocher désactivée (par défaut).	Supprimez uniquement la règle. Les tâches dont l'état n'est pas Ouvert sont exclues.
Case à cocher sélectionnée.	Incluez les tâches de rattrapage dans l'état Ouvert lorsque vous supprimez la règle de tâche de rattrapage. Supprimez la règle et toutes les tâches de rattrapage à l'état ouvert.

6. Choisissez une option et sélectionnez **Supprimer**.

Créer des règles de fermeture automatique pour Réponse aux vulnérabilités pour conteneurs

Utilisez les règles de fermeture automatique pour fermer automatiquement les éléments vulnérables de conteneurs (CVIT) plus anciens en fonction des conditions de filtre que vous avez définies.

Avant de commencer

Rôle requis : sn_vul.container_manage_auto_close_stale_vi

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités du conteneur** > **Éléments vulnérables de conteneurs** > **Règles de fermeture automatique**.

   Le système de base fournit les règles de fermeture automatique suivantes : **Dernière analyse des vulnérabilités du conteneur** : les vulnérabilités non signalées au cours des 90 derniers jours passent à l'état Périmé.

2. Sélectionnez **Nouveau** pour créer une règle de fermeture automatique.
3. Renseignez les champs du formulaire.

Champ	Valeur
Nom	Nom de la règle de fermeture automatique.
Actif	Option permettant d'activer la règle. Si elle est activée, elle ferme automatiquement toutes les détections correspondant à ses critères de filtre.
Ordre d'exécution	Valeur unique pour l'exécution de la règle de fermeture automatique. Cette valeur détermine l'ordre d'exécution. La valeur par défaut est 100.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Type d'intégration	Intégration de vulnérabilité du conteneur **Remarque :** Pour analyser les vulnérabilités de l'hôte à l'aide de l'intégration Prisma Cloud Compute, sélectionnez **Intégration du scanner de vulnérabilité**.
Description	Description de la règle de fermeture automatique.
Condition	Conditions de filtre utilisées pour identifier les détections qui doivent être fermées.

4. Sélectionnez **Soumettre**.
   Les travaux planifiés des règles **de fermeture automatique** s'exécutent quotidiennement. Il identifie les CVIT en fonction des conditions spécifiées et fait passer ceux qui correspondent à l'état **Périmé.** Dans les cas où il existe des CVIT avec à la fois des statuts Fermé et Périmé, le CVIT est fermé avec le sous-état défini sur Fixe.

Suppression des affectations des éléments vulnérables et des tâches de rattrapage de conteneur

Vous pouvez effacer les champs **Affecté à** et **Groupe d'affectation** des éléments vulnérables des conteneurs directement à partir des enregistrements d'élément vulnérable et de tâche de rattrapage que vous déterminez comme susceptibles d'être incorrectement affectés à vous ou à vos groupes.

Vue d'ensemble du workflow

Si vous déterminez que les éléments vulnérables de conteneurs (CVIT) et les tâches de rattrapage (CVUL) ne sont pas dans votre périmètre pour le rattrapage, ou si vous pensez que des enregistrements vous ont été incorrectement affectés ou ont été affectés à vos groupes, vous pouvez vous supprimer ou supprimer vos groupes des champs **Affecté à** et **Groupe d'affectation** des enregistrements CVIT et CVUL.

Le workflow de désaffectation est pris en charge dans l'espace de travail et dans les vues classique et d'espace de travail pour les CVIT et les CVUL.

Vous avez la possibilité d'envoyer des demandes pour effacer les champs d'affectation pour approbation. Voir Approuver ou rejeter une demande de désaffectation dans Réponse aux vulnérabilités et Suppression des affectations des éléments vulnérables et des tâches de rattrapage pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'action d'interface utilisateur **Annuler l'affectation** s'affiche sur les enregistrements CVIT et CVUL dans tout état autre que Fermé ou Résolu.

  Remarque : Une fois que la demande d'effacement des champs est approuvée pour une CVUL, tous les champs **Affecté à** et **Groupe d'affectation** sur les CVIT qui ont le même groupe d'affectation ne sont plus affectés. Si une CVIT sur une CVUL a un groupe d'affectation différent de celui de la CVUL associée, elle n'est pas désaffectée. Dans la plupart des cas, ces CVIT ont été attribués manuellement. Voir Tâches de rattrapage de Container Vulnerability Response et vue d'ensemble des règles de tâche et Suppression des affectations des éléments vulnérables et des tâches de rattrapage pour plus d'informations.

- Tous les enregistrements que vous mettez à jour avec l'action d'interface utilisateur ou manuellement sont affichés dans le module Non affecté pour Container Vulnerability Response.

Consultez la rubrique Supprimer les affectations des éléments vulnérables et des tâches de rattrapage pour plus d'informations sur les étapes permettant d'effacer les champs d'affectation.

Propriétés système et notifications d'approbation

Si un propriétaire de rattrapage sélectionne **Annuler l'affectation** sur un enregistrement, par défaut, la propriété système sn_vul.unassign_vr.approval_required déclenche le flux d'approbation et crée un enregistrement d'approbation de changement d'état à l'état Révision, et la demande est acheminée pour approbation. La demande s'affiche dans la liste Mes approbations pour les utilisateurs avec le sn_vul_container.unassign_approver.

Remarque : En tant qu'administrateur de vulnérabilité [sn_vul.vulnerability_admin], vous pouvez définir la *`sn_vul.unassign_vr.approval_required`* propriété système sur **false** pour désactiver le processus d'approbation.

En outre, vous pouvez modifier la valeur de la *`sn_vul.default_assignment_group`* propriété système de sorte qu'un groupe spécifique est affecté si les champs d'affectation sont effacés. Par exemple, si un utilisateur clique sur **Annuler l'affectation** d'un enregistrement et que vous souhaitez le rediriger vers un groupe spécifique pour révision, vous pouvez ajouter l'ID système du groupe de votre choix dans le champ de valeur de la propriété système.

Remarque : Si vous modifiez cette valeur, les notifications pour tous les VIT, AVIT et CVIT qui ne sont pas affectés sont envoyées au groupe que vous spécifiez.

Fermer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage d'application peut être fermé immédiatement sans analyse supplémentaire, vous pouvez utiliser la fonction **Fermer** . À partir de la version 2.10 de , le bouton **Fermer** a été supprimé pour une tâche de rattrapage de Réponse aux vulnérabilités pour conteneurs conteneur.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Dans les espaces de Réponse aux vulnérabilités travail, une tâche de rattrapage passe par les mêmes états que dans les versions précédentes de Réponse aux vulnérabilités. Lorsque tous les éléments vulnérables (VIT) d'une tâche de rattrapage sont fermés, la tâche de rattrapage passe à l'état Inactif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Vous pouvez déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à l'autre sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'un CHG a changé d'état, ou que vous ajoutez un CHG ou le supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement les tâches de rattrapage des états Fermé ou Différé .

Procédure

1. Ouvrez l'enregistrement pour lequel vous souhaitez demander une révision.
2. Sélectionnez le bouton **Fermer** .
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
État	Sélectionnez l'état *Fermé*.
Motif	Entrez le motif de la fermeture du problème.
Informations supplémentaires	Entrez toute autre information pertinente.

4. Sélectionnez **Soumettre**.
   La tâche de rattrapage est marquée comme **fermée**.

Gestion des opérations IT et la découverte de modèles

Lorsque la détection est activée, les informations sont reçues de l'équipe Information Technology Operations Management (ITOM). Si la détection est activée, vous pouvez voir les ITOM espaces de noms Kubernetes, les grappes Kubernetes et les services Kubernetes lorsque vous ouvrez un élément vulnérable de conteneur (CVIT). Sinon, vous pouvez voir les informations de charge utile Prisma.

Les étiquettes d'image des charges utiles Prisma sont stockées en tant que paires clé-valeur sous l'image Docker. Les étiquettes d'une charge utile Prisma sont stockées dans la table cmdb_key_value. Pour activer cette fonctionnalité, une règle d'identification est envoyée pour cmdb_ci_docker_image par l'équipe ITOM. Ouvrez l'image de Docker pour afficher la liste des éléments connexes. La plupart des éléments sont renseignés par l'équipe ITOM . L'entrée d'identification d'une image de Docker est expédiée pour afficher les valeurs sous forme de paires clé-valeur.

La criticité opérationnelle est déterminée en fonction des informations sur la criticité du service reçues de l'équipe ITOM . Une tâche planifiée est exécutée pour extraire les données de tous les services associés à une image. Il calcule la criticité opérationnelle en fonction du mappage des services. Comme le score de risque peut dépendre de la criticité opérationnelle, le score de risque est également calculé en fonction de celle-ci.

Solutions d'analyse et de reporting pour Réponse aux vulnérabilités pour conteneurs

Celui-ci Solution d'analyse des performances et génération de rapports contient du contenu préemballé Platform Analytics à utiliser avec d'autres ServiceNow AI Platform produits. Cela Solution d'analyse des performances et génération de rapports fournit une exposition sur la façon dont les vulnérabilités sont gérées à travers les différents graphiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur ServiceNow AI Platform (admin) : installer et activer cette solution d'analyse et de génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Administrateur Platform Analytics (pa_admin) : passer en revue les indicateurs, les répartitions, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.

Tableau de bord de Réponse aux vulnérabilités pour conteneurs

Les solutions d'analyse et de génération de rapports comportent un contenu Analyse des performances et Reporting pré-paramétré pour être utilisé avec d'autres produits ServiceNow AI Platform. Cela Solution d'analyse des performances et génération de rapports vous permet de suivre le volume, les performances et la progression des vulnérabilités, de l'analyse initiale et de la détection au confinement ou à la correction. Vous pouvez filtrer les rapports par groupe d'affectation, exploits, cote de risque ou état.

Rôles ServiceNow AI Platform requis

- Administrateur ServiceNow AI Platform (admin) : installer et activer cette solution d'analyse et de génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Administrateur Analyse des performances (pa_admin) : passer en revue les indicateurs, les répartitions, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.

Accéder au tableau de bord Réponse aux vulnérabilités pour conteneurs

Pour ouvrir le tableau de bord, accédez à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Vue d'ensemble**.

Important :

À partir de la version 2.2 de , ce tableau de Réponse aux vulnérabilités pour conteneurs bord peut également être affiché dans l'interface Next Experience utilisateur. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et sélectionnez l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, sélectionnez la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez Page Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités et Page Tableaux de bord dans Espace de travail de remédiation IT.

Remarque :

- Si vous êtes un nouvel utilisateur, vous pouvez afficher les tableaux de bord uniquement à partir des espaces de travail.
- Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

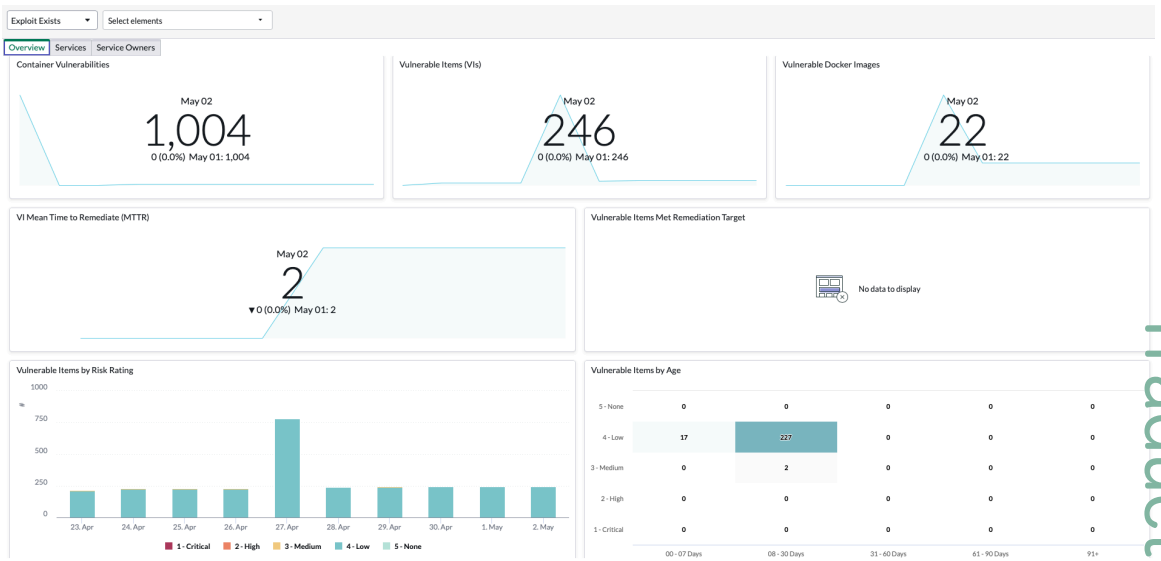
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglets Gestion de la vulnérabilité du conteneur

Ce tableau de bord vous permet de voir les vulnérabilités présentes dans les conteneurs. Vous pouvez afficher les vulnérabilités et leurs données connexes par région, âge, services et autres répartitions.

L'onglet **Vue d'ensemble** fournit l'état général de la gestion de la vulnérabilité du conteneur dans le

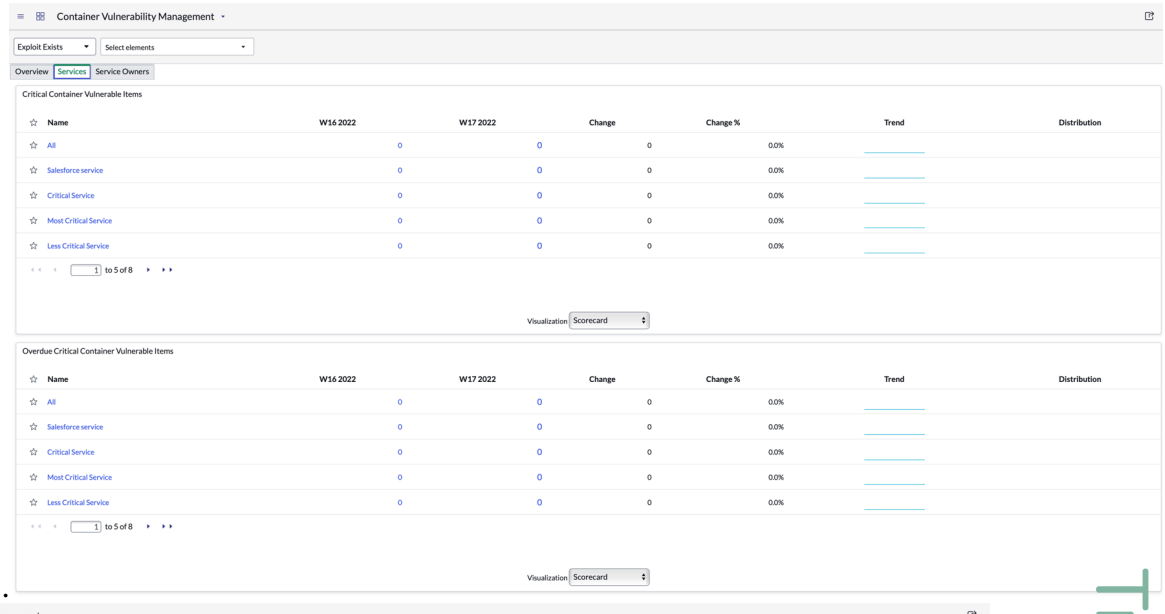


système.

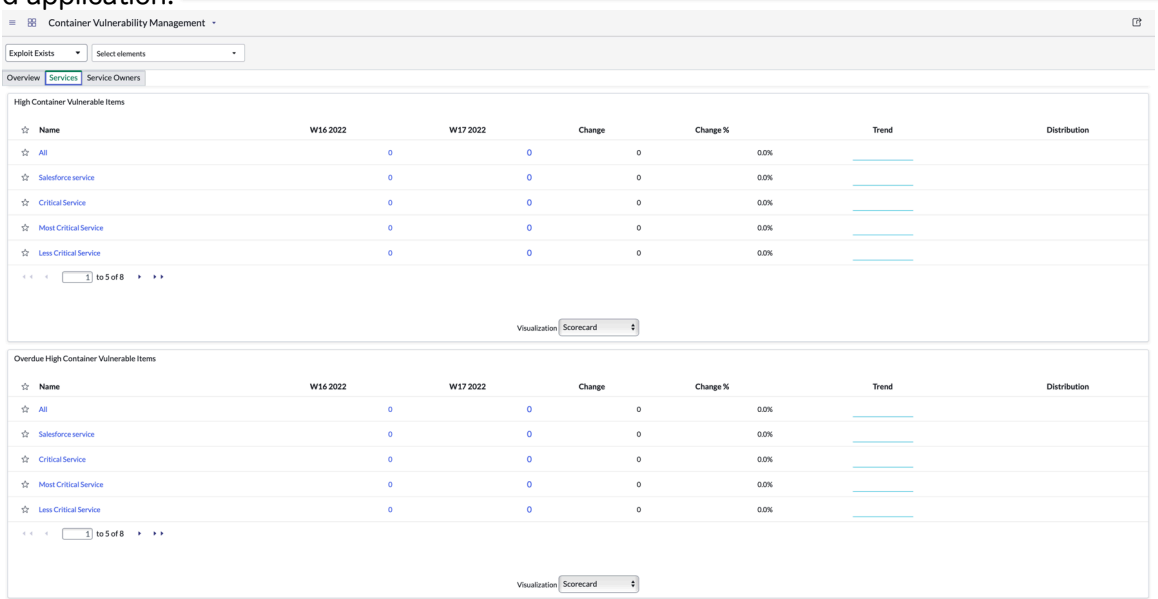
L'onglet **Services** affiche les éléments vulnérables de conteneurs ayant un impact sur les services

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



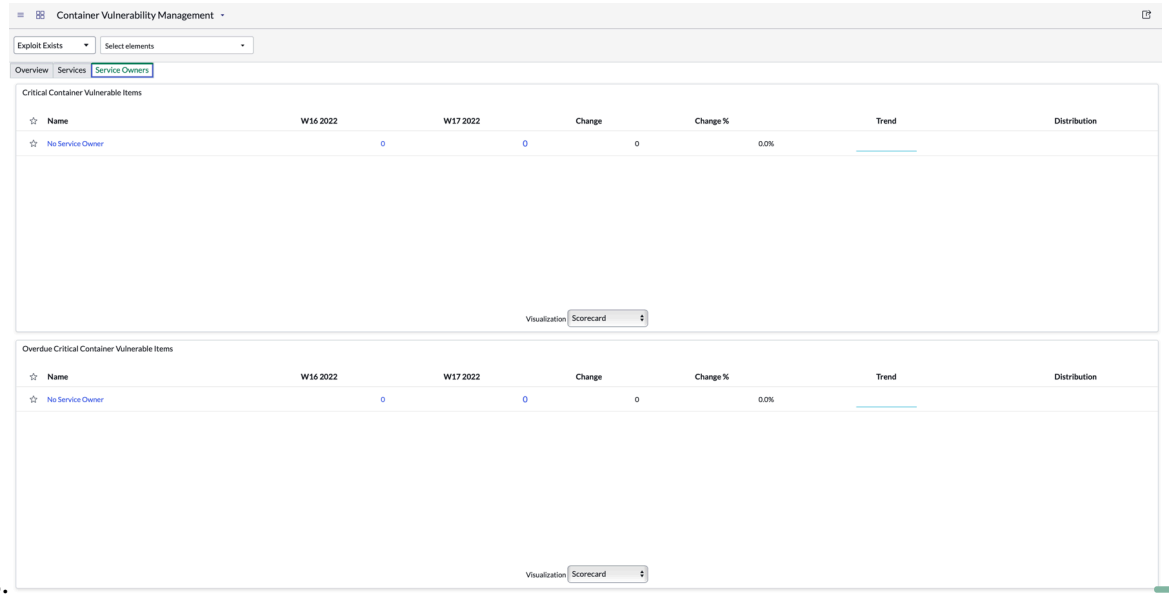
d'application.



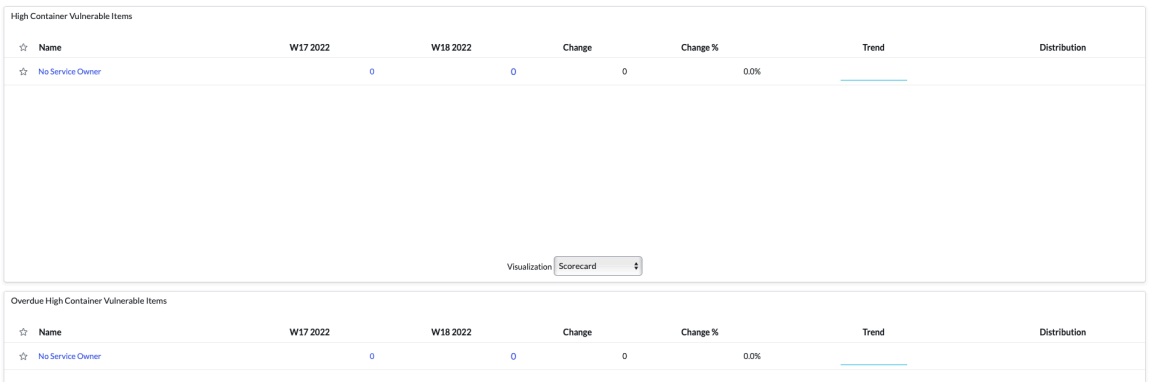
L'onglet **Propriétaires de service** affiche les éléments vulnérables de conteneurs ayant un impact sur les propriétaires de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



services.



Répartitions

- Un exploit existe
- Vecteur d'attaque de l'exploit
- Niveau de compétence de l'exploit
- État de la cible de la remédiation
- Cotes de risque
- État
- Groupe d'affectation

Traduction automatique

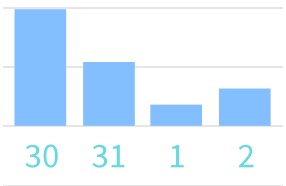
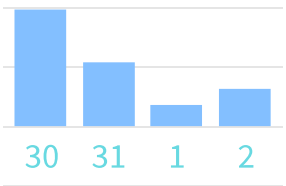
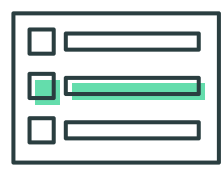
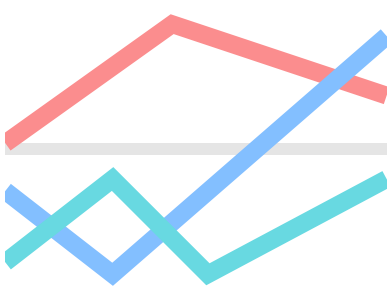
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations des données

Nom	Type	Description
Vulnérabilités du conteneur	Score unique 	Nombre de vulnérabilités de conteneur associées à un ou plusieurs éléments vulnérables de conteneur actifs.
Éléments vulnérables (VI)	Score unique 	Nombre d'éléments vulnérables actifs (non fermés) de conteneur.
Images Docker vulnérables	Score unique 	Nombre d'images docker associées aux éléments vulnérables des conteneurs actifs.
Délai moyen de rattrapage (MTTR) du VI	Score unique 	Le délai moyen de rattrapage (fermeture) d'un élément vulnérable, affiché comme moyenne d'exécution de 30 jours.
Éléments vulnérables ayant atteint la cible de rattrapage	Score unique 	Pourcentage d’éléments vulnérables de conteneur fermés qui ont atteint leur date cible de rattrapage au cours des trimestres actuels et précédents. Les cibles de rattrapage sont calculées à partir de la dernière date d’ouverture additionnée au nombre de jours.

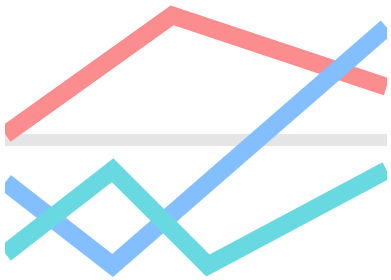
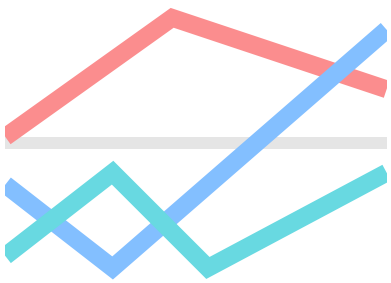
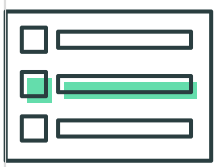
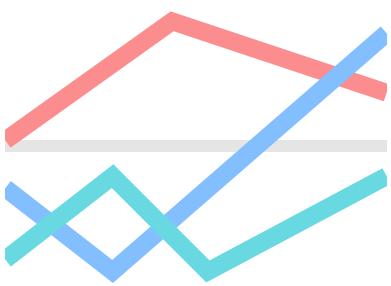
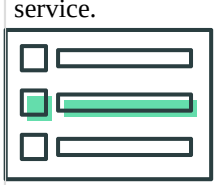
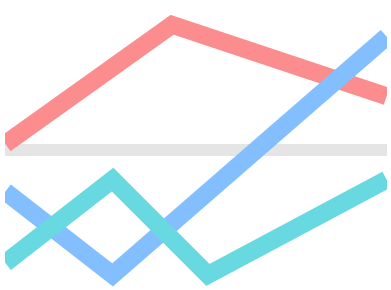
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Éléments vulnérables par cote de risque		Nombre d'éléments vulnérables de conteneur actifs regroupés par cote de risque au cours de la période sélectionnée.
Éléments vulnérables par âge		Nombre d'éléments vulnérables de conteneur actifs regroupés par cote de risque et par âge (en jours). **Remarque :** La personnalisation du calcul de l'âge et de l'âge fermé pour les éléments vulnérables (CVI) de conteneur peut entraîner une forte hausse ou une baisse des rapports d'Analyse des performances (PA) qui incluent ces mesures. Pour plus d'informations sur la personnalisation du calcul de l'âge et de l'âge fermé pour les CVI, consultez l'article de la base de connaissances KB1703270 .
Éléments vulnérables du conteneur critiques	Liste et   de ligne	Nombre d'éléments vulnérables de conteneur actifs ayant une cote de risque critique, regroupés par service.

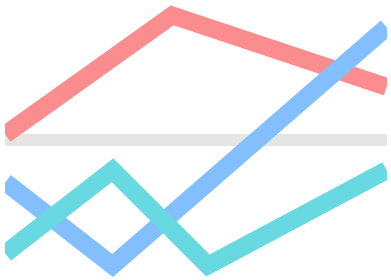
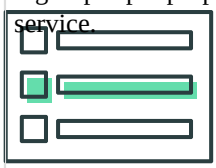
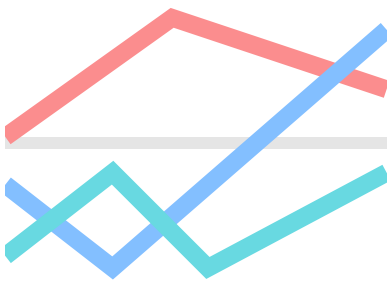
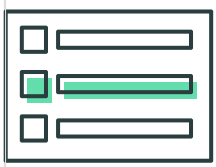
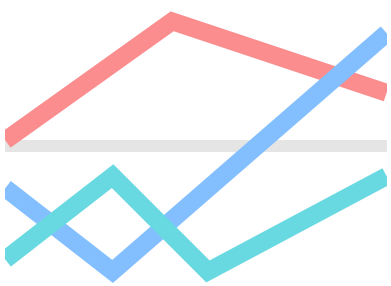
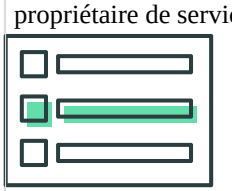
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Éléments vulnérables du conteneur critiques en retard	Liste et ligne 	Nombre d'éléments vulnérables de conteneur actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par service. 
Éléments du conteneur hautement vulnérables	Liste et ligne 	Nombre d'éléments vulnérables de conteneurs actifs ayant une cote de risque élevée, regroupés par service. 
Éléments hautement vulnérables du conteneur en retard	Liste et ligne 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée et dépassant les dates cibles de rattrapage, regroupés par service. 
Éléments vulnérables du conteneur critiques	Liste et ligne 	Nombre d'éléments vulnérables de conteneur actifs ayant une cote de risque critique, regroupés par propriétaire de service. 

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Type	Description
Éléments vulnérables du conteneur critiques en retard	Liste et ligne 	Nombre d'éléments vulnérables de conteneurs actifs ayant une cote de risque critique et dépassant les dates cibles de rattrapage, regroupés par propriétaire de service. 
Éléments du conteneur hautement vulnérables	Liste et ligne 	Nombre d'éléments vulnérables de conteneurs actifs ayant une cote de risque élevée, regroupés par propriétaire de service. 
Éléments hautement vulnérables du conteneur en retard	Liste et ligne 	Nombre d'éléments vulnérables actifs ayant une cote de risque élevée et dépassant les dates cibles de rattrapage, regroupés par propriétaire de service. 

Traduction automatique

Cadre de travail des rapports agrégés pour Réponse aux vulnérabilités pour conteneurs

À l'aide de l'infrastructure des rapports agrégés, vous pouvez créer des rapports pour les données qui impliquent des requêtes à la volée complexes et de longue durée pour de meilleures performances.

Le cadre de travail des rapports agrégés améliore les performances en :

- en utilisant moins de ressources et en rendant les rapports plus rapidement,
- l'agrégation des données et la réutilisation des agrégations et des répartitions (Grouper par) et
- réduire les requêtes à la base de données

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous avez plus d’un million d’éléments vulnérables de conteneur (CVIT), utilisez le cadre de travail des rapports agrégés en même temps que les rapports standard.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur ServiceNow AI Platform (admin) : installer et activer cette Solution d'analyse des performances et génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Analyse des performances Administrateur (pa_admin) : Examinez les agrégations, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.
- Administrateur (sn_vul_cmn.admin) : créer des agrégations.
- VR write(sn_vul_cmn.write) : modifiez les données dans les agrégations et les résultats agrégés.
- VR read (sn_vul_cmn.read) : passez en revue les données dans les agrégations et les résultats agrégés.
- Analyste de vulnérabilité (sn_vul.vulnerability_analyst) : examinez les résultats agrégés.

Information associée

Configurer une agrégation pour les données sources

Exécuter plusieurs agrégations simultanément

Configurer le nombre d’agrégations qui peuvent s’exécuter simultanément

Créer un rapport à l’aide d’une agrégation

Référence Réponse aux vulnérabilités pour conteneurs

Rubriques de référence contenant des informations sur les tables, les rôles et les propriétés installés avec le Réponse aux vulnérabilités pour conteneurs.

Composants installés avec Réponse aux vulnérabilités pour conteneurs

Plusieurs types de composants sont installés lors de l'activation de l'application Réponse aux vulnérabilités pour conteneurs, notamment des tables, des rôles d'utilisateur et des tâches planifiées.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

À partir de la version 2.11 de Réponse aux vulnérabilités pour conteneurs, les propriétés système les plus fréquemment utilisées sont désormais accessibles au sein de l’application Réponse aux vulnérabilités pour conteneurs . Pour afficher ces propriétés système, accédez à **Tous**Réponse aux vulnérabilités pour conteneurs**Propriétés**.

Rôles installés avec Réponse aux vulnérabilités pour conteneurs

Des rôles sont ajoutés avec l'activation de Réponse aux vulnérabilités pour conteneurs.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs et les groupes peuvent voir et faire dans l’application Réponse aux vulnérabilités .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour une première affectation des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration. Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Remarque :

Si vous êtes un client de mise à niveau, l'accès des utilisateurs et des groupes auxquels vous avez affecté les autorisations sn_vul.vulnerability_read et sn_vul.vulnerability_write avant la version 10.3 n'a pas changé. Les utilisateurs et les groupes conservent ces rôles jusqu'à ce que vous les modifiiez. Toutefois, à partir de la version 10.3, vous préférerez peut-être attribuer des rôles granulaires pour plus de contrôle sur ce que les utilisateurs et les groupes peuvent faire et voir dans l'application Réponse aux vulnérabilités . Pour obtenir une vue d'ensemble et plus d'informations sur la gestion de ces rôles, consultez Réponse aux vulnérabilités Profils et rôles granulaires et Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Titre du rôle [name]	Description
V2.10 : sn_vul_container.supprimer	Supprime les enregistrements sou Contient les rôles sn_vul_cmn.de sn_vul_container.delete_vi.
sn_vul_container.ci_manager	Gère la reclassificati des éléme configuration (CI) sans correspon
sn_vul_container.configure_integrations	Configure les intégrations de con
sn_vul_container.configure_vi_granularity	Configure la granularité des élém des conteneurs.
sn_vul_container.create_vi	Peut créer manuellement des élér vulnérables de conteneur.
sn_vul_container.delete_vi	Peut supprimer les éléments vuln conteneur créés manuellement.
sn_vul_container.exception_approver	Approuve les exceptions, les repo fermetures des éléments vulnérab conteneur. Contient le rôle sn_vul.view_manager_works À partir de la version 2.3, l granulaire, sn_vul_containe a été supprimé pour ce rôle vous puissiez accéder aux é vulnérables et aux tâches d de conteneurs affectés à vo groupe, au lieu de tous les vulnérables et tâches de ra conteneurs.
sn_vul_container.approbateur_faux_positif	Approuve ou rejette la fermeture vulnérables du conteneur comme

Traduction automatique.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description
	Contient le rôle sn_vul.view_manager_works
sn_vul_container.manage_assignment_rules	Définit et met à jour les règles d'éléments vulnérables de conteneu
sn_vul_container.manage_auto_close_stale_vi	Configurer les éléments vulnérab conteneurs périmés à fermeture a
sn_vul_container.manage_auto_exception_rule	Gérer (créer/lire/mettre à jour/sup règles d'exception
sn_vul_container.manage_normalized_severity	Peut mettre à jour le mappage po gravité.
sn_vul_container.manage_permissions	Peut affecter des rôles de réponse vulnérabilités des conteneurs aux
sn_vul_container.manage_remediation_targ...	Définit et met à jour les règles de rattrapage de conteneurs.
sn_vul_container.manage_risk_score_confi...	Définit et met à jour les calculate risque, les règles de risque et les déploiement de vulnérabilité pou vulnérables de conteneur.
sn_vul_container.read_all	Peut afficher tous les éléments vu conteneur et les informations con Contient le rôle sn_vul.view_manager_works
sn_vul_container.read_assigned	Peut afficher les éléments vulnéra conteneurs qui vous sont affectés affectés à vos groupes dans l'inte classique ou Espace de travail de dans . Contient le rôle sn_vul.view_rem_workspace **Important :** A partir de 24.0 de Réponse aux vulnéra rôle sn_vul_container.read_ privilège d'accéder Espace remédiation IT au .
sn_vul_container.read_assignment_rules	Peut afficher les éléments vulnéra conteneur Règles d'affectation.
sn_vul_container.read_auto_exception_rule	Règles d'exception en lecture
sn_vul_container.lire_image_découverte_	Peut afficher les éléments détecté
sn_vul_container.read_integrations	Peut afficher les résultats des exé d'intégration.
sn_vul_container.read_normalized_severity	Peut afficher le mappage de grav

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description
sn_vul_container.read_remediation_target...	Peut afficher les règles de cibles
sn_vul_container.read_risk_score_configu...	Peut afficher les calculateurs de s risque, les règles de risque et les déploiement de vulnérabilité pou vulnérables du conteneur.
sn_vul_container.remediation_owner	Lit et écrit les éléments vulnérabl qui leur sont affectés. Les enregis vulnérabilité sont également lisib utilisateur disposant de ce rôle.
sn_vul_container.update_assigned_to	Peut mettre à jour l'affecta éléments vulnérables du co Nécessite sn_vul_container sn_vul_container.write_assi
sn_vul_container.update_assignment_group	Peut mettre à jour le group d'affectation pour les éléme vulnérables du conteneur. Nécessite sn_vul_container sn_vul_container.write_assi
sn_vul_container.update_state	Peut mettre à jour les états éléments vulnérables. Nécessite sn_vul_container sn_vul_container.write_assi
sn_vul_container.vulnerability_admin	Configure toutes les règles, intég etc., pour le Réponse aux vulnéra conteneurs produit.
sn_vul_container.analyste_vulnérabilité	Surveille le rattrapage de tous les vulnérables de conteneur.
sn_vul_container.écrire_tout	Peut mettre à jour tous les éléme et les tâches de rattrapage des co
sn_vul_container.write_assigned	Peut mettre à jour les éléments vu conteneur ou les tâches de rattrap affectées ou qui sont affectées à
sn_vul_container.read_watch_topic	Autorisation de lecture des rubric surveillance pour connaître les vu conteneurs.
sn_vul_container.create_watch_topic	Peut créer des rubriques de surve vulnérabilités des conteneurs.
sn_vul_container.edit_watch_topic	Peut modifier les rubriques de su détecter les vulnérabilités des co
sn_vul_container.manage_exception_configuration	Peut gérer les configurations de g exceptions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables installées avec Réponse aux vulnérabilités pour conteneurs

Les tables sont ajoutées avec l'activation de Réponse aux vulnérabilités pour conteneurs (CVR).

Table	Description
Résultat d'image de conteneur sn_vul_container_image_findings	Stocke des informations sur les vulnérabilités associées, la couche d'image, l'image de Docker, le référentiel d'images et l'image détectée. À partir de la version 2.11.3 de , vous pouvez également afficher le chemin d'accès Réponse aux vulnérabilités pour conteneurs où le résultat est affiché.
Couche d'image du conteneur sn_vul_container_image_layer	Contient les informations de chaque couche d'image. Une image est un fichier statique avec du code exécutable qui peut créer un conteneur sur un système informatique.
Package d'images du conteneur sn_vul_container_image_package	Fournit des informations sur les packages où se trouvent les vulnérabilités. Les détails du package binaire sont également fournis sous forme de valeurs séparées par des virgules. À partir de la version 2.11.3 de Réponse aux vulnérabilités pour conteneurs, vous pouvez également afficher l'URL du package (PURL).
Élément vulnérable de conteneur sn_vul_container_image_vulnerable_item	Contient les détails de chaque résultat et de la vulnérabilité correspondante. À partir de la version 2.11.3 de Réponse aux vulnérabilités pour conteneurs, vous pouvez également afficher des informations sur la date de la dernière analyse d'une image exécutée en tant que conteneur.
Entrée de vulnérabilité (v2.11.3) sn_vul_entry	Fournit des informations sur la gravité d'une CVE et toute information supplémentaire envoyée par Prisma.
Image du conteneur détecté sn_vul_container_image	Fournit des informations sur l'ID de l'image, l'image Docker et le référentiel d'images. Il stocke également les informations de la couche et les associe à l'image découverte. À partir de la version 2.11.3 de Réponse aux vulnérabilités pour conteneurs, il fournit également des informations sur la synthèse d'image d'une image Docker et la date de la dernière analyse d'une image s'exécutant en tant que conteneur et registre.
Recherche de correspondances sn_vul_container_finding_m2m_vul_item	Relation M2M entre les résultats d'image de conteneur et les éléments vulnérables de conteneur (CVIT).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Éléments vulnérables à fermeture automatique sn_vul_container_image_auto_close_config	Contient des informations sur la façon de fermer les résultats d'image de conteneur périmés et de déployer l'état sur les CVIT.
Clés de vulnérabilité de l'image du conteneur sn_vul_container_image_vulnerability_keys	Contient la configuration de granularité pour la création de CVIT à partir des résultats de l'image du conteneur.
Services associés au Doker sn_vul_container_m2m_ci_services	Contient tous les services aux entreprises associés à une image de conteneur.
Nombres de conteneurs VR sn_vul_container_vr_container_counts	Contient la moyenne mobile des instances de conteneur créées à partir d'une image de conteneur au cours des 90 derniers jours.
Élément de tâche de rattrapage de conteneur sn_vul_container_m2m_vul_group_item	Table M2M entre le CVIT et les tâches de rattrapage de conteneur.
Tâche de rattrapage de conteneur sn_vul_container_vulnerability	Contient des tâches de rattrapage de conteneurs.
Manifeste de tâche de rattrapage de conteneur sn_vul_container_rt_manifest	Toutes les mises à jour de la tâche de rattrapage seront effectuées à l'aide de cette table de manifestes par les travaux planifiés.

Tâches planifiées installées avec Réponse aux vulnérabilités pour conteneurs

Des tâches planifiées sont ajoutées à l'activation d'Réponse aux vulnérabilités pour conteneurs.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Tâche planifiée	Description
Associer les VI de conteneurs existants à la règle d'exception automatique	Associe automatiquement la règle d'exception automatique aux éléments vulnérables de conteneur existants (CVIT).
Vérifier l'expiration du report de l'élément vulnérable de conteneur	Envoie des notifications si les éléments vulnérables du conteneur ou les vulnérabilités du conteneur ont expiré (et s'ils expirent dans une semaine).
Nombre de conteneurs de Vulnerability Response (Application : Vulnerability Response et Configuration	S'exécute quotidiennement pour remplir la table sn_vul_container_vr_container_counts qui calcule la moyenne mobile de 90 jours pour les conteneurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Compliance pour conteneurs)	
CVIT à fermeture automatique	Ferme automatiquement les éléments de vulnérabilité de conteneur qui correspondent à la condition définie dans la configuration de fermeture automatique. Leur état est changé en « corrigé ».
Calculer la criticité opérationnelle pour CVIT	Traite tous les CVIT actifs et met à jour le champ Criticité opérationnelle, en fonction des services affectés de l'image Docker de la CVIT.
Fermer annuler les CVIT qui n'ont pas d'image Docker associée	Expire automatiquement les CVIT auxquels aucun CI n'est associé. Leur état est défini sur Fermé et leur sous-état sur Annulé.
Calculer le nombre de VI associés pour la tâche de rattrapage de conteneur	Calcule les nombres sur les enregistrements de tâche de rattrapage de conteneur.
Déployer les valeurs d'éléments vulnérables du conteneur sur la vulnérabilité et le groupe	Calcule les vulnérabilités et les déploiements de groupes pour les éléments vulnérables des conteneurs. **Remarque :** À partir de la version 2.10 de Réponse aux vulnérabilités pour conteneurs, la tâche planifiée est améliorée pour créer des tâches en arrière-plan avec des options multithreading. Cette mise à niveau implique de segmenter la tâche en plusieurs tâches enfants plus petites, qui sont exécutées en parallèle ou simultanément. Cette modification permet de traiter plusieurs enregistrements simultanément, ce qui accélère considérablement la tâche globale.

Réponse aux vulnérabilités pour conteneurs glossaire

En savoir plus sur les termes et concepts propres à Réponse aux vulnérabilités pour conteneurs.

Termes clés

Conteneur

Unité logicielle, qui regroupe le code et toutes ses dépendances afin que l'application s'exécute de manière transparente et fiable d'un environnement informatique à un autre.

Image du conteneur

Un fichier statique avec du code exécutable qui peut créer un conteneur sur un système informatique. Une image de conteneur ne peut pas être modifiée et peut donc être déployée de manière cohérente dans n'importe quel environnement.

Grappe

Ensemble d'ordinateurs de travail, appelés nœuds, qui exécutent des applications conteneurisées.

Docker

Logiciel pour créer, déployer et gérer des conteneurs d'applications sur des serveurs et dans le cloud.

Image de Docker

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fichier de modèle contenant le code, les bibliothèques requises, les configurations, etc. Le fichier est utilisé pour lancer des instances de conteneur. Il se compose d'une union de systèmes de fichiers en couches.

Fichier Dockerfile

Fichier texte contenant des instructions pour créer des images de conteneur en ajoutant plusieurs couches. Par exemple, la superposition du code de base Ubuntu, Nginx et App.

Composition de Docker

Un outil pour définir et exécuter des applications complexes avec Docker. Avec Compose, vous pouvez définir une application multi-conteneur dans un seul fichier.

Conteneur Docker

Un conteneur Docker est une instance d'exécution lancée à partir d'une image Docker.

Couche d'image

Un calque est une modification apportée à une image. Il est représenté par une instruction dans le Dockerfile. Les calques sont appliqués en séquence à l'image de base pour créer l'image finale.

Référentiel d'images

Une collection d'images Docker avec différentes balises ou versions.

Étiquettes d'images

Ensemble de paires clé-valeur stockées avec l'image en tant que métadonnées.

Espace de noms

Abstraction utilisée par Kubernetes pour prendre en charge l'isolation de groupes de ressources au sein d'un seul cluster.

Pod

Un ensemble de conteneurs en cours d'exécution (une autre abstraction au-dessus d'un conteneur).

Registre

Service hébergé contenant des référentiels d'images.

Service

Une façon abstraite d'exposer une application exécutée sur un ensemble de pods en tant que service réseau.

Balise

Une balise est une étiquette appliquée à une image Docker dans un référentiel d'images donné. Les balises sont la façon dont les différentes images d'un référentiel sont distinguées les unes des autres.

Traduction automatique

Champs du formulaire Élément vulnérable de conteneur

Les éléments vulnérables de conteneur (CVIT) sont automatiquement créés lors des importations d'intégration de vulnérabilité tierce.

Champs du formulaire d'élément vulnérable de conteneur

À l'exception des champs **Groupe d'affectation**, **Affecté à** et **Notes**, tous les autres champs de la CVIT sont en lecture seule.

Champ	Description
Numéro	Identificateur CVIT généré automatiquement pour cet enregistrement.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Scanner qui a identifié la vulnérabilité.
Cote de risque	**Score de risque** quantifié séparant les éléments vulnérables en Critique, Élevé, Moyen, Faible et Aucun.
Score du risque	Quantité calculée de risque que la CVIT représente pour votre environnement.
Règle de cible de remédiation	Règle de cible de rattrapage selon laquelle la date cible de rattrapage est calculée.
Cible de remédiation	Date à laquelle les CVIT doivent être corrigés, dès lors qu'ils ont été identifiés pour la première fois. S'affiche uniquement le cas échéant.
Statut de la remédiation	État du rattrapage pour la CVIT.
Vulnérabilité	ID de la vulnérabilité associée à l'élément vulnérable de cette application.
Image de Docker	Fichier de modèle contenant le code, les bibliothèques requises, les configurations, etc. Le fichier est utilisé pour lancer des instances de conteneur. Il se compose d'une union de systèmes de fichiers en couches.
Image du conteneur détecté	Enregistrement unique pour chaque ID d'image.
Image de base	Image de base utilisée pour créer des applications conteneurisées, contenant le système d'exploitation et les bibliothèques essentiels. Il sert de point de départ pour la création et la personnalisation d'applications dans des environnements tels que Docker.
Grappes d'images	Groupes d'images connexes utilisées dans divers contextes, tels que la mise en grappe d'images similaires dans l'apprentissage machine ou d'images de conteneurs dans un référentiel.
Espace de noms d'image	Utilisé pour organiser et isoler les images de conteneurs dans un registre, permettant à différentes équipes ou projets de gérer des collections séparées.
État	Ce champ est défini par défaut sur **Ouvert** lors de sa création. Consultez États des éléments vulnérables de l'application (AVI) pour plus d'informations sur la façon dont les états sont mappés.
Groupe d'affectation	Groupe sélectionné pour travailler sur cette CVIT.
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cette CVIT. Peut être ajouté ou modifié manuellement par un gestionnaire App-Sec.
Créées	Date et heure de création d'une CVIT.
Dernières ouvertures	Date et heure les plus récentes auxquelles la CVIT est rouverte.
Mis à jour	Date et heure de la dernière modification de la CVIT.
Premier trouvé (v2.12.1)	Date à laquelle la vulnérabilité a été trouvée pour la première fois. À partir de la v2.12.1, vous pouvez voir la date et l'heure précises de sa première découverte, ce qui garantit la clarté et tient compte des différents fuseaux horaires. Pour renseigner les premiers détails de date et d'heure trouvés, l'intégration doit être réexécutée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Dernier trouvé (v2.12.1)	Date de la dernière découverte de la vulnérabilité. À partir de la version 2.12.1, vous pouvez voir la date et l'heure précises de la dernière découverte, ce qui garantit la clarté et tient compte des différents fuseaux horaires. Pour renseigner les derniers détails de la date et de l'heure trouvés, l'intégration doit être réexécutée.
Date de résolution (v2.12.1)	Date à laquelle la vulnérabilité a été résolue. À partir de la version 2.12.1, vous pouvez voir la date et l'heure précises auxquelles il a été résolu, ce qui garantit la clarté et tient compte des différents fuseaux horaires. La date de résolution est renseignée lorsque la CVIT est résolue dans le cadre du workflow.
Dernière ouverture (v2.12.1)	Date de la dernière ouverture de la vulnérabilité. À partir de la version 2.12.1, vous pouvez voir la date et l'heure précises de la dernière ouverture, ce qui garantit la clarté et tient compte des différents fuseaux horaires. La tâche *`Add default values for last_opened_dt_tm from last _opened`* planifiée renseigne les données de ce champ. Elle ne doit être exécutée qu'une seule fois à la demande.
Vulnérabilité	
Résumé	Description de la vulnérabilité.
Gravité	Degré de gravité normalisé de cette vulnérabilité. Les cartes de gravité sont fournies pour la base de données de vulnérabilité nationale (NVD) et avec les intégrations tierces ServiceNow.
Score de vulnérabilité (v3)	Score CVSS (Common Vulnerability Scoring System) v3.
Score de vulnérabilité (v2)	Score CVSS v2.
Existence de l'exploit	Oui, si au moins un exploit est associé aux vulnérabilités associées à cet élément vulnérable.
Vecteur d'attaque de l'exploit	Vecteur d'attaque le plus vulnérable des exploits pour les vulnérabilités associées à cet élément vulnérable.
Niveau de compétence de l'exploit	Niveau de compétence le plus bas requis pour exploiter les vulnérabilités associées à cet élément vulnérable.
Date de publication	Date de publication de la vulnérabilité.
Dernière modification	Date de la dernière modification de la vulnérabilité.
Menace	Informations pertinentes sur la menace. Extrait de l'enregistrement d'entrée vulnérable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Tous les changements apportés ici mettent à jour l'enregistrement de l'entrée vulnérable.
Notes de rattrapage	Solution pertinente à la menace, extraite de l'enregistrement d'entrée vulnérable.
Notes	
Notes de travail	Toute information pertinente. Sélectionnez la zone de texte pour les notes de travail afin d'ajouter des informations.
Conclusions de l'image	Résultats de l'analyse des images de conteneurs pour détecter les vulnérabilités.
Approbations demandées	Demande d'approbation émise pour la CVIT.
Approbations de changement de l'état	Demande d'approbations de changement de l'état émise pour la CVIT.

Calculs de l'âge d'une CVIT :

- La colonne Âge de la liste des CVIT affiche la durée (format : Jours HH :MM :SS) pendant laquelle une CVIT est active. La valeur Âge est nulle pour une CVIT fermée.
- La colonne Âge fermé de la liste des CVIT affiche la durée (format : Jours HH :MM :SS) pendant laquelle une CVIT est active avant sa fermeture. Pour les CVIT autres qu'à l'état Fermé, la valeur Âge clôturé est égale à zéro.

Pour plus d'informations sur la personnalisation du calcul de l'âge et des durées d'âge fermé, consultez l'article KB1703270 .

Formulaire Configuration des calculs dans le cloud Prisma

Le formulaire de configuration de calcul dans le cloud Prisma est accessible à partir du module d'intégration de calcul dans le cloud Prisma.

Pour afficher le formulaire de configuration des calculs dans le cloud Prisma, accédez à **Tous** > **Intégration des calculs dans le cloud Prisma** > **Administration** > **Configuration**.

Configuration des calculs dans le cloud Prisma

Champ	Description
Instance d'intégration	Nom de la nouvelle instance d'intégration. Vous pouvez créer une instance ou cliquer sur l'icône de recherche pour sélectionner une instance existante.
URL de base de l'API	URL à intégrer à Prisma Cloud Compute.
Nom d'utilisateur	Nom d'utilisateur pour accéder à Prisma Cloud Compute.
Mot de passe	Mot de passe pour accéder à Prisma Cloud Compute.
Serveur MID	Une application Java qui s'exécute en tant que service Windows ou démon UNIX sur un serveur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration des calculs dans le cloud Prisma (suite)

Champ	Description
	de votre réseau local. Le serveur MID permet la communication et le mouvement de données entre une instance et des ServiceNow applications, sources de données et services externes.
Utiliser des projets	Option permettant de configurer les projets. Lorsque vous cochez la case, vous pouvez sélectionner des projets dans la page de configuration et exécuter les intégrations en fonction des projets configurés pour renseigner les détails spécifiques au projet. **Remarque :** Si cette case est cochée, l'onglet **Configurer les projets** est activé. Cliquez sur **Suivant** pour poursuivre la configuration des projets.

Formulaire de demande d'exception

Demandez des exceptions à la politique à l'aide de l'aptitude de GRC gestion des exceptions de politique de l'application à partir de Réponse aux vulnérabilités pour conteneurs.Gestion de la politique et de la conformité

Pour afficher le formulaire de configuration des calculs dans le cloud Prisma, accédez à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Éléments vulnérables de conteneurs** (ou **Tâches de remédiation**)>**Toutes**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.

Formulaire de demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date actuelle. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et à laquelle l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de demande d'exception (suite)

Champ	Description
	Remarque : Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale de l'exception (jours)** que vous définissez pour la politique dans Politique et conformité. Pour plus d'informations, consultez Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés au motif pour lequel cette demande est effectuée. Ce champ doit être renseigné par le propriétaire du rattrapage.

Formulaire Règle d'exception

Créez une règle pour demander automatiquement une exception pour une condition spécifique pour un groupe d'éléments vulnérables de conteneurs (CVIT), telle qu'une règle avec une condition basée sur la gravité de vulnérabilité de ces CVIT. Avec cette règle, vous pouvez différer automatiquement les CVIT nouveaux et existants s'ils correspondent à la condition de règle approuvée.

Pour afficher le formulaire Règle d'exception, accédez à **Tous** > **Réponse aux vulnérabilités du conteneur** > **Administration** > **Règles d'exception**.

Formulaire Règle d'exception

Champ	Description
Nom	Nom de la règle d'exception.
Début de validité	Date à partir de laquelle cette règle est active pour différer les CVIT.
Date de fin de validité	Date à partir de laquelle la tâche de rattrapage cesse d'accepter de nouveaux CVIT.
Motif	Raison de la création de cette règle d'exception.
Groupe d'affectation	Groupe auquel la tâche de rattrapage créée pour le suivi des CVIT différés est affectée.
Informations supplémentaires	Informations supplémentaires que le demandeur souhaite fournir à l'approbateur. Ces informations sont renseignées dans le champ Description de la tâche de rattrapage.
Condition	Condition de filtre pour les CVIT qui peut être définie lors du traitement des CVIT.
Exécuter sur les données existantes	Option qui vous permet d'exécuter cette règle sur des données existantes la première fois que cette règle est exécutée.
Étape du workflow	État d'approbation actuel de la règle d'exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Règle d’exception (suite)

Champ	Description
État	État de la règle d’exception.
Ordre d'exécution	Ordre unique pour chaque règle d’exception
Reporté jusqu'à	Date à laquelle les VUL et les CVIT sont reportés. À cette date, la VUL créée est fermée, tous les CVIT sortent du groupe et les règles de groupe sont réappliquées.

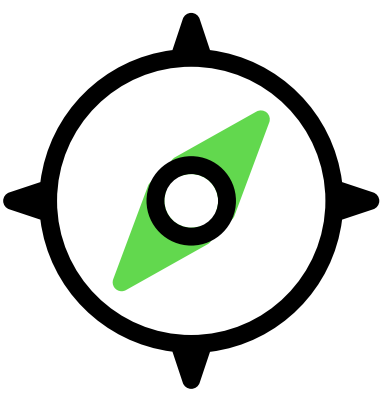
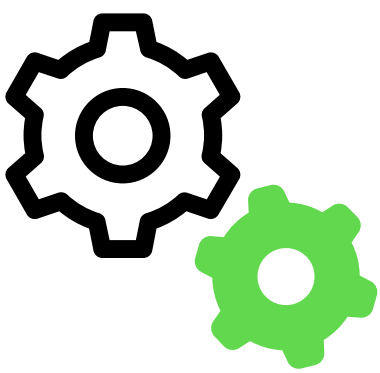
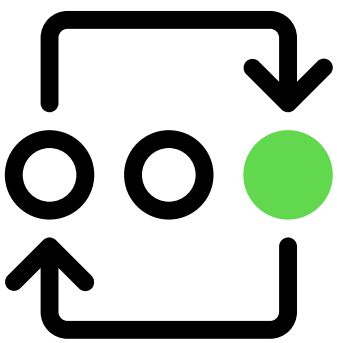
Conformité de la configuration

Il s’agit ServiceNow® Conformité de la configuration d’une application SCA (Secure Configuration Assessment) qui regroupe les résultats de l’analyse à partir d’intégrations avec des applications tierces d’analyse de configuration. Vous pouvez prioriser les problèmes de conformité de la configuration à l’aide de votre Base de données de gestion des configurations (CMDB). Conformité de la configuration s’intègre étroitement au processus de Gestion des changements informatiques pour corriger vos configurations non conformes.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Conformité de la configuration

Explorer	Installer, installer et configurer	Intégrer
		
En savoir plus sur les concepts et les fonctionnalités de Configuration Compliance	Configurer Configuration Compliance	Étendre Configuration Compliance en l’intégrant à d’autres applications

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

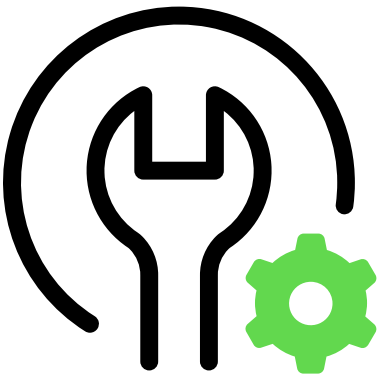
Conformité de la configuration (suite)

Utiliser les espaces de travail Vulnerability Response



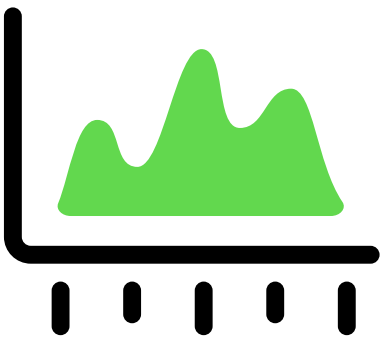
Découvrez comment surveiller, gérer et corriger les problèmes de configuration dans les espaces de travail Gestionnaire des vulnérabilités, Rattrapage informatique et Évaluation des vulnérabilités.

Corriger



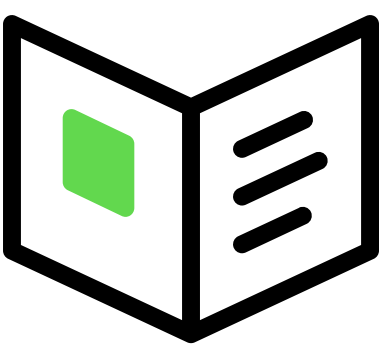
Découvrez comment corriger vos actifs non conformes avec Configuration Compliance

Analyses et rapports



Afficher les rapports et les tableaux de bord dans Configuration Compliance

Référence



Obtenir des détails sur les composants Configuration Compliance tels que les champs, les tables et les propriétés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Explorer Conformité de la configuration

Utilisez les résultats des tests obtenus à partir d'intégrations SCA (Secure Configuration Assessment) tierces pour vérifier la conformité aux politiques de sécurité ou d'entreprise. Identifiez, classez par ordre de priorité et corrigez les éléments de configuration non conformes.

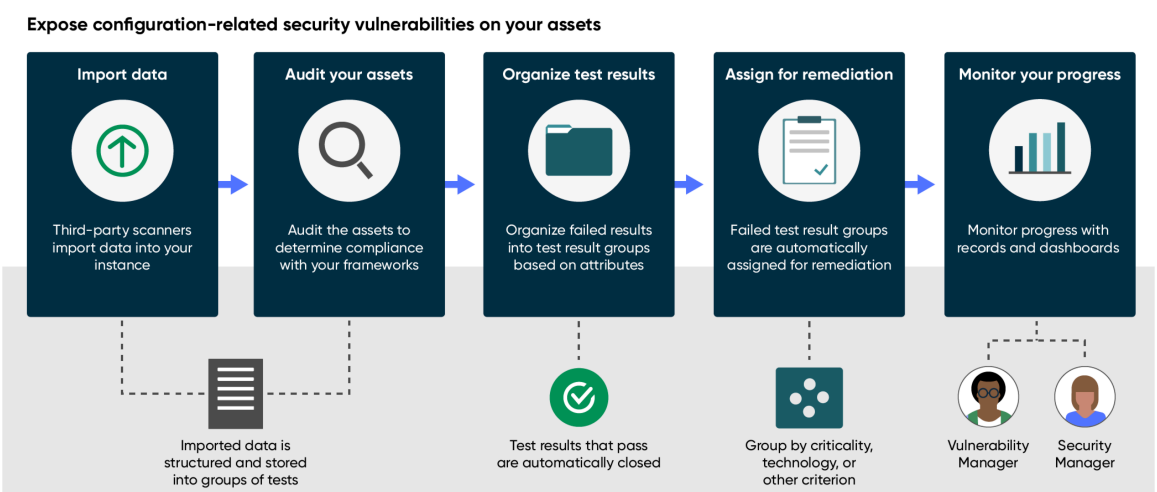
Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Qu'est-ce que Conformité de la configuration ?

L'application ServiceNow® Conformité de la configuration vous permet de hiérarchiser et de corriger rapidement et efficacement les vulnérabilités liées à la configuration les plus critiques de votre environnement. Conformité de la configuration est disponible par abonnement dans le ServiceNow® Store.



Fonctionnalités principales de Conformité de la configuration

Utilisez le dans votre ServiceNow AI Platform® pour vous aider à exposer et à corriger vos vulnérabilités de sécurité les plus critiques liées à la Base de données de gestion des configurations (CMDB) configuration. Concentrez vos ressources de rattrapage sur les activités qui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

réduisent le risque le plus. Rationalisez le processus de rattrapage pour les personnes concernées par la sécurité, l'informatique et votre processus business. L'application Conformité de la configuration comprend les fonctionnalités clés suivantes :

- Grâce aux intégrations tierces prises en charge, importez automatiquement les politiques, les tests, les sources de référence et les technologies. Consultez la section Intégrations de Conformité de la configuration pour plus d'informations sur les intégrations prises en charge.
- Corrélez les politiques et les tests aux éléments de configuration (actifs) pour identifier les vulnérabilités liées à la configuration et vous aider à vérifier que vos actifs sont en conformité avec vos politiques et contrôles.
- Unifiez l'évaluation, l'affectation et la correction de la configuration sur tous vos actifs.
- Le contenu de l'analyse de la configuration peut être importé à partir des principales applications d'intégration de l'écosystème SCA (Secure Configuration Assessment).
- Les résultats de configuration, les échecs de test, peuvent être regroupés et acheminés automatiquement en fonction des compétences du spécialiste du rattrapage et des domaines de responsabilité. Des flux de travail intelligents et une intégration étroite à Change Management permettent un transfert fluide des tâches entre les groupes.
- Lorsqu'ils sont utilisés avec l'application (GRC), les ServiceNow Gouvernance, risque et conformité tests de configuration peuvent Conformité de la configuration être déployés sur leurs contrôles GRC correspondants.
- Grâce à la gestion des changements améliorée, créez des demandes de changement préremplies directement à partir du service informatique pour vous aider dans vos tâches de Conformité de la configuration rattrapage qui nécessitent des ressources supplémentaires.
- Grâce aux tableaux de bord, affichez les mesures d'état de rattrapage sur les enregistrements de tâche de rattrapage, de test de conformité et de politique.

Qui utilise Conformité de la configuration

Conformité de la configuration Les activités peuvent impliquer de nombreux niveaux de gestion.

- Administrateurs système
- Administrateurs de vulnérabilité
- Responsables des vulnérabilités
- Analystes de vulnérabilité
- Administrateurs de conformité

Conformité de la configuration Les tâches impliquent les rôles suivants.

- sn_vulc.admin : peut lire, écrire, supprimer
- sn_vulc.write — peut lire et écrire
- sn_vulc.remediation_owner : autorisation de lecture et de mise à jour des enregistrements affectés

  Remarque : Le rôle sn_vulc.remediation_owner est également affecté automatiquement lorsqu'un utilisateur est affecté au rôle itil.

- sn_vulc.read : peut lire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conformité de la configuration et Opérations de sécurité

Lorsque le Qualys Vulnerability Integration et le sont installés, l'accès Tenable Vulnerability Integration à Réponse aux vulnérabilités devient disponible. Vous pouvez avoir plusieurs déploiements de ces intégrations. Les données provenant de chaque déploiement sont identifiées et disponibles dans une instance unique de GRC.

Versions disponibles pour Zurich

Version de mise en production	Notes de publication
Conformité de la configuration v15.4	Notes de publication de Configuration Compliance . Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response Reportez-vous à la section Installation, installation et configuration de l'application Conformité de la configuration pour plus d'informations sur l'activation de l'application.

Conformité de la configuration Données importées

L'application Conformité de la configuration importe les politiques, les tests, les sources de référence et les résultats des tests à partir d'intégrations tierces et les stocke dans des modules pour consultation.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Intégrations prises en charge

Les intégrations tierces importent les résultats de l'évaluation de la configuration, les groupes de tests, les tests, les technologies, les sources de référence et les résultats des tests dans l'application Conformité de la configuration . Les gestionnaires de vulnérabilité ou les analystes de vulnérabilité peuvent utiliser ces données pour identifier les vulnérabilités liées à la configuration de vos actifs et y répondre.

Pour en savoir plus sur les intégrations prises en charge, reportez-vous à la section Intégrations de Conformité de la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupes de test

Les groupes de tests sont liés à des documents et des enregistrements de tests faisant autorité. Un groupe de tests de configuration définit les groupes de tests. Les groupes de tests s'alignent généralement sur une classe de technologie, par exemple Windows, bases de données Oracle, Cisco IOS, et sont souvent dérivés de la norme industrielle primaire. Les groupes de tests peuvent être modifiés pour répondre aux besoins de l'organisation. Un seul test de configuration peut appartenir à plusieurs groupes de tests.

Intégration	Description
Qualys Vulnerability Integration	Les groupes de tests sont récupérés et les ID de contrôle sont renseignés par la tâche planifiée, les **politiques de PC Qualys** à 1h00 du matin. Vous pouvez afficher la tâche planifiée en accédant à **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Politiques de PC Qualys**. **Remarque :** Si vous choisissez d'exécuter l'intégration manuellement, exécutez d'abord **Qualys PC Policies** .
Tenable Vulnerability Integration	L'intégration des résultats de conformité de la tâche Tenable.io planifiée importe les politiques. Si vous choisissez d'exécuter les intégrations manuellement, exécutez-les dans l'ordre suivant jusqu'à ce que vous rapprochiez les actifs ignorés avec les données d'évaluation : • Tenable.io Intégration des actifs • Tenable.io Intégration des résultats de la conformité • Tenable.io Intégration du remplissage des résultats de la conformité • Tenable.io Intégration des actifs • Tenable.io Intégration du remplissage des résultats de la conformité Pour afficher l'enregistrement de politique, accédez à **Tous** > **Configuration Compliance** > **Groupes de tests**. Pour identifier et créer correctement les enregistrements de groupes de tests, les informations d'audit des groupes de tests sont importées et affichées dans le champ **Description brève** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests

Les tests sont des bibliothèques d'enregistrements de données qui organisent les analyses des ressources informatiques. Les tests de configuration définissent la manière dont une classe d'actifs technologiques doit être gouvernée.

Un Conformité de la configuration test est le mécanisme utilisé par les applications d'intégration tierces pour regrouper les actifs par type de vulnérabilité. Certaines solutions d'analyse VA tierces telles que Qualys ont de très grandes bibliothèques de tests (jusqu'à 8 000) qui sont mappées à des politiques et des « cadres » de sources faisant autorité.

Un test peut avoir plusieurs valeurs, un-à-plusieurs, attendu ou réel, etc. Un test est tout ce qui peut être utilisé pour identifier une classe d'actif logiciel ou matériel qui n'est pas conforme. Par exemple, un numéro de version ou de matériel.

Intégration	Description
Qualys Vulnerability Integration	La tâche planifiée, **Qualys PC Controls**, récupère les tests. Vous pouvez afficher la tâche planifiée en accédant à **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Contrôles de PC Qualys**. **Remarque :** Si vous choisissez d'exécuter l'intégration manuellement, exécutez les **contrôles du PC Qualys** après **les politiques du PC Qualys**.
Tenable Vulnerability Integration	L'intégration des résultats de conformité de la tâche Tenable.io planifiée importe les tests de configuration (tests). Si vous choisissez d'exécuter les intégrations manuellement, exécutez-les dans l'ordre suivant jusqu'à ce que vous rapprochiez les actifs ignorés avec les données d'évaluation : • Tenable.io Intégration des actifs • Tenable.io Intégration des résultats de la conformité • Tenable.io Intégration du remplissage des résultats de la conformité • Tenable.io Intégration des actifs • Tenable.io Intégration du remplissage des résultats de la conformité Pour afficher l'enregistrement du test de configuration, accédez à **Configuration Compliance** > **Tests**. Sur l'enregistrement, les données importées sont affichées dans le champ **Brève description** et les onglets État du rattrapage, Description et Rattrapage. Les données sont également

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
	affichées dans les liens connexes **Contenus des documents de référence**, **Politiques** et **Résultats des tests** .

Technologies

L'une des techniques utilisées par les scanners de vulnérabilité tiers pour créer des groupes de test d'éléments de configuration logiciels et matériels à analyser consiste à les organiser par technologie. Les technologies sont une bibliothèque importée de systèmes d'exploitation, d'appareils réseau, de bases de données et d'applications associés à des politiques. Les tests ont plusieurs implémentations pour différentes technologies. La remédiation est également spécifique à la technologie.

Vous pouvez afficher les technologies applicables pour un test, afin de mieux comprendre à quels types d'actifs logiciels ou matériels le contrôle peut être appliqué. CentOS 7.x, Windows 8.1, Windows 2016 Server, entre autres, sont des exemples de technologies pouvant être appliquées aux contrôles. La liste des technologies est en lecture seule et correspond aux technologies définies dans l'application Qualys Cloud Platform .

Les technologies sont importées uniquement pour les évaluations de configuration liées à la base de données. Le (s'il n'est *db_type* pas vide) de l'importation est utilisé pour créer une technologie. Affichez les technologies renseignées dans la section Technologies sur les enregistrements de tests de configuration, les enregistrements de résultats de tests, les enregistrements de politique et à **Configuration Compliance** > **Données associées** > **Technologies**.

Sources d'autorité

Conformité de la configuration utilise des sources et des contenus des documents de référence lors de la génération d'alertes de vulnérabilité pour les tests. Les sources faisant autorité correspondent généralement à des sections de normes industrielles publiées, telles que « NIST 800-53 version 3 (2009) 3 : 2009, SA-4 ».

Remarque : Dans le Qualys Vulnerability Integration, cette combinaison est appelée cadre.

Les sources et les citations faisant autorité (également appelées mandats) sont importées des scanners de vulnérabilité tiers.

Les notices sources faisant autorité contiennent des références à des informations sur des problèmes connus de configuration logicielle et matérielle provenant d'experts dans le domaine de la sécurité informatique. Ils définissent les exigences en matière de politiques et de procédures de sécurité. Les tests de configuration peuvent référencer plusieurs sources faisant autorité via des citations. Les sources faisant autorité peuvent rendre compte de la conformité à une norme donnée en vue d'un audit.

Intégration	Description
Qualys Vulnerability Integration	La tâche planifiée, **Détail des politiques de PC Qualys**, récupère les sources et les contenus des documents de référence faisant autorité. Vous pouvez afficher cette tâche planifiée en accédant à **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Détail des politiques de PC Qualys**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
	Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez **Détail des politiques du PC Qualys** après **Politiques du PC Qualys**.
Tenable Vulnerability Integration	La tâche Tenable.io planifiée Intégration des résultats de conformité importe les sources faisant autorité dans le cadre des données de contenu des documents de référence. Si vous choisissez d'exécuter les intégrations manuellement, exécutez-les dans l'ordre suivant jusqu'à ce que vous rapprochiez les actifs ignorés avec les données d'évaluation : • Tenable.io Intégration des actifs • Tenable.io Intégration des résultats de la conformité • Tenable.io Intégration du remplissage des résultats de la conformité • Tenable.io Intégration des actifs • Tenable.io Intégration du remplissage des résultats de la conformité Les données sont affichées sur le lien connexe **Contenu des documents de référence** sur les enregistrements de tests de configuration.

Résultats des tests

Conformité de la configuration ne calcule pas les résultats des tests, mais les importe dans le cadre d'une intégration tierce. Une fois visibles dans , ils sont corrigés à Conformité de la configuration l'aide de **tâches de rattrapage**. Consultez Conformité de la configuration corrélation pour plus d'informations.

Intégration	Description
Qualys Vulnerability Integration	Vous pouvez récupérer les résultats des tests de l'une des manières suivantes : La tâche planifiée, **Résultats des PC Qualys**, récupère les résultats des tests. Vous pouvez afficher cette tâche planifiée en accédant à **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Résultats PC Qualys**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
	Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez **Résultats du PC Qualys** après **Politiques du PC Qualys** et **Détails des politiques du PC Qualys**. L'importation **des résultats de PC Qualys** utilise le paramètre dans l'onglet**Détails d'intégration***`Start Time`*. Toutes les autres Conformité de la configuration importations apportent toutes les données disponibles, quel que soit le *`Start Time`*. Lorsque l'importation des **résultats du PC Qualys** est terminée, un événement est déclenché pour déclencher les calculs de fin d'importation. Pour plus d'informations, reportez-vous à la section Conformité de la configuration États. Alternativement, à partir de la version 14.5, vous pouvez également exécuter les intégrations suivantes pour récupérer les résultats des tests : • Qualys Intégration de l'hôte de la politique PCRS : récupère les ID d'hôte pour chaque politique. Pour afficher cette tâche planifiée, accédez à : Intégration de vulnérabilité Qualys > Intégrations principales > Intégration de l'hôte de politique Qualys PCRS. **Remarque :** Si vous choisissez d'exécuter l'intégration manuellement, exécutez l'intégration de l'hôte de politique Qualys PCRS après Politiques du PC Qualys et Détails des politiques du PC Qualys. Une fois cette tâche planifiée terminée, elle déclenche automatiquement l'intégration des résultats des tests Qualys PCRS. • Qualys Intégration des résultats des tests PCRS : récupère les résultats des tests pour chaque ID d'hôte. Pour afficher cette tâche planifiée, accédez à Intégration de vulnérabilité Qualys > Intégrations primaires > Intégration des résultats des tests Qualys PCRS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration	Description
	Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez l'intégration des résultats des tests Qualys PCRS après les intégrations des scripts Qualys PC Policies, Qualys PC Policies Detail et Qualys PCRS Policy Host Integration. Cette intégration utilise le paramètre Heure de début dans l'onglet Détails de l'intégration.
Tenable Vulnerability Integration	L'intégration des résultats de conformité de la tâche Tenable.io planifiée importe les résultats des tests. Si vous choisissez d'exécuter les intégrations manuellement, exécutez-les dans l'ordre suivant jusqu'à ce que vous rapprochiez les actifs ignorés avec les données d'évaluation : • Tenable.io Intégration des actifs • Tenable.io Intégration des résultats de la conformité • Tenable.io Intégration du remplissage des résultats de la conformité • Tenable.io Intégration des actifs • Tenable.io Intégration du remplissage des résultats de la conformité Pour afficher l'enregistrement du test de configuration, accédez à **Configuration Compliance** > **Résultats des tests**. Sur l'enregistrement, les données importées sont affichées dans les champs**Test** et **Élément de configuration** . Les données sont également affichées dans les onglets **Valeurs attendues**, **Valeurs réelles** et **Rattrapage** . Les liens connexes **Tâches de remédiation** et **Historique des résultats des tests** sont renseignés.

Détection de Conformité de la configuration

Conformité de la configuration les données sont importées à partir d'applications tierces de scanner SCA. Ils structurent des groupes de tests logiciels et matériels dans des enregistrements de données pour accélérer la réalisation des évaluations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Lorsqu'une importation est terminée, un événement est envoyé pour indiquer les actions de fin d'importation. Pour chaque tâche de rattrapage active, les actions suivantes sont mises en œuvre :

- Les tâches de rattrapage résolues avec des résultats échoués reviennent à l'état **En attente d'implémentation** .
- Les tâches de rattrapage pour lesquelles tous les résultats ont été réussis sont **fermées**.
- L'état des résultats des tests qui sont dans les tâches de rattrapage actives est mis à jour.
- L'indicateur indiquant si un résultat fait partie d'une tâche de rattrapage active est mis à jour.

Conformité de la configuration corrélation

Conformité de la configuration Assure la hiérarchisation et le regroupement des résultats des tests (dans une tâche de rattrapage) pour faciliter la remédiation des problèmes de non-conformité.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Priorisation centrée sur les actifs

Les analyses de configuration peuvent produire un grand nombre de résultats. Classer les résultats par ordre de priorité pour une meilleure réduction des risques. La priorité inclut à la fois la criticité des tests de configuration et la criticité des actifs. La priorité du résultat du test de configuration est exprimée sous la forme d'un score de risque sur une échelle de 0 à 100. Les groupes de calculateurs calculent le score de risque et peuvent être personnalisés.

Lorsque l'importation tierce est terminée, Conformité de la configuration envoie un événement pour indiquer les actions de fin d'importation. Pour chaque groupe de résultats actif, les actions suivantes sont mises en œuvre :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les tâches de rattrapage résolues avec des résultats échoués reviennent à l'état **En attente d'implémentation** .
- Tâches de rattrapage dans lesquelles tous les résultats obtenus sont **fermés**.
- L'état des résultats des tests qui sont dans les tâches de rattrapage actives est mis à jour.
- L'indicateur indiquant si un résultat fait partie d'une tâche de rattrapage active est mis à jour.

Tâches de remédiation Ordre de priorité

Lorsque les résultats des tests appartiennent à plusieurs groupes, **l'état** d'un résultat de test est dérivé selon un ordre de priorité.

Les champs **État** et **Résolution** du formulaire de **test de configuration** et le champ **Résultat** du formulaire de **résultat du test** sont calculés selon cet ordre de priorité.

Remarque :

La priorité d'appartenance au groupe s'applique uniquement aux éléments pour lesquels l'élément n'a pas réussi le test de configuration. **Les éléments réussis** sont toujours à l'état **Fermé-Fixe** .

La valeur **Résultat** détermine l'état. Nous ignorons les tâches de rattrapage à l'état **Fermé-Corrigé** et **Fermé-Annulé** . L'état de l'élément est calculé à partir des états de toutes les autres tâches de rattrapage auxquelles il appartient ou il est défini sur **Ouvert**, si aucun autre groupe n'existe pour l'élément.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

Création des tâches de remédiation

Conformité de la configuration Les tâches de rattrapage sont créées manuellement.

Il existe deux façons de créer et de remplir des **tâches de rattrapage**.

- Depuis le module **Tâches de remédiation** et à l'aide de filtres qui remplissent automatiquement l'onglet **Résultats des tests** .

  Cette méthode est utile lorsque vous savez quel filtrage vous souhaitez utiliser. Par exemple, capturer tous les résultats des tests échoués qui sont de criticité modérée et élevée, affectent l'infrastructure Windows et s'appliquent uniquement à l'application de chaîne d'approvisionnement SAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- En sélectionnant les résultats des tests dans la liste **Résultats des tests** et en créant une tâche de rattrapage à partir du menu **Actions sur les lignes sélectionnées...**

  Cette méthode est utile pour les résultats difficiles à filtrer ou pour les situations dans lesquelles vous souhaitez spécifier des résultats de test pour correction. Par exemple, des valeurs aberrantes qui n'ont rien en commun.

Remarque : Si vous créez une tâche de rattrapage à partir de la liste **Résultats des tests** et que vous décidez ultérieurement d'utiliser un filtre pour cette tâche de rattrapage, vos entrées d'origine sont supprimées et remplacées par les résultats du filtre.

Résultats des tests dégroupés

Les résultats des tests non groupés contiennent tous les résultats des tests qui n'ont pas réussi et qui ne sont pas membres d'une tâche de rattrapage active (non **fermée**). Ce module est mis à jour après chaque importation et chaque fois que des résultats de test sont ajoutés ou supprimés d'une tâche de rattrapage.

Éléments détectés pour Conformité de la configuration

Les actifs sont automatiquement mis en correspondance avec des éléments de configuration (CI) à l'aide des règles de recherche de CI, lorsqu'ils sont importés à l'aide des intégrations hôte et résultats des tests. Les éléments détectés vous donnent une visibilité sur la façon dont l'identification des actifs est mappée sur les CI dans le CMDB.

Les éléments détectés sont considérés comme **ayant une correspondance**, **sans correspondance** ou **reclassés**. Les CI identifiés sont dans l'état **Correspondance** .

Pour faciliter la recherche de problèmes de correspondance potentiels, la règle de recherche de CI correspondant au CI apparaît dans le champ Règle de **correspondance de CI** .

Remarque : La prise en charge du champ **de règle de correspondance CI** n'est disponible que pour l'intégrationQualys.

Si aucune correspondance n'est trouvée, un CI est créé dans la classe de *`CI sans correspondance`*[sn_sec_cmn_unmatched_ci],[cmdb_ci_unclassed_hardware] ou [cmdb_ci_incomplete_ip] du CMDB. Si le CI d'origine sans correspondance a été reclassé, les enregistrements d'éléments détectés sont mis à jour pour refléter cet état. Pour plus d'informations, consultez CI sans correspondance et Afficher et reclasser les éléments de configuration sans correspondance pour plus d'informations.

Par défaut, le paramètre **Security Operations** > **CMDB** > **Éléments détectés** Le module répertorie les éléments de configuration sans correspondance Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour obtenir une description des champs dans Éléments détectés, consultez Champs du formulaire Éléments détectés.

Changements de CI pour les éléments détectés pour Conformité de la configuration

La valeur par défaut de la propriété `sn_sec_cmn.update_on_ci_change` est `vrai`. Ainsi, lorsque l'élément de configuration (CI) d'un élément détecté est mis à jour, les résultats des tests sont également mis à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

L'ID externe du résultat du test est mis à jour et le score de risque, les règles d'affectation, les règles de tâche de rattrapage et la règle de cible de rattrapage sont réévalués. Si un résultat de test existe avec le même test et le même CI, les résultats des tests sont mis à jour avec le résultat de test existant et le résultat de test actuel est fermé avec le sous-état invalidCI. Des notes de travail sont ajoutées en conséquence.

Si vous ne souhaitez pas mettre à jour le CI pour le résultat des tests existants, définissez la propriété sur faux. Dans ce cas, si un CI change, un nouveau résultat de test est créé et le résultat existant est fermé comme un CI non valide.

Rapprocher les éléments détectés sans correspondance pour Conformité de la configuration

Créez une tâche planifiée pour rapprocher les éléments détectés sans correspondance. Lorsqu'un résultat de test est créé, l'élément de configuration (CI) qui lui a été ajouté au moment de la création peut être obsolète.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Si les informations dans la CMDB changent, les informations CI sans correspondance ne sont pas rapprochées. Pour effectuer le rapprochement, appliquez des règles de recherche de CI sur les résultats des tests qui sont dans un état sans correspondance lorsque la CMDB est mise à jour avec les derniers CI.

Une tâche planifiée est exécutée sur demande pour réappliquer la règle de correspondance CI aux éléments détectés dans un état sans correspondance. Si le CI change après réapplication des règles de recherche, les éléments détectés sont mis à jour avec le nouveau CI. Les résultats des tests impactés sont également mis à jour. Pour plus de détails, voir Changements de CI pour les éléments détectés pour Conformité de la configuration.

Remarque :

Conformité de la configuration À partir de la version v24, vous pouvez ignorer la réapplication des règles de recherche de CI sur les éléments détectés avec le sous-état « CI désactivé » en activant la propriété *sn_sec_cmn.skipItemsWithCIDecommissioned*système.

Procédure

1. Accédez à la **Tous** > **Security Operations > rapprocher les éléments détectés sans correspondance**.
2. Sur la page Tâches en arrière-plan, cliquez sur **Créer une tâche de rapprochement**.
3. Remplissez les champs du formulaire.

Remarque : Vous ne pouvez modifier que le champ Paramètres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche en arrière-plan

Champ	Description
Numéro	Numéro de tâche unique.
Créé par	Utilisateur qui a créé la tâche.
Paramètres	Paramètres pour rapprocher les éléments détectés sans correspondance : ○ limite : nombre maximal d'éléments détectés à rapprocher. Si vous ne saisissez pas de valeur, 10 000 éléments détectés sont rapprochés. ○ firstDiscovereditem : premier élément détecté qui doit être rapproché. Si vous ne saisissez pas de valeur, le processus de rapprochement commence à partir du premier élément détecté.
État	État actuel de la tâche en arrière-plan.
Description d'état	Description de l'état actuel de la tâche en arrière-plan.
Type de tâche	Type de tâche. La valeur est **Rapprocher les éléments détectés sans correspondance**
Démarré à	Heure de début de la tâche.
Heure de fin	Heure à laquelle la tâche a été terminée.
Durée de la tâche	Temps total nécessaire pour terminer la tâche.
Sous-état	Sous-état de l'état sélectionné.
Notes	Nombre d'enregistrements traités.

4. Cliquez sur **Envoyer**.

Remarque :

- Pour arrêter l'exécution de la tâche, cliquez sur **Annuler**.
- Vous ne pouvez pas rapprocher les CI sans correspondance ou réappliquer des règles de recherche de CI lors de l'importation d'hôtes ou de résultats de tests.

Réappliquer des règles de recherche de CI sur les éléments découverts sélectionnés pour Conformité de la configuration

Réappliquez les règles de recherche d'éléments de configuration (CI) sur les éléments détectés sélectionnés à partir des actions de sélection de la vue de listes des éléments détectés. L'administrateur peut être amené à modifier ou à mettre à jour une règle de recherche pour plusieurs raisons. Si la règle de recherche change, ils peuvent les réappliquer aux éléments détectés.

Avant de commencer

Rôles requis :

Traduction automatique

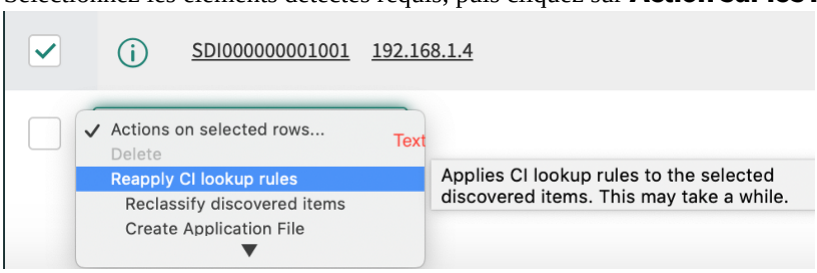
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Si le CI change après la réapplication des règles de recherche de CI, les éléments détectés sont mis à jour avec le nouveau CI et les résultats des tests. Pour plus d'informations, consultez Changements de CI pour les éléments détectés pour Conformité de la configuration.

Procédure

1. Accédez à la **Tous** > **Opérations de sécurité** > **CMDB** > **Éléments détectés**.
2. Sélectionnez les éléments détectés requis, puis cliquez sur **Action sur les lignes sélectionnées**.



3. Sélectionnez **Réappliquer les règles de recherche de CI** dans la liste.

Les règles sont réappliquées à ces éléments détectés.

Remarque :

Conformité de la configuration À partir de la version 15.1.5, vous pouvez ignorer la réapplication des règles de recherche de CI sur les éléments détectés avec le sous-état « CI désactivé » en activant la propriété *sn_sec_cmn.skipItemsWithCIDecommissioned*système .

Le Tenable Vulnerability Integration avec Conformité de la configuration

Le Tenable.io produit des politiques d'importation, des contrôles (résultats des tests) et des tests de Tenable Vulnerability Integration configuration pour le traitement dans l'application Conformité de la configuration .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Tenable.io

Le Tenable Vulnerability Integration est pris en charge.

Vous pouvez utiliser les données importées pour :

- Identifiez les vulnérabilités liées à la configuration sur vos actifs répertoriés dans votre Base de données de gestion des configurations (CMDB)
- Vérifiez que vos actifs sont conformes à vos politiques et contrôles.

Traduction automatique

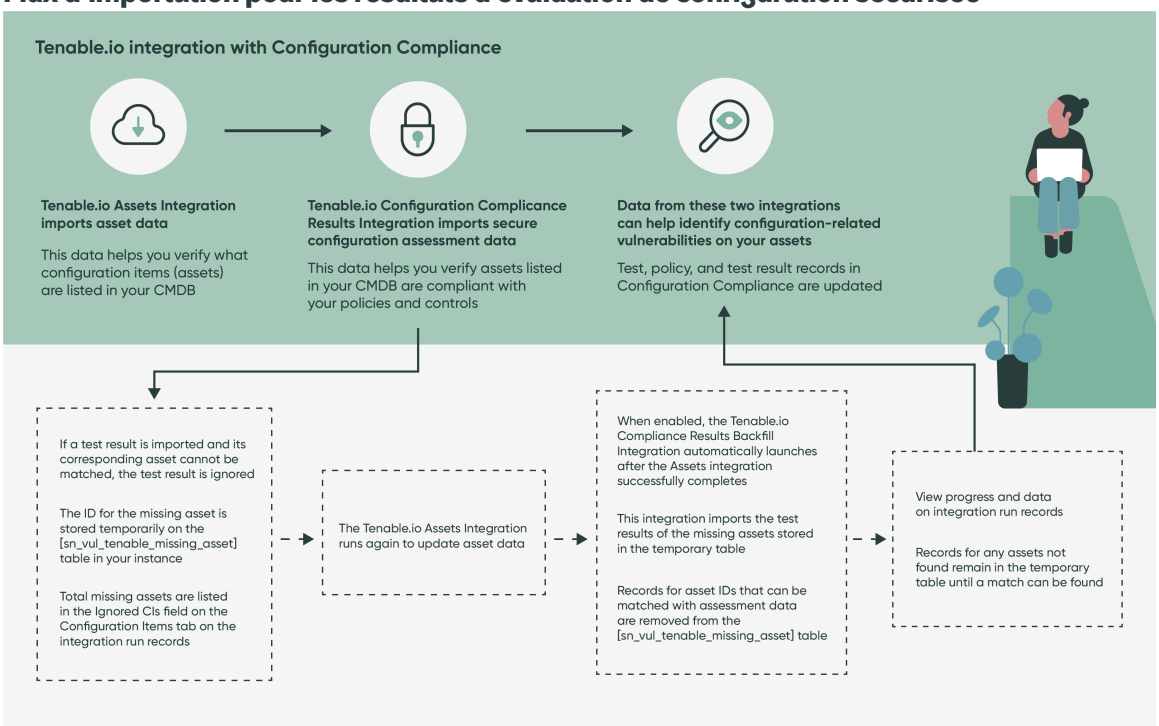
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les données de ressources, les politiques, les contrôles (résultats des tests) et les tests de configuration sont importés avec les intégrations suivantes :

- Tenable.io Intégration des actifs
- Tenable.io Intégration des résultats de la conformité
- Tenable.io Intégration du remplissage des résultats de la conformité

L'image suivante illustre la façon dont les intégrations fonctionnent ensemble pour importer des données d'évaluation des actifs et des configurations et rapprocher les CI ignorés lors d'une importation.

Flux d'importation pour les résultats d'évaluation de configuration sécurisée



Les données sont importées, mises à jour et affichées sur les enregistrements de résultat des tests, de politiques et de tests de configuration dans l'application Conformité de la configuration .

Dans certains cas, le nombre d'éléments de configuration (CI) importés est différent pour l'intégration des actifs et l'intégration Tenable.io des résultats de conformité Tenable.io . Lorsque cela se produit, des enregistrements temporaires sont créés et stockés pour les ID d'actifs ignorés. Ces enregistrements peuvent être mis en correspondance ultérieurement avec les données d'évaluation importées par importation à partir de l'intégration de remplissage des résultats de conformité.

Par exemple, imaginons que l'intégration des actifs importe 80 actifs lors d'une exécution d'intégration, mais que l'intégration des résultats de la conformité en importe 100.

Remarque : Vous pouvez vérifier le nombre de CI ignorés lors des exécutions d'intégration en accédant à **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**. Cliquez sur le nom d'une intégration pour ouvrir l'enregistrement. Sur le lien connexe **Exécutions d'intégration de vulnérabilité** , ouvrez un enregistrement d'exécution d'intégration et sélectionnez l'onglet **Éléments** pour afficher la valeur dans le champ **CI ignorés** . Ce champ suit le total des actifs ignorés (manquants) à partir de l'importation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En comparant les valeurs des champs **CI ignorés** sur chaque enregistrement d'exécution d'intégration, on obtient une différence de 20 CI ignorés. Par conséquent, l'intégration de remplissage s'exécute automatiquement, comme illustré dans l'image précédente. Cette intégration importe les informations d'évaluation de la configuration pour les 20 actifs supplémentaires trouvés par l'intégration des résultats de la conformité, mais manqués par l'intégration des actifs. Étant donné que les données d'évaluation des actifs manquants ne sont pas importées, l'intégration Tenable.io de remplissage des résultats de conformité importe jusqu'à 200 ID d'actifs par exécution d'intégration pour rapprocher les actifs manquants avec leurs données d'évaluation correspondantes. Tous les enregistrements créés pour les actifs manquants ou ignorés et répertoriés dans la table temporaire sont supprimés une fois que ces actifs et leurs données ont été mis en correspondance.

Remarque : L'importation de tous les actifs ignorés peut nécessiter plusieurs exécutions de ces intégrations.

Pour plus d'informations sur l'activation et la configuration de l'intégration Tenable.io des actifs, reportez-vous à la section Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration. Consultez la section Présentation de l'intégration de vulnérabilité Tenable pour en savoir plus sur l'intégration.

L'intégration Tenable.io des résultats de conformité et l'intégration du Tenable.io remplissage des résultats de conformité sont inactives par défaut.

Pour les activer :

1. Accédez à la **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
2. Dans la liste des intégrations Tenable, cliquez sur un nom d'intégration pour ouvrir l'enregistrement et cochez la case **Actif** pour l'activer. Vous préférez peut-être laisser les paramètres de calendrier dans leurs valeurs par défaut pour que ces intégrations démarrent.

Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Conformité de la configuration vulnérabilité tierces

Lorsque les données sont importées à partir d'une intégration tierce, Conformité de la configuration utilise automatiquement les données de l'hôte pour rechercher des correspondances dans le Base de données de gestion des configurations (CMDB). Pour ce faire, il utilise les **règles de recherche de CI**. Ces règles sont utilisées pour identifier les éléments de configuration (CI) et les ajouter à l'enregistrement des résultats des tests pour faciliter le rattrapage.

Au fur et à mesure que les actifs sont importés, une recherche est d'abord effectuée sur la liste **des éléments détectés** à l'aide d'ID tiers afin de trouver des correspondances avec les éléments de configuration (CI) des importations précédentes. Lorsqu'une correspondance d'ID d'hôte est trouvée, elle est utilisée comme champ **d'élément de configuration** dans l'enregistrement des résultats du test.

Vous pouvez voir comment les actifs importés sont mappés aux CI à l'aide de la liste **des éléments détectés** . Si aucune correspondance n'est trouvée ou si le champ cmdb_ci est vide, les règles utilisent les autres informations de l'hôte pour tenter d'identifier correctement le CI. Si aucune correspondance n'est toujours trouvée, un CI d'espace réservé est créé et désigné comme **CI sans correspondance**. Voir CI sans correspondance pour plus d'informations sur la façon dont ces CI sont gérés.

Un nouvel élément détecté est créé et mappé à ce CI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les règles de recherche de CI ne sont disponibles que pour l'intégration Qualys des opérations de sécurité.

Les règles de recherche de CI peuvent être séparées par domaine et sont spécifiques à la source. Chaque source peut avoir plusieurs déploiements. Qualys peut avoir plusieurs déploiements de l'intégration Qualys. Chaque déploiement a son propre ensemble de règles de recherche de CI.

Remarque : Les règles de recherche de CI sont partagées par tous les déploiements de l'intégration de vulnérabilité. Si une règle est supprimée ou modifiée, la suppression ou les changements affectent tous les déploiements de l'intégration de vulnérabilité.

Lors d'une tentative de correspondance, la première étape consiste à rechercher un ID de fournisseur pour trouver une correspondance exacte entre la source, le source_instance et l'ID du fournisseur. Ensuite, les règles de recherche sont exécutées dans l'ordre, de la plus basse à la plus élevée, et s'arrêtent lorsqu'une règle ne renvoie qu'un seul CI comme correspondance. Si une règle est créée de telle sorte qu'elle renvoie plusieurs CI, seule la première correspondance est utilisée.

Remarque : Pour éviter la mise en correspondance sur des éléments de réseau de bas niveau, si un CI correspondant est l'un des `dscy_switchport`, `cmdb_ci_network_adapter`, `cmdb_ci_nic` ou `cmdb_ci_ip_address`, le CI parent est renvoyé.

Une propriété système permettant d'exclure des classes CI est disponible. Cette propriété n'est pas disponible avec la mise à niveau. Pour plus d'informations et d'instructions sur la mise à niveau, reportez-vous Ignorer les classes CI à la section Configurer la propriété.

Pour faciliter la recherche de problèmes correspondants, lorsqu'une correspondance est trouvée, la règle de recherche de CI utilisée pour la trouver est ajoutée à l'enregistrement d'élément détecté dans le champ de **règle de correspondance CI** . Les règles de recherche sont évaluées en fonction **de la valeur d'ordre** la plus faible en premier.

Voici quelques-unes des règles de recherche de Qualys CI fournies avec le système de base :

- ID D'HÔTE QUALYS
- FQDN
- NetBIOS
- DNS
- IP

Voici quelques-unes des règles de recherche de CI Microsoft Defender fournies avec le système de base :

- Catégorie S3
- Nom
- ID de ressource

Voici quelques-unes des règles de recherche de CI dans le cloud Palo Alto Prisma fournies avec le système de base :

- Catégorie S3
- Nom
- ID de ressource

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'importation des données de résultats de test peut être éprouvante pour une instance et des problèmes de performances avec les ressources peuvent survenir si les règles ne sont pas soigneusement construites. La logique utilisée pour itérer et effectuer la correspondance dans peut entraîner de longs délais de CMDB traitement. Pour éviter toute dégradation potentielle des ressources ou toute complication des performances, testez toutes les règles de recherche de CI écrites sur mesure ou les modifications apportées aux **règles de recherche de CI prédéfinies**. Consultez Étapes pour empêcher les enregistrements dupliqués ou orphelins après l'exécution Réponse aux vulnérabilités de règles de recherche de CI pour plus d'informations sur la prévention des enregistrements orphelins en double, la suppression des données et le nettoyage des données.

Réapplication des règles de recherche de CI mises à jour

Lorsque vous modifiez une règle de recherche de CI, cliquez sur **Appliquer les modifications** sur la page de liste Règles de recherche de CI pour réexécuter toutes les règles sur les éléments détectés qui :

- Ont été mis à jour et correspondent aux règles
- Ne correspondent à aucune règle

Si l'élément de configuration (CI) change après la réapplication des règles de recherche, les éléments détectés sont mis à jour avec le nouveau CI. Les résultats des tests sont également mis à jour. Pour plus d'informations, consultez Changements de CI pour les éléments détectés pour Conformité de la configuration.

Déduplication d'éléments de configuration existants pour Conformité de la configuration

Le correcteur de CI en double pour les tâches de déduplication est mis à jour avec la propriété `sn_sec_cmn_src_ci.cmdb_ci` .

Chaque fois qu'une tâche de déduplication est utilisée pour mettre à jour les éléments de configuration (CI), elle met également à jour les éléments détectés associés à ces CI. Par conséquent, les résultats des tests sont mis à jour avec le CI. Pour plus de détails, voir Changements de CI pour les éléments détectés pour Conformité de la configuration.

Création de CI pour Conformité de la configuration l'utilisation du moteur Identification et réconciliation

Conformité de la configuration À partir de la version 11.1, vous pouvez créer des éléments de configuration (CI) dans le Base de données de gestion des configurations (CMDB) à l'aide de l'API du moteur Identification et réconciliation (IRE). En utilisant l'API IRE pour créer des CI, vous pouvez empêcher la création de CI en double et vous pouvez rapprocher les attributs de CI en autorisant uniquement les sources de données de référence à écrire CMDB.

Une classe CI (table) est le nom de table d'origine dans la base de données d'instance. CMDB contient des classes système de base qui stockent des données sur les CI.

Utilisation d'IRE pour la création de CI

Avant la version 11.1, si un CI correspondant n'était pas trouvé dans la liste des éléments détectés ou CMDB, un CI était créé dans la classe de CI sans correspondance (`sn_sec_cmn_unmatched_ci`).

Pour plus d'informations, voir CI sans correspondance.

À partir de la version 11.1, vous pouvez utiliser l'API IRE pour créer des CI dans CMDB. Au lieu d'utiliser la classe CI sans correspondance, un CI est créé dans la classe Matériel non classé ou Appareil identifié IP incomplet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

CMDB Classes CI

Remarque : Pour utiliser les nouvelles classes, activez le module d'extension Modèles de CMDB classe CI. Dans le cas contraire, les CI sont créés dans la classe de CI sans correspondance.

À partir de la version 11.1, si l'hôte que vous avez importé à partir d'un scanner tiers est introuvable dans la liste des éléments détectés ou CMDB, il est stocké dans l'une des nouvelles CMDB classes de CI suivantes.

CMDB Classes CI

CMDB Classe CI	Description
Adresse IP incomplète de l'appareil identifié (cmdb_ci_incomplete_ip)	Le CI est créé dans cette table si seule l'adresse IP est disponible dans les informations hôte reçues du scanner.
Matériel non classé (cmdb_unclassed_hardware_ci)	Le CI est créé dans cette table si l'une des informations suivantes est disponible dans les informations hôtes reçues du scanner : • Nom d'hôte • Adresse IP • DNS • NETBIOS • Adresse MAC **Remarque :** Si l'adresse MAC est disponible, l'entrée de carte réseau est créée et associée au CI matériel non classé. Si les adresses IP et MAC sont disponibles, le CI d'adresse IP est également créé et associé au CI matériel non classé.

Le système utilise automatiquement une classe CI sans correspondance si l'une des situations suivantes se produit :

- Le module d'extension CMDB Classe CI n'est pas activé.
- IRE déclenche une exception lors de la création d'un nouveau CI.

Information associée

Application de stockage CMDB CI Class Models

Moteur Identification et réconciliation (IRE)

Conformité de la configuration Vue d'ensemble des règles d'affectation

Définissez les critères selon lesquels les résultats des tests sont automatiquement affectés à un groupe d'affectation à des fins de correction.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Une règle d'affectation par défaut, **Affecter au groupe de support CI**, est incluse dans l'affectation des résultats des tests du système de base au **groupe de support CI**. Inactif par défaut.

Les groupes d'affectation définis par les règles d'affectation sont utilisés par les **règles de tâche de rattrapage** pour affecter des propriétaires à des tâches de rattrapage (RT).

Affectation automatique des résultats des tests

Il existe trois façons différentes d'affecter des résultats de test à l'aide **de l'option Affecter à l'aide de** :

- Groupe d'affectation : cette option vous permet de sélectionner n'importe quel groupe d'utilisateurs existant ServiceNow AI Platform® .
- Champ de groupe d'affectation : cette option vous permet de choisir n'importe quel champ de groupe d'affectation disponible à l'aide de la table cmdb_ci. Par défaut, les trois champs de groupe suivants s'affichent :
  - Aucune : n'indique aucune valeur par défaut pour ce champ obligatoire
  - Élément de configuration : groupe d'approbation
  - Élément de configuration : groupe d'affectation
  - Élément de configuration : groupe de support
- Script : cette option vous permet de définir les conditions à l'aide d'un script. Cette option nécessite un codage ou une expertise avancée ServiceNow® .

Voir Créer ou modifier Conformité de la configuration des règles d'affectation pour plus d'informations sur la création de règles d'affectation.

Le rôle sn_vulc.remediation_owner vous permet d'afficher et de mettre à jour les résultats des tests et les tâches de rattrapage qui leur sont affectées ou qui sont affectées à leurs groupes d'affectation. Pour afficher les modules, accédez à **Tous** > **Configuration Compliance** > **Résultats des tests** > **Mes résultats des tests ouverts**ou **Configuration Compliance** > **Tâches de remédiation** > **Mes tâches ouvertes**.

Le rôle sn_vulc.remediation_owner peut être affecté directement à un utilisateur ou, automatiquement, lorsque vous affectez le rôle itil à un utilisateur.

Processus d'évaluation des règles d'affectation

Lorsqu'un nouveau résultat de test est importé ou rouvert après avoir été fermé, les règles d'affectation sont évaluées en fonction de celui-ci. Les règles d'affectation sont évaluées après la correspondance des CI et les calculs du score de risque. Un résultat de test n'est automatiquement évalué que lors de l'importation initiale et lorsqu'une règle est modifiée,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sauf s'il est rouvert après avoir été fermé. Vous pouvez réappliquer manuellement des règles après des changements.

Le processus suivant est utilisé pour chaque résultat de test nouveau ou rouvert :

- Pour chaque règle d'affectation de résultat de test, le résultat du test est comparé au filtre d'affectation, en commençant par la règle d'ordre le plus bas.
- Lorsque la condition est remplie, le résultat du test est affecté à un groupe d'affectation. La recherche s'arrête.
- Si toutes les règles ne correspondent pas aux conditions, le résultat du test n'est pas affecté.

Réapplication des règles d'affectation

Lorsque vous modifiez une règle d'affectation, utilisez le bouton **Appliquer les modifications** sur la page de liste Règles d'affectation pour réexécuter toutes les règles modifiées sur tous les résultats des tests ouverts actifs, à l'exception de ceux qui ont été affectés manuellement.

Remarque : Les règles d'affectation ne réévaluent pas les affectations créées manuellement.

La tâche planifiée [*Reapply all assignment rules*] est inactive, par défaut. Lorsqu'elle est activée, elle évalue tous les résultats des tests ouverts par rapport à toutes les règles actives, à l'exception de celles affectées manuellement. Il peut s'exécuter quotidiennement, hebdomadairement, mensuellement, périodiquement, une fois ou sur demande.

Important : En tant qu'administrateur et analyste, vous pouvez obtenir les dernières affectations pour les résultats des tests sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités. Cette méthode est plus efficace que la réapplication des règles d'affectation pour tous les résultats des tests dans l'interface classique utilisateur, ce qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Règles d'affectation et affectation de tâche de rattrapage

En règle générale, vous affecterez votre tâche de rattrapage (RT) au même groupe d'affectation que les résultats du test dans celui-ci. C'est ce que font les règles de tâche de rattrapage, par défaut.

Par exemple, si votre RT effectue un regroupement par classe d'élément de configuration, la tâche de rattrapage créée peut être divisée en différents groupes d'affectation. Un TRG de base de données Oracle peut être affecté au groupe 1 et un TRG de base de données Oracle au groupe 2.

Lorsque le groupe d'affectation est modifié au niveau de la tâche de rattrapage, tous les résultats des tests de cette tâche de rattrapage qui ont le même groupe d'affectation sont mis à jour vers le nouveau groupe d'affectation. Les résultats des tests sont marqués comme affectés manuellement et ne sont pas éligibles à une évaluation plus approfondie des règles.

Suppression des affectations des tâches de Conformité de la configuration rattrapage

Vous pouvez effacer les champs **Affecté à** et **Groupe d'affectation** sur les tâches de rattrapage et leurs résultats de test associés directement à partir des enregistrements de résultats des tests et des tâches de rattrapage qui, selon vous, pourraient être incorrectement affectés à vous ou à vos groupes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble du workflow

Les propriétaires de rattrapage peuvent mettre à jour les enregistrements pour la réaffectation à l'aide du bouton **Annuler l'affectation** .

Cas d'utilisation de sn_vulc.remediation_owner

Si vous déterminez que les RT et leurs résultats de test associés ne sont pas dans votre champ d'application pour le rattrapage, ou si vous pensez que des enregistrements vous ont été affectés de manière incorrecte ou ont été affectés à vos groupes, vous pouvez vous supprimer ou supprimer vos groupes des champs **Affecté à** et **Groupe d'affectation** de ces enregistrements de tâche de rattrapage.

Annuler l'affectation du module

Le bouton **Annuler l'affectation** s'affiche sur la tâche de rattrapage et les enregistrements de résultats des tests dans tout état autre que l'état Fermé ou Résolu.

Si vous sélectionnez **Annuler l'affectation**, vous êtes invité à réaffecter tous les résultats des tests associés à la tâche de rattrapage et à passer au type d'affectation **Non affecté** .

Remarque : Si un résultat de test d'une tâche de rattrapage a un groupe d'affectation différent de celui de sa tâche de rattrapage, il n'est pas désaffecté. Dans la plupart des cas, ces résultats de test ont été affectés manuellement.

Tous les enregistrements que vous mettez à jour avec le bouton d'interface utilisateur ou manuellement sont affichés dans le module Non affecté sous Conformité de la configuration.

Pour connaître les étapes de réaffectation des enregistrements à l'aide de l'action d'interface utilisateur, reportez-vous à la *Unassigned* section Supprimer les affectations des tâches de rattrapage pour vous ou vos groupes.

Propriété système et notifications

Si vous êtes administrateur avec le rôle sn_vulc.vulnerability_admin, lorsque vous sélectionnez **Annuler l'affectation** sur un enregistrement, par défaut, la propriété `sn_vulc.unassign_test_result_group.approval_required` système déclenche l'enregistrement Approbation du changement d'état et l'enregistrement Approbation demandée. En outre, la demande s'affiche dans la liste Mes approbations de l'approbateur.

Remarque : En tant qu'administrateur de vulnérabilités, vous pouvez définir la `sn_vulc.unassign_test_result_group.approval_required` propriété système sur **false** pour désactiver le processus d'approbation.

- Si l'approbateur approuve votre demande, par défaut, la propriété système, `sn_vulc.default_assignment_group` efface les champs Affecté à et Groupe d'affectation, et remplit le champ Type d'affectation avec **Non affecté**. En tant qu'administrateur de vulnérabilités, vous pouvez modifier la valeur de la `sn_vulc.default_assignment_group` propriété système afin que les champs d'affectation soient effacés et qu'un groupe spécifique soit ensuite affecté. Par exemple, si un utilisateur sélectionne **Annuler l'affectation** d'un enregistrement et que vous souhaitez le rediriger vers un groupe spécifique pour révision, vous pouvez ajouter un ID système pour le groupe de votre choix dans le champ de valeur de la propriété système.
- Si l'approbateur rejette votre demande, le motif du rejet s'affiche dans l'onglet **Notes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sinon, si n'est *sn_vulc.default_assignment_group* pas configuré pour un groupe spécifique, par défaut, les utilisateurs que vous ajoutez au groupe d'utilisateurs de notification Désaffecter sont alertés lorsque des enregistrements sont désaffectés. La propriété *sn_vulc.default_notification_group* système détermine les notifications à ce groupe.

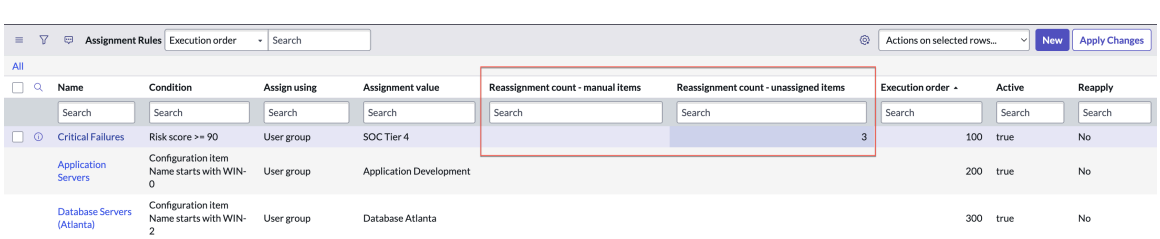
Le type d'affectation, qu'il soit **manuel**, **règle** ou **non affecté**, est disponible dans les enregistrements RT et la vue de liste. Le type d'affectation **non affecté** s'affiche une fois que les champs **Affecté à** et **Groupe d'affectation** sont effacés par la propriété système de la fonctionnalité.

Surveillance de vos règles d'affectation avec la tâche planifiée pour cette fonctionnalité

Une tâche planifiée quotidienne compte les enregistrements lorsqu'ils passent au type d'affectation **Non affecté** . Avec ce nombre, les analystes de vulnérabilité peuvent surveiller et ajuster toutes les règles d'affectation susceptibles de ne pas fonctionner correctement en fonction des règles d'affectation qui ont un nombre plus élevé de RT non affectés.

La *Reassignment count for assignment rules* tâche planifiée s'exécute quotidiennement et publie le nombre total de tâches de rattrapage qui ne sont pas affectées par cette fonctionnalité pour une règle d'affectation particulière.

La tâche compte également tous les enregistrements qui ne sont pas affectés manuellement. Les décomptes manuels et les décomptes collectés par cette fonctionnalité sont publiés dans la liste Règles d'affectation de vulnérabilité dans deux colonnes : *Reassignment count - manual items* et *Reassignment count - unassigned items*.



1. En tant qu'administrateur de vulnérabilités, vous pouvez consulter ces nombres en accédant à **Configuration Compliance** > **Administration** > **Règles d'affectation**.
2. Sélectionnez l'icône d'engrenage dans le coin supérieur droit de la liste et sélectionnez les éléments **Nombre de réaffectations (éléments manuels**) et **Nombre de réaffectations (éléments non affectés**) pour l'afficher.
3. Tout RT qui a été affecté à l'origine par une règle, mais qui a ensuite été automatiquement ou manuellement réaffecté, contient une référence à la règle d'origine dans la vue de liste.

Conformité de la configuration Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage

Créez automatiquement des tâches de rattrapage pour analyser les résultats en bloc à l'aide des règles de tâche de rattrapage. Les critères selon lesquels les tâches sont formées sont configurés de manière à ce que vous n'ayez pas à affecter manuellement les résultats des tests aux tâches de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Comprendre les tâches de rattrapage

Les tâches de rattrapage représentent un ensemble de résultats des tests à corriger. Le regroupement des résultats des tests présente de nombreux avantages. Vous pouvez déplacer les résultats des tests d'un état de rattrapage à un autre, les marquer comme étant en cours d'examen, les différer, les marquer comme résolus en bloc à l'aide de groupes. Vous pouvez créer des conditions pour regrouper automatiquement tous les résultats avec des résultats, des technologies, des scores de risque et toutes les autres données spécifiques associés aux résultats des tests. Les résultats des tests peuvent appartenir à plusieurs tâches de rattrapage, ce qui vous donne la possibilité de travailler activement avec une tâche de rattrapage et d'en surveiller une autre. Tout dépend des besoins de votre organisation. Par exemple, vous pouvez regrouper par affectation et créer un groupe contenant des technologies.

Les tâches de rattrapage sont créées comme suit.

- Manuellement, à l'aide de l'une des deux options, pour ajouter des résultats de test au groupe.
  - **Manuel** : crée une tâche de rattrapage sans entrée. Les résultats des tests doivent être ajoutés manuellement.
  - **Filtre** : crée une tâche de rattrapage et utilise des conditions pour ajouter automatiquement des résultats de test à cette tâche de rattrapage.

    Remarque : Les résultats des tests ajoutés manuellement ne sont pas automatiquement supprimés des tâches de rattrapage par les règles ou les conditions de tâche de rattrapage.

- Automatiquement, en utilisant les règles de la tâche de rattrapage. Cette option est l'option la plus simple. Une fois configurées, les règles de tâche de rattrapage créent toutes les tâches de rattrapage souhaitées.

À partir d'une tâche de rattrapage, le groupe de résultats des tests peut être affecté à un utilisateur, différé à plus tard, utilisé pour créer une **demande de changement**, etc.

Remarque :

Le rôle sn_vulc.remediation_owner vous permet d'afficher et de mettre à jour les résultats des tests et les tâches de rattrapage qui vous sont affectées ou à vos groupes d'affectation. Pour afficher les modules, accédez à **Tous** > **Configuration Compliance** > **Résultats des tests** > **Mes résultats des tests ouverts**ou **Configuration Compliance** > **Tâches de remédiation** > **Mes tâches ouvertes**.

Lorsqu'il est déterminé qu'un nouveau résultat de test peut être ajouté à une tâche de rattrapage, le résultat du test est inclus dans la liste connexe Résultats des **tests** de la tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lors de la mise à jour de l'état d'une tâche de rattrapage, les résultats des tests associés peuvent voir leur état mis à jour pour correspondre à cette tâche de rattrapage. Pour plus d'informations sur les changements d'état, reportez-vous à la section Conformité de la configuration États.

Comprendre les règles de tâche de rattrapage

Les règles de tâche de rattrapage vous permettent de définir comment les résultats des tests sont automatiquement regroupés et affectés. Une règle par défaut, **Groupe d'affectation, Test**, est incluse dans le système de base regroupant les résultats des tests en fonction d'un **groupe d'affectation** de résultats de test et du champ **Test** . Cette règle est désactivée par défaut. Vous pouvez effectuer un regroupement par tout autre ensemble de valeurs dans des colonnes accessibles à partir du résultat du test. Vous pouvez utiliser jusqu'à six touches et n'importe quel nombre de conditions. Pour plus d'informations, consultez Créer ou modifier des Conformité de la configuration règles de tâche de rattrapage.

Important : En tant qu'administrateur et analyste, vous pouvez évaluer les règles de tâche de rattrapage pour les résultats de tests sélectionnés dans l'espace de travail du gestionnaire de vulnérabilités. Cette méthode est plus efficace que la réapplication des règles de tâche de rattrapage dans l'interface utilisateur classique, qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Par exemple, vous pouvez regrouper vos résultats de tests par groupe d'affectation ou par technologie et élément de configuration (CI). Un autre ensemble de règles peut être utilisé pour les résultats des tests qui exposent l'entreprise à plus de risques. Vous pouvez avoir une règle de tâche de rattrapage pour les CI de faible gravité ou de faible risque. Consultez la rubrique Afficher les Conformité de la configuration résultats des tests pour plus d'informations sur les champs disponibles.

Lorsqu'un nouveau résultat de test est importé ou rouvert après avoir été fermé, les règles de la tâche de rattrapage sont évaluées en fonction de celui-ci. Un résultat de test n'est évalué qu'une seule fois, sauf s'il est rouvert après avoir été fermé.

Les règles de tâche de rattrapage sont évaluées après la correspondance des CI, le calcul du score de risque et les règles d'affectation.

Le processus suivant est utilisé pour chaque résultat de test nouveau ou rouvert :

- Pour chaque règle de tâche de rattrapage, le résultat du test est comparé au filtre de condition.
- Pour chaque règle dans laquelle la condition de règle correspond, elle extrait les données des colonnes de clé de groupe sur le résultat du test. La règle vérifie s'il existe une tâche de rattrapage **ouverte** correspondante affectée au même groupe d'affectation que le résultat du test.

  Si la tâche de rattrapage est trouvée, le résultat du test est ajouté à la tâche de rattrapage existante à l'état **Ouvert** .

- Si aucune tâche de rattrapage à l'état **Ouvert** n'est trouvée, la règle crée une tâche de rattrapage, l'affecte en fonction du **groupe d'utilisateurs** ou de la valeur **de clé** dans la règle, puis y place le résultat du test.

Plusieurs règles de résultat de test peuvent être définies, pour regrouper différents types de résultats. Étant donné que chaque résultat est comparé aux conditions de la règle avant de le placer dans une tâche de rattrapage, trop de règles peuvent avoir un impact sur les performances.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsqu'une règle de tâche de rattrapage est supprimée, vous avez la possibilité de supprimer toutes les tâches ouvertes créées par la règle. Cela s'applique à la fois à la vue de formulaire de règle et à la vue de liste.

Lorsqu'une affectation de tâche de rattrapage est effectuée ou modifiée, les champs **Groupe d'affectation** et **Affecté à** se déploient à tous les résultats des tests, à l'exception de ceux dont le résultat du test a un groupe d'affectation différent de celui du RT. Pour plus d'informations sur les règles d'affectation, reportez-vous à Conformité de la configuration Vue d'ensemble des règles d'affectation. Ces affectations sont utilisées automatiquement pour ce groupe lors de la prochaine importation.

Suivre le nombre de reports pour les résultats des tests et les tâches de rattrapage

À partir de la version 14.3, suivez le nombre de fois où un résultat de test ou une tâche de rattrapage est différé dans le module Reports multiples. Un travail planifié, **défini Nombres de reports**, s'exécute quotidiennement pour valider les décomptes des enregistrements différés plusieurs fois dans la colonne Nombre de reports des enregistrements répertoriés dans le module Reports multiples.

Configurer des groupes de calculateurs et des calculateurs pour Conformité de la configuration

Les calculateurs de Configuration Compliance sont utilisés pour mettre à jour les valeurs d'enregistrement lorsque des conditions prédéfinies sont remplies. Les calculateurs sont regroupés en fonction des critères utilisés pour déterminer le mode de mise à jour des enregistrements.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Calculateurs de Configuration Compliance

L'application Configuration Compliance comprend deux types de calculateurs, les calculateurs de risque et les calculateurs de déploiement des scores de risque. Ces groupes de calculateurs sont activés par défaut.

Le groupe de calculateurs de score de risque a été renommé Calculateurs de risque.

Les calculateurs de déploiement des scores de risque comprennent des calculateurs de déploiement pour les tests de configuration et les tâches de rattrapage.

La configuration des calculateurs de risque et de déploiement pour le rattrapage des résultats des tests et des tâches de rattrapage comprend les tâches suivantes :

- Créer un calculateur de risque
- Créer un calculateur de déploiement de score de risque

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois le calculateur de risque créé, il est disponible pour les calculs lors de la prochaine ingestion de données. Après l'avoir créé, vous pouvez également l'appliquer à la demande.

Pour plus d'informations sur les calculateurs et les groupes de calculateurs, reportez-vous à la section Conformité de la configuration Groupes de calculateurs.

Conformité de la configuration Vue d'ensemble de la gestion des exceptions

Lorsque votre organisation n'est pas en mesure de se conformer à une politique, une norme ou une directive publiée en matière de gestion des vulnérabilités ou de sécurité, vous pouvez demander une exception. La gestion des exceptions implique la demande, l'examen, l'approbation ou le rejet d'exceptions pour une tâche de rattrapage qui ne peut pas être corrigée conformément à la politique.

Important : La gestion des exceptions est prise en charge dans l'espace de travail du gestionnaire de vulnérabilités et l'espace de travail de la correction informatique.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Certaines vulnérabilités peuvent ne pas avoir de correctif, de correctif ou de solution existant. Lorsqu'une exception est approuvée, cela signifie également que vous acceptez un risque, car vous reconnaissez et acceptez les conséquences de ne pas corriger la vulnérabilité liée à la configuration.

Cycle de vie d'une exception

Une exception est une demande de différer le rattrapage d'une tâche de rattrapage pour une période spécifiée.

Le cycle de vie d'une exception est le suivant :

- Demande d'exception
- Approbation d'une demande d'exception
- Suivi d'une demande d'exception
- Expiration d'une demande d'exception

Demande d'exception

En tant que propriétaire du rattrapage, vous pouvez demander une exemption pour une tâche de rattrapage à l'aide du processus de gestion des exceptions. Pendant le processus d'approbation, la tâche de rattrapage reste à l'état **En cours de révision** . Une fois que l'approbateur d'exception a approuvé cette demande, la tâche de rattrapage passe à un état **Différé** .

Important : Vous pouvez demander une exception à l'espace de travail de remédiation informatique. Pour plus d'informations, consultez Demander une exception dans le Espace de travail de remédiation IT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Approbation d'une demande d'exception

Les tâches de rattrapage qui ne peuvent pas être corrigées immédiatement sont examinées, évaluées pour le risque et approuvées pour report jusqu'à ce qu'elles puissent être corrigées. L'approbation d'une demande d'exception peut être un workflow à deux niveaux. Si seul l'approbateur de premier niveau est présent, l'exception peut être demandée et approuvée. Toutefois, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Consultez Ajouter un approbateur d'exception pour Conformité de la configuration pour plus d'informations.

Important : Vous pouvez approuver ou rejeter une demande d'exception à partir de Vulnerability Manager Workspace. Pour plus d'informations, consultez Demander des exceptions pour les tâches et les enregistrements de rattrapage dans Espace de travail du gestionnaire de vulnérabilités.

Remarque :

À partir de la Conformité de la configuration version 13.0, si vous déployez l'application CC pour la première fois, le concepteur de flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow.

Une fois qu'une demande d'exception pour une tâche de rattrapage est approuvée, vous pouvez effectuer les actions suivantes :

- Rouvrir
- Supprimer

Remarque : Les commentaires de rejet sont affichés dans les notes de travail d'une tâche de rattrapage. Si une demande d'exception est rejetée, cette tâche de rattrapage revient à son état précédent.

Suivi d'une demande d'exception

Après avoir levé l'exception, vous pouvez suivre son état à l'aide de l'onglet **Approbations de changement d'état** de la tâche de rattrapage. Si une action est effectuée sur une tâche de rattrapage, vous ne pouvez pas suivre l'état des résultats des tests individuels dans cette tâche de rattrapage.

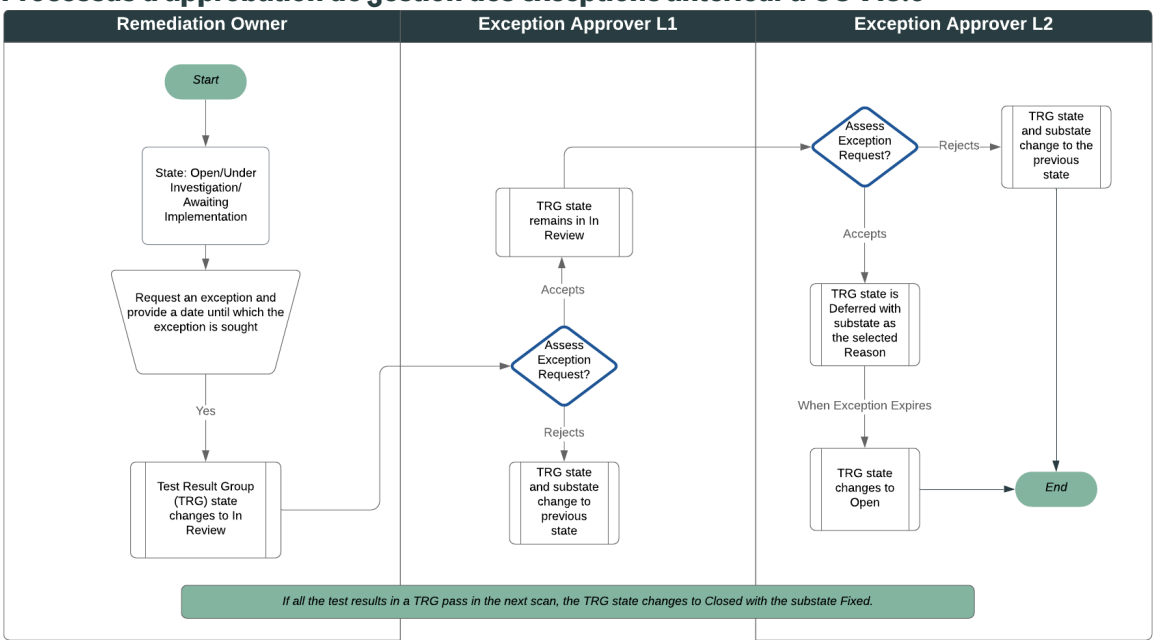
Expiration d'une demande d'exception

Lorsqu'une demande d'exception pour une tâche de rattrapage expire, la tâche de rattrapage revient à son état **Ouvert** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Processus d'approbation de gestion des exceptions antérieur à CC v13.0



Conformité de la configuration gestion des changements

En tant que propriétaire d'un rattrapage informatique, vous pouvez créer et gérer des demandes de changement (CHG) directement à partir des tâches de rattrapage (RT) dans l'application Conformité de la configuration .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Les demandes de changement et le Conformité de la configuration workflow

Les demandes de changement et la gestion des changements font partie du processus de rattrapage Conformité de la configuration du workflow. Au cours de cette phase de rattrapage, vous pouvez utiliser les demandes de changement pour vous aider à classer par ordre de priorité, à suivre et à corriger les résultats des tests.

L'application Conformité de la configuration fonctionne avec le processus de gestion des changements informatiques pour vous aider à corriger les ServiceNow AI Platform® logiciels et technologies non conformes dans votre environnement.

Avec Gestion des changements dans l'application Conformité de la configuration , vous pouvez associer des résultats de tests à des demandes de changement existantes, ou diviser une tâche de rattrapage et créer une nouvelle tâche de rattrapage uniquement pour les résultats des tests sélectionnés.

Pour plus d'informations, consultez Créer une demande de changement dans Conformité de la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Termes clés

Tests

Les tests sont des bibliothèques d'enregistrements de données qui organisent les analyses des ressources informatiques. Les tests de configuration définissent la manière dont une classe d'actifs technologiques doit être gouvernée. Un test est tout ce qui peut être utilisé pour identifier une classe de logiciels ou un actif matériel qui n'est pas conforme.

Résultats des tests

Les résultats des tests sont importés par des intégrations tierces. Une fois visibles dans , ils sont corrigés à Conformité de la configuration l'aide de **tâches de rattrapage**. Les groupes sont affectés au rattrapage en fonction des règles d'affectation.

Remarque : À partir de la version 14.9 de , le résultat du Conformité de la configuration test est *étiqueté Résultat*.

Tâche de rattrapage

Les résultats des tests sont regroupés en tâches de rattrapage en fonction des règles d'affectation et affectés automatiquement aux propriétaires de rattrapage pour le rattrapage.

Remarque : À partir de la version 14.9 de , le résultat du test est étiqueté Tâche de Conformité de la configuration*rattrapage*.

Groupes de test

Les groupes de tests sont liés à des documents et des enregistrements de tests faisant autorité. Un groupe de tests de configuration définit les groupes de tests.

Demandes de changement

Les demandes de changement vous aident à implémenter des processus contrôlés pour le rattrapage. Vous pouvez utiliser des demandes de changement avec des tâches Conformité de la configuration de rattrapage pour vous aider à identifier, suivre et résoudre les actifs non conformes (éléments de configuration) qui nécessitent des ressources supplémentaires ou que vous pouvez cibler pour un report.

Pour plus d'informations sur les résultats des tests et les tâches de rattrapage, reportez-vous à la section Conformité de la configuration Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage.

Quand utiliser les demandes de changement dans Conformité de la configuration

Les demandes de changement vous aident à lancer et à suivre des activités de rattrapage sur vos résultats de test. Lorsque les propriétaires de rattrapage disposent d'un grand nombre de résultats des tests ou d'éléments de configuration non corrigés, ils peuvent utiliser des demandes de changement pour identifier les résultats des tests à différer. Ils peuvent également identifier et regrouper les résultats des tests et les éléments de configuration qui nécessitent plus de ressources que celles initialement identifiées dans la tâche de rattrapage initiale.

Créer des demandes de changement à partir d'une tâche de rattrapage

Créez une demande de changement directement à partir d'une tâche de rattrapage pour tous les résultats des tests de la tâche de rattrapage, ou utilisez le filtrage pour identifier uniquement les résultats des tests qui correspondent à des critères spécifiques. Créez une demande de changement avec des informations pré-remplies pour accélérer votre enquête sur les résultats des tests qui nécessitent une intervention manuelle.

Fractionner une tâche de rattrapage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir d'une tâche de rattrapage existante, identifiez un sous-ensemble de résultats des tests que vous souhaitez déplacer vers une nouvelle tâche de rattrapage. En créant un nouveau TRG, vous pouvez utiliser un groupe spécifique de résultats des tests sans impact sur la tâche de rattrapage d'origine.

Associer les résultats des tests à une demande de changement existante

Associez les résultats des tests aux tâches existantes pour éviter de créer des demandes de changement en double lorsque vous travaillez à la résolution de vos tâches de rattrapage. En associant une tâche de rattrapage à une demande de changement déjà disponible dans votre instance, vous pouvez utiliser des listes de tâches existantes.

Types de demandes de changement pour une tâche de rattrapage

Vous pouvez créer, approuver, implémenter, examiner et fermer des demandes de changement directement à partir des tâches de rattrapage qui vous sont affectées. Vous pouvez créer trois types de demandes de changement avec des informations pré-remplies à partir d'une tâche de rattrapage :

- Standard. Un changement pré-autorisé à risque faible, relativement commun et qui suit une procédure ou une instruction de travail spécifique.
- Normal. Les demandes de changement normal suivent un processus prescriptif qui requiert deux niveaux d'approbation avant leur implémentation, revue et fermeture.
- Urgence. Un changement pour résoudre un incident majeur.

Installation, installation et configuration de l'application Conformité de la configuration

Avant d'exécuter l'application dans votre ServiceNow AI Platform® instance, vous devez d'abord télécharger et installer l'application Conformité de la configuration à partir du ServiceNow® Store. Cette application est disponible sous forme d'abonnement distinct.

Effectuez les étapes de liste de vérification de configuration suivantes répertoriées dans le tableau suivant avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Pour plus d'informations sur les versions publiées de l'application Conformité de la configuration , ainsi que sur les applications tierces et ServiceNow compatibles avec celle-ci, consultez l'article Matrice de compatibilité de la réponse aux vulnérabilités et changements de schéma de mise en production [KB0856498] dans la base de connaissances HI.

Pour en savoir plus sur l'obtention d'autorisations pour les applications de l'App Store, reportez-vous à la section Opérations de sécurité et le ServiceNow Store.

Configurer les tâches de liste de vérification

Tâches de configuration	Description
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • Si elle n'est pas déjà affectée, l'administrateur système [admin] installe l'application et lui attribue le rôle d'administrateur de Configuration Compliance [sn_vulc.admin].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les tâches de liste de vérification (suite)

Tâches de configuration	Description
	• L'administrateur de Configuration Compliance [sn_vulc.admin] supervise la configuration et vérifie les résultats attendus. • Le propriétaire du rattrapage [sn_vulc.remediation_owner] lit et met à jour les enregistrements affectés. Le rôle sn_vulc.remediation_owner est également affecté automatiquement lorsqu'un utilisateur est affecté au rôle itil.
Intégrations prises en charge	Avant de pouvoir Conformité de la configuration corriger des éléments de configuration, vous devez installer une intégration d'analyse tierce et effectuer au moins une analyse réseau. Vérifiez que l'application est installée et activée avant de configurer les Réponse aux vulnérabilités intégrations tierces prises en charge. Consultez Installer Réponse aux vulnérabilités. Pour vérifier que les applications d'intégration sont installées et activées, accédez à **Gestion des abonnements** > **Abonnements** dans votre instance. La liste affiche les abonnements que votre organisation a achetés. Pour plus d'informations sur les intégrations tierces et une liste des produits pris en charge, reportez-vous à la section Intégrations de Conformité de la configuration.

Qualys Vulnerability Integration

- Si le est déjà installé sur votre système et que vos informations d'identification d'API Qualys Vulnerability Integration sont différentes de celles que vous souhaitez utiliser pour Conformité de la configuration, accédez à l'Assistant de configuration (dans Réponse aux vulnérabilités) et affectez-les à chaque intégration de **PC Qualys** .
- Accédez à la **Intégration de vulnérabilité Qualys** > **Intégrations principales** et modifiez le champ **Informations d'identification de l'API Qualys** sous l'onglet **Détails REST Qualys** .

Pour en savoir plus sur le , reportez-vous à la Qualys Vulnerability Integration section Présentation de Qualys Vulnerability Integration.

Vous êtes maintenant prêt à installer l'application Conformité de la configuration . Consultez Installer Conformité de la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer Conformité de la configuration

Avant d'exécuter Conformité de la configuration dans votre ServiceNow AI Platform® instance, vous devez d'abord télécharger et installer l'application Conformité de la configuration à partir du ServiceNow Store. Cette application est disponible sous forme d'abonnement distinct.

Avant de commencer

Complétez la liste de vérification de configuration décrite dans avant Installation, installation et configuration de l'application Conformité de la configuration l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Rôle requis : admin

Procédure

1. Pour vous abonner aux ServiceNow produits, suivez les étapes de la section S'abonner auxServiceNow Store produits .
2. Pour installer une application que vous avez achetée à partir du , suivez les étapes de la ServiceNow Store section Installer une ServiceNow Store application .
3. **Facultatif :** Si vous souhaitez gérer votre autorisation pour l'application Conformité de la configuration sur d'autres ServiceNow AI Platform instances, procédez comme suit Gérer les autorisations de votre ServiceNow instance dans .
4. Si vous avez déjà installé l'application Conformité de la configuration et que vous la mettez à jour, reportez-vous à la section Installer une mise à jour dans une ServiceNow Store application .
5. Installer les applications prises en charge.

   Des applications tierces distinctes acquièrent et transforment des données dans Conformité de la configuration. Avant de pouvoir Conformité de la configuration corriger des éléments de configuration, vous devez installer une intégration d'analyse tierce et effectuer au moins une analyse réseau.

   Pour en savoir plus sur l'installation d'intégrations tierces pour , reportez-vous à Conformité de la configuration la section Intégrations de Conformité de la configuration.

Créer ou modifier Conformité de la configuration des règles d'affectation

Créez des règles pour affecter automatiquement des résultats des tests en fonction des conditions de filtre. Ces règles affectent les résultats des tests au fur et à mesure de leur importation.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Le système de base est fourni avec une règle d'affectation Conformité de la configuration , **Affecter au groupe de support CI**, qui affecte les résultats des tests au même groupe d'affectation que le groupe de support CI. Cette règle est désactivée par défaut. Vous pouvez modifier à l'aide des conditions de filtre. Les règles d'affectation vous permettent de définir une ou plusieurs conditions d'affectation et l'ordre d'exécution. Une fois que le résultat d'un test correspond à une condition de règle, la recherche d'affectation s'arrête.

Remarque : Les règles nouvelles ou mises à jour sont automatiquement évaluées lors de l'importation suivante ou manuellement à l'aide du bouton **Appliquer les modifications** de la liste Règles d'affectation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Règles d'affectation**.
2. Ouvrez la règle **Affecter au groupe de support CI** ou cliquez sur **Nouveau**.
3. Modifiez la règle **Affecter au groupe de support CI** ou, si **c'est Nouveau**, remplissez les champs du formulaire comme il convient.

Règle d'affectation de la conformité de la configuration

Champ	Description
Nom	Nom de la règle d'affectation.
Ordre d'exécution	Ordre dans lequel les règles sont évaluées. Le nombre le plus bas est évalué en premier. Les règles de priorité élevée, les résultats des tests qui nécessitent une gestion spéciale, lorsque le risque est critique ou un résultat de test qui doit être géré par la conformité réglementaire doivent être exécutés en premier. Ensuite, exécutez vos règles générales, où aucune manipulation spéciale n'est requise, et vous savez qui doit en être responsable. Enfin, créez une règle par défaut pour affecter les résultats des tests au groupe qui détermine à quel groupe d'affectation il doit appartenir. Ce groupe pourrait ajouter une autre règle pour couvrir ses décisions. Cette règle par défaut s'exécute en dernier.
Actif	Indique si la règle d'affectation est active.
Condition	
Champs de condition	Conditions à remplir. La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.
Nouveau critère	Ajoute d'autres champs de filtre de condition à choisir.
Description	Texte décrivant la règle d'affectation.
Affecter à l'aide de	Pour automatiser l'affectation des groupes créés en fonction de cette règle, choisissez l'une des options disponibles. ○ Groupe d'utilisateurs : sélectionner un groupe d'utilisateurs dans la table de recherche ○ Champ de groupe d'utilisateurs : sélectionnez un champ de groupe d'utilisateurs dans le menu déroulant. ○ Script : créez ou modifiez un script. **Remarque :** La création ou la modification d'un script nécessite une ServiceNow expertise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Champ du groupe d'utilisateur	Sélectionnez le groupe d’utilisateurs responsable de la correction des tests qui correspondent aux conditions des règles d’affectation.

4. Cliquez sur **Envoyer**.

Conformité de la configuration Règles de cibles de rattrapage

Les règles de cibles de rattrapage vous permettent de définir les délais prévus pour le rattrapage des résultats des tests. Vous pouvez envoyer des notifications aux utilisateurs et aux groupes lorsque les dates cibles approchent et lorsqu’elles sont dépassées.

Important : En tant qu’administrateur ou analyste de Configuration Compliance, vous pouvez obtenir la dernière date cible de rattrapage pour un ensemble spécifique de résultats de tests dans l’espace de travail Responsable des vulnérabilités. Cette méthode est plus efficace que l’exécution des règles de cibles de rattrapage pour tous les résultats des tests dans l’interface utilisateur classique, qui est un processus chronophage. Pour plus d'informations, consultez Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités.

Rôles requis : administrateur Configuration Compliance (sn_vulc_admin) ou gestionnaire disposant du rôle sn_vulc.manage_remediation_target_rules.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Règles de cibles de rattrapage

Une tâche planifiée, *`Evaluate and notify remediation targets`*, s’exécute quotidiennement et utilise des règles de cibles de rattrapage actives pour évaluer les enregistrements de résultats des tests actifs. Chaque fois que les enregistrements de résultats des tests associés aux tâches de rattrapage sont mis à jour ou modifiés, les valeurs modifiées sont évaluées par les règles cibles, et les changements sont déployés et affichés sur les tâches de rattrapage associées.

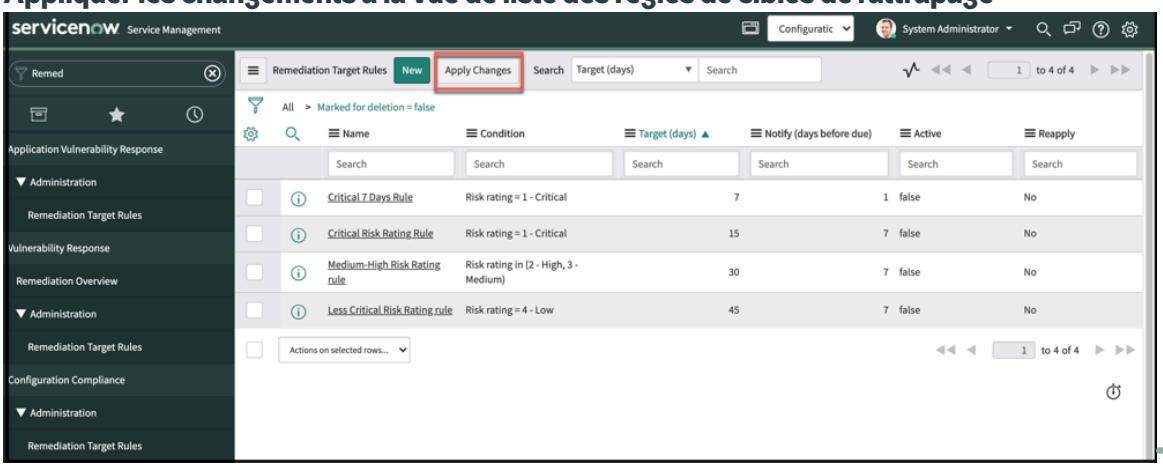
Vous pouvez modifier, désactiver ou supprimer les règles de cibles de rattrapage existantes et en créer de nouvelles. Lorsque vous modifiez, désactivez ou créez une règle, vous pouvez cliquer sur **Appliquer les changements** à partir de la vue de liste Règles de cibles de rattrapage et appliquer manuellement les changements que vous avez introduits avant le prochain travail planifié. Avec cette option, vous pouvez réévaluer vos enregistrements de résultats de test sans avoir à attendre. Si vous choisissez de ne pas appliquer vos changements manuellement, la tâche planifiée quotidienne suivante récupère vos changements et les applique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Règles de cibles de remédiation** pour afficher les règles de cibles de rattrapage.

Appliquer les changements à la vue de liste des règles de cibles de rattrapage



2. Cliquez sur une règle dans la colonne Nom pour ouvrir son enregistrement.
3. Cochez la case **Actif** sur l'enregistrement de règle de cible de rattrapage pour activer (vrai) toutes les règles désactivées (faux).

Chaque fois que vous modifiez ou ajoutez une règle cible, que vous choisissiez d'appliquer les modifications manuellement ou d'attendre la tâche planifiée suivante, vos modifications sont utilisées pour évaluer tous les résultats des tests actifs ainsi que toutes les autres règles cibles affectées par vos modifications. Lorsque vous choisissez d'appliquer manuellement les changements, cette évaluation peut prendre un certain temps si vous avez un grand nombre de résultats de tests actifs, car toutes les règles impactées par vos changements sont utilisées pour une évaluation.

Par exemple, la valeur par défaut pour le nombre de jours de rattrapage ciblé est 30. Si vous créez une règle qui dispose également de 30 jours pour le rattrapage ciblé, cette règle et toutes les règles cibles dont les dates cibles sont de 30 jours ou plus sont appliquées à vos résultats des tests.

Règles cibles désactivées et supprimées

Lorsqu'une règle est active, la valeur « vrai » s'affiche dans la colonne Actif de la vue de liste Règles de cibles de rattrapage. Une fois qu'une règle est désactivée (faux), elle n'est plus appliquée aux nouveaux résultats des tests. Toutefois, la tâche planifiée continue de suivre tous les résultats des tests existants auxquels la règle a été appliquée. Si la ou les règles désactivées sont réactivées par la suite, tout résultat de test dont le champ Date **cible de rattrapage** est vide est évalué par rapport aux règles réactivées. Cela inclut les résultats des tests créés alors que les règles étaient désactivées.

Lorsque des règles sont supprimées, la **date cible de rattrapage** et les champs associés sur les résultats des tests fermés sont conservés. La **date cible de rattrapage** et les champs connexes sur les résultats des tests non fermés sont effacés, et toutes les règles dépendantes sont réappliquées.

Pour désactiver une règle, à partir de l'enregistrement de règle de cible de rattrapage, désactivez la case à cocher active, puis cliquez sur **Mettre à jour**. Faux s'affiche dans la colonne Actif de la vue de liste Règles de cibles de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour supprimer une règle, cliquez sur **Supprimer** dans le formulaire ou, dans la vue de liste, sélectionnez la ou les règles, puis cliquez sur **Supprimer** dans la liste **Actions sur les lignes** . La règle n'est plus affichée dans la liste et la règle suivante dans l'ordre d'opération remplace la règle supprimée.

Si vous désactivez ou supprimez une règle et choisissez d'appliquer vos changements avant la prochaine tâche planifiée, la référence de règle est effacée du champ, mais la date de rattrapage et les données d'état sont conservées. Si vous n'appliquez pas vos changements manuellement, la référence de règle est effacée du champ avec la tâche planifiée suivante.

À propos des règles cibles et de la tâche planifiée Évaluer et notifier les cibles de rattrapage

La *`Evaluate and notify remediation targets`* tâche planifiée s'exécute une fois à 4:30:00 quotidiennement. Il récupère toutes les règles de cibles de rattrapage actives et évalue tous les résultats des tests actifs, en commençant par les résultats des tests avec la date cible de rattrapage la plus ancienne. Il évalue tous les résultats des tests qui répondent aux critères suivants :

- ne sont pas à l'état **Fermé** .
- N'ont pas de date cible de rattrapage.
- Ont des dates cibles de rattrapage postérieures aux dates indiquées dans les règles de cibles de rattrapage.
- sont créés une fois l'importation d'un scanner terminée. La tâche planifiée récupère et évalue tous les nouveaux résultats des tests créés à la suite d'une importation.

Une fois qu'une règle cible est définie, les dates cibles de rattrapage sont calculées par la *`Evaluate and notify remediation targets`* tâche planifiée. La tâche planifiée ajoute une date cible de rattrapage, s'il n'en existe pas, ou, si cette règle contient une date antérieure à celle de l'enregistrement, elle met à jour la date cible existante.

Tous les enregistrements expirés et les dates de rappel qui correspondent aux règles cibles sont récupérés par la tâche et des notifications sont envoyées. Pour les règles désactivées, la tâche efface les champs de rattrapage des enregistrements de résultats des tests et arrête d'envoyer des notifications.

Lorsqu'elle est activée, la propriété sn_sec_cmn.evaluate_targetmissed_records empêche la tâche planifiée d'évaluer les *`Evaluate and notify remediation targets`* résultats des tests manqués cibles. Cette propriété est activée par défaut.

Affichage des dates cibles et de l'état sur la liste et les vues de formulaire

Conformité de la configuration Les gestionnaires peuvent voir la date cible de rattrapage à la fois dans le formulaire de résultats des tests et dans les vues de listes. Les règles de cibles de rattrapage sont également exécutées après l'importation d'un scanner et réexécutées si un résultat de test est rouvert.

La tâche planifiée met à jour la **cible de rattrapage** et l'état du **rattrapage** dans la vue de liste des résultats des tests, ainsi que les champs **Règle de cible de rattrapage**, Cible de **rattrapage** et **État du rattrapage** sur le formulaire des résultats des tests.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

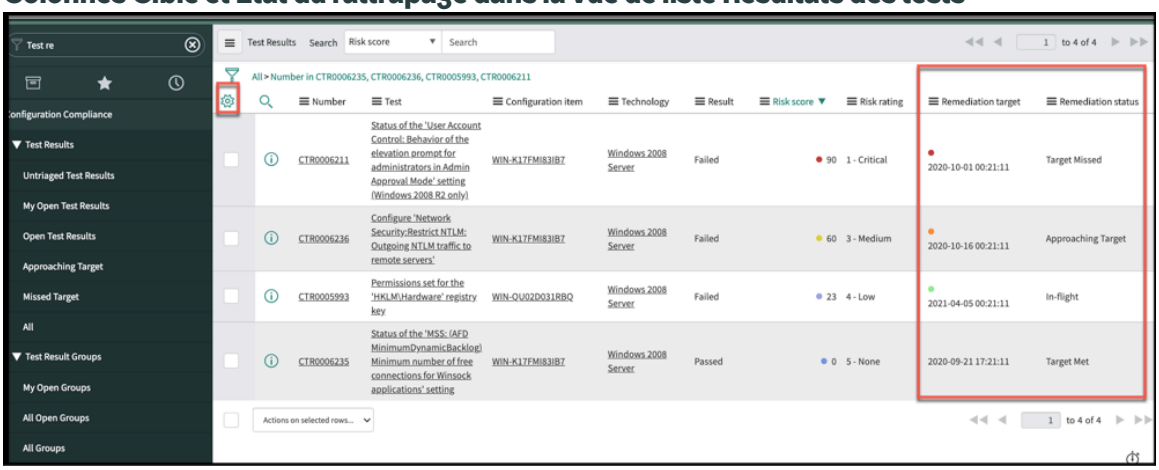
Remarque : Par défaut, les colonnes **Cible de rattrapage** et **État du rattrapage** ne sont pas affichées dans la vue de liste Résultats des tests. Pour afficher ces colonnes, vous devez également les ajouter à la vue de liste. De même, ajoutez les champs **Règle de cible de rattrapage**, **Cible de rattrapage** et **État du rattrapage** au formulaire de résultats des tests.

Utilisez les zones de liste double dans les menus Paramètres et Action supplémentaire, respectivement, comme illustré dans les images suivantes, pour afficher ces colonnes et champs. Pour le menu Action supplémentaire sur l'enregistrement des résultats du test, cliquez sur l'icône de menu, puis sur **Configurer** et **Mettre en page un formulaire** pour afficher la zone de sélection et déplacer les champs de **Disponible** à **Sélectionné**.

La date cible de rattrapage est codée dans la vue de liste des résultats des tests sous forme de points colorés :

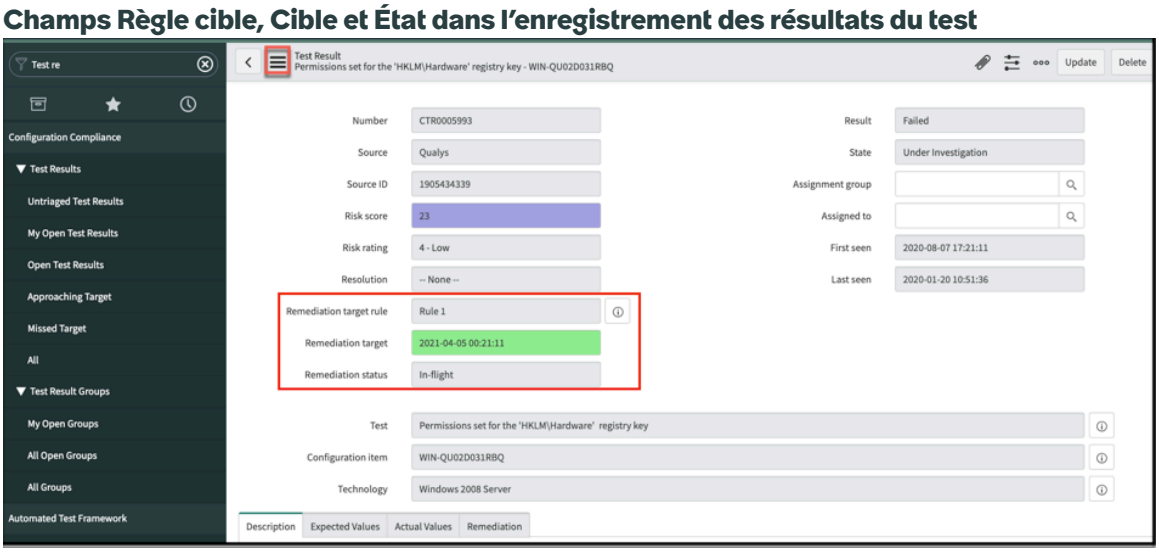
- Les résultats des tests qui n'ont pas encore atteint leur date de notification sont affichés en vert.
- Les résultats des tests approchant de la date cible de rattrapage sont affichés en orange.
- Les résultats des tests après la date cible de rattrapage s'affichent en rouge.

Colonnes Cible et État du rattrapage dans la vue de liste Résultats des tests



- Cible manquée : la date cible est dépassée
- En cours : le résultat du test est en cours

Champs Règle cible, Cible et État dans l'enregistrement des résultats du test



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les enregistrements des résultats des tests sont également affichés visuellement sur le tableau de Conformité de la configuration bord. Accédez à la **Tous** > **Configuration Compliance** > **Vue d'ensemble** et consultez le tableau de bord pour connaître l'état. La vue d'ensemble inclut les widgets existants et l'état de rattrapage. Les couleurs des graphiques correspondent aux couleurs affichées dans la vue de liste Résultats des tests et l'enregistrement des résultats des tests.

Scénario de règle de cible de rattrapage

Lorsque plusieurs règles cibles de rattrapage sont appliquées au même résultat de test, la règle la plus restrictive s'applique.

Par exemple, si un résultat de test identifié pour la première fois le 03/01/2018 répond aux conditions de deux règles de cible de rattrapage :

- Règle de cible de rattrapage 1 : définie le 03/07/2018 ; la cible de rattrapage est de 15 jours depuis la première observation ; La date cible de rattrapage calculée est le 16/03/2018 10:00:00.
- Règle de cible de rattrapage 2 : définie le 03/10/2018 ; la cible de rattrapage est de 10 jours depuis sa première observation ; La date cible de rattrapage calculée est le 11/03/2018 10:00:00.

Remarque :

Les cibles de rattrapage sont **calculées** à partir de la date du dernier observé additionnée au nombre de jours (mesurés par incréments de 24 heures).

À partir de la version 14.5, les cibles de rattrapage sont calculées à partir **de la cible à partir du (date).** La valeur par défaut reste **Dernier observé**. À partir de la version 14.12, la valeur par défaut est **Dernière passe**.

Dans ce scénario, la règle de cible de rattrapage 2 s'applique au résultat du test, car elle a la date la plus restrictive : 10 jours depuis que le résultat du test a été identifié pour la première fois contre 15 jours.

Créer ou modifier des règles cibles et réappliquer les changements

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Règles de cibles de remédiation** pour afficher, modifier et créer de nouvelles règles de cibles de rattrapage.
2. Dans la colonne Nom, cliquez sur une règle pour ouvrir une règle cible et modifier l'enregistrement, ou cliquez sur **Nouveau** pour créer une règle cible.
3. Remplissez le formulaire pour définir le délai de rattrapage prévu, spécifier les résultats des tests auxquels cette règle s'applique avec conditions, et déterminer quand envoyer des rappels aux utilisateurs ou aux groupes, ou aux deux.

Formulaire Règle de cible de rattrapage

Champ	Description
Nom	Nom de votre règle.
Actif	Activez ou désactivez la règle. La règle est automatiquement activée (vrai) par défaut et sera appliquée à vos résultats de test si vous choisissez d'appliquer les changements manuellement ou après la tâche planifiée suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Cible (jours)	Définissez la date limite ciblée pour le rattrapage en nombre de jours. La valeur par défaut pour le nombre de jours de rattrapage ciblé est 30. Par exemple, si vous créez une règle qui a également 30 pour une valeur cible, votre nouvelle règle et toutes les autres règles existantes qui ont également 30 jours ou plus comme dates cibles seront appliquées à vos résultats des tests.
(date) à partir de la cible	Date à partir de laquelle les dates cibles sont calculées. Vous pouvez spécifier uniquement les champs de date ou le type de date et d'heure. À partir de la version 14.12, la valeur par défaut est *Dernière passe*. Sélectionnez l'une des options suivantes : ○ Dernier observé ○ Premier observé ○ Créées ○ Dernière transmission Si la dernière transmission est vide, la date de création est prise en compte pour le calcul de la cible de rattrapage. ○ Dernières ouvertures Pour personnaliser les valeurs de ce champ, consultez KB1642413 .
Notifier (jours avant l'échéance)	Définissez un nombre de jours avant la date limite pour rappeler les utilisateurs et les groupes.
Description	Brève description de la règle.
Condition	Utilisez le générateur de conditions pour spécifier les résultats des tests auxquels cette règle s'applique. Par exemple, définissez une date cible de rattrapage de 30 jours pour tous les résultats des tests dont le score de risque est supérieur à 70. Envoyer des rappels aux utilisateurs ou aux groupes, ou aux deux, sept jours avant la date de rattrapage. La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire. Avant la version 12.0, le respect de la casse est pris en charge pour le texte de recherche que vous saisissez dans le générateur de conditions.
Utilisateur et groupes d'utilisateurs ou les deux	Sélectionnez des utilisateurs ou des groupes, ou les deux, pour envoyer des notifications sur les dates cibles proches et dépassées que vous avez définies.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Envoyer**. Sinon, pour enregistrer les règles modifiées, cliquez sur **Mettre à jour**.

   La vue de liste s'affiche avec votre règle mise à jour ou nouvelle. Les règles de la liste sont classées dans l'ordre et s'exécutent en commençant par la règle dont la date cible de rattrapage est la plus basse. Si vous désactivez ou supprimez une règle, la règle suivante dans la séquence d'ordre remplace la règle inactive ou supprimée.

5. Pour appliquer vos nouveaux changements maintenant, cliquez sur **Appliquer les changements**.

Conformité de la configuration Groupes de calculateurs

Conformité de la configuration Les calculateurs sont utilisés pour mettre à jour les valeurs d'enregistrement lorsque des conditions prédéfinies sont remplies. Les calculateurs sont regroupés en fonction des critères utilisés pour déterminer le mode de mise à jour des enregistrements.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Conformité de la configuration Groupes de calculateurs

Depuis l'enregistrement du calculateur de risque par défaut, les règles du calculateur peuvent être appliquées à tous les résultats de tests et collections affectés sur demande. Les gestionnaires de vulnérabilité peuvent utiliser cette fonctionnalité pour ajuster la configuration de leur calculateur de risque. Ils peuvent expérimenter plusieurs schémas de hiérarchisation au début de leur déploiement et appliquer ces changements à la demande pour voir leur impact sur les résultats d'importation.

Le groupe de calculateurs de score de risque a été renommé Calculateurs de risque.

Les calculateurs de déploiement des scores de risque sont inclus avec Conformité de la configuration. Il existe deux types de calculateurs de cumul individuel :

Déploiement des risques du test de configuration

Calculateurs qui cumulent les scores de risque de tous les résultats des tests avec le même test de configuration afin de fournir un score de risque global pour le test de configuration. La valeur cumulée s'affiche dans les champs Score de risque.

Déploiement du score de risque de la tâche de rattrapage

Ces calculateurs cumulent les scores de risque de tous les résultats de test d'une tâche de rattrapage afin de fournir un score de risque global pour cette tâche de rattrapage. La valeur cumulée s'affiche dans les champs Score de risque.

Le groupe de calculateurs de score de risque et le groupe de calculateurs de déploiement de score de risque sont activés par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations, consultez les termes clés suivants pour Conformité de la configuration les calculateurs :

Résultat de test

Un résultat de test est le résultat du test de configuration sur un élément de configuration (CI) et la technologie associée. Les résultats des tests à l'état Échec, Erreur et Inconnu identifient le matériel, les logiciels et les actifs qui ne sont pas conformes à vos politiques.

Tâche de rattrapage

Les résultats des tests sont regroupés au moment de l'importation des données en fonction des règles de tâche de rattrapage prédéfinies. Ces tâches de rattrapage sont similaires aux groupes de vulnérabilité dans Réponse aux vulnérabilités. Les tâches de rattrapage organisent les résultats des tests en groupes pour l'analyse en bloc et représentent un ensemble d'éléments à corriger.

Score du risque dans un résultat de test

Valeur calculée par les calculateurs de score de risque qui est basée sur le contexte professionnel d'une ressource et la sévérité du test associé. Il s'agit de la moyenne de la criticité opérationnelle de l'actif affecté telle que définie dans la CMDB, et de la gravité du test telle que communiquée par le scanner.

Plusieurs services peuvent être associés à chaque actif. La criticité opérationnelle d'un actif est déterminée par le service présentant la criticité la plus élevée.

La valeur calculée est affichée dans les champs Score de risque des résultats des tests. Les scores affichent des valeurs comprises entre 0 et 100. Les champs sont également codés par couleur pour vous fournir la gravité en un coup d'œil.

Score de risque dans la tâche de rattrapage

Ce score est affiché sur l'enregistrement de tâche de rattrapage et est la valeur cumulée des scores de risque pour tous les résultats des tests actifs dans une tâche de rattrapage. Ce score change au fur et à mesure que les résultats des tests sont corrigés dans la tâche de rattrapage.

Score du risque dans le test de configuration

Ce score s'affiche sur les tests de configuration et correspond à la valeur cumulée des scores des risques pour tous les résultats des tests actifs avec ce test de configuration. Ce score change à mesure que les résultats des tests associés à ce test de configuration sont corrigés.

Cote de risque

Degré de risque qu'un résultat de test échoué pose à votre système. Il est basé sur une gamme de scores de risque sur une échelle numérique de 1 à 5 qui évalue les risques de critiques (1) à aucun (5). Le score est basé sur une plage de scores de risque et s'affiche dans les champs de cote de risque.

Plages de cote de risque

Cote de risque	Score du risque
1 - Critique	90 à 100
2 : élevé	70 à 89
3 - Moyen	40 à 69 ans
4 : faible	1 à 39
5 : aucun	0

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculateurs de déploiement des scores du risque

Il existe deux types de calculateurs de déploiement :

- Déploiement des risques du test de configuration : ces calculateurs regroupent les scores de risque de tous les résultats des tests avec le même test de configuration afin de fournir un score de risque global pour le test de configuration. La valeur cumulée s'affiche dans les champs Score de risque. Vous pouvez modifier les valeurs de script pour le poids et le score de ces calculateurs.
- Déploiement du score de risque de la tâche de rattrapage : ces calculateurs cumulent les scores de risque de tous les résultats des tests d'une tâche de rattrapage afin de fournir un score de risque global pour cette tâche de rattrapage. La valeur cumulée s'affiche dans les champs Score de risque. Vous pouvez modifier les valeurs de script pour le poids et le score de ces calculateurs. Pour obtenir un exemple de calculateur de déploiement de score Risk et de la manière dont il calcule les scores, reportez-vous à la section Exemple de calcul de déploiement de risque pour Conformité de la configuration (avant la version 15.0).

Score de risque historique

Le score de risque inhérent sur tous les résultats des tests réussis dans une tâche de rattrapage. Ce champ affiche la quantité de risque qui a été corrigée par un groupe de tests et s'affiche uniquement lorsqu'un groupe de tests est à l'état « Fermé » et que le score de risque est nul.

Les scores sont calculés chaque fois que le score de risque change ou lorsque les résultats des tests sont ajoutés ou supprimés d'une tâche de rattrapage.

Remarque : Pour fonctionner correctement, ce script nécessite le module d'extension. Mappage des services est disponible sous forme Mappage des services d'abonnement distinct et nécessite une activation par ServiceNow le personnel.

Créer un groupe de Conformité de la configuration calculateurs

Conformité de la configuration Les groupes de calculateurs sont utilisés pour regrouper les calculateurs en fonction de la façon dont vous souhaitez les utiliser.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Le Conformité de la configuration système de base comprend un groupe de calculateurs : **le score de risque**. Lorsque vous créez d'autres calculateurs, vous pouvez les ajouter à ce groupe ou créer d'autres groupes et calculateurs. Dans chaque groupe, le premier calculateur qui correspond au résultat du test s'exécute.

Deux groupes de calculateurs sont inclus dans l'application Conformité de la configuration :

- Calculateurs de risques
- Calculateurs de déploiement des scores du risque

Les calculateurs de risque calculent le score de risque et la cote de risque d'un résultat de test.

Les calculateurs de déploiement des scores de risque regroupent les scores de risque pour tous les résultats des tests et tâches de rattrapage avec le même test de configuration afin de fournir un score de risque global.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

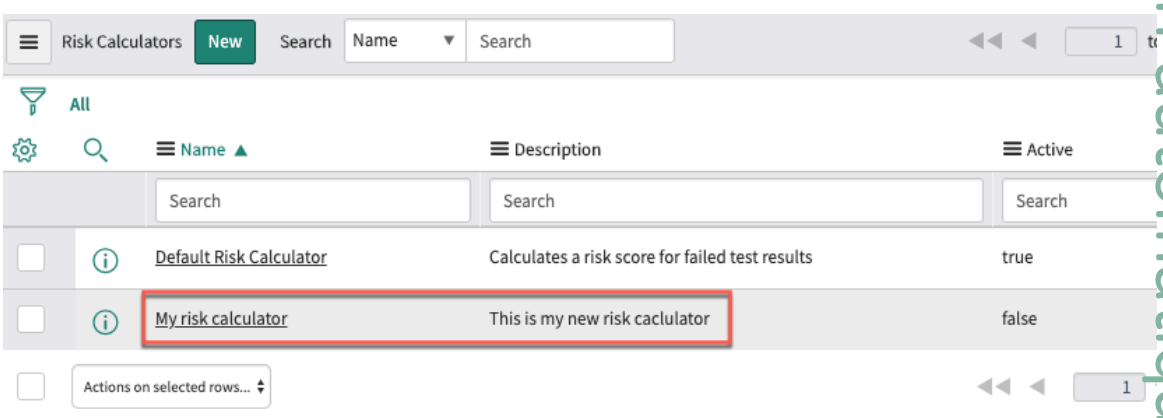
Vous pouvez également créer de nouveaux calculateurs directement à partir de ces groupes.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Groupes de calculateurs**.
2. Accédez à la **Tous** > **Configuration Compliance** > **Administration** et sélectionnez **Calculateurs de risque** ou **Calculateurs de déploiement des scores de risque**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom du calculateur.
Description	Description de ce groupe de calculateurs.
Actif	Activez ou désactivez le groupe de calculateurs.

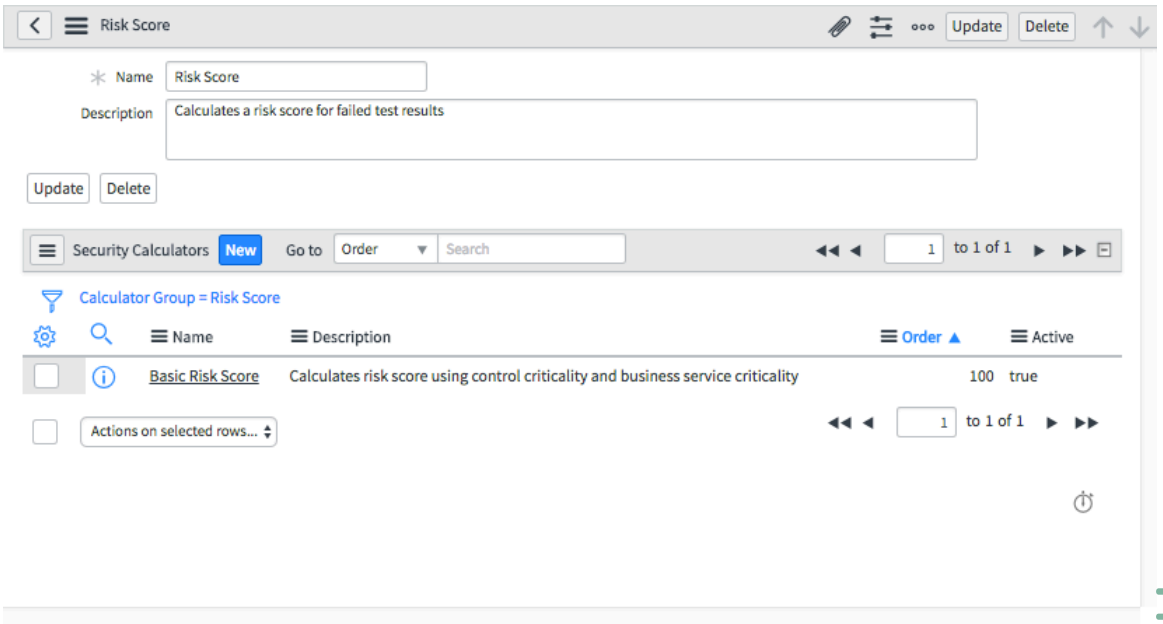
5. Cliquez avec le bouton droit sur **Enregistrer** dans l'en-tête du formulaire ou cliquez sur **Soumettre**.
   Le nouveau groupe de calculateurs s'affiche dans la liste des groupes avec les autres calculateurs. Cliquez sur le nom du nouveau groupe de calculateurs pour ouvrir l'enregistrement. Voir Créer, modifier et réappliquer des calculateurs de risque pour Conformité de la configuration pour plus d'informations sur la définition des conditions et des valeurs affichées et la réapplication des calculateurs.



La liste connexe **Calculateurs de sécurité s'affiche** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Nouveau** pour ajouter des calculateurs ainsi que leurs conditions au groupe.

   La sensibilité à la casse du texte de recherche que vous saisissez dans le générateur de conditions n'est pas prise en charge sur cet enregistrement ou ce formulaire.

Conformité de la configuration Calculatrices et règles de la calculatrice

Conformité de la configuration Automatiser le calcul des valeurs initiales des champs sur les résultats des tests. La condition de chaque calculateur est évaluée dans l'ordre, et le premier calculateur correspondant est utilisé.

Conformité de la configuration Calculatrices

Le système de base Configuration Compliance inclut un calculateur de Configuration Compliance (**calculateur de risque par défaut**) qui définit le **score de risque** de base sur le résultat du test. Les calculateurs de Configuration Compliance peuvent être créés pour classer par ordre de priorité et évaluer l'impact des résultats des tests en fonction de n'importe quel critère à l'aide de filtres de condition. Qu'il s'agisse de l'impact commercial de la vulnérabilité, de la classe de l'élément de configuration (CI), vous pouvez créer des calculateurs de conformité de la configuration supplémentaires pour définir d'autres champs sur les résultats des tests ou personnaliser les calculateurs de conformité de la configuration existants. Une calculatrice peut être rédigée pour refléter n'importe quel ensemble de priorités.

Chaque calculateur contient une liste de règles du calculateur, avec une condition déterminant quand l'appliquer. Lorsque le calculateur est exécuté, la condition de chaque règle est évaluée dans l'ordre et la première règle correspondante est utilisée.

Tous les calculateurs Configuration Compliance activés définissent les champs sélectionnés chaque fois qu'un résultat de test est créé, lorsqu'un CI ou un test de configuration associé change ou lorsque le lien connexe **Calculer le score de risque** dans un résultat de test est utilisé. Par exemple, le score de risque est automatiquement mis à jour sur les enregistrements de résultats de test lorsque la valeur control.criticality est mise à jour sur un résultat de test importé. Une fois qu'une importation de résultat de test a mis à jour un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

score de résultat de test, vous pouvez recalculer le score de risque des résultats de test en sélectionnant le bouton **Réappliquer le calculateur** .

À partir d'un résultat de test existant, si vous sélectionnez le lien connexe **Calculer le score de risque** et que l'un des calculateurs est activé, le champ Score de risque du résultat du test est mis à jour.

Remarque :

- Le lien connexe **Calculer le score de risque** n'est visible que lorsqu'au moins un calculateur de Configuration Compliance est activé.
- À partir de la version 22.0 de , vous pouvez mettre à jour le score de risque pour un résultat de Réponse aux vulnérabilités test dans l'espace de travail du gestionnaire de vulnérabilité et l'espace de travail de rattrapage informatique en sélectionnant le bouton **Calculer le score de risque** dans sa vue d'enregistrement.
- À partir de la version 14.13 de , chaque fois que le score de risque d'un résultat de Conformité de la configuration test change, les détails suivants sont documentés dans la section Notes du résultat du test :
  - Nom du groupe de calculateurs
  - Nom du calculateur : selon que la règle du calculateur est basée sur un modèle ou un script, le nom est ajouté avec les détails entre crochets. Pour modifier ou afficher la base de la règle du calculateur, sélectionnez une règle et cochez la case Vue **avancée** . Dans la liste déroulante **Type de valeur** , sélectionnez l'option requise. **Si Modèle** est sélectionné, le score de risque est mis à jour en fonction de la condition spécifiée dans la règle. Si **Script** est sélectionné, vous pouvez ajouter ou mettre à jour le script existant.
  - Valeurs des champs avec leur pondération et leur contribution au score de risque
  - Score de risque final
  - La propriété `sn_sec_cmn.risk_score_changes_add_worknotes` système permet de renseigner la section des notes de travail. À partir de la version 15.2.1 de Conformité de la configuration, la propriété `sn_sec_cmn.risk_score_changes_add_worknotes` système est inactive par défaut. Si vous l'activez, vous pouvez alors seulement voir tous les changements liés au score de risque d'un résultat de test dans la section Notes de travail. En outre, les notes de travail ne sont mises à jour qu'en cas de changement du score de risque.

Conformité de la configuration Règles du calculateur

Par défaut, un **calculateur de risque par défaut du** système de base est fourni. Si vous souhaitez créer une règle de risque pour ce calculateur, vous devez définir le champ cible du **calculateur de risque par défaut** sur **Score de risque**. Sélectionnez le bouton **Nouvelle règle de risque** pour créer une nouvelle règle de risque. Cela crée une règle de calcul de résultat de test spécialisée, appelée **règle de risque**, qui, à son tour, calcule le **score de risque** en fonction de plusieurs valeurs. Par défaut, les valeurs suivantes sont prises en compte pour calculer le score de risque :

- Criticité opérationnelle
- Criticité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez ajuster les valeurs à utiliser dans la **règle de risque par défaut** et le poids à donner à chacune de ces valeurs. Les poids sont utilisés pour ajuster le nombre de chaque élément lors de la définition du **score de risque** de base.

À partir Conformité de la configuration de la version 13.0, vous pouvez personnaliser les critères de la règle de risque par défaut. Pour plus d'informations, voir Définir des champs et des poids pour la règle de risque.

Affectation d'un pourcentage de pondération

Vous pouvez également affecter un pourcentage de pondération (0-100) au niveau de la valeur du champ. Par exemple, vous pouvez affecter un pourcentage de pondération à chaque niveau de gravité (de Aucun à Critique). Si la pondération de criticité est de 50 pour la règle de risque et que les valeurs de pondération suivantes sont affectées au niveau de criticité :

Affecter un pourcentage de pondération

Criticité	Score du risque
Critique	100
Élevé	50
Moyen	20
Aucun	0

Si la criticité est critique, la pondération correspondante est 50. Si la criticité est élevée, la pondération est égale à 25, et si la criticité est moyenne, la pondération est égale à 10. Si la criticité est nulle, la pondération correspondante est 0. Pour plus d'informations, consultez l'exemple de calcul du score de risque pour Configuration Compliance.

Chaque règle a un paramètre **d'ordre** . Toutefois, la première à correspondre aux conditions met à jour le champ de **score de risque** dans le résultat du test. Les règles de calculateur non scriptées ont généralement un impact moindre sur les performances que les règles de calculateur scriptées.

Le calculateur du système Conformité de la configuration de base contient des règles de calcul qui attribuent à chaque niveau de criticité (Aucun à Critique) une valeur (0-100) pour le **score de risque** en fonction de la gravité. Un score de risque de 100 est automatiquement affecté à une gravité inconnue. Ces valeurs peuvent être ajustées, par exemple le calculateur de risque par défaut, de nouvelles règles de calcul ou de nouvelles règles de risque peuvent être créées.

Poids du score de risque de vulnérabilité

Toutes les vulnérabilités se voient attribuer un score de risque et une cote de risque en fonction de facteurs tels que la gravité, la criticité, les informations sur l'exploitation, et ainsi de suite. La règle *`Update Risk Rating from Risk Score`* métier de la table des éléments vulnérables est responsable du calcul de la cote de risque. Chaque fois que le score de risque change, la cote de risque est calculée et renseignée pour les éléments vulnérables. Avant la version 17.1 de l'application Réponse aux vulnérabilités (VR), les cotes de risque suivantes étaient fournies dans le cadre du script include VulnerabilityUtils, qui étaient codées en dur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur (cote de risque)	Poids (score de risque)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

À partir de la version 18.0 de Réponse aux vulnérabilités,

- Les types de cote de risque sont expédiés dans la table de base sous forme de cc_risk_rating. Ces types sont transmis dans le cadre de la règle métier sur chaque table où la cote de risque est calculée.
- Le script a été modifié afin que vous puissiez interroger les entrées dans les valeurs de la table Poids du score de risque pour le calcul de la cote de risque.
- Ajoutez des entrées supplémentaires pour un type existant ou créez-en un nouveau. Lorsque vous créez un nouveau type, assurez-vous d'ajouter les étiquettes pour la nouvelle cote de risque et de modifier les scripts et les règles métier associés. Vous devez également ajouter un nouveau style pour le nouveau score de risque.
- Modifiez le script pour interroger les enregistrements dans la table de base.

Vous pouvez accéder à la table des pondérations des scores de risque en saisissant sn_sec_cmn_risk_score_weight dans le navigateur de filtre.

En outre, le score de risque est automatiquement recalculé dans les scénarios suivants :

- Lorsqu'un élément de configuration (CI) passe d'un mode non accessible sur Internet à un élément accessible sur Internet.
- Lorsque les vulnérabilités et expositions communes (CVE) ou les entrées tierces (TPE) associées sur les éléments de vulnérabilité (VI) sont liées à une vulnérabilité d'exploitation connue (KEV) CVE.

Définir des champs et des poids pour la règle de risque

Personnalisez les paramètres et les pondérations de la règle de risque afin de pouvoir générer des scores de risque qui utilisent les données de test et d'actif propres à votre organisation. En sélectionnant les champs qui sont inclus dans la règle de risque, vous pouvez définir un cadre de travail de notation des risques efficace.

Avant de commencer

Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Calculateurs de risques**.
2. Cliquez sur **Calculateur de risque par défaut**.
3. Sélectionnez le champ cible comme **score de risque**.
   Le bouton **Nouvelle règle de risque** s'affiche dans la table Règle du calculateur.
4. Cliquez sur le bouton **Nouvelle règle de risque** pour accéder au formulaire **Règle de risque de Configuration Compliance** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans la section Critères du calculateur de risque, définissez le poids de chaque critère en fonction de son importance dans le calcul du score de risque global.
6. Décochez la case **Actif** pour désactiver la règle.
7. Cliquez sur **Ajouter des critères** pour ajouter des champs de règles de risque aux critères du calculateur de risque.
8. Remplissez les champs du formulaire.

Formulaire de champ de règle de risque

Champ	Description
Choisir la table de référence	Table que vous utilisez pour définir la pondération du score de risque. Sélectionnez une option parmi les suivantes : ○ Résultat du test : ajoutez des champs auxquels vous pouvez accéder directement depuis le résultat du test (TR). ○ Résultat du test : élément de configuration : Ajoutez des champs accessibles à la visite avec point qui font partie des extensions de table de base, telles que la table Matériel. Ces champs ne font pas partie de la table cmdb_ci de base. ○ Résultat de test - Test : ajoutez des champs parcourables par point qui font partie des tables qui étendent la table de base, par exemple, Entrée tierce. Ces champs ne font pas partie de la table de base du test de configuration. ○ Table de référence des résultats des tests : ajoutez des champs qui font partie des tables connexes (m2m) ou des tables qui font référence au résultat des tests. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du résultat des tests. ○ Table de référence de l'élément de configuration : ajoutez des champs qui font partie des tables connexes (m2m) de cmdb_ci ou tables ayant une référence à cmdb_ci. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du TR. ○ Table de référence de test : ajoutez des champs qui font partie des tables connexes (m2m) de sn_vulc_test ou

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	des tables qui ont une référence à sn_vulc_test. Ces champs ne sont pas directement accessibles par une remontée pas à pas à partir du TR. ○ Conditions personnalisées : utilisez cette option pour affecter des poids à la règle en évaluant la condition. Par exemple, le filtre orienté vers Internet détermine si un élément de configuration (CI) est externe ou interne.
Champ	Champ utilisé pour le calcul du score de risque pour cette règle.
Pondération	Pondération de ce champ dans la règle de risque. La valeur doit être un nombre entier compris entre 0 et 100.
Table	○ Résultat de test > élément de configuration ○ Résultat de test > test ○ Table de référence de résultats des tests ○ Table de référence de l'élément de configuration ○ Table de référence de test Ce champ est disponible uniquement lorsque l'une des options répertoriées est sélectionnée dans le champ Choisir la table de référence.
Agrégation	Sélectionnez la valeur minimale ou maximale à prendre en compte pour les calculs lorsque le champ est sélectionné dans les tables connexes (m2m). Ce champ apparaît uniquement lorsqu'une table de référence est sélectionnée dans le champ Choisir la table de référence.
Définir la pondération de la valeur	Composant permettant d'attribuer des poids à chaque valeur de champ. Pour les champs numériques, définissez les valeurs de champ sous forme de plage (par exemple, 1 à 5). La valeur doit être un nombre entier compris entre 0 et 100. Ce champ n'apparaît pas si l'option Conditions personnalisées est sélectionnée dans le champ Choisir la table de référence.
Table de condition	Sélectionnez une condition dans la liste. Ce champ est disponible uniquement lorsque l'option Conditions personnalisées

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	est sélectionnée dans le champ Choisir la table de référence.
Nom de champ	Entrez un nom pour les critères de risque. Ce champ est disponible uniquement lorsque l'option Conditions personnalisées est sélectionnée dans le champ Choisir la table de référence.
Condition	Prévisualisez les éléments de cette table qui correspondent aux conditions définies. Ce champ est disponible uniquement lorsque l'option Conditions personnalisées est sélectionnée dans le champ Choisir la table de référence.

9. Cliquez sur **Envoyer**.

Que faire ensuite

Sur la page Règle, activez et réappliquez la règle pour réévaluer le score de risque sur le résultat des tests actifs.

Modifier les calculateurs de déploiement des risques pour Conformité de la configuration

Modifiez un calculateur de déploiement de risque existant.

Avant de commencer

Rôle requis : Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** et sélectionnez **Calculateurs de déploiement des scores de risque**.
2. Une fois la liste des calculateurs de déploiement des scores de risque affichée, cliquez sur un calculateur pour ouvrir l'enregistrement et modifier le formulaire.

Champ	Description
Nom	Nom du calculateur de déploiement du test de configuration ou de la tâche de rattrapage.
Description	Description du calculateur de déploiement de risque.
Table	Table sur laquelle le calculateur de déploiement est appliqué.
Inclure le report	Inclut les résultats des tests différés pendant le déploiement du score de risque.

3. Définissez les pondérations de l'une des façons suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dans la section Poids de déploiement, affectez des pondérations pour les éléments suivants :

Poids des déploiements

Champ	Description	Pondération par défaut
Score du risque maximal	Score de risque maximal des résultats des tests pris en compte.	85
Score de risque moyen	Agrégat des scores de risque de tous les résultats des tests pris en compte.	0
Nombre de résultats des tests	Nombre de résultats des tests.	15

- Sélectionnez la case à cocher Vue **avancée** et, dans l'éditeur de **valeurs de script** , modifiez les valeurs du script selon vos besoins.

Remarque : La modification d'un script nécessite une connaissance approfondie de l'application et de l'application ServiceNow AI PlatformConformité de la configuration .

4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Les calculateurs de déploiement sont des travaux planifiés qui s'exécutent toutes les heures pour récupérer des changements. Ces travaux planifiés comprennent également les scores de risque globaux pour les tests de configuration et la tâche de rattrapage. Les valeurs cumulées s'affichent dans les champs de score de risque.

Pour obtenir un exemple sur la façon dont un calculateur de déploiement de risque détermine les scores, reportez-vous à la section Exemple de calcul de déploiement de risque pour Conformité de la configuration (avant la version 15.0).

Créer, modifier et réappliquer des calculateurs de risque pour Conformité de la configuration

Les règles du calculateur peuvent être appliquées à tous les résultats de tests et collections affectés sur demande. Les gestionnaires de vulnérabilité peuvent utiliser cette fonctionnalité, ajuster la configuration de leur calculateur de risque et appliquer des changements sur demande pour importer les résultats.

Avant de commencer

Rôle requis : sn_vulc.admin

Procédure

1. Pour créer un nouveau calculateur de risque, procédez comme suit.

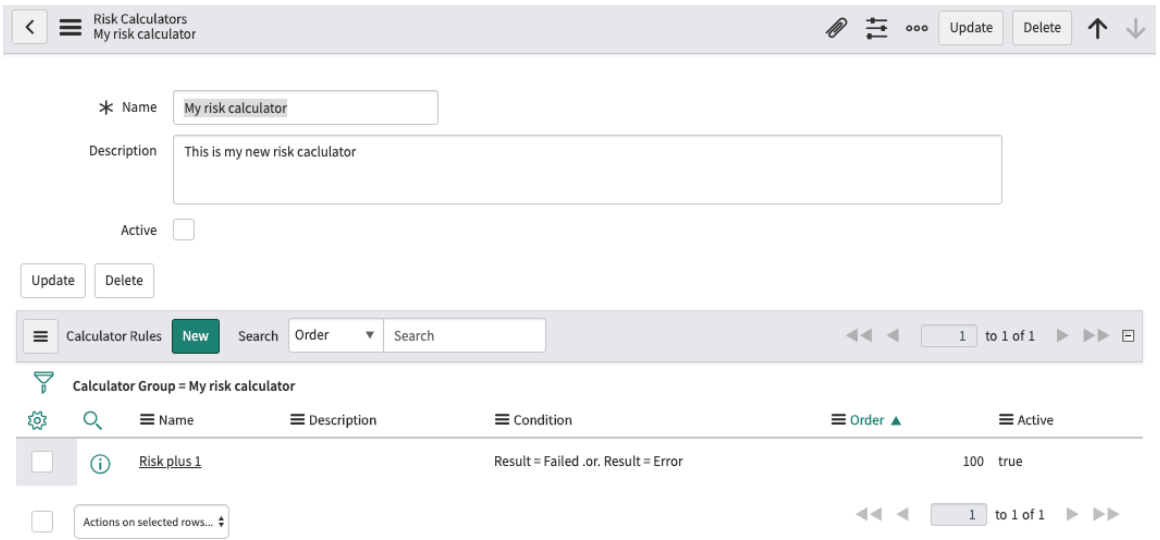
   a. Accédez à la **Tous** > **Configuration Compliance** > **Administration** et sélectionnez **Calculateurs de risque**.

   b. Dans la liste du calculateur de risque, cliquez sur **Nouveau**.

   c. Entrez un nom et une description pour votre nouveau calculateur, puis cliquez sur **Soumettre**.
   Le nouveau calculateur s'affiche dans la liste Calculateur de risque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Dans la liste, cliquez sur le nouveau calculateur pour créer les conditions dans lesquelles le calculateur s'exécute et spécifiez les champs et les valeurs que vous souhaitez afficher sur les enregistrements de résultats des tests et les tâches de rattrapage.

e. Dans l'enregistrement qui s'affiche, cliquez sur **Nouveau**.

f. Renseignez les champs des onglets comme il convient.

Onglet	Description
Quand cette condition est remplie	Utilisez le générateur de conditions pour créer les conditions dans lesquelles le calculateur s'exécute. Par exemple : Le résultat est un échec ou le résultat est une erreur.
Définir ces valeurs	Utilisez le modèle pour sélectionner les champs et les valeurs que vous souhaitez afficher.

g. Cliquez sur **Envoyer**.
L'enregistrement s'affiche avec les nouvelles règles du calculateur et le groupe auquel il appartient.

2. Pour réappliquer un calculateur existant aux résultats des tests ou modifier les règles et les valeurs affichées d'un calculateur de risque existant, procédez comme suit.

a. Dans la liste Calculateurs de risque ou Calculateur de déploiement de risque, sélectionnez le calculateur que vous souhaitez modifier.

b. Pour réappliquer un calculateur de risque à vos données de résultats de test existantes à partir de l'enregistrement, cliquez sur **Réappliquer le calculateur**.
Tous les résultats des tests qui répondent aux conditions du calculateur sont mis à jour.

Remarque : En fonction du nombre de résultats des tests, cette mise à jour peut prendre du temps.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Pour modifier les conditions et les valeurs, cliquez sur le nom du calculateur en bas à gauche de la colonne Nom.
Pour les calculateurs de risque, les onglets Enregistrement et **Définir ces valeurs** sont **affichés**.

d. Remplissez le formulaire comme il vous convient.

Onglet	Description de champ
Quand cette condition est remplie	Utilisez le générateur de conditions de filtre pour créer les conditions dans lesquelles vous souhaitez que le calculateur s'exécute.
Définir ces valeurs	Choisissez-en un pour continuer. ▪ Type de valeur : modèle. Choisissez les champs de la liste et les valeurs correspondantes. ▪ Script : saisissez vos modifications dans l'éditeur. **Remarque :** La modification d'un script nécessite une connaissance approfondie de l'application et de l'application ServiceNow AI PlatformConformité de la configuration .

3. Facultatif : Pour appliquer les nouvelles règles sur demande à vos données de résultats de test existantes, procédez comme suit.

a. Une fois la liste des calculateurs de risque affichée, cliquez sur un calculateur que vous souhaitez appliquer.
L'enregistrement s'affiche.

b. Cliquez sur **Réappliquer le calculateur** pour tester et appliquer vos modifications sur demande à vos résultats d'importation.

4. Affichez vos modifications en fonction des résultats des tests et continuez à modifier vos calculateurs au besoin.

Exemples pour Conformité de la configuration le calcul du score de risque

À partir de la version 13.0 de , vous pouvez personnaliser les critères de la règle de Conformité de la configuration risque par défaut. Utilisez les scores de risque fournis par des fournisseurs tiers comme Qualys et Tenable pour calculer les scores de risque.

Les fournisseurs tiers, comme Qualys et Tenable, fournissent leurs propres scores. Ces scores sont renseignés dans le champ Criticité de la table sn_vulc_test. Utilisez ce champ pour les calculs de score de risque. Pour utiliser ce score afin de calculer le score de risque, procédez comme suit :

Ajouter la criticité de la source comme critère pour une règle de risque

Utilisez les scores basés sur la criticité fournis par des fournisseurs tiers pour calculer les scores de risque.

Avant de commencer
Rôle requis : sn_vulc.admin

Traduction automatique

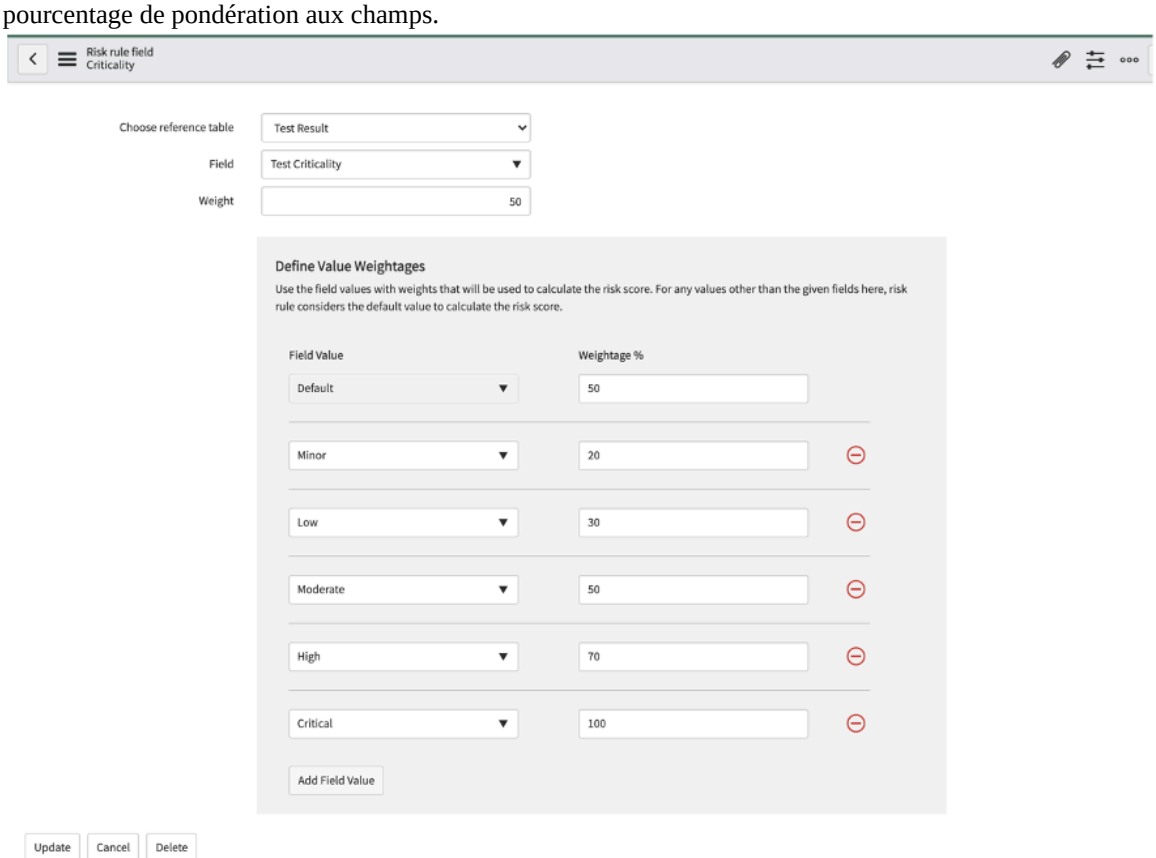
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Les fournisseurs tiers, comme Qualys et Tenable, fournissent leurs propres scores de risque. Ces scores sont renseignés dans le champ Criticité de la table sn_vulc_test. Utilisez ce champ pour le calcul du score de risque et le calcul du score de risque.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Calculateurs de risques**.
2. Accédez au formulaire Règle de risque.
3. Décochez la case **Actif** pour désactiver la règle.
4. Cliquez sur **Ajouter des critères**.
5. Dans la liste **Choisir la table de référence** , sélectionnez **Résultat des tests**.
6. Dans la liste **Champ** , sélectionnez **Test.Criticité**.
7. Dans le champ **Poids** , spécifiez l'importance relative de ce champ.
   La valeur doit être un nombre entier compris entre 0 et 100.
8. Dans la section **Définir les pondérations des valeurs** , ajoutez des valeurs de champ et affectez un pourcentage de pondération aux champs.



9. Cliquez sur **Envoyer**.

Ajouter la criticité opérationnelle comme critère pour une règle de risque

Spécifiez une valeur de criticité pour les services aux entreprises et utilisez la criticité opérationnelle pour calculer les scores de risque.

Avant de commencer

Rôle requis : sn_vulc.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

En supposant que votre organisation dispose de nombreux services aux entreprises et qu'un élément de configuration (CI) est utilisé par les services suivants :

Criticité des services aux entreprises

Service d'entreprise	Criticité
Gestion cloud	1 – Très critique
Commerce électronique	2 – Assez critique
Services aux clients	3 – Peu critique
Déplacements et dépenses	4 – Non critique

Le mappage entre le CI et les services est stocké dans la table Services [cmdb_ci_services]. Lorsqu'un CI ne réussit pas un test de configuration, un résultat de test (TR) est créé. Vous pouvez utiliser la valeur de la criticité opérationnelle des services affectés pour calculer le score de risque pour ce TR. Suivez la procédure pour utiliser la valeur de criticité de ces services pour calculer le score de risque.

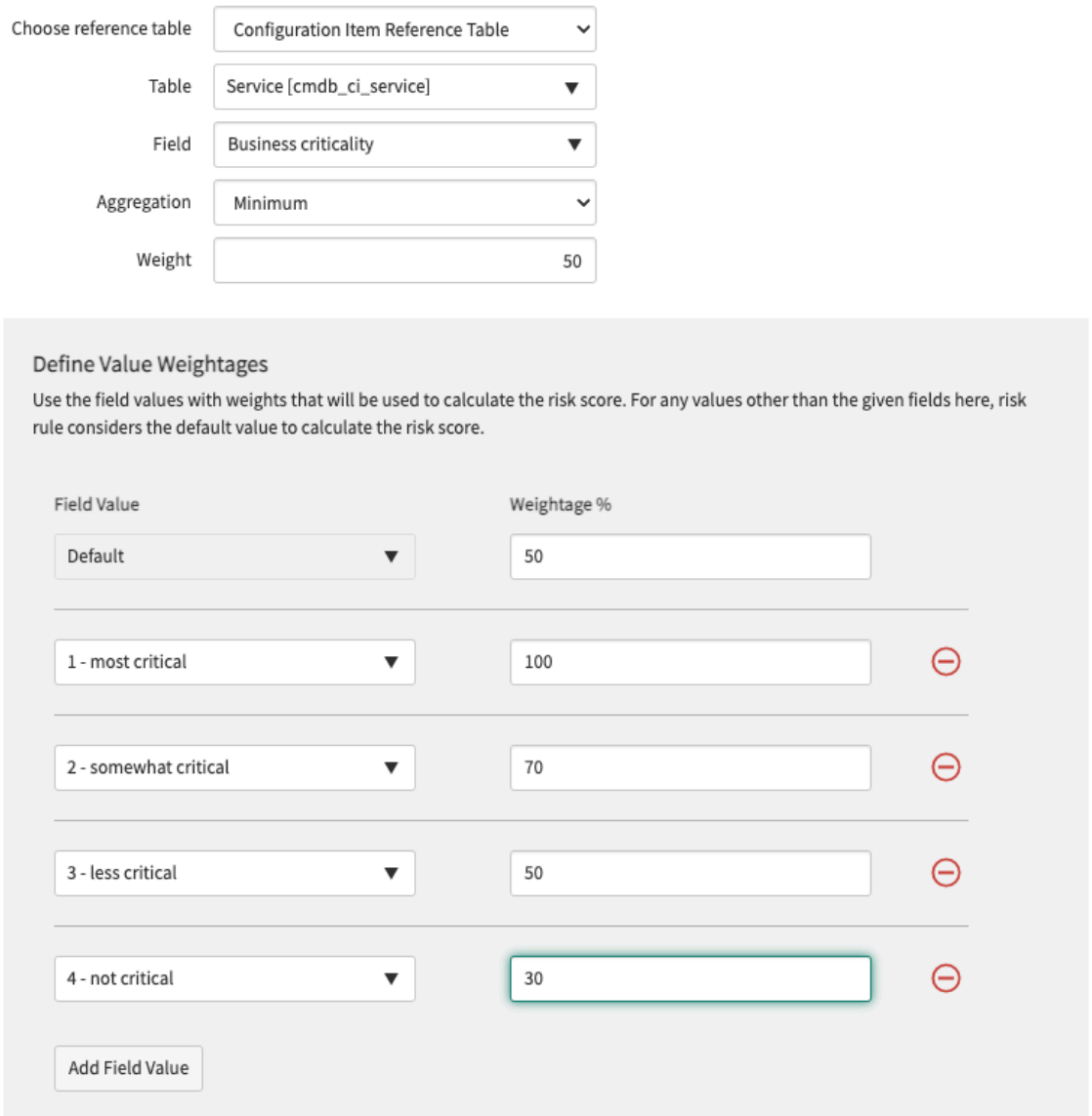
Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Calculateurs de risques**.
2. Accédez au formulaire Règle de risque à partir de la section **Règles du calculateur** .
3. Décochez la case **Actif** pour désactiver la règle.
4. Cliquez sur **Ajouter des critères**.
5. Dans la liste **Choisir la table de référence** , sélectionnez **Table de référence de l'élément de configuration**.
6. Dans la liste **Table**, sélectionnez **Service [cmdb_ci_service].**
7. Dans la liste **Champ** , sélectionnez **Criticité opérationnelle**.
8. Dans le champ **Agrégation** , sélectionnez **Minimum** pour récupérer le service le plus critique pour ce cas d'utilisation (1 : valeur la plus critique) ou **Maximum** pour récupérer le service le moins critique pour ce cas d'utilisation (4 : valeur non critique).
9. Dans le champ **Poids** , spécifiez l'importance relative de ce champ.
   La valeur doit être un nombre entier compris entre 0 et 100.
10. Dans la section **Définir les pondérations des valeurs** , ajoutez des valeurs de champ et affectez des pondérations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pondération de la règle de risque de criticité opérationnelle personnalisée



Traduction automatique

11. Cliquez sur **Envoyer**.

Ajouter un critère conditionnel au calculateur de risque

Utilisez des conditions personnalisées de la règle de risque pour le calcul du score de risque.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

En supposant que votre organisation dispose de plusieurs éléments de configuration (CI), dont seuls quelques-uns peuvent être consultés par un utilisateur externe. Les utilisateurs peuvent ajouter des pondérations de score de risque pour ces CI orientés vers l'extérieur.

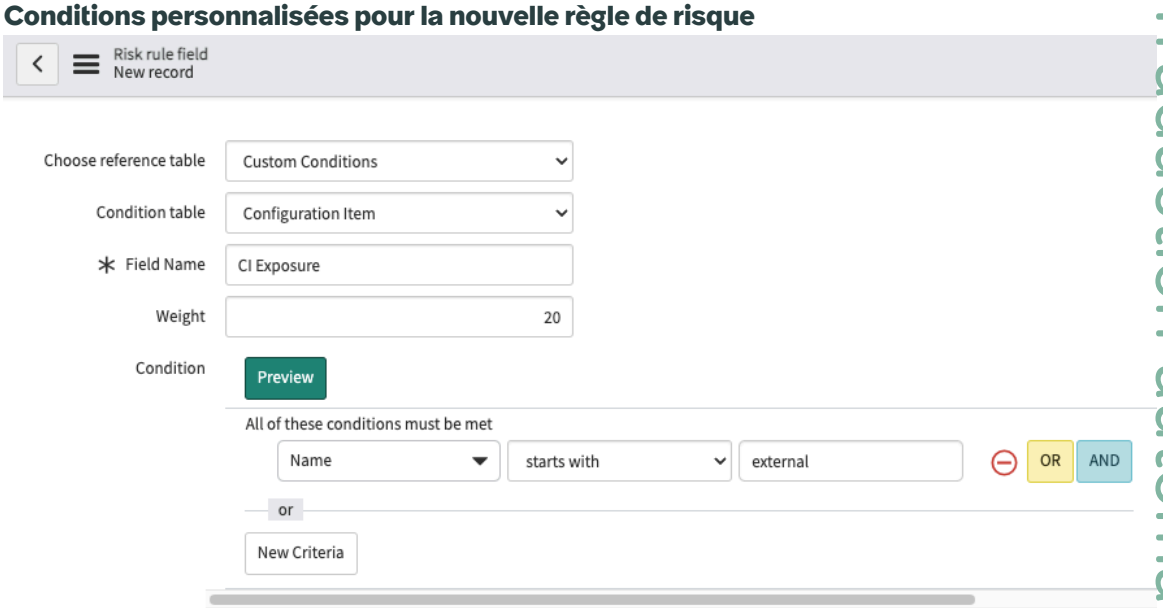
Remarque : Vous pouvez identifier ces CI par leur nom. Les noms commencent par « externe ».

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Calculateurs de risques**.
2. Accédez au formulaire Règle de risque.
3. Décochez la case **Actif** pour désactiver la règle.
4. Cliquez sur **Ajouter des critères**.
5. Dans la liste **Choisir la table de référence** , sélectionnez **Conditions personnalisées**.
6. Dans la liste Table de **condition** , sélectionnez **Élément de configuration**.
7. Dans le champ **Nom du champ** , entrez Exposition CI.
8. Dans le champ **Poids** , spécifiez l'importance relative de ce champ.
   La valeur doit être un nombre entier compris entre 0 et 100.
9. Dans le champ **Condition** , sélectionnez **Nom > commence par**, spécifiez la valeur externe.

Conditions personnalisées pour la nouvelle règle de risque



10. Cliquez sur **Envoyer**.

Information associée

Groupes de calculateurs Configuration Compliance

Exemple de calcul de score de risque pour Conformité de la configuration

Déterminez les calculateurs de score de risque pour générer des scores de risque qui utilisent les données de test et d'actif spécifiques à votre organisation.

Exemple de détermination des scores des calculateurs de règles de risque

L'exemple suivant montre comment les scores des calculateurs de règles de risque sont déterminés. Supposons qu'un calculateur de règle de risque est configuré avec les champs de cette table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déterminer les scores du calculateur de règle de risque

Champ	Pondération	Répartition du poids
Contrôle.Criticité	50	Par défaut : 0 Mineure : 20 Basse : 30 Modéré : 50 Maximum : 70 Critique : 100
Business_Criticality	50	Par défaut : 0 Mineure : 20 Basse : 30 Modéré : 50 Hauteur : 70 Critique : 100

Supposons que les résultats des tests indiqués dans cette table figurent dans le système.

Mappage des résultats des tests

ID	Criticité opérationnelle	Criticité du contrôle
CTR0000001	1 – Très critique	Mineur
CTR0000002	1 – Très critique	Faible
CTR0000003	2 – Assez critique	Mineur
CTR0000004	2 – Assez critique	Modéré
CTR0000005	3 – Peu critique	Faible

Le calcul du score de risque pour le résultat du test est calculé en fonction de la formule suivante :

Score de risque = (W(control.criticality) * FV (control.criticality). + W(business_criticality) * FV(business_criticality)) / 100 où W est le poids et FV est le pourcentage de poids de la valeur de champ.

Le score de risque résultant pour ces résultats de test est décrit dans cette table :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Score du risque basé sur les résultats des tests

ID	Criticité opérationnelle (50 %)	Criticité du contrôle (50 %)	Score de risque résultant
CTR0000001	1 – Très critique (50 % x100)	Mineure (50 % x 20)	60
CTR0000002	1 – Très critique (50 % x100)	Faible (50 % x 30)	65
CTR0000003	2 – Assez critique (50 % x 70)	Mineure (50 % x 30)	45
CTR0000004	2 – Assez critique (50 % x 70)	Modérée (50 % x 50)	60
CTR0000005	3 – Peu critique (50 % x 50)	Faible (50 % x 30)	40

Si le pourcentage de pondération est modifié pour l'une des valeurs de champ, consultez ce tableau pour connaître les résultats :

Résultats pour pourcentage de pondération modifié

Champ	Pondération	Répartition du poids
Contrôle.Criticité	50	Par défaut : 0 Mineure : 20 Basse : 30 Modéré : 60 Hauteur : 70 Critique : 100
Business_Criticality	50	Par défaut : 50 1 – Le plus critique : 100 2 – Assez critique : 70 3 – Peu critique : 20 4 – Non critique : 30

Le score de risque pour les résultats du test après réapplication du calculateur est indiqué dans cette table :

Score du risque pour les TR sur réapplication du calculateur

ID	Criticité opérationnelle (50 %)	Criticité du contrôle (50 %)	Score de risque résultant
CTR0000001	1 – Très critique (50 % x 100)	Mineure (50 % x 20)	60
CTR0000002	1 – Très critique (50 % x 100)	Faible (50 % x 30)	65
CTR0000003	2 – Assez critique (50 % x 70)	Mineure (50 % x 30)	45

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Score du risque pour les TR sur réapplication du calculateur (suite)

ID	Criticité opérationnelle (50 %)	Criticité du contrôle (50 %)	Score de risque résultant
CTR0000004	2 – Assez critique (50 % x 70)	Modérée (50 % x 60) *Valeur révisée	65 *Valeur révisée
CTR0000005	3 – Peu critique (50 % x 20) *Valeur révisée	Faible (50 % x 30)	25 *Valeur révisée

Exemple de calcul de déploiement de risque pour Conformité de la configuration (avant la version 15.0)

L'exemple suivant montre comment déterminer les scores des calculateurs de déploiement des risques.

Pour le calculateur de déploiement de tâche de rattrapage suivant, la formule de calcul du score de risque de tâche de rattrapage est la suivante :

(score de risque maximal/100) * 85 + (facteur * 15).

Le facteur de l'équation précédente est déterminé par le nombre de résultats d'essai, comme indiqué dans le tableau suivant.

Nombre de résultats des tests	Facteur
<10	0,2
10-99	0,4
100-1000	0,6
1001-9999	0,8
> 10000	1

Pour la tâche de rattrapage suivante, TRG0003066, avec trois scores de risque de résultats de test, le score maximal est 90.

Numéro	Score du risque	Tâche de rattrapage	Résultat	Statut
CTR000123	90.0	TRG0003066	Échoué	Ouvert
CTR000124	70	TRG0003066	Échoué	Ouvert
CTR000125	40	TRG0003066	Échoué	Ouvert

Pour la tâche de rattrapage, TRG0003066 :

Le score de risque est de 79, (90/100) * 85 + 0,2 * 15 = Math.floor (76,5 +3) = 79.

Le score de risque historique est nul, car la tâche de rattrapage est toujours « Ouverte ».

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après l'ingestion de données, les résultats des tests sont « Réussi » et la tâche de rattrapage passe à « Fermé », comme indiqué dans la table suivante.

Numéro	Score du risque (avant la version 15.0)	Tâche de rattrapage	Résultat	Statut
CTR000123	0	TRG0003066	Réussi	Fermé
CTR000124	0	TRG0003066	Réussi	Fermé
CTR000125	0	TRG0003066	Réussi	Fermé

L'historique des résultats des tests est affiché dans le tableau suivant.

Numéro	Score du risque	Dernier résultat	Résultat
CTRH000111	90.0	CTR000123	Échoué
CTRH000112	70	CTR000124	Échoué
CTRH000113	40	CTR000125	Échoué

Le score de risque est nul, car il n'y a aucun résultat de test actif dans la tâche de rattrapage.

Pour la tâche de rattrapage, TRG0003066 :

Le score de risque historique est de 79 : (90/100) * 85 + 0,2 * 15 = Math.floor (76,5 +3) = 79.

Exemple de calcul de déploiement de risque pour Conformité de la configuration (v15.0 et versions ultérieures)

L'exemple suivant montre comment déterminer les scores des calculateurs de déploiement des risques.

Pour le calculateur de déploiement de tâche de rattrapage suivant, la formule de calcul du score de risque de tâche de rattrapage est la suivante :

(Score de risque maximal* 80/100) + (Score de risque moyen* 5/100) + (Facteur * 15)

Où les poids sont les suivants :

- Score de risque maximal : 80
- Score de risque moyen : 5
- Facteur : 15

Le poids par défaut du score de risque moyen est de 0. Pour plus d'informations sur le réglage des pondérations, reportez-vous à la section Modifier les calculateurs de déploiement des risques pour Conformité de la configuration.

Le facteur de l'équation précédente est déterminé par le nombre de résultats d'essai, comme indiqué dans le tableau suivant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nombre de résultats des tests	Facteur
<10	0,2
10-99	0,4
100-1000	0,6
1001-9999	0,8
> 10000	1

Pour la tâche de rattrapage suivante, TRG0003066, avec trois scores de risque de résultats de test, le score de risque maximal est de 90 et le score de risque moyen est de 66,67.

Numéro	Score du risque	Tâche de rattrapage	Résultat	Statut
CTR000123	90.0	TRG0003066	Échoué	Ouvert
CTR000124	70	TRG0003066	Échoué	Ouvert
CTR000125	40	TRG0003066	Échoué	Ouvert

Pour la tâche de rattrapage, TRG0003066 :

Le score de risque est de 81, (90* 80/100) + (66,67* 5/100) + (0,2 * 15) = Math.floor (78,3 +3) = 81.

Le score de risque historique est nul, car la tâche de rattrapage est toujours « Ouverte ».

Après l'ingestion de données, les résultats des tests sont « Réussi » et la tâche de rattrapage passe à « Fermé », comme indiqué dans la table suivante. À partir de la version 15.0 de , le score de risque d'un résultat de Conformité de la configuration test réussi est rempli pour déterminer le risque atténué.

Numéro	Score du risque	Tâche de rattrapage	Résultat	Statut
CTR000123	90.0	TRG0003066	Réussi	Fermé
CTR000124	70	TRG0003066	Réussi	Fermé
CTR000125	40	TRG0003066	Réussi	Fermé

L'historique des résultats des tests est affiché dans le tableau suivant.

Numéro	Score du risque	Dernier résultat	Résultat
CTRH000111	90.0	CTR000123	Échoué
CTRH000112	70	CTR000124	Échoué
CTRH000113	40	CTR000125	Échoué

Le score de risque de la tâche de rattrapage est nul, car il n'y a aucun résultat de test actif dans la tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour la tâche de rattrapage, TRG0003066 :

Le score de risque historique est de 81 : (90* 80/100) + (66,67* 5/100) + (0,2 * 15) = Math.floor (78,3 +3) = 81.

Créer ou modifier des Conformité de la configuration règles de tâche de rattrapage

Vous pouvez créer des règles pour regrouper automatiquement les résultats des tests en fonction des conditions de filtre. Ces règles regroupent automatiquement les résultats des tests à mesure qu'ils sont importés. Utilisez le filtre pour limiter les résultats des tests regroupés par cette règle, par exemple en sélectionnant tous les résultats des tests avec des exploits.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Le système de base est fourni avec une règle de tâche de rattrapage, **un groupe d'affectation, un test**, qui regroupe les résultats des tests par groupe d'affectation (pré-rempli à partir des **règles d'affectation**) et le champ **Test** de résultat de test. Cette règle peut être modifiée à l'aide des conditions de filtre et des clés de groupe. Les clés de groupe sont des colonnes dans la table des résultats des tests. Sélectionnez jusqu'à six touches pour indiquer les valeurs à utiliser pour regrouper les résultats des tests.

À partir de la version 14.7 de , la règle de tâche de test de groupe **d'affectation**Conformité de la configuration est désactivée pour les nouvelles implémentations.

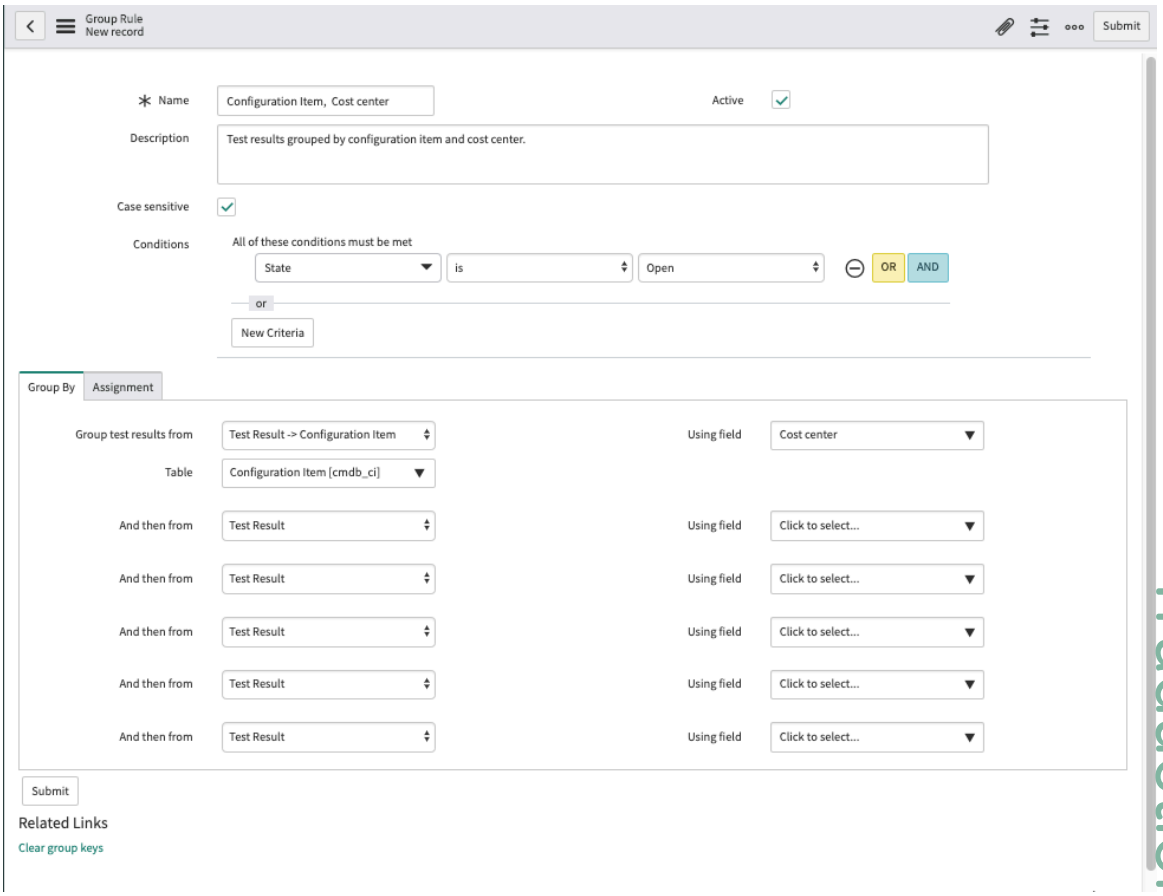
Remarque : Les règles nouvelles ou mises à jour sont automatiquement évaluées lors de l'importation suivante ou manuellement à l'aide du bouton **Réappliquer** du formulaire Règle de tâche de rattrapage.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Règles de la tâche de rattrapage**.
2. Ouvrez le **groupe d'affectation, testez** la règle ou cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. S'il s'agit **d'un nouveau**, renseignez les champs du formulaire comme il convient.

Conformité de la configuration Règle de la tâche de rattrapage

Champ	Description
Nom	Nom de la règle de la tâche de rattrapage.
Actif	Indique si la règle de tâche de rattrapage est active.
Description	Description de texte de cette règle de tâche de rattrapage.
Sensible à la casse	Détermine si la correspondance des règles est sensible à la casse ou non. **Remarque :** La valeur par défaut est insensible à la casse.
Conditions	Conditions à remplir. Par défaut (case **sensible à la casse** désactivée), le texte de recherche que vous saisissez dans le générateur de conditions sur les enregistrements et les formulaires de règles de tâche de rattrapage n'est pas sensible à la casse. Vous pouvez activer les recherches sensibles à la casse sur les enregistrements et les formulaires de groupes.
Grouper par	
Résultats des tests de groupe de	Automatiser la création de groupes basés sur cette règle. Choisissez l'une des options disponibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Résultat de test | Utilisation du champ ○ Résultat des tests > élément de configuration | Tableau | Utilisation du champ Si un champ **Table** étendue est sélectionné, les résultats des tests qui n'utilisent pas la table étendue correspondante sont regroupés dans une tâche de rattrapage distincte.
Affectation	
Affecter des groupes de résultats de tests par	Automatisez l'affectation des groupes créés en fonction de cette règle. Choisissez l'une des options disponibles. ○ Clé du groupe Lorsque cette option est sélectionnée, un champ de valeur de clé apparaît. Les champs disponibles sont répertoriés dans un menu déroulant. ○ Groupe d'utilisateurs Lorsque cette option est sélectionnée, un champ de recherche de groupe d'utilisateurs s'affiche.

4. Cliquez sur **Envoyer**.

Remarque : Le lien connexe **Effacer le groupe par clés** supprime les clés de groupe de l'onglet Grouper par du formulaire.

Spécifier la durée d'une exception demandée pour une tâche de rattrapage

Utilisez les propriétés système pour limiter la durée pendant laquelle une exception est demandée pour une tâche de rattrapage. Le rattrapage de la tâche de rattrapage est différé pour la période spécifiée.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
La propriété `sn_vulc.exception_max_request_days` est utilisée pour spécifier le nombre maximal de jours pendant lesquels une exception pour une tâche de rattrapage peut être demandée. La valeur par défaut est de 365 jours.

Remarque : Vous pouvez utiliser la propriété `sn_vulc.exception_approval_required` pour désactiver le workflow d'approbation d'exception pour la tâche de rattrapage si elle n'est pas nécessaire. Par défaut, cette propriété est activée et sa valeur est `vrai`.

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Toutes les propriétés**.
2. Sur la page Propriétés système, recherchez `sn_vulc.exception_max_request_days`.
3. Cliquez sur le nom de la propriété pour ouvrir l'enregistrement Propriété système.
4. Pour pouvoir modifier cet enregistrement, assurez-vous que est sélectionnée en tant qu'application Conformité de la configuration actuelle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Entrez une **valeur** positive et cliquez sur **Mettre à jour**.
   L'enregistrement est mis à jour et enregistré.

Configurer la gestion des exceptions pour Conformité de la configuration

Limitez la durée d'une exception demandée et ajoutez un questionnaire à l'exception à l'aide du Conformité de la configuration module. Par défaut, une exception est demandée à l'aide du ServiceNow® Réponse aux vulnérabilités module. Vous pouvez également demander une exception à l'aide de l'intégration GRC : Gestion de la politique et de la conformité .

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
Si Réponse aux vulnérabilités cette option est activée, vous pouvez limiter la durée pendant laquelle une exception peut être demandée. De même, si le GRC : Gestion de la politique et de la conformité module est installé, vous pouvez sélectionner GRC : Gestion de la politique et de la conformité sur l'écran de configuration. L'activation de cette option vous permet de demander une exception qui spécifie l'objectif de politique et de contrôle à partir de GRC.

Si vous ajoutez un questionnaire, il est envoyé à la personne qui émet la demande d'exception ou de faux positif. Vous pouvez utiliser le questionnaire par défaut ou en créer un en fonction de vos besoins.

Il est utile que l'approbateur d'exceptions comprenne la raison de la demande d'exception.

Procédure
1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Gestion des exceptions**.
2. Dans le formulaire Configuration de gestion de l'exception, sélectionnez la façon dont vous souhaitez gérer une exception en sélectionnant une option dans la liste Gérer les exceptions à l'aide.
   - Réponse aux vulnérabilités

     Remarque : À partir de la version 22.0 de Réponse aux vulnérabilités, vous pouvez également configurer un questionnaire pour les demandes de faux positif pour l'option Réponse aux vulnérabilités .

   - GRC : Gestion de la politique et de la conformité

     Remarque : Vous devez activer le module d'extension GRC à utiliser GRC : Gestion de la politique et de la conformité pour demander une exception.

   Remarque : La modification de la configuration n'a pas d'impact sur les données existantes.

3. Renseignez les champs du formulaire.

Paramètres pour le formulaire de gestion des exceptions CC

Champ	Description
Durée	Période pour laquelle une exception peut être demandée.
Unité	Unité de temps pour la période spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Activer le questionnaire pour demander une exception	Option permettant d'ajouter un questionnaire à la demande d'exception en cours d'émission.
Questionnaire pour demander une exception	Option permettant d'afficher le questionnaire que vous avez sélectionné pour demander une exception. Le questionnaire d'exceptions s'affiche par défaut.
Activer le questionnaire pour marquer comme faux positif	Option permettant d'ajouter un questionnaire à la demande de faux positif émise.
Questionnaire pour marquer comme faux positif	Option permettant d'afficher le questionnaire que vous avez sélectionné pour le marquer comme faux positif. Le questionnaire pour une demande de faux positif s'affiche par défaut.

4. Sélectionnez **Enregistrer**.

Ajouter un approbateur d'exception pour Conformité de la configuration

Ajoutez des utilisateurs aux groupes d'approbateurs afin de pouvoir demander une exception pour une tâche de rattrapage dans Conformité de la configuration.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Une demande d'exception pour une tâche de rattrapage est approuvée à l'aide du workflow d'approbation à deux niveaux par défaut. L'ajout d'utilisateurs au groupe de premier niveau est obligatoire. Si aucun utilisateur ne se trouve dans le deuxième niveau, la demande est automatiquement approuvée après l'approbation de premier niveau.

Remarque : S'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée.

Remarque : Jusqu'à Conformité de la configuration la version 13.0, s'il n'y a pas d'approbateur de premier niveau, une exception ne peut pas être demandée. Toutefois, à partir de la version 13.0, si vous déployez l'application CC pour la première fois, le concepteur de Conformité de la configuration flux pour la gestion des exceptions est activé par défaut. Si vous utilisez déjà le workflow, vous pouvez effectuer une mise à jour vers Flow Designer. Dans les deux cas, vous ne pouvez pas revenir au workflow.

Procédure

1. Accédez à la **Tous** > **Sécurité de système** > **Utilisateurs et groupes** > **Groupes**.
2. Dans la colonne Nom, recherchez **Exception**, puis cliquez sur **Approbateur d'exception - Niveau 1 CC.**

Remarque : À partir de la Conformité de la configuration version 14.7.5, vous pouvez utiliser les propriétés système fournies dans le système de base pour les approbations d'exception via workflow dans la table Propriétés système [sys_properties]. Ainsi, lorsqu'une demande d'exception est émise via le workflow, elle est envoyée pour approbation aux ID de groupe définis dans la propriété système. Accédez à la **Tous** > **Propriétés système** et sélectionnez `sn_vulc.exception_approver_L1_CC` ou `sn_vulc.exception_approver_L2_CC` pour modifier la valeur de la propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans le formulaire Approbateur d'exceptions de groupe - Niveau 1 CC, accédez à **Membres de groupes** > **Nouveau** (ou **Modifier**).
4. Remplissez les champs du formulaire.

Formulaire d'utilisateur

Champ	Description
ID d'utilisateur	Identificateur unique pour l'utilisateur.
Prénom	Prénom de l'utilisateur.
Nom de famille	Nom de famille de l'utilisateur.
Titre	Fonction de l'utilisateur. Saisissez un titre ou une description de poste, ou sélectionnez-en un dans la liste.
Département	Département de l'utilisateur.
Mot de passe	Mot de passe affecté à l'utilisateur. Ce mot de passe peut être permanent ou temporaire.
Mot de passe à réinitialiser	Option permettant à l'utilisateur de réinitialiser le mot de passe pour garantir la sécurité.
Verrouillé	Option permettant de verrouiller l'utilisateur hors de l'instance et de mettre fin à toutes les sessions actives de l'utilisateur. Le système empêche les utilisateurs ayant le rôle admin de se verrouiller.
Actif	Option pour rendre cet utilisateur actif. Vous seul pouvez voir un utilisateur inactif dans les zones suivantes : ○ Listes d'utilisateurs ○ Liste de sélection sur les champs de référence (icône de loupe) ○ Liste de saisie semi-automatique qui s'affiche lorsque vous tapez dans un champ de référence
Accès au service Web uniquement	Option permettant de désigner cet utilisateur comme utilisateur non interactif.
Utilisateur d'intégration interne	Option permettant de désigner cet utilisateur comme utilisateur d'intégration interne.
E-mail	Adresse e-mail de l'utilisateur.
Langue	Langue préférée de l'utilisateur.
Intégration du calendrier	Calendrier utilisé pour gérer le calendrier de travail. Par exemple, Outlook.
Fuseau horaire	Fuseau horaire de l'emplacement de cet utilisateur.
Format de date	Format préféré de l'utilisateur pour les dates.
Tél. professionnel	Téléphone professionnel de l'utilisateur.
Tél. mobile	Téléphone mobile de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Photo	Photo que vous pouvez télécharger en cliquant sur **Cliquez pour ajouter...**.

5. Cliquez sur **Envoyer**.
6. **Facultatif :** Répétez les étapes 1 à 5 pour créer un approbateur d'exceptions - CC de niveau 2.

> **Remarque :** Lors de la création d'un approbateur de deuxième niveau, sélectionnez **Approbateur d'exception - Niveau 2 CC**

7. **Facultatif :** Si vous sélectionnez **Modifier**, déplacez les utilisateurs de la **collection** vers le panneau **Membres du groupe** , puis cliquez sur **Enregistrer**.
   L'approbateur doit accéder à **Tous** > **Configuration Compliance** > **Mes approbations** et approuver les demandes.

Créer une carte de Conformité de la configuration criticité

Conformité de la configuration Le mappage de criticité fournit une carte de transformation des champs de criticité source tierce en champs reconnaissables dans Conformité de la configuration la gravité.

Avant de commencer

Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Mappage de criticité**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Mappage de champs

Champ	Description
Source	Nom de la source pour le mappage de criticité.
Valeur de la source	Valeur de criticité de la source.
Valeur cible	Valeur cible. Les choix possibles sont les suivants : **Critique** Le problème de configuration associé au contrôle entraîne une interruption pour un ou plusieurs CI critiques pour l'entreprise. **Élevé** Le problème de configuration associé au contrôle constitue une menace, mais n'entraîne pas l'arrêt des ressources réseau critiques. **Modéré** Le problème de configuration associé au contrôle est un risque, mais n'est pas une menace immédiate. **Faible** Le problème de configuration associé au contrôle est une menace de faible niveau et peut être ignoré en faveur des CI plus à risque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Mineur Le problème de configuration associé au contrôle est un risque mineur et peut être ignoré si nécessaire.

4. Cliquez sur **Envoyer**.

Créer des notifications par e-mail

Les administrateurs de vulnérabilité peuvent modifier la notification ou en ajouter de nouvelles, en spécifiant quand envoyer la notification, qui reçoit la notification et quel contenu contient la notification.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez créer des modèles d'e-mail pour différents types de notifications par e-mail. Pour plus d'informations sur la création de modèles d'e-mail, consultez Définir des Réponse aux vulnérabilités modèles d'e-mail.

Procédure
1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Notifications**.
2. Sélectionnez l'enregistrement de notification de la cible de rattrapage ou sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.
   Pour plus d'informations sur les champs de formulaire, consultez Créer une notification par e-mail .
4. Sélectionnez **Afficher l'aperçu** de la notification pour afficher le message.

Résultats
À partir de la version 14.11 de , lorsqu'un destinataire clique sur les liens d'une Conformité de la configuration notification par e-mail, les enregistrements s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités ou Espace de travail de remédiation IT en fonction de son rôle.

- Des liens s'ouvrent dans le Espace de travail du gestionnaire de vulnérabilités pour les utilisateurs ayant le rôle sn_vulc.admin.
- Des liens s'ouvrent Espace de travail de remédiation IT pour les utilisateurs disposant du rôle sn_vulc.remediation_owner.

Si le destinataire ne possède aucun des rôles précédents, les liens d'une notification par e-mail s'ouvrent dans l'interface utilisateur classique.

Configurer les règles d'approbation pour la gestion des exceptions dans Conformité de la configuration

Utilisez le concepteur de flux pour approuver les demandes d'exception pour la gestion des exceptions et les règles d'exception. Si vous déployez Conformité de la configuration pour la première fois, le concepteur de flux est activé par défaut.

Avant de commencer
Rôle requis : sn_vulc.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

La valeur de la propriété *sn_vulc.flow_designer_activation* système est définie sur vrai. Cela signifie que Flow Designer est activé par défaut.

Remarque : Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer. Pour une comparaison détaillée entre le workflow et Flow Designer, reportez-vous à la section Comparaison entre le workflow de gestion des exceptions et le concepteur de flux dans Conformité de la configuration.

Pour utiliser Flow Designer, créez des règles à l'aide du module Règles d'approbation. À l'aide de ce module, vous pouvez configurer des règles d'approbation pour chacun des workflows de gestion des exceptions suivants.

- Règles d'approbation d'exception pour la tâche de rattrapage
- Règle d'approbation des règles d'exception automatique

Remarque : Vous pouvez également définir des conditions contenant plusieurs niveaux d'approbation dans une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant. Pour plus d'informations sur la configuration des niveaux d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions dans Conformité de la configuration.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Règles d'approbation** > **Règles d'approbation d'exception pour la tâche de rattrapage**.
2. Sur la page Règles d'approbation, sélectionnez le groupe pour lequel vous souhaitez définir la règle d'approbation.
3. Remplissez les champs du formulaire.

Formulaire Règle d'approbation

Champ	Description
Nom	Nom de configuration de l'approbation.
Table	Table sur laquelle la règle est appliquée.
Application	La valeur par défaut est Conformité de la configuration.
Type de règle	Spécifie le type de règle. Par exemple, gestion des exceptions ou règle d'exception.
Actif	Activé par défaut, ce qui signifie que la règle d'approbation est utilisée.
Description	Brève description des règles d'approbation.
Expirationde l'approbation (jours)	Date jusqu'à laquelle l'approbateur peut approuver la demande.
Notification de l'approbateur (jours)	Date après laquelle l'approbateur est notifié pour effectuer des actions.

4. Sélectionnez **Mettre à jour**.
   Dans l'onglet Configurations d'approbation, deux niveaux d'approbateurs sont configurés par défaut. Vous pouvez sélectionner une règle pour définir les conditions en fonction de différents cas d'utilisation au sein

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d’une règle. Pour en savoir plus, reportez-vous à Créer des configurations pour une règle d’approbation dans Conformité de la configuration.

Remarque : Dans chaque page de configuration, vous pouvez créer plusieurs niveaux d’approbation. Pour plus d'informations, consultez Créer des niveaux d’approbation pour la gestion des exceptions dans Conformité de la configuration.

Example:
En fonction de différents cas d’utilisation, vous pouvez définir différents processus d’approbation pour les mêmes résultats de test trouvés dans différentes tâches de rattrapage.

Créer des configurations pour une règle d’approbation dans Conformité de la configuration

Définissez les conditions de filtrage des tâches de rattrapage correspondantes pour un niveau d’approbation.

Avant de commencer
Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche
Dans le module Configurations d’approbation, vous pouvez configurer plusieurs niveaux d’approbation pour différentes configurations. Définissez des règles basées sur des conditions, chaque règle contenant plusieurs niveaux d’approbation.

Remarque : Utilisez le module Règles d’approbation pour configurer les règles d’approbation pour les workflows de gestion des exceptions. Pour plus d’informations sur la configuration des règles d’approbation, reportez-vous à la section Créer des niveaux d’approbation pour la gestion des exceptions dans Conformité de la configuration.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Règles d'approbation**.
2. Sélectionnez une règle d’approbation et accédez à l’onglet **Configurations d’approbation** .
3. Sélectionnez une configuration.
4. Remplissez les champs du formulaire.

Formulaire de configuration de l’approbation

Champ	Description
Nom	Nom de configuration de l’approbation.
Règle d'approbation	Contient les détails de la table et du type pour la règle d’approbation.
Ordre	Ordre d’exécution de diverses configurations au sein d’une règle. Par exemple, une configuration avec une entrée de commande de 100 est exécutée avant une configuration avec une entrée de commande de 200.
Actif	Activé par défaut, ce qui signifie que la configuration de l’approbation est utilisée.
Description	Brève description des niveaux de configuration de l’approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Définissez une condition pour les résultats des tests ou les tâches de rattrapage de l'une des façons suivantes :

Champ	Description
Condition	Identifie les résultats des tests ou tâches de rattrapage correspondants.
Condition avancée	Script qui définit la condition pour les résultats des tests ou les tâches de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous cochez la case **Avancé** .

6. Sélectionnez **Mettre à jour**.
   Vous pouvez définir des conditions contenant plusieurs niveaux d'approbation dans une règle. Le concepteur de flux hérite automatiquement des règles créées dans ce module et traite le workflow d'approbation correspondant. Pour plus d'informations sur la configuration des niveaux d'approbation, reportez-vous à la section Créer des niveaux d'approbation pour la gestion des exceptions dans Conformité de la configuration.

Example:
Vous pouvez définir différents chemins d'approbation pour différents types de tâches de rattrapage.

Créer des niveaux d'approbation pour la gestion des exceptions dans Conformité de la configuration

Définissez les niveaux d'utilisateurs et les groupes d'utilisateurs qui vont approuver les demandes d'exception.

Avant de commencer
Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Règles d'approbation**.
2. Sélectionnez une règle d'approbation et accédez à l'onglet **Configurations d'approbation** .
3. Sélectionnez une configuration.
4. Dans la section **Niveaux de l'approbateur** , sélectionnez un niveau d'approbateur.
5. Remplissez les champs du formulaire.

Formulaire Niveau d'approbateur

Champ	Description
Nom	Nom du niveau d'approbation.
Approbation requise	Sélectionnez le nombre d'approbations requises pour le niveau sélectionné : ○ Un approbateur requis ○ Approbation de tous les utilisateurs requise
Actif	Activé par défaut, ce qui signifie que le niveau d'approbation est utilisé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ordre	Ordre d’exécution de diverses configurations au sein d’une règle. Par exemple, une configuration avec une entrée d’ordre de 100 s’exécute avant une configuration avec une entrée d’ordre de 200.
Règle d'approbation	Contient les détails de la table et du type pour la règle d’approbation. Ce champ est en lecture seule.
Configuration de l'approbation	Contient les configurations d’approbation. Ce champ est en lecture seule.
Affecter à l'aide de	Sélectionnez une option dans : ○ Utilisateur et groupe d'utilisateurs ○ Champ de la table des approbations ○ Script
Groupes	Groupe au niveau de l’approbateur composé de plusieurs utilisateurs. L’utilisateur doit disposer de l’un des rôles suivants pour la gestion des exceptions et les règles d’exception : ○ sn_vulc.exception_approver ○ sn_vulc.lire ○ sn_vulc.read_auto_exception_rule
Utilisateurs	Modifiez les utilisateurs répertoriés dans les groupes.

6. Pour enregistrer les changements, sélectionnez **Mettre à jour**.

Remarque : Avant la version 13.0, le processus de workflow était fonctionnel s’il n’y avait que des utilisateurs au niveau d’exception 1. Cependant, à partir de la version 13.0, il doit y avoir au moins un utilisateur dans chaque niveau.

Avant la version 13.0, dans le workflow, s’il n’y avait pas d’utilisateur dans le deuxième niveau, la tâche de rattrapage était reportée. Toutefois, à partir de la version 13.0, s’il n’y a pas d’utilisateur dans le deuxième niveau, la demande d’approbation est automatiquement rejetée.

Example:
Il peut y avoir différents niveaux d’approbation pour les tâches de rattrapage pour les serveurs Linux et Windows.

Comparaison entre le workflow de gestion des exceptions et le concepteur de flux dans Conformité de la configuration

Conformité de la configuration À partir de (CC) v13.0, si vous déployez CC pour la première fois, le concepteur de flux pour l’approbation des demandes d’exception dans la gestion des exceptions est activé par défaut. Si vous êtes un utilisateur CC existant, l’option par défaut est workflow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparaison entre Workflow et Flow Designer

Considérations	Workflow	Flow Designer
Version	Avant la version 13.0 de CC.	À partir de la v13.0 de CC.
Option par défaut	Option par défaut si vous êtes un utilisateur CC existant.	Option par défaut pour les nouveaux utilisateurs CC à partir de la version 13.0.
Définition du processus d'approbation	La gestion des exceptions inclut des demandes d'exception ainsi que des règles d'exception.	Inclut la définition de différents niveaux et l'ajout d'approbateurs différents pour différents cas d'utilisation. Plus facile à mettre en œuvre que le workflow. La gestion des exceptions inclut des demandes d'exception ainsi que des règles d'exception.
Mise à niveau vers Flow Designer	Vous pouvez effectuer une mise à niveau vers Flow Designer à partir du workflow. Toutefois, les demandes existantes ne peuvent être approuvées qu'à l'aide du workflow.	Flow Designer est activé par défaut.
Propriété système `sn_vulc.flow_designer_activation`	Si vous utilisiez le workflow pour la gestion des exceptions avant la version 13.0, la propriété système est définie sur false. Pour activer Flow Designer, définissez cette propriété sur vrai. **Remarque :** Vous ne pouvez pas revenir à l'utilisation du workflow après avoir activé Flow Designer.	Si vous utilisez CC pour la première fois pour la version 13.0 ou ultérieure, la valeur de la propriété système est définie sur vrai par défaut.
Module Règles d'approbation	Une fois la propriété système définie sur true, la tâche planifiée **Activer les règles d'approbation de module** s'exécute dans les 24 heures. Cette tâche planifiée active le module **Règles d'approbation** . Pour activer ce module instantanément, exécutez cette tâche manuellement.	Si vous avez déployé CC pour la première fois à partir de CC v13.0, ce module est disponible par défaut.
Niveaux d'approbation	Permet de définir uniquement deux niveaux d'approbateurs.	Fournit plusieurs options telles que la définition d'un nombre quelconque de configurations, de niveaux d'approbateurs et l'ajout dynamique d'approbateurs pour chaque règle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Conformité de la configuration

Les intégrations tierces importent les résultats d'évaluation de la configuration, les politiques, les tests, les technologies, les sources de référence, les résultats des tests, ainsi que d'autres données de vulnérabilité dans l'application Conformité de la configuration .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

L'application Conformité de la configuration prend en charge les intégrations tierces suivantes :

- À partir de la version 14.11, corrigez les failles de sécurité dans vos actifs d'entreprise identifiées par l'application Contrôle de la posture de sécurité en publiant les résultats sous forme de résultats de test dans l'application Conformité de la configuration . L'application Contrôle de la posture de sécurité et ses applications prises en charge sont disponibles avec des abonnements distincts de .ServiceNow® Store Consultez Contrôle de la posture de sécurité pour plus d'informations.
- Microsoft Defender for Cloud Integration pour Opérations de sécurité
- Intégration des vulnérabilités dans le cloud Palo Alto Prisma
- Qualys intégration avec Conformité de la configuration
- Produit Tenable.io de l'intégration de vulnérabilité Tenable

Remarques supplémentaires sur les intégrations

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 14.8.5 de , des horodatages (intervalles de Conformité de la configuration mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Microsoft Defender for Cloud Integration pour Opérations de sécurité

Le Microsoft Defender for Cloud Integration produit est un système de gestion de la sécurité de l'infrastructure qui améliore la posture de sécurité de vos environnements cloud.

Microsoft Defender for Cloud Integration pour Opérations de sécurité s'intègre à l'application Conformité de la configuration pour mapper les tests aux éléments de configuration (CI) afin de créer des résultats de test. Il découvre en permanence les nouvelles ressources cloud déployées sur les charges de travail et détermine si elles sont configurées conformément aux normes de sécurité telles que le Center for Internet Security (CIS).

À partir de la version 2.2, Microsoft Azure Security Center est renommé Microsoft Defender for Cloud Integration en .Opérations de sécurité

Versions disponibles

Application	Version
Microsoft Defender for Cloud Integration pour Opérations de sécurité	2.3
Conformité de la configuration	14.3
Security Support Common	13.2
Réponse aux vulnérabilités	16.2

Déploiements multiples de la Microsoft Defender pour le cloud plateforme

Si vous avez plusieurs déploiements de l'application de plateforme Microsoft Defender pour le cloud , vous pouvez ajouter une intégration pour chaque déploiement. Les ressources qui sont identifiées par plusieurs déploiements tiers, sont consolidées et rapprochées avec votre Base de données de gestion des configurations (CMDB). Cette consolidation a lieu même lorsque les processus d'analyse se chevauchent entre les multiples déploiements.

ServiceNow Microsoft Defender pour le cloud Intégrations

Le Microsoft Defender for Cloud Integration pour Opérations de sécurité enrichit les données de conformité sur votre instance en récupérant les données de Microsoft Defender pour le cloud. Une série de travaux planifiés appelle automatiquement les intégrations. Vous pouvez également exécuter manuellement ces travaux planifiés. Les travaux planifiés simplifient le cycle de vie de rattrapage des résultats des tests en maintenant l'instance synchronisée avec Microsoft Defender pour le cloud.

Il existe un utilisateur run-as configuré pour chaque enregistrement d'intégration, avec la valeur par défaut **VR. système**. Cette valeur doit rester la même.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous ne définissez pas d'utilisateur d'exécution valide, des pièces jointes de récupération de données en double ou multiples sont créées pour les enregistrements de source de données. Le nombre de pièces jointes augmente à chaque exécution de l'intégration. Cela augmente le temps de traitement, ce qui entraîne des résultats de transformation incohérents.

Microsoft Defender pour le cloud Les tâches d'intégration de plateforme impliquent les rôles suivants.

- sn_vul_asc.configure_integration : capacité à lire, écrire et supprimer des enregistrements.
- sn_vul_asc.read_integration : capacité à lire des enregistrements.

Affichage des Microsoft Defender pour le cloud intégrations

Affichez les intégrations en accédant à **Tous** > **Intégration de Microsoft Defender pour le cloud** > **Intégrations**.

Les intégrations suivantes sont incluses dans le système de base.

Intégration	Description
Intégration de définition de politique	Récupère les politiques et crée des entrées de politique dans votre instance.
Intégration des métadonnées d'évaluation	Récupère les métadonnées d'évaluation et crée des tests dans votre instance.
Intégration des normes de conformité et des contrôles	Récupère les normes et les contrôles, et crée la source d'autorisation et le contenu des documents de référence. Il les relie ensuite aux tests créés.
Intégration de l'évaluation	Récupère les évaluations et les traite dans votre instance. Le résultat de cette intégration est des résultats de tests.

Créer des CI à l'aide du moteur Identification et réconciliation

Utilisez le moteur Identification et rapprochement (IRE) pour créer des CI, lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte importé à partir d'un scanner tiers.

Si un CI ne correspond pas dans la CMDB, un CI est créé dans la `cmdb_ci_cmp_resource` classe. Par la suite, lorsqu'une découverte détecte le même CI, elle l'enrichit ou en crée un autre.

Remarque : Le rapprochement automatique ne se produit pas pour les ressources cloud.

Installer et configurer Microsoft Defender for Cloud Integration pour Opérations de sécurité

Installez et configurez le Microsoft Defender for Cloud Integration pour Opérations de sécurité afin de Microsoft Defender pour le cloud pouvoir utiliser les données importées de pour classer par ordre de priorité et corriger toute mauvaise configuration sur vos actifs.

Avant de commencer

Créez une nouvelle inscription d'application sur Azure Active Directory pour le Microsoft Defender for Cloud Integration. Pour plus d'informations sur l'enregistrement d'une nouvelle application sur Azure Active Directory, consultez le site de documentation produit Microsoft . Pour plus d'informations sur les rôles Azure, consultez Rôles Azure .

Rôle requis : sn_vulc.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Modules d'extension**.
2. Dans la barre de recherche, recherchez Microsoft Defender pour Cloud Integration pour Security Operations.
3. Sélectionnez **Installer**.

   Toutes les dépendances qui seront installées s'affichent.
4. Accédez à la **Tous** > **Intégration de Microsoft Defender pour le cloud** > **Administration** > **Configuration** > **Configuration de Microsoft Defender pour le cloud**.
5. Remplissez les champs du formulaire.

Microsoft Defender pour le cloud Formulaire de configuration

Champ	Description
URL D'API	URL de ressource de l'instance. Exemple : https://management.azure.com (cloud public Azure)
ID de locataire	Identité du locataire de votre organisation.
Instance d'intégration	Instance par défaut. Vous pouvez également créer une instance pour apporter les données à partir de plusieurs locataires ou abonnements Microsoft Defender .
ID client	Identité du client générée après l'enregistrement de l'application Microsoft Defender for Cloud Integration .
Secret client	Secret client généré après l'enregistrement de l'application Microsoft Defender for Cloud Integration .
Importer les conclusions à partir de	Ressources et évaluations qui correspondent aux ID de groupe d'administration et aux ID d'abonnement sélectionnés à récupérer.
ID des groupes de gestion	Ressources et évaluations qui correspondent aux ID des groupes d'administration à récupérer. **Remarque :** Ce champ s'affiche uniquement lorsque vous sélectionnez **des groupes d'administration spécifiques** dans le champ **Importer les conclusions depuis** .
ID d'abonnements	Numéros d'identification des abonnements pour lesquels les ressources et les évaluations doivent être récupérées. **Remarque :** Ce champ s'affiche uniquement lorsque vous sélectionnez **Abonnements spécifiques** dans le champ **Importer les conclusions depuis** .
État de validation	Indique si les informations d'identification et l'ID d'abonnement fournis sont valides.

6. Configurez ou exécutez les intégrations en sélectionnant **Enregistrer et tester**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conformité de la configuration Données importées pour Microsoft Defender for Cloud Integration

Conformité de la configuration Importe les politiques, les tests, les sources de référence et les résultats des tests à partir d'intégrations tierces et les stocke dans des modules pour consultation.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Groupes de test

Un groupe de tests de configuration constitue un groupe de tests. Les groupes de tests sont liés à des documents et des enregistrements de tests faisant autorité, et ils peuvent être modifiés pour répondre aux besoins de votre organisation. Un test de configuration peut appartenir à plusieurs groupes de tests.

Si l'est Microsoft Defender for Cloud Integration installé, les groupes de tests sont récupérés et renseignés par la tâche planifiée, **Intégration des définitions de politiques**. Vous pouvez afficher la tâche planifiée en accédant à **Tous** > **Intégration de Microsoft Defender pour le cloud** > **Administration** > **Intégrations** > **Intégration de définitions de politiques**.

Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez d'abord **l'intégration des définitions de politique** .

Tests

Les tests sont des bibliothèques d'enregistrements de données qui organisent les analyses des ressources informatiques. Les tests de configuration définissent la manière dont les actifs doivent être gouvernés.

Un Conformité de la configuration test est le mécanisme utilisé par les applications d'intégration tierces pour regrouper les actifs par type de résultats des tests.

Si l'est Microsoft Defender for Cloud Integration installé, la tâche planifiée, **Intégration des métadonnées d'évaluation**, récupère les tests. Vous pouvez afficher la tâche planifiée en accédant à **Intégration** > **Intégrations principales** > **Intégration des métadonnées d'évaluation**.

Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez **l'intégration des métadonnées d'évaluation** après l'intégration des **définitions de politiques**.

À partir de la version 15.0 de , le groupe de Conformité de la configuration tests auquel un test appartient est renseigné dans la colonne **Groupes de tests** de la liste Tests.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sources d'autorité

Conformité de la configuration Utilise des sources et des citations faisant autorité lors de la génération d'alertes de vulnérabilité pour les tests. Les sources faisant autorité correspondent généralement à des sections de normes industrielles publiées, telles que **ISO 27001** et **PCI DSS 3.2.1**.

Ces documents sources contiennent des références à des informations sur des problèmes de configuration logiciels et matériels connus provenant d'experts dans le domaine de la sécurité informatique. Ils définissent les exigences en matière de politiques et de procédures de sécurité.

Si l'est Microsoft Defender for Cloud Integration installé, la tâche planifiée, **Normes et contrôles de conformité**, récupère les sources et les citations faisant autorité. Vous pouvez afficher cette tâche planifiée en accédant à **Tous** > **Intégration de Microsoft Defender pour le cloud** > **Intégrations** > **Intégration des normes de conformité et des contrôles**.

Remarque : Si vous choisissez d'exécuter l'intégration manuellement, exécutez **l'intégration des normes et contrôles de conformité** après **l'intégration des métadonnées d'évaluation**.

Ressources

L'intégration de l'évaluation fournit des informations essentielles telles que les balises de ressource et les attributs dans le cloud. Ces informations sont affichées dans le formulaire Élément détecté. #Il est principalement utilisé pour le filtrage dans les Conformité de la configuration règles de tâche d'affectation et de rattrapage.

- Balises de ressource : toutes les balises de ressource dans le cloud sont importées en tant que balises hôtes dans le cadre de **l'intégration de l'évaluation**. Les balises dans le cloud de tout type de ressource dans le cloud sont stockées ici, que la ressource soit un hôte ou non.
  - Le stockage des balises n'est pas sensible à la casse. Si une balise Tokyo est créée, une balise **TOKYO** ne peut pas être stockée dans la table des balises d'hôte. **Tokyo** et **TOKYO** sont considérées comme le même tag hôte. Quelle que soit la balise importée en premier, elle gagne.
  - L'utilisation de balises d'hôte comme clé de groupe dans une règle de groupe peut avoir des résultats inattendus. Les balises d'hôte sont destinées à être utilisées uniquement dans le générateur de conditions.
- Attributs dans le cloud pour les actifs : Voici les attributs dans le cloud que les intégrations récupèrent :Microsoft Defender pour le cloud
  - Compte dans le cloud
  - Région du cloud
  - Type de ressource dans le cloud
  - Fournisseur de services dans le cloud

Résultats des tests

Conformité de la configuration ne calcule pas les résultats des tests, mais les importe dans le cadre d'une intégration tierce. Une fois visibles dans , ils sont corrigés à Conformité de la configuration l'aide de **tâches de rattrapage**.

Si l'intégration Microsoft Defender pour le cloud est installée, la tâche planifiée, **Assessment Integration**, récupère les résultats des tests. Vous pouvez afficher cette tâche planifiée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

en accédant à **Tous** > **Intégration de Microsoft Defender pour le cloud** > **Intégrations** > **Intégration de l'évaluation**.

L'importation d'intégration d'évaluation est la seule intégration qui utilise le paramètre dans l'onglet **Détails de l'intégration**`Start Time`. Toutes les autres Conformité de la configuration importations apportent toutes les données disponibles, quel que soit le `Start Time`.

Lorsque l'importation de **l'intégration de l'évaluation** est terminée, un événement est lancé pour déclencher les calculs de fin d'importation.

L'intégration de l'évaluation extrait les évaluations de données uniquement en cas de changement d'état par rapport à la dernière exécution réussie de l'intégration pour le dernier jour par défaut. Donc, si l'évaluation échoue continuellement au cours des derniers jours, l'intégration ne récupérera pas l'évaluation, car il n'y a aucun changement d'état pour l'évaluation. Pour maintenir les résultats des tests à jour avec les évaluations Defender, une nouvelle **intégration d'évaluation complète** est ajoutée et extrait les données des sept derniers jours. Il s'exécute chaque semaine et extrait tous les résultats des tests, qui ne sont pas réussis.

Règles de recherche de CI pour identifier les CI à partir des Microsoft Defender pour le cloud intégrations

Lorsque les données sont importées à partir d'une intégration tierce, Conformité de la configuration utilise automatiquement les données de ressource pour rechercher des correspondances dans le , à l'aide des règles de Base de données de gestion des configurations (CMDB) recherche de CI. Ces règles sont utilisées pour identifier les éléments de configuration (CI) et les ajouter à l'enregistrement des résultats des tests pour faciliter le rattrapage. Les règles de recherche de CI du système de base sont disponibles pour l'ID de ressource, le nom et la catégorie S3. Pour plus d'informations sur les règles de recherche de CI, consultez Règles de verrouillage de CI pour Microsoft Defender pour Cloud Integration pour Security Operations.

Présentation de Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Prisma Cloud est une solution de sécurité d'infrastructure cloud basée sur des API. Il se connecte à votre environnement cloud et surveille les ressources déployées sur les environnements de cloud public, tels que Amazon Web Services (AWS), Microsoft Azure, etc. Vous bénéficiez d'une visibilité et d'un contrôle complets sur les risques au sein de votre infrastructure de cloud public.

L'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud facilite l'ingestion des politiques et des alertes à partir de Prisma Cloud, respectivement en tant que tests et résultats de tests, dans l'application Conformité de la configuration . Avec la configuration correcte, les résultats des tests peuvent être gérés de manière transparente en affectant des scores de risque appropriés, puis en les regroupant et en les affectant aux utilisateurs et groupes pertinents.

Versions disponibles

Le tableau répertorie les applications dont elles dépendent, ainsi que Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud la version de l'application.

Application	Version
Intégration de Prisma Cloud pour Security Operations	2.3

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application	Version
Conformité de la configuration	14.7
Security Support Common	13.5
Réponse aux vulnérabilités	18.0

ServiceNow Intégrations dans le cloud Prisma

L'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud permet d'importer les données Prisma dans votre ServiceNow instance afin d'enrichir votre instance pour une meilleure gestion. Une série de travaux planifiés appelle automatiquement les intégrations. Vous pouvez également exécuter manuellement ces travaux planifiés. Les travaux planifiés simplifient le cycle de vie de rattrapage des résultats des tests en maintenant l'instance à jour en récupérant périodiquement les données de Prisma Cloud.

Les tâches d'intégration de Prisma Cloud impliquent les rôles suivants.

- sn_vul_prismacloud.configure_integration : capacité à lire, écrire et supprimer des enregistrements.
- sn_vul_prismacloud.read_integration : capacité à lire des enregistrements.

Affichage des intégrations

Vous pouvez afficher les intégrations qui font partie de Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud **Intégration dans le cloud Prisma** > **Intégrations**.

Les intégrations suivantes sont disponibles dans le système de base.

Séquence d'exécution	Planifier	Intégration	Description
1	Hebdomadaire	Intégration de la politique Prisma	• Récupère les politiques du cloud Prisma et crée des entrées de test dans votre instance. • Il ne fournit pas de soutien supplémentaire. Si vous exécutez l'intégration au cours des 10 derniers jours, elle affiche également le résultat des exécutions d'intégration précédentes.
2	Quotidien	Intégration d'alertes Prisma	• Récupère les alertes du cloud Prisma et crée des entrées de résultats des tests dans votre instance. • Fournit une prise en charge incrémentielle. L'intégration s'exécute tous les jours après l'heure de la dernière exécution de l'intégration.

Préparation de l'installation du Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Préparez l'installation de en effectuant des Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud tâches de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Pour intégrer Vulnerability Response à Palo Alto Prisma Cloud, vous devez disposer d'un groupe d'autorisations dans Prisma qui fournit un accès en lecture seule aux données de politique et d'alertes. Vous trouverez plus d'informations sur les groupes d'autorisations dans Rôles d'administrateur cloud Prisma .

Pour plus d'informations sur les rôles attribués aux différents groupes d'autorisations, consultez la page Autorisations de l'administrateur du cloud Prisma .

De plus, des clés d'accès doivent être créées pour permettre la lecture des alertes. Pour plus d'informations sur la création de clés d'accès, consultez Créer et gérer des clés d'accès .

Pour installer et configurer le Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud, utilisez la liste de vérification suivante. Avant d'installer l'application, vérifiez que les éléments énumérés sont terminés.

Liste de vérification de la préparation de l'intégration

Tâche	Description
☐	Vérifiez que vous disposez des ensembles d'informations suivants : • URL de base de l'API • ID de clé d'accès • Clé secrète • Nom d'utilisateur et mot de passe pour accéder au cloud Prisma. Ces informations d'identification sont utilisées pour se connecter à l'instance Prisma Cloud à partir de l'instance ServiceNow AI Platform® . L'ID de clé d'accès et la clé secrète doivent être générés à partir du portail cloud Prisma après l'inscription.
☐	Si elle n'est pas déjà installée et activée, installez l'application Réponse aux vulnérabilités avant de l'installer Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud . Pour plus d'informations sur l'installation et l'activation de l'application, reportez-vous à la Réponse aux vulnérabilités section Installer Réponse aux vulnérabilités. Cette intégration nécessite la version 15.2.0 ou Réponse aux vulnérabilités ultérieure.
☐	Si vous n'avez pas encore l'application sur votre instance, obtenez les autorisations et téléchargez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud sur votre ServiceNow AI Platform® instance. Consultez .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification de la préparation de l'intégration (suite)

Tâche	Description
☐	Assurez-vous d'avoir installé les modules d'extension suivants pour une exécution fluide de l'intégration : • Réponse aux vulnérabilités • Conformité de la configuration • Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud Les modules d'extension suivants sont facultatifs mais peuvent être utiles : • Mise en service et gouvernance du cloud • Schémas de découverte et de mappage des services
☐	Estimez le nombre de résultats des tests que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre de résultats de test que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance ou si vous avez besoin d'aide, contactez ServiceNow l'assistance technique.
☐	Vérifiez qu'un administrateur est chargé de gérer les intégrations et de corriger les résultats des tests : L'administrateur installe l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud . S'il n'est pas affecté, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles.

Vous êtes prêt à Installer et configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud.

Installer et configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Installez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud pour utiliser les données importées à partir du cloud Prisma. Utilisez ces données pour classer par ordre de priorité et corriger les erreurs de configuration sur vos actifs.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Définition du système** > **Modules d'extension**.
2. Dans la barre de recherche, recherchez Vulnerability Response Integration with Palo Alto Prisma Cloud.
3. Cliquez sur **Installer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Toutes les dépendances qui seront installées s'affichent.

4. Accédez à la **Tous** > **Intégration dans le cloud Prisma** > **Administration** > **Configuration** > **Configuration du cloud Prisma**.
5. Remplissez les champs du formulaire.

Champ	Description
Instance d'intégration	Nom de la nouvelle instance d'intégration. Vous pouvez créer une instance ou cliquer sur l'icône de recherche pour sélectionner une instance existante.
URL D'API	URL à intégrer au cloud Prisma.
ID de clé d'accès	Clé unique pour authentifier la demande d'accès au cloud Prisma. **Remarque :** Vous devez générer la clé après vous être connecté au portail cloud Prisma.
Clé secrète	Clé privée pour authentifier la demande d'accès au cloud Prisma. **Remarque :** Vous devez générer la clé secrète après vous être connecté au portail cloud Prisma.

6. Cliquez sur **Enregistrer et tester**.

Que faire ensuite
Une fois l'installation terminée, accédez à **Intégration dans le cloud Prisma** > **Configuration** pour poursuivre la configuration.

Configurer l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Configurez l'application Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud . Utilisez les données importées de Prisma Cloud pour classer par ordre de priorité et corriger les erreurs de configuration sur vos actifs.

Avant de commencer
Rôle requis : admin

Procédure
1. Accédez à la **Intégration dans le cloud Prisma** > **Configuration**.
2. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration du cloud Prisma

Champ	Description
Instance d'intégration	Nom de la nouvelle instance d’intégration. Vous pouvez créer une instance ou cliquer sur l’icône de recherche pour sélectionner une instance existante.
URL D'API	URL à intégrer à Prisma Cloud.
ID de clé d'accès	Une clé unique pour authentifier la demande d’accès au cloud Prisma. Vous devez générer la clé après vous être connecté au portail cloud Prisma.
Clé secrète	Une clé privée pour authentifier la demande d’accès au cloud Prisma. Vous devez générer la clé secrète après vous être connecté au portail cloud Prisma.

3. Cliquez sur **Enregistrer et tester**.

Que faire ensuite

Une fois la configuration terminée, accédez à **Intégration dans le cloud Prisma** > **Intégrations** pour vérifier que l’intégration s’exécute correctement.

Vérifier l’état de l’exécution de l’importation Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud

Utilisez l’état de l’exécution Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud de l’importation pour vérifier la réussite de vos exécutions d’intégration et identifier les problèmes.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Au cours de l’exécution de l’intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d’attente d’importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d’une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d’expiration de l’intégration. L’intégration continue de traiter les données malgré l’erreur de délai d’expiration. Pour éviter cette mauvaise communication, à partir de la version 14.8.5 de , des horodatages (intervalles de Conformité de la configuration mise à jour) sont envoyés périodiquement pour indiquer si la file d’attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d’attente d’importation est mis à jour en fonction du nombre d’enregistrements créés ou mis à jour par la file d’attente d’importation. Si une entrée de file d’attente d’importation dépasse la limite d’une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s’il date également de plus d’une heure. Si c’est le cas, cela indique que l’entrée de file d’attente d’importation est bloquée et qu’elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Intégration dans le cloud Prisma** > **Intégrations**.
2. Cliquez sur **Intégration des politiques Prisma**.
3. Cliquez sur **Exécuter maintenant**.
   Lorsque cette intégration est exécutée, les tables suivantes sont renseignées dans cet ordre :
   a. sn_vulc_test.list (tests de configuration)
   b. sn_vulc_auth_src (source de référence)
   c. sn_vulc_citation (contenu des documents de référence)
4. Sous l'onglet **Éléments** , affichez le nombre de nouveaux tests créés, mis à jour et ignorés en cliquant sur l'exécution de l'intégration de vulnérabilité.

   Remarque : Les politiques sont définies dans Prisma Cloud pour l'instance de cloud sélectionnée. L'instance est analysée en fonction des politiques définies.

5. Cliquez sur **Intégration des alertes Prisma**.
6. Cliquez sur **Exécuter maintenant**.
   Les tables suivantes sont renseignées en fonction de l'intégration :
   - Résultats des tests
   - Éléments détectés : si les éléments de configuration ne sont pas disponibles dans le système, ils sont créés. La classe est toujours Ressource cloud. Sur la page Élément détecté, trois nouveaux champs sont créés : **Type de ressource dans le cloud**, **Fournisseur de services dans le cloud** et **Catégorie d'actif**.

     Sous l'onglet **Éléments** , cliquez sur l'exécution de l'intégration de vulnérabilité pour afficher le nombre de nouveaux résultats de tests importés, mis à jour et ignorés. L'onglet **Éléments de configuration** est également renseigné en fonction du nombre de résultats des tests créés.

Mappage de données

Les données de Prisma Cloud sont importées dans le Conformité de la configuration module de l'instance ServiceNow .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Les données de Prisma Cloud sont importées avec un nom différent, comme Conformité de la configuration indiqué dans le tableau.

Mappage des données du cloud Prisma dans Configuration Compliance

Prisma Cloud	Configuration Compliance
Politique	Test
Alerte	Résultat de test
Norme de conformité	Source de référence
Sections	Citation
Actif	Élément de découverte/Élément de configuration (CI)

Tests

Une politique dans Prisma Cloud est importée en tant que test dans Conformité de la configuration. Les politiques sont liées à des documents faisant autorité et à des enregistrements de tests, et elles peuvent être modifiées pour répondre aux besoins de votre organisation. Vous pouvez afficher les tests en accédant à **Configuration Compliance** > **Tests**.

Si **l'intégration de Vulnerability Response à Palo Alto Prisma Cloud** est installée, la tâche `Prisma Policy Integration` d'intégration récupère les tests. Vous pouvez afficher cette tâche d'intégration en accédant à **Tous** > **Intégrations dans le cloud Prisma** > **Intégration de la politique Prisma**.

Résultats des tests

Une alerte dans Prisma Cloud est importée en tant que résultat de test dans Conformité de la configuration. Les alertes sont corrigées à l'aide de **tâches de correction**. Vous pouvez afficher les résultats des tests en accédant à **Configuration Compliance** > **Résultats des tests**.

L'importation Conformité de la configuration des résultats des tests dans le cadre d'une intégration tierce Une fois qu'ils sont visibles sur l'application Conformité de la configuration , ils sont corrigés à l'aide de tâches de remédiation.

Si **Vulnerability Response Integration with Palo Alto Prisma Cloud** est installée, la tâche d'intégration **Prisma Alert Integration** récupère les résultats des tests. Vous pouvez afficher cette tâche d'intégration en accédant à **Tous** > **Intégration dans le cloud Prisma** > **Intégrations** > **Intégration d'alerte Prisma**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'intégration des alertes Prisma est une tâche d'intégration qui s'exécute quotidiennement et extrait les résultats des tests avec le changement d'état après l'heure définie dans le champ **Heure de début** de l'onglet **Intégration**.

Remarque : Si vous exécutez manuellement la tâche d'intégration **Intégration d'alerte Prisma** , exécutez-la après avoir exécuté la tâche d'intégration, **Intégration de politique Prisma**.

Lorsque **l'intégration des alertes Prisma** termine l'importation des données, un événement est lancé pour déclencher les calculs de fin d'importation. Si l'alerte échoue continuellement au cours des derniers jours, l'intégration ne récupère pas les alertes, car il n'y a aucun changement d'état pour l'alerte. Ainsi, pour maintenir les données des résultats des tests à jour avec les alertes Prisma, une nouvelle tâche d'intégration, **l'intégration complète des alertes Prisma** , qui extrait les alertes mises à jour au cours des sept derniers jours, est ajoutée. Il s'exécute chaque semaine et extrait tous les résultats des tests, qui ne sont pas réussis.

Sources de référence

Conformité de la configuration Utilise des sources et des citations faisant autorité lors de la génération d'alertes de vulnérabilité pour les tests. Les sources faisant autorité correspondent généralement à des sections de normes industrielles publiées, telles que ISO 27001 et PCI DSS 3.2.1.

Ces documents sources contiennent des références à des informations sur des problèmes de configuration logiciels et matériels connus provenant d'experts dans le domaine de la sécurité informatique. Les références définissent les exigences relatives aux politiques et procédures de sécurité. Accédez à la **Configuration Compliance** > **Sources de référence** pour afficher les sources faisant autorité.

Ressources

Si l'est Intégration de Réponse aux vulnérabilités à Palo Alto Prisma Cloud installé, la tâche `Prisma Alerts Integration` planifiée capture les informations relatives à l'alerte dans le module ou la table Éléments détectés. Vous pouvez afficher cette tâche planifiée en accédant à **Intégration dans le cloud Prisma** > **Intégrations**.

L'intégration des alertes Prisma importe d'autres types d'informations, telles que les balises de ressource et les attributs dans le cloud qui sont stockés dans des tables. Ces informations s'affichent dans le formulaire Éléments détectés.

- Balises d'hôte : une ressource peut avoir plusieurs balises. Les balises d'hôte sont disponibles sous forme de paire de valeurs clés. Par exemple, le système d'exploitation est Windows 10 et la version Java est 1.8.
- Attributs dans le cloud pour les actifs : les attributs dans le cloud suivants sont disponibles :
  - Compte dans le cloud : fournit l'ID de compte de l'intégration. Les informations sont renseignées à partir des comptes dans le cloud [sn_sec_cmn_cloud_account. LIST].
  - Région du cloud : fournit l'emplacement où la ressource a été hébergée. Les informations sont renseignées à partir des régions du cloud [sn_sec_cmn_region. LIST].
  - Type de ressource dans le cloud : fournit des informations sur le type de ressource, par exemple s'il s'agit d'un ordinateur virtuel ou d'une instance de base de données, entre autres. Les informations sont renseignées à partir du type de ressource cloud [sn_sec_cmn_cloud_resource_type. LIST].
  - Fournisseur de services dans le cloud : fournit des informations sur le fournisseur de services dans le cloud, qu'il s'agisse d'Amazon Web Services (AWS), d'Oracle Cloud,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

entre autres. Les informations sont renseignées à partir du fournisseur de services dans le cloud [sn_sec_cmn_cloud_service_provider. LIST].

- Groupes de comptes dans le cloud : fournit des informations sur les groupes de comptes. Les informations sont renseignées à partir de la table Groupes de comptes dans le cloud [sn_vul_prismacloud_account_group.list].

Remarque : L'attribut Groupes de comptes dans le cloud est disponible uniquement pour Prisma.

Règles de recherche de CI

Les règles de recherche de CI du système de base sont disponibles pour l'ID de ressource, le nom et la catégorie S3. Pour plus d'informations sur les règles de recherche de CI, reportez-vous à la section Règles de recherche de CI pour Microsoft Defender for Cloud IntegrationOpérations de sécurité et Palo Alto Prisma Cloud.

Prisma Cloud REST Messages

Les messages REST Prisma sont utilisés pour passer des appels à l'interface de programmation d'application (API) Prisma afin d'extraire les données de conformité.

Les messages REST suivants sont fournis avec le système de base.

Intégrations dans le cloud Prisma

Toutes les intégrations dans le cloud Prisma utilisent le jeton Web JSON (JWT) pour l'authentification et l'autorisation.

Message REST de connexion Prisma

Point de terminaison	Description	Fonction de message REST	Détails	Lien vers la documentation d'API
/connectez-vous	Obtient le jeton JWT à utiliser dans toutes les intégrations suivantes.	*POST*	`{ "username": <<access key id >>, "password": <<secret access key>>}`	https://pan.dev/prisma-cloud/api/cspm/app-login/

Message REST du jeton d'actualisation Prisma

Point de terminaison	Description	Fonction de message REST	Détails	Lien vers la documentation d'API
/auth_token/étendre	Renouvelle automatiquement le jeton JWT à son expiration. La durée par défaut pour l'expiration du jeton est de 60 minutes.	*GET*	N/A	https://pan.dev/prisma-cloud/api/cspm/extend-session/

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Message REST de la politique Prisma

Point de terminaison	Description	Fonction de message REST	Détails	Lien vers la documentation d'API
/v2/politique	Récupère toutes les données de politique à partir de Prisma.	`GET`	N/A	https://pan.dev/prisma-cloud/api/cspm/get-policies/

Message REST d'alerte Prisma

Point de terminaison	Description	Fonction de message REST	Détails	Lien vers la documentation d'API

/v2/alerte	Récupère toutes les alertes de Prisma.	`POST`	<pre>{
			"detailed": "false",
			"filters": [
			{
			"name": "timeRange.type",
			"operator": "=",
			"value": "ALERT_STATUS_UPDATED"
			}
			],
			"sortBy": [
			"resource.id"
			],
			"pageToken": "",
			"offset": 0,
			"limit": 2000,
			"timeRange": {
			"type": "absolute",
			"value": {
			"startTime": <<Import since at integration level>>,
			"endTime": << Current integration run time>>
			}
			}
			}</pre>
				https://pan.dev/prisma-cloud/api/cspm/post-alerts/

Pour l'intégration de l'alerte de compréhension Prisma, les filtres du corps POST ci-dessus doivent être remplacés comme suit :

```
"filters": [
{
                "name": "alert.status",
                "operator": "=",
                "value": "open"
            },
            {
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
            "name": "alert.status",
            "operator": "=",
            "value": "dismissed"
        },
        {
            "name": "alert.status",
            "operator": "=",
            "value": "snoozed"
        },
        {
            "name": "alert.status",
            "operator": "=",
            "value": "pending_resolution"
        },
        {
            "name": "timeRange.type",
            "operator": "=",
            "value": "ALERT_UPDATED"
        }

],
```

Qualys intégration avec Conformité de la configuration

Policy Qualys Compliance collecte les données et les envoie automatiquement à l'application Qualys , qui analyse et met en corrélation les informations en permanence. Elle s'intègre facilement en tant qu'intégration Qualys pour Security Operations pour mapper les résultats de configuration aux CI et aux services d'entreprise afin de déterminer l'impact et la priorité des erreurs de configuration potentielles.

Si vous avez plusieurs déploiements de l'application Qualys Cloud Platform , vous pouvez ajouter une intégration pour chaque déploiement. Les actifs, identifiés par plusieurs déploiements tiers et leurs vulnérabilités, sont consolidés et rapprochés avec votre CMDB. Cette consolidation se produit même lorsque les processus d'analyse se chevauchent entre les multiples déploiements. Les données provenant de chaque déploiement sont identifiées et disponibles dans une instance unique de Réponse aux vulnérabilités.

Remarque : Vous ne pouvez pas supprimer l'intégration de vulnérabilité d'origine, mais vous pouvez la désactiver. Les intégrations créées à partir de modèles inactifs sont désactivées par défaut.

Balises d'hôtes

Toutes les balises d'hôte sont importées dans le cadre de l'intégration de la Qualys liste d'hôtes. Les balises d'hôte sont principalement utilisées pour le filtrage dans les règles de Réponse aux vulnérabilités tâche d'affectation et de rattrapage. Ils s'affichent dans le formulaire Élément détecté.

Remarque : L'intégration Qualys de la liste d'hôtes doit être exécutée avant de créer les règles de tâche d'affectation ou de rattrapage afin Réponse aux vulnérabilités que toutes les balises puissent être présentes dans les règles et avant que les éléments vulnérables ne soient importés et regroupés.

- Le stockage des balises n'est pas sensible à la casse. Si une balise **San Diego** est créée, une balise **SAN DIEGO** ne peut pas être stockée dans la table des balises d'hôte. « San Diego » et « SAN DIEGO » sont considérés comme le même tag d'hôte. Quelle que soit la balise importée en premier, elle gagne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'utilisation de balises d'hôte comme clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises d'hôte sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'hôte sont contrôlées par la propriété système globale **sn_vul.import_host_tags**. Cette propriété est définie sur vrai par défaut. La désactivation des balises les désactive dans toutes les instances.

Les balises d'hôte (également appelées balises d'actif) sont utilisées pour organiser et suivre les actifs de votre organisation. Vous pouvez affecter des balises à vos ressources hôtes. Ensuite, lors du lancement des analyses, vous pouvez sélectionner les balises associées aux hôtes que vous souhaitez analyser. Le module Balises d'hôte vous permet de télécharger de manière planifiée les données de balises d'hôte vers Qualys votre instance.

Association d'un test à son groupe de tests

Pour renseigner le champ Groupe de test sur un formulaire de test, activez la *sn_vulc.add_policy_as_key* propriété système. Pour en savoir plus sur la façon dont un test est associé à son groupe de tests, sur l'impact de l'activation de cette propriété système et sur les conditions préalables, consultez KB1644268 article.

Avertissement : Vous ne pouvez pas désactiver la *sn_vulc.add_policy_as_key* propriété système une fois qu'elle est activée. Passez donc en revue la section Impact de l'article KB1644268 avant d'activer cette propriété système.

Lorsque vous activez cette propriété système, après l'ingestion suivante, le champ **Groupe de test** est ajouté dans la table de test et remplit le groupe de test auquel un test appartient. Ainsi, vous pouvez facilement :

- identifier le groupe de tests auquel appartient un résultat de test en remontée pas à pas d'un groupe de test à l'autre.
- Différencier les enregistrements de test avec le même ID de test qui sont associés à différents groupes de tests.

Intégration Qualys à l'application ServiceNow® Conformité de la configuration

Si le est déjà installé sur votre système et que vos informations d'identification d'API Qualys Vulnerability Integration sont différentes de celles que vous souhaitez utiliser pour Conformité de la configuration, accédez à l'Assistant de configuration (dans Réponse aux vulnérabilités) et affectez-les à chaque intégration de **PC Qualys** .

Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Intégrations principales** et modifiez le champ **Informations d'identification de l'API Qualys** sous l'onglet **Détails REST Qualys** .

Configurer les paramètres PCRS

À partir de la version 12.6.3 de Intégration Qualys pour Opérations de sécurité, vous pouvez utiliser l'intégration de l'hôte de politique PCRS et l'intégration Qualys des résultats des tests Qualys PCRS pour importer des résultats de tests avec de nouveaux ensembles d'API Qualys . Ces intégrations ont besoin d'une URL de passerelle à partir de Qualys laquelle extraire des informations.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Lorsque vous installez le Intégration Qualys pour Opérations de sécurité pour Réponse aux vulnérabilités, vous pouvez configurer la **gateway_url** des nouvelles intégrations PCRS dans Conformité de la configuration. Pour plus d'informations sur la façon de trouver l'URL de passerelle pour l'URL de votre API, consultez Identifier votre plateforme Qualys .

L'URL de la passerelle doit être ajoutée dans votre ServiceNow instance.

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Instances d'intégration**.

   Remarque : Assurez-vous que le périmètre dans lequel vous vous trouvez est Qualys pour Security Operations.

2. Ouvrez l'instance utilisée par les intégrations PCRS.
3. Dans l'onglet Paramètres d'instance d'intégration, ajoutez l'URL de la passerelle pour **gateway_url** configuration.

   Remarque : L'intégration des résultats des tests Qualys PCRS dépend de l'intégration de l'hôte de politique Qualys PCRS. Ainsi, si vous antidatez les résultats des tests PCRS Qualys d'intégration, vous devrez peut-être les exécuter à nouveau dans le même ordre.

Composants installés avec Qualys Integration for Security Operations

Les rôles, travaux planifiés et tables suivants sont installés avec Qualys Integration for Security Operations.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Afficher les listes filtrées des composants installés avec une application

Filtrez la table Fichiers d'applications afin de n'afficher que les rôles, les travaux planifiés et les tables installés avec une application. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés dans l'instance et dans la table de métadonnées. Suivez ces étapes pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application. Par exemple : **Application** > **est** > **Réponse aux vulnérabilités**.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, sélectionnez **ET,** puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
sn_vul_qualys.read	Dispose d'un Qualys Vulnerability Integration accès en lecture aux enregistrements.	
sn_vul_qualys.utilisateur	Utilisateur pour Qualys Vulnerability Integration. Peut lire et écrire des enregistrements	sn_vul_qualys.read
sn_vul_qualys.admin	Administrateur pourQualys Vulnerability Integration. Par exemple, vous pouvez modifier les dates de début d'intégration et définir des paramètres de configuration avancés.	• sn_vul_qualys.utilisateur • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_integration	Peut configurer le Qualys Vulnerability Integration	sn_vul_qualys.admin

Travaux planifiés installés

Tâche planifiée	Description
Qualys Politiques de PC	Récupère les politiques à partir de Qualys. La sortie est stockée dans la table sn_vulc_policy. L'API utilisée dans cette intégration ne prend pas en charge la pagination, c'est pourquoi toutes les politiques sont téléchargées sur une seule page.
Qualys Détail des politiques PC	Récupère les détails complets de la politique, tels que les technologies et les sections, par exemple.
Qualys Contrôles PC	Récupère les informations sur les contrôles de conformité pour différents ID de contrôle à partir de Qualys.
Qualys Résultats PC	Récupère les enregistrements de posture de conformité à partir de Qualys. Le résultat de cette intégration est Résultats des tests. Par défaut, les détails des paramètres sont transmis pour importer les informations sur l'hôte, les dates/heures de la dernière analyse, l'ID de contrôle et les informations de preuve.
Qualys Résultats complets du PC	Récupère les enregistrements de posture de conformité en fonction de Qualys la date de la dernière évaluation pour les résultats des tests qui n'ont pas été réussis. Cette tâche fonctionne une fois par semaine. Le résultat de cette intégration est des résultats de tests. Par défaut, les détails du paramètre sont transmis pour importer les informations sur l'hôte, les dates/heures de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
	la dernière analyse, l'ID de contrôle et les informations de preuve.
Qualys Intégration de l'hôte de la politique PCRS	Récupère les données de l'hôte Qualys et les traite dans votre instance. Le résultat de cette intégration est les ID d'hôtes de politique. Les Qualys données hôtes sont importées dans cette intégration. **Remarque :** • Cette tâche planifiée s'affiche uniquement lorsque Conformité de la configuration est installé. • Configurez les paramètres d'instance d'intégration gateway_url et pcrs_page_size avant d'exécuter cette intégration. Ces deux intégrations seront OOB inactives. Si vous activez l'une ou l'autre de ces intégrations, les intégrations de résultats PC seront désactivées. Ces deux intégrations sont ajoutées en fonction des nouvelles API de streaming de Qualys.
Qualys Intégration des résultats des tests PCRS	Récupère les résultats des tests pour chaque ID d'hôte. Cette intégration utilise le paramètre Heure de début dans l'onglet Détails de l'intégration. **Remarque :** • Cette tâche planifiée s'affiche uniquement lorsque Conformité de la configuration est installé. • Configurez les paramètres d'instance d'intégration gateway_url et pcrs_page_size avant d'exécuter cette intégration. • Si vous choisissez d'exécuter l'intégration manuellement, exécutez Qualys l'intégration des résultats des tests PCRS après Qualys Politiques PC, Qualys Détails des politiques PC et Qualys Intégration de l'hôte de politique PCRS.

Remarque : L'intégration de l'hôte Qualys de politique PCRS et Qualys des résultats des tests PCRS est inactive par défaut. Ces deux intégrations sont basées sur les nouvelles API de streaming de Qualys. Si vous activez l'une de ces intégrations, l'intégration des résultats PC sera désactivée et vice versa.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables installées

Table	Description
Qualys Importation de résultat PC sn_vul_qualys_pc_result_import	Table étendant la ligne de jeu d'importation. La transformation des cartes de champs est ignorée et la pièce jointe de réponse est traitée directement avec le script onComplete.
ID d'hôte de politique sn_vul_qualys_policy_host_id	Table stockant le mappage entre la politique et l'hôte pour lequel cette politique a été analysée. Cette table est utilisée dans la nouvelle Qualys intégration PCRS. **Remarque :** Cette table n'apparaît que lorsque Conformité de la configuration est installé.
Qualys Importation de l'hôte de la politique PCRS sn_vul_qualys_pcrs_policy_host_import	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de réponse est traitée directement avec le script onComplete. **Remarque :** Cette table s'affiche uniquement lorsque Conformité de la configuration est installé.
Qualys Importation de politique PC sn_vul_qualys_pc_policy_import	Table étendant la ligne de jeu d'importation. La transformation de la carte de champ est ignorée et la pièce jointe de réponse est traitée directement avec le script onComplete.

Mettre à jour les éléments de configuration avec l'identificateur de partition de réseau pour l'intégration Qualys

Créez des éléments de configuration (CI) uniques pour les actifs de votre environnement qui partagent des adresses IP. Identifiez les actifs distincts dans votre environnement et mettez automatiquement à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous fournir plus de détails sur vos vulnérabilités.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Par défaut dans l'application Réponse aux vulnérabilités , une façon d'identifier vos actifs est l'adresse IP. Dans certains cas, les actifs peuvent partager des adresses IP, mais elles sont stockées sous la forme d'un seul CI dans votre CMDB.

Par exemple, comme indiqué dans les tables suivantes, plusieurs actifs (CI) de votre environnement peuvent partager des adresses IP, mais ont des ID de réseau et de référentiel uniques. Toutefois, par défaut, ces actifs sont généralement identifiés et stockés sous la forme d'un seul CI (CI 1) lors de la recherche d'adresse IP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche d'adresses IP et création de CI par défaut

Source	Adresse IP	NETWORK_ID	Élément de configuration
Qualys Vulnerability Integration: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	Adresse IP	REPOSITORY_ID	Élément de configuration
Qualys Vulnerability Integration: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Vous pouvez créer des CI individuels pour des actifs qui ont la même adresse IP afin de les identifier comme des actifs distincts. À partir d'une importation de données récente, vous pouvez mettre à jour vos CI existants avec plus de granularité qui inclut l'identificateur de partition de réseau [network_partition_identifier] en exécutant la tâche planifiée, *`Update existing discovered items with network partition identifier`*.

Cette tâche planifiée est désactivée par défaut. Activez cette fonctionnalité pour les intégrations Actifs et Vulnérabilités immobilisées et ouvertes dans Qualys Vulnerability Integration l'assistant de configuration afin d'afficher cet identificateur sur vos enregistrements.

Lorsqu'elle est activée, cette tâche planifiée ajoute l'identificateur de partition de réseau [network_partition_identifier] aux enregistrements de CI existants à partir des données importées. Les CI existants créés par l'IRE sont également mis à jour. La tâche planifiée crée également des CI qui incluent l'identificateur de partition de réseau à partir de l'importation suivante. Vous pouvez également lancer la tâche à la demande pour mettre à jour vos données existantes.

À partir des Réponse aux vulnérabilités versions 14.0 et 12.1 de Vulnerability Qualys Vulnerability Integration Integration, les modèles de classe CI CMDB (1.0.21.) sont pris en charge. Les modèles de classes ont l'identificateur de partition de réseau [network_partition_identifier] dans les règles d'identification IRE (Identification et rapprochement).

Option	Description
Exécuter les travaux planifiés sur demande.	Mettez à jour vos éléments détectés existants. Les CI de vos données existantes Qualys Vulnerability Integration sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau. Les éléments détectés, les éléments vulnérables et les

Traduction automatique

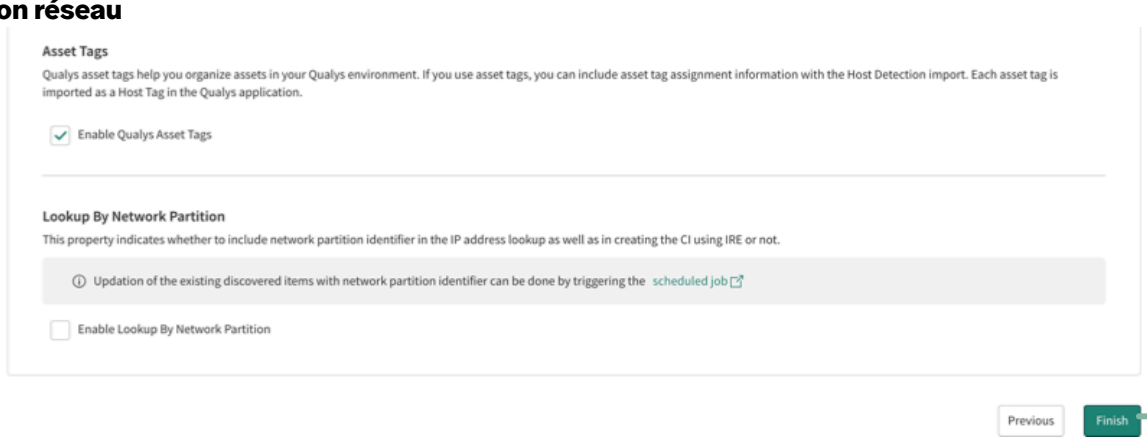
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

Option	Description
	enregistrements de détection sont tous mis à jour avec les nouveaux CI.
Attendez les importations de données fraîches à partir des intégrations avec les travaux planifiés suivants.	Créez des CI pour chaque nouvel actif à l'aide de l'identificateur de partition de réseau en commençant par la tâche planifiée suivante. Les enregistrements de CI, d'éléments vulnérables et de détection sont tous mis à jour pour inclure la nouvelle granularité. De nouveaux CI sont créés lorsqu'aucune correspondance exacte n'est trouvée.

Procédure

1. Accédez à la **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
2. Choisissez Qualys Vulnerability Integration.
3. **Modifiez** l'intégration requise.
4. Choisir **Configuration de la détection de l'hôte**.
5. Choisir **Activer la recherche par partition de réseau** case à cocher dans le **Rechercher par partition réseau**



section.

6. Cliquez sur **Terminer**.

Les identificateurs de partition de réseau NETWORK_ID et REPOSITORY _ID inclus dans la recherche d'adresses IP et la création de CI

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
Qualys Vulnerability Integration: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	03712	CI 1	CI 1

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
	123.12.12.141	03713	CI 1	CI 2

Source	Adresse IP	REPOSITORY_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
Qualys : intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Les règles de recherche d'identification de CI d'adresse IP et d'adresse IP incomplète incluent automatiquement l'attribut d'identificateur de partition de réseau pour une importation de données à partir des intégrations Actifs et Vulnérabilités fixes et ouvertes pour Qualys Vulnerability Integration.

Après avoir activé le travail planifié et enregistré les enregistrements, vous pouvez également mettre à jour vos éléments détectés existants avec des CI qui incluent l'identificateur de partition de réseau en lançant des travaux planifiés à la demande. Les CI de vos enregistrements d'élément détecté, d'élément vulnérable et de détection existants sont automatiquement mis à jour.

Définir des paramètres de filtre supplémentaires pour Qualys les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec Qualys Vulnerability Integration le pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec les intégrations prises en charge Qualys .

Avant de commencer

Cas d'utilisation : en tant que responsable ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que des détails spécifiques de la vulnérabilité. Par exemple, supposons que vous souhaitiez afficher les vulnérabilités importées qui sont filtrées par des adresses IP ou des plages d'adresses IP spécifiques. Vous souhaitez également importer uniquement les machines qui sont dans votre champ d'application, par exemple, uniquement les machines de votre réseau d'entreprise qui ne sont pas des périphériques externes.

Pour vous aider à collecter ces données, vous pouvez ajouter Qualys des paramètres pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, cette fonctionnalité vous permet de personnaliser vos informations de requête HTTP avec Qualys les paramètres de votre ServiceNow AI Platform. Vous modifiez ou ajoutez ces valeurs à votre enregistrement de méthode HTTP sous la méthode REST pour les intégrations prises en charge Qualys de la Qualys Vulnerability Integration.

Rôle requis : sn_vul.vulnerability_admin

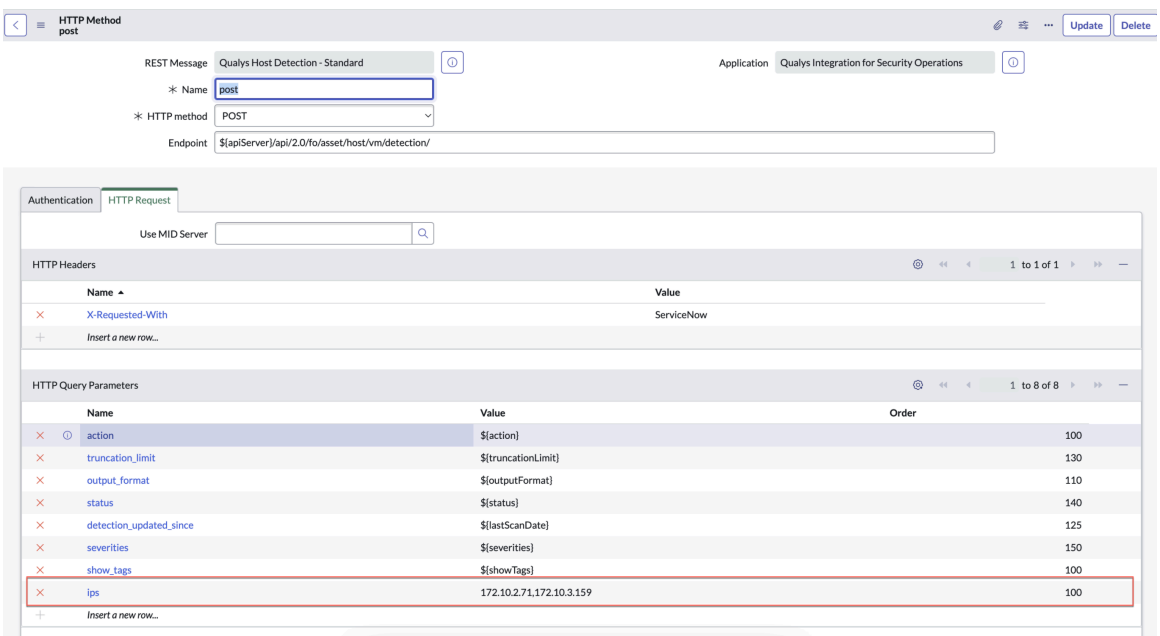
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Recherchez les paramètres pris en charge par le Qualys produit sur le site développeur que vous souhaitez utiliser pour votre filtrage.
   Les paramètres et les Qualys valeurs que vous saisissez à partir du produit ne sont pris en charge qu'au niveau de l'instance d'intégration dans votre ServiceNow AI Platform. Toutes les Qualys intégrations prennent en charge le filtrage à l'aide de paramètres de requête.
2. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
3. Sur la Qualys page de liste Intégrations, cliquez sur l'enregistrement de l'intégration pour laquelle vous souhaitez ouvrir l'enregistrement.
4. Une fois l'onglet Qualys Détails REST sélectionné, recherchez et cliquez sur l'icône d'informations (I) pour la méthode REST, puis sur **Ouvrir l'enregistrement** pour ouvrir l'enregistrement de la méthode HTTP.
5. Sélectionnez l'onglet **de demande HTTP** .
6. Dans les paramètres de requête HTTP du corps de la demande, ajoutez les valeurs que vous avez obtenues sur le Qualys site développeur.

   Dans l'image suivante, à titre d'exemple, le paramètre qui ingère uniquement certaines adresses `ips={value}` /plages IP a été ajouté. Dans ce cas, la **valeur** est une ou plusieurs adresses IP/plages que vous spécifiez. Les entrées multiples sont séparées par des virgules, 172.10.2.71, 172.10.3.159, et une plage est spécifiée par un trait d'union, 10.10.10.1-10.10.10.100. Consultez le site du Qualys développeur pour plus d'informations.



   Si vous souhaitez entrer plusieurs paramètres, consultez la documentation pour plus d'informations sur la Qualys façon de séparer chaque valeur.

   Remarque : Vous devez connaître vos exigences en matière d'API. Vous devrez peut-être ajouter ces propriétés API aux paramètres de requête ou au contenu du corps.

   Quelques autres paramètres que vous pourriez trouver utiles sur le Qualys site du développeur :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- `ag_ids` - ID de listes de groupes d'actifs à récupérer. Ce paramètre garantit que seules les machines sous votre champ d'application sont introduites.
- `qids` - Ce paramètre limite les résultats à certaines vulnérabilités seulement (QID dans la table Third-Party Entry). Ce paramètre empêche d'inonder votre système d'enregistrements d'informations.

7. Cliquez sur **Mettre à jour**.

Configurer la granularité du résultat de test Qualys

Configurez la granularité des résultats des tests Qualys pour vous assurer que le système importe les résultats à un niveau plus détaillé en fonction des clés de configuration que vous avez sélectionnées. En plus des clés par défaut, vous pouvez configurer des clés supplémentaires en fonction de vos besoins pour augmenter la granularité. Les importations granulaires permettent aux équipes de gérer leurs ressources respectives de manière indépendante et empêchent le remplacement des données lorsque plusieurs enregistrements partagent des identificateurs communs.

Avant de commencer

Rôle requis :

- sn_vulc.admin

Procédure

1. Accédez à la **Tous** > **Configurer la granularité du résultat de test Qualys**.
2. Dans le formulaire Configuration de clé, vérifiez que :
   - **L'intégration source** est Qualys Cloud Platform.
   - **La table** est définie sur Résultat du test.
3. Dans la section **Clé de configuration** , choisissez le champ pour lequel vous souhaitez créer des résultats de test uniques.
   Par exemple, la sélection `instance` crée des résultats de test uniques pour chaque instance d'une base de données.

   Remarque : Utilisez cette fonctionnalité avec prudence. Chaque clé de configuration supplémentaire augmente le temps d'intégration. Pour maintenir des performances optimales, limitez votre utilisation à un maximum de trois touches supplémentaires.

4. Entrez *vrai* à `instance` côté de pour activer la granularité ou *faux* pour la désactiver.
5. Sélectionnez **Mettre à jour** pour enregistrer vos changements.

Résolution des Qualys problèmes d'intégration de vulnérabilité

Certains problèmes couramment rencontrés, ainsi que des solutions de contournement sont abordés.

Les pièces jointes n'apparaissant pas après l'importation

Si les pièces jointes n'apparaissent pas comme prévu pour les sources de données ou sur un incident de sécurité après les importations d'intégrations tierces, vérifiez vos restrictions IP.

Les restrictions d'accès IP peuvent empêcher les pièces jointes d'être vues, sauf si vous êtes connecté à partir d'une adresse IP sécurisée. Étant donné qu'une nouvelle pièce

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

jointe est ajoutée à chaque importation, cela peut entraîner des doublons que vous devez supprimer.

Par exemple, lorsque vous exécutez une intégration d'importation d'hôte tierce, si vous ne voyez aucune pièce jointe sur vos sources de données, vérifiez vos restrictions IP et ajoutez des utilisateurs à la liste sûre avant l'importation.

Modifier les cartes de transformation

Les cartes de transformation sont fournies avec des configurations de base et sont généralement suffisantes. Vous pouvez modifier les mappages de transformation en fonction des besoins de votre organisation.

Avant de commencer

Rôle requis : sn_vul_qualys.admin + import_admin

Procédure

1. Accédez à la **Tous** > **Ensembles de données à importations système** > **Administration** > **Cartes de transformation** pour afficher les messages REST.
2. Filtrez la liste résultante par application et limitez la liste à l'application **Qualys Vulnerability Integration** .
3. Modifiez les cartes de transformation selon les besoins du client.

   Pour plus d'informations sur les données fournies par l'API Qualys, consultez la documentation de l'API Qualys .

Vérifier la taille de la propriété de la pièce jointe XML

Vérifie que la propriété de pièce jointe XML est suffisante pour les fichiers volumineux.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Importer/exporter**.
2. Faites défiler vers le bas jusqu'à **Propriétés d'importation** > **Format XML** en bas de la page.



3. Si nécessaire, remplacez la valeur par 250 et cliquez sur **Enregistrer**.

Information associée

Propriétés système disponibles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Limites de la récupération de données

Par défaut, il n'existe aucune restriction sur la façon dont les données sont récupérées à partir de Qualys. De nombreux enregistrements peuvent être liés à des vulnérabilités de faible gravité qu'un client n'est pas disposé à corriger à l'aide de son processus de réponse aux vulnérabilités. La mise à jour des paramètres de message/méthode REST correspondants peut modifier ce comportement.

Le message/la méthode REST responsable de cette mise à jour est **Qualys Host Detection – Standard/POST**. Pour mettre à jour les valeurs, ajoutez un nouveau paramètre de requête HTTP à la méthode POST avec les valeurs suivantes :

- Nom : gravités
- Valeur : 3-5 (ou toute autre sévérité appropriée souhaitée)

L'intégration de la base de connaissances Qualys échoue

Résolvez Qualys l'échec de l'intégration de la base de connaissances en réduisant la taille de la pièce jointe de Qualys la charge utile reçue à la limite spécifiée.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Assurez-vous que la taille de la pièce jointe de la charge utile se trouve dans la limite spécifiée.
   a. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration**.
   b. Sélectionnez l'onglet **Paramètres d'instance d'intégration** .
   c. Sélectionnez **max_delta_days** et modifiez la valeur par défaut sur 3.
2. Si l'intégration échoue toujours, procédez comme suit :
   a. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Intégrations principales**.
   b. Sélectionnez **la base de connaissances Qualys**.
   c. Sélectionnez l'onglet **Détails de l'intégration** .
   d. Dans le champ **Heure de début** , sélectionnez la date actuelle pour ignorer l'exécution de l'exécution pour ce jour.
   e. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Instances d'intégration**.
   f. Sélectionnez l'onglet **Paramètres d'instance d'intégration** .
   g. Sélectionnez **kb_backfill_full_import** et remplacez la valeur par défaut par true.

Résultats

L'exécution de l'intégration du remplissage de la base de connaissances Qualys met à jour toutes les entrées tierces (TPE) dans le système. Alors que l'intégration de la détection d'hôte Qualys crée une entrée d'espace réservé, l'intégration du remplissage de la base de connaissances Qualys la met à jour.

Qualys Graphique de l'état d'exécution de l'intégration

Le Qualys module État de l'exécution de l'intégration est une vue graphique de l'état des exécutions de l'intégration Qualys .

Pour afficher l'état des exécutions d'intégration, accédez à **Intégration de vulnérabilité Qualys** > **État de l'exécution de l'intégration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

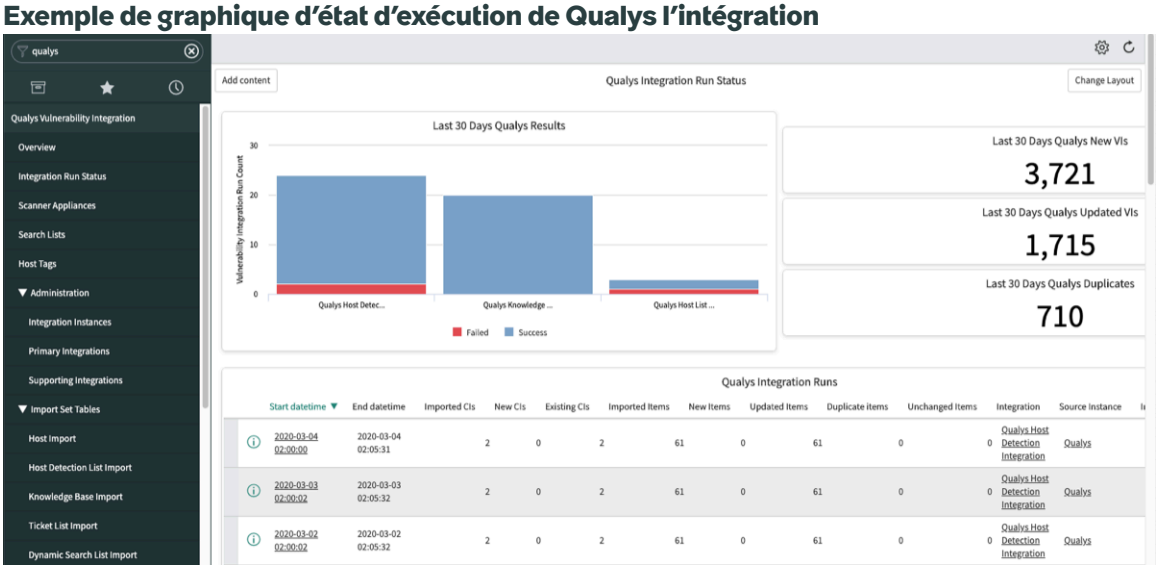
Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Dans le graphique, pointez sur n'importe quelle partie (barre, secteur, point de données, etc.) pour afficher des données générales spécifiques à cette partie. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

L'état Qualys de l'exécution de l'intégration affiche l'état d'exécution de l'intégration de vulnérabilité au cours des 30 derniers jours. Le nombre de VI mis à jour Qualys [qualys] indique le nombre de détections uniques dans le même actif. L'élément vulnérable est ensuite mis à jour avec la nouvelle détection.

Remarque : Le nombre d'exécutions de l'intégration de vulnérabilité n'est affiché que pour les intégrations, qui sont définies sur l'état actif. Accédez à la **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales** et définissez l'état sur actif.

Exemple de graphique d'état d'exécution de Qualys l'intégration



- Les valeurs de la colonne Éléments importés représentent le nombre total d'enregistrements créés à partir d'une exécution d'intégration.
- La colonne Nouveaux éléments affiche le nombre d'enregistrements créés à partir d'une exécution d'intégration.
- La colonne Éléments en double n'est plus renseignée. Vous préférez peut-être supprimer cette colonne de l'affichage.
- La colonne Éléments mis à jour affiche le nombre de fois que les enregistrements sont mis à jour au cours d'une exécution d'intégration. Cette valeur n'est pas le nombre d'enregistrements uniques qui sont mis à jour. Si, par exemple, un enregistrement est mis à jour deux fois pendant l'exécution de l'intégration, il est compté deux fois et s'affiche sous la forme de 2 éléments mis à jour.
- La colonne Éléments inchangés affiche les enregistrements trouvés pendant l'exécution de l'intégration qui existent déjà dans la base de données, mais qui n'ont pas été mis à jour, car aucune des valeurs de champ pertinentes n'a changé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'intégration s'exécute sans résultat pour les quatre valeurs suivantes : **Nouveaux CI**, **CI existants**, **Nouveaux éléments** et **Éléments mis à jour** sont filtrés hors de la liste des **exécutions d'intégration Qualys** .

Qualys Rapports des graphiques d'état d'exécution de l'intégration

Nom	Description
Résultats des 30 derniers jours Qualys	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Exécuter dans un visuel de barre.
Nouveaux VI au cours des 30 derniers jours Qualys	Nombre de nouveaux enregistrements importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour au cours des 30 derniers jours Qualys	Nombre d'enregistrements mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Doublons des 30 derniers jours Qualys	Nombre d'enregistrements en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Qualys Exécutions des intégrations	Les enregistrements d'exécution de l'intégration dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection dans la `sn_vul_detection` table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, une fois l'exécution de l'intégration terminée.
Mesures de performance d'ingestion d'élément vulnérables au cours des 30 derniers jours Qualys	Mesures des performances quotidiennes des éléments vulnérables comparées aux 30 derniers jours.
Rendement de performance d'ingestion d'élément vulnérable au cours des 30 derniers jours Qualys	Débit quotidien d'ingestion d'éléments vulnérables mesuré pour l'intégration de la détection d'hôte Qualys au cours des 30 derniers jours.

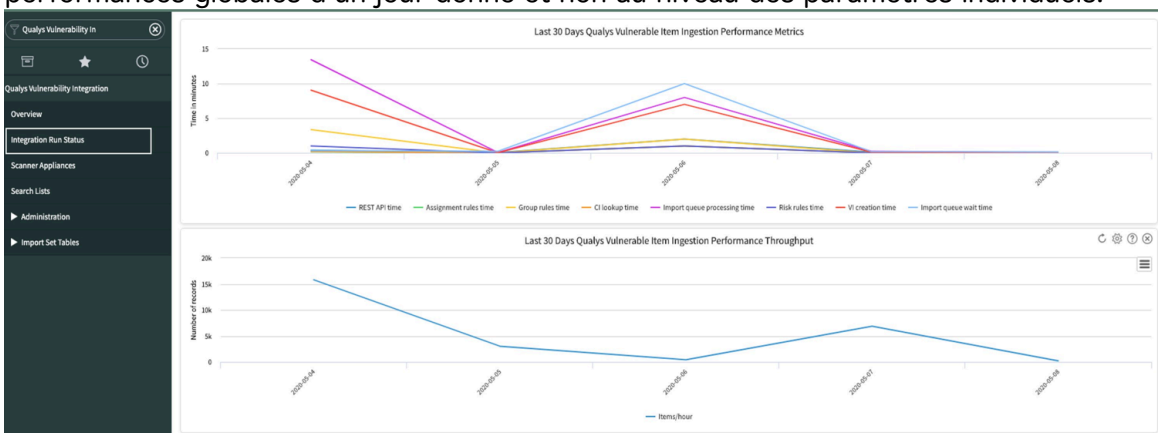
Plusieurs facteurs peuvent avoir un impact sur les performances de l'exécution de l'intégration, comme la quantité de données et le temps nécessaire pour traiter ces données. Deux graphiques comparent les mesures des performances :

- Qualys Mesures de performance d'ingestion d'élément vulnérable : comparez les mesures de performances quotidiennes pour les règles d'affectation, les règles de groupe, les règles de risque, le temps d'attente de la file d'attente, le temps de traitement de la file d'attente et d'autres statistiques relatives aux éléments vulnérables au cours des 30 derniers jours, afin d'identifier la cause de tout écart de performance. La performance est calculée en fonction du temps nécessaire pour chaque activité. Ces paramètres sont calculés et associés au niveau de l'exécution de l'intégration. Chaque paramètre est codé par couleur pour faciliter l'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Qualys Débit de performance d'ingestion d'élément vulnérable : comparez le débit quotidien d'ingestion d'éléments vulnérables pour l'intégration de la détection d'hôte Qualys . Le débit est mesuré en éléments par heure. Ce rapport montre les performances globales d'un jour donné et non au niveau des paramètres individuels.



Messages REST Qualys

Les messages REST Qualys sont utilisés pour passer des appels à l'API Qualys afin d'extraire les données de conformité.

Les messages REST suivants sont fournis avec le système de base.

Message REST de politiques de PC Qualys

Le message REST Politiques des PC Qualys récupère les données de politique de Qualys. Les changements apportés à l'enregistrement de méthode de message REST ont un impact sur la demande de récupération des informations de politique faite à Qualys.

Politiques de PC Qualys Paramètres de message REST

Nom de paramètre	Valeur	Description
action	liste	Indique le type d'opération demandée. Paramètre requis.
Détails	Tous	Indique le niveau de détail affiché pour les politiques récupérées. Il est sûr de modifier selon vos besoins.

Message REST sur les contrôles de PC Qualys

Le message REST Qualys PC Controls récupère les informations sur les contrôles de conformité pour différents ID de contrôle à partir de Qualys.

Paramètres de message REST des contrôles de PC Qualys

Nom de paramètre	Valeur	Description
action	liste	Indique le type d'opération demandée. Paramètre requis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de message REST des contrôles de PC Qualys (suite)

Nom de paramètre	Valeur	Description
Détails	Tous	Indique le niveau de détail affiché pour les contrôles récupérés. Il est sûr de modifier selon vos besoins.

Message REST de détail des politiques de PC Qualys

Le message REST Détail des politiques de PC Qualys récupère les détails complets de la politique, tels que les technologies et les sections.

Détail des politiques de PC Qualys Paramètres de message REST

Paramètre	Valeur	Description
action	liste	Indique le type d'opération demandé. Paramètre requis.
show_user_controls	Booléen	• Définissez la valeur sur 1 pour inclure les contrôles définis par l'utilisateur (UDC) dans la sortie XML. • Lorsqu'ils ne sont pas spécifiés, les CDU ne sont pas inclus. Il s'agit d'un paramètre facultatif. Il est sûr de modifier selon vos besoins.
show_appendix	Booléen	(Facultatif) Définissez la valeur sur 1 pour afficher la section d'annexe dans la sortie XML. Lorsqu'il n'est pas spécifié.

Message REST des résultats PC Qualys

Le message REST de Qualys PC Results récupère les enregistrements de posture de conformité de Qualys.

Résultats PC Qualys Paramètres de message REST

Champ source	Valeur	Description
action	liste	Indique le type d'opération demandée. Paramètre requis. Il n'est pas recommandé d'apporter des modifications.
show_extended_evidence	Booléen	• Définir sur 1 pour afficher les informations de preuves étendues dans la sortie. • Définissez sur 0 ou si elles ne sont pas spécifiées, les informations de preuves étendues ne sont pas affichées dans la sortie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats PC Qualys Paramètres de message REST (suite)

Champ source	Valeur	Description
		Remarque : • Vous ne pouvez pas spécifier `show_extended_evidence=1` dans la même demande que `hide_evidence=1`. Il en résulterait une erreur. La preuve étendue fait partie des données de preuve et elle n'est affichée que lorsque des données de preuve sont affichées. • Ce paramètre n'est pas fourni avec le système de base.
cause_of_failure	Booléen	Si vous réussissez la réponse « 1 », Qualys renvoie la cause de l'échec. Si vous transmettez « 0 », Qualys ne renvoie pas ces attributs. **Remarque :** Ce paramètre n'est pas fourni avec le système de base.
policy_id		Affiche les enregistrements d'informations sur la posture de conformité pour une politique spécifiée. Un ID de politique valide est requis.
Détails	Tous	Indique le niveau de détail affiché pour les postures récupérées . Il est sûr de modifier selon vos besoins.
show_remediation_info		(Facultatif) Définissez la valeur sur 1 pour afficher les informations de rattrapage dans la sortie XML ou CSV. Par défaut, la sortie n'inclut pas les informations de rattrapage. Lorsqu'elles ne sont pas spécifiées, les informations de rattrapage ne sont pas incluses dans la sortie.

Message REST d'intégration de l'hôte de politique Qualys PCRS

L'intégration de l'hôte de politique Qualys PCRS récupère les données de l'hôte à partir de Qualys et les traite dans votre instance.

Politique Qualys PCRS Paramètres du message REST d'intégration de l'hôte

Nom de paramètre	Valeur	Description
policyId	${lastRunDatetime}	ID de politiques pour l'évaluation de la conformité.

Intégration des résultats des tests Qualys PCRS

La table affiche les paramètres de demande envoyés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres du message REST de l'intégration des résultats des tests Qualys PCRS

Nom de paramètre	Valeur	Description
evidenceRequired	${lastRunDatetime}	• La valeur par défaut est 0, ce qui indique que les données de preuve ne seront pas récupérées pour la posture de l'hôte. • Définissez la valeur sur 1 pour récupérer les données de preuve. **Remarque :** Le changement de la valeur sur 1 augmente le temps nécessaire pour extraire les données de posture.
compressionObligatoire		• La valeur par défaut est 1, ce qui indique que la sortie sera compressée. • Définissez la valeur sur 0 si vous ne souhaitez pas que les données soient compressées. **Remarque :** Ne pas compresser les données augmente le temps nécessaire pour extraire les données de posture.

Présentation de l'intégration de vulnérabilité Tenable

L'application Vulnerability Response integration with Tenable développée par ServiceNow l'ingénierie pour l'intégration de vulnérabilité Tenable utilise les données importées de , Tenable.ioTenable.sc et Tenable.cs les produits pour vous aider à classer par ordre de priorité et à corriger les vulnérabilités de vos actifs. L'application est disponible avec un abonnement distinct du ServiceNow® Store.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

L'intégration Tenable Vulnerability utilise trois intégrations Tenable, Tenable.io et , Tenable.sc pour Tenable.cs importer des données d'analyseurs tiers concernant vos actifs et vos vulnérabilités. L'application Vulnerability Response integration with Tenable prend en charge le produit à partir de la version 5.13 et Tenable.cs le produit à partir de la Tenable.sc version 5.0.1.

- Tenable.io est une intégration d'entreprise basée sur le cloud.
- Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le Tenable.sc produit et votre ServiceNow AI Platform instance se trouvent dans le même environnement.

Traduction automatique

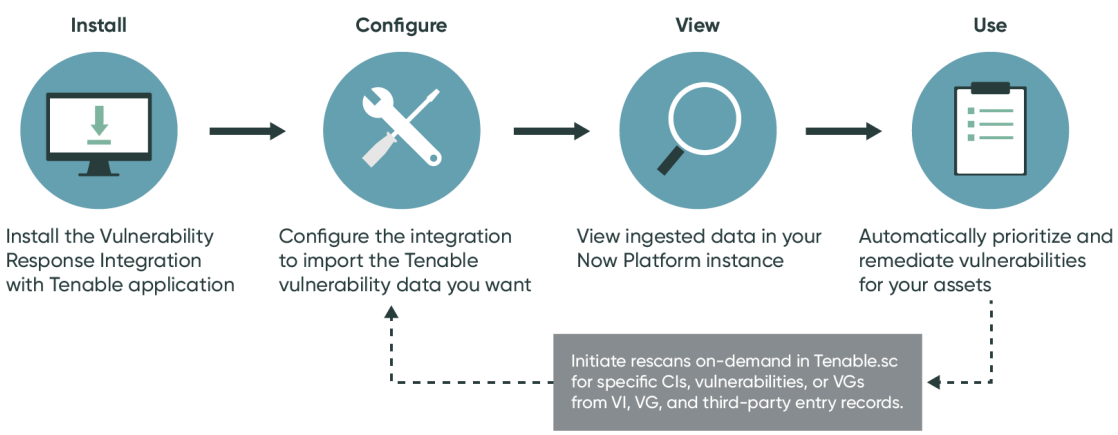
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si le Tenable.sc produit et votre ServiceNow AI Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID.
- Tenable.cs est une intégration d'entreprise basée sur le cloud.

L'application Vulnerability Response integration with Tenable est disponible sur le ServiceNow Store avec un abonnement séparé.

Pour obtenir la liste et la description des intégrations dans , consultez Tenable.sc Intégrations avec l'application Réponse aux vulnérabilitésTenable.io Intégrations avec les Réponse aux vulnérabilités applications et Conformité de la configuration et Tenable Vulnerability Integration.

Intégration de vulnérabilité Tenable



Versions disponibles pour Zurich

Version de mise en production	Notes de publication
Vulnerability Response integration with Tenable v3.13.1, v4.1, v5.0.1	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response

Termes et fonctionnalités clés des intégrations

Éléments vulnérables et vulnérabilités

Un élément vulnérable est créé dans votre ServiceNow AI Platform instance lorsque :

- Une vulnérabilité importée à partir d'un scanner tiers est mise en correspondance avec un actif existant (un élément de configuration dans votre CMDB). Le produit Tenable appelle ces **correspondances des vulnérabilités**.
- Une vulnérabilité importée à partir d'un scanner tiers ne correspond pas à un actif existant dans votre CMDB. Dans ce cas, un CI sans correspondance est également créé avec un élément vulnérable.

  Pour les CI sans correspondance, vous pouvez également utiliser le moteur IRE (Identification et rapprochement) pour créer des CI dans deux nouvelles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

classes lorsqu'un CI existant ne peut pas être mis en correspondance avec un hôte. Dans le cas contraire, des CI sans correspondance sont créés dans les classes de CI sans correspondance. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation.

Entrées de vulnérabilité tierces et modules d'extension

Les entrées de vulnérabilité tierces sont importées à partir d'analyseurs tiers et répertoriées dans la table Entrées de vulnérabilité tierces de votre ServiceNow AI Platform instance. À partir de la version 24.0 de Réponse aux vulnérabilités, la colonne Logiciels de la table Entrées de vulnérabilité tierces renseigne les énumérations de plateforme communes (CPE) associées à une entrée tierce. Les entrées de vulnérabilité tierces de Tenable sont ingérées et mises en correspondance avec les actifs existants répertoriés Réponse aux vulnérabilités dans votre CMDB. Tenable fait référence aux entrées de vulnérabilité tierces sous forme de **modules d'extension.**

Élément de configuration (CI)

Les éléments de configuration sont les actifs existants répertoriés dans votre CMDB.

Élément découvert

Les actifs ingérés à partir de l'importation d'actifs Tenable correspondent aux éléments de configuration existants dans votre CMDB. Les actifs importés sont mis à jour.

Si aucune correspondance n'est trouvée, un CI est créé dans la classe CI sans correspondance du CMDB. Si le module d'extension Modèles de classe CI CMDB est activé, le moteur Identification et rapprochement (IRE) crée des CI à l'aide de nouvelles classes. Pour plus d'informations, consultez Création de CI pour Réponse aux vulnérabilités l'utilisation du moteur Identification et réconciliation. Si le CI d'origine sans correspondance est reclassé, les enregistrements d'éléments détectés sont mis à jour pour refléter l'état. Les éléments détectés vous donnent une visibilité sur la façon dont les actifs sont identifiés et mappés aux CI dans le CMDB.

Règles de recherche de CI

Lorsque les données sont importées à partir d'une intégration tierce, Vulnerability Response utilise automatiquement les données de l'hôte (actif) pour rechercher des correspondances dans la Base de données de gestion des configurations (CMDB). Les règles de recherche de CI sont utilisées pour identifier les CI et les ajouter aux enregistrements de VI lorsque des VIT sont créés pour vous aider dans la correction.

Analyse de nouveau et analyse de rattrapage

Vous pouvez lancer une commande de nouvelle analyse ciblée sur un élément de configuration, une tâche de rattrapage ou une entrée tierce directement à partir des enregistrements d'entrée d'élément vulnérable, de tâche de rattrapage et de vulnérabilité tierce dans votre ServiceNow AI Platform instance. Tenable appelle cette nouvelle analyse une analyse de **correction**.

Fermer automatiquement les anciens VI

Avec le module Fermer automatiquement les éléments vulnérables périmés dans votre ServiceNow AI Platform, vous pouvez nettoyer les éléments vulnérables plus anciens et périmés (EV) qui n'ont pas été trouvés récemment par vos intégrations tierces. Le déplacement de ces VI vers **Fermé** vous aide à réduire le nombre d'éléments vulnérables actifs et de tâches de rattrapage, et à rapprocher les actifs dans votre CMDB. Vous pouvez utiliser toutes les intégrations avec Vulnerability Response integration with Tenable pour fermer automatiquement les VI périmés.

Instance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce terme fait référence à une occurrence distincte de votre ServiceNow AI Platform® application.

Intégration

Une intégration est une référence spécifique à un produit à une intégration, telle que l'intégration Tenable.io des actifs ou l'intégration des modules d'extension Tenable.sc . Il s'agit des intégrations distinctes qui appartiennent à des produits Tenable spécifiques dans l'intégration de vulnérabilité Tenable de votre instance.

Instance d'intégration

Ce terme fait référence aux intégrations Tenable distinctes répertoriées par leurs Tenable.io et Tenable.sc produits.

Déploiement

Lorsqu'une intégration prend en charge le multisource, une existence d'intégration unique et distincte est appelée un déploiement de votre intégration. Le terme est utilisé pour désigner la ou les intégrations et les produits dans votre environnement. Par exemple, vous pouvez avoir plusieurs déploiements de diverses intégrations de Tenable.io produits dans Tenable.sc votre environnement.

Les Tenable.io intégrations , Tenable.sc, et incluent Tenable.cs également les fonctionnalités clés suivantes :

- Les résultats de l'évaluation de la configuration, c'est-à-dire les résultats des tests ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources faisant autorité peuvent être importés dans l'application Conformité de la configuration avec le Tenable.io produit. Consultez Tenable.io Intégrations avec les Réponse aux vulnérabilités applications et Conformité de la configuration et Explorer Conformité de la configuration pour plus d'informations sur le fonctionnement de cette intégration avec l'application Conformité de la configuration .
- À partir de la version 2.1 de , Tenable Vulnerability Integration créez des éléments de configuration (CI) uniques qui incluent différents identificateurs de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. Identifiez les actifs distincts dans votre environnement et mettez à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous donner plus de détails sur vos vulnérabilités.
- Vous pouvez planifier le moment où vous souhaitez que les tâches s'exécutent pour toutes les Tenable.io intégrations et Tenable.scTenable.cs . Vous pouvez également exécuter des travaux planifiés manuellement à la demande.
- Pour les importations d'actifs avec Tenable.io, vous pouvez activer les balises d'actifs pour organiser et suivre les actifs répertoriés dans CMDB votre Tenable.io environnement.
- Les Tenable.io intégrations de , Tenable.sc et Tenable.cs vous permettent de configurer des règles de recherche de CI pour définir la façon dont les données d'actifs de sources tierces sont utilisées pour identifier les éléments de configuration (CI) dans votre ServiceNow AI Platform CMDB.
- Les Tenable.io intégrations de , Tenable.sc et Tenable.cs vous permettent de définir des filtres d'importation sur l'importation des vulnérabilités afin d'importer uniquement les vulnérabilités de Tenable que vous souhaitez. Pour Tenable.io, vous avez la possibilité d'importer les vulnérabilités **corrigées** de Tenable avec l'importation des vulnérabilités.
- Pour Tenable.sc, vous avez la possibilité de lancer de nouvelles analyses sur demande directement à partir d'un élément vulnérable, d'une tâche de rattrapage et d'enregistrements d'entrée tiers dans votre ServiceNow AI Platform instance. Si les VI sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

passés à **l'état Fermé/Corrigé,** mais ne sont pas encore mis à jour dans votre instance, vous pouvez vérifier que les vulnérabilités sur des éléments de configuration spécifiques ont été corrigées. Consultez Lancer une nouvelle analyse pour l'intégration Tenable.sc.

Les sections suivantes répertorient plus de détails sur les intégrations Tenable.

Rôles ServiceNow AI Platform requis

Les tâches d'intégration nécessitent les rôles suivants dans votre ServiceNow AI Platform instance.

administrateur

L'administrateur système utilise l'assistant de configuration pour installer l'application Vulnerability Response integration with Tenable . S'il n'est pas affecté, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'assistant de configuration.

sn_vul.vulnerability_admin

Une fois affecté, l'administrateur de vulnérabilité termine la configuration des intégrations Tenable dans l'assistant de configuration. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. L'administrateur de vulnérabilité configure toutes les applications et règles de réalité virtuelle pour les intégrations tierces installées.

sn_vul_tenable.configure_integration

Ce rôle contient le rôle granulaire sn_vul_tenable.read_integration et les utilisateurs disposant de ce rôle peuvent configurer l'application Vulnerability Response integration with Tenable .

sn_vul_tenable.read_integration

Les utilisateurs disposant de ces rôles peuvent afficher (lire) mais pas modifier les enregistrements de l'application Vulnerability Response integration with Tenable .

Groupe de réponse aux vulnérabilités

Par défaut, le groupe Réponse aux vulnérabilités est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Réponse aux vulnérabilités héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner.

Éléments vulnérables

Les éléments vulnérables sont regroupés en tâches de rattrapage en fonction des règles de tâche de rattrapage et affectés au rattrapage en fonction de vos règles d'affectation. Pour plus d'informations, consultez Réponse aux vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage et Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Règles de recherche d'éléments de configuration (CI)

Les règles de recherche de CI identifient les CI et déterminent quand les ajouter à un élément vulnérable. Pour en savoir plus sur le fonctionnement des règles de recherche de CI, reportez-vous à la section Règles de recherche de CI pour identifier les éléments de configuration à partir d'intégrations de Réponse aux vulnérabilités vulnérabilité tierces.

Remarque : Une fois supprimées, les règles ne peuvent pas être récupérées. Plutôt que de supprimer les règles existantes, désactivez-les lors de leur création.

Les règles de recherche suivantes Tenable.io sont fournies avec le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- MAC_ADDRESS
- FQDN
- NetBIOS
- Nom d'hôte
- DNS
- IP

Remarque : Les Tenable.io règles de recherche de CI classent par ordre de priorité et renseignent les valeurs d'interface réseau non vides (FDQN, IPV4 et MacAddress) par rapport aux valeurs FDQN, IPV4 et MacAddress normales d'un élément détecté. Lorsque ces valeurs d'interface réseau sont vides, les valeurs FDQN, IPV4 et MacAddress normales sont renseignées pour un élément détecté.

Les règles de recherche suivantes Tenable.sc sont fournies avec le système de base.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Remarque : Plusieurs valeurs pour ip_address, mac_address, FQDN et network_interfaces sont utilisées pour un actif. Toutes les valeurs sont prises en compte dans les règles de recherche de CI pour la mise en correspondance. Toutes les valeurs sont utilisées pour créer plusieurs cartes réseau à l'aide d'IRE.

L'ID Tenable.cs de ressource cloud de règle de recherche est fourni avec le système de base.

Pour plus d'informations sur la configuration de la catégorisation des ressources cloud sans correspondance dans votre classe CI préférée, reportez-vous à la section Mise à jour de la classe CI pour les actifs cloud sans correspondance.

Nouvelles propriétés à ignorer Adresses IP

Dans Tenable.io, deux propriétés sont disponibles si vous souhaitez ignorer plusieurs adresses IP ou plusieurs adresses Mac dans le cadre de vos règles de recherche de CI :

ignoreIPAddress

Une liste d'adresses IP à ignorer pour la recherche et la création de CI.

ignoreMacAddress

Une liste d'adresses MAC à ignorer pour la recherche ou la création de CI.

Éléments découverts

Ce module répertorie les éléments de configuration détectés lors de l'importation à partir des intégrations d'éléments vulnérables Tenable et des intégrations d'actifs Tenable.

Remarque : Le filtre par défaut de cette liste est défini sur Sans correspondance. Vous pouvez afficher tous les éléments détectés à partir d'une importation en supprimant le filtre.

Pour en savoir plus sur le module Éléments détectés, reportez-vous à la section Éléments détectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette d'actifs

Les balises d'actif (également appelées balises d'hôte) sont utilisées pour organiser et suivre les actifs de votre organisation. Vous pouvez affecter des balises à vos actifs. Ensuite, lors du lancement des analyses, vous pouvez sélectionner des balises associées aux ressources que vous souhaitez analyser. Le module Balises d'actifs vous permet de télécharger de manière planifiée des données de balises d'actifs vers Tenable.io votre instance. Les données d'actif qui incluent des balises d'actif sont extraites des cartes de transformation de l'intégration de Tenable.io Asset Transform et transformées à l'aide de Tenable.io ces derniers.

Toutes les balises d'actifs sont importées dans le cadre de l'intégration Tenable.io des actifs. Les balises d'actif sont utilisées pour le filtrage dans les règles d'affectation et les Réponse aux vulnérabilités règles de tâche de rattrapage. Les balises sont affichées dans le formulaire Élément détecté.

Remarque : Exécutez l'intégration Tenable.io des actifs avant de créer Réponse aux vulnérabilités des règles d'affectation ou des règles de tâche de rattrapage dans l'application Réponse aux vulnérabilités afin que toutes les balises soient disponibles pour ces règles avant que les éléments vulnérables ne soient importés et regroupés. Notez également les points suivants concernant les balises :

- Le stockage des balises n'est pas sensible à la casse. Par exemple, si vous créez une balise pour décrire les actifs de votre emplacement à San Diego et que vous créez la balise San Diego , vous ne pouvez pas également créer une balise SAN DIEGO et la stocker dans la table Balise d'actif. San Diego et SAN DIEGO sont considérés comme le même actif par le système. La balise importée en premier est la balise qui est stockée et reconnue à l'avenir.
- L'utilisation de balises d'actifs comme clé de groupe dans une règle de tâche de rattrapage peut avoir des résultats inattendus. Les balises d'actif sont destinées à être utilisées uniquement dans le générateur de conditions.
- Les balises d'actif sont contrôlées par la propriété système globale sn_vul.import_asset_tags. Cette propriété est définie sur vrai par défaut. La désactivation des balises les désactive dans toutes les ServiceNow AI Platform® instances.

Filtres de récupération de données

Les paramètres de récupération de données vous aident à déterminer précisément le type et l'étendue des données que vous souhaitez importer de l'application Tenable vers votre ServiceNow AI Platform® instance. Pour obtenir la liste des paramètres les plus couramment utilisés, reportez-vous à la section Paramètres de récupération de données pour l'intégration de vulnérabilité Tenable.

Évaluation de la priorité de vulnérabilité (VPR)

L'évaluation de priorité de vulnérabilité (VPR) est un attribut du produit Tenable qui est importé et utilisé avec un nouveau calculateur de risque par défaut dans Réponse aux vulnérabilités. La règle de risque Tenable est installée avec l'application dans le Vulnerability Response integration with Tenable cadre du calculateur de risque par défaut dans les calculateurs de vulnérabilité de Réponse aux vulnérabilités.

Cette règle de risque est inactive par défaut.

En activant la règle du calculateur de risque Tenable, les valeurs VPR importées sont utilisées pour calculer le score de risque des éléments vulnérables. La distribution de poids par défaut pour ce calculateur de risque est la suivante : VPR = 70 %, Actif = 15 % et Criticité opérationnelle = 15 %. L'activation de cette règle du calculateur de risque Tenable peut avoir un impact sur vos performances d'ingestion de données. Pour plus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'informations sur Réponse aux vulnérabilités les calculateurs et la règle du calculateur de risque Tenable, reportez-vous à la section Réponse aux vulnérabilités Calculateurs et règles du calculateur de vulnérabilité.

Installation et configuration

Après avoir téléchargé le Vulnerability Response integration with Tenable , l'installation et la ServiceNow® Store configuration sont prises en charge par l'assistant de configuration dans Réponse aux vulnérabilités. Consultez Configuration Réponse aux vulnérabilités à l'aide de l'assistant de configuration pour plus d'informations.

Tenable.io Intégrations avec les Réponse aux vulnérabilités applications et Conformité de la configuration

Les Tenable.io intégrations dans l'application Vulnerability Response integration with Tenable sont disponibles dans les Réponse aux vulnérabilités applications et Conformité de la configuration .

Liste des Tenable.io intégrations

Le multisource est pris en charge pour toutes les Tenable.io intégrations et Tenable.sc . Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'assistant de configuration dans Réponse aux vulnérabilités. Vous installez et configurez également l'application à partir de l'Assistant Vulnerability Response integration with Tenable de configuration.

Tenable.io est une intégration d'entreprise basée sur le cloud. Consultez le tableau suivant pour connaître les noms et les descriptions des intégrations prises en charge pour le Tenable.io produit.

L'intégration Tenable.io des résultats de conformité et l'intégration du Tenable.io remplissage des résultats de conformité sont inactives par défaut.

Pour les activer :

1. Accédez à la **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
2. Dans la liste des intégrations Tenable, cliquez sur un nom d'intégration pour ouvrir l'enregistrement et cochez la case **Actif** pour l'activer. Vous préférez peut-être laisser les paramètres de calendrier dans leurs valeurs par défaut pour que ces intégrations démarrent.

Intégrations de Tenable.io

Intégration	Description
Tenable.io Intégration des actifs	• Récupère toutes les données d'actif, y compris les balises d'actif Tenable.io , à partir du produit et les traite dans votre instance. • À partir de la version 3.0, si l'intégration des résultats de la Tenable.io conformité est activée, vous pouvez importer des données d'évaluation de configuration sécurisée avec les données d'actif importées. Ces données peuvent vous aider à identifier et à répondre aux vulnérabilités liées à la configuration de vos actifs. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de messages REST à l'API d'actif. • Cette intégration génère des éléments détectés. • Les données sont importées en blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. • À partir de la version v2.2, `Last Scan Time` est importé et mis à jour uniquement pour les actifs qui présentent des vulnérabilités.
Tenable.io Intégration des résultats de la conformité	• À partir de la version 3.0, les données d'évaluation de la configuration sécurisée importées à partir de l'intégration des résultats de la conformité, ainsi que les données importées de l'intégration des actifs peuvent vous aider à identifier les vulnérabilités liées à la configuration sur vos actifs et à y répondre. • Si cette option est activée, elle récupère les données d'évaluation de la configuration sécurisée de haut niveau et les traite dans votre ServiceNow AI Platform instance. Les données importées comprennent les résultats des tests ainsi que les politiques, les tests de configuration (contrôles) et les citations avec des sources faisant autorité. • Les données d'évaluation des actifs manquants ou des actifs sans ID d'actif ne sont pas importées. • Si un résultat de test est importé et que son actif correspondant ne peut pas être mis en correspondance dans votre instance, le résultat du test est ignoré et l'ID de l'actif manquant est stocké dans un enregistrement temporaire dans la table [sn_vul_tenable_missing_asset]. • La valeur totale des actifs ignorés (manquants) est répertoriée dans le champ **CI ignorés** de l'onglet **Configuration** de l'enregistrement d'exécution de l'intégration pour cette intégration.
Tenable.io Intégration du remplissage des résultats de la conformité	• Lorsqu'elle est activée, cette intégration s'exécute automatiquement une fois que l'intégration des actifs est terminée avec succès dans le cadre d'une exécution d'intégration chaînée. Cette intégration met en correspondance les données d'évaluation de la configuration avec les actifs manquants répertoriés dans la table [sn_vul_tenable_missing_asset].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	• Importe jusqu'à 200 ID d'actifs pour tous les actifs manquants découverts ou présents dans l'instance une fois l'importation de l'intégration des actifs terminée. • Supprime les enregistrements temporaires de la table [sn_vul_tenable_missing_asset] lorsque les actifs peuvent être mis en correspondance avec les données d'évaluation de la configuration correspondantes.
Tenable.io Intégration des informations d'identification de numérisation	• Cette intégration récupère les informations d'identification de numérisation configurées dans Tenable.io. • Coordonne les appels de messages REST à l'API d'informations d'identification. • La sortie de cette intégration est les informations d'identification de numérisation renseignées dans la table [sn_vul_tenable_scan_credential]. • Les informations d'identification importées sont utilisées pour accéder au scanner lorsque des demandes d'analyse sont lancées à partir de .ServiceNow AI Platform • Cette intégration est planifiée pour s'exécuter chaque semaine.
Tenable.io Intégration de modèles	Un enregistrement de modèle est envoyé lors de la Tenable.io nouvelle analyse. Cette intégration récupère les informations d'identification disponibles Tenable.io à utiliser pour les nouvelles analyses. Les informations d'identification sont spécifiques à l'instance et un enregistrement de modèle unique est importé et stocké temporairement en toute sécurité sur la table [sn_vul_tenable_io_template].
Tenable.io Intégration de module d'extension	• Récupère les données du module d'extension à partir du Tenable.io produit. Les données récupérées sont basées sur la date à laquelle les modules d'extension ont été mis à jour pour la dernière fois par une exécution d'intégration Tenable.io . • Cette importation garantit que les Tenable.io identificateurs (dix ID) sont à jour. • Coordonne les appels de messages REST à l'API du module d'extension. • Le résultat de cette intégration est les vulnérabilités tierces.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
Tenable.io Intégration des vulnérabilités corrigées	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.io produit et les traite dans votre instance. Les éléments vulnérables sont créés pour les enregistrements de détection avec les états **Ouvert** et **Rouvert** , car ces enregistrements requièrent une correction. Les éléments vulnérables existants sont mis à jour par Vulnerability Response si les détections sont **corrigées**, mais les éléments vulnérables ne sont pas créés pour les détections **fixes** par défaut, car Tenable considère que les vulnérabilités **corrigées** sont **atténuées**. • Lorsque le marqueur **Créer des périodes vulnérables pour les détections de vulnérabilité fixes** est activé dans l'Assistant de configuration, de nouveaux VI sont créés à l'état **Fixe** afin que vous ayez une visibilité sur les détections qui les ont créés. Étant donné que les VI sont créés pour des détections **fixes** qui n'existent pas déjà dans votre instance, cela peut avoir un impact négatif sur vos performances d'importation. Vous préférez peut-être laisser cette fonctionnalité désactivée afin que les détections **fixes** ne fassent qu'actualiser les états des éléments vulnérables existants. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de messages REST à l'API de vulnérabilités. • La sortie de cette intégration est Éléments vulnérables (VI) **fermés/corrigés** . Il crée également des actifs et des entrées tierces s'ils n'existent pas. • Les données sont importées en blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. Cette exécution de l'intégration est planifiée. Il s'agit d'une intégration chaînée, ce qui signifie qu'une fois l'exécution terminée avec succès, l'intégration des vulnérabilités ouvertes décrite ci-dessous est déclenchée. À partir de Tenable v3.3, vous pouvez afficher les informations suivantes pour les exécutions d'intégration de vulnérabilité : • **Blocs au total :** Nombre total de blocs générés par Tenable • **Blocs disponibles :** Nombre de blocs disponibles au téléchargement pour ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
Tenable.io Intégration des vulnérabilités ouvertes	• Cette intégration est déclenchée une fois que l'intégration Tenable.io des vulnérabilités corrigées est terminée. • Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.io produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent la même adresse IP. • Coordonne les appels de messages REST à l'API de vulnérabilités. • La sortie de cette intégration est Éléments vulnérables (VI) **nouveaux/rouverts** . Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas. Tenable considère les vulnérabilités actives **cumulatives** (actuelles). • Les données sont importées en blocs et stockées dans la table [sn_vul_tenable_chunk_status]. Le nettoyeur de table supprime automatiquement les données stockées de cette table après 30 jours. À partir de Tenable v3.3, vous pouvez afficher les informations suivantes pour les exécutions d'intégration de vulnérabilité : • **Blocs au total :** Nombre total de blocs générés par Tenable • **Blocs disponibles :** Nombre de blocs disponibles au téléchargement pour ServiceNow
Tenable.io/scan Intégration des métadonnées	Cette intégration récupère les métadonnées à partir du point de terminaison /scans. Il extrait les informations d'analyse en fonction des last_schedule_id des données d'actif existantes dans Tenable.io. L'intégration du point de terminaison /scans à partir de Tenable.io implique les étapes d'implémentation suivantes : • **Création de table** : une nouvelle table personnalisée, **sn_vul_tenable_scan**, est créée pour stocker les métadonnées d'analyse récupérées à partir du Tenable.io point de terminaison /scans. Il s'agit notamment de détails tels que l'ID d'analyse, le nom, l'état, l'heure de début, l'heure de fin et le type d'analyse. • **Association de données** : un champ de référence est établi entre les éléments découverts (éléments de configuration ou vulnérabilités) et le dernier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.io (suite)

Intégration	Description
	enregistrement d'analyse correspondant dans la table **sn_vul_tenable_scan** . Ce couplage vous permet de : ○ Affichez les informations d'analyse les plus récentes associées à chaque élément découvert. ○ Améliorez le contexte pour les décisions de triage et de rattrapage des vulnérabilités. ○ Améliorez la vérifiabilité et les capacités de génération de rapports en conservant un enregistrement historique des activités d'analyse.

Tenable.sc Intégrations avec l'application Réponse aux vulnérabilités

Les Tenable.sc intégrations dans l'application Vulnerability Response integration with Tenable .

Réponse aux vulnérabilités À partir de la version 20.0, si un actif est analysé par un agent, la colonne « L'agent existe » dans la liste des éléments détectés affiche la valeur comme « vrai ». Cela indique que l'analyse est authentique.

Liste des Tenable.sc intégrations

Le multisource est pris en charge pour toutes les Tenable.io intégrations et Tenable.sc . Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'application à partir de l'Assistant Vulnerability Response integration with Tenable de configuration.

- Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le Tenable.sc produit et votre ServiceNow AI Platform instance se trouvent dans le même environnement.
- Si le Tenable.sc produit et votre ServiceNow AI Platform instance ne se trouvent pas dans le même environnement, vous devez utiliser un serveur MID.

Intégrations de Tenable.sc

Intégration	Description
Tenable.sc Intégration des actifs	Pour éviter de créer des éléments détectés en double avec des données d'actifs importées, l'intégration des actifs du Tenable.sc produit comprend deux intégrations. **L'intégration Tenable.sc des actifs ouverts** Cette intégration importe des données de vulnérabilité sur vos actifs que Tenable considère comme **cumulatives** (actuelles) ou **ouvertes**. Les éléments vulnérables (VI) qui sont créés dans votre instance avec ces données d'actif importées sont considérés comme ouverts, c'est-à-dire à l'état **Ouvert** . Ces éléments vulnérables nécessitent une enquête et peuvent nécessiter une correction. **L'intégration Tenable.sc des actifs immobilisés**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	Cette intégration importe les données de vulnérabilité de vos actifs que Tenable considère comme **atténuées** (n'étant plus vulnérables) ou **corrigées**. Les éléments vulnérables de ces actifs passent de l'état **Ouvert** à l'état **Fermé/Fixe** dans votre instance, car les résultats des analyses montrent qu'ils ne sont plus vulnérables. • Récupère toutes les données d'actif du Tenable.sc produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent une adresse IP. • Coordonne les appels de messages REST à l'API Assets. • Cette intégration génère des éléments détectés. • Le filtre de requête Tenable que vous sélectionnez dans l'assistant de configuration s'applique également à l'intégration Tenable.sc des actifs. Seuls les actifs présentant les vulnérabilités qui correspondent aux conditions du filtre de requête sont importés.
Tenable.sc Intégration de module d'extension	• Récupère les données du module d'extension à partir du Tenable.sc produit. Les données récupérées sont basées sur la date à laquelle les modules d'extension ont été mis à jour pour la dernière fois par une exécution d'intégration Tenable.sc . • Cette importation garantit que les Tenable.sc identificateurs (dix ID) sont à jour et que seules les vulnérabilités actives sont importées. • Coordonne les appels de messages REST à l'API des modules d'extension. • Le résultat de cette intégration est les vulnérabilités tierces.
Tenable.sc Intégration des vulnérabilités corrigées	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.sc produit et les traite dans votre instance. Les éléments vulnérables sont créés pour les enregistrements de détection avec les états **Ouvert** et **Rouvert** , car ces enregistrements requièrent une correction. Les éléments vulnérables existants sont mis à jour par Vulnerability Response si les détections sont **corrigées**, mais les éléments vulnérables ne sont pas créés pour les détections **fixes** par défaut, car Tenable considère que les vulnérabilités **corrigéessont atténuées**. • Lorsque le marqueur **Créer des moments vulnérables pour les détections de vulnérabilité fixes** est activé dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	l'Assistant de configuration, il crée des VI à l'état **Fixe** afin que vous ayez une visibilité sur les détections qui les ont créées. Comme des VI sont créés pour des détections **fixes** qui n'existent pas dans votre instance, cela peut avoir un impact négatif sur vos performances d'importation. Vous préférez peut-être laisser cette fonctionnalité désactivée afin que les détections **fixes** ne fassent qu'actualiser les états des éléments vulnérables existants. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent une adresse IP. • Coordonne les appels de messages REST à l'API de vulnérabilités. La sortie de cette intégration est Éléments vulnérables (VI) **fermés/corrigés** . Il crée également des actifs et des entrées tierces s'ils n'existent pas. Cette exécution d'intégration est une exécution planifiée. Il s'agit d'une intégration chaînée, ce qui signifie qu'une fois l'exécution terminée avec succès, l'intégration Tenable.sc des vulnérabilités ouvertes décrite ci-dessous est déclenchée. **Remarque :** Par défaut, les ID de famille 0 et 39 sont exclus de cette intégration.
Tenable.sc Intégration des vulnérabilités ouvertes	• Cette intégration est déclenchée lors de la réussite de l'intégration Tenable.sc des vulnérabilités corrigées. • Récupère les données de vulnérabilité en fonction des filtres de requête sélectionnés dans le Tenable.sc produit et les traite dans votre instance. • Crée les éléments vulnérables correspondants pour les vulnérabilités actives. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants avec l'attribut d'identificateur de partition de réseau pour les actifs de votre environnement qui partagent une adresse IP. • Coordonne les appels de messages REST à l'API de vulnérabilités. • Le résultat de cette intégration est **Mettre à jour/Créer de nouveaux** éléments vulnérables (VI) s'ils n'existent pas. Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.sc (suite)

Intégration	Description
	Remarque : Par défaut, les ID de famille 0 et 39 sont exclus de cette intégration.
Tenable.sc Intégration des informations d'identification de numérisation	• Cette intégration récupère les informations d'identification de numérisation configurées dans Tenable.sc. • Coordonne les appels de messages REST à l'API d'informations d'identification. • La sortie de cette intégration est les informations d'identification de numérisation renseignées dans la table [sn_vul_tenable_scan_credential]. • Les informations d'identification importées sont utilisées pour accéder au scanner lorsque des demandes d'analyse sont lancées à partir de .ServiceNow AI Platform • Cette intégration est planifiée pour s'exécuter chaque semaine.

Tenable.sc Intégration des vulnérabilités de remplissage	• Cette intégration de remplissage importe toutes les vulnérabilités ouvertes et corrigées qui auraient pu être manquées lors d'une importation.
	• Cette intégration importe les vulnérabilités ouvertes et corrigées des sept derniers jours pour mettre à jour vos détections et vos éléments vulnérables.
	• Cette intégration peut avoir un impact sur vos performances.
	• Cette intégration est désactivée par défaut.
	• Pour mettre à jour vos données de vulnérabilité et éviter d'éventuels problèmes de performances, vous pouvez planifier l'exécution des intégrations Tenable.sc Vulnérabilités corrigées et Vulnérabilités ouvertes lorsqu'aucune autre analyse n'est en cours d'exécution.
	• Le résultat de cette intégration est :
	  ○ Éléments vulnérables (VI) **fermés/corrigés**. Il crée également des actifs et des entrées tierces s'ils n'existent pas.
	  ○ **pour mettre à jour/créer de nouveaux** éléments vulnérables (VI) s'ils n'existent pas. Il crée également des éléments de configuration et des entrées tierces s'ils n'existent pas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification utilisateur et Tenable.sc

L'authentification utilisateur est prise en charge par votre instance et la ServiceNow AI Platform®Tenable.sc version 5.13 du produit. L'authentification utilisateur est requise si vous utilisez la version 5.12 et antérieure du Tenable.sc produit.

Lorsque vous sélectionnez l'authentification utilisateur pour les intégrations, les jetons peuvent expirer et être remplacés pendant l'exécution de l'intégration Tenable.sc . Dans la colonne Notes de l'enregistrement d'exécution de l'intégration de vulnérabilité (VIN), le message suivant s'affiche pour un processus lorsqu'un jeton expire, Erreur : la validation du jeton a échoué. Aucune action n'est requise si ce message s'affiche. Les jetons expirés sont automatiquement actualisés en arrière-plan et le message n'indique pas de pause ou d'erreur dans le processus d'intégration.

Tenable.cs Intégrations avec l'application Réponse aux vulnérabilités AND Réponse aux vulnérabilités pour conteneurs

Les Tenable.cs intégrations dans l'application Vulnerability Response integration with Tenable sont disponibles dans Vulnerability Response et Réponse aux vulnérabilités pour conteneurs les applications.

À partir de la version 20.0 Réponse aux vulnérabilités, si un actif est analysé par un agent, la colonne « L'agent existe » dans la liste des éléments détectés affiche « vrai », indiquant que l'analyse est authentique.

Liste des Tenable.cs intégrations

Le multisource est pris en charge pour toutes les Tenable.io intégrations , Tenable.sc et .Tenable.cs Vous pouvez ajouter et déployer plusieurs instances des intégrations suivantes dans votre environnement à partir de l'assistant de configuration dans Réponse aux vulnérabilités. Vous pouvez également installer et configurer l'application à partir de l'Assistant Vulnerability Response integration with Tenable de configuration.

Tenable.cs est une intégration d'entreprise basée sur le cloud. Consultez le tableau suivant pour connaître les noms et les descriptions des intégrations prises en charge pour le Tenable.cs produit.

Intégrations de Tenable.cs

Intégration	Description
Tenable.cs Intégration des actifs de conteneur dans le cloud	• Récupère toutes les données d'actif du conteneur à partir du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants. Coordonne les appels de messages REST à l'API d'actif. La sortie de cette intégration est les images de conteneur détectées, les images Docker et les référentiels de conteneur.
Tenable.cs Intégration ouverte des vulnérabilités du conteneur dans le cloud	Lorsqu'elle est activée, cette intégration s'exécute automatiquement une fois que l'intégration des actifs du conteneur est terminée avec succès dans le cadre d'une exécution d'intégration chaînée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.cs (suite)

Intégration	Description
	• Récupère les données de vulnérabilité du conteneur en fonction des filtres de gravité du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants. • Coordonne les appels de messages REST à l'API de vulnérabilités. La sortie de cette intégration est Éléments vulnérables de conteneur (CVI) nouveaux/réouverts. S'ils n'existent pas, il crée également des images de conteneurs découverts, des images Docker, des référentiels de conteneurs, des résultats d'image, des entrées tierces et des vulnérabilités et expositions courantes (CVE).
Tenable.cs Correction des vulnérabilités du conteneur dans le cloud : intégration	Cette intégration est déclenchée lors de la réussite de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud ouverts. • Récupère les données de vulnérabilité du conteneur en fonction des filtres de gravité du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants • Coordonne les appels de messages REST à l'API de vulnérabilités. Le résultat de cette intégration est Éléments vulnérables de conteneur (CVI) nouveaux/rouverts. S'ils n'existent pas, il crée également des images de conteneur de détection, des images Docker, des référentiels de conteneur, des résultats d'image, des entrées tierces et des CVE. Les résultats d'image sont créés à l'état Fermé.
Tenable.cs Intégration ouverte des vulnérabilités de l'hôte dans le cloud	• Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants. • Coordonne les appels de messages REST à l'API de vulnérabilités. La sortie de cette intégration est Éléments vulnérables (VI) nouveaux/rouverts. S'ils n'existent pas, il crée également des éléments de configuration, des entrées tierces et des CVE. Les détections de vulnérabilité sont créées à l'état ouvert.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations de Tenable.cs (suite)

Intégration	Description
Tenable.cs Intégration des vulnérabilités de l'hôte dans le cloud corrigées	Cette intégration est déclenchée lors de la réussite de l'intégration des vulnérabilités de l'hôte dans le Tenable.cs cloud ouvert. • Récupère les données de vulnérabilité en fonction des filtres de gravité du Tenable.cs produit et les traite dans votre instance. • Crée des CI uniques pour les actifs sans correspondance ou met à jour les CI existants. • Coordonne les appels de messages REST à l'API de vulnérabilités. Le résultat de cette intégration est Fermer les éléments vulnérables (VI). S'ils n'existent pas, il crée également des éléments de configuration, des entrées tierces et des CVE. Les détections de vulnérabilité sont créées à l'état Fermé.

Authentification utilisateur et Tenable.sc

L'authentification utilisateur est prise en charge par votre instance et la ServiceNow AI Platform®Tenable.sc version 5.13 du produit. L'authentification utilisateur est requise si vous utilisez la version 5.12 et antérieure du Tenable.sc produit.

Lorsque vous sélectionnez l'authentification utilisateur pour les intégrations, les jetons peuvent expirer et être remplacés pendant l'exécution de l'intégration Tenable.sc . Dans la colonne Notes de l'enregistrement d'exécution de l'intégration de vulnérabilité (VIN), le message suivant s'affiche pour un processus lorsqu'un jeton expire, Erreur : la validation du jeton a échoué. Si ce message s'affiche, aucune action n'est requise. Les jetons expirés sont automatiquement actualisés en arrière-plan et le message n'indique pas de pause ou d'erreur dans le processus d'intégration.

Préparation à l'intégration de vulnérabilité Tenable

Préparez l'intégration de Tenable ServiceNow® Vulnerability en effectuant les tâches de configuration suivantes.

Avant de commencer

Une intégration réussie nécessite une planification et une exécution minutieuse des tâches préalables à l'intégration. Pour une installation et une configuration fluides de l'application Vulnerability Response integration with Tenable , vous pouvez imprimer la liste de vérification suivante et vérifier que les éléments énumérés sont renseignés avant d'installer l'application et d'importer les données de vulnérabilité dans votre ServiceNow AI Platform® instance.

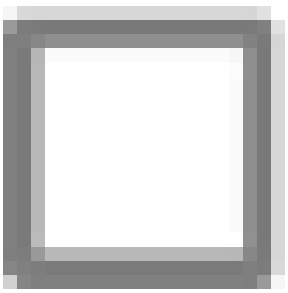
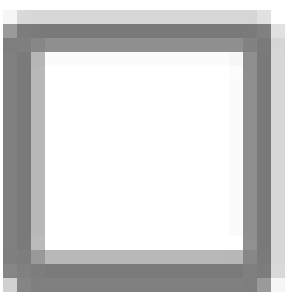
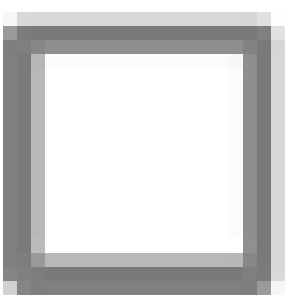
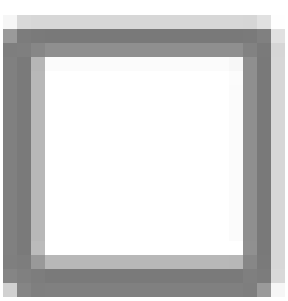
Remarque : Si vous avez importé des données avec l'intégration créée par Tenable et que vous souhaitez commencer à utiliser l'intégration ServiceNow® de réponse aux vulnérabilités avec Tenable, consultez les

Pour obtenir des informations à jour sur le nettoyage des données et la migration de l'intégration créée par Tenable vers l'intégration créée par ServiceNow, consultez les directives de migration de l'intégration Tenable Vulnerability Response vers l'article Intégration ServiceNow Vulnerability Response avec Tenable [KB0960667].

Traduction automatique

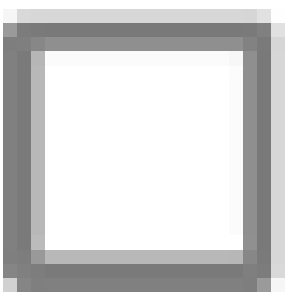
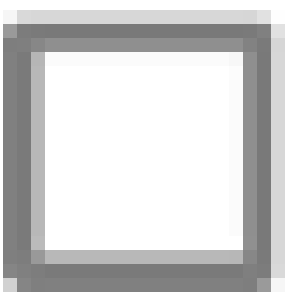
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : administrateur pour télécharger et installer l'application.

Tâche	Description
	(Facultatif) Si elle n'est pas déjà installée et activée, vous préférerez peut-être installer l'application Réponse aux vulnérabilités avant d'installer l'application tierce. Pour plus d'informations sur l'installation et l'activation de l'application, Installer Réponse aux vulnérabilités reportez-vous à la Réponse aux vulnérabilités section . Cette intégration requiert la version 12.1 ou ultérieure Réponse aux vulnérabilités .
	Si vous ne l'avez pas déjà sur votre instance, obtenez des autorisations et téléchargez l'application Vulnerability Response integration with Tenable sur votre ServiceNow AI Platform® instance. L'application Vulnerability Response integration with Tenable prend en charge le produit à partir de la version 5.13 et Tenable.cs le produit à partir de la Tenable.sc version 5.0.1. .
	Estimez le nombre d'éléments vulnérables que vous prévoyez d'importer. Vérifiez que votre instance peut accepter le nombre d'éléments vulnérables que vous prévoyez d'importer. Une instance sous-dimensionnée peut entraîner de longs temps de chargement. Si vous ne connaissez pas la taille de votre instance, ou si vous avez besoin d'aide, contactez ServiceNow® l'assistance technique.
	Vérifiez que vous disposez de groupes ou d'utilisateurs pour gérer les intégrations et corriger les éléments vulnérables. **administrateur** L'administrateur système utilise l'assistant de configuration pour installer l'application Vulnerability Response integration with Tenable . S'il n'est pas affecté, l'administrateur affecte l'administrateur de vulnérabilité (sn_vul.vulnerability_admin) et d'autres rôles dans l'assistant de configuration. **sn_vul.vulnerability_admin** Une fois affecté, l'administrateur de vulnérabilité termine la configuration des intégrations Tenable. Ce rôle dispose d'un accès complet à l'application Réponse aux vulnérabilités (VR) et à ses enregistrements. Configure toutes les applications et règles VR et configure les intégrations tierces. **sn_vul_tenable.configure_integration** Peut configurer l'intégration de vulnérabilité Tenable. Ce rôle contient le rôle granulaire sn_vul_tenable.read_integration.

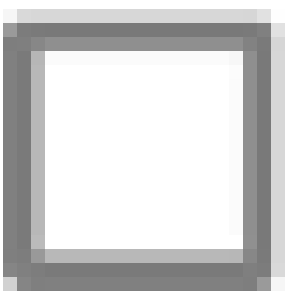
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	sn_vul_tenable.read_integration Peut afficher (lire) les enregistrements de l'intégration de vulnérabilité Tenable. **Groupe de réponse aux vulnérabilités** Par défaut, le groupe Réponse aux vulnérabilités est disponible dans l'Assistant de configuration. Les utilisateurs affectés au groupe Réponse aux vulnérabilités héritent automatiquement des rôles sn_vul.read_all et sn_vul.remediation_owner. L'administrateur système effectue l'affectation initiale des rôles aux utilisateurs et aux groupes dans l'assistant de configuration pour l'intégration. Par défaut, le groupe Vulnerability Response est disponible. Si ce n'est pas déjà fait, vous préférerez peut-être créer des groupes supplémentaires et ajouter des utilisateurs avec le module Administration utilisateurs dans votre instance avant d'utiliser l'Assistant de configuration. Voir Créer un groupe d'utilisateurs . Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.
	Pour améliorer les performances de votre première importation, vous pouvez désactiver certaines fonctionnalités, règles ou travaux dans votre instance. • Désactivez les calculateurs de vulnérabilité si vous ne les utilisez pas. Ces calculateurs, ainsi que ceux que vous avez définis, s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est créé ou mis à jour. Voir Désactiver les calculateurs de vulnérabilité. • Lors de l'importation initiale d'enregistrements, certaines règles métier liées aux notifications peuvent entraîner la génération de nombreuses notifications, ce qui a un impact sur les performances. Avant votre importation initiale, vous préférerez peut-être désactiver les règles métier liées aux notifications, comme décrit dans .Importer des modifications pour l'intégration de vulnérabilité Tenable
	Vérifiez que vous avez activé toutes les fonctionnalités, règles, dépendances, modules d'extension ou tâches dans votre instance requis pour l'intégration. • Tenable.sc est une intégration locale qui vous donne la possibilité d'utiliser un serveur MID si le Vulnerability Response integration with Tenable produit et votre ServiceNow AI Platform instance se trouvent dans le même environnement. Si le Tenable.sc produit et votre ServiceNow AI Platform instance ne se trouvent pas dans le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	même environnement, vous devez utiliser un serveur MID. Pour plus d'informations sur les serveurs MID dans votre instance, consultez Serveur MID . • Vérifiez que le module d'extension Centre d'intégration est installé et activé. Ce module d'extension permet aux composants du système de base d'appeler des systèmes externes à l'aide d'API d'intégration et active les étapes de protocole telles que REST. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous** et localisez le module d'extension. S'il n'est pas installé dans votre instance, installez-le et activez-le.
	Obtenir les informations d'identification Tenable. Vérifiez que vous disposez des noms de compte, mots de passe et autres informations de service requis par vos produits Tenable afin d'y avoir accès. Tenable.io nécessite l'accès Administrateur avec un attribut d'autorisation supérieur ou égal à 64. Tenable.sc nécessite l'accès d'analyste ou de gestionnaire de sécurité. **Remarque :** À partir de la version 3.8 de , l'accès Vulnerability Response integration with TenableTenable.io ne nécessite plus de privilèges d'administrateur. Un utilisateur de base avec un attribut d'autorisation égal à 16 peut également accéder au produit.

Vous êtes prêt à Installer l'application à l'aide de l'assistant Vulnerability Response integration with Tenable de configuration.

Installer l'application à l'aide de l'assistant Vulnerability Response integration with Tenable de configuration

Avant d'exécuter l'intégration ServiceNow® de vulnérabilité Tenable, vous devez télécharger l'application Vulnerability Response integration with Tenable à partir de et ServiceNow Store l'installer et la configurer à l'aide de l'assistant de configuration de l'application Réponse aux vulnérabilités .

Avant de commencer

Avant d'installer l'application Tenable, vérifiez que vous avez rempli tous les éléments de la liste de vérification dans Préparation à l'intégration de vulnérabilité Tenable.

Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Rôles requis : administrateur pour l'affectation initiale du rôle sn_vul.vulnerability_admin et l'installation de l'application Tenable dans l'assistant de configuration. Administrateur de vulnérabilité (sn_vul.vulnerability_admin ou sn_vul.admin (obsolète) pour configurer l'application dans l'Assistant de configuration après son installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration** > **Installation de l'application d'intégration**.

   Après quelques instants, les applications disponibles pour installation sur votre instance s'affichent.

2. Localisez la tuile **Tenable (Tenable Platform)** et cliquez sur **Installer**.

   Cette action installe l'application Vulnerability Response integration with Tenable que vous avez téléchargée à partir du ServiceNow Store.

3. Suivez les instructions fournies dans l'assistant de configuration pour poursuivre l'installation.

4. Pour plus d'informations sur l'installation d'applications à l'aide de l'Assistant de configuration, reportez-vous à la section Installer Réponse aux vulnérabilités des applications tierces à l'aide de l'assistant de configuration.

Que faire ensuite

Une fois l'installation terminée dans l'Assistant de configuration, accédez à **Configuration de l'intégration>Intégrations des scanners dans l'Assistant** de configuration pour poursuivre la configuration. Si vous souhaitez obtenir plus d'informations pour compléter les invites fournies dans l'Assistant de configuration, reportez-vous à la section Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration.

Paramètres de récupération de données pour l'intégration de vulnérabilité Tenable

Les paramètres de récupération de données suivants vous aident à déterminer spécifiquement le type et l'étendue des données que vous souhaitez importer de l'intégration ServiceNow® de vulnérabilité Tenable vers votre ServiceNow AI Platform® instance.

Les paramètres décrits dans les sections suivantes vous aident à contrôler les données que vous souhaitez importer. En outre, vous pouvez définir les valeurs de ces filtres dans les instances d'intégration. Pour afficher les instances d'intégration, accédez à **Intégration de vulnérabilité Tenable** > **Instances d'intégration** et sélectionnez votre intégration, Tenable.io, Tenable.sc ou Tenable.cs.

Sur la page Instance d'intégration qui s'affiche, sélectionnez les paramètres d'instance d'intégration pour afficher une liste de paramètres, ou les onglets Intégrations de vulnérabilité pour un calendrier, les détails REST, les détails de l'intégration, les sources de données et les informations sur l'exécution de l'intégration.

Paramètres et filtres de gravité et de récupération communs pour Tenable.io et Tenable.scTenable.cs dans votre ServiceNow AI Platform instance

Les paramètres suivants sont disponibles pour les Tenable.io intégrations , Tenable.sc et dans Tenable.cs votre ServiceNow AI Platform instance. Ces paramètres de configuration et d'autres sont affichés sur la page Instance d'intégration de votre ServiceNow AI Platform instance. Vous préférez peut-être laisser ces paramètres par défaut pour les premières exécutions d'intégration.

Tenable.io

insert_fixed

Si vous activez le marqueur **insert_fixed** dans l'assistant de configuration pour l'intégration d'importation des vulnérabilités, de nouveaux éléments vulnérables sont créés pour les détections à l'état **Fixe** qui n'existent pas dans votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

severity_critical

Ce filtre est activé par défaut (vrai) pour recevoir les Tenable.io vulnérabilités de gravité critique à partir des intégrations de vulnérabilités ouvertes et Tenable.io de vulnérabilités corrigées.

severity_high

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de gravité élevée à partir des intégrations de Tenable.io vulnérabilités ouvertes et Tenable.io de vulnérabilités corrigées.

severity_medium

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité moyenne à partir des intégrations de Tenable.io vulnérabilités ouvertes et Tenable.io de vulnérabilités corrigées.

severity_info

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité au niveau des informations à partir des Tenable.io intégrations Vulnérabilités ouvertes et Tenable.io Vulnérabilités corrigées.

severity_low

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité faible provenant des intégrations de Tenable.io vulnérabilités ouvertes et Tenable.io de vulnérabilités corrigées.

taille

Ce paramètre définit le nombre d'enregistrements de module d'extension à inclure dans le jeu de résultats de l'intégration des modules d'extension Tenable.io . Doit être au format int32. La valeur par défaut est 1 000. La taille maximale est de 10 000.

num_assets

Le nombre maximal de vulnérabilités par bloc exporté à partir des intégrations de vulnérabilités corrigées et Tenable.io de Tenable.io vulnérabilités ouvertes. La valeur par défaut est 50.

chunk_size

Spécifie le nombre d'actifs par bloc exporté par l'intégration Tenable.io des actifs. La valeur par défaut est 1 000.

Tenable.sc

async_request

Ce paramètre est désactivé par défaut (faux). Activez ou désactivez ce paramètre pour effectuer des appels d'API asynchrones ou synchrones avec Tenable.sc respectivement. Pour les appels synchrones, s'il y a un délai d'expiration de 30 secondes, contactez le support du produit Tenable pour régler la boîte. Ce paramètre, une fois activé, est applicable à toutes les intégrations de Tenable.sc. Pour les clients existants utilisant des appels asynchrones, un script correctif est disponible, qui ajoute un nouveau paramètre async_request aux instances d'intégration existantes Tenable.sc . Pour afficher les scripts correctifs, accédez à **Définition du système** > **Scripts correctifs**.

insert_fixed

Si vous activez le marqueur **insert_fixed** dans l'assistant de configuration pour l'intégration d'importation des vulnérabilités, de nouveaux éléments vulnérables sont créés pour les détections à l'état **Fixe** qui n'existent pas dans votre instance.

décalage

Spécifie le nombre d'actifs, de modules d'extension et de vulnérabilités importés en une seule exécution d'intégration.

Filtres de requête

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les filtres de requête sont configurés à partir de la console Tenable. Ces filtres de requête ont des ID qui peuvent être sélectionnés à partir de l'Assistant de configuration ou de la page Instances d'intégration de votre ServiceNow AI Platform instance. Ces filtres sont appliqués lors de la récupération des données à partir des Tenable.sc intégrations.

Tenable.cs

compute_severity_critical

Ce filtre est activé par défaut (vrai) pour recevoir les vulnérabilités de gravité critique de l'intégration des vulnérabilités de l'hôte dans le cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte dans le Tenable.cs cloud corrigé.

compute_severity_high

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de gravité élevée provenant de l'intégration des vulnérabilités de l'hôte cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte Tenable.cs cloud fixe.

compute_severity_medium

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité moyenne provenant de l'intégration des vulnérabilités de l'hôte cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte Tenable.cs cloud corrigé.

compute_severity_info

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de gravité de niveau d'informations provenant de l'intégration des vulnérabilités de l'hôte cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte Tenable.cs cloud corrigé.

compute_severity_low

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de faible gravité provenant de l'intégration des vulnérabilités de l'hôte cloud ouverte et Tenable.cs de l'intégration des vulnérabilités de l'hôte Tenable.cs cloud fixe.

container_severity_critical

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de conteneur de gravité critique à partir de l'intégration des vulnérabilités des conteneurs dans le cloud ouverts et Tenable.cs de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

container_severity_high

Ce filtre est activé par défaut (vrai) pour recevoir des vulnérabilités de conteneur de gravité élevée à partir de l'intégration des vulnérabilités des conteneurs dans le cloud ouverts et Tenable.cs de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

container_severity_medium

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de conteneur de gravité moyenne à partir de l'intégration des vulnérabilités des conteneurs dans le cloud ouverte et Tenable.cs de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

container_severity_info

Ce filtre est inactif par défaut (faux). Activer ce filtre pour recevoir des vulnérabilités de gravité de niveau d'informations Vulnérabilités du conteneur Vulnérabilités de l'intégration des vulnérabilités des conteneurs dans le cloud ouvert et Tenable.cs intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

container_severity_low

Ce filtre est inactif par défaut (faux). Activez ce filtre pour recevoir des vulnérabilités de conteneur de gravité faible à partir de l'intégration des vulnérabilités des conteneurs dans le cloud ouverte et Tenable.cs de l'intégration des vulnérabilités des conteneurs dans le Tenable.cs cloud corrigés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

asset_page_limit

Ce paramètre définit le nombre d'enregistrements d'actifs de conteneur à inclure dans l'ensemble de résultats de Cloud Tenable.cs Container Assets Integration. La valeur par défaut est 1 000. La taille maximale est de 1 000.

vuln_page_limit

Ce paramètre définit le nombre d'enregistrements de vulnérabilités à inclure dans l'ensemble de résultats de l'intégration des vulnérabilités de l'hôte cloud ouvert, Tenable.cs de l'intégration Tenable.cs des vulnérabilités de l'hôte cloud fixe, de l'intégration des vulnérabilités du conteneur cloud ouvert et Tenable.cs de l'intégration Tenable.cs des vulnérabilités du conteneur cloud fixe. La valeur par défaut est 1 000. La taille maximale est de 10 000.

Messages REST pour l'intégration de vulnérabilité Tenable

Les ServiceNow® messages REST de l'intégration de vulnérabilité Tenable sont utilisés pour effectuer des appels à l'API Tenable.

Tenable.io Message REST sur les actifs

Le Tenable.io message REST Actifs récupère les informations sur les actifs pour l'intégration Tenable.io des actifs. Les changements apportés à l'enregistrement de la méthode de message REST ont un impact sur les demandes de Tenable.io récupération des informations sur les actifs. La tâche d'exportation des actifs est soumise avec les filtres suivants :

- « is_deleted » : faux
- « is_licensed » : vrai

Tenable.io Message REST des modules d'extension

Le Tenable.io message REST Modules d'extension récupère les informations sur le module d'extension pour l'intégration du module d'extension Tenable.io . Les changements apportés à l'enregistrement de la méthode de message REST ont un impact sur les demandes de récupération des informations des modules d'extension Tenable.io .

Tenable.io Message REST de vulnérabilités

Le Tenable.io message REST sur les vulnérabilités récupère les informations sur les vulnérabilités ouvertes et fermées à partir de l'intégration Tenable.io des vulnérabilités. Les changements apportés à l'enregistrement de la méthode de message REST ont un impact sur les demandes de Tenable.io récupération des informations sur les vulnérabilités.

Tenable.sc requêtes du message REST

Le message REST Tenable.sc requêtes récupère les informations du filtre de requête pour l'intégration des actifs Tenable.sc et l'intégration des vulnérabilités Tenable.sc où le filtre de requête est configuré.

Tenable.sc Message REST des modules d'extension

Le Tenable.sc message REST du module d'extension récupère les informations sur le module d'extension pour l'intégration des modules d'extension Tenable.sc . Les changements apportés au message REST Obtenir l'enregistrement de méthode des modules d'extension ont un impact sur les demandes effectuées pour récupérer les informations des modules d'extension Tenable.sc .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Valeur	Description
type	actif	Indique la source à partir de laquelle Tenable extrait les données. Utilisé par le code. Il n'est pas recommandé d'apporter des changements.
champs	id, description, cvssVector,cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, family, riskFactor, cpe, seeAlso, solution, exploitAvailable, exploitFrameworks, type, copyright, version, sourceFile, dependencies, requiredPorts, requiredUDPPorts, srcPort, dstPort,protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	Indique la liste des champs importés de Tenable.

Tenable.sc Message REST de vulnérabilités

Le Tenable.sc message REST de vulnérabilités récupère les informations sur les vulnérabilités à partir de l'intégration Tenable.sc . Les modifications apportées au message REST La méthode Extraire les vulnérabilités ou Extraire les vulnérabilités corrigées ou, à partir des versions 14.0 Réponse aux vulnérabilités et 2.2 de l'intégration de vulnérabilité Tenable, Extraire l'enregistrement des vulnérabilités de remplissage a un impact sur les demandes effectuées Tenable.sc pour récupérer les informations sur les vulnérabilités.

Tenable.sc Message REST des informations d'identification de numérisation

Tenable.sc Message REST de la politique

Le Tenable.sc message POST REST de la politique ajoute une politique pour les modules d'extension demandés. La politique générée est utilisée dans les Tenable.sc demandes d'analyse.

Tenable.sc Analyser le message REST

Le message REST POST de l'analyse Tenable.sc ajoute une analyse qui dépend de l'accès et de l'autorisation définis dans le corps de la demande du message REST. Elle utilise la politique, l'ID du module d'extension et la ou les adresses IP dans le corps de la demande pour la demande d'analyse.

Tenable.sc Message REST du résultat de l'analyse

Le Tenable.sc message REST GET de résultat d'analyse fournit les détails de l'analyse générée à l'aide du message REST d'analyse. Elle utilise scanResultId dans la réponse des messages REST d'analyse et récupère les détails de l'analyse déclenchée.

Tenable.sc Informations d'identification de numérisation

Le Tenable.sc message REST des informations d'identification de numérisation récupère les informations d'identification à partir de Tenable.sc. Les modifications apportées à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'enregistrement de la méthode « Importer » du message REST ont un impact sur les demandes de Tenable.sc récupération des informations d'identification.

Nom de paramètre	Valeur	Description
champs	ID, nom, description, type	Indique la liste des champs importés à partir de Tenable.sc
filtre	utilisable	Indique que l'intégration extrait uniquement les informations d'identification utilisables de Tenable.sc Il n'est pas recommandé de modifier l'un ou l'autre des paramètres.

Tenable.cs Message REST GraphQL : le Tenable.cs message REST GraphQL récupère les informations sur l'actif du conteneur, l'hôte et les informations de vulnérabilité du conteneur pour Tenable.cs l'intégration. Les modifications apportées au message REST Extraire les actifs du conteneur, Extraire les vulnérabilités du conteneur, Extraire les vulnérabilités de calcul Impact de l'enregistrement Tenable.cs de la méthode Impact des demandes effectuées pour récupérer les informations sur les actifs et les vulnérabilités.

Transformation des données pour l'intégration de vulnérabilité Tenable

Une fois que vous avez identifié les données à importer, elles sont récupérées à partir du produit Tenable et traitées via un ensemble de sources de données et transformées dans votre instance.

Lors de l'installation, les cartes de gravité normalisées sont installées dans le module Mappage de gravité normalisée. Ces cartes transforment les niveaux de gravité Tenable importés en niveaux de gravité standard pour le traitement dans votre instance. Pour plus d'informations sur la création de cartes de gravité, consultez Créer une carte de gravité de Vulnerability Response dans la Réponse aux vulnérabilités documentation.

Importation d'actif Tenable.io

Les données d'actif importées sont d'abord chargées dans la table d'importation d'actif Tenable.io [sn_vul_tenable_io_asset_import].

La carte de transformation de l'intégration des actifs Tenable.io est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données de l'importation d'actif Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez Tenable.io transformation d'actif.

La table suivante répertorie les champs de carte de transformation par intégration.

Tenable.io Champs de carte de transformation d'actif

Champ source	Champ cible	Description
u_id	source_id	Tenable fournit un ID unique pour les actifs et les mappe à l'enregistrement de l'élément

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.io Champs de carte de transformation d'actif (suite)

Champ source	Champ cible	Description
		détecté et est utilisé pour la recherche de CI.
u_ipv4s	ip_address	Mappe la première valeur IP au champ ip_address de l'enregistrement de l'élément détecté.
u_mac_addresses	mac_address	Mappe la première valeur mac_address au champ d'adresse mac de l'enregistrement d'élément détecté.
u_fqdns	fqdn	Mappe la première valeur FQDN au champ FQDN de l'enregistrement d'élément détecté.
u_netbios_names	Netbios	Mappe la première valeur NetBIOS au champ NetBIOS de l'enregistrement d'élément détecté.
u_operating_systems	système d'exploitation	Mappe la première valeur du système d'exploitation au champ du système d'exploitation de l'enregistrement de l'élément détecté.
(Avant les versions 14.0 Réponse aux vulnérabilités et 2.2 de l'intégration de vulnérabilité Tenable u_last_scan_time	last_scan_date	Mappé au champ last_scan_date de l'enregistrement de l'élément détecté.
u_last_authenticated_scan_date	last_auth_scan_date	Mappé au champ last_auth_scan_date de l'enregistrement de l'élément détecté.
[script]	nom	Mappe le nom d'hôte à l'aide de la logique du script.
u_tags		Les balises sont enregistrées dans sn_sec_cmn_host_tag. Le mappage des balises aux actifs est enregistré dans sn_sec_cmn_m2m_src_ci_tag.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Tenable.io Transformation de l'actif : script, synchronisation et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Initialise les valeurs du import_set pour le processus d'intégration. Ce script est destiné à un usage interne,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque le script est exécuté	Objectif
	et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Met à jour les valeurs dans l'hôte et vérifie si l'hôte existe. En fonction des résultats, modifie les valeurs d'un import_set. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Définit les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Intégration des modules d'extension Tenable.io

La carte de transformation des modules d'extension Tenable.io est utilisée pour transformer les modules d'extension importés à partir de Tenable.io.

Remarque : Les modifications apportées à cette carte de transformation modifient la façon dont les données reçues des modules d'extension Tenable sont traitées.

Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la transformation du module d'extension Tenable.io.

La charge utile des modules d'extension tenable.io contient tous les champs de la colonne u_attributes de la table sn_vul_tenable_io_plugin_import. Le champ d'attributs est analysé et mappé aux enregistrements de la table d'entrée tierce, tels que répertoriés dans la table suivante.

Champ source	Champ cible	Description
id	id	Mappe l'ID à partir de la source et y ajoute le préfixe TEN. Par exemple, si l'ID reçu est 12345, l'ID dans la table cible est TEN-12345.
Description	résumé	Mappe la description du module d'extension à la colonne de résumé.
[script]	source	La source de l'entrée tierce importée (TPE) est Tenable.io.
[script]	source_instance	Référence au déploiement Tenable qui importe cet enregistrement.
famille	catégorie	Mappe la famille de module d'extension à la colonne de catégorie
plugin_modification_date	last_modified	Mappe le plugin_modification_date au champ de la dernière modification.
plugin_publication_date	date_published	Mappe le plugin_publication_date à la date de publication.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
has_patch	remediation_type	Mappe le type de rattrapage à partir de has_patch valeur.
synopsis	menace	Mappe les informations sur cette vulnérabilité.
cvss_base__score	score	Mappe le score de base du système de notation des vulnérabilités courantes (CVSS) à la colonne de score dans la table d'entrée tierce.
solution	solution	Mappe la solution fournie par le scanner à la colonne de solution dans la table d'entrée tierce.
exploit_available	exploit	Mappe le exploit_available fourni par le scanner à la colonne Exploit dans la table d'entrée tierce.
vpr.score	source_risk_score	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9–10 – Critique • 7–9 – Élevé • 4 à 7 – Moyen • 0–4 : faible
vpr.drivers.age_of_vuln	age_of_vuln	Mappe l'âge de la vulnérabilité du scanner à la colonne age_of_vuln dans la table d'entrée tierce.
vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
vpr.drivers.product_coverage	product_coverage	Mappe la couverture du produit du scanner à product_coverage dans la table d'entrée tierce.
vpr.drivers.threat_sources_last28	threat_sources	Mappe les sources de menace au cours des 28 derniers jours, du scanner au threat_sources dans la table tierce.
vpr.drivers.threat_intensity_last28	threat_intensity	Mappe l'intensité de menace au cours des 28 derniers jours du scanner à la threat_intensity dans la table d'entrée tierce.
vpr.drivers.threat_recency	threat_recency	Mappe les informations sur la récence des menaces du scanner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		à la threat_recency dans la table d'entrée tierce.
vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mappe le score d'impact cvss3 à v3_impact_subscore colonne de la table d'entrée tierce.
cvss_temporal_score	cvss_temporal_score	Mappe le score temporel pour CVSS v2.
cvss_v3_temporal_score	v3_temporal_score	Mappe le score temporel pour CVSS v3.
risk_factor	source_severity	Mappe à la gravité de la source dans la table d'entrée tierce.
nom	nom	Mappe le nom du module d'extension au nom dans la table d'entrée tierce.
stig_severity	stig_severity	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
plugin_type	check_type	Mappe le type de module d'extension à check_type dans la table d'entrée tierce.
unsupported_by_vendor	unsupported_by_vendor	Mappe le champ unsupported_by_vendor à la colonne unsupported_by_vendor.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction du exploit_available et de l'v3_attack_vector des colonnes.

En plus des champs directs, d'autres informations sont ajoutées en tant que listes connexes aux entrées tierces.

Champ source	Description
cve	Insère les données liées à CVE dans la table de référence (sn_vul_nvd_entry). Si les mêmes vulnérabilités et expositions courantes (CVE) dans la table d'entrée NVD (sn_vul_nvd_entry) sont trouvées, elles associent la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
offre	La liste des transactions de bogues est ajoutée à titre de référence.
see_also	La liste des URL est ajoutée en tant que référence.
xrefs	La liste de X-REF est ajoutée à titre de référence.
[script]	Liste des exploits pour ce module d'extension et mappage des insertions pour le cadre de travail de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
	l'exploit et le module d'extension applicables à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Initialise les valeurs du import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Met à jour les valeurs de l'entrée tierce et vérifie si l'entrée tierce existe. En fonction des résultats, modifie les valeurs d'une entrée tierce. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Définit les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

L'include de script TenableIOPluginsImportProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de l'intégration des modules d'extension de Tenable.io et la transforme en ServiceNow AI Platform entrées de vulnérabilité tierces. Tout changement apporté à cet include de script peut altérer la transformation des données des modules d'extension de Tenable.io dans la table d'entrée tierce.

Tenable.io l'importation des vulnérabilités

La carte de transformation d'élément vulnérable Tenable.io est utilisée pour transformer les informations sur les vulnérabilités ouvertes et corrigées importées à partir de Tenable.io.

Remarque : Les changements apportés à cette carte de transformation modifient la façon dont les données de l'importation des vulnérabilités de Tenable sont traitées.

La même carte de transformation est utilisée pour l'intégration des vulnérabilités corrigées Tenable.io et l'intégration des vulnérabilités ouvertes Tenable.io. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la carte de transformation de l'élément vulnérable Tenable.io.

Champ source	Champ cible	Description
u_asset.uuid	id	L'UUID est mappé au champ d'ID de l'enregistrement cmdb_ci.
u_asset.ipv4	ip_address	Le champ ipv4 est mappé au champ d'adresse IP de l'enregistrement cmdb_ci.
u_asset.last_authenticated_results	last_auth_scan_date	La date de la dernière analyse authentifiée est mappée à la date de la dernière

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		analyse d'authentification de l'enregistrement cmdb_ci.
u_asset.mac_addess	mac_address	L'adresse Mac est mappée au champ adresse MAC de l'hôte de l'enregistrement cmdb_ci.
nom_bios u_asset.net	Netbios	NetBIOS est mappé au champ NetBIOS de cmdb_ci enregistrement.
u._plugin.cvss3_base_score	v3_base_score	Le score de base CVSS v3 est mappé au score de base v3 de l'enregistrement d'entrée tierce.
u._plugin.cvss3_score_temporal	v3_temporal_score	Le score temporel CVSS v3 est mappé au score temporel v3 dans l'enregistrement d'entrée tierce.
u._plugin.cvss_score_base	score	Le score de base CVSS est mappé au champ de score de l'enregistrement d'entrée du tiers.
u._plugin.cvss_temporal_score	temporal_score	Le score temporel est mappé au score temporel dans l'enregistrement d'entrée tierce.
u_plugin.description	résumé	La description est mappée au champ Résumé de l'enregistrement d'entrée tierce.
u_plugin.famille	catégorie	Mappe la famille de modules d'extension à la colonne catégorie de l'enregistrement d'entrée tiers.
u_plugin.modification_date	last_modified	La date de la dernière modification est mappée à la date de la dernière modification du module d'extension dans l'enregistrement d'entrée tierce.
u_plugin.publication_date	date_published	La date de publication est mappée au champ de date de publication de l'enregistrement d'entrée tierce.
u_plugin.facteur_risque	source_severity	Le facteur de risque est mappé au champ source_severity de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		l'enregistrement d'entrée tierce.
u_plugin.solution	solution	La solution est mappée au champ de solution de l'enregistrement d'entrée tierce.
u_plugin.synopsis	menace	Synopsis est mappé au champ Menace de l'enregistrement d'entrée tierce.
u_severity_id	Priorité	La priorité est mappée à l'ID de gravité de la charge utile. La valeur par défaut est de 5.
u_plugin.exploit_available	exploit	Mappe le exploit_available fourni par le scanner à la colonne Exploit dans la table d'entrée tierce.
vpr.score	source_risk_score	Mappe le score VPR fourni par le scanner au source_risk_score dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9–10 – Critique • 7–9 – Élevé • 4 à 7 – Moyen • 0–4 : faible
u_plugin.vpr.drivers.age_of_vuln	age_of_vuln	Mappe l'âge de vulnérabilité du scanner à age_of_vuln dans la table d'entrée tierce.
u_plugin.vpr.drivers.exploit_code_maturity	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_plugin.vpr.drivers.product_coverage	product_coverage	Mappe la couverture du produit du scanner à product_coverage dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_sources_last28	threat_sources	Mappe les sources de menace au cours des 28 derniers jours à partir du scanner pour threat_sources dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_intensity_last28	threat_intensity	Mappe l'intensité de menace au cours des 28 derniers jours du scanner à la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		threat_intensity dans la table d'entrée tierce.
u_plugin.vpr.drivers.threat_recency	threat_recency	Mappe les informations sur la récence des menaces du scanner aux threat_recency dans la table d'entrée tierce.
u_plugin.vpr.drivers.cvss3_impact_score	v3_impact_subscore	Mappe le score d'impact CVSS3 v3 à v3_impact_subscore colonne de la table d'entrée tierce.
u_plugin.type	check_type	Mappe le type de module d'extension à check_type dans la table d'entrée tierce.
u_plugin.unsupported_by_vendor	unsupported_by_vendor	Mappe le champ unsupported_by_vendor dans le module d'extension à la colonne unsupported_by_vendor.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction du exploit_available et de l'v3_attack_vector des colonnes.
u_plugin.family_id	Family_id	Mappe l'ID de famille du module d'extension à family_id colonne dans la table d'entrée tierce.
port	port	Le port est mappé au champ port de l'enregistrement d'élément vulnérable.
protocol	protocol	Le protocole est mappé au champ Protocole de l'enregistrement d'élément vulnérable.
u_first_found	first_found	Le premier trouvé est mappé au champ premier trouvé de l'enregistrement d'élément vulnérable.
u_last_found	last_found	Dernier trouvé est mappé au champ Dernier trouvé de l'enregistrement d'élément vulnérable.
u_state	État	L'état est mappé au champ État dans l'enregistrement d'élément vulnérable

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
[script]	source	La source de l'intégration est renseignée. Les éléments vulnérables créés à partir de cette intégration ont Tenable.io comme source.
[script]	integration_instance	Le integration_instance est le nom de l'instance à partir de laquelle l'élément vulnérable est importé.
u_plugin.nom	nom	Mappe le nom du module d'extension au nom dans la table d'entrée tierce.
u_plugin.stig_severity	stig_severity	Mappe la gravité stig du module d'extension à la colonne de gravité stig dans la table d'entrée tierce

En plus des champs directs, d'autres informations sont ajoutées en tant que listes connexes aux entrées tierces.

Champ source	Description
cve	Insère les données liées à CVE dans la table de référence (sn_vul_nvd_entry). Si le même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvé, il associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
offre	La liste des transactions de bogues est ajoutée à titre de référence.
see_also	La liste des URL est ajoutée en tant que référence.
xrefs	La liste de X-REF est ajoutée à titre de référence.
[script]	La liste des exploits pour ce module d'extension et insère le mappage pour le cadre de travail de l'exploit et le module d'extension applicables à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	TTriggers Processeurs de vulnérabilités IO Tenable qui importe les données de Tenable.io à l'aide du jeu d'importation et charge chaque enregistrement dans la table CI CMDB, la table Éléments vulnérables et la table Vulnérabilité tierce. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque le script est exécuté	Objectif
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Vérifie si l'entrée et les détections tierces existent. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. n'est pasCe script est destiné à un usage interne. Il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Met à jour le nombre de CI, de VIT et de détections tels qu'importés à partir de Tenable.io. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Importation d'actif Tenable.sc

Les données d'actif importées à partir de Tenable.sc sont d'abord chargées dans la table d'importation d'actif Tenable.sc (sn_vul_tenable_sc_asset_import). La carte de transformation de l'intégration des actifs Tenable.sc est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données de l'importation d'actif Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez la transformation de l'actif Tenable.sc.

Champ source	Champ cible	Description
u_uuid	id	L'uuid n'est pas renseigné à partir de l'API Tenable, c'est pourquoi l'attribut « u_uniqueness » est utilisé pour créer un champ uuid unique pour les actifs et le mapper à l'enregistrement cmdb_ci.
u_ip	ip_address	Mappe le champ IP de l'API au champ ip_address d'un enregistrement cmdb_ci.
u_macaddress	mac_address	Mappe le champ d'adresse mac de l'API au champ d'adresse de l'enregistrement cmdb_ci.
u_dnsname	fqdn	Mappe le champ dnsname de l'API au champ FQDN sur l'enregistrement cmdb_ci.
u_netbiosname	Netbios	Mappe le champ netbios de l'API au champ netbios sur l'enregistrement cmdb_ci.
u_oscpe	système d'exploitation	Les informations sur le système d'exploitation sont extraites de l'attribut oscpe dans la charge utile et les mappent au champ du système d'exploitation de l'enregistrement cmdb_ci.
u_lastauthrun	last_auth_scan_date	Mappe le champ lastauthrun de l'API au champ last_auth_scan_date de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		l'enregistrement de l'élément détecté.
u_lastauthrun et u_lastunauthrun	last_scan_date	Le lastauthrun est extrait de l'API Tenable ou lastunauthrun. Le champ last_scan_date de l'enregistrement d'élément détecté est renseigné en fonction de la valeur qui apparaît dans la charge utile.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Initialise les valeurs du import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Met à jour les valeurs dans l'hôte et vérifie si l'hôte existe. En fonction des résultats, modifie les valeurs d'un import_set. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Définit les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.sc l'importation des modules d'extension

Les données de modules d'extension importées à partir de Tenable.sc sont d'abord chargées dans la table d'importation de modules d'extension Tenable.sc (sn_vul_tenable_sc_plugin_import). La carte de transformation du module d'extension Tenable.sc est utilisée pour transformer les informations des modules d'extension qui ont été importées. Les changements apportés à cette transformation modifient la façon dont les données provenant de l'importation du module d'extension Tenable sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Recherchez Tenable.sc carte de transformation du module d'extension.

Champ source	Champ cible	Description
u_id	id	Mappe l'ID à partir de la source et ajoute le préfixe TEN. Par exemple, si l'ID reçu est 12345, l'ID dans la table cible est TEN-12345.
u_description	résumé	Mappe la description du module d'extension à la colonne de résumé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
[script]	source	Le TPE importé à partir de cette intégration a Tenable.sc comme source.
[script]	source_instance	Référence au déploiement Tenable qui importe cet enregistrement.
u_family	catégorie	Mappe le champ nom dans l'objet de famille du module d'extension à la colonne catégorie.
u_plugin_modification_date	last_modified	Mappe le plugin_modification_date au champ de la dernière modification.
u_plugin_publication_date	date_published	Mappe le plugin_publication_date à la date de publication.
u_has_patch	Remediation_type	Mappe le type de rattrapage à partir de has_patch valeur.
u_synopsis	menace	Mappe les informations sur cette vulnérabilité.
u_cvss_base_score	score	Mappe le score de base CVSS à la colonne de score dans la table d'entrée tierce.
u_solution	solution	Mappe la solution fournie par le scanner à la colonne de solution dans la table d'entrée tierce.
u_cvss_temporal_score	cvss_temporal_score	Mappe le score temporel pour CVSS v2.
u_cvss_v3_temporal_score	v3_temporal_score	Mappe le score temporel pour CVSS v3.
u_risk_factor	Gravité de la source	Mappe à la gravité de la source dans la table d'entrée tierce.
u_cvss_v3_base_score	v3_base_score	Mappe le score de base CVSS dans la table d'entrée tierce.
u_exploit_available	exploit	Mappe l'exploitAvailable fourni par le scanner à la colonne exploit dans la table d'entrée tierce.
u_vpr_score	source_risk_score	Mappe le score VPR du scanner au score de risque source dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9–10 – Critique • 7–9 – Élevé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		• 4 à 7 – Moyen • 0–4 : faible
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mappe l'âge de la vulnérabilité du scanner à age_of_vuln dans la table d'entrée tierce.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à exploit_code_maturity dans la table d'entrée tierce.
u_vpr_context[id=product_coverage]	product_coverage	Mappe la couverture du produit du scanner à product_coverage dans la table d'entrée tierce.
u_vpr_context[id="threat_sources_last_28"]	threat_sources	Mappe les sources de menace au cours des 28 derniers jours, du scanner au threat_sources dans la table tierce.
u_vpr_context[id="threat_intensity_last_28"]	threat_intensity	Mappe l'intensité de menace au cours des 28 derniers jours du scanner à la threat_intensity dans la table d'entrée tierce.
u_vpr_context[id="threat_recency"]	threat_recency	Mappe les informations sur la récence des menaces du scanner à threat_recency dans la table d'entrée de tiers.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mappe le score d'impact CVSS v3 du scanner à v3_impact_subscore dans la table d'entrée tierce.
u_name	nom	Mappe le nom du module d'extension à la colonne nom dans la table d'entrée tierce.
u_stig_severity	stig_severity	Mappe le champ stig_severity dans le module d'extension à stig_severity dans la table d'entrée tierce.
u_check_type	check_type	Mappe le type de vérification à check_type dans la table d'entrée tierce.
u_family.id	family_id	Mappe le module d'extension family_id à family_id dans la table d'entrée tierce.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table d'entrée tierce est renseignée en fonction du exploit_available et de l'v3_attack_vector des colonnes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En plus des champs directs, d'autres informations sont ajoutées en tant que listes connexes aux entrées tierces.

Champ source	Description
u_cpe	La liste des CPE est ajoutée à titre de référence.
u_see_also	La liste des URL est ajoutée en tant que référence.
u_exploit_frameworks	Liste des exploits pour ce module d'extension et mappage des insertions pour le cadre de travail de l'exploit et le module d'extension applicables à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Cette transformation permet d'initialiser les valeurs dans le import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Fonction utilisée pour mettre à jour les valeurs de l'entrée tierce et vérifier si l'entrée tierce existe. En fonction des résultats, modifie les valeurs d'une entrée tierce. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des modules d'extension créés et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

L'include de script TenableSCPluginsImportProcessor est appelé à partir du script de transformation onBefore. Il prend la sortie de l'intégration des modules d'extension Tenable.sc et la transforme en ServiceNow entrées de vulnérabilité tierces. Toute modification apportée à cet include de script peut altérer la transformation des données des modules d'extension de Tenable.sc dans la table d'entrée tierce.

Tenable.sc l'importation des vulnérabilités

La carte de transformation des vulnérabilités ouvertes Tenable.sc est utilisée pour transformer les données importées à partir de l'intégration des vulnérabilités ouvertes Tenable.sc, et la carte de transformation des vulnérabilités Tenable.sc et corrigées est utilisée pour transformer les données importées à partir de l'intégration des vulnérabilités corrigées Tenable.sc.

Remarque : Les changements apportés à ces cartes de transformation modifient la façon dont les données de l'importation de vulnérabilités Tenable corrigées/ouvertes sont traitées.

Pour accéder aux Tenable.sc cartes de transformation des vulnérabilités ouvertes et corrigées, accédez à **Intégration de vulnérabilité Tenable** > **Administration** > **Instances d'intégration** > **Tenable.sc l'intégration des vulnérabilités corrigées/ouvertes** > **Sources de données** > **Tenable.sc vulnérabilités ouvertes/corrigées** > **Les transformations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_pluginID	ID	Utilisé comme identificateur du module d'extension. Ce champ est mappé à l'ID du module d'extension dans l'enregistrement d'entrée tierce.
u_riskfactor	source_severity	Ce champ est mappé à source_severity dans l'enregistrement d'entrée tierce.
u_severity	Priorité	Le champ de priorité est mappé avec la gravité. La valeur par défaut est de 5.
u_hasbeenmitigated	État	A été atténué est mappé au champ d'état de l'enregistrement de vulnérabilité. Pour l'intégration des vulnérabilités corrigées, tous les VI sont à l'état « Fermé ».
u_ip	ip_address	L'adresse IP est mappée au champ IP de l'hôte de cmdb_ci table.
u_port	port	Le port est mappé au champ port de l'enregistrement d'élément vulnérable.
u_protocol	protocol	Le protocole est mappé au champ de port de l'enregistrement d'élément vulnérable.
u_firstSeen	first_found	La première valeur vue est mappée au premier champ trouvé de l'enregistrement de VI.
u_lastSeen	last_found	La dernière valeur vue est mappée au champ dernier trouvé de l'enregistrement de VI.
u_exploitAvailable	exploit	ExploitAvailable est mappé au champ d'exploit dans l'enregistrement d'entrée tierce.
u_synopsis	menace	Synopsis est mappé au champ Menace dans l'enregistrement d'entrée tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_description	résumé	La description est mappée au champ Résumé de l'enregistrement d'entrée tierce.
u_solution	solution	La solution est mappée au champ Solution dans l'enregistrement d'entrée tierce.
u_basescore	score	BaseScore est mappé au champ de score dans l'enregistrement d'entrée tierce.
u_temporalScore	temporal_score	Le score temporel est mappé au score temporel dans l'enregistrement d'entrée tierce.
u_cvssv3basescore	v3_base_score	Cvssv3basescore est mappé au score de base v3 dans l'enregistrement d'entrée tierce.
u_cvsstemporalscore	v3_temporal_score	Le score temporel Cvssv3 est mappé au score temporel v3 dans l'enregistrement d'entrée tierce.
u_pluginpubdate	date_published	La date de publication du module d'extension est mappée à la date de publication du module d'extension dans l'enregistrement d'entrée tiers.
u_pluginmoddate	last_modified	La date de la dernière modification est mappée à la date de la dernière modification du module d'extension dans l'enregistrement d'entrée tierce.
u_dnsname	fqdn	DnsName est mappé au champ FQDN de l'enregistrement cmdb_ci.
u_macaddress	mac_address	MacAddress est mappé au champ mac_address de l'enregistrement cmdb_ci.
u_netbiosName	Netbios	NetbiosName est mappé au champ NETBIOS de l'enregistrement cmdb_ci.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
u_ip	ip	L'adresse IP est mappée au champ IP de cmdb_ci enregistrement.
hostUniqueness	uuid	L'unicité de l'hôte n'est mappée à aucun champ, mais est utilisée pour déterminer l'uuid de l'hôte.
u_family	catégorie	Mappe le champ nom de l'objet famille du module d'extension à la colonne catégorie de l'enregistrement d'entrée tierce.
u_plugintext	proof	Le texte du module d'extension est mappé à la preuve dans l'enregistrement TPE.
[script]	source	La source de l'intégration est renseignée. Les éléments vulnérables créés à partir de cette intégration ont Tenable.sc comme source.
[script}	integration_instance	Le integration_instance est le nom de l'instance à partir de laquelle l'élément vulnérable est importé.
u_vpr_score	source_risk_score	Mappe le score VPR du scanner au score de risque source dans la table d'entrée tierce.
[script]	source_risk_rating	Mappe le score VPR à la cote de risque standard en fonction des plages de scores : • 9 - 10 – Critique • 7 – 9 – Élevé • 4 à 7 – Moyen • 0–4 : faible
u_vpr_context[id=age_of_vuln]	age_of_vuln	Mappe l'âge de la vulnérabilité du scanner à age_of_vuln dans la table d'entrée tierce.
u_vpr_context[id=exploit_code_maturity]	exploit_code_maturity	Mappe la maturité du code d'exploitation du scanner à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Champ cible	Description
		exploit_code_maturity dans la table d'entrée tierce.
u_vpr_context[id=product_coverage]	product_coverage	Mappe la couverture du produit du scanner à product_coverage dans la table d'entrée tierce.
u_vpr_context[id="threat_sources_last_28]	threat_sources	Mappe les sources de menace au cours des 28 derniers jours, du scanner aux threat_sources dans la table tierce.
u_vpr_context[id="threat_intensity_last_28]	threat_intensity	Mappe l'intensité de menace au cours des 28 derniers jours du scanner à la threat_intensity dans la table d'entrée tierce.
u_vpr_context[id="threat_recency"]	threat_recency	Mappe les informations sur la récence des menaces du scanner à threat_recency dans la table d'entrée de tiers.
u_vpr_context[id=cvssV3_impactScore]	v3_impact_subscore	Mappe le score d'impact CVSS v3 du scanner à v3_impact_subscore dans la table d'entrée tierce.
u_pluginname	nom	Mappe le nom du module d'extension à la colonne de nom dans la table d'entrée tierce.
u_stigseverity	stig_severity	Mappe le champ stig_severity dans le module d'extension à stig_severity dans la table d'entrée tierce.
u_checktype	check_type	Mappe le type de vérification à check_type dans la table d'entrée tierce.
u_family.id	family_id	Mappe le module d'extension family.id à family_id dans la table d'entrée tierce.
[script]	exploit_attack_vector	La colonne exploit_attack_vector de la table third_party_entry est renseignée en fonction de la exploit_available et de la v3_attack_vector des colonnes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ source	Description
u_cve	Insère les données liées à CVE dans la table de référence (sn_vul_nvd_entry). Si le même CVE dans la table d'entrée NVD (sn_vul_nvd_entry) est trouvé, il associe la vulnérabilité actuelle à l'entrée NVD. Le mappage se trouve dans sn_vul_m2m_entry_cve.
u_bid	La liste des transactions de bogues est ajoutée à titre de référence.
u_cpe	La liste des CPE est ajoutée à titre de référence.
u_seealso	La liste des URL est ajoutée en tant que référence.
u_xrefs	La liste des X-REF est ajoutée à titre de référence.
u_exploitframeworks	La liste des exploits pour ce module d'extension et insère le mappage pour le cadre de travail de l'exploit et le module d'extension applicables à sn_vul_m2m_framework_vul.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Cette transformation permet d'initialiser les valeurs dans le import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Fonction utilisée pour mettre à jour les valeurs de la vulnérabilité et vérifier si la vulnérabilité existe. En fonction des résultats, modifie les valeurs d'une table d'éléments vulnérables. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux VI créés et des VI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.cs Importation d'actif de conteneur

Les données d'actif importées sont d'abord chargées dans la table d'importation d'actif Tenable.cs de conteneur [sn_vul_tenable_cs_container_asset_import].

La Tenable.cs carte de transformation d'actif de conteneur est utilisée pour transformer les informations sur les actifs importés. Les changements apportés à cette transformation modifient la façon dont les données de l'importation d'actif de Tenable.cs conteneur sont traitées. Pour accéder à cette carte de transformation, accédez à Jeux d'importation système > Cartes de transformation. Recherchez la transformation de Tenable.cs l'actif de conteneur.

Les tables suivantes répertorient les champs de carte de transformation par intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation d'actif de conteneur

Champ source	Champ cible	Description
u_digest	Image_id	Tenable fournit une synthèse unique pour les actifs du conteneur et est mappé à l'image du conteneur détecté et à l'enregistrement de l'image Docker. Il est utilisé pour la recherche de CI.
u_digest	Image_digest	Tenable fournit une synthèse unique pour les actifs du conteneur et est mappé à l'image du conteneur détecté et à l'enregistrement de l'image Docker. Il est utilisé pour la recherche de CI.
u_name	nom	Mappé au champ de nom de l'enregistrement d'image Docker.
u_repositoryuri	nom	Mappé à l'enregistrement du référentiel du conteneur
u_repositoryuri	réf.	Mappe à l'enregistrement d'image du conteneur détecté.
u_virtualmachines	host_list	Mappe à l'enregistrement d'image du conteneur détecté
u_labels	Image_labels	Mappe la première valeur du système d'exploitation au champ de système d'exploitation de l'enregistrement de l'élément détecté.
u_clusters	image_cluster	Mappe à l'enregistrement d'image du conteneur détecté
u_imagetags	balises	Mappe à l'enregistrement d'image du conteneur détecté
u_cloudprovider	cloud_providers	Mappe à l'enregistrement d'image du conteneur détecté
u_accountid	cloud_account_ids	Mappe à l'enregistrement d'image du conteneur détecté
u_region	cloud_regions	Mappe à l'enregistrement d'image du conteneur détecté
u_operatingsystem	système d'exploitation	Mappe à l'enregistrement d'image du conteneur détecté
u_scantime	last_scan_date	Mappe à l'enregistrement d'image du conteneur détecté

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Actif conteneur, carte de transformation, script, minutage et objectif

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Cette transformation permet d'initialiser les valeurs dans le import_set pour le processus d'intégration. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Fonction utilisée pour mettre à jour les valeurs de l'hôte et vérifier si l'hôte existe. En fonction des résultats, modifie les valeurs d'un import_set. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Cette transformation est utilisée pour définir les valeurs des nouveaux CI créés et des CI qui ont été mis à jour et ignorés. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.cs Importation de vulnérabilité du conteneur

Les données de vulnérabilité du conteneur importées sont d'abord chargées dans la table d'importation de vulnérabilité du Tenable.cs conteneur [sn_vul_tenable_cs_container_vuln_import].

La Tenable.cs carte de transformation de vulnérabilité du conteneur est utilisée pour transformer les informations de vulnérabilité du conteneur importé. Les changements apportés à cette transformation modifient la façon dont les données de l'importation Tenable.cs de vulnérabilité de conteneur sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Cartes de transformation**. Tenable.cs Recherchez Transformation de vulnérabilité de conteneur.

Les tableaux suivants répertorient les champs de carte de transformation par intégration.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur

Champ source	Champ cible	Description
[script]	Image_id	La synthèse est extraite du champ Resource.Id de l'API et mappée au champ de image_id'image du conteneur détecté et de l'enregistrement de l'image Docker.
[script]	Image_digest	La synthèse est extraite du champ Resource.Id de l'API et mappée au champ de image_digest'image du conteneur découvert et de l'enregistrement de l'image Docker.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
[script]	nom	Les informations du référentiel sont extraites du champ de nom et mappées à l'image Docker et à l'enregistrement du référentiel du conteneur.
[script]	réf.	Les informations du référentiel sont extraites du champ de nom et mappées pour détecter l'enregistrement d'image du conteneur.
u_resource. Étiquettes	Image_labels	Mappe à l'enregistrement d'image du conteneur détecté
u_resource. Fournisseur de cloud	cloud_providers	Mappe à l'enregistrement d'image du conteneur détecté
u_resource. AccountId	cloud_account_ids	Mappe à l'enregistrement d'image du conteneur détecté
u_resource. Région	cloud_regions	Mappe à l'enregistrement d'image du conteneur détecté
u_vulnerability. ID	id	Mappe l'ID à partir de la source et ajoute le préfixe TEN-. Par exemple, si l'ID reçu est 12345, l'ID dans la table d'entrée tierce est TEN-12345.
u_vulnerability. Description Id	ID résumé	Mappe à l'enregistrement d'entrée du tiers. ou un enregistrement CVE.
u_vulnerability. Sévérité	v4_base_severity	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Score VPR	source_risk_score	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Gravité VPR	source_severity	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Vecteur d'attaque	v4_attack_vector	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Maturité de l'exploit	v4_exploit_maturity	Mappe à l'enregistrement d'entrée du tiers.
[script]	source	La source pour le TPE importé est Tenable.cs.
u_vulnerability. Id	nom	Mappé à l'enregistrement des références de vulnérabilité
u_vulnerability. Liens	URL	Mappé à l'enregistrement des références de vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
	vulnerability	Référence de TPE ou CVE dans l'enregistrement des références de vulnérabilité
u_software. Nom	nom	Mappé à l'enregistrement du package d'images du conteneur
u_software. Version	version	Mappé à l'enregistrement du package d'images du conteneur
u_software. Type	package_type	Mappé à l'enregistrement du package d'images du conteneur
u_softwarepaths	chemin d'accès	Mappé à l'enregistrement du package d'images du conteneur
u_resolved	état	Mappé à l'enregistrement de résultat d'image du conteneur
u_firstscantime	first_found	Mappé à l'enregistrement de résultat d'image du conteneur
u_resource. Analyser l'heure	last_found	Mappé à l'enregistrement de résultat d'image du conteneur
u_vulnerability. Description	proof	Mappé à l'enregistrement de résultat d'image du conteneur
u_resolved	État	Mappé à l'enregistrement de l'élément vulnérable du conteneur
u_firstscantime	first_found	Mappé à l'enregistrement de l'élément vulnérable du conteneur
u_resource. Analyser l'heure	last_found	Mappé à l'enregistrement de l'élément vulnérable du conteneur
[script]	source	La source de l'enregistrement d'élément vulnérable de conteneur est Tenable.cs.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Tenable.cs Vulnérabilité du conteneur : synchronisation et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Déclenche les vulnérabilités du conteneur TenableCS Processeur qui importe les données à partir de l'utilisation du Tenable.cs jeu d'importation et charge chaque enregistrement dans la table CI CMDB, la table Élément vulnérable, la table Entrée de vulnérabilité tierce, la table Référence de vulnérabilité, le package d'images de conteneur, le résultat d'image de conteneur et l'élément vulnérable

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Vulnérabilité du conteneur : synchronisation et objectif du script de carte de transformation (suite)

Lorsque le script est exécuté	Objectif
	de conteneur. Il n'est pas recommandé de modifier ou de supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation)	Vérifie si les conclusions d'entrée et d'image tierces existent. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation)	Met à jour le nombre de CI, de VIT et de conclusions tels qu'importés à partir de Tenable.cs. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.cs Importation de la vulnérabilité de calcul

Les données de vulnérabilité de l'hôte importées sont d'abord chargées dans la table d'importation de Tenable.cs vulnérabilité de calcul [sn_vul_tenable_cs_compute_vuln_import].

La Tenable.cs carte de transformation Vulnérabilité de calcul est utilisée pour transformer les informations de vulnérabilité de l'hôte importé. Les changements apportés à cette transformation modifient la façon dont les données de l'importation Tenable.cs de vulnérabilité de calcul sont traitées. Pour accéder à cette carte de transformation, accédez à **Ensembles de données à importations système** > **Ensembles de données à importations système**. Tenable.cs Recherchez Transformation de vulnérabilité de calcul.

La table suivante répertorie les champs de carte de transformation par intégration.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur

Champ source	Champ cible	Description
u_resource. Id	object_id	Mappé à l'enregistrement CI CMDB.
u_resource. Nom	nom	Mappé à l'enregistrement CI CMDB.
	asset_category	Le cloud est mappé en tant que catégorie d'actif dans l'enregistrement de l'élément détecté.
U_resource. Fournisseur de cloud	cloud_service_provider	Mappé à l'enregistrement de l'élément détecté
u_resource. Région	cloud_region	Mappé à l'enregistrement de l'élément détecté
u_resource. ID de compte	cloud_account	Mappé à l'enregistrement de l'élément détecté
u_resource. CloudProvider	cloud_resource_type	Mappé à l'enregistrement de l'élément détecté

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
u_resource. Id	resource_id	Mappé à l'enregistrement de l'élément détecté
u_resource. Nom	resource_name	Mappé à l'enregistrement de l'élément détecté
u_vulnerability. Id	id	Mappe l'ID à partir de la source et ajoute le préfixe TEN-. Par exemple, si l'ID reçu est 12345, l'ID dans la table d'entrée tierce est TEN-12345. Mappe également l'ID aux CVE.
u_vulnerability. Description	résumé	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Sévérité	v4_base_severity	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Score VPR	source_risk_score	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Gravité VPR	source_severity	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Vecteur d'attaque	v4_attack_vector	Mappe à l'enregistrement d'entrée du tiers.
u_vulnerability. Maturité de l'exploit	v4_exploit_maturity	Mappe à l'enregistrement d'entrée du tiers.
[script]	source	La source du TPE importé est Tenable.cs.
u_vulnerability. Id	nom	Mappé à l'enregistrement des références de vulnérabilité
u_vulnerability. Liens	URL	Mappé à l'enregistrement des références de vulnérabilité
	vulnerability	Référence de TPE ou CVE dans l'enregistrement des références de vulnérabilité
u_resolved	état	Mappé à l'enregistrement de détection d'éléments vulnérables
u_firstscantime	first_found	Mappé à l'enregistrement de détection d'éléments vulnérables
u_resource. Analyser l'heure	last_found	Mappé à l'enregistrement de détection d'éléments vulnérables
u_softwarepaths	proof	Mappé à l'enregistrement de détection d'éléments vulnérables

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
u_softwareresolutionversions	solution_summary	Mappé à l'enregistrement de détection d'éléments vulnérables
u_resolved	État	Mappé à l'enregistrement d'élément vulnérable
u_firstscantime	first_found	Mappé à l'enregistrement d'élément vulnérable
u_resource. Analyser l'heure	last_found	Mappé à l'enregistrement d'élément vulnérable
[script]	source	La source de l'enregistrement d'élément vulnérable est Tenable.cs.

Trois scripts de transformation sont exécutés au cours du processus de transformation. La table suivante répertorie l'exécution de chaque script et son objectif.

Tenable.cs Vulnérabilité de calcul, synchronisation et objectif du script de carte de transformation

Lorsque le script est exécuté	Objectif
onStart (lorsqu'un jeu d'importation a commencé la transformation)	Déclenche le processeur de vulnérabilités de calcul Tenable CS qui importe les données à l'aide du Tenable.cs jeu d'importation et charge chaque enregistrement dans la table CI CMDB, la table Éléments vulnérables et la table Vulnérabilité tierce. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onBefore (avant qu'un jeu d'importation n'ait terminé la transformation).	Vérifie si l'entrée et les détections tierces existent. Dans le cas contraire, ces enregistrements sont créés dans leurs tables respectives. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.
onComplete (lorsqu'un jeu d'importation a terminé la transformation).	Met à jour le nombre de CI, de VIT et de détections tels qu'importés à partir de Tenable.cs. Ce script est destiné à un usage interne, et il n'est pas recommandé de le modifier ou de le supprimer.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur

Champ source	Champ cible	Description
u_digest	Image_id	Une synthèse unique fournie par Tenable pour les actifs du conteneur. Il est mappé à l'image du conteneur découvert et à l'enregistrement de l'image Docker et est utilisé pour la recherche de CI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tenable.cs Champs de carte de transformation vulnérabilité du conteneur (suite)

Champ source	Champ cible	Description
u_name	nom	Mappé au champ de nom de l'enregistrement d'image Docker.

Définir des paramètres de filtre supplémentaires pour Tenable.io les importations

Personnalisez les paramètres de filtrage de vos requêtes planifiées avec le Tenable Vulnerability Integration pour vous aider à affiner davantage les données de vulnérabilité que vous importez avec le Tenable.io produit.

Avant de commencer

Cas d'utilisation : en tant que responsable ou analyste des vulnérabilités, vous souhaiterez peut-être filtrer les données de vos requêtes afin de ne pouvoir examiner que des détails spécifiques de la vulnérabilité. Par exemple, supposons que vous souhaitiez afficher les vulnérabilités importées qui sont filtrées par `cidr_range`, `num_assets`, `indexed_at`et `plugin_family`. Ou supposons que vous souhaitiez exécuter une Tenable.io intégration de telle sorte qu'une exécution importe uniquement les vulnérabilités critiques toutes les quatre heures et qu'une autre s'exécute toutes les 24 heures pour extraire toutes les autres vulnérabilités non critiques.

Pour vous aider à collecter ces données, vous pouvez ajouter des paramètres pris en charge par Tenable pour vous aider à importer les détails de vulnérabilité spécifiques dont vous avez besoin.

Sans ajouter d'appels d'API ou de codage supplémentaires, cette fonctionnalité vous permet de personnaliser vos informations de requête HTTP avec les paramètres Tenable dans votre ServiceNow AI Platform. Les intégrations suivantes Tenable.io prennent en charge le filtrage en fournissant du contenu JSON dans le corps de la demande :

- Intégration des actifs
- Intégration de vulnérabilité corrigée
- Intégration des vulnérabilités ouvertes

Vous devez savoir comment utiliser JSON les chaînes pour cette fonctionnalité.

Rôle requis : sn_vul.vulnerability_admin

Procédure

1. Recherchez les paramètres pris en charge par le Tenable.io produit sur le site développeur que vous souhaitez utiliser pour votre filtrage.

   Les paramètres et les valeurs que vous saisissez à partir du Tenable.io produit ne sont pris en charge qu'au niveau de l'instance d'intégration.

2. Accédez à la **Tous** > **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
3. Sur la page de liste Intégrations Tenable, cliquez sur l'enregistrement de l'intégration Tenable.io que vous souhaitez ouvrir.
4. Une fois l'onglet Méthodes REST Tenable sélectionné, cliquez sur l'icône d'informations (I) de la méthode REST, puis sur **Ouvrir l'enregistrement**.
5. Sélectionnez l'onglet **de demande HTTP** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Pour modifier l'enregistrement, en haut de la page, cliquez sur le lien dans Pour modifier l'enregistrement, cliquez **ici**.
7. Dans le champ Contenu de l'enregistrement Méthode REST, saisissez le contenu JSON que vous souhaitez inclure dans le corps de la demande.

   Par exemple, vous pouvez définir le paramètre de gravité pour les vulnérabilités importées comme, `{"filters": {"severity": ["critical"]}}` pour l'intégration Tenable.io des actifs afin qu'elle importe uniquement les vulnérabilités critiques (score CVSS de 10,0).

   Si vous souhaitez entrer plusieurs paramètres, consultez la documentation pour plus d'informations sur la Tenable.io façon de séparer chaque valeur.
8. Cliquez sur **Mettre à jour**.

Génération de rapports sur l'intégration de vulnérabilité Tenable

Affichez les rapports sur les vulnérabilités et les éléments vulnérables sur les tableaux de Réponse aux vulnérabilités bord.

Visualisations de données dans les Réponse aux vulnérabilités espaces de travail

Les Réponse aux vulnérabilités espaces de travail incluent des visualisations de données qui peuvent vous aider à surveiller la progression de votre rattrapage. Vous pouvez déterminer le niveau de menace pour votre organisation en affichant le nombre et la gravité des vulnérabilités actives qui sont importantes pour votre organisation sur des visualisations de données dynamiques qui sont mises à jour à mesure que les données de vulnérabilité changent. Consultez Réponse aux vulnérabilités Espaces de travail et Exploration de l'Espace de travail du gestionnaire de vulnérabilitésExploration de l'Espace de travail de remédiation IT pour plus d'informations sur les visualisations de données dynamiques disponibles.

Versions précédentes de Réponse aux vulnérabilités

Le tableau de bord de vue d'ensemble de Réponse aux vulnérabilités (Gestion de la vulnérabilité) fournit une vue d'ensemble des vulnérabilités et des éléments vulnérables, ce qui aide l'administrateur des vulnérabilités à identifier rapidement les zones de préoccupation. Le tableau de bord de rattrapage de Vulnerability Response (Vulnerability Remediation) permet à un spécialiste du rattrapage de se concentrer sur les tâches de rattrapage et les éléments vulnérables qu'il possède.

Consultez Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités pour plus d'informations.

Rôle requis : propriétaire du rattrapage.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher le tableau de bord, accédez à **Réponse aux vulnérabilités** > **Aperçu du rattrapage**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Graphique de l'état d'exécution de l'intégration pour l'intégration de vulnérabilité Tenable

Le module État de l'exécution de l'intégration Tenable vous fournit une vue graphique de l'état des exécutions de l'intégration Tenable.

Dans le graphique, pointez sur n'importe quelle partie du graphique pour afficher un résumé des données spécifiques à cette partie. Si vous cliquez sur une partie du graphique à barres, une liste s'ouvre pour fournir des informations plus détaillées.

Rôle requis : administrateur de vulnérabilité.

Des rôles de profil et granulaires sont disponibles pour vous aider à gérer ce que les utilisateurs peuvent faire et voir dans l'application Vulnerability Response. Pour l'affectation initiale des rôles de profil dans l'Assistant de configuration, reportez-vous à la section Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration.

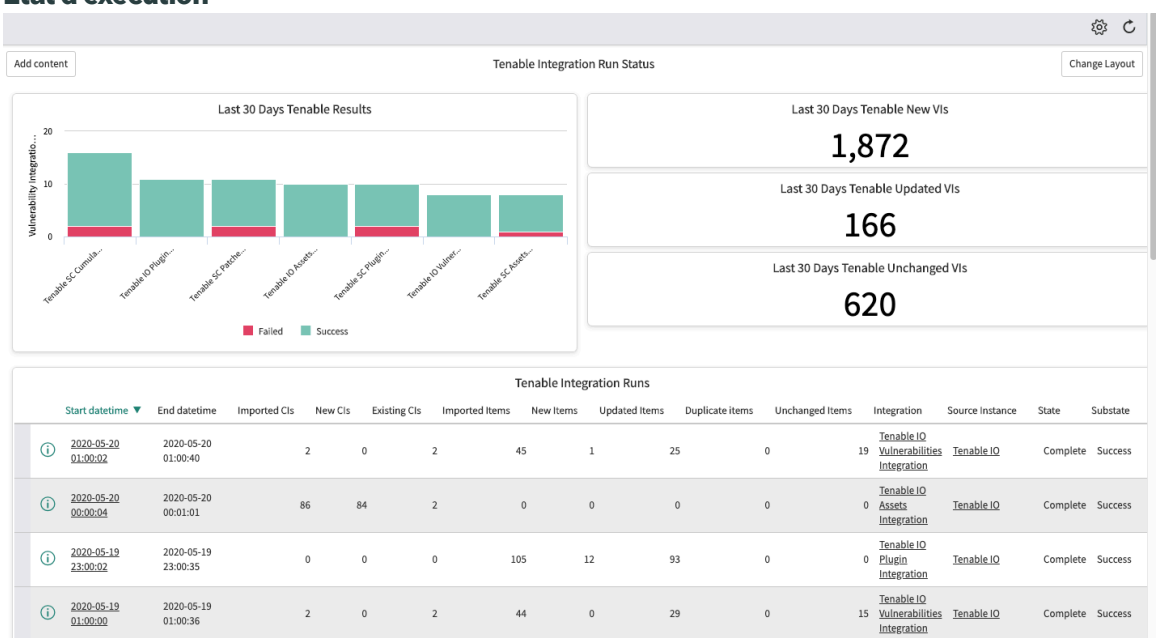
Pour plus d'informations sur la gestion des rôles granulaires, reportez-vous à la section Gérer le profil et les rôles granulaires pour Réponse aux vulnérabilités.

Pour afficher les données, accédez à **Tous** > **Intégration de vulnérabilité Tenable** > **État de l'exécution de l'intégration**.

À partir de la version 19.0 de , ce tableau de Réponse aux vulnérabilités bord est disponible dans la nouvelle interface utilisateur.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

État d'exécution



Rapports des graphiques d'état d'exécution de l'intégration Tenable

Nom	Description
Résultats Tenable au cours des 30 derniers jours	Nombre d'exécutions d'intégration terminées pour chaque intégration. Affiche les exécutions réussies et échouées. Chaque exécution s'affichait sous la forme d'une barre dans le graphique.

Traduction automatique

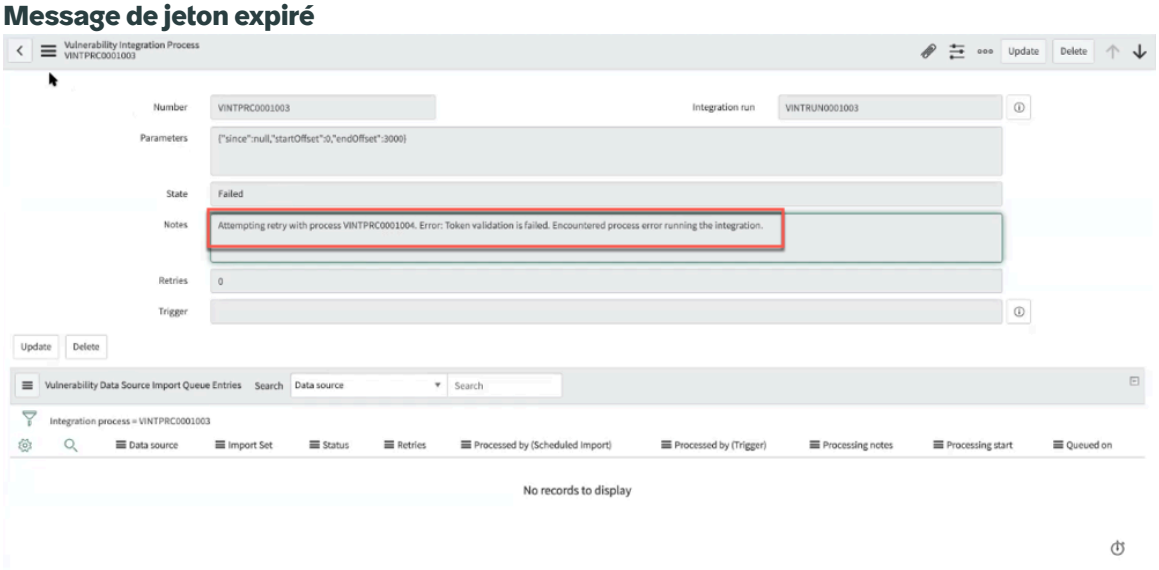
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
Nouveaux VI Tenable au cours des 30 derniers jours	Nombre de nouveaux éléments vulnérables importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI mis à jour Tenable au cours des 30 derniers jours	Nombre d'éléments vulnérables mis à jour importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
VI non modifiés Tenable au cours des 30 derniers jours	Nombre d'éléments vulnérables en double importés au cours des 30 derniers jours. Affiché sous forme de nombre entier.
Exécutions d'intégration Tenable	Les enregistrements d'exécution de l'intégration dans une liste. **Remarque : V16.1 :** Pour vérifier les détections pour cette intégration, comparez les détections ou les résultats avec les ServiceNow données de détection dans la `sn_vul_detection` table. Pendant que l'intégration est en cours, il peut y avoir un changement dans le nombre de détections ou de résultats. Ce rapport affiche le nombre de détections dans la colonne « Nombre jusqu'à ce jour » dans l'instance, une fois l'exécution de l'intégration terminée.

Expiration de la validation du jeton

Si l'exécution d'une intégration de Tenable.sc échoue pour une raison quelconque, le jeton d'authentification de Tenable.sc expire automatiquement et un message s'affiche dans l'enregistrement du processus d'intégration de vulnérabilité.

Message de jeton expiré



Un nouveau jeton est automatiquement généré pour le processus d'intégration suivant. Tous les processus d'intégration, ayant échoué ou réussi, sont affichés dans l'onglet Processus d'intégration de vulnérabilité de l'enregistrement du processus d'intégration de vulnérabilité.

Lancer une nouvelle analyse pour l'intégration Tenable.sc

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans la plateforme Tenable. Vous pouvez lancer une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

nouvelle analyse sur demande des éléments vulnérables pour le Tenable.sc produit à partir de votre ServiceNow AI Platform® instance.

Avant de commencer

Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Remarque : Tenable.sc ne prend pas en charge le lancement de RECAN sur les machines basées sur agent.

Vérifiez que votre scanner est activé avant de commencer. Accédez à la **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.

Pourquoi et quand exécuter cette tâche

Pour lancer une nouvelle analyse à partir des espaces de travail, reportez-vous à la section Analyser Tenable.io de nouveau et Tenable.sc les éléments vulnérables à partir des espaces de Réponse aux vulnérabilités travail.

Suivez les étapes énumérées ci-dessous pour lancer une nouvelle analyse dans l'environnement classique.

Pour réduire les frais généraux et le volume liés aux analyses complètes planifiées, les propriétaires de rattrapages, les spécialistes informatiques, les analystes de vulnérabilité ou les gestionnaires de vulnérabilité peuvent lancer de nouvelles analyses ciblées à la demande pour détecter des vulnérabilités spécifiques sur les actifs (éléments de configuration) de leurs environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de rattrapage (RT), d'entrée tierce (TPE) ou d'éléments découverts à partir de votre ServiceNow AI Platform instance.

Les nouvelles analyses permettent à vos propriétaires de rattrapage et à vos analystes de vulnérabilité de vérifier que vos activités de rattrapage, correctifs et autres actions ont corrigé avec succès des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Par exemple, l'ensemble de votre environnement est analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été terminée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines pour la prochaine analyse planifiée afin de vérifier qu'elle a été corrigée. Pour vérifier que votre correctif a corrigé avec succès une vulnérabilité critique découverte lors d'une analyse précédente, vous pouvez lancer une nouvelle analyse ciblée à partir de votre ServiceNow AI Platform pour rechercher Tenable.sc les éléments vulnérables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous demandez une nouvelle analyse à partir de votre ServiceNow AI Platform® instance, la sélection des informations d'identification Vulnerability Response integration with Tenable est facultative. L'intégration ServiceNow® Tenable.sc des informations d'identification de numérisation importe et met à jour les informations d'identification Tenable.sc du scanner du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable.

Notez que ces données importées n'incluent pas les mots de passe Tenable ni d'autres informations sensibles sur le compte Tenable. L'intégration ServiceNow® Tenable.sc des informations d'identification d'analyse est activée (active) automatiquement à partir de l'assistant de configuration de votre instance lorsque vous configurez les Tenable.sc intégrations de vulnérabilités (Tenable.sc intégrations de vulnérabilités ouvertes et corrigées).

Notez les informations suivantes concernant les informations d'identification que vous importez afin que vos utilisateurs puissent les consulter selon les besoins de votre ServiceNow AI Platform instance :

- Les informations d'identification créées avec le rôle d'utilisateur administrateur sont disponibles pour les Tenable.sc utilisateurs de toutes vos organisations.
- Les informations d'identification créées avec le rôle d'utilisateurs de l'organisation Tenable.sc ne sont disponibles que pour les utilisateurs de cette organisation. Ces informations d'identification ne sont pas importées dans le ServiceNow AI Platform pour les utilisateurs extérieurs à l'organisation du créateur, sauf si elles sont partagées avec le compte de l'utilisateur utilisé pour se connecter à l'instance.

Consultez le site web de la Tenable.sc documentation pour plus d'informations.

Pour plus d'informations sur la configuration de l'application, reportez-vous à la Tenable.sc section Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration . Pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation, accédez à **Tous** > **Intégration de vulnérabilité Tenable** > **Intégrations** > **Intégration des informations d'identification de numérisation Tenable.sc**.

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- *sn_sec_cmn.record_threshold_heartbeat*: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- *sn_sec_cmn.maximum_heartbeat_delay*: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Vous ne pouvez lancer de nouvelles analyses que pour les VI ayant Tenable.sc comme source. Vérifier Tenable.sc s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le générateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue de liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône **Personnaliser la liste** (icône Engrenage) et utilisez la zone de liste double pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** pour la tâche de rattrapage ou les enregistrements d'entrée tierce, respectivement, que vous souhaitez utiliser pour la nouvelle analyse.

   Selon votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

   - Sur un enregistrement de VI unique, l'élément vulnérable doit provenir du Tenable.sc produit et se trouver dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent provenir du produit Tenable.sc et dans un état autre que **Fermé**.
   - Sur un enregistrement RT, la tâche de rattrapage peut être dans n'importe quel état autre que **Fermé**, et tous les VI associés doivent provenir du Tenable.sc produit.
   - Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du Tenable.sc produit dans un état autre que **Fermé**.

4. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**.
   Vous êtes invité à choisir les informations d'identification du scanner pour accéder au scanner. Il s'agit des informations d'identification importées par l'intégration des informations d'identification Tenable.sc de numérisation.
5. Dans la boîte de dialogue, sélectionnez les filtres et les types d'informations d'identification souhaités.
6. Cliquez sur **Demander une analyse**.

   Un message s'affiche pour indiquer que votre analyse est en cours de traitement. L'état de toutes les nouvelles analyses peut être trouvé à tout moment dans les listes associées à l'analyse sur les enregistrements VI, RT, TPE que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

   Le champ État de l'enregistrement d'analyse parent est marqué comme terminé une fois que toutes les analyses enfants ont été terminées avec succès. Les analyses enfants

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

importent des données. L'enregistrement d'analyse parent est un conteneur pour les analyses enfants.

Votre ServiceNow AI Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform® votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée. Tous les éléments vulnérables qui sont passés ou passeront à l'état **Fermé/Corrigé** sont importés lors de la prochaine importation planifiée de l'intégration des vulnérabilités corrigées Tenable.sc.

Lancer une nouvelle analyse pour l'intégration Tenable.io

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés en lançant de nouvelles analyses dans la plateforme Tenable. Vous pouvez lancer une nouvelle analyse sur demande des éléments vulnérables pour le Tenable.io produit à partir de votre ServiceNow AI Platform® instance.

Avant de commencer

Rôles requis : sn_vul.write_all ou sn_vul.write_assigned

Vérifiez que votre scanner est activé avant de commencer. Accédez à la **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.

Pourquoi et quand exécuter cette tâche

- Consultez et Analyser de nouveau les enregistrements et les tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et pour Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT lancer une nouvelle analyse dans les espaces de travail Réponse aux vulnérabilités.
- Suivez les étapes énumérées ci-dessous pour lancer une nouvelle analyse dans l'environnement classique.

Remarque : Tenable.io ne prend pas en charge le lancement de RECAN sur les machines basées sur agent.

Pour réduire les frais généraux et le volume liés aux analyses complètes planifiées, en tant que propriétaire de rattrapage, informaticien, analyste de vulnérabilité ou gestionnaire de vulnérabilité, vous pouvez lancer de nouvelles analyses ciblées à la demande. Vous pouvez rechercher des vulnérabilités spécifiques sur les actifs (éléments de configuration) de vos environnements. Vous pouvez lancer de nouvelles analyses à partir d'enregistrements d'éléments vulnérables (VI), de tâches de rattrapage (VUL), d'entrée tierce (TPE) ou d'éléments découverts (SDI) à partir de votre ServiceNow AI Platform instance. Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, correctifs et autres actions ont correctement corrigé des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous demandez une nouvelle analyse à partir de votre ServiceNow AI Platform® instance, la sélection des informations d'identification Vulnerability Response integration with Tenable est facultative. L'intégration ServiceNow® Tenable.io des informations d'identification de numérisation importe et met à jour les informations d'identification Tenable.io du scanner du produit dans votre instance. Cette intégration s'exécute chaque semaine pour importer et stocker en toute sécurité vos données d'informations d'identification Tenable.

Notez que ces données importées n'incluent pas les mots de passe Tenable ni d'autres informations sensibles sur le compte Tenable.

Les informations suivantes décrivent les informations d'identification que vous importez afin que vos utilisateurs puissent les afficher selon les besoins à partir de votre ServiceNow AI Platform instance :

- Les informations d'identification créées avec le rôle d'utilisateur administrateur sont disponibles pour les Tenable.io utilisateurs de toutes vos organisations.
- Les informations d'identification créées avec le rôle d'utilisateurs de l'organisation Tenable.io ne sont disponibles que pour les utilisateurs de cette organisation. Ces informations d'identification ne sont pas importées dans le ServiceNow AI Platform pour les utilisateurs extérieurs à l'organisation du créateur, sauf si elles sont partagées avec le compte de l'utilisateur utilisé pour se connecter à l'instance.

  Consultez le site web de la Tenable.io documentation pour plus d'informations.

- L'intégration Tenable.io du modèle et l'intégration des informations d'identification Tenable.io de numérisation doivent être activées avant de lancer de nouvelles analyses. Pour afficher plus d'informations sur l'intégration des informations d'identification de numérisation, accédez à **Intégration de vulnérabilité Tenable** > **Intégrations** > **Intégration des informations d'identification Tenable.io Scan**.

  Par défaut, les intégrations de modèle et d'informations d'identification d'analyse sont désactivées. Lorsque vous saisissez vos informations d'identification pour Tenable.io, toutes les Tenable.io intégrations sont automatiquement activées. Pour activer ou désactiver manuellement ces intégrations :

  1. Accédez à la **Tous** > **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
  2. Dans la liste qui s'affiche, recherchez les enregistrements d'intégration Tenable.io souhaités.
  3. Ouvrez chaque enregistrement et cochez la case **Actif** pour activer l'intégration.
  4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
  5. Revenez à l'assistant de configuration pour poursuivre votre configuration pour le Tenable Vulnerability Integration avec Réponse aux vulnérabilités.

Pour plus d'informations sur la configuration des produits andTenable.sc, reportez-vous Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration à la Tenable.io section .

Supposons que l'ensemble de votre environnement soit analysé une fois toutes les trois semaines. L'analyse complète la plus récente a été terminée il y a une semaine, mais vous avez appliqué un correctif hier pour corriger une vulnérabilité critique. En raison de la nature de cette vulnérabilité, vous ne pouvez pas attendre deux semaines pour la prochaine analyse planifiée afin de vérifier qu'elle a été corrigée. Pour vérifier que votre correctif a corrigé avec succès une vulnérabilité critique découverte lors d'une analyse précédente,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vous pouvez lancer une nouvelle analyse ciblée à partir de votre ServiceNow AI Platform pour rechercher Tenable.io les éléments vulnérables.

Vous pouvez afficher les résultats mis à jour sur les enregistrements à partir desquels vous avez lancé les analyses après la prochaine importation planifiée de l'intégration des vulnérabilités corrigées.

Au cours de l'exécution de l'intégration, plusieurs processus sont générés et les données sont reçues sous forme de pages. Chaque processus peut contenir une ou plusieurs entrées de file d'attente d'importation avec des données jointes dans les pages. Ces entrées doivent traiter les données dans le délai d'une heure. Toutefois, si la taille de la charge utile est importante, le temps de traitement peut dépasser une heure ou être bloqué, ce qui entraîne une erreur de délai d'expiration de l'intégration. L'intégration continue de traiter les données malgré l'erreur de délai d'expiration. Pour éviter cette mauvaise communication, à partir de la version 18.2.4 de , des horodatages (intervalles de Réponse aux vulnérabilités mise à jour) sont envoyés périodiquement pour indiquer si la file d'attente est active et traite des données. Le champ **Dernier enregistrement traité** de la page Entrée de file d'attente d'importation est mis à jour en fonction du nombre d'enregistrements créés ou mis à jour par la file d'attente d'importation. Si une entrée de file d'attente d'importation dépasse la limite d'une heure, le système vérifie le champ **Dernier enregistrement traité** pour voir s'il date également de plus d'une heure. Si c'est le cas, cela indique que l'entrée de file d'attente d'importation est bloquée et qu'elle a expiré pour éviter tout retard supplémentaire dans le traitement.

Remarque : Le champ **Dernier enregistrement traité** est mis à jour en fonction de ce qui est défini dans les propriétés système suivantes :

- `sn_sec_cmn.record_threshold_heartbeat`: définit le nombre d'enregistrements traités, après quoi les intervalles de mise à jour (horodatage) sont envoyés à l'entrée de file d'attente d'importation.
- `sn_sec_cmn.maximum_heartbeat_delay`: définit le délai après lequel l'entrée de file d'attente d'importation doit expirer.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**.
2. Localisez l'enregistrement d'élément vulnérable à partir duquel vous souhaitez déclencher une nouvelle analyse et ouvrez-le.

   Remarque : Si vous utilisez le Tenable.io scanner, vous ne pouvez lancer de nouvelles analyses que pour les éléments vulnérables ayant Tenable.io comme source. Vérifier Tenable.io s'affiche dans la colonne **Source** des vues de listes des VI ou dans les champs **Source** des enregistrements individuels. Vous pouvez utiliser le générateur de conditions pour regrouper les VI par source. Ou, si la colonne Source n'est pas affichée dans la vue de liste des VI, dans le coin supérieur gauche de la liste, cliquez sur l'icône **Personnaliser la liste** (icône Engrenage) et utilisez la zone de liste double pour déplacer la **source** de **Disponible** à **Sélectionné**.

3. Vous pouvez également accéder à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** ou **Réponse aux vulnérabilités** > **Bibliothèques** > **Tiers** pour les enregistrements que vous souhaitez utiliser pour la nouvelle analyse.

   Selon votre choix, le bouton **Analyser de nouveau** est disponible sur les enregistrements suivants :

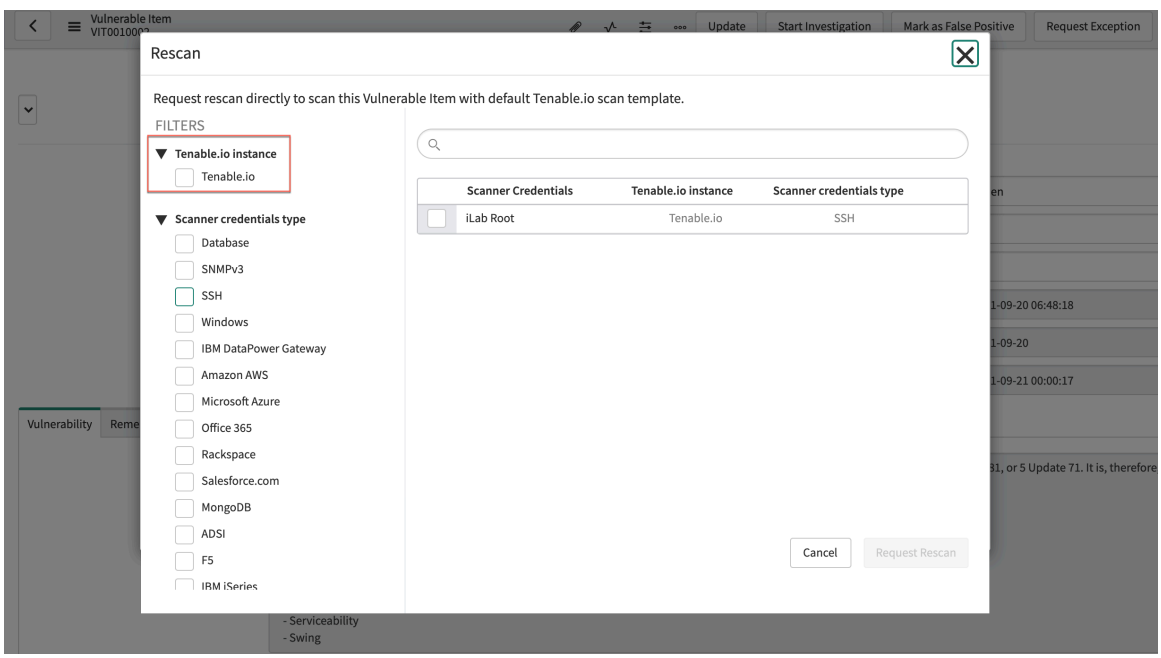
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sur un enregistrement de VI unique, le VI doit être dans un état autre que **Fermé**. Pour plusieurs enregistrements de VI, tous les VI doivent provenir du Tenable.io produit et dans un état autre que **Fermé**.
- Pour les enregistrements de tâche de rattrapage, seules les tâches de rattrapage dans un état autre que **Fermé** sont prises en charge. Tous les VI associés doivent être dans un état autre que **Fermé** et être utilisés Tenable.io comme source.
- Sur un enregistrement d'entrée tierce (TPE), l'enregistrement doit avoir au moins un enregistrement de VI associé du Tenable.io produit dans un état autre que **Fermé**.
- Sur les enregistrements d'éléments détectés, l'enregistrement doit avoir au moins un enregistrement de VI associé du Tenable.io produit dans un état autre que **Fermé**.
- Dans la liste Éléments vulnérables, vous pouvez sélectionner des éléments vulnérables individuels que vous souhaitez analyser à nouveau. Utilisez le menu Actions sur les lignes sélectionnées en bas à gauche de l'écran pour lancer la nouvelle analyse. Vous êtes invité à saisir vos informations d'identification.

4. Dans l'angle supérieur droit d'un enregistrement, cliquez sur **Analyser à nouveau**.
   Vous êtes invité à choisir l'instance ou les instances pour la nouvelle analyse et les informations d'identification du scanner que vous souhaitez utiliser pour accéder au scanner. Les informations d'identification affichées sont celles importées par l'intégration des informations d'identification Tenable.io de numérisation.
5. Dans la boîte de dialogue, sélectionnez l'instance et/ou les instances et les types d'informations d'identification que vous souhaitez utiliser.

   Dans l'image suivante, une instance d'intégration, Tenable.io s'affiche. Si vous avez plusieurs Tenable.io instances, elles sont toutes affichées dans la section Tenable.io du formulaire.



Champ	Description
Instance Tenable.io	Choisissez une Tenable.io instance d'intégration à partir de laquelle vous souhaitez lancer la nouvelle analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Toutes vos instances d'intégration pour Tenable.io s'affichent. Si un élément vulnérable existe dans plusieurs instances d'intégration, vous pouvez utiliser ce filtre pour limiter ou développer les instances que vous souhaitez analyser. **Remarque :** Si vous choisissez d'analyser à nouveau les éléments vulnérables à partir d'un enregistrement de tâche de rattrapage pour une seule instance d'intégration, seuls les éléments vulnérables actifs associés à cette tâche de rattrapage, pour cette instance, à l'aide des informations d'identification que vous sélectionnez sont analysés.
Filtre de type d'informations d'identification du scanner	Utilisez ce filtre pour afficher les informations d'identification par type.
Volet avec les informations d'identification du scanner, Tenable.io instance, type d'informations d'identification du scanner	Il s'agit des informations d'identification de scanner disponibles importées à partir des Tenable.io produits. Choisissez une ou plusieurs informations d'identification à utiliser pour l'analyse.

6. Cliquez sur **Demander une nouvelle analyse**.

Un message s'affiche pour indiquer que votre analyse est en cours de traitement et qu'un enregistrement d'analyse parent est créé. L'état de toutes les analyses enfants peut être trouvé à tout moment dans les listes connexes d'analyse sur les enregistrements du VI, de la tâche de rattrapage, du TPE et du SDI que vous avez utilisés pour lancer les nouvelles analyses. Dans le message, cliquez sur **Afficher les détails** pour afficher l'état de la nouvelle analyse et afficher toutes les autres nouvelles analyses lancées à partir d'un enregistrement donné.

Le champ État de l'enregistrement d'analyse parent est marqué comme terminé une fois que toutes les analyses enfants ont été terminées avec succès. Les analyses enfants importent des données. Chaque analyse prend en charge une combinaison unique d'instance d'intégration, de TPE, d'adresse IP et d'ID de réseau. Vous pouvez voir plusieurs analyses enfants sur un enregistrement d'analyse parent. Par exemple, le nombre maximum d'adresses IP qu'une analyse enfant peut prendre en charge est de 1 000. S'il existe 1 002 adresses IP pour un élément vulnérable, deux analyses enfants sont créées et répertoriées dans la liste connexe Analyses pour prendre en charge la demande. L'enregistrement d'analyse parent est un conteneur pour les analyses enfants et son état reflète l'état des analyses enfants.

Votre ServiceNow AI Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité. Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform® votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée. Tous les VI qui sont passés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ou passeront à **l'état Fermé/Corrigé** sont importés avec la prochaine importation planifiée de l'intégration Tenable.io des vulnérabilités corrigées.

Pour les analyses qui présentent une erreur, vous pouvez vérifier les analyses enfants sur l'enregistrement d'analyse parent. Affichez l'erreur dans la charge utile de la réponse de l'analyse enfant.

Vous pouvez afficher les résultats mis à jour sur les enregistrements à partir desquels vous avez lancé les analyses après la prochaine importation planifiée de l'intégration des vulnérabilités corrigées.

Mettre à jour les éléments de configuration avec l'identificateur de partition réseau pour le Tenable Vulnerability Integration

Créez des éléments de configuration (CI) uniques pour les actifs de votre environnement qui partagent des adresses IP. Identifiez les actifs distincts dans votre environnement et mettez automatiquement à jour les CI sur vos enregistrements existants d'élément détecté, d'élément vulnérable et de détection pour vous fournir plus de détails sur vos vulnérabilités.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Par défaut dans l'application Réponse aux vulnérabilités , une façon d'identifier vos actifs est l'adresse IP. Dans certains cas, les actifs peuvent partager des adresses IP, mais elles sont stockées sous la forme d'un seul CI dans votre CMDB.

Par exemple, comme indiqué dans les tables suivantes, plusieurs actifs (CI) de votre environnement peuvent partager des adresses IP, mais ont des ID de réseau et de référentiel uniques. Toutefois, par défaut, ces actifs sont généralement identifiés et stockés sous la forme d'un seul CI (CI 1) lors de la recherche d'adresse IP.

Recherche d'adresses IP et création de CI par défaut

Source	Adresse IP	Network_id	Élément de configuration
Tenable.io: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Source	Adresse IP	Repository_id	Élément de configuration
Tenable.sc: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Vous pouvez créer des CI individuels pour des actifs qui ont la même adresse IP afin de les identifier comme des actifs distincts. À partir d'une importation de données récente, vous pouvez mettre à jour vos CI existants avec plus de granularité qui inclut l'identificateur de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

partition de réseau [network_partition_identifier] en exécutant la tâche planifiée, *Update existing discovered items with network partition identifier*.

Cette tâche planifiée est désactivée par défaut. Activez cette fonctionnalité pour les intégrations Actifs et Vulnérabilités immobilisées et ouvertes pour les produits dans Tenable.sc l'assistant de configuration afin d'afficher Tenable.io cet identificateur sur vos enregistrements.

Lorsqu'elle est activée, cette tâche planifiée ajoute l'identificateur de partition de réseau [network_partition_identifier] aux enregistrements de CI existants à partir des données importées. Les CI existants créés par l'IRE sont également mis à jour. La tâche planifiée crée également des CI qui incluent l'identificateur de partition de réseau à partir de l'importation suivante. Vous pouvez également lancer la tâche à la demande pour mettre à jour vos données existantes.

Lorsque vous effectuez une mise à niveau à partir des Réponse aux vulnérabilités versions 14.0 et 2.2 de l'intégration de vulnérabilité Tenable, les modèles de classe CI CMDB (1.0.21) sont pris en charge. Les modèles de classes ont l'identificateur de partition de réseau [network_partition_identifier] dans les règles d'identification IRE (Identification et rapprochement).

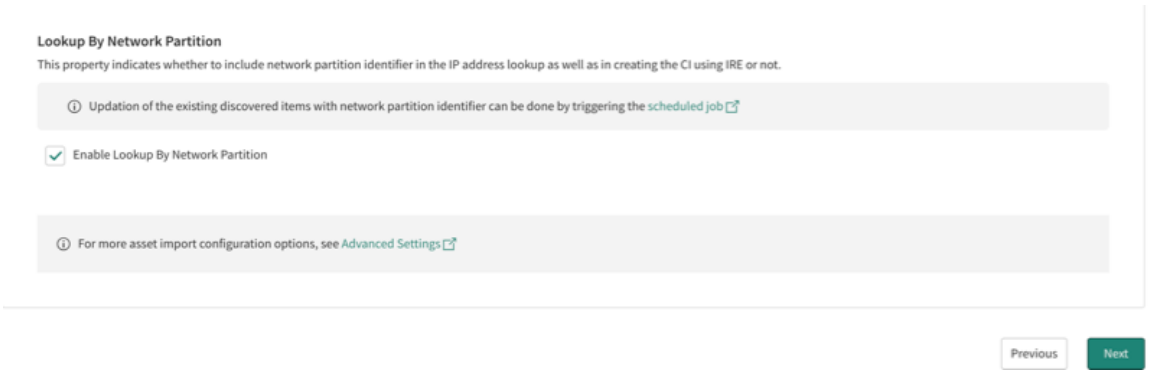
Option	Description
Exécuter les travaux planifiés sur demande.	Mettez à jour vos éléments détectés existants. Les CI de vos données Tenable existantes sont créés ou mis à jour pour inclure la granularité de l'identificateur de partition de réseau. Les éléments détectés, les éléments vulnérables et les enregistrements de détection sont tous mis à jour avec les nouveaux CI.
Attendez les importations de données fraîches à partir des intégrations avec les travaux planifiés suivants.	Créez des CI pour chaque nouvel actif à l'aide de l'identificateur de partition de réseau en commençant par la tâche planifiée suivante. Les enregistrements de CI, d'éléments vulnérables et de détection sont tous mis à jour pour inclure la nouvelle granularité. De nouveaux CI sont créés lorsqu'aucune correspondance exacte n'est trouvée.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Assistant de configuration** > **Configuration de l'intégration** > **Intégrations de scanners**.
2. Sélectionnez Tenable.io des intégrations ou Tenable.sc des intégrations.
3. **Modifiez** l'intégration requise.
4. Sélectionner **Configuration de l'importation d'actifs**.
5. Sélectionner **Activer la recherche par partition de réseau** case à cocher dans le **Activer la recherche par partition de réseau** section.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Suivant**.

Les identificateurs de partition de réseau NETWORK_ID et les _ID REPOSITORY sont inclus et mettent à jour les CI existants ou créent des CI avec la tâche planifiée suivante.

Attribut d'identificateur de partition de réseau inclus dans la recherche d'adresses IP et la création de CI

Source	Adresse IP	NETWORK_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
Tenable.io: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Source	Adresse IP	REPOSITORY_ID	CI pour les actifs sans identificateur de partition de réseau	Actifs de CI avec identificateur de partition de réseau
Tenable.sc: intégrations des actifs et des vulnérabilités immobilisées et ouvertes	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Avec la prochaine tâche planifiée, les règles de recherche d'identification d'adresse IP et d'adresse IP incomplète incluent automatiquement l'attribut d'identificateur de partition de réseau pour une importation de données à partir des intégrations Actifs et Vulnérabilités fixes et ouvertes pour les et les Tenable.ioTenable.sc produits.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que vous avez activé la propriété système et enregistré les enregistrements, vous pouvez également mettre à jour vos éléments détectés existants avec des CI qui incluent l'identificateur de partition de réseau en lançant les travaux planifiés à la demande.

Importer des modifications pour l'intégration de vulnérabilité Tenable

Configurez des modifications facultatives et rationalisez certaines des données spécifiquement pour l'intégration d'importation des vulnérabilités Tenable dans l'intégration ServiceNow® des vulnérabilités Tenable.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Cet ensemble de tâches nécessite du codage et des connaissances avancées sur le ServiceNow AI Platform.

Suivez ces étapes pour créer des importations séparées par domaine pour les intégrations de vulnérabilités Tenable. L'exemple suivant concerne l'intégration des vulnérabilités ouvertes Tenable.io, mais ce contenu s'applique aux autres intégrations Tenable.

Procédure

1. Créez un domaine.
2. Pour chaque domaine que vous créez, créez un utilisateur et affectez-le à ce domaine.

   Considérez cet utilisateur comme un espace réservé run_as pour le domaine dans Tenable.io.

3. Intégration des vulnérabilités ouvertes.
   L'utilisateur est l'équivalent du VR. Utilisateur système dans le domaine global et doit avoir les rôles suivants : sn_vul.tenable_configure_integration, import_admin et sn_vul.vulnerability_write. Cet utilisateur doit avoir accès aux sources de données, aux cartes de transformation et aux données de vulnérabilité.

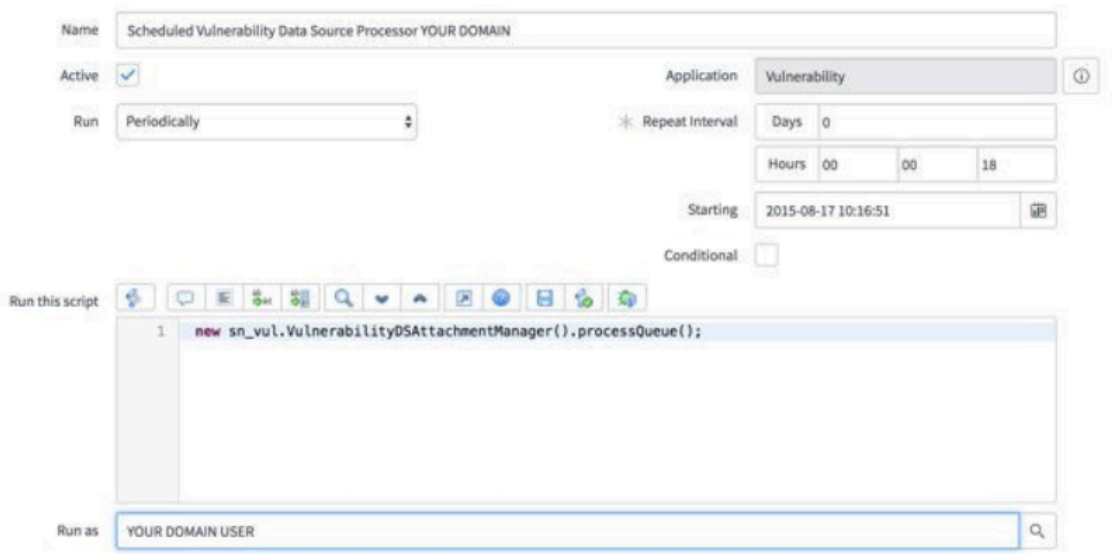
   Remarque : Considérez cet utilisateur comme spécifique à ce rôle. L'utilisateur ne doit pas avoir d'autre but

4. Dans chaque domaine, créez une tâche planifiée en copiant le processeur de source de données de vulnérabilité planifiée trouvé sous **Définition du système** > **Travaux planifiés**.
5. Ajoutez le domaine au nom pour identifier la tâche planifiée.
6. Remplacez l'utilisateur run_as par l'utilisateur que vous avez créé à l'étape précédente.

   Remarque : Modifiez l'action d'interface utilisateur suivante afin que l'intégration s'exécute dans le domaine de l'utilisateur run_as.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Modifiez l'action d'interface utilisateur Exécuter maintenant dans l'intégration des vulnérabilités ouvertes Tenable.io pour ajouter ce bloc de code en haut du fichier.

```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
```

Remarque : Modifiez les includes de script suivants afin que l'intégration s'exécute dans le domaine de l'utilisateur run_as.

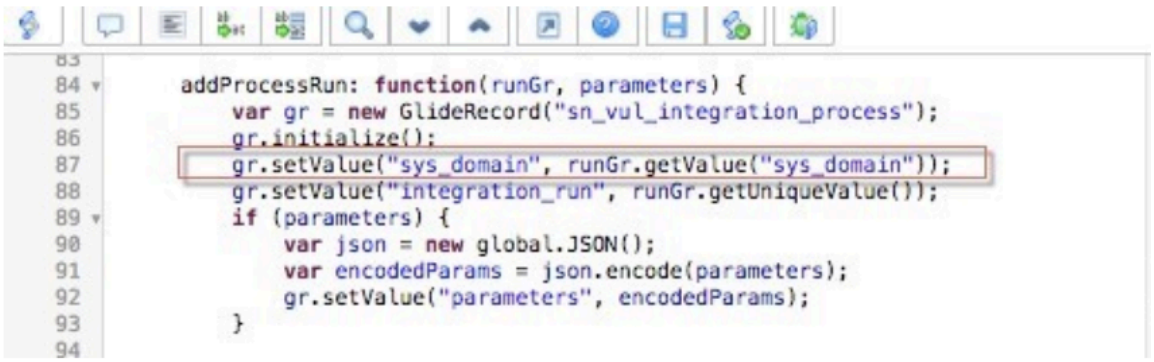
8. Modifiez la méthode d'include de script VulnerabilityIntegrationUtils, addIntegrationRun, pour ajouter le code en surbrillance.

```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

9. Modifiez la méthode d'include de script VulnerabilityIntegrationUtils, addProcessRun, pour ajouter le code en surbrillance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Modifiez la méthode d'include de script DataSourceVulnReportRefreshProcessor _processFromDataSourceGroups pour modifier ce code d'origine : Code _processFromDataSourcesGroups original en code _processFromDataSourcesGroups modifié.
11. Modifiez la méthode d'include de script VulnerabilityDSAttachmentManager, queueItem pour ajouter les blocs de code en surbrillance suivants, queueItem, _getNext _processQueueEntry fonction.

Vous êtes prêt pour les importations de détections d'hôtes séparés par domaine.

Désactiver les calculateurs avant l'importation

Suivez ces étapes pour désactiver le calculateur par défaut s'il n'est pas utilisé. Si vous n'utilisez pas de calculateurs de vulnérabilité, il est préférable de désactiver les calculateurs par défaut en plus de ceux que vous avez définis. Les calculateurs de vulnérabilité s'exécutent chaque fois qu'un enregistrement d'élément vulnérable est consulté et peuvent avoir un impact sur les performances de l'instance.

Rôle requis : sn_vul.vulnerability_admin.

12. Accédez à la **Tous** > **Vulnérabilité** > **Administration** > **Calculateurs de vulnérabilités**.
13. Ouvrez le groupe Impact de vulnérabilité.
14. Ouvrez le calculateur de score et d'impact basé sur le service.
15. Désélectionnez le champ Actif pour désactiver le calculateur.
16. Cliquez sur Mettre à jour.

Vous avez désactivé le calculateur par défaut.

Désactiver les règles métier basées sur la notification avant l'importation initiale

Procédez comme suit pour désactiver les règles métier liées aux notifications avant l'importation initiale de l'enregistrement. Lors de l'importation initiale d'enregistrements, certaines règles métier liées aux notifications peuvent générer de nombreuses notifications, ce qui a un impact sur les performances. Ces règles métier doivent être modifiées pour les désactiver au cours de l'importation.

Le rôle requis est sn_vul.vulnerability_admin.

17. Accédez à la **Tous** > **Définition du système** > **Règles métier**.
18. Rechercher les notifications de CI affectés.
19. Ouvrez la règle métier et insérez la condition suivante : `current.sys_class_name != "sn_vul_vulnerable_item"`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

20. Cliquez sur **Mettre à jour**.
21. Répétez cette procédure pour les règles métier suivantes :
    - Notifications des centres de coûts affectés
    - Notifications des groupes affectés
    - Notifications des emplacements affectés

    Remarque : Une fois l'importation de l'enregistrement initial terminée, vous avez la possibilité de réactiver ces règles métier. Cependant, envisagez de les laisser désactivés. Elles peuvent générer un grand nombre de notifications et avoir un impact sur les performances de votre instance.

    Modifier une date de début initiale

    Procédez comme suit pour modifier une date de début initiale. Lors de l'installation à l'aide de l'Assistant de configuration, vous définissez une date de début initiale pour les intégrations Tenable. Vous pouvez réinitialiser cette date de début dans l'Assistant de configuration ou à partir de l'intégration principale, comme indiqué dans les étapes suivantes.

22. Accédez à la **Tous** > **Intégration de vulnérabilité Tenable** > **Administration** > **Intégrations**.
23. Cliquez sur n'importe quelle intégration.
24. Cliquez sur Détails de l'intégration.
25. Définissez le champ Heure de début sur une valeur dans le passé, de sorte que toutes les vulnérabilités analysées et détectées depuis cette heure soient détectées.

    Si vous avez configuré Tenable à l'aide de l'assistant de configuration, le champ Heure de début est pré-rempli, initialement jusqu'à trois mois avant la date d'aujourd'hui, puis jusqu'à la date d'aujourd'hui. Remarque : Envisagez de définir la valeur sur un maximum d'un mois dans le passé. Cela empêche une grande quantité de données de dépasser les limites de débit de l'API de Tenable et de déclencher des délais d'exécution.

26. Cliquez sur **Envoyer** ou **Mettre à jour**.
27. **Facultatif :** Cliquez sur **Exécuter maintenant** pour l'exécuter immédiatement.

Fractionner les détections Tenable en fonction de l'instance de vulnérabilité pour diviser les éléments vulnérables

ServiceNow® Vulnerability Response permet de séparer les détections des scanners Tenable, ce qui permet de créer un élément vulnérable unique (VIT) pour chaque instance de vulnérabilité détectée. Cette répartition permet l'affectation de VIT à diverses équipes de remédiation, améliorant ainsi la gestion et le suivi des vulnérabilités.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
La charge utile du scanner Tenable contient des données de détection, chaque chemin d'accès de la preuve étant utilisé pour diviser les détections. La balise de sortie dans la charge utile identifie l'emplacement de la vulnérabilité, ce qui facilite l'identification et la gestion précises des vulnérabilités en fonction de leurs chemins spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans la table Intégrations tierces [sn_sec_int_integration], définissez la valeur de la colonne **Inclure la preuve dans la clé du VI** sur vrai pour Tenable.io, Tenable.sc et .Tenable.cs
2. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Configurer la granularité VI**.
3. Pour Tenable.cs le produit, accédez à la table **Configuration de clé de détection** [sn_vul_detection_key_config], sélectionnez Tenable.cs Enregistrer et mettre à jour,
4. Dans le formulaire Inclure le port, cochez la case **Inclure le port** et sélectionnez le lien **cliquer ici** (s'applique uniquement aux Tenable.io et Tenable.sc).
5. Dans la liste Ajouter une preuve aux clés de VI, sélectionnez **Nouveau**.
6. Dans le formulaire Ajouter une preuve à la clé de VI- Nouvel enregistrement, dans le champ **Vulnérabilité** , ajoutez l'ID Tenable pour lequel vous souhaitez inclure la preuve.

   Remarque : Vous pouvez diviser les détections en fonction des informations de chemin d'accès ou en combinant les détails de chemin d'accès et de version. Pour plus de détails, reportez-vous à la section « Fractionnement des détections à partir des scanners Tenable » sur cette page.

7. Dans le champ **Expression régulière pour diviser les VIT Tenable** :
   - Divisez la détection en fonction du chemin d'accès uniquement en saisissant Chemin d'accès\s+ :\s+([A\n]+).
   - Divisez la détection en fonction du chemin d'accès et des versions installées et corrigées en saisissant Chemin\s+ :\s+([A\n]+)\n\s+Installed\s+version\s+ :\s+([A \n]+)\n\s+Fixe\s+version\s+ :\s+([A\n]+).
8. Sélectionnez **Soumettre**.

Example: Fractionnement des détections à partir des scanners Tenable

La détection suivante à partir d'un scanner Tenable montre la preuve dans la balise de sortie qui inclut à la fois des informations sur le chemin et la version.

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
                     "Microsoft Windows Server 2019 Datacenter Build 17763"


                "network_id": "00000000-0000-0000-0000-000000000008",
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
                "tracked": true

            "output": "In                    C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                    Path
            "plugin":
                "bid":
                    123456

                "checks_for_default_account": false,
               "checks_for malware": false,

                 "coe":
                "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"

                 "cvSs3_base_score": 7.8,
                "cvss3 temporal score": 7.0,

                "cvss3_temporal_vector": {
                    "exploitability": "Proof-of-Concept",
                    "remediation level": "Official Fix",
                     "report_confidence": "Confirmed",
                     "raw": "E: P/RL:0/RC: C"
```


Explorer les intégrations des résultats des tests Wiz et des problèmes avec Conformité de la configuration

Importez des données de configuration dans le cloud avec les résultats des tests Wiz et les intégrations de problèmes incluses Conformité de la configuration dans l'intégration Wiz Réponse aux vulnérabilités .

Wiz Intégration des résultats des tests

Importez les résultats des tests de configuration pour détecter les configurations dans le cloud non conformes et vous aider à appliquer les politiques et les normes de Wiz sécurité dans votre environnement cloud.

Les résultats sont mappés aux résultats des tests dans le cloud (CTR) dans l'application Conformité de la configuration .

Remarque : Les configurations d'hôte ne Wiz sont pas importées.

Wiz Intégration des problèmes

Importez les données Wiz des problèmes pour aider les responsables des vulnérabilités, les analystes et les équipes de sécurité et de risque du cloud à identifier les combinaisons de vulnérabilités susceptibles de révéler un chemin d'attaque potentiel dans votre infrastructure cloud.

Ces résultats sont également mappés à des CTR avec des problèmes Wiz étiquetés comme source dans l'application Conformité de la configuration pour vous aider à suivre et à corriger les actifs qui peuvent présenter des risques multivectoriels complexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les autres intégrations incluses dans les étapes d'intégration et d'installation Wiz Réponse aux vulnérabilités et de configuration, reportez-vous à la section Présentation de Wiz Réponse aux vulnérabilités l'intégration.

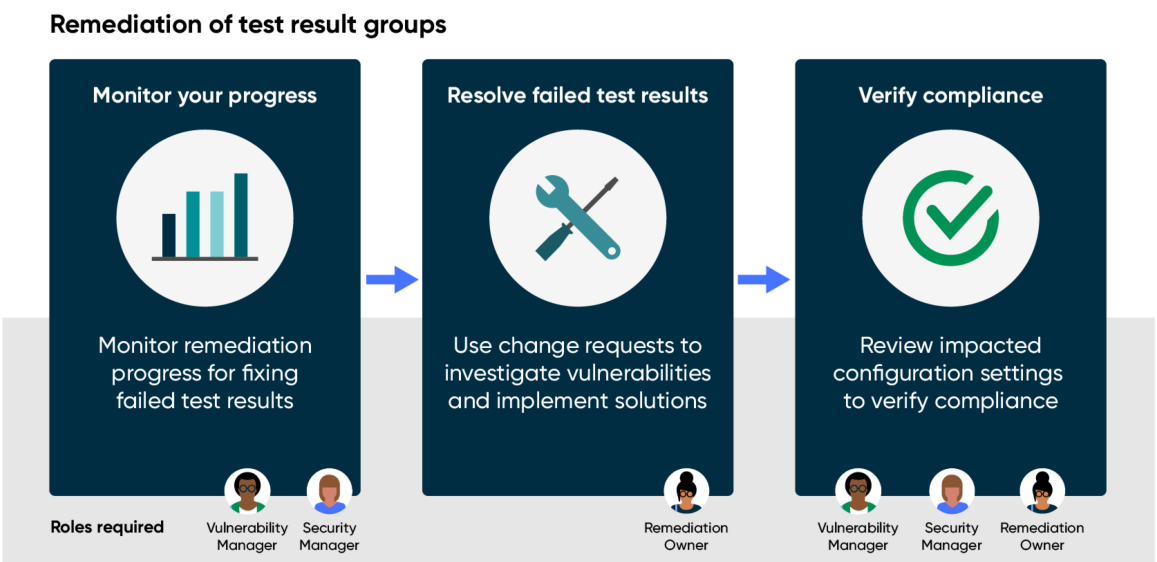
Conformité de la configuration Correction

Conformité de la configuration Le rattrapage est principalement un processus manuel complété par des travaux planifiés (intégrations), des tâches de rattrapage, des workflows et des demandes de changement.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test



Des modules d'extension SCA tiers distincts acquièrent et transforment des données dans Conformité de la configuration. Avant de pouvoir Conformité de la configuration corriger des éléments de configuration, vous devez installer une intégration d'analyse tierce et effectuer au moins une analyse réseau.

Utilisez les demandes de changement pour corriger les échecs de test individuels des tâches de rattrapage.

Les états des tâches de rattrapage passent automatiquement à mesure que les demandes de changement associées avancent dans leur cycle de vie avec Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage. Les utilisateurs disposant du rôle itil peuvent créer et gérer des demandes de changement directement à partir des tâches de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

- Créer manuellement une tâche de Conformité de la configuration rattrapage
- Créer manuellement une Conformité de la configuration tâche de rattrapage à partir de la liste Résultats des tests
- Créer une demande de changement dans Conformité de la configuration
- Associer une tâche de rattrapage à une demande de changement existante
- Supprimer les affectations des tâches de rattrapage pour vous ou vos groupes
- Fermeture automatique des résultats des tests
- Fermer une tâche de rattrapage
- Configurer les règles d'approbation pour la gestion des exceptions dans Conformité de la configuration

Créer manuellement une tâche de Conformité de la configuration rattrapage

Vous pouvez créer manuellement une tâche de rattrapage à partir du module **Tâches de rattrapage** et effectuer un rattrapage.

Important : Vous pouvez créer des tâches de rattrapage dans :

- Espace de travail du gestionnaire de vulnérabilités en tant qu'utilisateur disposant du rôle sn_vulc.admin.
- Espace de travail de remédiation IT en tant qu'utilisateur disposant du rôle sn_vulc.remediation_owner.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

L'utilisation des règles de tâche de rattrapage remplit automatiquement l'onglet **Résultats des tests** . La création manuelle est utile pour une tâche de rattrapage qui n'a pas besoin de règle ou qui doit être répétée.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

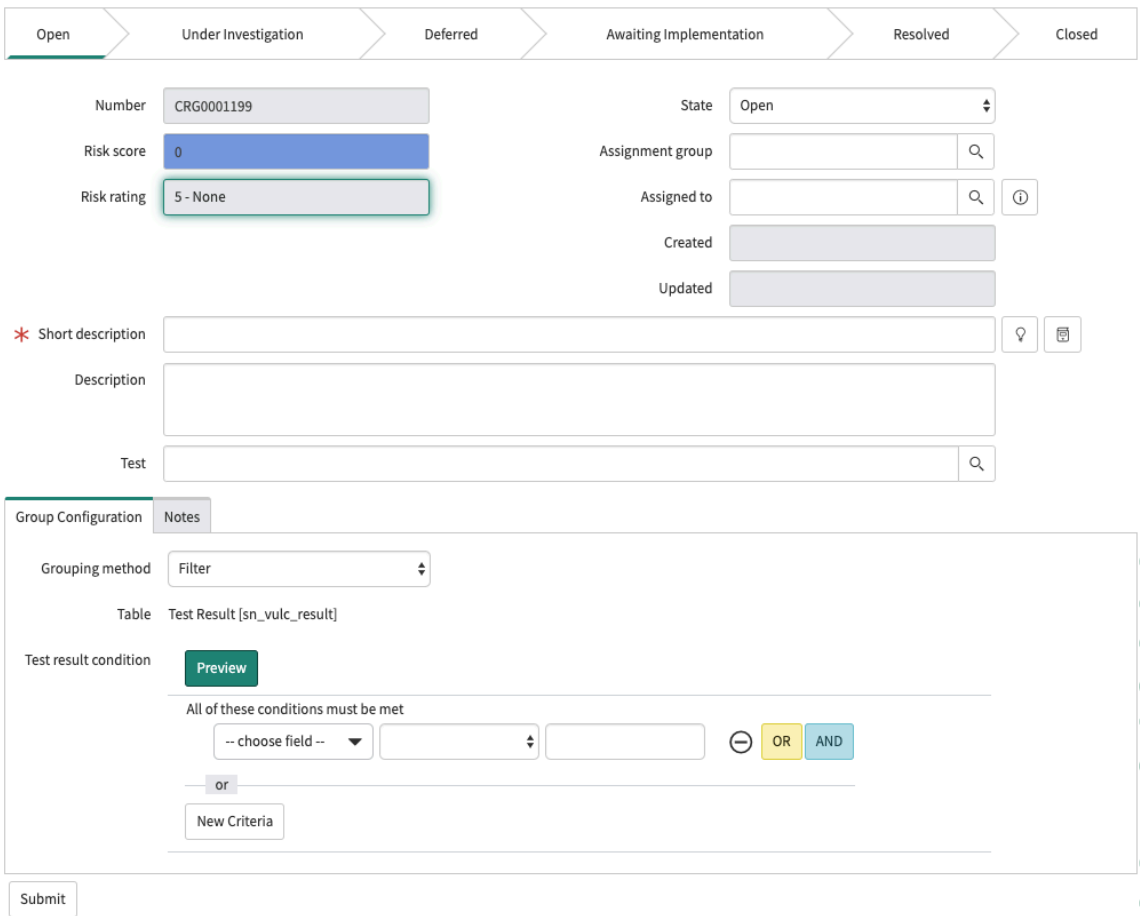
Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Tâches de remédiation**.
2. Dans le panneau de navigation, cliquez sur **Mes tâches ouvertes** ou **Toutes les tâches ouvertes** pour afficher la liste.
3. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de tâche de rattrapage



4. Renseignez les champs du formulaire Tâche de rattrapage, le cas échéant.

Formulaire de tâche de rattrapage

Champ	Description
Numéro	ID affecté automatiquement dans le système.
Score du risque	Renseigné automatiquement par le calculateur de score de risque. Il s'agit d'un score de risque de déploiement. Ce score de risque est pondéré : 85 % du score du score de risque maximal pour tous les résultats des tests n'étant pas « fermés » (Ouvert, En cours d'examen, En attente d'implémentation, Différé, Résolu) et 15 % du score provenant du nombre de résultats des tests qui ne sont pas « Fermés ».
Cote de risque	Renseigné automatiquement par le calculateur de score de risque. Basé sur une plage de scores de risque sur une échelle numérique de 1 à 5 qui évalue le risque global en fonction d'une plage de scores de risque allant de 1 - Critique à 5 - Aucun. Ce champ remplace le champ Priorité des versions précédentes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

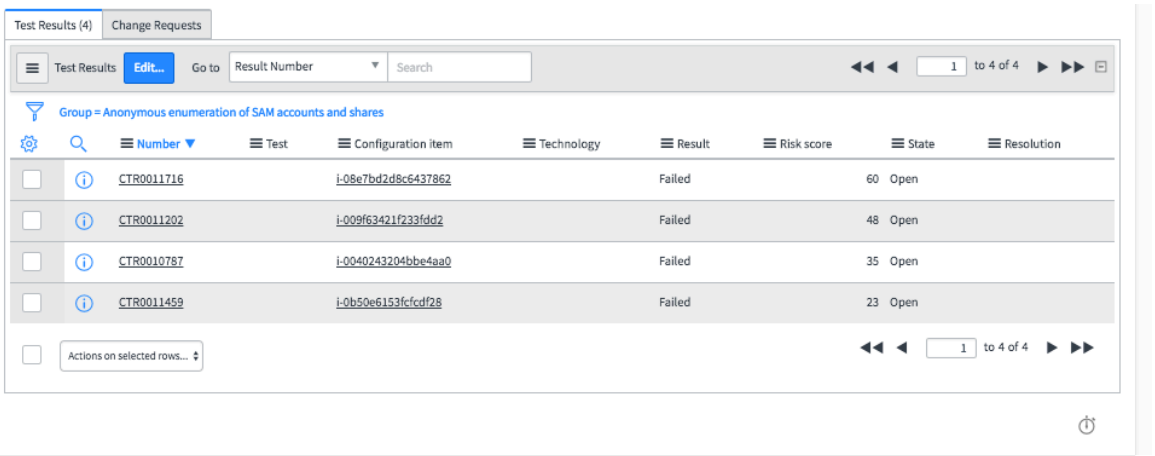
Champ	Description
État	**Initialement ouvert**, indique l'état de rattrapage de la tâche de rattrapage. Pour plus d'informations, consultez Conformité de la configuration États.
Groupe d'affectation	Affectez la tâche de rattrapage à un groupe de rattrapage.
Affecté à	Affecter du personnel pour corriger la tâche de rattrapage.
Créées	Date à laquelle vous avez créé cette tâche de rattrapage.
Mis à jour	Date de mise à jour de cette tâche de rattrapage.
Description brève	Nom de la tâche de rattrapage.
Description	Description de cette tâche de rattrapage.
Test	Sélectionnez un test de configuration pour cette tâche de rattrapage.
Onglets associés	
Configuration du groupe	Méthodes de regroupement à utiliser : ◦ Manuel (par défaut) : ◦ Règle de filtre ou de groupe : Table : présélectionnée comme résultat de test [sn_vulc_result] Condition du résultat du test : Choisissez les filtres à utiliser. **Remarque :** Le lien des conditions de correspondance des enregistrements au-dessus des conditions de filtre affiche les enregistrements de résultats de test que vous avez choisis dans une nouvelle fenêtre. Cliquez sur **Aperçu** pour afficher le nombre de résultats renvoyés par vos critères de filtre avant d'enregistrer le nouveau groupe. La liste connexe des résultats des tests doit être créée manuellement en cliquant sur le bouton **Modifier** dans l'onglet connexe **Résultats des tests** .
Notes	Notes de travail relatives à cette tâche de rattrapage.

5. Cliquez avec le bouton droit dans l'en-tête pour **enregistrer** ou cliquez sur **Soumettre** pour enregistrer et revenir à la liste des tâches de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affiche les listes connexes **Résultats des tests** et **Demande de changement** .



Créer manuellement une Conformité de la configuration tâche de rattrapage à partir de la liste Résultats des tests

Vous pouvez créer manuellement une tâche de rattrapage à partir de la liste **des résultats des tests** et effectuer un rattrapage à partir de la tâche de rattrapage résultante.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Cette méthode nécessite de sélectionner les résultats des tests à inclure et de créer le groupe à partir du menu **Actions sur les lignes sélectionnées.** Cette méthode est utile pour les résultats difficiles à filtrer ou pour les situations dans lesquelles vous souhaitez spécifier des résultats de test pour correction.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

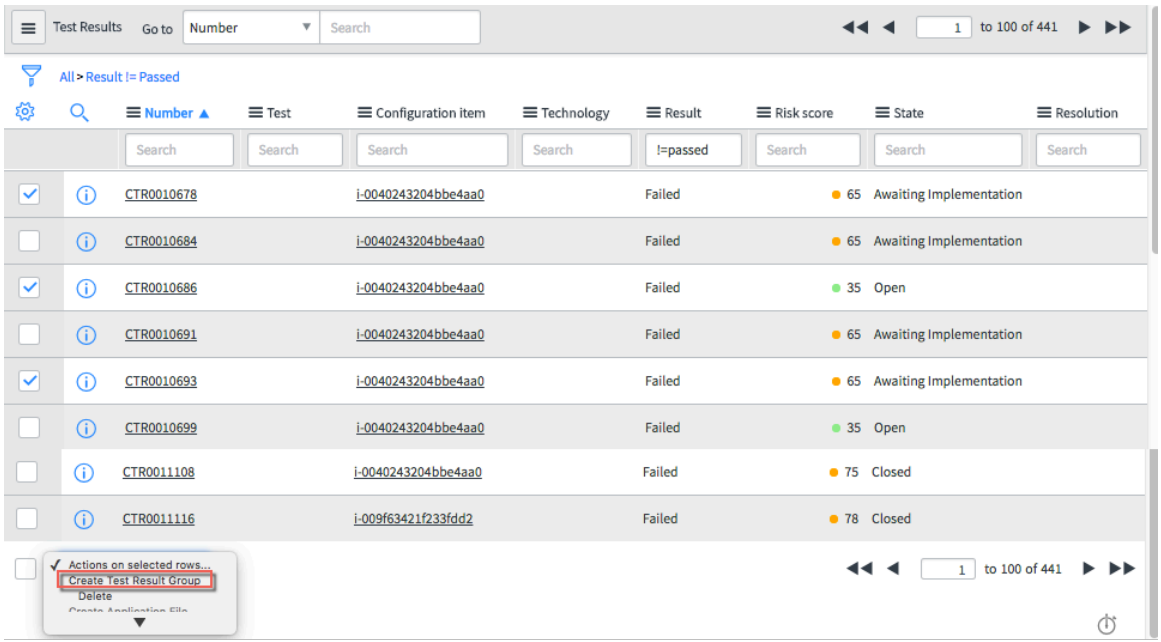
Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

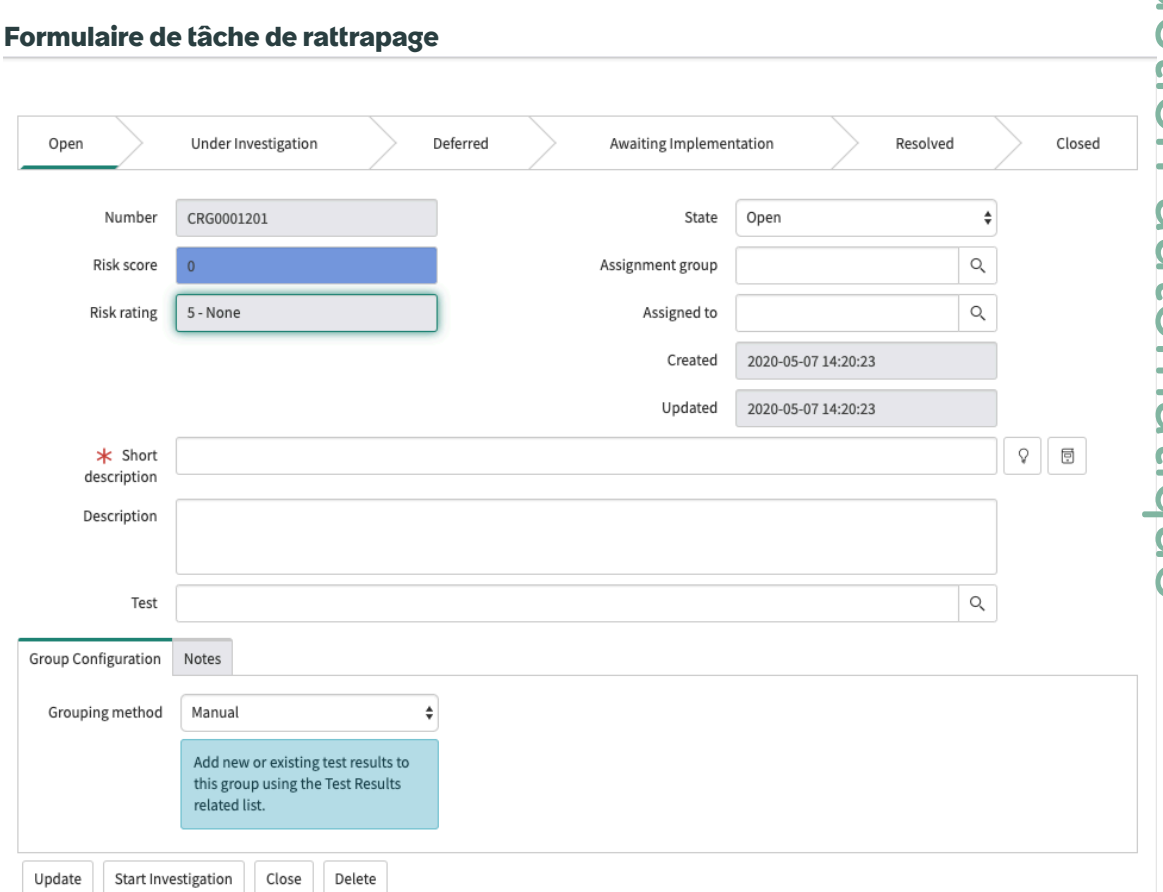
1. Accédez à la **Tous** > **Configuration Compliance** > **Résultats des tests**.
2. Dans le panneau de navigation, sélectionnez un module de résultat de test pour ouvrir une liste.
3. Sélectionnez les résultats des tests à inclure dans la tâche de rattrapage en cochant la case en regard de chacun.
4. Ouvrez le menu **Actions sur les lignes sélectionnées...** en bas de la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



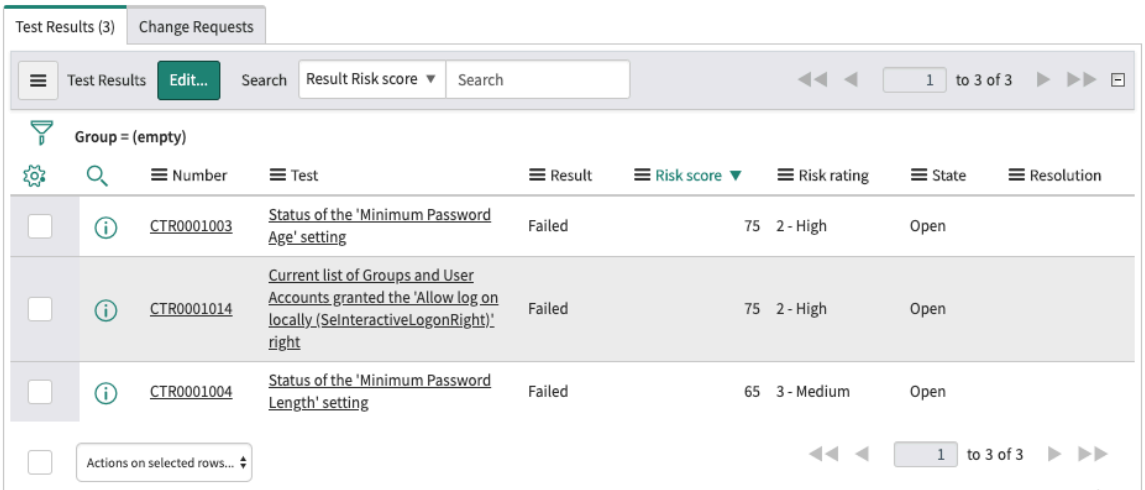
5. Choisissez **Créer une tâche de rattrapage**.
La tâche de rattrapage est créée et s'ouvre.



Les résultats des tests que vous avez sélectionnés pour la tâche de rattrapage sont affichés dans la liste connexe Résultats des tests, avec toutes les demandes de changement associées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Renseignez les champs du formulaire comme il convient.

Champ	Description
Numéro	ID affecté automatiquement dans le système.
Score	Renseigné automatiquement par le calculateur de déploiement des scores de risque. Il s'agit d'un score de risque de déploiement. Ce score de risque est pondéré : 85 % du score du score de risque maximal pour tous les résultats des tests n'étant pas « fermés » (Ouvert, En cours d'examen, En attente d'implémentation, Différé, Résolu) et 15 % du score provenant du nombre de résultats des tests qui ne sont pas « Fermés ».
Évaluation	Renseigné automatiquement par le calculateur de déploiement des scores de risque. Basé sur une plage de scores de risque sur une échelle numérique de 1 à 5 qui évalue le risque global en fonction d'une plage de scores de risque allant de 1 - Critique à 5 - Aucun. Ce champ remplace le champ Priorité des versions précédentes.
Score de risque historique	Renseigné automatiquement par le calculateur de déploiement des scores de risque. Le score de risque inhérent sur tous les résultats des tests réussis dans une tâche de rattrapage. Ce champ affiche la quantité de risque qui a été corrigée par un groupe de tests et s'affiche uniquement lorsqu'un groupe de tests est à l'état « Fermé » et que le score de risque est nul.
État	**Initialement ouvert**, indique l'état de rattrapage de la tâche de rattrapage. Pour plus d'informations, consultez Conformité de la configuration États.
Groupe d'affectation	Affectez la tâche de rattrapage à un groupe de rattrapage.
Affecté à	Affecter du personnel pour corriger la tâche de rattrapage.
Créées	Date à laquelle vous avez créé cette tâche de rattrapage.
Mis à jour	Date de mise à jour de cette tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description brève	Nom de la tâche de rattrapage.
Description	Texte descriptif de cette tâche de rattrapage.
	Sélectionnez un test de configuration pour cette tâche de rattrapage.
Onglets associés	
Configuration du groupe	Méthodes de regroupement à utiliser : ○ Manuel (par défaut) ○ Filtre Table : présélectionnée comme résultat de test Condition du résultat du test : Choisissez les filtres à utiliser. **Remarque :** Le lien des conditions de correspondance des enregistrements au-dessus des conditions de filtre affiche les enregistrements de résultats de test que vous avez choisis dans une nouvelle fenêtre. Cliquez sur **Aperçu** pour voir le nombre de résultats renvoyés par vos critères de filtre avant d'enregistrer la nouvelle tâche de rattrapage.
Notes	Notes de travail relatives à cette tâche de rattrapage.
Listes connexes	
Résultats des tests	Résultats des tests inclus dans cette tâche de rattrapage.
Demandes de changement	Demandes de changement associées à cette tâche de rattrapage.

7. Cliquez avec le bouton droit sur l'en-tête pour **enregistrer** ou cliquez sur **Soumettre** pour enregistrer et revenir à la liste des tâches de rattrapage.

Créer une demande de changement dans Conformité de la configuration

Vous pouvez créer une demande de changement à partir d'une tâche de rattrapage dans l'application Conformité de la configuration .

Avant de commencer
Rôle requis : utilisateur disposant du rôle itil

Pourquoi et quand exécuter cette tâche
En tant qu'informaticien ou spécialiste du rattrapage, créez une demande de changement (CHG) directement à partir d'une tâche de rattrapage pour tous les résultats des tests qu'elle contient. Créez une demande de changement avec des informations pré-remplies pour accélérer votre enquête sur les vulnérabilités qui nécessitent une intervention manuelle.

Vous pouvez créer, approuver, implémenter, examiner et fermer des demandes de changement directement à partir des tâches de rattrapage qui vous sont affectées. Vous pouvez créer trois types de demandes de changement avec des informations pré-remplies à partir d'une tâche de rattrapage :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Standard

Un changement pré-autorisé à risque faible, relativement commun et qui suit une procédure ou une instruction de travail spécifique.

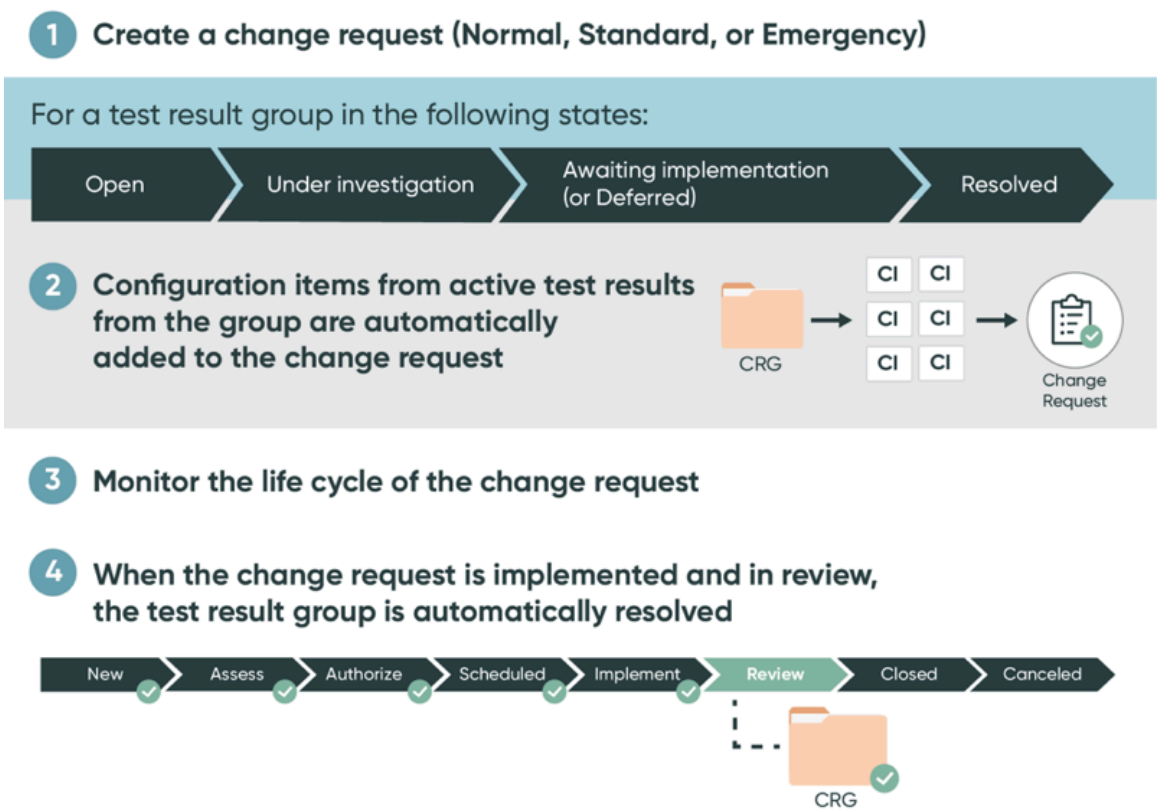
Normal

Les demandes de changement normal suivent un processus prescriptif qui requiert deux niveaux d'approbation avant leur implémentation, revue et fermeture.

Urgence

Un changement pour résoudre un incident majeur.

L'image suivante illustre le flux de base pour créer une demande de changement à partir d'une tâche de rattrapage. Les étapes détaillées de ce flux suivent l'image.



À partir de la version 19.0 de , vous pouvez créer des demandes de changement pour les tâches de rattrapage à partir de l'espace de Réponse aux vulnérabilités travail Rattrapage informatique. Pour plus d'informations, consultez Créer une demande de changement dans Espace de travail de remédiation IT.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Tâches de remédiation** > **Mes tâches ouvertes**.
   La liste des tâches de rattrapage affectées à vos groupes s'affiche.
2. Dans la colonne Nombre, cliquez sur la tâche de rattrapage pour laquelle vous souhaitez créer une demande de changement.
   Vous pouvez créer des demandes de changement à partir de tâches de rattrapage dont l'état n'est pas **Fermé** ou **En cours de révision**.

   L'enregistrement de la tâche de rattrapage s'affiche.
3. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Créer un changement**.
   Le formulaire de demande de changement s'affiche.
4. Renseignez les champs.
   a. Dans la liste du champ **S'applique à, choisissez-en** un pour continuer.

Option	Description
Tous les résultats des tests actifs dans ce groupe	Si cette option est sélectionnée, tous les résultats des tests actifs de cette tâche de rattrapage dont l'état n'est pas **Fermé** sont ajoutés automatiquement à la demande de changement une fois que vous avez cliqué sur **Créer un changement**.
Tous les résultats des tests actifs dans ce groupe correspondant à un ensemble de conditions	Si cette option est sélectionnée, le générateur de conditions s'affiche. Entrez des critères de filtre afin d'identifier les résultats des tests que vous souhaitez obtenir pour la nouvelle demande de changement. Un exemple de filtre que vous pouvez créer localiserait uniquement les résultats des tests de la tâche de rattrapage qui correspondent à un état et à un score de risque spécifiques : L'état est **Ouvert** et le score de risque est supérieur à **50**.

5. Pour la case **à cocher Ajouter des CI au CR** , choisissez-en un pour continuer.

Option	Description
Case à cocher sélectionnée	Sélectionné par défaut. Si la case à cocher est sélectionnée, tous les éléments de configuration (CI) qui appartiennent aux résultats des tests actifs de cette tâche de rattrapage sont ajoutés à cette demande de changement. Le résultat du test passe à **En attente d'implémentation**.
Case à cocher désactivée	Décochez la case si vous ne souhaitez pas que les CI des résultats des tests actifs de cette tâche de rattrapage soient ajoutés à la nouvelle demande de changement. La tâche de rattrapage reste dans son état actuel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans la liste du champ **Type de changement** , choisissez-en un pour continuer.

Option	Description
Urgence	Un changement pour résoudre un incident majeur.
Normal	Type de changement utilisé pour implémenter un changement apporté à un service qui n'est ni standard ni urgent.
Standard	Demande de changement préautorisée et à faible risque fréquemment implémentée. Les demandes de changement standard approuvées peuvent être prédéfinies dans un catalogue de modèles pour améliorer l'accès et le processus de demande d'un changement standard. Si cette option est sélectionnée, deux champs s'affichent. Sélectionnez-en un dans chaque liste pour remplir ces champs : ○ **Catégorie de changement** : sélectionnez une catégorie pour le changement dans votre catalogue existant, par exemple, Matériel, Changements standard du serveur, Logiciel. ○ **Modèle de changement** : sélectionnez un modèle disponible pour les demandes de changement avec des tâches de prise en charge prédéfinies à partir de votre catalogue. Pour en savoir plus sur les catégories de demandes de changement ITSM, les modèles et les types de changements, consultez Types de changements .

La fonctionnalité lit automatiquement les types de demandes de changement que vous configurez dans votre catalogue dans Gestion des changements ITSM. Par exemple, si vous changez le nom de vos demandes de changement standard dans ITSM de Standard à Préapprouvé, votre nouveau nom s'affiche automatiquement dans la liste Type de changement du formulaire Créer une demande de changement.

7. Les champs de la section Aperçu de la demande de changement du formulaire sont pré-remplis avec des informations provenant de la tâche de rattrapage.
Si nécessaire, modifiez ces champs.

8. Cliquez sur **Créer un changement**.
La demande de changement s'affiche. Dans la liste connexe CI affectés, les CI des résultats des tests qui correspondent à vos critères sont affichés. Si la demande de changement nécessite une approbation, le bouton **Demander l'approbation** s'affiche.

Une fois la demande de changement créée, le groupe de résultats des tests passe à l'état **En attente d'implémentation** . Une fois la demande de changement pour cette tâche de rattrapage résolue, s'il n'y a pas d'autres demandes de changement ouvertes associées à cette tâche de rattrapage, la tâche de rattrapage passe également à l'état **Résolu** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage pour plus d'informations.

Remarque : Vous pouvez toujours déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à un autre de leur cycle de vie sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'une demande de changement a changé d'état, ou que vous ajoutez une demande de changement ou la supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la tâche de rattrapage des états Fermé ou Différé .

Associer une tâche de rattrapage à une demande de changement existante

Associez une tâche de rattrapage dans Conformité de la configuration l'application à une demande de changement existante.

Avant de commencer

Rôle requis : un utilisateur avec le rôle itil

Pourquoi et quand exécuter cette tâche

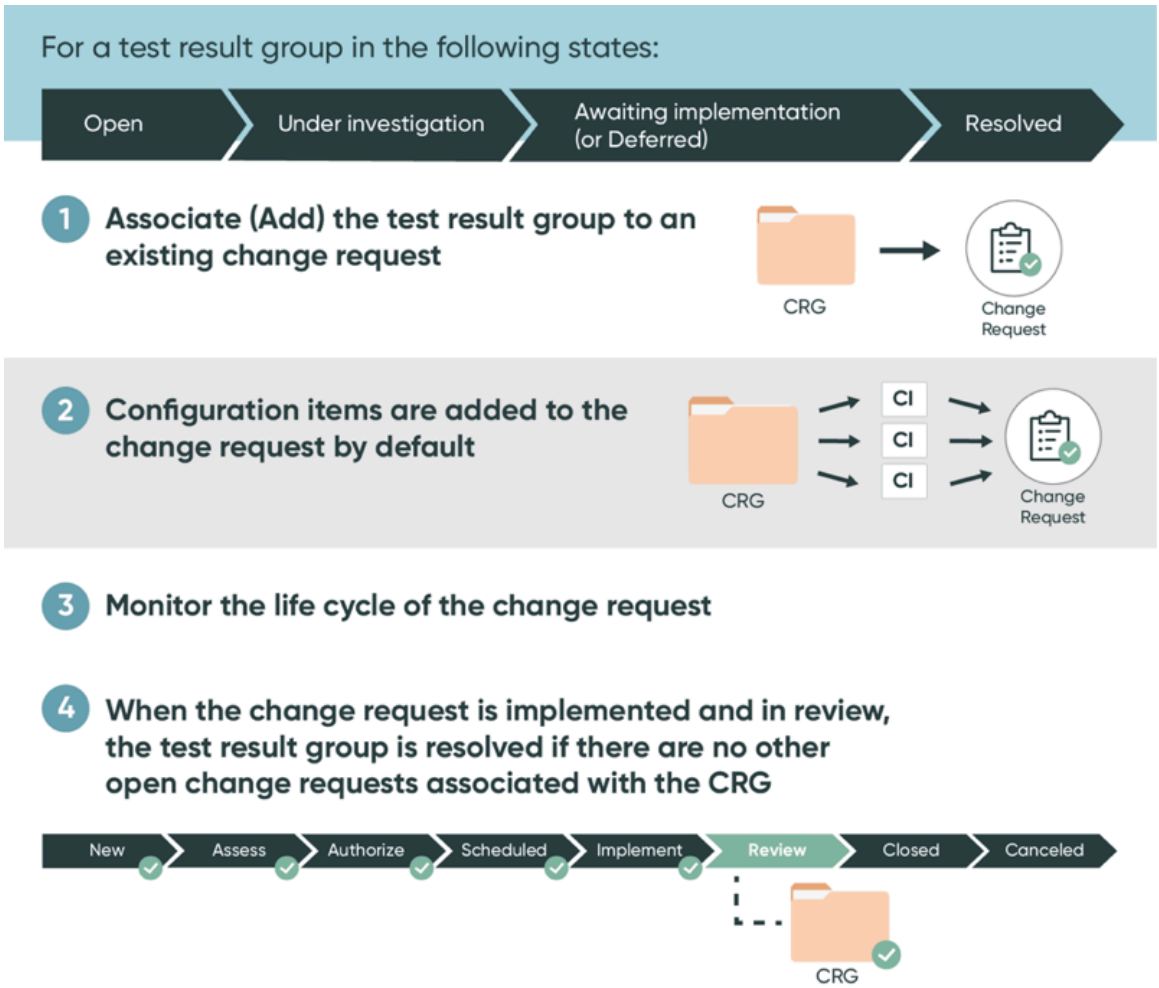
En tant qu'informaticien ou spécialiste du rattrapage, évitez de créer des demandes de changement en double lorsque vous travaillez à résoudre vos tâches de rattrapage en associant une tâche de rattrapage à une demande de changement déjà disponible dans votre instance.

Vous pouvez associer les tâches de rattrapage qui vous sont affectées ou qui sont affectées à votre groupe d'affectation à des demandes de changement existantes directement à partir des enregistrements de tâche de rattrapage. L'image suivante illustre le flux de base permettant d'associer une demande de changement existante à une tâche de rattrapage. Les étapes détaillées de ce flux suivent l'image.

Remarque : Vous pouvez associer une demande de changement existante à une tâche de **rattrapage** dans n'importe quel état autre qu'Annulé (**Ouvert**, **En cours d'examen**, **En attente d'implémentation**, **Fermé** et **Différé**). Vous pouvez associer des demandes de changement, y compris celles fermées au cours des 90 derniers jours, à partir du formulaire. Lorsque vous associez une demande de changement à une tâche de rattrapage existante, seuls les résultats des tests actifs et leurs éléments de configuration sont ajoutés à la demande de changement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Tâches de remédiation** > **Mes tâches ouvertes**.
   La liste des tâches de rattrapage affectées à vos groupes s'affiche.
2. Dans la colonne Nombre, cliquez sur la tâche de rattrapage pour laquelle vous souhaitez créer une demande de changement.

   L'enregistrement de la tâche de rattrapage s'affiche.
3. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Créer un changement**.
   Le formulaire de demande de changement s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Faites défiler jusqu'à la liste connexe Demandes de changement et sélectionnez-la.
   Toutes les demandes de changement associées à la tâche de rattrapage sont affichées avec le bouton **Ajouter** .
5. Cliquez sur **Ajouter**.
   La boîte de dialogue Ajouter une demande de changement existante à une tâche de rattrapage s'affiche.
6. Cliquez sur l'icône de recherche et sélectionnez un élément dans la liste.
   Vous pouvez filtrer la liste affichée pour affiner votre recherche.
7. Cliquez sur **Envoyer**.
   Le TRG s'affiche avec un message indiquant que la demande de changement a été associée avec succès à la tâche de rattrapage. La nouvelle demande de changement s'affiche sous la liste connexe des demandes de changement. Les CI de la tâche de rattrapage sont ajoutés par défaut à la demande de changement et s'affichent dans la liste connexe CI affectés. Vous pouvez également ajouter des CI à la demande de changement à partir de cette liste connexe. Un message indique le nombre de résultats des tests qui ont été transférés vers la nouvelle tâche de rattrapage, et le nouveau RT s'affiche.

   Remarque : Pour moins de 200 résultats de test, l'opération de division est effectuée de manière synchrone et les résultats des tests sont affichés dans la nouvelle tâche de rattrapage.

   Pour plus de 200 résultats de test, l'opération de fractionnement est effectuée de manière asynchrone en arrière-plan, et l'affichage des résultats de test dans la nouvelle tâche de rattrapage peut prendre quelques secondes. Le message suivant s'affiche également : n résultats des tests seront transférés prochainement de TRGxxxxxxx vers la nouvelle tâche de rattrapage GRCxxxxx.

   Vous pouvez associer toutes les demandes de changement à la tâche de rattrapage, à l'exception des exceptions suivantes :

   - Demandes de changement ayant l'état **Annulé** .
   - Demandes de changement dont l'état **est Fermé** depuis plus de 90 jours.
   - Demandes de changement déjà associées au RT. Le système ne vous permet pas d'associer une demande de changement qui est déjà associée au RT.

   Une fois la demande de changement pour cette tâche de rattrapage résolue, s'il n'y a pas d'autres demandes de changement ouvertes associées à cette tâche de rattrapage, la tâche de rattrapage passe également à l'état**Résolu** .

   Remarque : Vous pouvez toujours déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à un autre de leur cycle de vie sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'une demande de changement a changé d'état, ou que vous ajoutez une demande de changement ou la supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la tâche de rattrapage des états Fermé ou Différé .

   Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.

Fractionner une tâche de rattrapage

À partir d'une tâche de rattrapage existante dans l'application Conformité de la configuration , identifiez un sous-ensemble de résultats des tests que vous souhaitez déplacer vers une nouvelle tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : En tant qu'administrateur et propriétaire de rattrapage, vous pouvez fractionner une tâche de rattrapage à partir de l'espace de travail du gestionnaire de vulnérabilité et de l'espace de travail de rattrapage informatique respectivement.

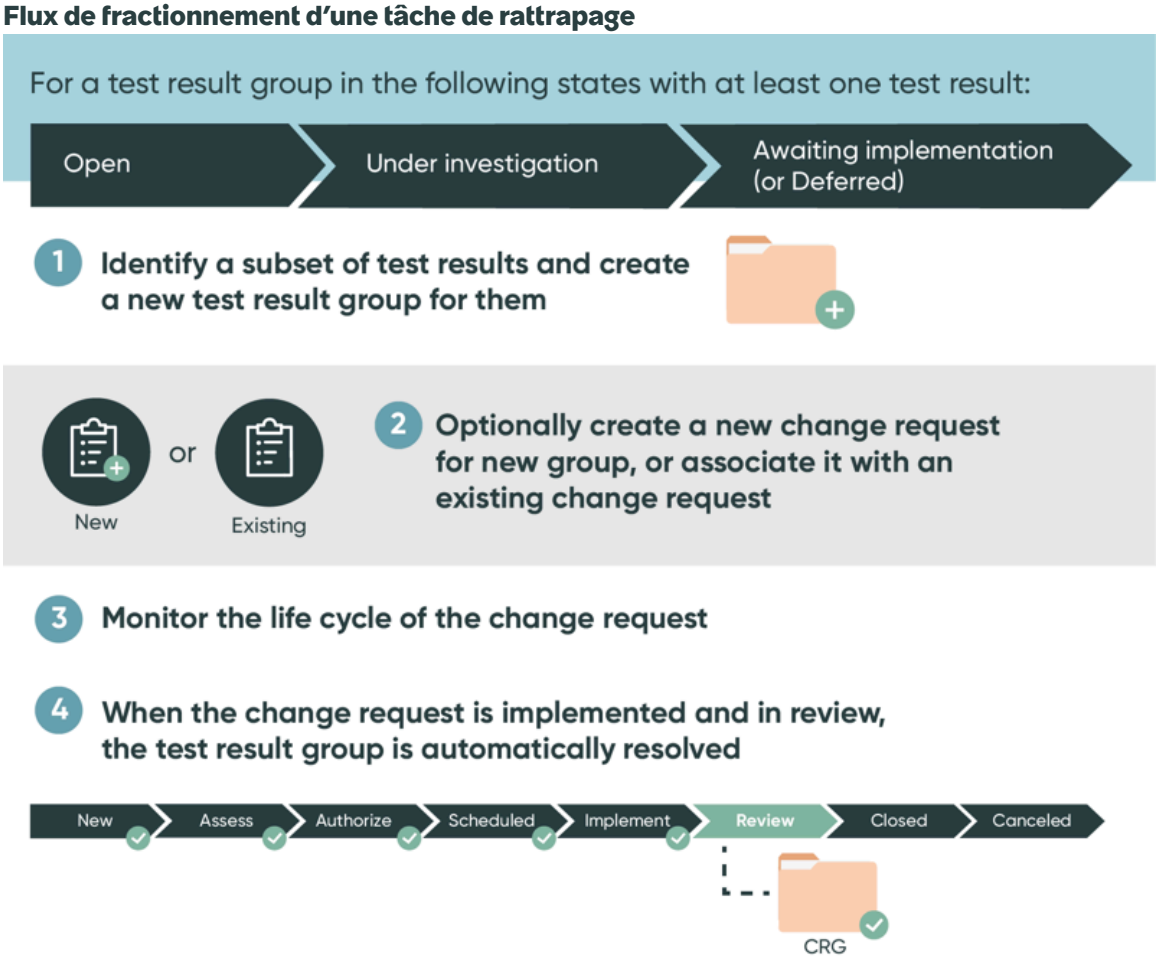
Avant de commencer
Rôle requis : un utilisateur avec le rôle itil

Pourquoi et quand exécuter cette tâche
En tant qu'informaticien ou spécialiste du rattrapage, vous pouvez diviser les tâches de rattrapage existantes dans les états **Ouvert**, **En cours d'examen** ou **En attente d'implémentation** avec plusieurs résultats de test. En créant une nouvelle tâche de rattrapage avec des résultats des tests qui correspondent à des critères spécifiques, vous pouvez utiliser un groupe spécifique de résultats des tests sans impact sur la tâche de rattrapage d'origine.

Lorsque vous spécifiez les conditions des résultats des tests que vous souhaitez déplacer vers une nouvelle tâche de rattrapage avec le générateur de conditions, seuls les résultats des tests actifs qui correspondent à vos critères sont déplacés vers la nouvelle tâche. Vous n'avez pas besoin de créer des demandes de changement lorsque vous fractionnez une tâche de rattrapage. Vous pouvez diviser une tâche de rattrapage en même temps que vous créez une demande de changement ou vous pouvez diviser une tâche de rattrapage sans créer de demande de changement.

L'image suivante illustre le flux de base pour diviser une tâche de rattrapage. Les étapes détaillées de ce flux suivent l'image.

Flux de fractionnement d'une tâche de rattrapage



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les cas d'utilisation pour diviser les résultats des tests de tâches de rattrapage existantes en nouvelles tâches peuvent inclure les exemples suivants :

- Lorsque vous souhaitez créer une demande de changement ou des demandes de changement pour une tâche fractionnée.
- Lorsque vous réaffectez une tâche fractionnée à un autre utilisateur de votre groupe d'affectation.
- Lorsque vous demandez un report ou une exception pour une tâche fractionnée parce que vous savez que certains résultats des tests sur des éléments de configuration (CI) spécifiques ne peuvent pas être corrigés dans un délai donné.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Tests** > **Tâches de remédiation** > **Mes tâches ouvertes**.
   La liste des tâches de rattrapage affectées à vos groupes s'affiche.
2. Dans la colonne Nombre, cliquez sur la tâche de rattrapage que vous souhaitez diviser.

   L'enregistrement de la tâche de rattrapage s'affiche.
3. Pour créer un sous-ensemble de résultats des tests pour une nouvelle tâche qui correspond à des critères spécifiques, procédez comme suit.

   Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Fractionner la tâche**.

   Vous préférez peut-être cette méthode de création d'une nouvelle tâche de rattrapage si vous travaillez à partir d'un grand groupe avec plusieurs résultats de test.

   Le formulaire Diviser le formulaire de tâche de rattrapage s'affiche.
4. Une fois le générateur de conditions affiché, spécifiez les conditions des résultats des tests que vous souhaitez déplacer vers une nouvelle tâche de rattrapage.

   Par exemple, vous pouvez filtrer uniquement les résultats des tests qui correspondent aux conditions suivantes :

   - À l'état **Ouvert** .
   - Scores de risque supérieurs à 75.
   - Le résultat est **Échec**.

   Si les résultats des tests correspondent à votre filtre après avoir saisi les conditions, un message s'affiche avec le nombre de résultats des tests correspondants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si un message s'affiche indiquant qu'aucun résultat de test ne correspond à votre filtre ou que tous vos résultats de test correspondent à vos critères, ajustez les conditions de sorte qu'au moins un résultat de test corresponde à vos critères de filtre.

5. Cliquez sur **Visualiser les éléments** pour afficher les résultats des tests correspondants.
   Une nouvelle fenêtre, Tâches de rattrapage, affiche les éléments.
6. Pour prévisualiser les détails des résultats des tests qui correspondent à vos critères de filtre, procédez comme suit avant de cliquer sur **Fractionner la tâche** pour créer le groupe.
   Ces détails incluent le groupe d'affectation et le destinataire de l'affectation du résultat du test. L'affichage de ces informations dans l'aperçu peut aider à s'assurer que la nouvelle tâche est correctement affectée.

   a. Une fois la liste Rattrapages affichée dans l'aperçu, cliquez sur un élément dans la colonne Résultat.
      L'enregistrement des résultats du test s'affiche.

   b. Vérifiez que les champs **Groupe d'affectation** et **Affecté à** sont corrects.

   c. Cliquez sur **Mettre à jour**.

7. Lorsque vous êtes prêt à créer la nouvelle tâche de rattrapage, cliquez sur **Fractionner la tâche**.
   Un message indique le nombre de résultats des tests qui sont transférés vers la nouvelle tâche de rattrapage, et la nouvelle tâche de rattrapage s'affiche. Pour vous aider à identifier la nouvelle tâche, vous pouvez modifier le texte dans le champ **Description brève** et modifier à nouveau les champs Groupe d'affectation ou Affecté à, si nécessaire.

   Remarque : Pour moins de 200 résultats de test, l'opération de fractionnement est effectuée de manière synchrone et les résultats des tests sont affichés dans la nouvelle tâche.

   Pour plus de 200 résultats de test, l'opération de fractionnement est effectuée de manière asynchrone en arrière-plan, et l'affichage des résultats du test dans la nouvelle tâche peut prendre quelques secondes. Le message suivant s'affiche également : n résultats des tests seront transférés prochainement de TRGxxxxxxx vers la nouvelle tâche de rattrapage GRCxxxxx.

8. Vous pouvez également créer une nouvelle tâche de rattrapage en sélectionnant les résultats des tests directement dans la liste connexe Résultats des tests d'une tâche de rattrapage.

   Vous pouvez préférer cette méthode si vous n'avez que quelques résultats de test dans une tâche de rattrapage, ou si vous savez exactement quels tests vous souhaitez déplacer vers une nouvelle tâche de rattrapage.

   a. Une fois l'enregistrement de la tâche de rattrapage affiché, accédez à la liste connexe Résultats des tests.

   b. Dans la colonne située tout à gauche, cochez les cases correspondant aux résultats des tests pour lesquels vous souhaitez créer une tâche de rattrapage.

   c. Dans la liste Actions sur les lignes sélectionnées située en bas à gauche de l'enregistrement, cliquez sur **Fractionner la tâche**.

   d. Dans le formulaire Diviser la tâche de rattrapage qui s'affiche, pour vous aider à identifier le nouveau groupe, vous préférez peut-être modifier le texte dans le champ **Brève description** .

   e. Cliquez sur **Fractionner la tâche**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un message indique le nombre de résultats des tests qui ont été déplacés vers la nouvelle tâche, et la nouvelle tâche de rattrapage s'affiche.

Une fois la demande de changement pour cette tâche de rattrapage résolue, s'il n'y a pas d'autres demandes de changement ouvertes associées à cette tâche de rattrapage, la tâche de rattrapage passe également à l'état **Résolu** .

Remarque : Vous pouvez toujours déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à un autre de leur cycle de vie sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'une demande de changement a changé d'état, ou que vous ajoutez une demande de changement ou la supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la tâche de rattrapage des états Fermé ou Différé .

Pour plus d'informations, consultez Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage.

Que faire ensuite

Vous pouvez créer ou associer des demandes de changement pour vos nouvelles tâches de rattrapage. Pour plus d'informations, consultez Associer une tâche de rattrapage à une demande de changement existante et Créer une demande de changement dans Conformité de la configuration.

Supprimer les affectations des tâches de rattrapage pour vous ou vos groupes

Réaffectez les enregistrements de résultats des tests dans l'application Conformité de la configuration s'ils vous ont été affectés de manière incorrecte à vous ou à votre groupe.

Avant de commencer

Rôle requis : sn_vulc.remediation_owner

Pourquoi et quand exécuter cette tâche

Si vous déterminez que les tâches de rattrapage (RT) et leurs résultats des tests associés ne se trouvent pas dans votre champ d'application pour le rattrapage, ou si vous pensez que des enregistrements vous ont été incorrectement affectés ou ont été affectés à vos groupes, vous pouvez vous supprimer ou supprimer vos groupes des champs Affecté à et Groupe d'affectation des enregistrements RT.

Le bouton **Annuler l'affectation** s'affiche sur les enregistrements de tâche de rattrapage dans tout état autre que l'état Fermé ou Résolu.

Procédure

1. Accédez à un enregistrement de tâche de rattrapage qui vous est affecté et dont l'état n'est pas Fermé ou Résolu.
2. Pour effacer les champs **Affecté à** et **Groupe d'affectation** , sélectionnez **Annuler l'affectation** en haut de l'enregistrement.
3. Dans la boîte de dialogue **Annuler l'affectation** , fournissez des notes de travail et sélectionnez **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les notes de travail que vous avez fournies sont affichées dans la section Notes.
- Dans l'onglet **Approbation du changement d'état** , l'enregistrement de l'approbation du changement d'état (CA#) affiche l'état En cours de révision, ce qui vous aide à suivre le workflow d'approbation.
- Sous l'onglet **Approbations demandées** , votre demande de suppression de vous ou de votre groupe d'affectation s'affiche sous l'état Demandé.

4. **Facultatif :** Vous pouvez également sélectionner **Annuler l'affectation** dans le menu Autres options () pour effacer les champs d'affectation.

Résultats

La demande est approuvée à l'aide d'un workflow d'approbation unique par défaut. Pour plus d'informations, consultez Approuver une demande de désaffectation dans Configuration Compliance.

- Si votre demande est approuvée, l'enregistrement d'approbation du changement d'état et l'enregistrement de l'approbation demandée passent à **l'état Approuvé**. Vos groupes et vous êtes retirés des champs **Affecté à** et **Groupe d'affectation** . Non affecté s'affiche dans le champ **Type d'affectation** et la tâche de rattrapage apparaît dans la liste du module Non affecté de l'application Conformité de la configuration .

  Les notifications indiquant que des enregistrements ne sont pas affectés sont envoyées automatiquement aux gestionnaires de vulnérabilité ou aux analystes du groupe de notification Annuler l'affectation. Pour plus d'informations sur les notifications et les propriétés de cette fonctionnalité, consultez Suppression d'affectations des groupes de résultats des tests Configuration Compliance.

- Si votre demande est rejetée, l'enregistrement d'approbation du changement d'état et l'enregistrement de l'approbation demandée passent à l'état Rejeté.

Remarque : En tant qu'administrateur de vulnérabilités, vous pouvez définir la `sn_vulc.unassign_test_result_group.approval_required` propriété système sur **false** pour désactiver le processus d'approbation.

Que faire ensuite

Accédez au module Non affecté de l'application, surveillez les enregistrements non affectés à la Conformité de la configuration recherche d'éléments susceptibles d'entrer dans votre champ d'application, puis réaffectez-les à vous-même.

Approuver une demande de désaffectation dans Conformité de la configuration

Approuvez les demandes de suppression des tâches de rattrapage d'un groupe d'affectation ou d'un utilisateur individuel dans l'application Conformité de la configuration .

Avant de commencer

Rôle requis : sn_vulc.unassign_approver

Pourquoi et quand exécuter cette tâche

Par défaut, une configuration d'approbation est fournie. Pour les approbations non affectées, un approbateur est requis dans le groupe d'approbation Approbateur de niveau 1. Par défaut, le groupe d'approbation Désaffecter (Désaffecter l'approbateur CC : niveau 1) est créé et les utilisateurs qui font partie de ce groupe peuvent approuver la demande. Par défaut, ce groupe contient le rôle d'approbateur de désaffectation,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sn_vulc.unassign_approver. Vous pouvez modifier ou créer un groupe et mettre à jour la configuration de l'approbation en accédant à **Tous** > **Configuration Compliance** > **Administration** > **Règles d'approbation** > **Demande de changement de champ de tâche de rattrapage** > **Tâches de rattrapage non affectées**.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande en ajoutant les commentaires appropriés.

Fermeture automatique des résultats des tests

Vous pouvez fermer automatiquement les résultats des tests associés aux éléments de configuration (CI) mis hors service.

Pour configurer l'option de fermeture automatique, accédez à la propriété système **sn_vulc.auto_close_test_results_linked_to_retired_CIs** et définissez-la sur vrai. Pour fermer automatiquement les résultats des tests associés aux CI mis hors service, reportez-vous à la section Fermer automatiquement les résultats des tests associés aux CI hors service.

Pour plus d'informations sur l'utilisation d'éléments de configuration mis hors service, reportez-vous à la section Utiliser des éléments de configuration mis hors service dans Configuration Compliance.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Utiliser des éléments de configuration mis hors service dans Configuration Compliance

Les éléments de configuration (CI) désactivés passent à l'état Mis hors service, Archivé ou Supprimé dans le Base de données de gestion des configurations (CMDB). Conformité de la configuration contient les résultats des tests (TR) qui sont constitués de CI. Lorsque l'état d'un CI est mis à jour sur mis hors service, les résultats des tests associés sont fermés avec le sous-état « CI désactivé ».

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si la CMDB modifie l'état de l'étape du cycle de vie d'un CI en Mis hors service, vous pouvez choisir de fermer automatiquement les résultats des tests associés. Pour plus d'informations sur la fermeture automatique des TR associés, reportez-vous à la section Fermer automatiquement les résultats des tests associés aux CI hors service.

Le CI mis hors service est finalement archivé ou définitivement supprimé du CMDB.

Impact de la mise hors service des CI :

- **Impact sur les éléments découverts :** Lorsque le CI est mis hors service, le DI connexe est marqué comme « CI désactivé ».
- **Impact sur les résultats des tests :** Lorsque l'état d'un élément de données est mis à jour sur « CI désactivé », le TR associé est fermé et la section Notes est automatiquement mise à jour.

> **Remarque :** L'état d'un élément de données est automatiquement mis à jour sur « CI désactivé » à chaque fois que l'état du cycle de vie d'un CI est mis à jour. D'autre part, l'état d'un TR n'est mis à jour sur Fermé que lorsque la propriété **sn_vulc.auto_close_test_results_linked_to_retired_CIs** est définie sur vrai. Pour plus d'informations sur la fermeture automatique des TR associés, reportez-vous à la section Fermer automatiquement les résultats des tests associés aux CI hors service.

La tâche *`Close Test Results for decommissioned CIs`* planifiée est exécutée quotidiennement pour les éléments de données mis à jour. Si l'option de configuration de fermeture automatique est activée pour les CI hors service, elle identifie le DI contenant un CI désactivé et ferme le TR associé avec le sous-état « CI désactivé ». Si tous les TR d'une tâche de rattrapage sont fermés et que leur sous-état est CI désactivé, la tâche de rattrapage est également fermée avec le sous-état « Annulé ».

> **Remarque :** Si un CI revient à l'état d'origine à partir de l'état « Mis hors service », l'entrée « Éléments détectés » est également mise à jour. Les TR sont automatiquement ouverts lorsque les données sont à nouveau ingérées à partir du scanner.

Fermer automatiquement les résultats des tests associés aux CI hors service

Si l'utilisateur modifie l'état Base de données de gestion des configurations (CMDB) de l'étape du cycle de vie d'un élément de configuration (CI) sur Mis hors service, vous pouvez choisir de fermer automatiquement les résultats des tests (TR) associés.

Avant de commencer

Rôle requis : sn_vulc.admin

Pourquoi et quand exécuter cette tâche

Pour fermer automatiquement les résultats des tests associés, vous devez activer la propriété système **sn_vulc.auto_close_test_results_linked_to_retired_CIs** pour fermer automatiquement les résultats des tests associés aux CI mis hors service. Si cette option est activée, les résultats des tests nouveaux et existants signalés pour le même CI sont automatiquement créés ou mis à jour dans l'état « Fermé ». Celles-ci sont basées sur l'ID d'actif dans la charge utile du scanner et l'état d'entrée des éléments détectés. Pour en savoir plus sur l'impact des CI hors service, reportez-vous à la section Utiliser des éléments de configuration mis hors service dans Configuration Compliance.

> **Remarque :** L'état d'un élément de données est mis à jour sur « CI désactivé » chaque fois que l'état du cycle de vie d'un CI est mis à jour. D'autre part, l'état d'un TR est mis à jour sur Fermé uniquement lorsque la propriété système **sn_vulc.auto_close_test_results_linked_to_retired_CIs** est activée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Propriétés système** > **Toutes les propriétés** et filtrez par `sn_vulc.auto_close_test_results_linked_to_retired_CIs` dans la colonne Nom.
2. Sélectionnez la propriété.
3. Pour fermer automatiquement les résultats des tests associés aux CI mis hors service, définissez la valeur de la propriété sur vrai.

Fermeture automatique des résultats des tests périmés dans Conformité de la configuration

Vous pouvez activer la fonctionnalité Fermer automatiquement les résultats des tests périmés pour fermer automatiquement les résultats des tests plus anciens qui n'ont pas été trouvés récemment par vos intégrations tierces. Le déplacement de ces résultats des tests vers **Fermé-Périmé** réduit le nombre de résultats des tests actifs et de tâches de rattrapage dans votre instance et vous aide à rapprocher les actifs dans votre Base de données de gestion des configurations (CMDB).

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Vue d'ensemble

Le module Fermer automatiquement les résultats des tests périmés vous aide à fermer automatiquement les résultats des tests anciens et périmés qui n'ont pas été trouvés récemment par vos intégrations tierces. Les résultats des tests sont déplacés vers **Fermé périmé** en fonction des conditions définies dans le générateur de conditions.

Termes clés

Résultat de test

Les résultats des tests sont importés à partir de bibliothèques de tests de configuration mappées sur des cadres de travail, des politiques et des sources faisant autorité qui définissent la manière dont une classe d'actifs technologiques doit être gouvernée. L'application Conformité de la configuration ne calcule pas les résultats des tests, mais les importe avec des intégrations tierces.

Date de dernière numérisation de l'actif

Fait référence à la valeur de la colonne Date de la dernière analyse Configuration Compliance de la table Élément détecté associée au résultat du test. Cette date fait référence à la date et à l'heure les plus récentes auxquelles un actif a été analysé pour la dernière fois par un scanner tiers.

Date du dernier échec

Fait référence à la date de la colonne Dernier observé de la table des résultats des tests lorsque la valeur du champ **Résultat** est [échec].

Résultats des tests périmés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fait référence aux résultats des tests de votre instance qui sont vieillis et qui n'ont pas été trouvés, mis à jour ou détectés par des analyses d'intégration tierces depuis une période significative.

Derniers résultats des tests trouvés

Cette option de recherche utilise une date et une heure fournies par le scanner tiers. Ce terme fait référence à la date la plus récente ou la plus récente (il y a plusieurs jours) à laquelle les résultats de test ont été retrouvés par le scanner. Ce paramètre peut être configuré.

Cas d'utilisation

Parfois, les actifs (éléments de configuration) peuvent être mis hors service dans votre environnement ou purgés par des scanners tiers. Lorsque cela se produit, les résultats des tests de configuration associés aux actifs ne sont pas mis à jour dans l'application Conformité de la configuration par les détections importées et ils deviennent inactifs (périmés).

Pour réduire le nombre de résultats des tests (TR) et de tâches de rattrapage (RT) actifs dans votre instance, activez la fonctionnalité Fermer automatiquement les résultats des tests périmés. Cette fonctionnalité ferme automatiquement les résultats des tests anciens dont l'état est inchangé ou qui n'ont pas été importés récemment par vos intégrations.

Par exemple, supposons qu'un élément de configuration (CI) particulier comporte plusieurs ID d'actifs et que l'un de ces ID n'a pas été importé sur les détections à partir d'un scanner tiers au cours des 90 derniers jours. Si vous configurez le générateur de conditions dans le module Fermer automatiquement les résultats des tests périmés pour fermer les résultats des tests qui n'ont pas été trouvés ou mis à jour au cours des 90 derniers jours ou plus, cette fonctionnalité ferme automatiquement tous les résultats des tests qui correspondent à ce filtrage.

Remarque : Cette fonctionnalité ferme uniquement les détections des résultats de test en fonction des conditions de filtre que vous avez définies dans le générateur de conditions et qui sont détectées par vos intégrations de scanners tiers.

Le champ Résolution

Pour différencier les détections fermées par des analyseurs tiers tels que les Qualys produits et Tenable.io la fonctionnalité Fermer automatiquement les résultats des tests périmés de votre instance, une nouvelle valeur a été ajoutée pour le champ **Résolution** , [Closed-Stale]. **Fermé-périmé** indique qu'un TR a été fermé par la fonction de fermeture automatique. **Fermé** ou **Fixe-Fermé** indique qu'un TR a été fermé par un scanner.

Déploiement des états TR sur les TRG avec la fonction de fermeture automatique

La progression et la préséance de l'état pour les résultats des tests sont les suivantes : **Ouvert** > **Fermé** > **Fixe-Fermé** > **Fermé : périmé**.

1. Si des TR d'un TRG sont **ouverts**, l'état du TRG n'est pas modifié.
2. Si au moins un TR est **Fermé - Corrigé** et que les autres sont **Fermé - Périmé**, l'état TRG passe à **Fermé - Corrigé**.
3. Si tous les TR d'un TRG sont **Fermé - Périmé**, l'état du TRG passe à **Fermé - Annulé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations prises en charge

Pour en savoir plus sur les intégrations tierces qui prennent en charge cette fonctionnalité, reportez-vous aux rubriques Présentation de Qualys Vulnerability Integration et Tenable.io Intégrations avec les Réponse aux vulnérabilités applications et Conformité de la configuration.

Utiliser la fermeture automatique des résultats des tests périmés dans Conformité de la configuration

Activez l'option Fermer automatiquement les résultats des tests périmés pour fermer automatiquement les anciens résultats des tests en fonction des conditions de filtre que vous définissez.

Avant de commencer

Pour en savoir plus sur cette fonctionnalité, les termes clés et les configurations éventuellement requises pour vos intégrations tierces qui importent des données de résultats de test, reportez-vous à la section Fermeture automatique des résultats des tests périmés dans Conformité de la configuration.

Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Administration** > **Fermer automatiquement les résultats des tests périmés**.
2. Renseignez les champs

Champ	Valeur
Nom	Nom de cet enregistrement de configuration.
Actif	Si cette option est sélectionnée, cet enregistrement est actif et ferme automatiquement tous les résultats des tests correspondant à ses critères de filtre.
Ignorer les résultats des tests périmés pour les résultats des tests différés	Si cette option est sélectionnée, tous les résultats des tests mappés à l'état **En cours de révision** ou **Différé** sont ignorés et non fermés. Si vous décochez cette option, tous les TR qui correspondent à vos critères seront fermés.
Ordre d'exécution	100 est la valeur par défaut. Cette valeur détermine l'ordre d'exécution par ordre croissant pour chaque enregistrement de configuration utilisé pour localiser et marquer les résultats des tests périmés.
Description	Description pour cet enregistrement. Ce texte peut vous aider à le retrouver facilement si vous créez un grand nombre d'enregistrements.
Condition	Conditions de filtrage utilisées pour trouver les résultats des tests que vous souhaitez fermer. Le filtre par défaut est **Élément détecté** > **Dernière analyse**.

3. Cliquez sur **Envoyer**.

La tâche planifiée, *Auto-Close Stale Test Results*, s'exécute quotidiennement. Cette tâche identifie les TR en fonction des conditions que vous avez fournies et fait passer ceux qui correspondent à l'état : **Fermé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que les TR sont marqués comme État : **Fermé-Périmé**, si le scanner les trouve à nouveau, les résultats des tests sont rouverts et les états repassent à**Ouvert**.

Si un TR est marqué comme État : **Fermé-Périmé** et que le scanner constate qu'il a été corrigé (Résolution : **Corrigé**), le TR passe à l'état : **Fermé** Résolution : **Corrigé**. Les TR qui ont un **résultat** : **Réussi** restent l'état : **Fermé** Résolution : **Corrigé**. Les états se déploient également aux tâches de rattrapage, comme décrit dans la liste suivante :

a. Si des TR d'une tâche de rattrapage sont **Ouverts**, l'état de la tâche de rattrapage n'est pas modifié.

b. Si au moins un TR est à l'état : **Fermé** Résolution : **Corrigé** et que les autres sont **Fermé-Périmé,** l'état de la tâche de rattrapage passe à **Fermé** Résolution : **Corrigé**.

c. Si tous les TR d'une tâche de rattrapage sont **Fermé** Résolution : **Corrigé**, l'état TRG passe à l'état : **Fermé** Résolution : **Annulé**.

Pour plus d'informations sur les transitions d'états, reportez-vous à la section Transitions d'états des résultats des tests et des tâches de rattrapage dans l'application Conformité de la configuration.

Fermer une tâche de rattrapage

Si vous déterminez que le problème associé à une tâche de rattrapage peut être fermé immédiatement sans analyse supplémentaire, vous pouvez utiliser la fonction **Fermer** .

Avant de commencer

Rôle requis :

- sn_vulc.admin
- sn_vulc.remediation_owner

Remarque : Le rôle sn_vulc.remediation_owner vous permet de réaffecter ou de fermer les tâches de rattrapage qui vous sont affectées ou qui sont affectées à vos groupes d'affectation.

Pourquoi et quand exécuter cette tâche

À partir de la version 15.0 de , le bouton **Fermer** a été supprimé pour une tâche de Conformité de la configuration rattrapage.

Lorsque vous résolvez une tâche de rattrapage, les notes de résolution sont reflétées dans les notes de travail de tous ses résultats de test.

Procédure

1. Ouvrez l'enregistrement de la tâche de rattrapage.

2. Sélectionnez le bouton **Fermer** .

3. Décrivez la raison pour laquelle le problème est fermé dans la fenêtre contextuelle.

4. Sélectionnez **Fermer**.

Information associée

Conformité de la configuration États

Demande et approbation d'une exception pour une tâche de rattrapage

Vous pouvez demander de reporter le rattrapage d'une tâche de rattrapage pour une période spécifiée. Les utilisateurs qui font partie du groupe d'approbateurs peuvent approuver les demandes d'exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Pour demander ou approuver des demandes d'exception, consultez :

- Demander une exception pour une tâche de rattrapage dans Conformité de la configuration
- Approuver une demande d'exception dans Conformité de la configuration

Remarque :

Des notifications par e-mail sont envoyées à chaque étape de la gestion des exceptions, fournissant l'état et d'autres détails d'une demande. Par exemple, lorsqu'une exception est demandée, le demandeur reçoit un e-mail confirmant que la demande est soumise. L'approbateur reçoit également un e-mail indiquant qu'une exception a été demandée.

À partir de la version 14.11 de , vous pouvez configurer les délais d'approbation des Conformité de la configuration exceptions, ainsi que les notifications par e-mail pour l'approbateur et le demandeur après un nombre de jours défini. Lorsqu'une demande est émise, le résultat des tests passe à l'état En cours de révision et un enregistrement de changement d'état est créé. Si l'approbateur ne répond pas dans le délai configuré, le résultat du test revient à l'état Ouvert. L'état précédent est stocké dans le champ **backup_state** . Pour en savoir plus, consultez la rubrique Configurer les règles d'approbation pour la gestion des exceptions.

Demander une exception pour une tâche de rattrapage dans Conformité de la configuration

Demandez une exception pour différer le rattrapage d'une tâche de rattrapage pour une période spécifiée s'il ne peut pas être corrigé immédiatement.

Avant de commencer

Rôle requis : sn_vulc.remediation_owner

Pourquoi et quand exécuter cette tâche

Important : Vous pouvez demander une exception pour :

- tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT. Pour plus d'informations, consultez Demander une exception dans le Espace de travail de remédiation IT.
- plusieurs résultats de tests simultanément du Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Demander une exception en bloc dans l'espace de travail du gestionnaire de vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Tâches de remédiation** > **Toutes les tâches**.
2. Sélectionnez la tâche de rattrapage pour laquelle vous souhaitez demander une exception.
   La tâche sélectionnée doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
3. Sur le formulaire Tâche de rattrapage, cliquez sur **Demande d'exception**.

   Remarque : Selon que ou Réponse aux vulnérabilitésGRC : Gestion de la politique et de la conformité est sélectionné dans le **Configuration Compliance** > **Gestion des exceptions** , le formulaire de demande d'exception change. Reportez-vous à la rubrique Configurer la gestion des exceptions pour Conformité de la configuration.

4. Si Réponse aux vulnérabilités est sélectionné dans l'écran Gestion des exceptions, procédez comme suit :

   a. Remplissez les champs du formulaire.

Formulaire de demande d'exception

Champ	Description
Jusqu'à	Date d'expiration de la demande d'exception. Cette date doit être comprise dans la durée sélectionnée dans le **Tous** > **Configuration Compliance** > **Administration** > **Gestion des exceptions** écran. Lorsque la demande d'exception expire, la tâche de rattrapage revient à son état Ouvert.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : À partir de la version 14.7 de (CC), si une tâche de rattrapage différée est rouverte par un scanner avant l'expiration de Conformité de la configuration la fenêtre d'exception, l'état de la tâche de rattrapage passe d'Ouvert à Différé. Cette fonctionnalité est désactivée par défaut. Pour activer cette fonctionnalité, définissez la valeur de la propriété `sn_vulc.auto_defer_test_result_in_active_exc` système sur vrai. En outre, la date de fin de report persiste même après la réouverture de la tâche de rattrapage après la date d'expiration.
Motif	Raison de l'exception. Les choix sont les suivants : ▪ Risque accepté ▪ En attente de fenêtre de maintenance ▪ Correctif non disponible ▪ Contrôle d'atténuation en place ▪ Autre Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir les mappages de motifs de politiques.
Informations supplémentaires	Détails liés au motif pour lequel cette demande est effectuée. Ce champ doit être mis à jour par le propriétaire du rattrapage.

b. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**.

Résultats

L'état de la tâche de rattrapage devient En cours de révision. Utilisez l'onglet **Approbation du changement d'état** pour suivre l'état de la demande d'exception.

Demander une extension pour une règle d'exception dans Conformité de la configuration

Demandez une extension pour une règle d'exception différée avant qu'elle n'atteigne sa date de report jusqu'à l'échéance. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.exception_approver

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension depuis les Réponse aux vulnérabilités espaces de travail. Pour plus d'informations, consultez Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Règles d'exception**.
2. Sélectionnez une règle d'exception approuvée.
3. Sélectionnez **Demande d'extension**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date jusqu'à laquelle la règle d'exception doit être prolongée.
Motif	Entrez le motif du report de la règle d'exception. Les choix sont les suivants : ○ Risque accepté ○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

5. Sélectionnez **Demander l'approbation**.
   Lors de l'approbation de la demande, les champs Différé jusqu'à, Motif et Informations supplémentaires sont mis à jour sur la règle d'exception et les tâches de rattrapage associées. Un e-mail est également déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Si une règle d'exception différée est à nouveau étendue, le nombre de reports d'extension augmente dans le back-end.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander une exception pour les tâches de rattrapage à l'aide de GRC : Gestion de la politique et de la conformité

Demandez des exceptions à la politique à l'aide de l'aptitude de GRC gestion des exceptions de politique de l'application à partir de Conformité de la configuration.Gestion de la politique et de la conformité

Avant de commencer

Avant de pouvoir utiliser l'intégration des exceptions de politique pour demander des exceptions de politique, vous devez télécharger l'application à partir GRC : Gestion de la politique et de la conformité du ServiceNow Store.

Rôle requis : sn_vulc.remediation_owner

Vous pouvez également demander des exceptions dans l'interface utilisateur classique.

Pourquoi et quand exécuter cette tâche

Important : En tant qu'administrateur et propriétaire de rattrapage, vous pouvez demander une exception de politique pour une tâche de rattrapage (RT) dans l'espace de travail du gestionnaire de vulnérabilité et l'espace de travail de rattrapage informatique respectivement.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités de l'application** > **Éléments vulnérables de l'application** (ou **Tâches de remédiation**)>**Toutes**, et ouvrez l'élément ou le groupe pour lequel vous souhaitez demander une exception.
   L'élément ou le groupe sélectionné doit être dans l'état Ouvert, En cours d'examen ou En attente d'implémentation.
2. Sur le formulaire sélectionné, cliquez sur **Demande d'exception**.
3. Si GRC : Gestion de la politique et de la conformité est sélectionné dans l'écran Gestion des exceptions, procédez comme suit.

   a. Remplissez les champs du formulaire.

Formulaire de demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commencera. La valeur par défaut est la date actuelle. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et à laquelle l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert. **Remarque :** Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale de l'exception (jours)** que vous définissez pour la politique dans Politique et conformité. Pour plus d'informations, consultez Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails liés au motif pour lequel cette demande est effectuée. Ce champ doit être renseigné par le propriétaire du rattrapage.

b. Soumettez la demande d'exception en cliquant sur **Demander l'approbation**.
L'état de la tâche de rattrapage est En cours de révision et une exception de politique est créée. Utilisez l'onglet **Approbation du changement d'état** pour suivre l'état de la demande d'exception.

c. Pour afficher l'exception de politique, cliquez sur la liste connexe Exceptions de politique.

d. Cliquez sur le numéro d'exception de politique.

e. Dans le champ **Approbateur** , sélectionnez son nom.

f. Cliquez sur l'onglet Source et sélectionnez un objectif de contrôle dans le champ **Objectif de contrôle** .

g. Cliquez sur l'onglet Évaluation des risques et sélectionnez l'évaluation du risque dans le champ **Évaluation du risque** .

h. Enregistrez le formulaire.

i. Cliquez sur l'onglet **Contrôles impactés** .

j. Ajoutez les commandes en cliquant sur **Ajouter**.

k. Enregistrez le formulaire.

Remarque : Vous pouvez effectuer un examen de conformité en cliquant sur **Demander un examen de conformité**.

Le formulaire d'approbation est envoyé à l'approbateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'approbateur peut approuver la demande en cliquant sur **Approuver** ou demander une approbation supplémentaire en cliquant sur **Demander une approbation supplémentaire**.

L'état de l'enregistrement devient Différé. Le motif indiqué est celui que vous avez sélectionné lors de l'émission de la demande d'exception. L'onglet **Report** fournit des notes supplémentaires sur l'enregistrement.

Remarque : Si la demande est rejetée, l'enregistrement revient à son état précédent.

4. Cliquez sur **Envoyer**.
   Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez Configuration facultative de Policy and Compliance Management .

Approuver une demande d'exception dans Conformité de la configuration

Approuvez les demandes d'exception pour les tâches de rattrapage qui ne peuvent pas être corrigées immédiatement. Vous devez évaluer ces demandes pour connaître le risque, puis approuver leur report jusqu'à ce qu'elles puissent être corrigées.

Important : En tant qu'administrateur ou analyste, vous pouvez approuver ou rejeter une demande d'exception à partir de l'espace de travail du gestionnaire des vulnérabilités.

Avant de commencer
Rôle requis : sn_vulc.exception_approver

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Mes approbations**.
2. Sélectionnez une demande dans votre file d'attente.
3. Approuvez ou rejetez la demande avec les commentaires appropriés.

Remarque : Dans le cas d'un workflow d'approbation à deux niveaux, après l'approbation de premier niveau, la demande est soumise au deuxième niveau pour une approbation supplémentaire. Si aucun utilisateur ne se trouve dans le deuxième niveau, la demande est automatiquement approuvée après l'approbation de premier niveau.

Une fois la demande approuvée, la tâche de rattrapage passe à un état Différé. En cas de rejet, la tâche de rattrapage revient à son état antérieur.

Définir les mappages de motifs de politiques

Vous pouvez définir les choix de motifs pour qu'ils soient accessibles à tout utilisateur qui demande une exception.

Avant de commencer
Rôle requis : sn_vul.compliance.manager et sn_vulc.admin

Procédure

1. Accédez à la **Tous** > **Politique et Conformité** > **Exceptions de politique** > **Registre d'intégration**.

Remarque : Vous pouvez sélectionner un motif parmi les choix de motifs disponibles dans la table Choix de motifs ou ajouter un nouveau motif.

2. Cliquez sur le registre d'intégration Container Vulnerability Response - CVIT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Pour ajouter un choix de motif existant, procédez comme suit :
   a. Dans la liste Choix des motifs, cliquez sur **Nouveau**.
   b. Cliquez sur l'icône de loupe pour sélectionner un motif.
4. Pour ajouter de nouveaux choix de motifs à la table Choix de motifs, procédez comme suit :
   a. Dans la liste Choix de motifs, cliquez sur **Nouveau**.
   b. Cliquez sur l'icône de loupe.
   c. Cliquez sur **Nouveau**.
   d. Remplissez les champs du formulaire.

Formulaire Liste de choix de motifs

Champ	Description
Étiquette	Étiquette unique pour ce choix.
Valeur	Valeur unique pour ce choix. Cette valeur est mappée dans la table Mappages de motif d'exception de politique pour les applications respectives. Pour accéder à cette table, saisissez sn_sec_cmn_policy_reason_mapping. LIST dans le navigateur de filtre.
Ordre	Ordre pour ce choix. Les motifs sont classés en fonction de ce nombre.
Par défaut	Option pour indiquer que ce choix de motif sera disponible chaque fois qu'une exception de politique sur demande est demandée. Si le registre d'intégration ne contient pas de choix spécifiques à l'application, tous les choix de motifs pour lesquels le champ **Par défaut** est sélectionné seront disponibles.
Actif	Option permettant d'afficher le choix dans la liste des choix de motifs.

5. Cliquez sur **Envoyer**.

Solutions d'analyse et de génération de rapports pour Conformité de la configuration

Les rapports suivants sont fournis à des fins de surveillance.

Affichez les politiques, les CI, les tests et les résultats des tests dans les rapports de vue d'ensemble Conformité de la configuration .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Conformité de la configuration Rapports

La Conformité de la configuration page d'accueil fournit une vue d'ensemble des politiques, des CI, des tests et des résultats des tests, ce qui aide le personnel de sécurité à identifier rapidement les zones de préoccupation. Conformité de la configuration Des tableaux de signification peuvent être ajoutés, selon les besoins. Vous pouvez également renvoyer Conformité de la configuration des informations liées à à l'aide de la fonction de recherche globale.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Dans chaque graphique, vous pouvez pointer vers n'importe quelle partie d'un graphique (barre, secteur, point de données) pour afficher des données générales spécifiques à cette partie du graphique. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

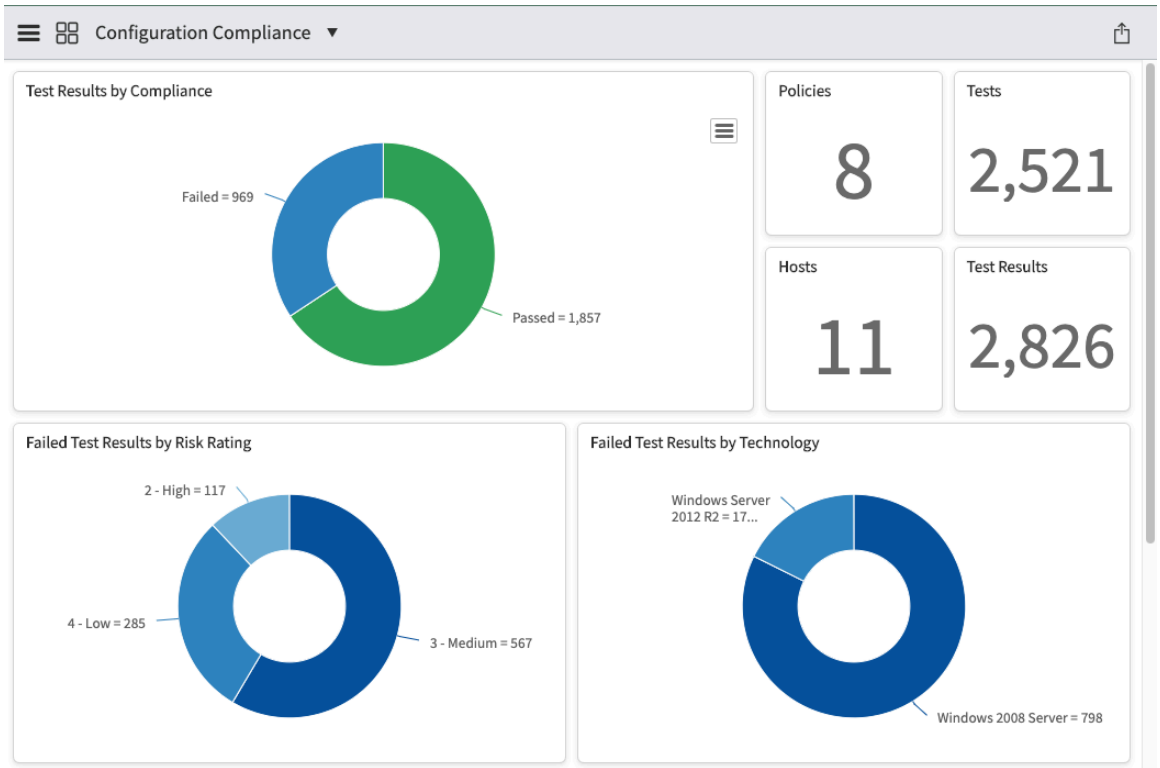
Remarque :

- Les tableaux de bord sur la page d'accueil Conformité de la configuration ne sont disponibles que lorsque l'application Analyse des performances pour Configuration Compliance est activée. Pour connaître la procédure d'activation de cette application, reportez-vous à la section Activer Analyse des performances pour Conformité de la configuration.
- Toute personne disposant du rôle sn_vulc.read peut afficher le tableau de bord. Toute personne disposant du rôle sn_vulc.write ou sn_vulc.admin peut créer et modifier un tableau de bord. Seul sn_vulc.admin peut supprimer un tableau de bord.

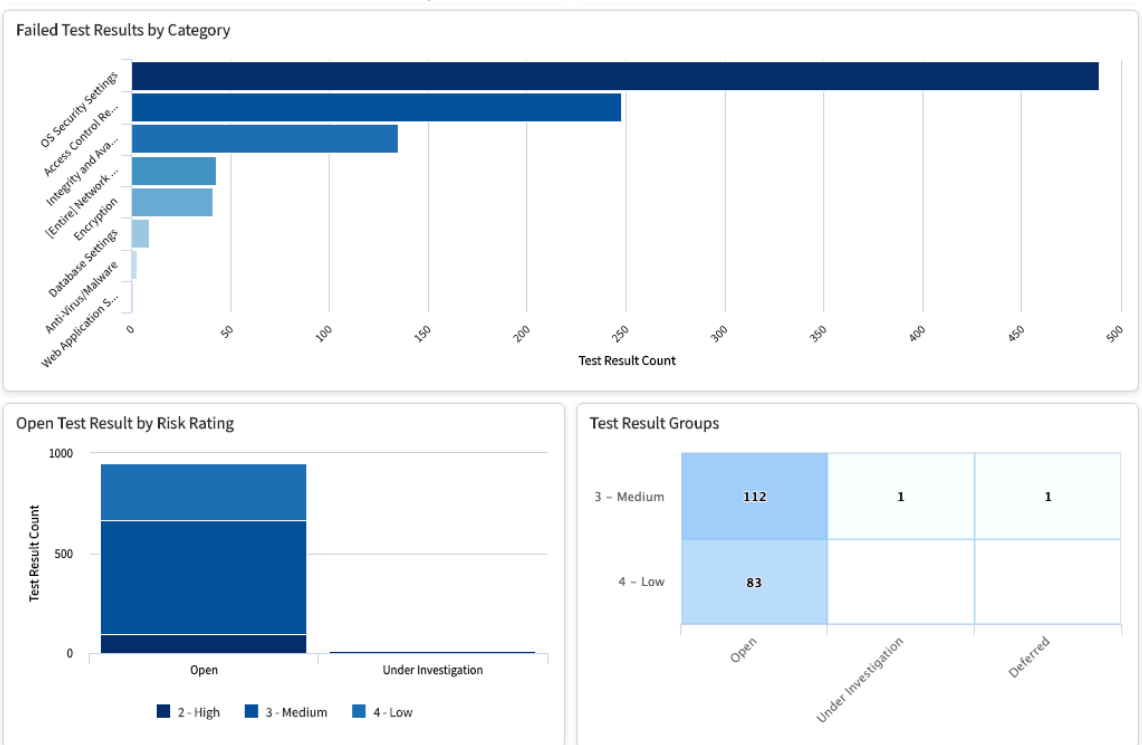
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble de la vulnérabilité



Rapport de conformité de la configuration



Rapports Vue d'ensemble de la vulnérabilité

Nom	Visuel	Description
Résultats des tests par conformité	Couronne	Affiche le nombre de tests ouverts qui ont réussi ou échoué.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble de la vulnérabilité (suite)

Nom	Visuel	Description
Politiques	Numéro	Nombre de politiques avec des résultats de test ayant échoué.
Tests	Numéro	Nombre de tests avec des résultats de test ayant échoué.
Hôtes	Numéro	Nombre d'hôtes avec des résultats de test ayant échoué.
Résultats des tests	Numéro	Affiche le nombre de résultats des tests.
Résultats des tests ayant échoué par cote de risque	Couronne	Affiche le nombre de tests ayant échoué par cote de risque.
Résultats des tests échoués par technologie	Couronne	Affiche les modèles avec des tests ayant échoué.
Résultats des tests échoués par catégorie	À barres	Affiche les catégories avec le plus grand nombre de résultats des tests ayant échoué.
Ouvrir le résultat des tests par cote de risque	À barres	Affiche le nombre de résultats des tests ouverts par cote de risque.
Tâches de remédiation	Graphique	Affiche les tâches de remédiation par état et cote de risque.

Conformité de la configuration tableau de bord

Contient Solution d'analyse des performances et génération de rapports du contenu préemballé Analyse des performances et Reporting du contenu à utiliser avec d'autres ServiceNow AI Platform produits. Cela Solution d'analyse des performances et génération de rapports fournit une visibilité sur les configurations non conformes au niveau de l'hôte et du plan de contrôle dans le cloud.

Cette solution Platform Analytics contient du contenu Performance Analytics and Reporting prédéfini à utiliser avec d'autres ServiceNow AI Platform produits. Cette solution Platform Analytics offre une visibilité sur les configurations non conformes au niveau de l'hôte et du plan de contrôle dans le cloud.

Le tableau de bord Analyse des performances pour Configuration Compliance contient plusieurs widgets qui présentent des données pour différentes dimensions. Elle fournit une vue complète des tendances de conformité, des problèmes de configuration, des tendances de rattrapage et de la gestion des exceptions.

Remarque : Le module d'extension Analyse des performances for Conformité de la configuration doit être installé pour afficher le tableau de Conformité de la configuration bord [PA] dans le cadre de Next Experience travail. S'il n'est pas installé, vous pouvez afficher le tableau de bord existant, qui est créé à l'aide de l'infrastructure de génération de rapports.

Activer Analyse des performances pour Conformité de la configuration

Activez l'application de pack ServiceNow Store de contenu pour le Solution d'analyse des performances et génération de rapports.

Avant de commencer

Activez la version complète de l'abonnement de Analyse des performances sur l'instance où vous activez cette Solution d'analyse des performances et génération de rapports. Vous pouvez activer Analyse des performances sur une instance de non-production sans acheter d'abonnement. Pour plus d'informations, consultez Activer votre abonnement Analyse des performances .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez besoin d'un compte et d'une autorisation pour demander des Now Support applications pour les instances à l'étude. Le Now Support compte et l'instance doivent faire partie de la même entreprise. Pour plus d'informations, voir Installer un produit ServiceNow dans le ServiceNow Store.

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Utilisez cette fonction Analyse des performances pour que le tableau de Conformité de la configuration bord génère des rapports sur les tâches de rattrapage, l'état de conformité, les actions de rattrapage et les demandes d'exception.

Procédure

1. Accédez à la **Tous** > **Applications système** > **Toutes les applications** > **ServiceNow Store**.
2. Recherchez Analyse des performances et vérifiez Conformité de la configuration que vous disposez des autorisations valides.
3. Recherchez Analyse des performances pour Configuration Compliance.
4. Installez l'application.

   Lorsque vous installez cette application, vous l'activez Conformité de la configuration également.

Afficher le pour le Analyse des performances Conformité de la configuration tableau de bord

Vous pouvez gérer vos problèmes de configuration les plus importants et les corriger rapidement en affichant les rapports sur le tableau de Conformité de la configuration Analyse des performances bord (PA).

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Rôles ServiceNow AI Platform requis

Les rôles suivants sont requis pour le tableau de Conformité de la configuration Analyse des performances bord :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- admin : un administrateur peut installer, activer Analyse des performances le pour Conformité de la configuration et apporter des modifications aux propriétés système.
- pa_admin : Un administrateur Performance Analytics peut créer et examiner les tâches en arrière-plan, les indicateurs, les répartitions, les widgets et les tableaux de bord. Cet administrateur peut également configurer et démarrer la collecte de données.
- sn_vulc.read : un utilisateur avec le rôle read peut examiner les données du tableau de bord.

Accéder au tableau de Conformité de la configuration bord

Pour ouvrir le tableau de bord, accédez à **Tous** > **Configuration Compliance** > **Vue d'ensemble**.

Important :

À partir de la version 14.9 de , ce tableau de Conformité de la configuration bord peut également être affiché dans l'interface utilisateur Next Experience. Pour afficher le tableau de bord dans la nouvelle interface utilisateur, accédez à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et cliquez sur l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher d'autres tableaux de bord, cliquez sur la liste déroulante en regard du nom du tableau de bord. Pour plus d'informations, consultez les tableaux de bord dans l'espace de travail Responsable des vulnérabilités et les tableaux de bord dans l'espace de travail Rattrapage informatique.

Remarque : Si vous êtes sur Tokyo, vous pouvez afficher les tableaux de bord dans l'interface utilisateur Next Experience, mais avec une perte fonctionnelle.

Conformité de la configuration Onglets du tableau de bord [PA]

Onglet Vue d'ensemble

L'onglet **Vue d'ensemble** fournit cinq filtres. Ces filtres sont la catégorie d'actif, le type de ressource dans le cloud, le fournisseur de services dans le cloud, le compte dans le cloud et la région du cloud, que vous pouvez appliquer pour visualiser les rapports pour les filtres appliqués. Si vous sélectionnez une catégorie et appliquez les modifications, tous les widgets prenant en charge la catégorie sont actualisés. Chaque widget affiche le filtre appliqué en bas et le nombre de filtres appliqués sur l'icône de filtre du widget. Cliquez sur le rapport dans un widget pour afficher les informations supplémentaires dans l'onglet **Détails des KPI** . Dans l'onglet **Détails des KPI** , vous pouvez :

- Affichez les enregistrements.
- Comparez les enregistrements.
- Modifiez le type de graphique.
- Sélectionnez la plage de dates.
- Affichez les tendances basées sur la durée.
- Appliquez les filtres supplémentaires, y compris ceux qui ne sont pas disponibles dans l'onglet **Vue d'ensemble** . Un exemple est la balise Host.

L'exemple suivant montre comment appliquer les filtres dans l'onglet **Vue d'ensemble** et effectuer les actions dans l'onglet **Détails des KPI** .

Onglet Vue d'ensemble dans le tableau de bord Configuration Compliance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Conformité

L'onglet **Conformité** affiche le pourcentage de conformité pour les différentes sources de référence, telles que la loi HIPAA (Health Insurance Portability and Accountability Act) et la DISA (Data Interchange Standards Association). Vous pouvez affiner cette liste en utilisant les filtres d'en-tête de colonne et en sélectionnant une catégorie.

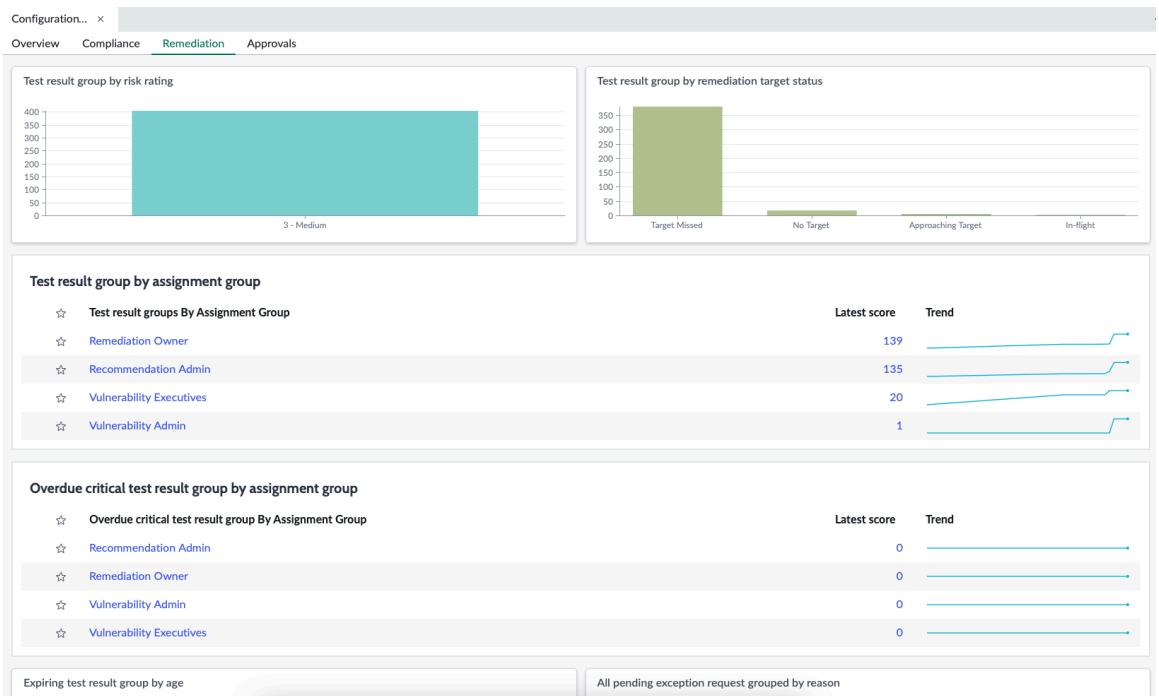
L'exemple suivant montre comment filtrer les données dans l'onglet **Conformité** .

Onglet Conformité du tableau de bord Configuration Compliance

Onglet Rattrapage

L'onglet **Rattrapage** affiche les informations sur la progression du rattrapage. Vous pouvez utiliser cet onglet pour en savoir plus sur l'hygiène du rattrapage des erreurs de configuration.

L'exemple suivant montre l'onglet **Correction** .



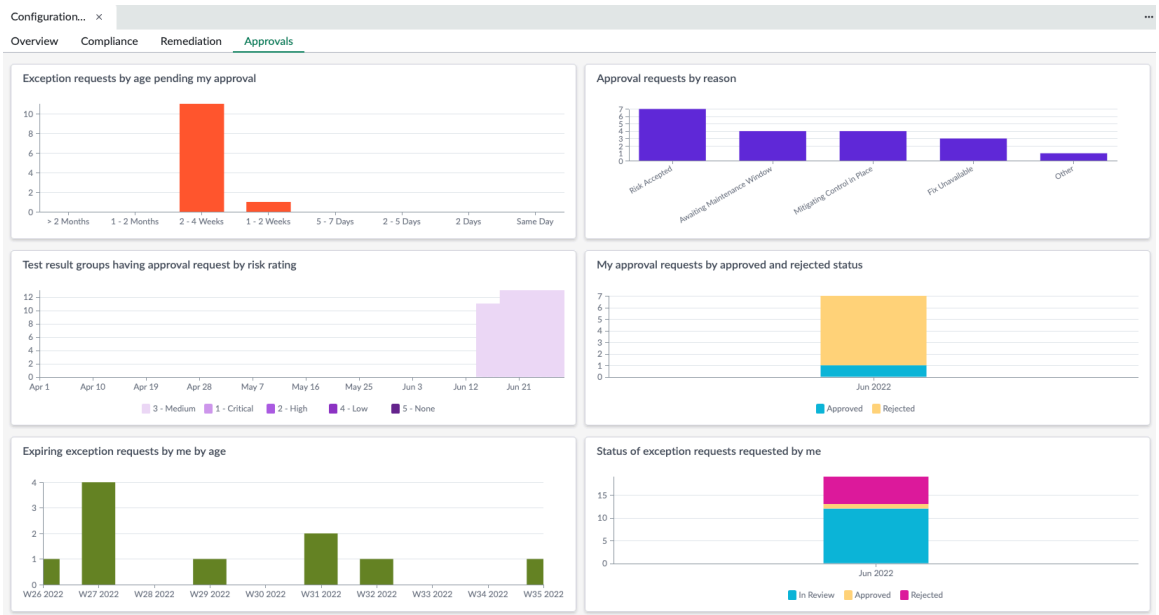
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Approbations

Les rapports de l'onglet **Approbations affichent les** informations relatives aux demandes d'exception et leur état d'approbation.

L'exemple suivant montre l'onglet **Approbations** .



Répartitions

Les répartitions utilisées par les indicateurs sont les suivantes :

- Raison de l'ajournement
- Âge
- Groupe d'affectation
- Statut de la remédiation
- Résultat
- Cote de risque
- Catégorie d'actif
- Balise d'hôte
- Test de configuration
- Fournisseur de services dans le cloud
- Région du cloud
- Compte dans le cloud
- Type de ressource dans le cloud

Remarque : La personnalisation du calcul de l'âge et de l'âge fermé pour les résultats des tests peut entraîner une forte hausse ou une baisse des rapports d'Analyse des performances (PA) qui incluent ces mesures. Pour plus d'informations sur la personnalisation du calcul de l'âge et de l'âge fermé pour les résultats des tests, consultez l'article de la base de connaissances KB1703270 .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Filtres

Dans l'onglet **Vue d'ensemble** , vous pouvez appliquer les filtres suivants aux widgets pour visualiser les données filtrées.

Nom	Type	Description
Catégorie d'actif	Choix	Type d'actif. Les quatre options sont les suivantes : • Cloud • Conteneur • Infra • OT
Type de ressource dans le cloud	Choix	Type de ressource. Un exemple est un ordinateur virtuel. Les données du filtre sont renseignées lorsque vous exécutez l'intégration.
Fournisseur de services dans le cloud	Choix	Fournisseur de services pour le cloud. Les trois options sont les suivantes : • Amazon Web Services (AWS • Microsoft Azure • Google Cloud Platform (GCP)
Compte dans le cloud	Choix	ID de compte créé lorsqu'un compte est créé dans un service dans le cloud. Par exemple, AWS. Les données d'ID de compte sont renseignées dans le filtre lorsque vous exécutez l'intégration.
Région du cloud	Choix	Emplacement où la ressource est hébergée.

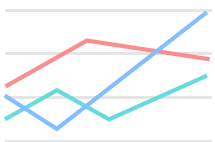
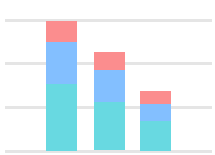
Remarque : Vous pouvez sélectionner plusieurs options dans les filtres et sélectionner **Appliquer**. Chaque widget affiche les filtres appliqués et ceux qui ne le sont pas. En fonction des données disponibles, le rapport est généré. Le widget affiche également le nombre de filtres pris en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations des données

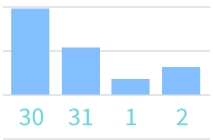
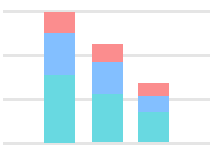
Visualisations de l'onglet Vue d'ensemble

Nom du rapport	Type	Table source	Description
Tendance de conformité	Graphique en courbes 	Résultats des tests	Informations sur la tendance de conformité : • Ressources : nombre total de ressources disponibles dans le système. • Échec : nombre de ressources avec au moins un résultat de test ayant échoué. • Réussite : nombre de ressources avec tous les résultats des tests à l'état Réussi.
Tâche de remédiation	Score unique 	Résultats des tests	Nombre de tâches de rattrapage qui sont présentes dans le système et qui sont à l'état actif.
Tâches de remédiation critiques proches de l'échéance	Score unique 	Résultats des tests	Nombre de tâches de rattrapage dont la cote de risque est « critique » et dont l'état de rattrapage est « proche de la cible ».
Résultats des tests par cote de risque	À barres 	Résultats des tests	Résultats des tests à l'état Échec, qui sont regroupés en fonction de la cote de risque.
Résultats des tests par âge	À barres	Résultats des tests	Résultats des tests à l'état Échec, qui sont regroupés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations de l'onglet Vue d'ensemble (suite)

Nom du rapport	Type	Table source	Description
			en fonction de la date de création des résultats des tests. **Remarque :** La personnalisation du calcul de l'âge et de l'âge fermé pour les résultats des tests peut entraîner une forte hausse ou une baisse des rapports d'Analyse des performances (PA) qui incluent ces mesures. Pour plus d'informations sur la personnalisation du calcul de l'âge et de l'âge fermé pour les résultats des tests, consultez l'article de la base de connaissances KB1703270 .
Résultats des tests fermés par respect de la cible de rattrapage	À barres 	Résultats des tests	Résultats des tests à l'état réussi, qui indique que ce test est fermé.
Résultats des tests critiques en retard par groupe d'affectation	Liste et score 	Résultats des tests	Nombre de résultats des tests où la cote de risque est « critique » et l'état de rattrapage est « cible manquée ». Le rapport indique que les résultats des tests sont à l'état Ouvert. Si les résultats des tests dépassent la date cible de rattrapage, ils sont considérés comme en retard.
Résultats des tests en retard : services	Liste, score et tendance	Vue de la base de données des tableaux de bord PA pour les services	Nombre de résultats des tests pour les services dont l'état de rattrapage est « cible manquée ». Ce

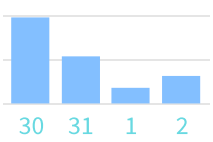
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations de l'onglet Vue d'ensemble (suite)

Nom du rapport	Type	Table source	Description
			rapport affiche également le nom des services ou départements avec les résultats de test les plus élevés.
Résultats des tests en retard : propriétaires de services	Liste, score et tendance 	Vue de la base de données des tableaux de bord PA pour les services	Nombre de résultats des tests pour les propriétaires de services dont l'état de rattrapage est « cible manquée ». Ce rapport affiche également le nom des services ou départements avec les résultats de test les plus élevés.

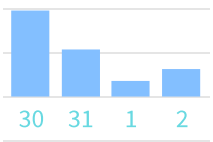
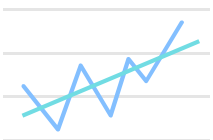
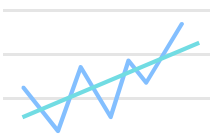
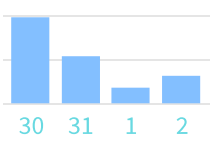
Visualisations de l'onglet Rattrapage

Titre	Type	Table source	Description
Tâches de remédiation par cote de risque	À barres 	Tâche de rattrapage	Répartition des cotes de risque de tous les groupes de résultats des tests qui sont à l'état actif.
Tâches de remédiation par état de la cible de remédiation	À barres	Tâche de rattrapage	Répartition des cibles de rattrapage de tous les résultats des tests Groupes qui ont manqué la cible, qui n'ont pas de cible et qui s'en approchent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

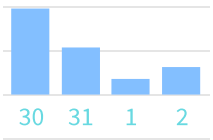
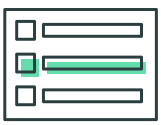
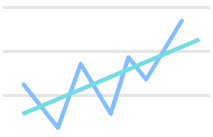
Visualisations de l'onglet Rattrapage (suite)

Titre	Type	Table source	Description
			
Tâche de remédiation par groupe d'affectation	Liste, score et tendance  	Tâche de rattrapage	Répartition des tâches de rattrapage basées sur un groupe d'affectation.
Tâche de remédiation critique en retard par groupe d'affectation	Liste, score et tendance  	Tâche de rattrapage	Répartition des tâches de rattrapage basées sur un groupe d'affectation. Ces tâches de rattrapage ont une cote de risque comme « critique » et leur cible de rattrapage n'a pas été atteinte.
Tâches de remédiation arrivées à expiration par âge	À barres 	Tâche de remédiation	Tâches de rattrapage qui vont arriver à expiration au bout d'une certaine durée. Un maximum de 10 compartiments de durée peut être créé.
Toutes les demandes d'exception en attente regroupées par motif	À barres	Approbation de changement de l'état	Demandes d'approbation de changement d'état

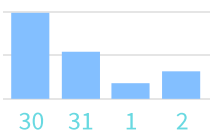
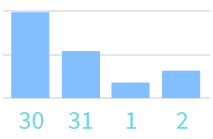
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations de l'onglet Rattrapage (suite)

Titre	Type	Table source	Description
			regroupées par motif de l'exception.
Exceptions critiques sur les résultats des tests par groupe d'affectation	Liste, score et tendance  	Résultats des tests	Résultats des tests qui sont dans un état différé et critique et qui sont regroupés en fonction du groupe d'affectation.

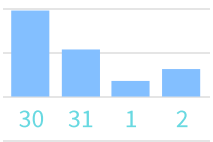
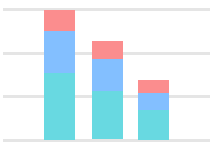
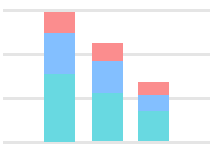
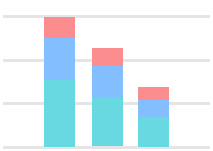
Visualisations de l'onglet Approbations

Rapports	Type	Table source	Description
Demandes d'exception par âge en attente de mon approbation	À barres 	Approbation	Les demandes d'exception que vous avez créées et qui sont en attente d'approbation. Les demandes sont regroupées en fonction de leur durée.
Demandes d'approbation par motif	À barres 	Approbation de changement de l'état	Demandes d'approbation de changement d'état pour créer une exception et inclure le motif de celle-ci.
Tâches de remédiation avec une demande d'approbation par cote de risque	À barres	Tâche de rattrapage	Tâches de rattrapage dont la demande d'approbation est basée sur la criticité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations de l'onglet Approbations (suite)

Rapports	Type	Table source	Description
			
Mes demandes d'approbation par état approuvé et rejeté	À barres 	Approbation de changement de l'état	Les demandes d'exception regroupées par état approuvé et rejeté.
Mes demandes d'exception arrivant à échéance par âge	À barres 	Approbation de changement de l'état	Les demandes d'exception qui vont arriver à expiration dans les semaines à venir. Les demandes d'exception sont regroupées en fonction des semaines. Chaque fois qu'une demande d'exception est créée, une date est sélectionnée pour la validité de la demande d'exception. Le calcul de l'âge de la demande est basé sur cette date.
État des demandes d'exception demandées par moi	À barres 	Approbation de changement de l'état	Demandes d'exception que vous créez et qui sont regroupées en fonction des états suivants : • En cours de révision • Approuvé • Rejeté

Cadre de travail des rapports agrégés pour Conformité de la configuration

À l'aide de l'infrastructure des rapports agrégés, vous pouvez créer des rapports pour les données qui impliquent des requêtes à la volée complexes et de longue durée afin d'améliorer les performances.

Le cadre de travail des rapports agrégés améliore les performances en :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- en utilisant moins de ressources et en rendant les rapports plus rapidement,
- l’agrégation des données et la réutilisation des agrégations et des répartitions (Grouper par) et
- réduire les requêtes à la base de données

Lorsque vous avez plus d’un million de résultats de tests de configuration, utilisez le cadre de travail des rapports agrégés en même temps que les rapports standard.

Rôles requis

Les tâches et rôles suivants sont associés à cette solution :

- Administrateur ServiceNow AI Platform (admin) : installer et activer cette Solution d'analyse des performances et génération de rapports, et apporter les modifications nécessaires aux propriétés système.
- Analyse des performances Administrateur (pa_admin) : Examinez les agrégations, les widgets et les tableaux de bord. Configurer et démarrer la collecte de données. Partager les tableaux de bord avec les personnes concernées appropriées.
- Administrateur (sn_vul_cmn.admin) : créer des agrégations.
- VR write(sn_vul_cmn.write) : modifiez les données dans les agrégations et les résultats agrégés.
- VR read (sn_vul_cmn.read) : passez en revue les données dans les agrégations et les résultats agrégés.
- Analyste de vulnérabilité (sn_vul.vulnerability_analyst) : examinez les résultats agrégés.

Information associée

Configurer une agrégation pour les données sources

Exécuter plusieurs agrégations simultanément

Configurer le nombre d’agrégations qui peuvent s’exécuter simultanément

Créer un rapport à l’aide d’une agrégation

Conformité de la configuration Informations de référence

Plusieurs types de composants sont installés avec l’activation de l’application, notamment les tables, les travaux planifiés et les Conformité de la configuration rôles d’utilisateur.

Les rubriques suivantes vous fournissent des informations de référence, de dépannage, en plus des données de champ sur les formulaires et les enregistrements trouvés dans Conformité de la configuration.

- Composants installés avec Conformité de la configuration
- Champs de formulaire des résultats des tests
- Résolution des Conformité de la configuration problèmes d’importation
- Modifier la date de début des résultats du PC Qualys

Composants installés avec Conformité de la configuration

Plusieurs types de composants sont installés avec l'activation du module d'extension Conformité de la configuration, notamment les tables et les rôles des utilisateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 15.1.5 de Conformité de la configuration, les propriétés système les plus fréquemment utilisées sont désormais accessibles au sein de l'application Conformité de la configuration . Pour afficher ces propriétés système, accédez à **Tous**Conformité de la configuration**Propriétés**.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Afficher les listes filtrées des composants installés avec une application

Filtrez la table Fichiers d'applications afin de n'afficher que les rôles, les travaux planifiés et les tables installés avec une application. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés dans l'instance et dans la table de métadonnées. Suivez ces étapes pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application. Par exemple : **Application** > **est** > **Réponse aux vulnérabilités**.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, sélectionnez **ET,** puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
Administrateur de Configuration Compliance [sn_vulc.admin]	Capable de modifier les propriétés de l'application, la configuration, les règles de mise à jour, les intégrations de l'application	sn_vulc.écrire **Remarque :** Hérite des rôles requis pour l'administration des enregistrements de l'application Configuration Compliance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	Conformité de la configuration . À partir de la version 15.0, un utilisateur administrateur ne peut pas supprimer les enregistrements sources tels que les Expliots, les CVE, entre autres.	
Lire [sn_vulc.lire]	Lisez les listes et les enregistrements dans Configuration Compliance. **Important :** À partir de la version 24.0 de , le rôle sn_vulc.read a le privilège d'accéder Réponse aux vulnérabilitésEspace de travail du gestionnaire de vulnérabilités au .	• sn_sec_cmn.calc_read • sn_vul.view_manager_workspace
écrire [sn_vulc.écrire]	écrivez des listes et des enregistrements dans Configuration Compliance.	• sn_vulc.lire • sn_vulc.remediation_owner
Affectation d'écriture [sn_vulc.write_assignment	Écrire dans les champs d'affectation de résultat de test.	Contenu dans le rôle sn_vulc.remediation_owner.
Propriétaire de la résolution sn_vulc.remediation_owner	Affichez et mettez à jour l'autorisation pour les résultats des tests qui vous sont affectés ou qui sont affectés à votre groupe.	Contenu dans le rôle itil. Contient : • sn_sec_cmn.lire • sn_vulc.affectation_écriture • sn_vul.view_rem_workspace
CC.Système sn_vulc.import_admin	Exécute tous les travaux planifiés dans l'application Configuration Compliance.	• sn_vulc.écrire • import_admin • sn_vul_tenable.read_integration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	Remarque : Cet utilisateur est l'utilisateur run-as par défaut pour chaque tâche planifiée dans Configuration Compliance.	
VRCommon.System sn_vul_cmn.admin	Utilisateur d'exécution en tant que par défaut pour toutes les tâches planifiées dans l'application commune Réponse aux vulnérabilités.	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin
SecCommon.System sn_sec_cmn.admin	Utilisateur run-as par défaut pour toutes les tâches planifiées qui sont utilisées pour l'aptitude des tâches en arrière-plan dans l'application courante Prise en charge de la sécurité	• sn_sec_cmn.int_write • sn_sec_cmn.write • workflow_admin • sn_sec_cmn.calc_write • sn_sec_core.lire_dictionnaire • sn_sec_cmn.manage_approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.manage_classification_rules • sn_sec_cmn.manage_background_job
V14.7 : sn_vulc.edit_watch_topic	Modifiez les rubriques de surveillance pour la conformité de la configuration.	sn_vulc.read_watch_topic
V14.7 : sn_vulc.read_watch_topic	Lisez les rubriques de surveillance pour la conformité de la configuration.	cmdb_read
V14.7 : sn_vulc.create_watch_topic	Créez des rubriques de surveillance pour la conformité de la configuration.	sn_vulc.read_watch_topic
sn_vulc.auditeur	Autoriser la lecture pour tous les modules	sn_vulc.lire sn_vulc.lecture_avancée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	Configuration Compliance	
sn_vulc.lecture_avancée	Autoriser la lecture pour tous les modules d'administration de Configuration Compliance	sn_vulc.read_auto_close_rules sn_vulc.read_exception_configuration sn_vulc.read_assignment_rules sn_vulc.read_task_rules sn_vulc.read_auto_exception_rule sn_vulc.read_notifications sn_vulc.read_risk_score_configuration mappage sn_vulc.read_test_criticality_mapping sn_sec_cmn.read_approval_rules sn_vulc.read_auto_delete sn_vulc.read_remediation_target_rules
mappage sn_vulc.read_test_criticality_mapping	Autoriser la lecture pour le mappage de criticité des tests	
sn_vulc.read_task_rules	Autoriser la lecture pour les règles de tâche de rattrapage	
sn_vulc.read_assignment_rules	Autoriser la lecture pour les règles d'affectation	
sn_vulc.read_risk_score_configuration	Autoriser la lecture pour la configuration du score de risque	
sn_vulc.read_auto_close_rules	Autoriser la lecture pour la configuration de fermeture automatique	
sn_vulc.approbateur_faux_positif	Permet d'approuver/de rejeter la fermeture des tâches de rattrapage comme un faux positif	sn_vul.view_manager_workspace
sn_vulc.exception_approver	Demandes d'exception approuvées ou rejetées.	sn_vul.view_manager_workspace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
sn_vulc.supprimer	Supprime les enregistrements sources.	

Travaux planifiés installés

Tâche planifiée	Description
V15.0 : mettre à jour le groupe de tests sur les tests de configuration	Met à jour le groupe de tests sur les tests pour les sources Tenable et Microsoft Defender. Il s'agit d'un travail ponctuel.
V15.0 : renseigner les champs de résultats des tests existants	Met à jour les valeurs dans les colonnes nouvellement ajoutées (telles que Âge, Âge fermé, Actif, etc.) dans la table des résultats des tests, les filtres enregistrés et les modules. Il s'agit d'un travail ponctuel.
V15.0 : Remplir la table des CI vulnérables : supprimer et remplir à nouveau pour les résultats des tests	Renseigne le nombre total d'enregistrements dans la table CI vulnérables. Il s'agit d'un travail ponctuel.
Version 12.0 Calculer les mesures de rattrapage pour tous les groupes de résultats des tests	Calcule et met à jour les valeurs des mesures d'état sur les enregistrements de tâches de rattrapage.
Version 12.0 : Calculer les mesures de rattrapage pour tous les résultats des tests	Calcule et met à jour les valeurs des mesures d'état sur les enregistrements de résultats des tests.
Version 12.0 : Synchronisation de l'état de la demande de changement	Tâche à la demande qui synchronise les états de toutes les tâches de rattrapage (RT) existantes avec les demandes de changement (CHG). À mesure qu'une demande de changement avance dans son cycle de vie, elle modifie automatiquement les états de toutes les tâches de rattrapage connexes. Active la synchronisation de l'état à l'avenir.
Version 11.1 : Vérifier le report des groupes de résultats des tests Expiration	Envoie des notifications si les tâches de rattrapage ont expiré (et si elles expirent dans une semaine).
Nombre de CI de Configuration Compliance	Renseigne le nombre d'éléments de configuration (CI) distinct et la moyenne mobile sur 90 jours dans la table Nombre d'éléments de configuration [sn_vulc_cc_configuration_item_count].
Version 11.1 : Évaluer et notifier les cibles de rattrapage	Définit ou met à jour les dates cibles de rattrapage sur tous les résultats des tests. Détermine l'état des dates cibles de rattrapage par rapport aux règles. Envoie des notifications

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
V14.7 : Insérer des groupes de résultats de tests dans la tâche de rattrapage unifiée	Tâche planifiée ponctuelle pour insérer toutes les tâches de rattrapage créées dans l'interface utilisateur classique dans la tâche de rattrapage unifiée (sn_vul_remediation_task).
Version 12.0 : Renseigner CR-TRG m2m pour CR et CR-Parent	Remplit les demandes de changement sur les tâches de rattrapage.
Supprimé dans la version 11.1 : Rouvrir des groupes de résultats de tests différés **Remarque :** Déconseillé pour les versions antérieures à la version 11.1. Ne pas utiliser.	Rouvre les groupes différés lorsque la date d'échéance est dépassée.
Réappliquer toutes les règles d'affectation	Réapplique toutes les règles d'affectation.
Version 14.3 : Nombre de réaffectations pour les règles d'affectation	S'exécute quotidiennement et publie le nombre total de résultats des tests et de tâches de rattrapage qui ne sont pas affectés par cette fonctionnalité pour une règle d'affectation particulière.
Réévaluer l'état des groupes de résultats des tests	Réévalue l'état des tâches de rattrapage pour les entrées où **assess_state** est faux. S'exécute toutes les 15 minutes.
Déployer le score de risque du résultat des tests dans le groupe de résultats des tests et le test de configuration	S'exécute toutes les heures et calcule les scores de déploiement pour les tests de configuration et les tâches de rattrapage modifiés. • Calcule le score de risque de déploiement pour tous les tests dans sn_vulc_test_manifest et supprime l'enregistrement du manifeste une fois l'opération terminée. • Calcule le score de risque de déploiement pour tous les tests dans sn_vulc_result_group_manifest et supprime le manifeste une fois l'opération terminée.
Version 12.0 : Mettre à jour les mesures de rattrapage de la politique	À partir de la version 15.0 de , cette tâche planifiée a été renommée Mettre à jour les mesures de Conformité de la configuration rattrapage. • Calcule et met à jour les valeurs des mesures d'état sur les enregistrements de politique. • Calcule le % de conformité des résultats des tests d'un CI sur l'élément détecté.
Version 14.3 : Définir les nombres de reports	Collecte le nombre de fois où un résultat de test ou une tâche de rattrapage est reporté.
Mettre à jour la cote de risque pour les résultats des tests	Met à jour la cote de risque pour les résultats des tests.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche planifiée	Description
Mettez à jour le score de risque de déploiement pour tous les groupes de résultats et les tests de configuration non fermés.	Met à jour le score de risque de déploiement pour tous les groupes de résultats et Conformité de la configuration les tests non fermés.

Tables installées

Table	Description
Règle d'affectation [sn_vulc_assignment_rule]	Contient l'ensemble des règles évaluées pour définir le groupe d'affectation sur les résultats des tests.
Source de référence [sn_vulc_auth_src]	Stockez les sources de référence importées.
Calculateur [sn_vulc_calculator_risk_score]	Contient le calculateur qui définit certains champs de résultat de test lorsque certaines conditions sont remplies.
Nombre d'éléments de configuration CC [sn_vulc_cc_configuration_item_count]	Contient le nombre total d'éléments de configuration.
Version 12.0 : Association de demande de changement [sn_vulc_action_associate_cr]	Table intermédiaire utilisée pour associer des demandes de changement à des tâches de rattrapage.
Version 12.0 : Création d'une demande de changement [sn_vulc_action_create_cr]	Table intermédiaire utilisée pour créer des formulaires de demande de changement.
Version 12.0 : formulaire de demande de changement [sn_vulc_cr_form]	Table de base pour la gestion des demandes de changement.
Citation [sn_vulc_citation]	Contient le contenu des documents de référence importés
Test de configuration [sn_vulc_test]	Contient les données de test de configuration importées.
Manifeste de test de configuration	Contient les tests de configuration pour lesquels le score de risque de déploiement doit être calculé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vulc_test_manifest]	
Version 12.2 Table d’actifs manquante [sn_vul_missing_asset]	Contient des enregistrements d’actifs temporaires pour les données d’évaluation de Configuration Compliance importées avec des actifs sans correspondance.
Technologie de test de la configuration [sn_vulc_test_technology]	Contient les technologies de test de configuration importées.
Règle de la tâche de rattrapage [sn_vulc_grouping_rule]	Contient les règles qui définissent les critères selon lesquels les groupes sont automatiquement créés pour un ensemble de résultats des tests.
Groupes de tests [sn_vulc_policy]	Contient les politiques importées.
Test de configuration de la politique [sn_vulc_policy_test]	Contient les données de test de configuration de politique importées.
Règle de cible de rattrapage [sn_vulc_ttr_rule]	Définit le délai prévu pour corriger un résultat de test.
Calculateurs de risques [sn_vulc_calculator_group]	Contient le groupe de Conformité de la configuration calculateurs. L’ordre du groupe de calculateurs détermine quel groupe est évalué en premier, et dans chaque groupe, un calculateur au maximum est utilisé.
Calculateur de déploiement des scores du risque [sn_vulc_risk_score_rollup]	Contient les configurations du calculateur de déploiement.
Diviser les tâches de rattrapage [sn_vulc_action_split_trg]	Table intermédiaire utilisée pour diviser les tâches de rattrapage.
Approbation de changement de l'état [sn_vulc_state_change_approval]	Contient les données du processus d’état d’approbation.
Technologie [sn_vulc_technology]	Contient les technologies importées.
Tester le mappage de criticité	Contient des données de mappage de criticité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_vulc_test_criticality_map]	
Résultat de test [sn_vulc_result]	Contient les résultats des tests importés.
Tâches de remédiation [sn_vulc_result_group]	Contient les tâches de rattrapage importées.
Version 12.0 : Demandes de changement de tâche de rattrapage	Contient des demandes de changement pour les tâches de rattrapage.
Manifeste de tâche de rattrapage [sn_vulc_result_group_manifest]	Contient les tâches de rattrapage pour lesquelles le score de risque de déploiement doit être calculé.
Tâches de remédiation [sn_vulc_m2m_result_result_group]	Contient les données de la tâche de rattrapage.
Historique des résultats des tests [sn_vulc_result_history]	Contient l'historique des résultats des tests importés.
État de rattrapage des résultats des tests	État du résultat du test par rapport à la règle de cible de rattrapage appliquée la plus proche.
V14.7 : nombres de tests de rubriques de surveillance [sn_vulc_wt_test_counts]	Table de cache pour l'onglet Tests de configuration distincts dans l'espace de travail du gestionnaire de vulnérabilités.

Traduction automatique

Afficher les Conformité de la configuration groupes de tests

Une fois que vous avez importé les résultats d'une analyse tierce dans votre instance, vous pouvez voir la conformité de vos tests au niveau du groupe de tests. Utilisez cette vue avant un audit de ce groupe de tests et de tout enregistrement de test associé.

Avant de commencer

Rôle requis : sn_vulc.read et sn_vulc.remediation_owner pour afficher

Pourquoi et quand exécuter cette tâche

Les groupes de test sont des enregistrements importés et vous ne pouvez pas les modifier dans l'application Conformité de la configuration .

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Groupes de tests**.
   La liste des résultats des tests s'affiche. À partir de la version 15.0 de , la colonne **% de conformité** des Conformité de la configuration résultats des tests affiche le pourcentage de résultats des tests conformes aux tests d'un groupe de tests.

   % de conformité des résultats des tests = (nombre de résultats des tests fermés dans un groupe de tests/ nombre total de résultats des tests associés à un groupe de tests) * 100

2. Cliquez sur la **description brève** du groupe de tests que vous souhaitez afficher.

Conformité de la configuration Champs de formulaire Groupe de tests

Champ	Description
Source	Nom du système de l'analyseur tiers, ou nom saisi dans le module d'extension ServiceNow de l'API utilisé pour communiquer avec Conformité de la configuration.
Technologies	Liste des technologies associées au groupe de tests dans l'application d'analyse tierce.
ID source	Identificateur affecté à ce groupe de tests par le scanner tiers.
Source créée	Date et heure auxquelles le groupe de tests a été défini dans l'application de scanner tiers.
Source mise à jour	Date et heure auxquelles le groupe de tests a été modifié pour la dernière fois dans l'application d'analyse de troisième politique.
Description brève	Description ou titre de résumé affecté au groupe de test dans l'application de scanner tiers.
Description	Description détaillée du groupe de tests tel que défini dans l'application de scanner tiers.
Tests	Liste des tests qui font référence à ce groupe de tests. Importé à partir de l'analyseur tiers. Vous pouvez parcourir la liste pour obtenir des informations détaillées sur un test spécifique, si nécessaire.
État du rattrapage (version 12.0)	
Exclut les éléments différés	Ces valeurs n'incluent pas les CI des résultats des tests différés. ○ **CI restants** : nombre d'éléments de configuration (CI) avec des résultats des tests actifs (tout état autre que **Fermé**) pour cette politique. ○ **% des CI rattrapés** : pourcentage de CI conformes pour ce groupe de tests. Ce

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	nombre exclut les CI avec des résultats de test différés. ○ **CI totaux** : nombre total de CI impactés par ce groupe de tests. Ce nombre exclut les résultats des tests différés.
Inclut les éléments différés	Les valeurs représentent les CI de tous les résultats des tests actifs (tout état autre que **Fermé**). ○ **CI restants** : nombre de CI uniques associés à un ou plusieurs résultats des tests non fermés auxquels ce groupe de tests a été appliqué. ○ **% de CI rattrapés** : pourcentage de CI conformes pour ce groupe de tests. ○ **CI totaux** : nombre total de CI impactés par ce groupe de tests.

À partir de la version 12.0, pour mettre à jour ces valeurs à la demande, sous l'onglet État du rattrapage, cliquez sur le lien connexe État **de mise à jour** . Un message s'affiche pour indiquer que les données sont en cours d'actualisation. Cliquez sur le lien **Afficher l'état** pour afficher la progression de la mise à jour. Après quelques instants, toutes les données qui ont changé ou été mises à jour depuis la dernière tâche planifiée sont actualisées sur l'enregistrement. Les valeurs de champ mises à jour sont actualisées.

3. **Facultatif :** Désactivez l'importation des résultats des tests pour un groupe de tests en sélectionnant le bouton **Désactiver l'importation** .

   (Optional) La valeur de la colonne **Est une importation désactivée** devient *vrai*. Les résultats des tests pour le groupe de tests ne sont pas importés à partir de l'ingestion à venir.

   Remarque : Le bouton **Désactiver l'importation**Qualys n'est disponible que pour les résultats des tests obtenus à partir du scanner.

   À partir de la v23.0 de Réponse aux vulnérabilités:

   - Vous pouvez activer ou désactiver l'importation des résultats des tests pour un Qualys groupe de tests dans le Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Activer ou désactiver l'importation de résultats de tests pour un Qualys groupe de tests.
   - Le bouton **Marquer comme déconseillé** est renommé **Désactiver l'importation**.
   - La colonne **Est déconseillé** est renommée en **Est l'importation désactivée**.

Afficher les Conformité de la configuration sources de référence

Utilisez ce module pour afficher des informations récapitulatives sur chaque source faisant autorité et pour rechercher les publications sources qui ont été utilisées pour créer l'enregistrement.

Avant de commencer

Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vulc.admin à mettre à jour
- sn_vulc.remediation_owner pour afficher

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Données associées** > **Sources de référence**.
2. Cliquez sur la **description brève** de la source de référence que vous souhaitez afficher.

Conformité de la configuration Champs du formulaire Sources d'autorité

Champ	Description
Numéro	Numéro d'ID attribué à la source de référence par votre instance au cours du processus d'importation.
Source	Nom du système de l'application de scanner tierce, ou nom saisi dans le module d'extension du scanner pour l'API qui communique avec Conformité de la configuration.
ID source	Identificateur affecté à la source de référence par le scanner tiers.
Description brève	Nom donné à cette source de référence dans le scanner tiers.
Éditeur	Nom de l'organisation ou de la publication qui était la source d'information d'origine de cette source faisant autorité.
Contenu des documents de référence	Liste des informations citées sur les résultats des tests. Importé à partir de l'analyseur tiers. Vous pouvez accéder à cette liste pour obtenir des informations détaillées sur un test spécifique, si nécessaire.

3. **Facultatif :** Ajouter un **éditeur**.
4. Cliquez sur **Mettre à jour**.
5. Vous pouvez supprimer cet enregistrement en cliquant sur **Supprimer**.
   Supprime l'enregistrement de votre instance. S'il est toujours utilisé dans votre intégration tierce, il est renvoyé dans la prochaine importation

Afficher les Conformité de la configuration technologies

Utilisez ce module pour afficher des informations récapitulatives sur chaque source et citation faisant autorité (également appelé, dans Qualys, un cadre de travail). Vous pouvez rechercher les publications sources qui ont été utilisées pour créer l'enregistrement.

Avant de commencer

Rôle requis :

- sn_vulc.admin à mettre à jour
- sn_vulc.remediation_owner pour afficher

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Données associées** > **Technologies**.
2. Cliquez sur la **description brève** de la source de référence que vous souhaitez afficher.

Conformité de la configuration Champs du formulaire Sources d'autorité

Champ	Description
Numéro	Numéro d'ID attribué à la source de référence par votre instance au cours du processus d'importation.
Source	Nom du système du scanner tiers, ou nom saisi dans le module d'extension du scanner tiers pour l'API qui communique avec Conformité de la configuration.
ID source	Identificateur affecté à la source de référence par le scanner tiers.

3. Vous pouvez supprimer cet enregistrement en cliquant sur **Supprimer**.
   Supprime l'enregistrement de votre instance. S'il est toujours utilisé dans votre intégration tierce, il est renvoyé dans la prochaine importation

Afficher les Conformité de la configuration tests

Utilisez ce module pour rechercher des informations détaillées sur ces tests. Sont incluses les citations de sources d'experts qui ont été utilisées lors de leur création, les politiques de configuration tierces dans lesquelles elles sont utilisées et les résultats obtenus à partir de l'analyse.

Avant de commencer

Rôle requis :

- sn_vulc.admin à mettre à jour
- sn_vulc.remediation_owner pour afficher

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Contrôles**.
2. Accédez à la **Tous** > **Configuration Compliance** > **Tests**
3. Dans la liste, ouvrez le contrôle (test de conformité) que vous souhaitez afficher.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir de la version 12.0, pour mettre à jour ces valeurs à la demande, sous l'onglet État du rattrapage, cliquez sur le lien connexe Mettre **à jour l'état** . Un message s'affiche pour indiquer que les données sont en cours d'actualisation. Cliquez sur le lien **Afficher l'état** pour afficher la progression de la mise à jour. Après quelques instants, toutes les données qui ont changé ou été mises à jour depuis la dernière tâche planifiée sont actualisées sur l'enregistrement. Les valeurs de champ telles que le**score de risque**, la **cote de risque**, la **date cible de rattrapage**, **l'état** et les champs de l'onglet État du **rattrapage** sont actualisées.

Conformité de la configuration Tester les champs de formulaire

Champ	Description
Numéro	Numéro affecté au contrôle au cours du processus d'importation.
Résultat	Statut de l'analyse. Réussite ou échec. Si ce test appartient à plusieurs tâches de rattrapage, son état est déterminé selon un ordre de priorité.
Source	Nom du système de l'application d'intégration tierce ou nom saisi dans le module d'extension pour l'API utilisée pour communiquer avec Conformité de la configuration.
Criticité	Gravité du ou des problèmes de configuration associés au contrôle tel que défini dans l'intégration tierce. Le niveau de criticité est ajusté pour correspondre à la granularité d'indicateurs de vulnérabilité similaires disponibles dans Réponse aux vulnérabilités. Les niveaux possibles sont les suivants : **Critique** Le problème de configuration associé au contrôle entraîne une interruption pour un ou plusieurs CI critiques pour l'entreprise. **Élevé** Le problème de configuration associé au contrôle constitue une menace, mais n'entraîne pas l'arrêt des ressources réseau critiques. **Modéré** Le problème de configuration associé au contrôle est un risque, mais n'est pas une menace immédiate. **Faible** Le problème de configuration associé au contrôle est une menace de faible niveau et peut être ignoré en faveur des CI plus à risque. **Mineur**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Le problème de configuration associé au contrôle est un risque mineur et peut être ignoré si nécessaire.
ID source	Identificateur affecté au contrôle par l'intégration tierce.
Catégorie	Catégorie de classification majeure accordée à ce type de contrôle par le fournisseur tiers.
Score du risque	Il s'agit d'un score de risque de déploiement. Ce score de risque est pondéré : 85 % du score du score de risque maximal pour tous les résultats des tests n'étant pas « fermés » (Ouvert, En cours d'examen, En attente d'implémentation, Différé, Résolu) et 15 % du score provenant du nombre de résultats des tests qui ne sont pas « Fermés ». Valeur calculée à l'aide des calculateurs de score de risque basée sur les valeurs de criticité opérationnelle et de criticité des tests des résultats des tests.
Sous-catégorie	Sous-catégorie affectée à cette classe de test par le fournisseur tiers.
Cote de risque	Basé sur une plage de scores de risque sur une échelle numérique de 1 à 5 qui évalue le risque global en fonction d'une plage de scores de risque allant de 1 - Critique à 5 - Aucun. Ce champ remplace le champ Priorité des versions précédentes.
Technologies	Liste des technologies couvertes par ce test.
Source créée	Date à laquelle le test a été défini pour la première fois dans l'intégration tierce.
Source mise à jour	Date de la dernière mise à jour du test dans l'intégration tierce.
Description brève	Description ou titre de résumé saisi ou affecté au test dans l'intégration tierce.
État du rattrapage (v 12.0)	
Exclut les éléments différés	Ces valeurs n'incluent pas les résultats des tests différés. ○ **Résultats des tests ouverts** : nombre de résultats des tests actifs (tout état autre que **Fermé**) pour ce test de configuration. ○ **% des résultats des tests corrigés** : pourcentage des résultats des tests rattrapés pour cette tâche de rattrapage. ○ **Résultats des tests totaux** : nombre total de résultats des tests pour cette tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Inclut les éléments différés	Ces valeurs incluent les résultats des tests différés. ○ **Résultats des tests ouverts** : nombre de tous les résultats des tests actifs (tout état autre que **Fermé**) pour cette tâche de rattrapage. ○ **% des résultats des tests corrigés** : pourcentage des résultats des tests rattrapés pour cette tâche de rattrapage. ○ **Résultats des tests totaux** : nombre total de résultats des tests pour cette tâche de rattrapage.
Description	Longue description du test. Pour Qualys Vulnerability Integration, ce champ affiche par défaut le contenu de la Qualys Cloud Platform page de couverture.
Rattrapage	Étapes Instructions décrivant comment corriger la non-conformité.
Onglets associés	
Contenu des documents de référence	Liste des contenus des documents de référence saisis pour chaque source faisant autorité associée au test.
Groupes de tests	Liste des groupes de Conformité de la configuration test qui utilisent ce test.
Résultats des tests	Liste des CI affectés par le ou les problèmes de configuration associés à ce test. Vous pouvez accéder aux tests individuels, ServiceNow aux éléments de configuration ou à la liste des technologies affectées, si nécessaire.
Déclarations de politique GRC	Si le module d'extension GRC Gestion de la politique et de la conformité est installé, cet onglet contient la politique connexe GRC . Vous pouvez modifier cette liste pour ajouter ou supprimer des déclarations de politique.

Afficher les Conformité de la configuration résultats des tests

Affichez les Conformité de la configuration résultats des tests pour l'audit et le rattrapage. Les résultats des tests sont automatiquement créés lors des importations d'intégrations de vulnérabilités tierces.

Important : Vous pouvez afficher les résultats des tests créés lors des importations d'intégrations de vulnérabilités tierces dans l'espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Page de liste dans Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vulc.Lire pour afficher
- sn_vulc.remediation_owner pour afficher et mettre à jour
- sn_vulc.supprimer pour supprimer

Pourquoi et quand exécuter cette tâche

Conformité de la configuration ne crée ni ne met à jour les résultats des tests, mais les importe dans le cadre d'une intégration tierce. Une fois qu'ils sont visibles dans , ils sont corrigés à Conformité de la configuration l'aide de **groupes de résultats de tests**.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Résultats des tests**.
   À partir de la version 15.0 de Conformité de la configuration, les colonnes suivantes apparaissent dans la liste Résultats des tests.

Liste des résultats des tests

Colonne	Description
Actif	Indique si un résultat de test est actif. Un résultat de test est marqué : ○ Vrai : si l'état n'est pas Fermé. ○ Faux : si l'état est Fermé.
Âge	Période pendant laquelle un résultat de test est actif depuis sa dernière ouverture. Ce champ est vide pour un résultat de test fermé. Format : Jours HH :MM : SS Pour plus d'informations sur la personnalisation du calcul de l'âge, consultez l'article KB1703270 .
Âge à la fermeture	Période pendant laquelle un résultat de test était actif avant qu'il ne passe à « Fermé ». Lorsque le résultat du test passe à « Fermé », la valeur de la colonne Âge s'affiche dans le champ Âge fermé. Ce champ est vide pour un résultat de test actif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
	Format : Jours HH :MM : SS Pour plus d'informations sur la personnalisation du calcul de l'âge fermé, consultez l'article KB1703270 .
Fermé	Horodatage auquel un résultat de test est fermé. Format : JJ-MM-AAAA HH :MM : SS
Dernières ouvertures	Horodatage auquel un résultat de test est ouvert, c'est-à-dire lorsque la valeur du champ **Actif** prend la valeur *vrai*.

2. Ouvrez le contrôle que vous souhaitez afficher.

Conformité de la configuration Champs de formulaire de résultat de test

Champ	Description
Numéro	Numéro attribué au test au cours du processus d'importation.
Source	Nom système de l'application SCA tierce, ou nom saisi dans le module d'extension de l'application pour l'API qui est utilisé pour communiquer avec Conformité de la configuration.
ID source	Identificateur affecté au contrôle par l'application SCA.
Résultat	Réussi, Échec, Erreur ou Inconnu. Importé de Qualys.
Score du risque	Résultat du calculateur pour ce test. Avant la version 15.0 de Conformité de la configuration, le score de risque d'un résultat de test réussi est défini sur « 0 ». À partir de la version 15.0 sur Conformité de la configuration, le score de risque du résultat de test réussi n'est pas changé sur « 0 » afin que vous puissiez estimer le risque atténué. Le score de risque du résultat de test réussi n'est pas inclus dans le calcul du score de risque d'une tâche de rattrapage.
Cote de risque	Basé sur une plage de scores de risque sur une échelle numérique de 1 à 5 qui évalue le risque global en fonction d'une plage de scores de risque allant de 1 - Critique à 5 - Aucun. Ce champ remplace le champ Priorité des versions précédentes.
État	Calculé à partir des tâches de rattrapage auxquelles appartient le résultat du test. Si le résultat du test

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	appartient à plusieurs groupes, un ordre de priorité est appliqué pour déterminer l'état.
Résolution	Calculé à partir des tâches de rattrapage auxquelles appartient le résultat du test. Si le résultat du test appartient à plusieurs groupes, un ordre de priorité est appliqué pour déterminer la résolution.
Premier observé	Date de la première importation dans Conformité de la configuration. À partir de la version 13.1.1, le champ **Premier observé** affiche la date fournie par le scanner. Sinon, il affiche la date de la première importation dans Conformité de la configuration.
Dernier observé	Date de la dernière importation dans Conformité de la configuration. À partir de la version 13.1.1, le champ **Dernier observé** affiche la date fournie par le scanner. Sinon, il affiche la date de la dernière importation dans Conformité de la configuration.
Dernière transmission	Date la plus récente à laquelle le résultat du test est réussi.
Test	Nom du test.
Élément de configuration	Nom du CI joint au test.
Technologie	Version du logiciel en cours d'exécution sur le CI.
Description	Description du test
Valeurs attendues	Valeurs attendues configurées dans Qualys et importées par Conformité de la configuration. Cette valeur est une expression booléenne qui, lorsqu'elle est évaluée comme **vraie**, rend le résultat du test réussi. L'expression peut être une combinaison d'opérateurs logiques, d'ensembles ou d'expressions régulières.
Valeurs réelles	Valeurs renvoyées par le test. Ces valeurs sont insérées dans l'expression booléenne des valeurs attendues pour déterminer si le résultat doit réussir ou échouer. Ils sont importés de Qualys. À partir de la version 14.9 de Conformité de la configuration, les valeurs Preuve étendue et Cause d'échec sont ajoutées dans la colonne Valeurs réelles.
Rattrapage	Instructions de rattrapage.
Onglets associés	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Tâches de remédiation	Tâches de rattrapage associées à ce résultat de test.
Historique des résultats des tests	Liste connexe des résultats des tests qui affichent l'historique des résultats de réussite/d'échec pour le même CI/technologie/test.

Afficher une tâche de rattrapage

Vous pouvez afficher ou, alternativement, créer une tâche de rattrapage et effectuer un rattrapage.

Important : Vous pouvez afficher les tâches de rattrapage dans l'espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Page de liste dans Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vulc.admin pour mettre à jour ou créer
- sn_vulc.remediation_owner pour afficher

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Procédure

1. Accédez à la **Tous** > **Configuration Compliance** > **Tâches de remédiation**.
2. Dans la liste, cliquez sur l'enregistrement que vous souhaitez afficher.
3. Vous pouvez également cliquer sur **Nouveau** pour créer une nouvelle tâche de rattrapage et remplir les champs.

Champs du formulaire Tâche de rattrapage de Configuration Compliance

Champ	Description
Numéro	Numéro généré automatiquement pour cet enregistrement.
État	État d'avancement de la tâche de rattrapage. ○ Ouvert ○ En cours d'examen ○ En attente d'implémentation ○ Différé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Résolu ○ Fermé
Score du risque	Ce score est la valeur cumulée des scores de risque pour tous les résultats des tests actifs dans une tâche de rattrapage. Ce score change à mesure que les résultats des tests sont corrigés dans la tâche de rattrapage.
Groupe d'affectation	Groupe sélectionné pour travailler sur cette tâche de rattrapage.
Cote de risque	Degré de risque qu'un résultat de test échoué pose à votre système. Il est basé sur une gamme de scores de risque sur une échelle numérique de 1 à 5 qui évalue les risques de critiques (1) à aucun (5).
Affecté à	Personne du groupe d'affectation sélectionné qui travaille sur cet ensemble de tâches.
Cible de remédiation	Date à laquelle les résultats des tests doivent être corrigés, dès lors qu'ils ont été identifiés pour la première fois.
Créées	Date et heure de création de cette tâche de rattrapage.
Statut de la remédiation	État du rattrapage pour le groupe. Elle est déterminée par le résultat du test avec la date d'échéance la plus proche. Pour les groupes ouverts, les états incluent En cours, Cible presque atteinte et Cible manquée. Pour les groupes fermés, les états incluent Aucune cible, Cible atteinte et Cible manquée. Pour les dates cibles de rattrapage calculées, si la tâche de rattrapage est fermée, l'état global de tous les résultats des tests fermés est affiché dans la tâche de rattrapage. Ceux-ci déterminent si le groupe a respecté sa date ou non. L'état de rattrapage d'une tâche de rattrapage fermée est **Aucune cible** si aucun de ses résultats fermés n'avait de date cible de rattrapage. La **cible est manquée** si l'un de ses résultats fermés a manqué sa date cible. Il **est atteint** si au moins un résultat fermé a atteint son objectif et qu'aucun des autres ne l'a manqué.
Mis à jour	Date et heure de la dernière modification de cet enregistrement.
Description brève	Brève description de cette tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Description longue de la tâche de rattrapage qui comprend la liste des logiciels associés à cette tâche de rattrapage.
Test	Test de configuration associé à cette tâche de rattrapage.
État du rattrapage (version 12.0)	
Exclut les éléments différés	Ces valeurs n'incluent pas les résultats des tests différés. ○ **Résultats des tests ouverts** : nombre de résultats des tests actifs (tout état autre que **Fermé**) pour cette tâche de rattrapage. ○ **% des résultats des tests corrigés** : pourcentage de résultats des tests rattrapés (fermés) pour cette tâche de rattrapage. ○ **Résultats des tests totaux** : nombre total de résultats des tests pour cette tâche de rattrapage.
Inclut les éléments différés	Les valeurs représentent tous les résultats des tests actifs (tout état autre que **Fermé**). ○ **Résultats des tests ouverts** : nombre de résultats des tests actifs (tout état autre que **Fermé**) pour cette tâche de rattrapage. ○ **% des résultats des tests corrigés** : pourcentage de résultats des tests rattrapés (fermés) pour cette tâche de rattrapage. ○ **Résultats des tests totaux** : nombre total de résultats des tests pour cette tâche de rattrapage.
Configuration du groupe	Type de filtrage utilisé pour sélectionner les résultats des tests pour la tâche de rattrapage.
Méthode de regroupement	Nom de la méthode utilisée.
Règle de groupe	Nom de la règle de groupe utilisée.
Notes	Notes système associées à l'enregistrement.
Liens connexes	**Version 12.0 : mise à jour du lien d'état**. Mettez à jour les valeurs de l'enregistrement des résultats des tests à la demande. Affichez toutes les données qui ont changé ou ont été mises à jour depuis la dernière tâche planifiée.
Résultats des tests	Résultats des tests dans cette tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Demandes de changement (v 12.0)	Liste des demandes de changement associées à cette tâche de rattrapage.
Approbations de changement de l'état (v 12.0)	État et états des approbations de demandes de changement associées à cette tâche de rattrapage.

Transitions d'états des résultats des tests et des tâches de rattrapage dans l'application Conformité de la configuration

Les états des enregistrements de test de configuration et leurs tâches de rattrapage (RT) associées sont impactés si les enregistrements de résultats de test sont reportés, résolus, rouverts et transférés vers d'autres efforts de rattrapage (RE).

Scénarios de transition d'état entre les résultats des tests et les tâches de rattrapage

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Le tableau suivant détaille la manière dont les états et les sous-états alternent entre les résultats des tests de configuration et les tâches de rattrapage.

Si l'état d'une tâche de rattrapage passe de...	... Vers l'état/les sous-états	Les états des résultats des tests associés passent de...	... Vers l'état/les sous-états	Description
Ouvert	En cours d'examen	Ouvert	En cours d'examen	Les états effectuent une transition bidirectionnelle.
Ouvert	En cours de révision	Ouvert	En cours de révision	Les états effectuent une transition bidirectionnelle.
Ouvert	Reporté/avec n'importe quel motif sélectionné pour la résolution	Ouvert	Différé	Les résultats des tests conservent le même motif de résolution que la tâche de rattrapage.
Reporté/avec un motif quelconque de résolution	Ouvert	Les résultats des tests restent différés		Les résultats des tests conservent la même résolution que la tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si l'état d'une tâche de rattrapage passe de...	... Vers l'état/les sous-états	Les états des résultats des tests associés passent de...	... Vers l'état/les sous-états	Description
Ouvert	Résolu/Corrigé	Ouvert	Résolu	Les états/sous-états font une transition bidirectionnelle.
Ouvert	Résolu et résolu à Fermé/Corrigé	Ouvert	Résolu	Si une tâche de rattrapage passe à l'état Fermé/Corrigé, elle peut revenir à l'état Ouvert. Si la tâche passe à Ouvert, ses résultats des tests associés passent de Résolu à Ouvert.
Ouvert	Résolu	Ouverts	Résolu	Les états/sous-états font une transition bidirectionnelle.
Ouvert	Résolu/Annulé	Ouvert	Résolu	Les états/sous-états font une transition bidirectionnelle.
Ouvert	Résolu et Résolu à Fermé	Ouvert	Résolu	Si une tâche de rattrapage passe automatiquement à l'état Fermé, les résultats des tests associés peuvent revenir à l'état Ouvert.
Ouvert	Résolu et résolu à Fermé/Résultat non valide	Ouvert	Résolu et résolu à Fermé/Résultat non valide	Si une tâche de rattrapage passe à l'état Résolu, elle peut revenir à l'état Ouvert. Si une tâche de rattrapage passe à l'état Fermé/Résultat non valide, elle et les résultats des tests qui lui sont associés ne peuvent pas être rouverts.
Ouvert	Fermé/Corrigé	Les résultats des tests restent ouverts		

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- À partir de la version 14.12 de Conformité de la configuration, l'option **Résultat non valide** est supprimée dans le champ **Résolution** de la fenêtre modale Fermer.
- À partir de la version 14.12 de , le workflow **d'approbation de l'état de la tâche** de Conformité de la configuration rattrapage est déconseillé et remplacé par l'approbation de l'état de la tâche de rattrapage de flux dans le concepteur de flux.

Synchronisation de l'état entre les demandes de changement et les tâches de rattrapage

Il existe une relation synchronisée entre les champs État des tâches de rattrapage et les champs État des demandes de changement (CHG) dans l'application Conformité de la configuration .

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Au fur et à mesure qu'une demande de changement progresse dans son cycle de vie, elle modifie automatiquement l'état de toutes les tâches de rattrapage connexes. La synchronisation de l'état est activée par défaut par une propriété système (sn_vulc.cr_state_sync) dans votre instance lorsque vous téléchargez l'application Conformité de la configuration à partir de la ServiceNow Store version 12.0.

Lorsque la synchronisation de l'état est activée, le champ État du CHG modifie automatiquement le champ État de la tâche de rattrapage dans les cas suivants :

- Lorsqu'une nouvelle demande de changement est créée pour une tâche de rattrapage, si elle n'est pas en **attente d'implémentation**, l'état de la tâche de rattrapage passe à **En attente d'implémentation**.
- Lorsqu'une demande de changement existante est associée à une tâche de rattrapage, si elle n'est pas en **attente d'implémentation**, l'état de la tâche de rattrapage passe à **En attente d'implémentation**.
- Une fois que les tâches d'une demande de changement sont terminées (implémentées) et que le CHG est passé à l'état **Réviser** , la tâche de rattrapage passe à l'état **Résolu**.

Pour plus d'informations et d'exemples de synchronisation d'état, consultez les sections suivantes.

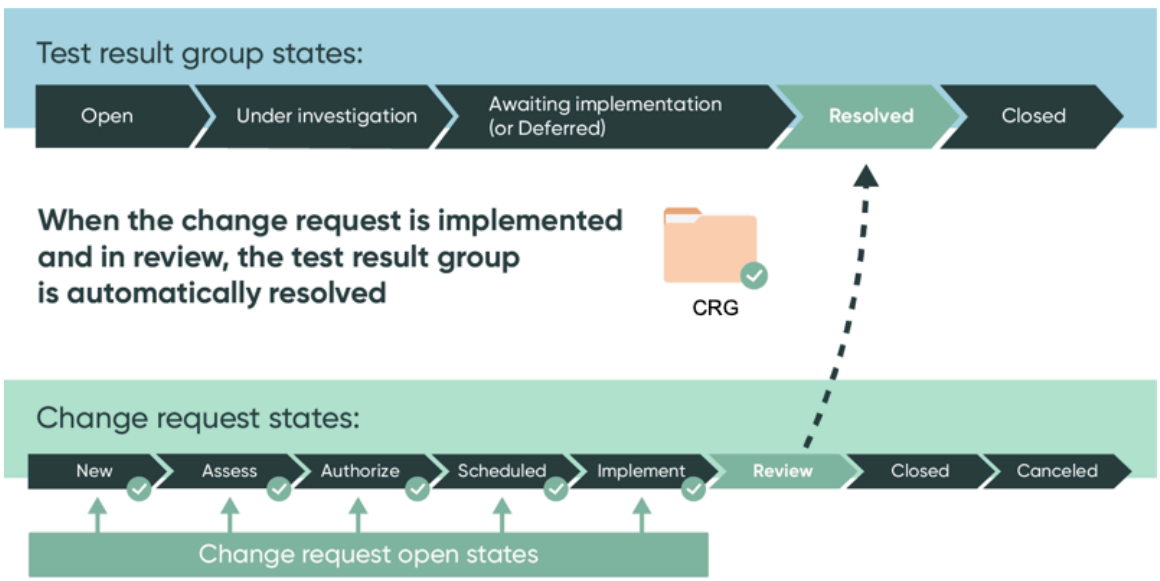
Remarque : Vous pouvez toujours déplacer manuellement les demandes de changement et les tâches de rattrapage d'un état à un autre de leur cycle de vie sur leurs enregistrements respectifs avec la synchronisation d'état activée, mais lorsque le système enregistre qu'une demande de changement a changé d'état, ou que vous ajoutez une demande de changement ou la supprimez d'une tâche de rattrapage, la synchronisation d'état peut potentiellement remplacer votre intervention manuelle. Toutefois, les états des demandes de changement ne déplacent pas automatiquement la tâche de rattrapage de **l'état Fermé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Synchronisation de l'état vers le bas

L'image suivante illustre comment les états CHG déplacent automatiquement les états des tâches de rattrapage dans un cycle de vie en avant, c'est-à-dire **d'Ouvert** à **Résolu**.



Vous pouvez créer de nouvelles demandes de changement pour n'importe quelle tâche de rattrapage dont l'état n'est pas **Résolu** ou **Fermé**. La synchronisation d'état déplace automatiquement le TRG de manière bidirectionnelle entre les états **Ouvert**, **En cours d'examen**, En **attente d'implémentation** et **Résolu** . Ce déplacement est basé sur certaines valeurs du champ État de la demande de changement. La synchronisation de l'état entre la demande de changement et la tâche de rattrapage est invoquée automatiquement sauf si la case à cocher (**Ajouter des CI au CR)** s'affiche sur un formulaire et que vous choisissez de la décocher.

La tâche de rattrapage ne passe pas à **l'état Résolu** lorsqu'un CHG est à l'état ouvert. Tous les CHG dont l'état est antérieur à **l'examen** dans son cycle de vie, tels que **Nouveau**, **Évaluer**, **Autoriser**, **Planifié** ou **Implémenter**, comme illustré à la figure précédente, sont considérés comme des états ouverts pour le CHG. Les états ouverts ne déplacent pas le champ d'état sur la tâche de rattrapage, car les enquêtes ou les tâches sur le CHG ne sont pas terminées. La synchronisation d'état est invoquée lorsqu'un CHG est créé pour la tâche de rattrapage ou associé à celle-ci, ou lorsque l'état d'une relation existante change sur le CHG. Les états CHG terminés sont **Examiner** et **Fermé** avec succès. Lorsqu'un CHG est fermé avec succès, ses codes de fermeture sont : **Réussi** ou **Réussi avec problèmes**, auquel cas la tâche de rattrapage passe à l'état **Résolu**.

Synchronisation de l'état en arrière

Au fur et à mesure qu'un CHG est traité au cours de son cycle de vie, il peut être annulé à un moment donné. Dans ce cas, si le CHG est **annulé** ou **fermé** (avec un code de fermeture **En échec**), la tâche de rattrapage revient automatiquement à En **cours d'examen**. La tâche de rattrapage revient à **En cours d'examen**, car il n'existe aucun plan actif pour corriger la vulnérabilité.

Si une tâche de rattrapage est à l'état **Résolu** et que vous créez un nouveau CHG ou l'associez à un CHG existant dans l'un des états ouverts initiaux, la tâche de rattrapage revient automatiquement à **l'état En attente d'implémentation**. La tâche de rattrapage revient à cet état, car davantage de tâches sont maintenant affectées au CHG.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de rattrapage avec plus d'un CHG

Si plusieurs CHG sont associés à une tâche de rattrapage en **attente d'implémentation** , la synchronisation de l'état est basée sur l'état du CHG dans l'état le plus précoce de son cycle de vie. Par exemple, supposons qu'une tâche de rattrapage soit associée à quatre CHG, CHG1, CHG2, CHG3 et CHG4, comme indiqué dans la table suivante.

Numéro de CHG	État du changement
1	**Implémenter**
2	**Annulé**
3	Fermé (code de fermeture en **échec**)
4	Fermé (code de fermeture **En échec**)

Dans ce cas, la synchronisation d'état entre le CHG et la tâche de rattrapage est basée sur CHG1, qui se trouve dans l'état le plus ancien des quatre CHG (**Implémenter**). Dans ce cas, la tâche de rattrapage reste **en attente d'implémentation**.

Dans un autre exemple, si une tâche de rattrapage est à l'état **Résolu** et qu'un CHG existant a été implémenté et est à l'état **Réviser** , et qu'un nouveau CHG est créé, la tâche de rattrapage revient de **Résolu** à **En attente d'implémentation**. La synchronisation d'état est basée sur le CHG dans l'état **Nouveau** , qui est le CHG dans l'état le plus ancien.

Numéro de CHG	État du changement
1	Revue
2	Nouveau

De même, lorsque les tâches de rattrapage ont plusieurs CHG, l'état de la tâche de rattrapage change automatiquement dans les cas suivants :

- Lorsqu'un CHG passe à **l'état Révision**, si tous les autres CHG associés à la tâche de rattrapage sont à l'état **Examen** ou **Fermé** (avec un code de fermeture réussi), la tâche de rattrapage passe automatiquement à **l'état Résolu**. Tous les autres CHG associés qui sont annulés ou fermés sans succès sont ignorés.
- Lorsqu'un CHG passe à **l'état Annulé** ou **Fermé** (code de fermeture en **échec**), si tous les autres CHG associés à la tâche de rattrapage sont dans le même état, la tâche de rattrapage revient automatiquement à **l'état En cours d'examen**.

Pour en savoir plus sur les états des tâches de rattrapage et sur ce que vous pouvez faire dans chaque état, reportez-vous à la section Conformité de la configuration États.

Séparation de domaine et Conformité de la configuration

L'application Séparation de domaine est prise en charge dans Conformité de la configuration. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Niveau de prise en charge : Standard

- Inclut tous les aspects du support de niveau **basique** .
- Les propriétés d'application sont sensibles au domaine selon les besoins.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Comment fonctionne Séparation de domaine dans Conformité de la configuration

Grâce à Séparation de domaine, vous pouvez standardiser les procédures (Conformité de la configuration) pour l'ensemble de la clientèle que vous servez, tout en réduisant les coûts d'exploitation et en améliorant la qualité de service.

Séparer les espaces de travail des clients pour les workflows, les tableaux de bord, les rapports, etc., garantit que les données client sont séparées et ne sont jamais exposées à d'autres clients.

Prise en charge de Domain Separation dans par Conformité de la configuration versions

Mise en production	Niveau de prise en charge	Notes
Orlando	Standard	
Paris	Standard	
Québec	Standard	
Rome	Standard	
San Diego	Standard	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prise en charge de Domain Separation dans par Conformité de la configuration versions (suite)

Mise en production	Niveau de prise en charge	Notes
Tokyo	Standard	
Utah	Standard	
Vancouver	Standard	

Séparation de domaine pour l'application Conformité de la configuration couvre les fonctionnalités de produit suivantes :

- Ingère les résultats des tests à partir d'analyseurs tiers (Qualys) dans le domaine approprié.

  Les données sont ingérées dans le même domaine que celui de l'utilisateur d'intégration, dont les informations d'identification sont utilisées pour l'intégration.
- Analyse à nouveau des hôtes spécifiques dans Conformité de la configuration le domaine à partir duquel ils ont été demandés.
- Utilise le processus de recherche de CI CMDB pour s'assurer que les informations CI provenant des scanners correspondent aux CI dans la CMDB du domaine de l'utilisateur d'intégration.
- Calcule les scores de risque au niveau du résultat du test selon le calculateur de score de risque défini dans le même domaine que celui de l'utilisateur d'intégration.
- La ou les règles de tâche de rattrapage peuvent être définies, affectées et rester dans le même domaine que le domaine de l'utilisateur d'intégration.
- Les tâches de rattrapage créées à l'aide des règles de tâche de rattrapage de document restent dans le même domaine que celui dans lequel les règles de tâche de rattrapage sont créées.
- Le workflow de report passe par le processus d'approbation dans le domaine pour lequel le report est demandé.
- Les rapports et les tableaux de bord affichent les états des résultats des tests, tels que l'âge des résultats des tests, les résultats des tests ouverts par CI, les résultats des tests par impact dans le domaine auquel ils appartiennent.
- Les connaissances provenant d'analyseurs tiers (Qualys) peuvent être ingérées dans le domaine global et les données peuvent être partagées entre plusieurs clients.

Remarque : Dans tous les cas ci-dessus, les principes généraux de la séparation dans des domaines séparés s'appliquent dans la Now Platform.

Cas d'utilisation

L'application Conformité de la configuration gère le cycle de vie d'un résultat de test de bout en bout. Les cas d'utilisation suivants sont sensibles à la séparation de domaine :

- **Ingérer les** résultats des tests à partir de Qualys
  - Ingérer des données à partir de plusieurs instances
  - Dédupliquer les résultats des tests
  - Correspondance avec le CI CMDB

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Enrichissement** des résultats des tests avec les scores de risque
  - Enrichissement des actifs (CMDB)
  - Score du risque
- **Regroupez** les résultats des tests et affectez la tâche de rattrapage
  - Regroupement automatique des résultats des tests
  - Affecter automatiquement la tâche de rattrapage
- **Rattraper**
  - Tâche de rattrapage affectée comme tâche de rattrapage
  - Cycle de vie complet des rattrapages
  - Workflow du report
- **Mesurer** la posture de sécurité de l'organisation et le programme de gestion de la conformité
  - Tendance des résultats, par conformité, catégorie, criticité et technologie
  - État et distribution des politiques, des tests, des hôtes, des résultats des tests et du score de risque

Configuration

La configuration de Séparation de domaine pour Conformité de la configuration ne nécessite aucune étape supplémentaire. Toutes les Conformité de la configuration tables acquièrent la colonne Domaine une fois que l'instance est séparée par domaine. Vous pouvez diriger les données d'importation d'intégration de résultats de test vers des domaines spécifiques. Pour plus d'informations, consultez Créer des importations séparées par domaine pour une intégration. Pour plus d'informations sur les précautions et les paramètres supplémentaires, reportez-vous à la section Paramètres supplémentaires pour la séparation de domaine.

Données séparées par domaine

Les données peuvent être séparées par domaine, ce qui signifie :

- Les résultats des tests ingérés à partir d'analyseurs tiers restent dans le même domaine que le domaine de l'utilisateur d'intégration et ne sont accessibles à partir d'aucun autre domaine.
- Les résultats des tests ou les hôtes d'un domaine ne peuvent pas être consultés à partir d'autres domaines.
- L'algorithme de notation des risques et les règles de groupe de résultats des tests ne peuvent être consultés par personne en dehors du domaine.
- Les workflows de report créés dans un domaine ne sont pas visibles dans un autre domaine.
- Toutes les notifications par e-mail sont contenues dans le domaine auquel elles appartiennent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment les analystes de conformité gèrent-ils leurs propres données d'application ?

- Les analystes créent leurs propres règles d'installation d'application, de gestion des applications multisources et de recherche de CI.
- Les analystes peuvent configurer des intégrations spécifiques exclusivement pour une utilisation dans le domaine.
- Les analystes peuvent créer leurs propres workflows de gestion des reports et des changements.
- Les analystes peuvent créer leurs propres règles de tâche de rattrapage, leur propre logique de notation des risques pour hiérarchiser avec précision les résultats, affecter automatiquement des tâches de rattrapage et les affecter au groupe d'affectation approprié.
- Les utilisateurs du domaine créent une tâche de rattrapage manuelle, puis la ferment.

Logique métier et processus pouvant être séparés par domaine par le propriétaire de l'instance

- Conformité de la configuration Utilisateurs et groupes
- Conformité de la configuration intégrations (à partir de la version Madrid)
- Configuration complète de la configuration (gestion des utilisateurs et des groupes, installation d'applications, gestion des applications multisources, règles de recherche de CI, règles de tâche de rattrapage, calculateurs de risque, etc.)
- Cycle de vie complet du rattrapage, y compris le report

Information associée

Séparation de domaine pour les fournisseurs de services

Conformité de la configuration Cartes de criticité

Conformité de la configuration Le mappage de criticité transforme les champs de criticité de la source en champs dans Conformité de la configuration.

Le Conformité de la configuration système de base est livré avec un mappage standard Qualys Cloud Platform à standard ServiceNow . La création ou la modification d'une carte de criticité est destinée uniquement aux mappages tiers personnalisés ou non standard dans votre environnement.

Conformité de la configuration États

Avec Conformité de la configuration, vous pouvez afficher un modèle d'état pour connaître l'état de la tâche de rattrapage à un moment donné. Les états des tâches de rattrapage contrôlent les états des résultats des tests par priorité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

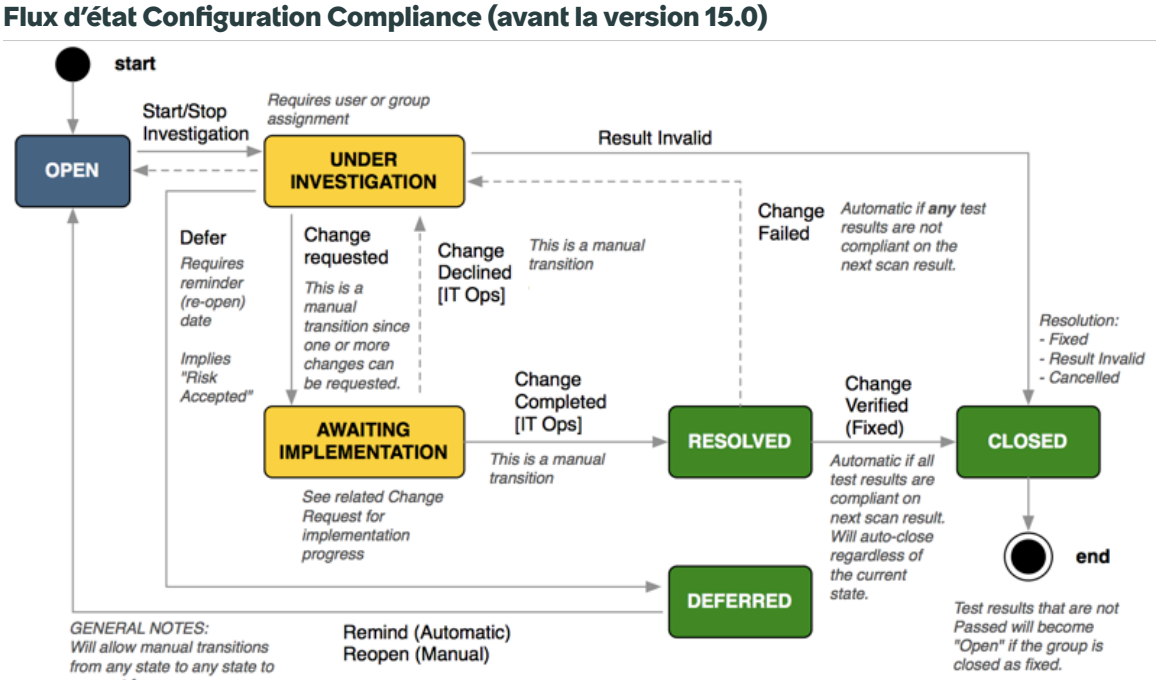
Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

États des tâches de rattrapage

Les tâches de rattrapage (RT) ont de nombreux états possibles. La transition automatique est disponible à partir de l'état Résolu en fonction des résultats de l'analyse suivante. Si tous les résultats des tests réussissent à l'analyse suivante, la tâche de rattrapage est fermée. Sinon, il passe à l'état En cours d'examen. Le système vérifie cet état de fermeture, mais il réévalue l'état de la tâche de rattrapage si un résultat de test est ajouté ou supprimé de la tâche de rattrapage. Les notes de travail sont mises à jour pour refléter la transition.

La figure suivante montre comment l'état d'une tâche de rattrapage passe de l'état Ouvert à l'état Fermé.

Flux d'état Configuration Compliance (avant la version 15.0)



Remarque :

- Chaque formulaire de tâche de rattrapage contient des boutons **Suivre** et **Mettre à jour** , qui sont standard pour ServiceNow les tâches.
- À partir de la version 15.0 de Conformité de la configuration, les éléments suivants ont été supprimés :
  - **Bouton Fermer**
  - le champ **Résolution** dans le modal Résoudre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le tableau suivant répertorie les Conformité de la configuration états.

États de Configuration Compliance

État	Description
Ouvert	État à la création.
En cours d'examen	Déclenché par le bouton **Démarrer l'examen** . À partir de cet état, vous pouvez : **Créer une demande de changement** Pour plus d'informations, consultez Créer une demande de changement dans Conformité de la configuration. **Demande d'exception** Indiquez un motif et sélectionnez une date de réouverture. **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage. **Marquer comme faux positif** Indiquez un motif et des notes. Marque la tâche de rattrapage comme un faux positif.
En cours de révision	Déclenché lorsque la tâche de rattrapage est en cours d'évaluation pour l'action suivante. Généralement utilisé pour valider les résultats des enquêtes ou approuver les changements/exceptions proposés avant l'implémentation. À partir de cet état, vous pouvez passer à l'un des éléments suivants en fonction de votre approbation ou de vos rejets : **En attente d'implémentation** Transition vers En attente d'implémentation si approuvé **En cours d'examen** Transition vers En cours d'examen si une analyse plus approfondie est nécessaire. **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage.
Différé	Déclenché par le bouton **Différer** . À partir de cet état, vous pouvez : **Rouvrir** Transition vers un état ouvert. **Supprimer** Confirmez la suppression. Supprime le groupe. Les informations sur le report s'affichent sous l'onglet connexe **Différer/Fermer** . À la date de report, le groupe rouvre pour correction.
En attente d'implémentation	Déclenché par le bouton **En attente d'implémentation** . À partir de cet état, vous pouvez : **Créer un incident de sécurité** Pour plus d'informations, consultez Créer un incident de sécurité. **Créer une demande de changement**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États de Configuration Compliance (suite)

État	Description
	Pour plus d'informations, consultez Créer une demande de changement dans Conformité de la configuration. **Résoudre** Dans les **notes de résolution**, ajoutez la raison pour laquelle vous résolvez la tâche de rattrapage. L'état devient Résolu. Les notes s'affichent sous l'onglet connexe **Résolution** . **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage.
Résolu	Déclenché à partir du bouton **Résoudre** . À partir de cet état, vous pouvez : **Créer un incident de sécurité** Pour plus d'informations, consultez Créer un incident de sécurité. **Rouvrir** Transition vers un état ouvert. **Supprimer** Confirmez la suppression. Supprime la tâche de rattrapage. Les notes apparaissent sous l'onglet **Notes** associées. Les informations sur la résolution apparaissent sous l'onglet **Résolution** connexe. Les notes sont reflétées dans les **notes de travail** de tous les résultats des tests associés à la tâche de rattrapage.
Fermé	Déclenché à partir du bouton **Fermer** ou du bouton **Marquer comme faux positif** . À partir de la version 14.12 de , vous pouvez fermer une tâche de Conformité de la configuration rattrapage en la marquant comme faux positif. À partir de cet état, vous pouvez : **Rouvrir** Transition vers un état ouvert. **Supprimer** Confirmez la suppression. Supprime le groupe. Les informations sur la fermeture apparaissent sous l'onglet connexe **Différer/Fermer** . Les notes sont reflétées dans les **notes de travail** de tous les résultats des tests associés à la tâche de rattrapage.

- Si la tâche de rattrapage est marquée comme fermée ou corrigée et si le résultat de test ajouté n'est pas lui-même fermé ou fixe, l'état du résultat du test ne change pas et l'état de la tâche de rattrapage devient Ouvert.
- Lorsque vous créez une nouvelle tâche de rattrapage ou divisez une tâche de rattrapage, les champs **Motif etJusqu'à** sont réévalués pour les tâches de rattrapage nouvelles et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

anciennes. Lorsque l'état de tous les résultats des tests est Différé, la valeur des champs Motif et **Jusqu'à** est déployée sur la tâche de rattrapage.

- Si tous les résultats des tests d'une tâche de rattrapage sont reportés et ont le même **motif**, alors la tâche de rattrapage est affectée au même **motif**. Sinon, le champ **Motif** est remplacé par **Aucun**.
- La date du champ **Jusqu'à** est mise à jour avec la date de fin la plus proche de toutes les tâches de rattrapage auxquelles appartiennent les résultats des tests.

Remarque : Cette évaluation est effectuée par la tâche planifiée, qui s'exécute `Rollup test result values to test result RT1nd configuration test` toutes les heures.

- Si la **dernière observation est postérieure** à la **date de résolution** d'un résultat de test résolu, le résultat du test est rouvert. Dans une tâche de rattrapage résolue, si au moins un résultat de test est rouvert pendant l'ingestion, la tâche de rattrapage passe à l'état En cours d'examen.

États des résultats des tests

L'état d'une tâche de rattrapage modifie également l'état de ses résultats des tests associés. Ce mécanisme comporte deux cas :

Résultats des tests qui appartiennent à une seule tâche de rattrapage

Les résultats correspondent à l'état de la tâche de rattrapage à trois exceptions près :

- Si la tâche de rattrapage passe à l'état Fermé et sa résolution (sous-état) à Corrigé, l'élément ignore ce changement et revient alors à l'état Ouvert.
- Si la tâche de rattrapage passe à l'état Fermé et sa résolution (sous-état) à Annulé, l'élément ignore ce changement et repasse à l'état Ouvert.
- Si l'état de la source du résultat de test est Fixe (mis à jour par une analyse ou une importation), lorsque la tâche de rattrapage change d'état, le résultat de test passe à l'état Fermé (Corrigé), quel que soit l'état de la tâche de rattrapage.

Résultats des tests qui appartiennent à plusieurs tâches de rattrapage

Les résultats des tests ne correspondent pas automatiquement à l'état de la tâche de rattrapage. Au lieu de cela, il recherche parmi tous les groupes associés pour trouver l'état avec la priorité la plus élevée à appliquer. Voici l'état de priorité :

Fermé > **Fermé (sous-état : faux positif)** > **Différé** > **Résolu** > **En cours de révision** > **En attente d'implémentation** > **En cours d'examen** > **Ouvert** > **Fermé (sous-état : annulé)** > **Fermé (sous-état : Fixe)**

Remarque : **Fermé (sous-état : Fixe)** et **Fermé (sous-état : Annulé)** sont deux cas particuliers.

Remarque : À partir de la version 15.0 de Conformité de la configuration, le sous-état **Résultat non valide** a été déconseillé.

Exemples d'états de tâches de rattrapage

Par exemple :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État des tâches de remédiation	État du résultat du test
RT1 : **Ouvert** > **En cours d'examen** RT2 : **Ouvert**	**En cours d'examen** Lorsque RT1 est En cours d'examen et RT2 est ouvert, le résultat du test passe à En cours d'examen, car après la recherche, entre RT1 et RT2, RT1 a l'état avec la priorité la plus élevée.
RT1 : **en cours d'examen** RT2 : **Ouvert** > **En cours d'examen**	**En cours d'examen** Lorsque RT2 est en cours d'examen et RT1 est en cours d'examen, le résultat du test reste en cours d'examen, car après la recherche, entre RT1 et RT2, ils ont l'état avec la même priorité.
RT1 : **en cours d'examen** RT2 : **En cours d'examen** > **En attente d'implémentation**	**En attente d'implémentation** Lorsque RT2 est En attente d'implémentation et RT1 est En cours d'examen, le résultat du test passe à En attente d'implémentation, car après la recherche, entre RT1 et RT2, RT2 a l'état avec la priorité la plus élevée.
RT1 : **En cours d'examen** > **Différé** RT2 : **En attente d'implémentation**	**Différé** Lorsque RT1 est Différé et RT2 est En attente d'implémentation, le résultat du test passe à Différé, car après la recherche, l'élément 1 a découvert qu'entre RT1 et RT2, RT1 a l'état avec la priorité la plus élevée
RT1 : **Différé** RT2 : **En attente d'implémentation** > **Fermé (résultat non valide)**	**Fermé (résultat non valide)** > **Différé** Lorsque RT2 est Fermé et que la résolution (sous-état) est Résultat non valide et que RT1 est Différé, le résultat du test passe à Fermé (résultat non valide), car après la recherche, entre RT1 et RT2, RT2 a l'état avec la priorité la plus élevée.
RT1 : **Différé** RT2 : **Fermé (résultat non valide)** > **Ouvrir (via Rouvrir)**	**Différé** Lorsque RT2 est rouvert et que son état devient Ouvert, et que RT1 est Différé, le résultat du test passe à Différé, car après la recherche, entre RT1 et RT2, RT1 a l'état ayant la priorité la plus élevée.
RT1 : **Différé** RT2 : **En attente d'implémentation** > **Fermé (faux positif)**	**Fermé (faux positif)** Lorsque RT2 est Fermé et que la résolution (sous-état) est Faux positif et que RT1 est Différé, le résultat du test passe à Fermé (faux positif), car après la recherche, entre RT1 et RT2, RT2 a l'état avec la priorité la plus élevée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas particuliers de l'état du résultat du test

État de la tâche de rattrapage	État du résultat du test
RT1 : **En cours d'examen** RT2 : **En attente d'implémentation** > **Fermé (fixe ou annulé)**	**En cours d'examen** Lorsque RT2 est Fermé (sous-état Fixe ou sous-état Annulé) et RT1 est En cours d'examen, le résultat du test passe de En attente d'implémentation (auparavant, la priorité la plus élevée) à En cours d'examen (actuellement, la priorité la plus élevée).
RT1 : n'importe quel état RT2 : n'importe quel état	Si l'état de la source du résultat de test est Fixe (mis à jour par une analyse ou une importation), lorsque la tâche de rattrapage change d'état, le résultat du test passe à l'état Fermé (Corrigé), quel que soit l'état des autres tâches de rattrapage associées. La recherche des résultats des tests pour l'état de la tâche de rattrapage ne se produit pas.

Scénarios de déploiement et de réduction de l'état

Les scénarios de déploiement et de réduction d'état synchronisent automatiquement l'état des tâches de rattrapage (RT) et le résultat des tests de configuration (CTR), garantissant des mises à jour en temps réel sur les deux. Cette interaction dynamique réduit le suivi manuel, améliore la précision et fournit aux utilisateurs une vue actualisée de la progression, ce qui rend la conformité de la configuration plus efficace et aide les utilisateurs à prendre rapidement des décisions éclairées.

Comportement de déploiement

Lorsque l'état du résultat du test de configuration (CTR) change, ces changements peuvent se propager jusqu'au niveau de la tâche de rattrapage (RT).

Le tableau suivant récapitule les principaux scénarios de déploiement dans lesquels les changements dans l'état du résultat des tests de configuration (CTR) peuvent influencer l'état de la tâche de rattrapage (RT) associée, en fonction des conditions de fermeture, des réaffectations et des reports.

Scénarios de déploiement

État CTR	État RT
Ouvert > Fermé-Corrigé	Ouvert > Fermé-Corrigé
Ouvert > fermé : périmé	Ouvert > Fermé-annulé

Comportement de réduction

Lorsque l'état d'une tâche de rattrapage change, l'état est souvent propagé aux CTR associés, sauf s'il est remplacé par des mises à jour manuelles ou des exceptions.

Le tableau suivant récapitule les principaux scénarios de déploiement dans lesquels les changements apportés à l'état de la tâche de rattrapage (RT) peuvent affecter l'état du résultat du test de configuration (CTR) associé, en fonction des règles de priorité et des conditions spéciales.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Scénarios de déploiement

État RT	État CTR
Ouvrir > en cours d'examen	Ouvrir > en cours d'examen
Ouvrir > en cours de révision	Ouvrir > en cours de révision
Ouvert > différé	Ouvert > différé
Différé > ouvert	Reste différé
Ouvert > Résolu-Corrigé	Ouvert > Résolu-Corrigé
Ouvert > Résolu-Corrigé > Fermé-Corrigé	Ouvert > Résolu-Corrigé > Fermé-Corrigé
Ouvrir > Résultat résolu non valide	Ouvrir > Résultat résolu non valide
Ouvert > Résolu-annulé	Ouvert > Résolu-annulé
Ouvert > Résolu-Annulé > Fermé	Ouvert > Résolu-Annulé > Fermé
Ouvrir > Résultat résolu non valide > Résultat fermé non valide	Ouvrir > Résultat résolu non valide > Résultat fermé non valide
Ouvert > Fermé-Corrigé	Ouvert > Fermé-Corrigé

Résolution des Conformité de la configuration problèmes d'importation

Résolvez les problèmes liés à l'importation d'intégration tierce.

Importer la résolution du problème

Problème	Résolution
Les résultats des tests sont manquants	Vérifiez le sur l'intégration *`Start Time`***de Qualys PC Results** . Il n'est peut-être pas assez reculé. Consultez Modifier la date de début des résultats du PC Qualys.
L'intégration échoue	Vérifiez l'état **d'exécution de l'intégration de vulnérabilité** . Les entrées des processus d'intégration individuelles contiennent le code XML importé, qui peut être examiné à la recherche d'informations inattendues. Accédez à la **Intégration de vulnérabilité Qualys** > **Intégrations principales** > **Résultats QualysPC** > **Exécutions d'intégration de vulnérabilité** onglet connexe. Choisissez la dernière exécution. Examinez l'état et les notes des entrées de la liste connexe **Processus d'intégration des vulnérabilités à la** recherche d'anomalies. .

Modifier la date de début des résultats du PC Qualys

Si des données sont manquantes pour la date de début dans l'importation des résultats des PC Qualys, elles peuvent être modifiées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_vul_qualys.admin

Procédure

1. Accédez à la **Tous** > **Intégration de vulnérabilité Qualys** > **Administration** > **Intégrations principales**.
2. Cliquez sur **Intégration de Qualys PC Results** .
3. Cliquez sur **Détails de l'intégration**.
4. Définissez le champ **Heure de début** sur une valeur passée, de sorte que tous les résultats des tests analysés et détectés depuis cette heure soient détectés.

   Remarque : Si la date est laissée vide, aucune donnée n'est renvoyée lors de la première exécution. Définissez la valeur sur un maximum d'un mois dans le passé. Ce paramètre empêche une grande quantité de données de dépasser les limites de débit de l'API Qualys et de déclencher des délais d'exécution.

5. Cliquez sur **Envoyer** ou **Mettre à jour**.
6. **Facultatif :** Cliquez sur **Exécuter maintenant** pour l'exécuter immédiatement.

Règles de recherche de CI pour Microsoft Defender for Cloud IntegrationOpérations de sécurité et Palo Alto Prisma Cloud

Vous pouvez utiliser les règles de recherche d'éléments de configuration (CI) pour les Microsoft Defender for Cloud Integration intégrations et Palo Alto Prisma Cloud afin de trouver une correspondance correcte avec les types de ressources couramment utilisés dans le Base de données de gestion des configurations (CMDB).

Vue d'ensemble

Le module Règles de recherche de CI contient les règles qui vous aident à définir les champs qui ont les données correspondantes dans le Base de données de gestion des configurations (CMDB). Vous pouvez utiliser ces règles pour identifier les applications et les mises en production de l'application. Tous les actifs et Palo Alto Prisma Cloud sont identifiés de manière unique par la combinaison de leur ID d'objet, de leur compte dans le cloud et de leur centre de données logique dans la ServiceNow plateforme. ServiceNow Discovery Microsoft Defender for Cloud Integration renseigne l'ID de ressource dans la colonne `Object_id` dans différents formats pour les différents types de CMDB ressources. La table suivante présente les formats d'ID d'objet des types de ressources couramment utilisés par le service de découverte pour remplir la colonne `Object_id` du CI. Tout scanner qui souhaite rechercher une ressource d'un type de ressource particulier doit effectuer la recherche à l'aide du bon format d'ID d'objet. Vous pouvez obtenir le bon format d'ID d'objet en consultant la colonne d'ID d'objet de la classe CI correspondante CMDB , puis essayer de construire l'ID d'objet à l'aide des valeurs reçues du scanner.

Format d'ID d'objet pour divers types de ressources

Type de ressource	Format
AWS::EC2::Instance	Identifiant d'objet
AWS::ElasticLoadBalancing::LoadBalancer	Nom de l'équilibreur de charge
AWS::S3::Bucket	arn :aws :s3 :::<nom de la catégorie>

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La correspondance de CI pour un résultat de test peut ne pas être trouvée avec précision dans le Base de données de gestion des configurations (CMDB) à moins que le même format de `object_id` ne soit utilisé dans la règle de recherche. La plupart du temps, les règles de recherche de CI OOB trouvent une correspondance pour les types de ressources les plus couramment utilisés pour Microsoft Defender for Cloud Integration et Palo Alto Prisma Cloud. Si les règles de recherche de CI suivantes ne trouvent pas les CI dans le CMDB pour vos résultats de test, vous pouvez créer une règle de recherche de CI pour un type de ressource. Pour en savoir plus sur la création d'une règle de recherche de CI, consultez Créer une règle de recherche de CI.

Règles de recherche de CI

Les règles de recherche de CI suivantes sont spécifiques au Microsoft Defender for Cloud Integration et Palo Alto Prisma Cloud.

Catégorie S3

Cette règle de recherche tente de trouver le CI dans le CMDB par la valeur obtenue en concaténant l'`arn :aws :s3 :::` et le nom de la ressource. La valeur obtenue est recherchée dans la colonne `object_id` de la table `cmdb_ci_cloud_object_storage` . Cette règle de recherche s'applique uniquement lorsque le type de ressource est `AWS ::S3 ::Bucket`.

Nom

Cette règle de recherche tente de trouver le CI dans le CMDB par nom. Le nom, qui est recherché dans la colonne `Object_id` de la classe CI, correspond à un type de ressource dans la table `sn_capi_resource_type` .

Remarque : Pour l'application Palo Alto Prisma Cloud, cette règle de recherche de CI s'exécute uniquement pour les types de ressources `AWS ::RDS ::D BInstance`, `AWS ::ElasticLoadBalancing ::LoadBalancer` et `AWS ::CloudTrail ::Trail`. Vous pouvez ajouter les types de ressources pour lesquels vous souhaitez exécuter cette règle de recherche de CI.

ID de ressource

Cette règle de recherche tente de trouver le CI par CMDB l'ID de ressource. L'ID de ressource, qui est recherché dans la colonne `Object_id` de la classe CI, correspond à un type de ressource dans la table `sn_capi_resource_type` .

Remarque : Vous pouvez définir la priorité d'une règle de recherche de CI dans le champ **Commande** . La règle de recherche de CI ayant la valeur d'ordre la moins élevée est exécutée en premier.

Réponse aux vulnérabilités Espaces de travail

Les espaces de travail Réponse aux vulnérabilités offrent une vue consolidée des fonctionnalités qui vous permet d'effectuer plusieurs tâches à partir du même volet tout en augmentant votre productivité et en vous faisant gagner du temps.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux vulnérabilités Espaces de travail

Espace de travail du gestionnaire de vulnérabilité	Espace de travail de remédiation informatique	Espace de travail de l'évaluation de la vulnérabilité
		
En savoir plus sur l’espace de travail du gestionnaire de vulnérabilité	En savoir plus sur l’espace de travail de remédiation informatique	En savoir plus sur l’espace de travail Évaluation de la vulnérabilité

Avant de commencer

Avant de pouvoir utiliser les espaces de travail :

- Vous devez effectuer quelques tâches de configuration. Pour plus d'informations, consultez Configurer les Réponse aux vulnérabilités espaces de travail.
- Consultez les informations importantes sur les mises à jour des tâches de rattrapage, les règles de tâche de rattrapage et les termes et concepts clés relatifs aux espaces de travail dans Réponse aux vulnérabilités Espaces de travail et mises à jour des tâches de rattrapage et des règles de tâche de rattrapage.

Dépannage et demande d'aide

- Security Operations sur ServiceNow Community
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Réponse aux vulnérabilités Vue d’ensemble des espaces de travail

Les espaces de travail Gestionnaire des vulnérabilités et Rattrapage informatique prennent en charge Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs et Conformité de la configuration.

Espaces de travail Gestionnaire des vulnérabilités, Rattrapage informatique et Évaluation de la vulnérabilité

Espace de travail du gestionnaire de vulnérabilités

En tant que gestionnaire des vulnérabilités, protégez les actifs de votre entreprise contre les programmes malveillants et les attaques malveillantes. À partir d’une seule zone de travail de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

votre ServiceNow AI Platform®, avec l'application, ainsi que les Réponse aux vulnérabilités données de vulnérabilité actuelles importées dans votre instance à partir de bibliothèques de vulnérabilités et d'applications de données d'analyse tierces, identifiez les vulnérabilités critiques et les erreurs de configuration, hiérarchisez-les et envoyez des listes de tâches de rattrapage au service informatique pour que ses spécialistes prennent des mesures.

Espace de travail de remédiation IT

En tant que spécialiste informatique, utilisez les listes ou les tâches de rattrapage envoyées par les gestionnaires de vulnérabilité pour surveiller et résoudre les vulnérabilités critiques qui vous sont affectées ou sont affectées à vos groupes. Corrigez les groupes d'éléments vulnérables à l'aide de correctifs, de solutions, de nouvelles analyses de vulnérabilité, de demandes de changement, d'exceptions et d'autres outils permettant de corriger les éléments vulnérables et de tester les résultats à partir d'un seul emplacement.

Espace de travail de l'évaluation de la vulnérabilité

En tant que gestionnaire d'événements de vulnérabilité, effectuez une évaluation de l'exposition et gérez de manière proactive les événements de vulnérabilité critiques, en particulier lors d'événements de vulnérabilité critiques tels qu'un événement zero-day.

Fonctionnalités principales

Les Réponse aux vulnérabilités espaces de travail incluent les fonctionnalités et améliorations suivantes.

- Utiliser la fonctionnalité de modification en bloc dans le Espace de travail du gestionnaire de vulnérabilités pour mettre à jour plusieurs enregistrements simultanément. Pour plus d'informations, consultez Utilisation de la modification en bloc dans le Espace de travail du gestionnaire de vulnérabilités.
- Consultez les tableaux de bord Gestion de la vulnérabilité (PA), Approbations de vulnérabilité, CISO, Vue d'ensemble de la gestion de la vulnérabilité du conteneur, Tableau de bord de gestion de la vulnérabilité des applications, Réponse aux vulnérabilités unifiée et Intégrité dans l'interface utilisateur Next Experience sur la page Tableaux de bord de l'espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Page Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités.
- Affichez le tableau de bord Rattrapage des vulnérabilités dans l'interface utilisateur Next Experience sur la page Tableaux de bord de l'espace de travail Rattrapage informatique. Pour plus d'informations, consultez Page Tableaux de bord dans Espace de travail de remédiation IT.
- Créez manuellement les tâches de rattrapage (VUL, AVUL, CVUL ou CRG) dans le Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT. Pour plus d'informations, consultez Créer une tâche de rattrapage manuellement dans le Espace de travail du gestionnaire de vulnérabilités et Créer une tâche de rattrapage manuellement dans le Espace de travail de remédiation IT.
- Divisez les tâches de remédiation (VUL, AVUL, CVUL et CRG) dans le Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT. Pour plus d'informations, voir Demander des exceptions pour les tâches et les enregistrements de rattrapage dans Espace de travail du gestionnaire de vulnérabilités et Fractionner une tâche de rattrapage dans le Espace de travail de remédiation IT respectivement.
- Demandez les exceptions de politique pour les éléments vulnérables (VIT, AVIT et CVIT) et les tâches de rattrapage (VUL, AVUL, CVIL et CRG) dans les espaces de travail Gestionnaire des vulnérabilités et Rattrapage informatique. Pour plus d'informations, voir Demander des exceptions pour les tâches et les enregistrements de rattrapage dans Espace de travail du

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

gestionnaire de vulnérabilités et Demander une exception à l'aide de GRC : Gestion de la politique et de la conformitéEspace de travail de remédiation IT respectivement.

- Créez et suivez les événements de vulnérabilité critiques via Vulnerability Crisis Management (VCM). Pour plus d'informations, consultez Explorer l'espace de travail de l'évaluation de la vulnérabilité.
- Ajoutez des commandes de compensation à la bibliothèque de commandes de compensation dans le Espace de travail du gestionnaire de vulnérabilités. Pour plus d'informations, consultez Ajouter un contrôle de compensation à la bibliothèque.
- Demandez une réduction du risque pour un élément vulnérable d'hôte et une tâche de rattrapage à partir de l'espace de travail de rattrapage informatique. Pour plus d'informations, consultez Demander une réduction du risque pour un élément vulnérable ou une tâche de rattrapage.
- Créez un problème Agile et un problème Jira pour les éléments vulnérables d'applications Espace de travail du gestionnaire de vulnérabilités et de conteneurs à partir du . Pour plus d'informations, consultez Créer manuellement un problème Agile à l'aide de l'action de formulaire et Créer manuellement un problème Agile à l'aide de l'action de liste.

Pour plus d'informations sur la compatibilité des versions avec les versions de famille, consultez l'article KB0856498 Vulnerability Response Compatibility Matrix and Release Schema Changes dans la base de connaissances HI.

Orchestration de correctifs avec les Réponse aux vulnérabilités espaces de travail

Vous pouvez gérer les correctifs et les déploiements de correctifs pour les vulnérabilités critiques pour de grands groupes de vos actifs avec l'orchestration de correctifs avec Réponse aux vulnérabilités.

Orchestration de correctifs dans les espaces de travail

L'orchestration des correctifs avec l'application Réponse aux vulnérabilités utilise des importations planifiées à partir d'intégrations de solutions tierces, de fournisseurs de correctifs et de scanners de vulnérabilité.

L'orchestration des correctifs avec l'application Réponse aux vulnérabilités est prise en charge à la fois dans l'environnement classique et dans les espaces de Réponse aux vulnérabilités travail. Les données corrélées sont déployées et affichées à la fois dans les espaces de travail et dans l'environnement classique. Pour obtenir une présentation des fonctions, des exigences et des informations relatives à l'orchestration des correctifs dans l'environnement classique, reportez-vous à la section Orchestration de correctifs avec Réponse aux vulnérabilités.

- Pour plus d'informations sur les intégrations prises en charge avec les fournisseurs de correctifs, consultez Présentation de l'intégration de l'orchestration de correctifs HCL BigFix avec Réponse aux vulnérabilités et Présentation de l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs à Microsoft SCCM.
- Pour plus d'informations sur la planification des enregistrements de formulaire de correctifs dans les espaces de travail, reportez-vous aux sections Planifier des correctifs avec l'intégration Microsoft SCCM avec Réponse aux vulnérabilités et Planifier des correctifs avec l'intégration d'orchestration Réponse aux vulnérabilités de correctifs HCL BigFix.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles des applications et dépendances requises pour l'intégration de l'orchestration des correctifs

Pour afficher les données d'orchestration des correctifs et les mises à jour disponibles (correctifs) dans les espaces de travail de Réponse aux vulnérabilités, les applications suivantes sont requises. Toutes les applications répertoriées sont disponibles dans le ServiceNow® Store. Certaines applications nécessitent des abonnements distincts. Consultez Orchestration de correctifs avec Réponse aux vulnérabilités.

Rôles requis

Outre les rôles sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin requis pour les espaces de Réponse aux vulnérabilités travail, les utilisateurs ont besoin de rôles spécifiques aux intégrations d'orchestration de correctifs que vous utilisez pour afficher les données et planifier les correctifs. Consultez les intégrations prises en charge suivantes pour en savoir plus sur ces rôles.

Consultez Présentation de l'intégration de l'orchestration de correctifs HCL BigFix avec Réponse aux vulnérabilités et Présentation de l'intégration de l'orchestration Réponse aux vulnérabilités des correctifs à Microsoft SCCM.

Données de correctifs dans les espaces de Réponse aux vulnérabilités travail

Dans l'espace de travail de remédiation informatique, vous pouvez afficher les données des correctifs dans les espaces de travail :

- Dans la vue d'accueil, cliquez sur tableaux de résultats pour afficher les enregistrements de solutions préférées sur les VI, de CI vulnérables et de correctifs préférés sur les VI.
- Dans la vue de liste, affichez tous les enregistrements de mise à jour de correctif (VPU) et les éléments vulnérables qui vous sont affectés et qui possèdent des correctifs à partir des liens disponibles.

Vous pouvez planifier des correctifs à partir des enregistrements suivants :

- Mise à jour de correctif (VPU)
- Tâche de rattrapage (RT)
- Élément détecté (SDI)

Dans le Espace de travail du gestionnaire de vulnérabilité, vous pouvez afficher les correctifs :

- À partir de la vue Accueil des rubriques de surveillance de l'onglet Éléments vulnérables, vous pouvez afficher les correctifs préférés et potentiels, les dates planifiées des correctifs et d'autres informations.
- Dans la vue de listes sur les enregistrements d'effort de rattrapage, vous pouvez afficher les données de correctifs sur les enregistrements VIT dans l'onglet Éléments vulnérables.

Réponse aux vulnérabilités Espaces de travail et mises à jour des tâches de rattrapage et des règles de tâche de rattrapage

Les tâches de rattrapage regroupent les enregistrements (VIT, AVIT, CVIT ou CTR) dans les espaces de Réponse aux vulnérabilités travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Termes clés pour les Réponse aux vulnérabilités espaces de travail

Espaces de travail Réponse aux vulnérabilités, ou workspaces

Réponse aux vulnérabilités prend en charge les espaces de Réponse aux vulnérabilités travail. Vous pouvez utiliser l'expérience classique Interface utilisateur principale ou les espaces de travail.

Interface utilisateur classique (héritée)

Fait référence à l'expérience Interface utilisateur principale . Vous effectuez toujours certaines actions et affichez quelques listes dans l'environnement classique.

Espace de travail du gestionnaire de vulnérabilité

Dans cet espace de travail, les gestionnaires surveillent les vulnérabilités ciblées et sélectionnent les éléments vulnérables et les résultats des tests qui leur tiennent le plus à cœur d'être affectés au service informatique.

Espace de travail de remédiation informatique

Dans cet espace de travail, les équipes informatiques peuvent se concentrer sur les vulnérabilités les plus importantes qui leur sont affectées par la sécurité. Les informations centrées sur l'informatique, qui incluent les éléments de configuration (CI) distincts impactés, les solutions et la progression du rattrapage sont facilement accessibles aux propriétaires de rattrapage dans cet espace de travail.

Espace de travail de l'évaluation de la vulnérabilité

Dans cet espace de travail, les analystes de vulnérabilité peuvent effectuer une évaluation de vulnérabilité pendant l'analyse de vulnérabilité zero-day. Une fois qu'une vulnérabilité zero-day est identifiée, ils peuvent évaluer l'impact potentiel et le risque associés à la vulnérabilité. Les analystes peuvent analyser le système, les applications ou les composants réseau affectés pour comprendre la gravité et les vecteurs d'attaque possibles au sein de l'organisation.

Rubrique de surveillance

Les rubriques de visualisation définissent un segment des éléments vulnérables que les gestionnaires de vulnérabilité et les analystes souhaitent surveiller dans l'espace de travail du gestionnaire de vulnérabilité. Les rubriques de visualisation présentent un ensemble de rapports ciblés relatifs à un segment d'éléments vulnérables et de résultats des tests avec des statistiques de tendance, de CI et liées aux vulnérabilités. Les tableaux de bord sur ces sujets peuvent être utilisés pour surveiller les tendances. Les tableaux de bord peuvent également aider les gestionnaires à :

- Afficher la progression du rattrapage sur les éléments critiques
- Déterminer l'existence de vulnérabilités sur les systèmes critiques
- Voir quand un nouvel exploit sort
- Favoriser une réponse rapide pour résoudre un ensemble particulier de vulnérabilités

Effort de rattrapage (RE)

Les efforts de rattrapage sont créés par les gestionnaires de vulnérabilités lorsqu'ils déterminent qu'il est temps pour le service informatique de corriger les vulnérabilités répertoriées dans une rubrique de visualisation. Les gestionnaires de vulnérabilité et les analystes peuvent choisir la façon dont ils souhaitent créer les tâches de rattrapage, par groupe d'affectation et par vulnérabilité, par exemple. Les tâches de rattrapage sont contenues dans l'effort de rattrapage.

Tâche de rattrapage (VUL)

Les équipes informatiques utilisent des tâches de rattrapage pour corriger les vulnérabilités qui leur sont affectées par la sécurité. Les tâches de rattrapage sont des listes des actions requises

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pour corriger les vulnérabilités. Les tâches de rattrapage sont créées automatiquement lorsque les gestionnaires de sécurité créent des efforts de rattrapage.

Développement des espaces de travail

Dans les versions précédentes de Réponse aux vulnérabilités, vous aviez deux options pour surveiller un ensemble d'enregistrements (VIT, AVIT, CVIT ou CTR) en tant qu'analyste de la sécurité et des vulnérabilités :

- Tableau de bord Vue d'ensemble, qui résume tous les VI
- Tâches de rattrapage

Les éléments vulnérables ont été triés automatiquement en tâches de rattrapage en fonction de vos règles de tâche de rattrapage prédéfinies. Les tâches de rattrapage ont été conçues pour aider les équipes informatiques à corriger les blocs gérables d'éléments vulnérables.

Cette automatisation a permis de regrouper automatiquement un très grand nombre d'enregistrements pour l'affectation et la correction en bloc. Cependant, les analystes et les responsables des vulnérabilités ont trouvé difficile de surveiller l'ensemble des enregistrements des tâches de remédiation. Outre les problèmes de performances avec de grands groupes, il peut être difficile de créer des règles de tâche de rattrapage fonctionnelles qui filtrent uniquement les vulnérabilités que vous trouvez les plus critiques.

Les Réponse aux vulnérabilités espaces de travail :

- Aidez les gestionnaires de sécurité à filtrer, surveiller les VI actifs et les résultats des tests au fil du temps, et à corriger les vulnérabilités qu'ils jugent les plus importantes.
- Fournissez aux équipes informatiques des informations centrées sur l'informatique en un seul endroit qu'elles peuvent utiliser pour corriger les vulnérabilités qui leur sont affectées par la sécurité.

Mises à jour des tâches de rattrapage dans les espaces de travail

Dans l'espace de travail du gestionnaire de vulnérabilité, les analystes et les gestionnaires de vulnérabilité utilisent les *rubriques de surveillance* et les *efforts de rattrapage* comme deux nouvelles méthodes pour surveiller et affecter des VI à des fins de correction.

Les groupes de vulnérabilité sont renommés *Tâches de rattrapage*. Ce changement s'applique aux étiquettes des listes, des enregistrements et des règles dans l'interface utilisateur héritée et dans les espaces de travail. Les tâches de rattrapage sont configurées de manière à ce que les équipes informatiques puissent travailler avec elles dans l'espace de travail de rattrapage informatique. La liste suivante illustre comment, en tant que gestionnaire de vulnérabilité ou analyste de vulnérabilité, vous pouvez surveiller les vulnérabilités et les résultats des tests, les filtrer et les affecter :

1. Dans l'espace de travail du gestionnaire de vulnérabilités, les gestionnaires surveillent les vulnérabilités importées et les erreurs de configuration sur les rubriques de visualisation. Les gestionnaires et les analystes utilisent des rubriques de surveillance pour surveiller un ensemble dynamique d'enregistrements filtrés au fil du temps qu'ils jugent les plus critiques.
2. Grâce aux rubriques de visualisation, les responsables de la sécurité peuvent déterminer quand et quel type d'éléments vulnérables transmettre aux équipes informatiques dans le cadre des efforts de rattrapage. Ces RE sont des listes statiques des éléments vulnérables que la sécurité souhaite que les équipes informatiques corrigent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À partir des efforts de rattrapage, les gestionnaires disposent de quatre options pour regrouper les enregistrements en tâches de remédiation (VUL, AVUL, CVUL ou CRG). Les tâches de rattrapage sont automatiquement affectées aux équipes informatiques en fonction des groupes d'affectation initialement associés aux enregistrements.

3. Les équipes informatiques travaillent sur les tâches de rattrapage dans l'espace de travail Rattrapage informatique sans avoir à trier tous les enregistrements.

   Une tâche de rattrapage passe par les mêmes états que dans les versions précédentes de Réponse aux vulnérabilités. Lorsque tous les enregistrements d'une tâche de rattrapage sont fermés, la tâche de rattrapage est fermée et définie sur **Inactif**.

   La progression du rattrapage est mise à jour sur les visualisations de données dans les rubriques de surveillance et sur la page d'accueil du rattrapage informatique.

Mises à jour des règles de tâche de rattrapage dans les espaces de travail

Les règles de groupe de vulnérabilité sont appelées *règles de tâche de rattrapage*. Cette modification s'applique aux étiquettes des listes, des enregistrements et des règles dans l'interface utilisateur héritée et dans les espaces de travail.

Les noms de table, par exemple [sn_vul_m2m_vul_group_item], ne sont pas modifiés.

Si vous avez créé des règles de groupes de vulnérabilité dans une version précédente de , elles sont toujours disponibles étiquetées comme règles de tâche de Réponse aux vulnérabilités rattrapage.

Toutefois, dans les espaces de travail, les règles de tâche de rattrapage ne sont plus utilisées comme méthode principale pour organiser un grand volume d'enregistrements en tâches de rattrapage. Vous préférez peut-être laisser vos règles de tâche de rattrapage inactives pendant que vous vous habituez aux espaces de travail.

Vous préférerez peut-être plutôt commencer à utiliser progressivement les Réponse aux vulnérabilités espaces de travail.

1. Si vous effectuez une mise à niveau à partir d'une version précédente de votre tâche de Réponse aux vulnérabilités rattrapage existante, les règles sont conservées. Ils sont toujours à votre disposition dans les espaces de travail. La règle de groupe par défaut, Vulnérabilité, est inactive par défaut.
2. Configurez des règles d'affectation et, si vous le souhaitez, des règles de risque, puis effectuez une importation.
3. En tant que gestionnaire ou analyste des vulnérabilités, vous pouvez choisir des segments à surveiller à partir des rubriques de surveillance de l'espace de travail du gestionnaire de vulnérabilités. Vous pouvez utiliser les rubriques de visualisation en tant que fonctionnalités autonomes. Sélectionnez un sous-ensemble d'enregistrements et utilisez le tableau de bord dessus pour surveiller les tendances. Avec eux, vous pouvez décider où et quand concentrer les efforts de rattrapage.
4. En tant que gestionnaire ou analyste des vulnérabilités, vous créez des efforts de rattrapage à partir de rubriques de surveillance lorsque vous décidez qu'il est temps de corriger un sous-ensemble d'enregistrements. Une tâche de rattrapage est également créée automatiquement et transmise au service informatique lorsque vous créez un effort de rattrapage.
5. Au fil du temps, en tant que gestionnaire ou analyste de vulnérabilité, vous pouvez découvrir des schémas de routine que vous pouvez gérer automatiquement avec les règles de tâches de remédiation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour afficher vos règles de tâche de rattrapage, accédez aux modules des **règles de tâche de rattrapage** respectifs dans , Réponse aux vulnérabilités des applicationsRéponse aux vulnérabilités pour conteneurs et Conformité de la configuration à Réponse aux vulnérabilités partir du menu **Tout**.

En savoir plus sur les règles d'affectation, les règles de tâche de rattrapage, les efforts de rattrapage et les éléments vulnérables dans les Réponse aux vulnérabilités espaces de travail

- Les enregistrements de tâches de rattrapage sont affichés sur des listes et des enregistrements dans l'environnement classique et dans les espaces de travail.
- Une tâche de rattrapage passe par les mêmes états qu'un groupe de vulnérabilité. Lorsque tous les enregistrements d'une tâche de rattrapage sont fermés, la tâche de rattrapage passe à l'état Inactif.
- Pour aider vos équipes à effectuer un rattrapage, un élément vulnérable ne peut faire l'objet que d'un seul effort de rattrapage. Une fois qu'il est dans un effort de rattrapage, un élément vulnérable n'est ajouté à aucun autre effort de rattrapage que vous créez.
- Si vous supprimez un effort de rattrapage, celui-ci devient inactif et tous les VI actifs sont disponibles pour de nouveaux efforts de rattrapage.
- Un enregistrement (VIT, AVIT, CVIT ou CTR) peut se trouver dans plusieurs tâches de rattrapage.
- Les tâches de rattrapage sont affectées automatiquement aux équipes informatiques en fonction du groupe d'affectation associé à un élément vulnérable dans un effort de rattrapage. Si vous créez une tâche de rattrapage sur demande, vous sélectionnez le groupe d'affectation.
- Si vous effectuez une mise à niveau à partir d'une version précédente de , vos règles d'affectation Réponse aux vulnérabilités ont été conservées dans l'interface utilisateur héritée.
- Si vous effectuez une mise à niveau à partir d'une version précédente de , vos utilisateurs et groupes actuels sont hérités et vous y ont accès dans les espaces de Réponse aux vulnérabilités travail.

Pour plus d'informations sur les cycles de vie des efforts de rattrapage, reportez-vous à la section Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Réponse aux vulnérabilités.

Configuration et configuration pour les Réponse aux vulnérabilités espaces de travail

Pour plus d'informations sur les règles d'affectation et les règles de tâche de rattrapage, reportez-vous aux sections Configurer les Réponse aux vulnérabilités espaces de travail et Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation.

Si vous êtes un nouveau client et que vous ne l'avez pas déjà ajouté, vous devez configurer les utilisateurs et les groupes de sorte que les éléments vulnérables et les tâches de rattrapage soient affectés aux groupes de rattrapage souhaités. Les règles d'affectation de Réponse aux vulnérabilités sont utilisées pour affecter le travail à des groupes.

Configurer les Réponse aux vulnérabilités espaces de travail

Avant de pouvoir utiliser les espaces de travail, confirmez que vous avez terminé les tâches de configuration suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin pour affecter des rôles aux utilisateurs et aux groupes, et les utilisateurs aux groupes.

sn_vul.vulnerability_admin pour la modification, la création de règles et la configuration de l'application Réponse aux vulnérabilités .

Confirmez que vous avez terminé les tâches de configuration suivantes. Consultez les étapes qui suivent la liste pour en savoir plus sur la façon d'effectuer ces tâches.

Tâche	Description
☐	Si ce n'est pas déjà fait, affectez les rôles appropriés aux utilisateurs et aux groupes afin qu'ils aient accès aux espaces de travail. Rôle requis : admin. Consultez les étapes ci-dessous pour plus d'informations.
☐	Configurez des règles d'affectation afin que les éléments vulnérables soient affectés aux groupes appropriés pour le rattrapage. Rôle requis : sn_vul.vulnerability_admin. Pour plus d'informations sur les règles d'affectation, reportez-vous à Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Vous créez et modifiez des règles d'affectation dans l'environnement classique.
☐	(Facultatif) : modifiez ou créez vos règles de tâche de rattrapage. Rôle requis : sn_vul.vulnerability_admin. **Remarque :** D'un point de vue fonctionnel, les règles de tâche de rattrapage fonctionnent comme les règles de tâche de rattrapage dans les versions précédentes de Réponse aux vulnérabilités. Toutefois, contrairement aux groupes de vulnérabilité qui ont été créés automatiquement à partir de vos règles de tâche de rattrapage, les tâches de rattrapage sont créées lorsque vous créez des efforts de rattrapage. Vous disposez des options suivantes pour regrouper les éléments vulnérables dans un effort de rattrapage en tâches de rattrapage : • Par groupe d'affectation • Par groupe d'affectation et élément de configuration • Par groupe d'affectation et vulnérabilité • Aucun : utilisez cette option si vous souhaitez ajouter manuellement des VI à une tâche de rattrapage. Consultez Créer une tâche de rattrapage sur demande à partir de Effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités pour plus d'informations. Pour plus d'informations sur la façon dont les VI sont automatiquement regroupés et comment les règles de groupe sont réappliquées dans l'environnement classique, reportez-vous à la section Réponse aux

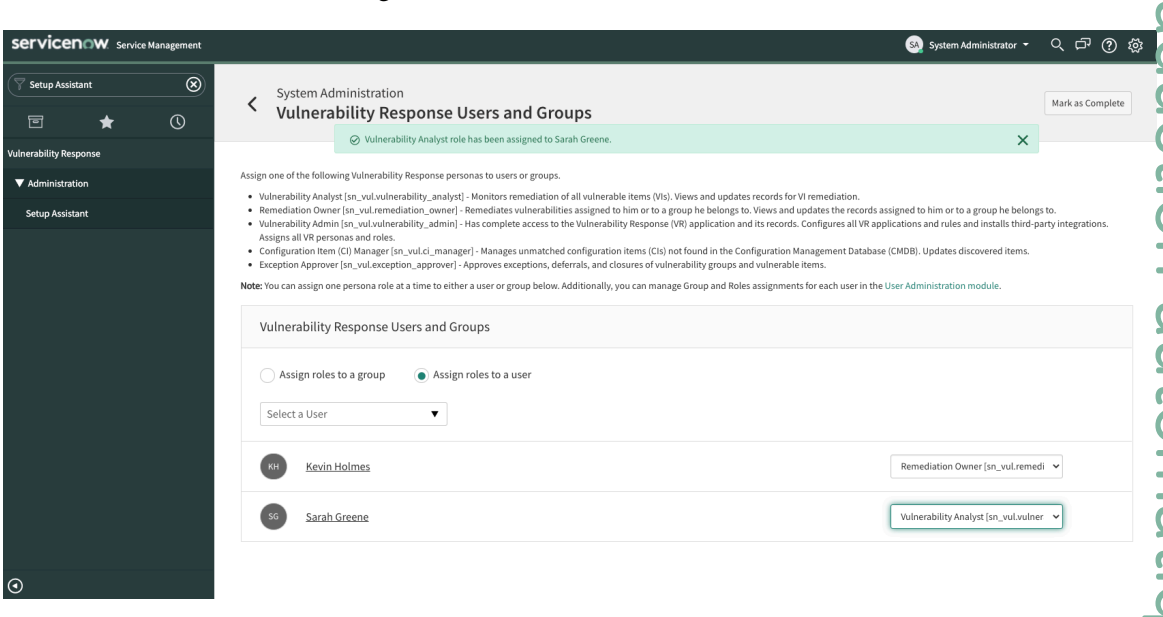
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	vulnérabilités Vue d'ensemble des tâches de rattrapage et des règles de tâche de rattrapage.
☐	Modifiez les règles de cibles de rattrapage. Rôle requis : sn_vul.vulnerability_admin. Ajoutez des règles de cibles de rattrapage dans l'environnement classique. Pour plus d'informations sur les règles de cibles de rattrapage, reportez-vous à la section Créer ou modifier Réponse aux vulnérabilités des règles de cibles de rattrapage.

Procédure

1. Après avoir installé et activé l'application Réponse aux vulnérabilités , dans l'environnement classique en tant qu'utilisateur disposant du rôle administrateur, accédez à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Assistant de configuration**.



2. Dans l'Assistant de configuration, affectez des utilisateurs aux groupes suivants.

> **Remarque :** 1 000 est la limite du nombre de groupes d'utilisateurs auxquels un utilisateur peut être affecté dans les espaces de travail Réponse aux vulnérabilités.

Les groupes suivants sont fournis avec l'application Réponse aux vulnérabilités et sont utilisés dans les espaces de travail. Vous pouvez leur affecter des utilisateurs dans l'assistant de configuration :

- Propriétaire de rattrapage : ce groupe est destiné aux propriétaires de rattrapage informatique dans l'espace de travail de rattrapage informatique. Les utilisateurs disposant de ce rôle corrigent les vulnérabilités qui leur sont affectées dans les tâches de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Si vous souhaitez que vos propriétaires de rattrapage créent et visualisent les demandes de changement ainsi que les données d'éléments de configuration (CI) vulnérables dans l'espace de travail Rattrapage informatique et dans l'environnement classique, affectez-leur le rôle itil. Vous préférez peut-être affecter le rôle itil à des utilisateurs individuels plutôt qu'à tous les membres d'un groupe. Le rôle cmdb_read est également une option permettant aux utilisateurs d'afficher les données CI dans les espaces de travail.

- À partir de la version 16.1, vous pouvez configurer des rappels par e-mail à l'intention de vos propriétaires de services de rattrapage informatique. Pour configurer des notifications par e-mail vers les espaces de travail, reportez-vous à la section Configurer des notifications par e-mail dans les Réponse aux vulnérabilités espaces de travail.
- Administrateur de vulnérabilité : ce groupe est destiné aux gestionnaires de vulnérabilité. Ce rôle configure l'application Réponse aux vulnérabilités dans l'assistant de configuration. Ce rôle a également l'autorisation de traiter les demandes d'exception et de faux positifs.
- Analyste de vulnérabilité : ce groupe est destiné aux gestionnaires de sécurité, aux gestionnaires de vulnérabilité et aux analystes dans l'espace de travail du gestionnaire de vulnérabilité. Ce rôle surveille les vulnérabilités, crée des rubriques de surveillance et des efforts de rattrapage, et surveille la progression du rattrapage.
- Approbateur de faux positif : les utilisateurs de ce groupe traitent les demandes de faux positif pour les éléments vulnérables ou les tâches de rattrapage. Une demande de faux positif nécessite un processus d'approbation à un seul niveau. Vous pouvez gérer l'affectation d'utilisateurs à ce groupe en dehors de l'assistant de configuration dans **l'administration utilisateur**.
- Approbateur d'exception : une demande d'exception pour un élément vulnérable ou une tâche de rattrapage est approuvée à l'aide d'un workflow d'approbation par défaut à deux niveaux. La demande d'exception nécessite deux niveaux d'approbateurs. Ajoutez des utilisateurs aux deux groupes d'approbation : Approbateur d'exception - Niveau 1 et Approbateur d'exception - Niveau 2. Une fois que la demande est approuvée par l'approbateur de niveau 1, elle est envoyée à l'approbateur de deuxième niveau. Vous gérez l'affectation d'utilisateurs à ce groupe en dehors de l'assistant de configuration dans **l'administration utilisateurs**.

Remarque : Ajoutez des utilisateurs aux groupes d'approbation avant de soumettre des demandes de faux positifs et d'exception. Si vous créez des demandes avant d'affecter des utilisateurs avec une autorisation d'approbation, les demandes peuvent ne pas être visibles par eux.

Vous pouvez également cliquer sur le lien **Administration utilisateurs** pour gérer et affecter les rôles granulaires suivants à vos utilisateurs et groupes existants. Ces rôles permettent aux utilisateurs d'effectuer des actions spécifiques au sein de l'application Réponse aux vulnérabilités et des espaces de travail.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- Pour créer et afficher des demandes de changement dans l'espace de travail Rattrapage informatique et dans l'environnement classique, affectez-leur le rôle itil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consultez Réponse aux vulnérabilités Profils et rôles granulaires et Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration pour plus d'informations sur l'affectation de rôles de profil aux utilisateurs et d'utilisateurs à des groupes.

3. Les tâches de rattrapage sont automatiquement transférées aux groupes d'affectation de rattrapage informatique pour traitement lorsqu'elles sont créées.
   - Par groupe d'affectation
   - Par groupe d'affectation et élément de configuration
   - Par groupe d'affectation et vulnérabilité
   - Aucun : utilisez cette option si vous souhaitez ajouter manuellement des VI à une tâche de rattrapage.

   Remarque : Pour la version 18.0 de Réponse aux vulnérabilités, l'option **Aucun** n'est disponible.

   Si vous effectuez une mise à niveau à partir d'une version précédente de , vos groupes d'affectation Réponse aux vulnérabilités sont conservés. Toutefois, vous préférerez peut-être modifier ces groupes afin que les éléments vulnérables soient associés à des groupes d'affectation spécifiques jusqu'à ce que vous vous habituiez au fonctionnement des rubriques de surveillance et des efforts de rattrapage. Par exemple, vous pouvez créer des groupes d'affectation par produit ou par région, mais vous pouvez utiliser n'importe quel critère qui convient le mieux à votre organisation.

   Vous pouvez également utiliser des règles d'affectation pour affecter des tâches de rattrapage à des groupes. Vous préférez peut-être exécuter uniquement des règles de priorité élevée pour les éléments suivants :
   - Éléments nécessitant une gestion spéciale
   - Éléments pour lesquels le risque est critique ou un VI nécessite une gestion par la conformité réglementaire

   Les règles d'affectation suivantes fournies avec l'application sont actives par défaut :
   - Règle d'affectation de CI mise hors service
   - Affecter au groupe de support CI
   - Règle d'affectation de la station de travail
   - Règle d'affectation de la base de données
   - Règle d'affectation d'application Web
   - Règle d'affectation Windows Server
   - Règle d'affectation non-Windows Server
   - Règle d'affectation Contact de secours

   Pour plus d'informations sur les règles d'affectation, reportez-vous à Réponse aux vulnérabilités Vue d'ensemble des règles d'affectation. Vous créez et modifiez des règles d'affectation dans l'environnement classique.

4. **Facultatif :** Modifiez ou créez vos règles de tâche de rattrapage.

   (Optional) Dans les espaces de travail, les tâches de rattrapage sont créées lorsque vous créez des efforts de rattrapage. Vous disposez des options suivantes pour regrouper les éléments vulnérables dans un effort de rattrapage en tâches de rattrapage :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Par groupe d’affectation
- Par groupe d’affectation et élément de configuration
- Par groupe d’affectation et vulnérabilité
- Aucun : utilisez cette option si vous souhaitez ajouter manuellement des VI à une tâche de rattrapage. Consultez Créer une tâche de rattrapage sur demande à partir de Effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités pour plus d'informations.

> **Remarque :** Dans la version 18.0 de Réponse aux vulnérabilités, l’option **Aucun** n’est disponible.

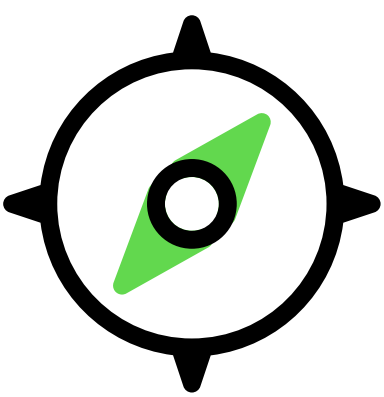
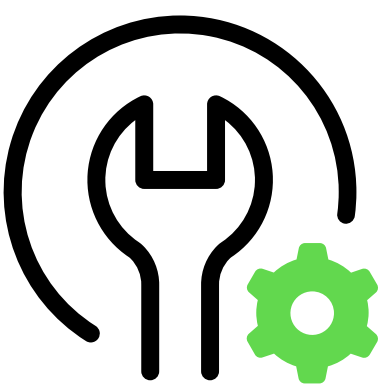
Pour plus d’informations sur la façon dont les VI sont automatiquement regroupés et comment les règles de groupe sont réappliquées dans l’environnement classique, reportez-vous à la section Réponse aux vulnérabilités Vue d’ensemble des tâches de rattrapage et des règles de tâche de rattrapage.

Espace de travail du gestionnaire de vulnérabilités

Cela Espace de travail du gestionnaire de vulnérabilités permet aux gestionnaires et aux analystes de surveiller les vulnérabilités et les erreurs de configuration qui les intéressent le plus et de décider stratégiquement des vulnérabilités qu’ils envoient aux équipes informatiques pour correction.

Démo d’Espace de travail du gestionnaire de vulnérabilité v18.0

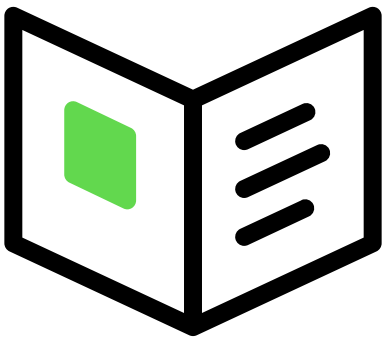
Premiers pas

Explorer	Surveiller et gérer	Corriger
		
En savoir plus sur les fonctionnalités de la Espace de travail du gestionnaire de vulnérabilités	Apprenez à surveiller et à gérer les éléments vulnérables (VIT, AVIT et CVIT) et les résultats des tests dans le Espace de travail du gestionnaire de vulnérabilités	Découvrez comment corriger les éléments vulnérables (VIT, AVIT et CVIT) et tester les résultats dans le Espace de travail du gestionnaire de vulnérabilités

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Référence



En savoir plus sur les informations supplémentaires requises pour utiliser le Espace de travail du gestionnaire de vulnérabilités

Dépannage et demande d'aide

- Security Operations sur ServiceNow Community
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Exploration de l'Espace de travail du gestionnaire de vulnérabilités

En tant que gestionnaire et analyste des vulnérabilités, obtenez une vue unifiée de tous les types de vulnérabilités dans le Espace de travail du gestionnaire de vulnérabilités. Vous pouvez afficher les vulnérabilités et les problèmes de configuration de l'hôte, de l'application et du conteneur, créer des rubriques de surveillance pour ces vulnérabilités et erreurs de configuration, créer des efforts de rattrapage et des tâches de rattrapage.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

Vous pouvez afficher les Espace de travail du gestionnaire de vulnérabilités en accédant à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.

Le Espace de travail du gestionnaire de vulnérabilités se compose des pages suivantes :

Page d'accueil

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Se compose de filtres prédéfinis qui sont utilisés pour visualiser le résumé des vulnérabilités d'hôte, d'application, de conteneur et des résultats des tests de configuration.

Pour en savoir plus sur la page d'accueil, reportez-vous à Page d'accueil dans Espace de travail du gestionnaire de vulnérabilités.

Remarque : À partir de la version 21.0 de Réponse aux vulnérabilités, les rubriques de visualisation apparaissent sur la page Rubriques de visualisation.

Page Rubriques de surveillance

Il s'agit d'une liste de rubriques de visualisation, classées en quatre modules : vulnérabilités d'hôte, vulnérabilités d'application, vulnérabilités de conteneur et résultats des tests de configuration.

Pour plus d'informations sur les rubriques relatives à la montre, reportez-vous à la section Page Rubriques de surveillance dans le Espace de travail du gestionnaire de vulnérabilités.

Page Tableaux de bord

Se compose des tableaux de bord Gestion des vulnérabilités, Gestion des vulnérabilités (PA), Approbations de vulnérabilité, CISO, Vue d'ensemble de la gestion de la vulnérabilité du conteneur, Gestion de la vulnérabilité des applications, Réponse aux vulnérabilités unifiée et Intégrité.

Pour plus d'informations, consultez Page Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités.

Remarque : La page Tableaux de bord apparaît à partir de la version 19.0 de Réponse aux vulnérabilités.

Page de liste

Se compose des pages de liste par défaut et personnalisées pour les efforts de rattrapage, les tâches de rattrapage, les éléments vulnérables d'hôte, les éléments vulnérables d'applications, les éléments vulnérables de conteneur, les résultats des tests de configuration, les exceptions, les approbations et les bibliothèques.

Pour plus d'informations, consultez Page de liste dans Espace de travail du gestionnaire de vulnérabilités.

Page d'accueil dans Espace de travail du gestionnaire de vulnérabilités

La page Espace de travail du gestionnaire de vulnérabilités d'accueil fournit un résumé des enregistrements actifs en présentant des visualisations de la cote de risque, de la progression du rattrapage, des affectations à des groupes d'affectation, des enregistrements dans les tâches de rattrapage et des vulnérabilités des ressources dans le cloud.

Sur la page d'accueil, vous pouvez afficher les visualisations des éléments vulnérables d'hôte préfiltrés, des éléments vulnérables de conteneur, des éléments vulnérables d'applications et des résultats des tests de configuration. Vous pouvez également afficher des visualisations pour un ensemble d'enregistrements souhaités en créant et en appliquant des filtres. Pour plus d'informations sur la création, la mise à jour, l'application et la suppression de filtres, reportez-vous à la section Créer et appliquer des filtres pour le résumé des enregistrements actifs (VIT, AVIT, CVIT et CTR).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conseil :

Si l'administrateur définit la *sn_vul_cmn_ws.navigate_to_workspace* propriété système sur true , lors de la sélection des liens de filtre prédéfinis dans les modules Éléments vulnérables, Éléments vulnérables de l'application, Éléments vulnérables de conteneurs et Résultats des tests dans le menu **Tous** , ces liens s'ouvrent dans la page d'accueil de avec la Espace de travail du gestionnaire de vulnérabilités sélection automatique du filtre enregistré correspondant.

Par exemple, si vous sélectionnez **Risque élevé** en accédant à **Tous** > **Réponse aux vulnérabilités** > **Éléments vulnérables**, ce lien est redirigé vers la page d'accueil du Espace de travail du gestionnaire de vulnérabilités avec sélection automatique du filtre **Risque élevé** dans l'onglet Vulnérabilités de l'hôte.

Sur la page d'accueil, vous pouvez effectuer les opérations suivantes :

- Explorez les données et affichez la liste des enregistrements en cliquant sur les visualisations.
- Accédez à la liste des enregistrements actifs dans l'interface utilisateur classique en sélectionnant le lien **Afficher la liste classique** .
- Ouvrez la liste des enregistrements actifs dans le Espace de travail du gestionnaire de vulnérabilités en sélectionnant le nombre d'enregistrements actifs en regard de la liste **déroulante Afficher par** .
- Mettez à jour les visualisations en sélectionnant l'icône **Actualiser le filtre enregistré sélectionné** .
- Affichez les dernières informations en sélectionnant l'option **Actualiser** dans le menu à trois points d'un widget.

Vulnérabilités d'hôte

L'onglet **Vulnérabilités de l'hôte** contient des visualisations qui fournissent un résumé global des vulnérabilités de l'hôte actif.

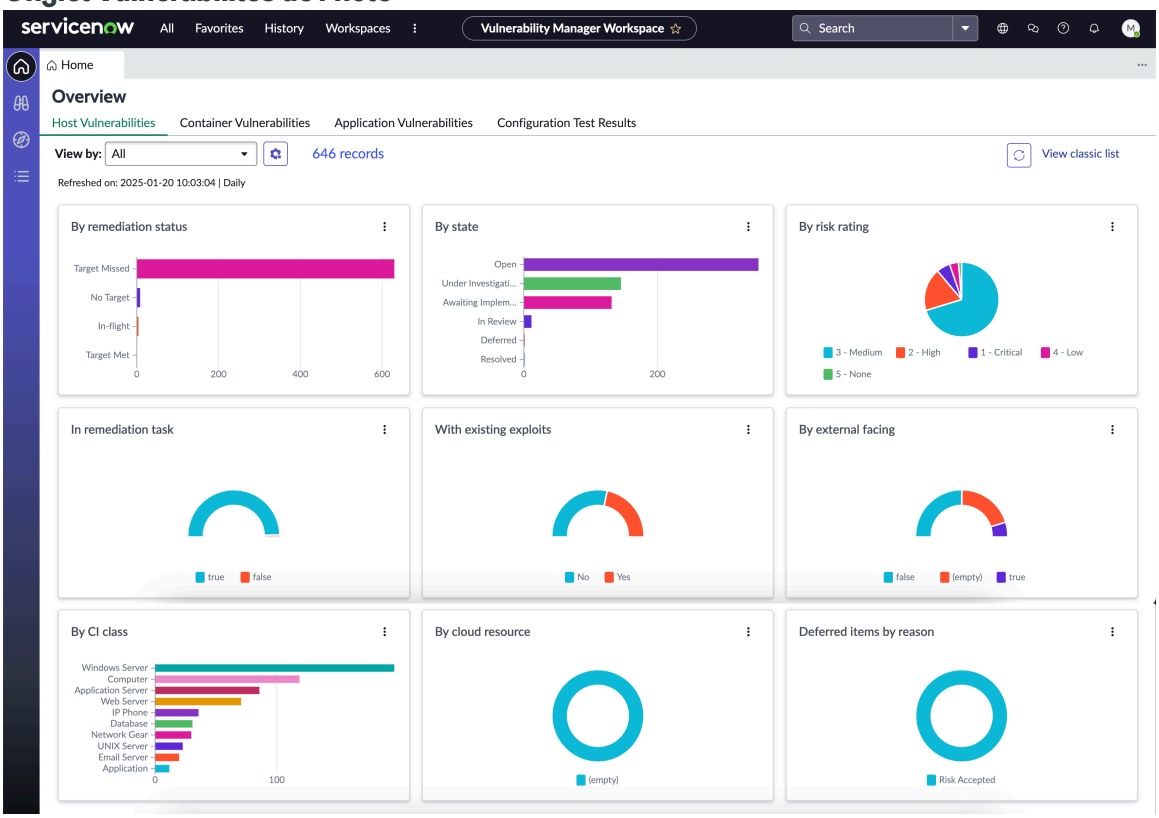
Rôles requis :

- sn_vul.vulnerability_analyst et sn_vul.vulnerability_admin pour afficher les visualisations en appliquant des filtres et créer des filtres.
- sn_vul.read_all rôle granulaire permettant d'afficher les visualisations en appliquant des filtres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vulnérabilités de l'hôte



Le tableau suivant décrit les visualisations de l'onglet Vulnérabilités de l'hôte de la page d'accueil. Sélectionnez ces visualisations pour obtenir la liste des enregistrements correspondants.

Visualisations dans l'onglet Vulnérabilités de l'hôte de la page d'accueil

Visualisation	Type	Description
Par groupe d'affectation et état de rattrapage	Barre de distribution	Enregistrements actifs affectés à divers groupes d'affectation regroupés par état de rattrapage.
Par état	À barres	Enregistrements actifs classés par différents états (Ouvert, En cours d'examen, En attente d'implémentation, En cours de révision, Résolu et Différé).
Par cote de risque	Graphique à secteurs	Enregistrements actifs classés par cote de risque (1 - Critique, 2 - Élevé, 3 - Moyen, 4 - Faible et 5 - Aucun)
Dans une tâche de remédiation	Anneau en demi-cercle	Enregistrements actifs qui font partie ou non de la tâche de rattrapage.
Avec exploits existants	Anneau en demi-cercle	Enregistrements actifs avec et sans exploits connus.
Par orientation vers l'extérieur	Anneau en demi-cercle	Enregistrements actifs classés par exposition des actifs à Internet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations dans l'onglet Vulnérabilités de l'hôte de la page d'accueil (suite)

Visualisation	Type	Description
Par classe CI	À barres	Enregistrements actifs classés par classes CI.
Par ressource de cloud	Couronne	Enregistrements actifs classés par diverses ressources dans le cloud.
Éléments différés par motif	Couronne	Enregistrements différés actifs regroupés par motif.

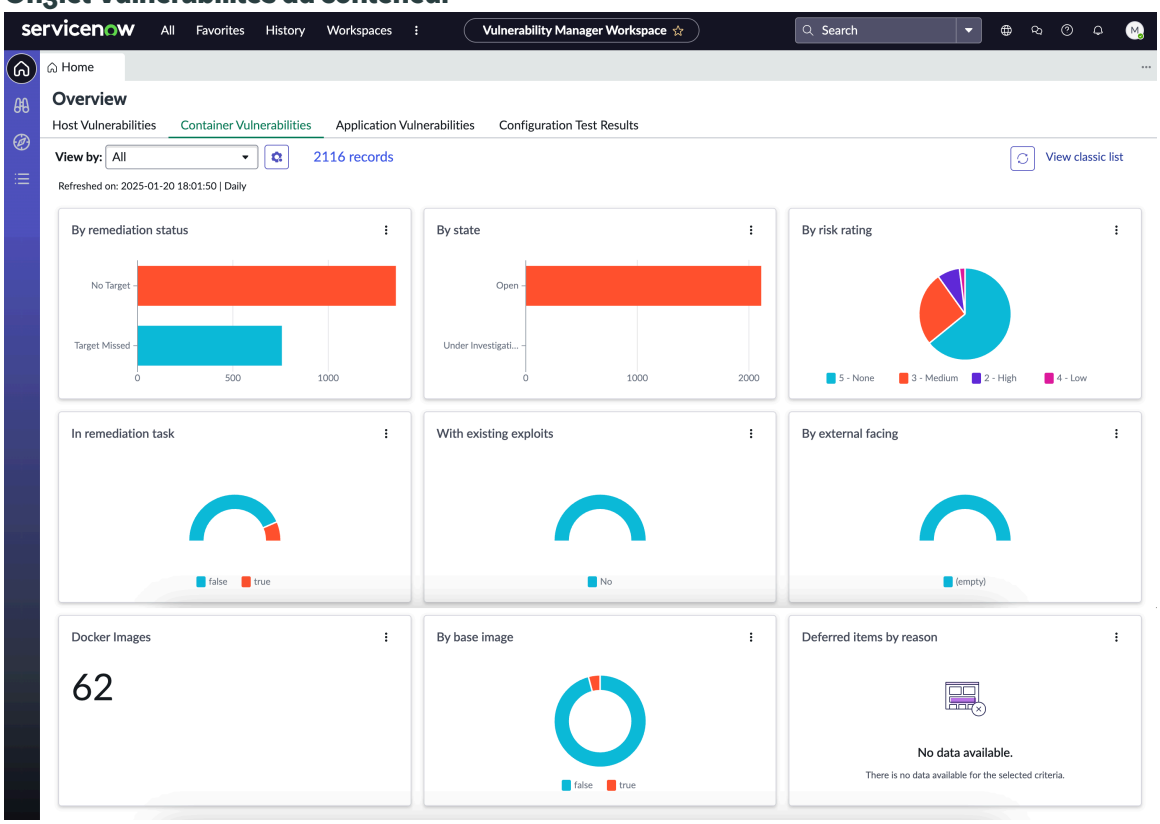
Vulnérabilités du conteneur

L'onglet **Vulnérabilités du conteneur** contient des visualisations qui fournissent un résumé global des éléments vulnérables actifs du conteneur.

Rôles requis :

- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour afficher les visualisations en appliquant des filtres et créer des filtres.
- sn_vul_container.read_all pour afficher les visualisations en appliquant des filtres.

Onglet Vulnérabilités du conteneur



Le tableau suivant décrit les visualisations de l'onglet Vulnérabilités de l'hôte de la page d'accueil. Sélectionnez ces visualisations pour obtenir la liste des enregistrements correspondants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations dans l'onglet Vulnérabilités du conteneur de la page d'accueil

Visualisation	Type	Description
Par groupe d'affectation et état de rattrapage	Barre de distribution	Enregistrements actifs affectés à divers groupes d'affectation regroupés par état de rattrapage.
Par état	À barres	Enregistrements actifs classés par différents états (Ouvert, En cours d'examen, En attente d'implémentation, En cours de révision, Résolu et Différé).
Par cote de risque	Graphique à secteurs	Enregistrements actifs classés par cote de risque (1 - Critique, 2 - Élevé, 3 - Moyen, 4 - Faible et 5 - Aucun)
Dans une tâche de remédiation	Anneau en demi-cercle	Enregistrements actifs qui font partie ou non de la tâche de rattrapage.
Avec exploits existants	Anneau en demi-cercle	Enregistrements actifs avec et sans exploits connus.
Par orientation vers l'extérieur	Anneau en demi-cercle	Enregistrements actifs classés par l'exposition des actifs à Internet.
Images de Docker	Nombre	Nombre d'images Docker uniques.
Par image de base	Couronne	Enregistrements actifs classés par type d'image.
Éléments différés par motif	Couronne	Enregistrements différés actifs regroupés par motif.

Vulnérabilités d'applications

L'onglet **Vulnérabilités de l'application** contient des visualisations qui fournissent un résumé global des vulnérabilités de l'application.

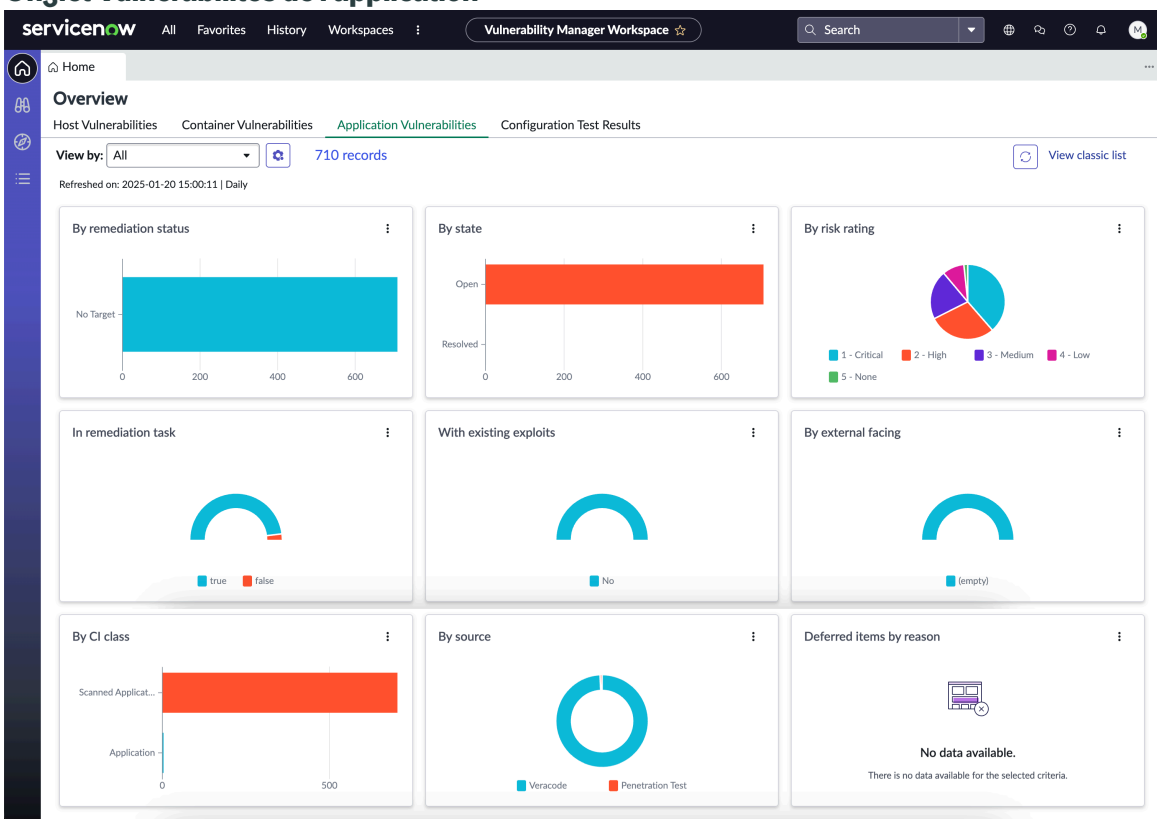
Rôles requis :

- sn_vul.app_sec_manager pour afficher les visualisations en appliquant des filtres et créer des filtres.
- sn_vul.app_read_all rôle granulaire permettant d'afficher les visualisations en appliquant des filtres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vulnérabilités de l'application



Le tableau suivant décrit les visualisations de l'onglet Vulnérabilités de l'hôte de la page d'accueil. Sélectionnez ces visualisations pour obtenir la liste des enregistrements correspondants.

Visualisations dans l'onglet Vulnérabilités de l'application de la page d'accueil

Visualisation	Type	Description
Par groupe d'affectation et état de rattrapage	Barre de distribution	Enregistrements actifs affectés à divers groupes d'affectation regroupés par état de rattrapage.
Par état	À barres	Enregistrements actifs classés par différents états (Ouvert, En cours d'examen, En attente d'implémentation, En cours de révision, Résolu et Différé).
Par cote de risque	Graphique à secteurs	Enregistrements actifs classés par cote de risque (1 - Critique, 2 - Élevé, 3 - Moyen, 4 - Faible et 5 - Aucun)
Dans une tâche de remédiation	Anneau en demi-cercle	Enregistrements actifs qui font partie ou non de la tâche de rattrapage.
Avec exploits existants	Anneau en demi-cercle	Enregistrements actifs avec et sans exploits connus.
Par orientation vers l'extérieur	Anneau en demi-cercle	Enregistrements actifs classés par exposition des actifs à Internet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations dans l'onglet Vulnérabilités de l'application de la page d'accueil (suite)

Visualisation	Type	Description
Par classe CI	À barres	Enregistrements actifs classés par classes CI.
Par ressource de cloud	Couronne	Enregistrements actifs classés par diverses ressources dans le cloud.
Éléments différés par motif	Couronne	Enregistrements différés actifs regroupés par motif.

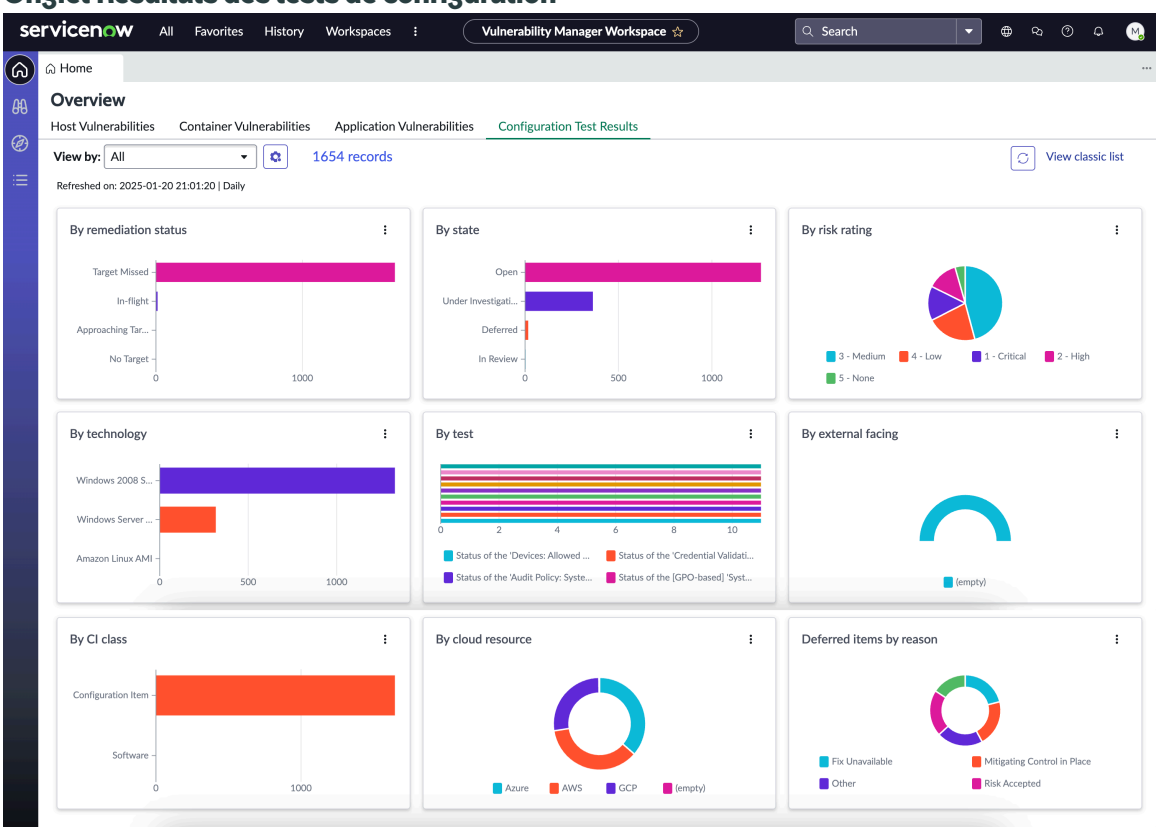
Résultats des tests de configuration

L'onglet **Résultats des tests de configuration** contient des visualisations qui fournissent un résumé global des erreurs de configuration actives des actifs de votre organisation.

Rôles requis :

- sn_vulc.admin pour afficher les visualisations en appliquant des filtres et créer des filtres.
- sn_vulc.Rôle granulaire Read pour afficher les visualisations en appliquant des filtres.

Onglet Résultats des tests de configuration



Le tableau suivant décrit les visualisations de l'onglet Résultats des tests de configuration de la page d'accueil. Sélectionnez ces visualisations pour obtenir la liste des enregistrements correspondants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations dans l'onglet Résultats des tests de configuration de la page d'accueil

Visualisation		Description
Par groupe d'affectation et état de rattrapage	Barre de distribution	Enregistrements actifs affectés à divers groupes d'affectation regroupés par état de rattrapage.
Par état	À barres	Enregistrements actifs classés par différents états (Ouvert, En cours d'examen, En attente d'implémentation, En cours de révision, Résolu et Différé).
Par cote de risque	Graphique à secteurs	Enregistrements actifs classés par cote de risque (1 - Critique, 2 - Élevé, 3 - Moyen, 4 - Faible et 5 - Aucun)
Par technologie	À barres	Enregistrements actifs classés par technologie.
Par test	À barres	Enregistrements actifs classés par tests.
Par orientation vers l'extérieur	Anneau en demi-cercle	Enregistrements actifs classés par exposition des actifs à Internet.
Par classe CI	À barres	Enregistrements actifs classés par classes CI.
Par ressource de cloud	Couronne	Enregistrements actifs classés par diverses ressources dans le cloud.
Éléments différés par motif	Couronne	Enregistrements différés actifs regroupés par motif.

Page Rubriques de surveillance dans le Espace de travail du gestionnaire de vulnérabilités

La page Rubriques de visualisation de vous Espace de travail du gestionnaire de vulnérabilités permet de créer et de modifier une rubrique de visualisation. Une *rubrique de surveillance* est un ensemble de visualisations de données qui vous permet de surveiller un ensemble filtré d'enregistrements (VIT, AVIT, CVIT et CTR) au fil du temps sur un tableau de bord susceptible d'intéresser ou de traiter en priorité votre organisation.

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Les données affichées sur les visualisations de données des rubriques de surveillance sont mises à jour dynamiquement à mesure que les données de vulnérabilité changent lors de l'importation. Utilisez les tableaux de bord pour surveiller les tendances, le champ d'application et les types de vulnérabilités, ainsi que vos éléments de configuration pour la rubrique de surveillance sélectionnée. Ces informations vous aident à déterminer l'impact des vulnérabilités de chaque rubrique de surveillance sur votre environnement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La page Rubriques de surveillance se compose de quatre modules : vulnérabilités d'hôte, vulnérabilités de conteneur, vulnérabilités d'application, résultats des tests de configuration et inactifs. Pour plus d'informations sur les onglets d'éléments connexes et leur visualisation dans une rubrique de visualisation, reportez-vous à la section Liste et visualisations d'éléments connexes dans une rubrique de surveillance.

Les rubriques de visualisation suivantes sont fournies avec le système de base dans le module Vulnérabilités de l'hôte sur la page Rubriques de surveillance :

- Vulnérabilités sur les actifs orientés vers l'extérieur
- Vulnérabilités avec exploits disponibles
- Vulnérabilités sur les serveurs Windows
- Vulnérabilités sur les serveurs LINUX
- Vulnérabilités critiques en retard
- Vulnérabilités critiques ne faisant pas partie des tâches de remédiation

Remarque : Si une visualisation de données montre qu'il n'existe aucun enregistrement pour cette catégorie, mais que vous pouvez voir une liste d'enregistrements lorsque vous cliquez sur l'icône de graphique, cochez la colonne avec le nom de la rubrique de surveillance sur la liste qui s'affiche. Vérifiez que la valeur de tous les enregistrements répertoriés dans la colonne de la rubrique de surveillance (par exemple, accessible sur Internet) est définie sur faux. Cette valeur dans cet exemple indique qu'il n'existe aucun enregistrement orienté vers Internet pour cette rubrique de visualisation.

Pour démarrer le rattrapage ou lorsqu'un besoin critique se fait sentir pour les enregistrements qui se trouvent dans une rubrique de visualisation, vous pouvez créer un *effort de rattrapage* à partir d'une rubrique de visualisation. Pour plus d'informations, consultez Créer un effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités.

Information associée

Liste et visualisations d'éléments connexes dans une rubrique de surveillance

Utiliser des rubriques de visualisation dans le Espace de travail du gestionnaire de vulnérabilités

Créer une rubrique de surveillance dans le Espace de travail du gestionnaire de vulnérabilités

Modifier ou supprimer une rubrique de surveillance dans Espace de travail du gestionnaire de vulnérabilités

Désactiver ou activer une rubrique de surveillance

Liste et visualisations d'éléments connexes dans une rubrique de surveillance

Sur la page Rubriques de visualisation de , vous pouvez créer des rubriques de visualisation classées en quatre modules : Vulnérabilités d'hôte, Vulnérabilités de conteneur, Vulnérabilités d'application et Résultats des Espace de travail du gestionnaire de vulnérabilités tests de configuration. Les onglets d'éléments connexes d'une rubrique de surveillance diffèrent pour chaque module.

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le volet de navigation de la page Rubriques de visualisation contient les modules suivants :

- Vulnérabilités de l'hôte : affiche les rubriques de surveillance qui incluent les éléments vulnérables de l'hôte.
- Vulnérabilités du conteneur : affiche les rubriques de surveillance qui incluent les éléments vulnérables du conteneur.
- Vulnérabilités d'applications : affiche les rubriques de visualisation qui incluent les éléments vulnérables de l'application.
- Résultats des tests de configuration : affiche les rubriques de visualisation qui incluent les éléments de configuration.
- Inactif : affiche les rubriques de surveillance inactives des quatre modules.

Le tableau suivant présente les onglets d'éléments connexes disponibles pour différents modules de rubrique de surveillance :

Rubrique de surveillance et ses éléments connexes

Rubrique de surveillance	Onglets Éléments connexes
Vulnérabilités d'hôte	Vue d'ensemble, CI impactés, vulnérabilités distinctes et éléments vulnérables
Vulnérabilités du conteneur	Vue d'ensemble, CI impactés, vulnérabilités distinctes et éléments vulnérables
Vulnérabilités d'applications	Vue d'ensemble et éléments vulnérables
Résultats des tests de configuration	Vue d'ensemble, CI impactés, tests de configuration distincts et résultats des tests de configuration

Le tableau suivant fournit une description des éléments, onglets et visualisations connexes dans une rubrique de visualisation.

Onglets et visualisation d'éléments connexes dans une rubrique de surveillance

Onglet et visualisation des éléments connexes	Description
Vue d'ensemble	
Éléments vulnérables actifs au fil du temps	Nombre d'éléments vulnérables (VI) actifs au fil du temps. Vous pouvez surveiller les tendances à partir de ces données au cours des 30 derniers jours. Vous pouvez également filtrer les données à l'aide des filtres Catégorie d'actif.
VI dans des efforts de rattrapage	Nombre de VI actifs par rapport au nombre total de VI déjà dans les efforts de rattrapage actifs.
Efforts de rattrapage actifs	Liste des efforts de rattrapage actifs.
CI impactés	
CI distincts	Nombre d'éléments de configuration (CI) (actifs) impactés par ces vulnérabilités.
VI par classe de CI	Nombre d'éléments vulnérables (VI) pour chaque Base de données de gestion des configurations (CMDB) classe CI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglets et visualisation d'éléments connexes dans une rubrique de surveillance (suite)

Onglet et visualisation des éléments connexes	Description
	Remarque : Ce widget s'affiche uniquement pour les rubriques de surveillance dans le module Vulnérabilités de l'hôte, de l'application et du conteneur.
Problèmes de configuration par classe CI	Nombre de CI pour chaque Base de données de gestion des configurations (CMDB) classe CI. **Remarque :** Ce widget s'affiche uniquement pour les rubriques de surveillance dans le module Problèmes de configuration.
VI accessibles sur Internet	Nombre de VI actifs par rapport au nombre total de VI de vos actifs qui sont exposés à Internet. **Remarque :** Ce widget s'affiche uniquement pour les rubriques de surveillance dans le module Vulnérabilités de l'hôte, de l'application et du conteneur.
Problèmes de configuration accessibles sur Internet	Nombre de CI actifs par rapport au nombre total de CI de vos actifs qui sont exposés à Internet. **Remarque :** Ce widget s'affiche uniquement pour les rubriques de surveillance dans le module Problèmes de configuration.
Vulnérabilités distinctes	
VI avec exploits existants	Des VI actifs avec des exploits connus.
Vulnérabilités distinctes	Nombre de vulnérabilités individuelles distinctes associées à vos actifs. Les vulnérabilités distinctes peuvent être filtrées en fonction du type de problème.
Éléments vulnérables avec vulnérabilités PCI	Nombre d'actifs distincts individuels qui ont des VI actifs avec des vulnérabilités PCI (Payment Card Industry).
Éléments vulnérables	
Éléments vulnérables d'hôte	Liste de tous les éléments vulnérables d'hôte. Vous pouvez filtrer cette liste de sorte que seuls les enregistrements que vous voulez afficher sont affichés. **Remarque :** Cette liste s'affiche uniquement pour les rubriques de surveillance du module Vulnérabilités de l'hôte.
Éléments vulnérables de l'application	Liste de tous les éléments vulnérables de l'application. Vous pouvez filtrer cette liste de sorte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglets et visualisation d'éléments connexes dans une rubrique de surveillance (suite)

Onglet et visualisation des éléments connexes	Description
	que seuls les enregistrements que vous voulez afficher sont affichés. **Remarque :** Cette liste s'affiche uniquement pour les rubriques de surveillance du module Vulnérabilités de l'application.
Éléments vulnérables de conteneurs	Liste de tous les éléments vulnérables de conteneur. Vous pouvez filtrer cette liste à afficher afin que seuls les enregistrements que vous souhaitez afficher soient affichés. **Remarque :** Cette liste s'affiche uniquement pour les rubriques de surveillance dans le module Vulnérabilités du conteneur.
Onglet Vue d'ensemble dans une rubrique de surveillance sous le module Résultats des tests de configuration	
Résultats des tests de configuration actifs au fil du temps	Nombre de résultats des tests de configuration actifs dans le temps. Vous pouvez surveiller les tendances à partir de ces données au cours des 30 derniers jours.
Résultats des tests de configuration dans les efforts de rattrapage	Nombre de résultats de tests de configuration actifs par rapport au nombre total d'enregistrements qui font déjà l'objet d'efforts de rattrapage actifs.
Efforts de rattrapage actifs	Liste des efforts de rattrapage actifs.
Onglet Tests de configuration distincts dans une rubrique de surveillance sous le module Résultats des tests de configuration	
Résultats des tests de configuration via la criticité des tests	Résultats des tests de configuration basés sur la criticité des problèmes.
Tests de configuration distincts	Nombre de tests de configuration distincts.
Onglet Résultats des tests de configuration dans une rubrique de surveillance sous le module Résultats des tests de configuration	Liste des résultats des tests de configuration.

Vous pouvez obtenir les derniers détails d'une rubrique de surveillance en sélectionnant le bouton **Actualiser** . Le dernier état d'actualisation et l'horodatage sont affichés sous le nom de la rubrique de visualisation. Lorsque vous actualisez une rubrique de visualisation, tous les détails de la rubrique de visualisation, y compris les graphiques et les efforts de rattrapage sont mis à jour. Une rubrique de visualisation est actualisée automatiquement lorsqu'elle est créée ou mise à jour.

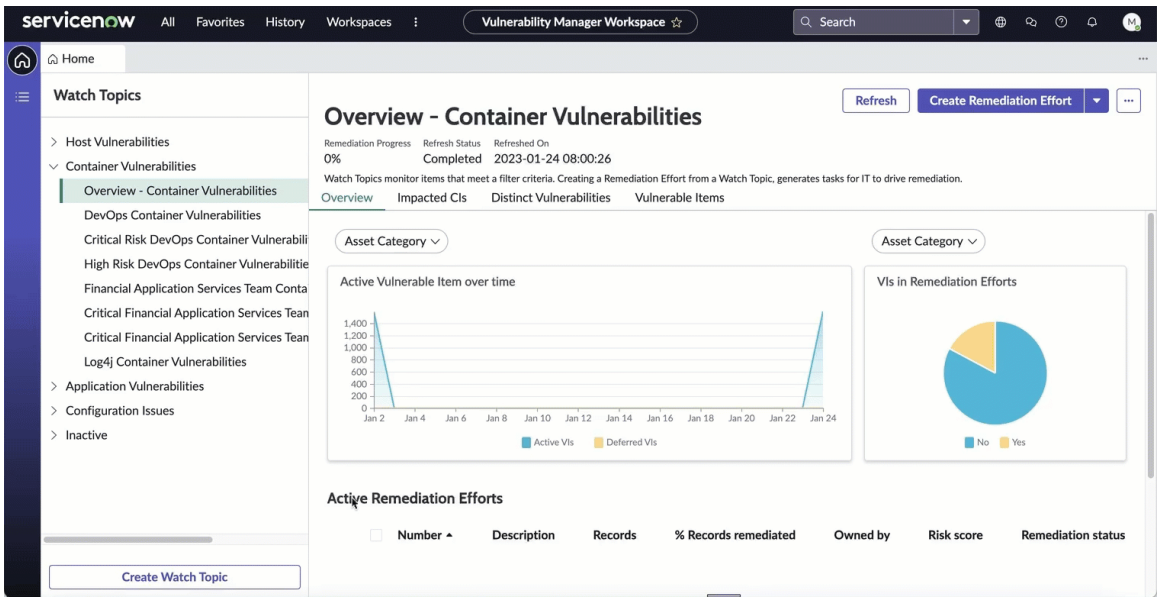
Remarque : Étant donné que vous ne pouvez pas actualiser une rubrique de visualisation inactive, le bouton **Actualiser** est inactif pour une rubrique de surveillance inactive.

Cliquez sur un tracé de données sur l'un des widgets pour afficher des informations supplémentaires sur les enregistrements.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example: Version 18.0 : visualisations de données dans une rubrique de surveillance



Efforts de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités

Un effort de rattrapage est un ensemble d'enregistrements associés à une rubrique de visualisation. Les enregistrements répertoriés dans un effort de rattrapage sont statiques. Elles ne sont pas mises à jour par les nouvelles données d'importation ou les modifications que vous apportez aux rubriques de visualisation.

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Avec **Actif** sélectionné dans la liste **Efforts de rattrapage** de la page Liste, cliquez sur un lien d'effort de rattrapage pour l'ouvrir. Pour classer les efforts de rattrapage en éléments vulnérables d'hôte (VIT), éléments vulnérables d'application (AVIT), éléments vulnérables de conteneurs (CVIT) et résultats des tests de configuration (CTR), sélectionnez le menu à trois points dans la colonne **Type d'enregistrement** , puis sélectionnez **Grouper par type d'enregistrement**.

Les éléments de liste connexes de l'enregistrement de l'effort de rattrapage vous permettent de visualiser la progression globale du rattrapage et l'état des enregistrements qui lui sont associés.

- Sous l'onglet **Vue d'ensemble** , surveillez les enregistrements associés à cet effort de rattrapage qui ont été fermés au fil du temps. À droite de l'enregistrement, cliquez sur l'icône de filtre sur le graphique pour afficher les filtres appliqués à la visualisation des données.
- Dans l'onglet **Détails** , affichez les détails de l'effort de rattrapage, y compris sa rubrique de surveillance associée et son état (actif ou inactif). Vous pouvez désactiver un effort de rattrapage à partir de cette page. Si vous désactivez l'effort de rattrapage avant que

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

tous les enregistrements ne soient fermés, tous les enregistrements actifs deviennent disponibles pour être ajoutés aux nouveaux efforts de rattrapage.

- Dans l'onglet **Tâches de rattrapage** , affichez les tâches de rattrapage associées à cet effort de rattrapage. Consultez le pourcentage des enregistrements associés à cette tâche qui sont corrigés.
- Dans l'onglet **Éléments vulnérables** , affichez les enregistrements associés à cet effort de rattrapage. Lorsque tous les enregistrements d'une tâche de rattrapage sont terminés et fermés, l'effort de rattrapage passe à Inactif. Lorsqu'un effort de rattrapage est inactif, tous les enregistrements fermés associés à l'effort de rattrapage ne sont pas disponibles pour être ajoutés aux nouveaux efforts de rattrapage.

  Remarque : L'onglet **Éléments vulnérables** s'affiche pour les efforts de rattrapage associés aux rubriques de surveillance dans les modules Vulnérabilités d'hôte, Vulnérabilités d'application et Vulnérabilités de conteneur.

- Dans l'onglet **Résultats des tests de configuration** , affichez les résultats des tests de configuration associés à l'effort de rattrapage. Lorsque tous les enregistrements d'une tâche de rattrapage sont terminés et fermés, l'effort de rattrapage passe à Inactif. Lorsqu'un effort de rattrapage est inactif, tous les enregistrements fermés associés à l'effort de rattrapage ne sont pas disponibles pour être ajoutés aux nouveaux efforts de rattrapage.

  Remarque : L'onglet **Résultats des tests de configuration** s'affiche pour les efforts de rattrapage associés aux rubriques de surveillance dans le module Résultats des tests de configuration.

Pour plus de détails et les actions d'interface utilisateur que vous pouvez effectuer à partir d'un effort de rattrapage, reportez-vous à la section Utiliser les enregistrements d'effort de rattrapage.

Information associée

Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Réponse aux vulnérabilités

Créer un effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités

Créer une tâche de rattrapage sur demande à partir de Effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités

Créer un effort de rattrapage récurrent dans le Espace de travail du gestionnaire de vulnérabilités

Transférer des enregistrements aux efforts de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités

Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Réponse aux vulnérabilités

Les états des enregistrements et leurs tâches de rattrapage (RT) associées sont impactés si les enregistrements sont différés, résolus, rouverts et transférés vers d'autres efforts de rattrapage (RE).

Rôles requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Création d'efforts de rattrapage

L'impact sur les états et les cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dépend de la façon dont un effort de rattrapage est créé, quand il est créé et s'il est désactivé.

Dans la liste en haut à droite d'une rubrique de visualisation, vous pouvez créer un effort de rattrapage en cliquant sur **Créer un effort de rattrapage** ou **Créer un effort récurrent**. Vous pouvez créer un effort de rattrapage récurrent par rubrique de visualisation. Si vous créez un effort de rattrapage récurrent, les efforts de rattrapage suivants pour la rubrique de surveillance associée sont créés automatiquement en fonction des critères que vous avez définis. Dans les deux cas :

- Pour faciliter le rattrapage, seuls les enregistrements actifs sont ajoutés aux efforts de rattrapage.
- Tous les enregistrements des nouveaux efforts de rattrapage sont placés dans les nouvelles tâches de rattrapage. Des enregistrements peuvent exister dans plusieurs tâches de rattrapage, mais un seul enregistrement peut être associé à un effort de rattrapage.

Remarque : Un effort de rattrapage est désactivé automatiquement lorsqu'il n'existe aucun enregistrement actif.

Transfert d'enregistrements ou transfert d'enregistrement

Vous pouvez transférer des enregistrements d'un effort de rattrapage à un autre lors de la création d'un effort de rattrapage en sélectionnant la case à cocher **Transférer les enregistrements correspondants à partir d'autres efforts de rattrapage actifs** . Pour en savoir plus sur le mode de transfert des enregistrements, reportez-vous à la section Transférer des enregistrements aux efforts de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités. Si les enregistrements sont transférés à partir d'un effort de rattrapage ou reportés dans des efforts de rattrapage récurrents :

Vers un nouvel effort de rattrapage dans la même rubrique de surveillance

- Toutes les tâches de rattrapage de l'ancien effort de rattrapage sont déplacées vers le nouvel effort de rattrapage.
- De nouvelles tâches de remédiation sont créées en fonction des critères de regroupement choisis pour les enregistrements qui ne faisaient auparavant partie d'aucune tâche de remédiation.
- L'ancien effort de rattrapage est désactivé.

Vers un nouvel effort de rattrapage dans une rubrique de surveillance différente

Tous les enregistrements de l'ancien effort de rattrapage sont déplacés vers le nouvel effort de rattrapage et les tâches de rattrapage sont créées en fonction des critères de regroupement choisis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si tous les enregistrements des tâches de rattrapage associées à l'ancien effort de rattrapage sont transférés, ces tâches de rattrapage sont fermées-annulées.
- Si seul un sous-ensemble d'enregistrements est transféré, les tâches de remédiation associées à l'ancien effort de remédiation sont divisées et restent actives.

Les tâches de rattrapage fermées associées à l'ancien effort de rattrapage ne sont pas affectées.

Remarque : Vous ne pouvez pas transférer les enregistrements d'efforts de rattrapage récurrents vers de nouveaux efforts de rattrapage. Toutefois, vous pouvez transférer des enregistrements d'efforts de rattrapage existants et non récurrents vers de nouveaux efforts de rattrapage. Pour en savoir plus sur le transfert d'enregistrements, reportez-vous Transférer des enregistrements aux efforts de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités à la section .

Page Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités

Sur la page Tableaux de bord de , Espace de travail du gestionnaire de vulnérabilités vous pouvez afficher les tableaux de bord de l'interface Next Experience utilisateur et utiliser ces tableaux de bord pour suivre et analyser les vulnérabilités.

Rôles requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Accéder aux tableaux de bord dans le Espace de travail du gestionnaire de vulnérabilités en accédant à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** et en sélectionnant l'icône **Tableaux de bord** . Le tableau de bord par défaut s'affiche en fonction de votre rôle.

La table suivante présente le tableau de bord par défaut qui s'affiche pour un rôle spécifique.

Tableau de bord par défaut

Tableau de bord par défaut	Rôle
Tableau de bord unifié	sn_vul_cmn_vulnerability_admin ou sn_vul_cmn_vulnerability_analyst
Tableau de bord de l'analyse des vulnérabilités	sn_vul_vulnerability_admin ou sn_vul_vulnerability_analyst
Vue d'ensemble de l'application	sn_vul_app_sec_manager
Vue d'ensemble du conteneur	sn_vul_container_vulnerability_admin ou sn_vul_container_analyst

Vous pouvez afficher les tableaux de bord suivants pour les tâches que vous souhaitez effectuer en les sélectionnant dans la liste déroulante de la page Tableaux de bord.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableaux de bord dans Espace de travail du gestionnaire de vulnérabilités

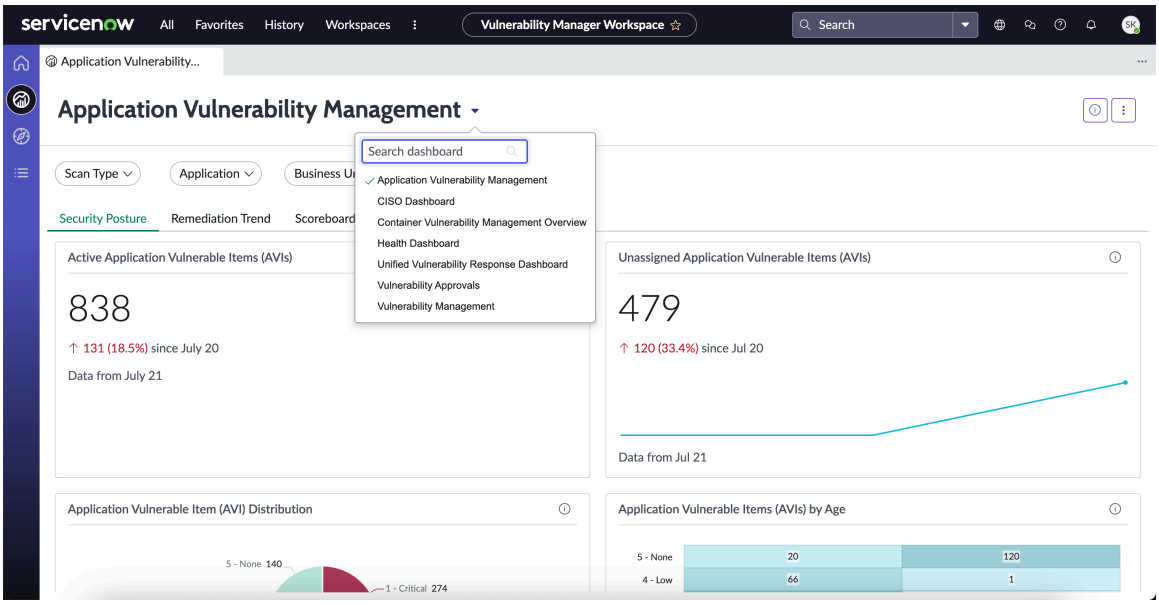
Tableau de bord	Description
Gestion de la vulnérabilité (PA)	Suivez le volume, les performances et la progression des vulnérabilités de l'hôte, de l'analyse initiale et de la détection au confinement ou à la correction. Pour plus d'informations, consultez Tableau de bord Gestion des vulnérabilités (PA).
Approbations de vulnérabilité	Affichez le nombre de demandes d'approbation approuvées, rejetées et en attente pour vous. Pour plus d'informations, consultez Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.
Tableau de bord des CISO	Révèle la posture de sécurité globale de votre organisation, y compris la vulnérabilité et les incidents de sécurité. Pour plus d'informations, consultez Tableau de bord Gestion des vulnérabilités des CISO.
Vue d'ensemble de la gestion de la vulnérabilité du conteneur	Suivez le volume, les performances et la progression des vulnérabilités des conteneurs, de l'analyse initiale et de la détection au confinement ou à la correction. Pour plus d'informations, consultez Tableau de bord de Réponse aux vulnérabilités pour conteneurs.
Tableau de bord de gestion de la vulnérabilité des applications	Suivez le volume, les performances et la progression des vulnérabilités des applications, de l'analyse initiale et de la détection au confinement ou à la correction. Pour plus d'informations, voir Gestion de la vulnérabilité des applications Tableau de bord (PA)
Tableau de bord de Vulnerability Response unifié	Fournit une visibilité à partir de plusieurs scanners de vulnérabilité et outils de sécurité pour fournir une vue complète des vulnérabilités et des risques d'une organisation. Pour plus d'informations, consultez Solutions d'analyse et de reporting pour le tableau de bord Vulnerability Response unifié.
Tableau de bord Intégrité de Vulnerability Response	Affiche le score d'intégrité global de l'application Vulnerability Response. Pour plus d'informations, consultez Tableau de bord Intégrité de SecOps Vulnerability Response.

L'image suivante montre la page Tableaux de bord dans le Espace de travail du gestionnaire de vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableaux de bord de la version 19.0 dans le Espace de travail du gestionnaire de vulnérabilités



Vous pouvez également créer un tableau de bord personnalisé en sélectionnant l'icône ⋮, puis Créer **un tableau de bord**.

Page de liste dans Espace de travail du gestionnaire de vulnérabilités

La page Liste de la Espace de travail du gestionnaire de vulnérabilités liste permet aux gestionnaires et analystes de vulnérabilité et de sécurité de voir la progression du rattrapage sur les enregistrements, d'explorer les enregistrements et d'afficher l'état de leurs demandes d'approbation et exceptions.

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Ces listes et liens vous permettent d'accéder facilement aux enregistrements et aux tâches. Il contient deux onglets :

- **Onglet Listes** : affiche les listes par défaut pour les efforts de rattrapage, les tâches de rattrapage, les éléments vulnérables, les résultats des tests de configuration, les solutions, les exceptions et les bibliothèques.
- **Onglet Mes listes** : affiche toutes les listes que vous avez renommées à partir de l'onglet Listes et toutes les listes que vous créez.

  Vous pouvez également créer votre propre liste pour surveiller la progression du rattrapage. Pour plus d'informations, consultez Créer une liste personnalisée des enregistrements.

Onglet Listes

Le tableau suivant présente les listes disponibles dans l'onglet Listes de la page Liste :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conseil :

Si la *sn_vul_cmn_ws.navigate_to_workspace* propriété système est définie sur vrai par un administrateur, lors de la sélection des liens de filtre prédéfinis dans les modules Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response et Configuration Compliance dans le menu **Tous** , ces liens s'ouvrent dans la page Liste en fonction de Espace de travail du gestionnaire de vulnérabilités votre rôle.

Par exemple, si vous sélectionnez **Affecté à mes groupes** en accédant à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**, ce lien est redirigé vers le Espace de travail du gestionnaire de vulnérabilités fichier . La liste **Affecté à mes groupes** du module Tâches de **remédiation** s'ouvre dans la page Liste de l'espace de travail du gestionnaire de vulnérabilité si vous avez le rôle d'administrateur ou d'analyste de vulnérabilité. Pour afficher les tâches de rattrapage de l'hôte, regroupez les tâches par type d'enregistrement.

Vous pouvez masquer le nombre d'enregistrements dans les listes à l'aide de la *glide.ui.list.seismic.omit.count* propriété système. Pour plus d'informations sur la façon de désactiver/d'activer le nombre d'enregistrements sur une liste, consultez l'article de la base de connaissances KBB0010402 .

Listes

Élément de liste	Description	Modules	Rôles requis
Efforts de rattrapage (RE)	Liste des ER actives et de toutes les ER affectées à vos groupes d'affectation. Regroupez les efforts de rattrapage par **type d'enregistrement** pour les classer par éléments vulnérables d'hôte, éléments vulnérables d'applications, éléments vulnérables de conteneurs et résultats des tests de configuration.	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.admin pour les résultats des tests de configuration (CTR)
Tâches de rattrapage	Contient les listes suivantes : • Actif : liste de toutes les tâches de rattrapage d'hôtes,	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	d'applications, de conteneurs et de résultats de tests actifs. • Tout : liste des tâches de rattrapage des hôtes, des applications, des conteneurs et des résultats des tests actifs et inactifs. • Mes affectations : liste des tâches de rattrapage qui vous sont affectées pour le rattrapage. • Affectés à mon groupe : tâches de rattrapage affectées à vos groupes d'affectation pour le rattrapage. Regroupez les tâches de rattrapage par **type d'enregistrement** pour les classer par éléments vulnérables d'hôte, éléments vulnérables d'application, éléments vulnérables de conteneurs et résultats des tests de configuration.	conteneurs, et Conformité de la configuration	• sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.admin pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	Remarque : La liste des tâches de rattrapage comprend les tâches générées lors de la création de l'effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités, ainsi que celles créées manuellement et par les règles de tâche de rattrapage et d'autres processus dans l'interface utilisateur classique. La colonne Effort de rattrapage est vide pour toutes les tâches de rattrapage qui n'ont pas été créées dans le cadre de l'effort de rattrapage.		
Éléments vulnérables d'hôte	Contient les listes suivantes • Actif : liste de tous les éléments vulnérables d'hôte actifs. • Tous : liste des éléments vulnérables de l'hôte actifs et inactifs. • Mes affectations : liste des éléments vulnérables d'hôte qui vous sont affectés pour correction. • Affecté à mon groupe : liste des éléments vulnérables	Réponse aux vulnérabilités	sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	d'hôte affectés à vos groupes d'affectation pour le rattrapage.		
Éléments vulnérables d'applications	Contient les listes suivantes : • Actif : liste de tous les éléments vulnérables actifs de l'application. • Tous : liste des éléments vulnérables de l'application actifs et inactifs. • Mes affectations : liste des éléments vulnérables d'applications qui vous sont affectés pour le rattrapage. • Affecté à mon groupe : liste des éléments vulnérables d'applications affectés à vos groupes d'affectation pour le rattrapage. Vous pouvez créer un nouvel élément vulnérable d'application en sélectionnant le bouton **Nouveau** .	Réponse aux vulnérabilités des applications	sn_vul.app_sec_manager
Éléments vulnérables de conteneurs	Contient les listes suivantes : • Actif : liste de tous les éléments vulnérables de conteneur actifs. • Tous : liste des éléments vulnérables de conteneurs actifs et inactifs.	Réponse aux vulnérabilités pour conteneurs	sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	• Affectés à moi : liste des éléments vulnérables de conteneurs qui vous sont affectés pour correction. • Affecté à mon groupe : liste des éléments vulnérables de conteneurs affectés à vos groupes d'affectation pour le rattrapage.		
Résultats des tests de configuration	Contient les listes suivantes : • Actif : liste de tous les résultats des tests actifs. • Tous : liste des résultats des tests actifs et inactifs. • Mes affectations : liste des résultats des tests qui vous sont affectés pour le rattrapage. • Affecté à mon groupe : liste des résultats des tests affectés à vos groupes d'affectation pour le rattrapage.	Conformité de la configuration	sn_vulc.admin
Solutions	Contient les listes suivantes : • Tout : affiche toutes les solutions disponibles que vous pouvez utiliser pour corriger les éléments vulnérables de l'hôte.	Réponse aux vulnérabilités	sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	• Priorité la plus élevée : affiche toutes les solutions utilisées pour renseigner les solutions préférées. • Avec éléments vulnérables : affiche les solutions qui sont utilisées en tant que solution préférée sur les éléments vulnérables.		
Exceptions	Affiche les états d'approbation de toutes les demandes d'exception et de faux positifs associées à vos groupes d'affectation. • Tout : liste des demandes d'approbation d'exception, de faux positif et de désaffectation liées aux VIT, AVIT et CVIT et à leurs tâches de rattrapage (VUL, AVUL et CVUL). • Tout (Conformité de la configuration) : liste des exceptions, des faux positifs et des demandes d'approbation non attribuées Résultats des tests et tâches de rattrapage (CTR#). Regroupez les exceptions par **type d'enregistrement**	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.admin pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	pour les classer par éléments vulnérables d'hôte, éléments vulnérables d'applications, éléments vulnérables de conteneurs et résultats des tests de configuration.		
Approbations	Affecté à moi : affiche les demandes d'approbation qui vous sont affectées pour traitement. Pour traiter vos approbations dans l'espace de travail, reportez-vous à la section Approuver ou rejeter les demandes dans le Espace de travail du gestionnaire de vulnérabilités.	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.admin pour les résultats des tests de configuration (CTR)
Bibliothèques	Comprend les listes suivantes : • CVE (NVD) : liste de toutes les vulnérabilités et expositions courantes (CVE) de Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications et Réponse aux vulnérabilités pour conteneurs. • TPE : liste des vulnérabilités tierces importées	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi pour les éléments vulnérables de conteneurs (CVIT)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	dans votre instance. Contient une liste des références, des éléments vulnérables, des exploits et des CVE connexes. • CWE : liste de toutes les énumérations de faiblesses courantes (CWE) de Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications et Réponse aux vulnérabilités pour conteneurs. • Vulnérabilités de l'application : liste de toutes les entrées de vulnérabilité de l'application tierce. • Groupes de tests : liste de tous les groupes de tests Conformité de la configuration . Vous pouvez afficher le pourcentage de conformité des CI et de conformité des résultats des tests pour un groupe de tests dans la vue d'enregistrement. • Tests : liste de tous les tests de .Conformité de la configuration Vous pouvez afficher le pourcentage de conformité des résultats des tests pour un		• sn_vulc.admin pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	test dans la vue d'enregistrement. • Contrôles compensatoires : liste de tous les contrôles compensatoires qui peuvent être utilisés pour les demandes de réduction des risques. Vous pouvez ajouter un contrôle de compensation en cliquant sur **Nouveau**. Pour plus d'informations sur l'ajout d'un contrôle de compensation, reportez-vous à la section Ajouter un contrôle de compensation à la bibliothèque.		
CMDB	Contient les listes suivantes • **Éléments détectés** : liste de tous les éléments détectés. • **Images du conteneur détectées** : liste des images du conteneur. Ces images de conteneur fournissent des informations sur l'ID d'image, l'image Docker et le référentiel d'images, ainsi que des informations sur la couche.	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.vulnerability_analy ou sn_vul_container.vulnerability_admi pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.admin pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	• **Table Applications détectées** ajoutée à la vue Espace de travail du gestionnaire de vulnérabilités. Permet de réappliquer sur les applications ou les éléments découverts sélectionnés ou filtrés dans l'espace de travail.		
Demandes d'évaluation de test de pénétration	Contient les listes suivantes : • **Actif** : liste des demandes d'évaluation de test de pénétration actives. • **Tout** : liste des demandes d'évaluation de test de pénétration actives et inactives • **Mes affectations** : Liste des demandes d'évaluation de test de pénétration que vous avez émises • **Affecté à mon groupe** : liste des demandes d'évaluation de test de pénétration émises par les utilisateurs de vos groupes d'affectation. Pour en savoir plus sur la création d'une demande d'évaluation de test de pénétration,	Réponse aux vulnérabilités des applications	sn_vul.app_sec_manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	reportez-vous à la section Créer une nouvelle demande d'évaluation de test de pénétration.		
Conclusions du test de pénétration	Contient les listes suivantes : • Actif : liste de tous les résultats actifs du test de pénétration. • Tous : liste des résultats du test de pénétration actifs et inactifs. • Affectés à moi : liste des conclusions du test de pénétration qui vous sont affectés pour correction. • Affecté à mon groupe : liste des conclusions du test de pénétration affectés à vos groupes d'affectation pour correction. Pour en savoir plus sur la création des conclusions d'un test de pénétration, reportez-vous à la section Créer les conclusions d'un test de pénétration basés sur un questionnaire d'évaluation.	Réponse aux vulnérabilités des applications	sn_vul.app_sec_manager
Correctifs	Tous : liste de tous les correctifs disponibles qui peuvent être utilisés pour corriger les éléments vulnérables de l'hôte.	Réponse aux vulnérabilités	sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin
Données associées	Contient les listes suivantes :	Conformité de la configuration	sn_vulc.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Modules	Rôles requis
	• **Sources faisant autorité** : Liste des sources faisant autorité qui fournissent des informations récapitulatives utiles pour rechercher les publications sources. • **Technologies** : liste des technologies qui fournissent les informations récapitulatives sur chaque source et citation faisant autorité (également appelée, dans Qualys, cadre de travail).		

Information associée

Utiliser la vue de liste dans le Espace de travail du gestionnaire de vulnérabilités

Modifier en bloc dans Espace de travail du gestionnaire de vulnérabilités

Dans , la Espace de travail du gestionnaire de vulnérabilités fonctionnalité de modification en bloc vous permet de mettre à jour simultanément plusieurs éléments vulnérables (VIT, AVIT ou CVIT) ou résultats des tests de configuration (TR), rationalisant ainsi le processus de gestion et de correction.

Avec la modification en bloc, vous pouvez sélectionner plusieurs vulnérabilités et appliquer des changements cohérents, tels que l'affectation de propriétaires de rattrapage, la mise à jour du statut, l'ajout de notes de travail, la demande d'exceptions et la demande de faux positif. Cela permet d'économiser du temps et des efforts en éliminant la nécessité de modifier individuellement les éléments vulnérables, favorisant ainsi une gestion efficace et cohérente des vulnérabilités.

La fonctionnalité de modification en bloc est disponible pour :

- éléments vulnérables d'hôte (VIT) à partir de la version 21.0 de Réponse aux vulnérabilités.
- éléments vulnérables de l'application (AVIT) et éléments vulnérables de conteneur (CVIT) à partir de la version 22.0 du Réponse aux vulnérabilités.
- résultats des tests (TR) à partir de la version 23.0 de Réponse aux vulnérabilités.

Rôles requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Vous pouvez effectuer les tâches suivantes à l'aide de la fonction de modification en bloc du :Espace de travail du gestionnaire de vulnérabilités

- Affecter des enregistrements à un groupe d'affectation en bloc
- Demander une exception en bloc dans l'espace de travail du gestionnaire de vulnérabilité
- Supprimer les affectations pour les éléments vulnérables d'hôte en bloc
- Modifier en bloc le faux positif dans l'espace de travail du gestionnaire de vulnérabilité
- Fermer les enregistrements en bloc dans le Espace de travail du gestionnaire de vulnérabilités

Comprendre les contrôles compensatoires pour la réduction des risques

Les contrôles compensatoires sont les mesures prises pour réduire le risque posé par les vulnérabilités qui ne peuvent pas être corrigées immédiatement. Elles peuvent être utilisées pour atténuer la probabilité ou l'impact d'un exploit réussi.

Remarque : La fonctionnalité de contrôles de compensation est disponible uniquement pour les vulnérabilités de l'hôte.

L'application de contrôles compensatoires peut aider à réduire le risque de vulnérabilité.

Le tableau suivant présente les cas d'utilisation des contrôles de compensation :

Cas d'utilisation pour les contrôles de compensation

Cas d'utilisation	Contrôle de compensation
Une vulnérabilité dans un serveur Web qui permet aux attaquants d'exécuter du code arbitraire.	Implémentez un pare-feu d'application Web (WAF) pour bloquer les demandes malveillantes au serveur Web.
Une vulnérabilité dans un système d'exploitation qui permet aux attaquants d'élever les privilèges à la racine.	Implémentez un contrôle d'application pour restreindre l'exécution d'applications sur le système hôte.
Une vulnérabilité dans un serveur de base de données qui permet aux attaquants d'accéder à des données sensibles.	Implémentez la segmentation du réseau pour isoler le serveur de base de données des autres hôtes et systèmes critiques.

Pour plus d'informations sur l'impact des contrôles compensatoires sur le score de risque d'un élément vulnérable et d'une tâche de rattrapage, reportez-vous à la section Impact des contrôles compensatoires sur le score de risque et la date d'expiration.

Information associée

Ajouter un contrôle de compensation à la bibliothèque

Associer des contrôles compensatoires à des CVE ou des TPE pour les demandes de réduction des risques

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Solutions d'analyse et de reporting pour le tableau de bord Vulnerability Response unifié

Le tableau de bord Vulnerability Response unifié est un tableau de bord agrégé centralisé qui fournit une visibilité à partir de plusieurs scanners de vulnérabilité et outils de sécurité pour fournir une vue complète des vulnérabilités et des risques d'une organisation.

Rôles requis

Les rôles et tâches suivants sont associés à cette solution. Ils sont requis pour afficher et partager les rapports :

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.analyste_vulnérabilité
- sn_vul.app_développeur
- sn_vulc.analyste_vulnérabilité

Tableau de bord de Vulnerability Response unifié

Le tableau de bord Unified Vulnerability Response fournit une vue complète des vulnérabilités et des risques d'une organisation. Les vulnérabilités liées à l'infrastructure, au cloud, aux applications et aux conteneurs peuvent être visualisées dans un tableau de bord centralisé pour une meilleure visibilité et une meilleure correction.

Regardez cette vidéo de quatre minutes pour en savoir plus sur le tableau de bord Vulnerability Response unifié.

https://player.vimeo.com/video/1046083623?h=74c3349c9c&badge=0&autopause=0&player_id=0&app_id=58479

Rôles ServiceNow AI Platform requis

Les rôles suivants sont associés à cette solution. Ils sont nécessaires pour afficher, modifier et partager les rapports :

- sn_vul.app_sec_manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_container.vulnerability_admin
- sn_vul_container.analyste_vulnérabilité
- sn_vul.app_développeur
- sn_vulc.analyste_vulnérabilité

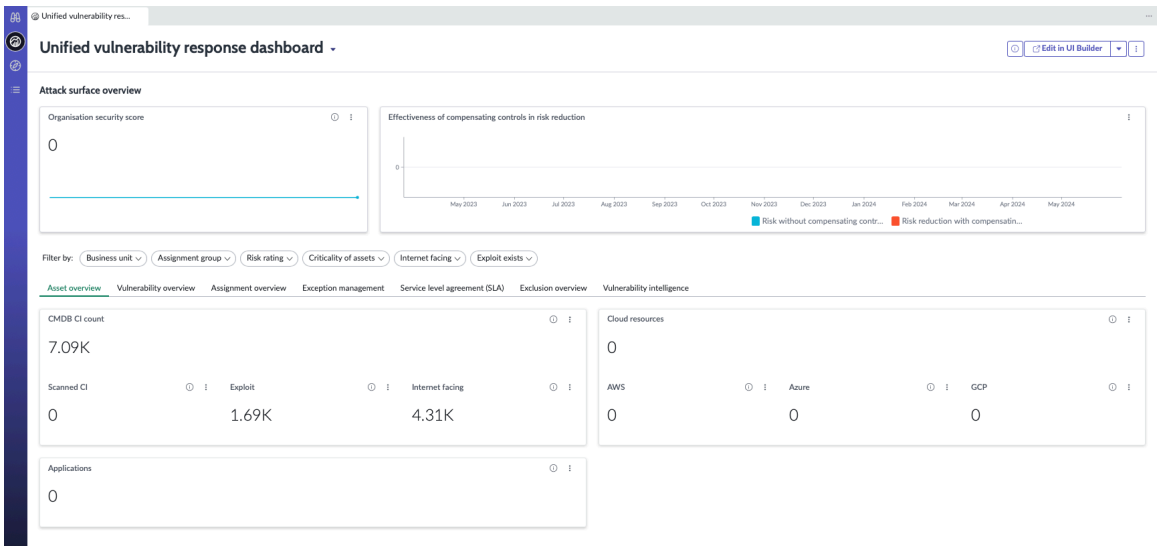
Accéder au tableau de bord de Vulnerability Response unifié

Pour ouvrir le tableau de bord, accédez à l'un des points suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Tous** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité** et sélectionnez l'icône **Tableaux de bord** . En fonction de votre rôle, le tableau de bord par défaut s'affiche. Pour afficher le tableau de bord Vulnerability Response unifié, sélectionnez la liste déroulante en regard du nom du tableau de bord.
- **Espaces de travail** > **Espace de travail d'analyse de plateforme** > **Tableaux de bord** > **Tableau de bord de Vulnerability Response unifié**.



Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateurs	Utilisation du tableau de bord
• Responsables des vulnérabilités • Analystes de vulnérabilité	• Fournit une visibilité en temps réel des risques présents dans l'infrastructure, les applications, les configurations et les conteneurs. Permet aux gestionnaires et aux analystes de vulnérabilité de classer les vulnérabilités par ordre de priorité et d'y remédier en temps opportun. • Fournit une vue d'ensemble de la surface d'attaque des actifs critiques, qui peut être utilisée pour suivre la progression et les efforts de rattrapage. • Fournit une vue d'ensemble des risques dans les unités business (BU). Vous pouvez utiliser des filtres pour sélectionner les BU et comparer la progression afin de réaffecter les ressources, le cas échéant. L'accès au niveau des rôles doit être fourni au chef de la BU. • Fournit une visibilité sur l'impact potentiel des BU. Vous pouvez utiliser le filtre CVE (Common Vulnerability and Exposure)

Traduction automatique

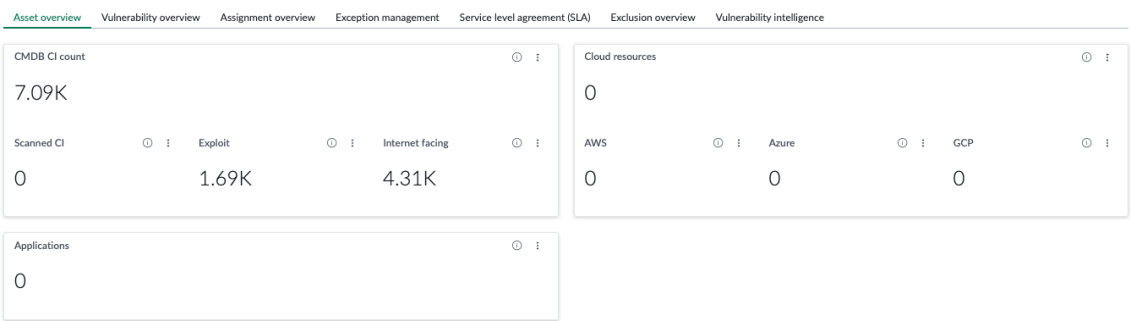
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs	Utilisation du tableau de bord
	pour identifier les expositions dans l'ensemble de l'organisation. • Fournit une visibilité sur les scores EPSS atteints par les entrées vulnérables qui existent dans le catalogue CISA KEV pour les éléments vulnérables d'application, d'hôte et de conteneur.

Onglets du tableau de bord de Vulnerability Response unifié

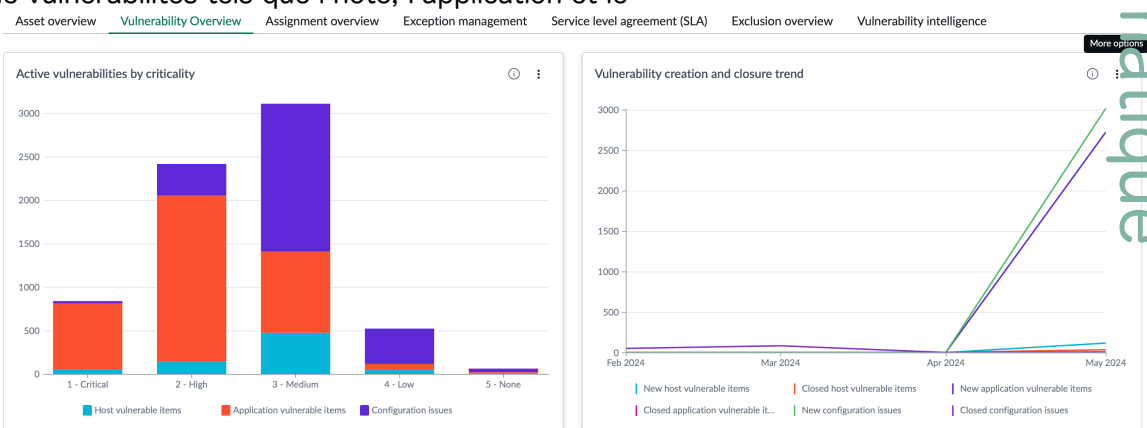
Ce tableau de bord vous permet de voir les vulnérabilités ou les problèmes présents dans les hôtes, le cloud, les configurations, les applications et les conteneurs. Vous pouvez afficher les vulnérabilités en fonction de l'unité business, du groupe d'affectation, de la cote de risque, de la criticité et de l'existence ou non d'un exploit pour ces vulnérabilités.

L'onglet **Vue d'ensemble des actifs** fournit l'état général des éléments de configuration (CI) dans le



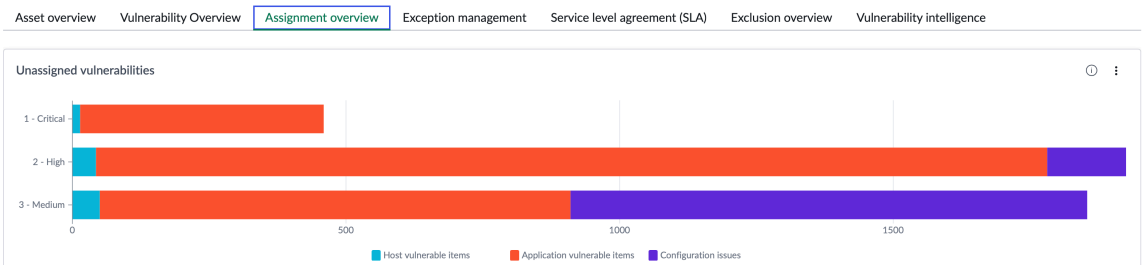
système.

L'onglet **Vue d'ensemble** de la vulnérabilité fournit un état sur les types de vulnérabilités tels que l'hôte, l'application et le



conteneur.

L'onglet **Vue d'ensemble de l'affectation** fournit un statut sur l'affectation des

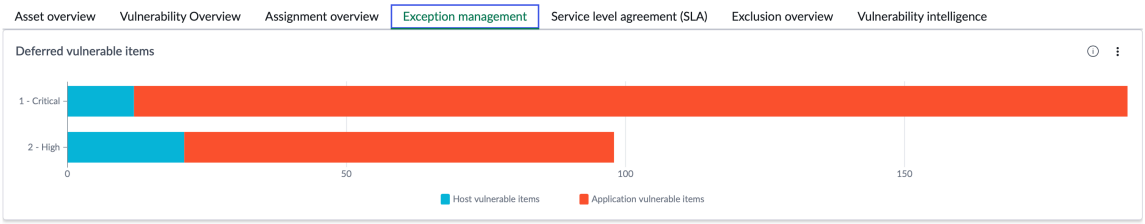


vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

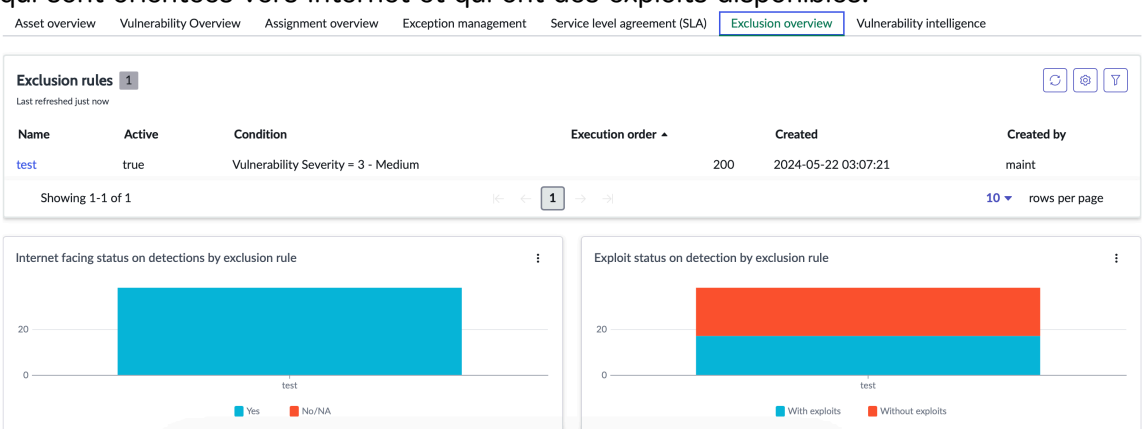
L’onglet **Gestion des exceptions** fournit un état sur les vulnérabilités différées.



L’onglet Accord sur les **niveaux de service (SLA)** fournit un état sur l’accord sur les niveaux de service conclu par différents groupes d’affectation.



L’onglet **Vue d’ensemble de l’exclusion** fournit un état des règles d’exclusion que vous avez créées, ainsi que celles qui affectent les détections qui sont orientées vers Internet et qui ont des exploits disponibles.

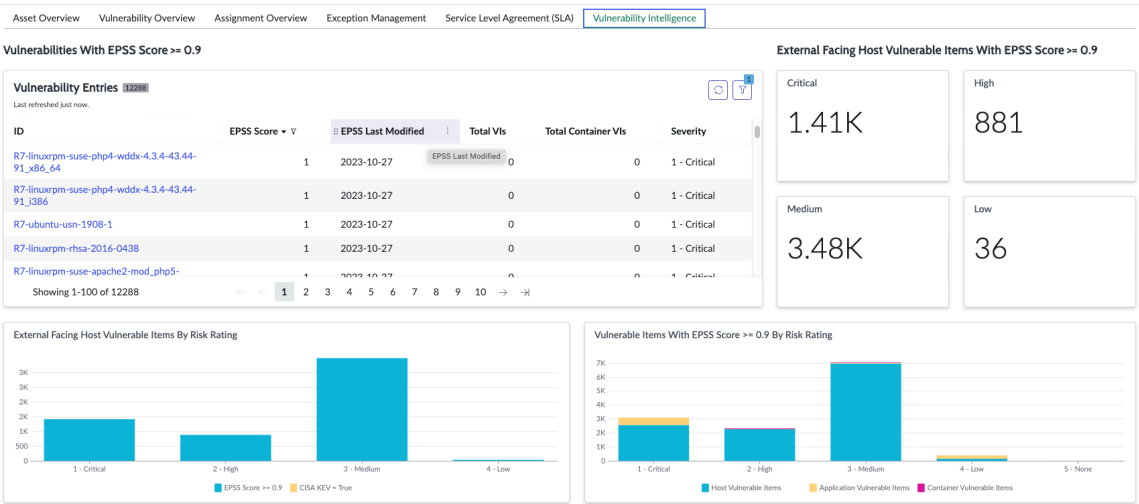


L’onglet Renseignements sur les **vulnérabilités** fournit un état des scores EPSS atteints par les vulnérabilités ayant le marqueur CISA KEV vrai et le score

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

EPSS >= 0,9 pour les éléments vulnérables de l’application, de l’hôte et du conteneur.



Filtres

Vous pouvez filtrer les widgets en fonction des éléments suivants :

- Unité business
- Groupe d'affectation
- Cote de risque
- État critiques des actifs
- Accessible sur Internet
- Existence de l'exploit

Lorsqu’un filtre est sélectionné, les données de tous les widgets sont mises à jour. Toutefois, si un filtre ne s’applique pas à un widget, un symbole de croix s’affiche à côté du nom du filtre.

Remarque : Seuls les filtres Unité business et Groupe d’affectation sont disponibles dans Tokyo. Tous les filtres sont disponibles à partir de Utah maintenant.

Indicateurs

Actifs analysés

Indicateur de formule pour les actifs analysés au cours des 60 derniers jours. Contient les actifs d’éléments détectés analysés, les actifs de mise en production d’applications analysés et les actifs d’image de conteneur détectés analysés comme indicateurs de contribution.

Actifs : l'exploit existe

Indicateur de formule pour les actifs où l’exploit existe dans les vulnérabilités. Contient les actifs de l’hôte : l’exploit existe, les actifs de l’application : l’exploit existe, les actifs du conteneur : l’exploit existe en tant qu’indicateurs de contribution.

Actif Infra : accessible sur Internet

Indicateur permettant d’extraire le nombre d’actifs qui sont accessibles sur Internet.

Éléments détectés basés sur le type de ressources dans le cloud

Indicateur permettant d’extraire le nombre d’actifs ayant une catégorie d’actifs telle que le cloud.

Images de base

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateur permettant d’extraire le nombre d’images de base.

Type d'actif CISA KEV

Indicateur de formule, qui donne le nombre d’éléments vulnérables de conteneurs et d’hôtes pour lesquels le marqueur CISA KEV (BOD 22-01) est défini sur vrai. Contient CISA existe CVR et CISA existe des éléments vulnérables en tant qu’indicateurs de contribution.

Éléments vulnérables existants CISA – Non affecté

Indicateur de formule, qui donne le nombre d’éléments vulnérables de conteneurs et d’hôtes lorsque le marqueur CISA KEV (BOD 22-01) est défini sur vrai et que les éléments vulnérables ne sont pas affectés. Contient les éléments vulnérables du conteneur non affectés et l’élément vulnérable de l’hôte non affecté comme indicateurs de contribution.

Éléments vulnérables existants CISA : cible manquée

Indicateur de formule, qui donne le nombre d’éléments vulnérables de conteneur et d’hôte lorsque le marqueur CISA KEV (BOD 22-01) est défini sur vrai et que les éléments vulnérables ont manqué la cible. Contient les éléments vulnérables existants CISA, CVR existant CISA comme indicateurs de contribution.

VIT d'hôtes actifs

Nombre d’éléments vulnérables de l’hôte (VIT) actifs.

VIT d'application actifs

Nombre d’éléments vulnérables de l’application (AVIT) actifs.

VIT de conteneurs actifs

Nombre d’éléments vulnérables de conteneurs actifs (CVIT).

Nouveaux VIT

Nombre de VIT ouverts sur une journée.

Nouveaux AVIT

Nombre d’AVIT qui ont ouvert un jour.

Nouveaux CVIT

Nombre de CVIT ouverts sur une journée.

Nouveaux résultats des tests

Nombre de résultats de tests (TR) qui ont été créés sur une journée.

AVIT fermés

Nombre de VIT fermés sur une journée.

VIT fermés

Nombre d’AVIT fermés sur une journée.

CVIT fermés

Nombre de CVIT fermés sur une journée.

Résultats des tests fermés

Nombre de résultats fermés sur une journée.

Problèmes de configuration ouverts : résultats des tests

Nombre de tous les résultats des tests ouverts, qui ont échoué.

Score de risque de l'organisation

Score de risque d’une organisation à partir de la table de score de risque de déploiement de l’application.

Élément vulnérable de l'application non affecté

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

AVIT sans groupe d’affectation ou affecté à.

Élément de vulnérabilité de l'hôte non affecté

VIT sans groupe d’affectation ni affecté à.

Éléments vulnérables du conteneur non affectés

CVIT sans groupe d’affectation ni affecté à.

Problèmes de configuration non affectés

TR sans groupe d’affectation ou affecté à.

VIT différés

VIT dans l’état différé.

AVIT différés

AVIT dans l’état différé.

CVIT différés

CVIT à l’état différé.

SLA hôte : fermé

Âge moyen de fermeture des VIT fermés.

SLA de l'application : fermé

Âge moyen fermé des AVIT fermés.

SLA de conteneur : fermé

Âge moyen fermé des CVIT fermés.

SLA de résultat de test : réussi

Âge moyen à la clôture des TR réussis.

SLA de l'hôte : fermé (critique et élevé)

Âge moyen à la fermeture des VIT critiques et élevées fermées.

SLA de l'application : fermé (critique et élevé)

Âge moyen à la fermeture des AVIT critiques et élevés.

SLA de conteneur : fermé (critique et élevé)

Âge moyen clôturé des CVIT critiques et élevées fermées.

SLA de résultat de test : réussi (critique et élevé)

Âge moyen clôturé des TR critiques et élevés réussis.

Regrouper MTTR

Âge moyen de fermeture des VIT, AVIT, CVIT et TR fermés.

SLA manqué

Âge moyen clôturé des VIT, AVIT, CVIT et TR fermés et manqués.

Vulnérabilités avec scores EPSS >= 0,9

Nombre d’entrées de vulnérabilité avec des scores EPSS supérieurs ou égaux à 0,9.

Répartitions

- Type de VIT (unifié)
- Accessible sur Internet (unifié)
- Évaluation du risque (unifiée)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'exploit existe (unifié)
- Type de ressource dans le cloud de l’élément détecté (unifié)
- CISA existe (unifié)
- Classe CMDB (unifiée)
- Unité business (unifiée)
- Criticité opérationnelle (unifié)
- Raison de l'ajournement (unifiée)
- Groupe d’affectation (unifié)
- État du rattrapage (unifié)

Visualisations des données

Onglet Vue d’ensemble des actifs

Titre	Type	Description
Vue d'ensemble de la surface d'attaque	Score unique 	Nombre représentant le score agrégé de la sécurité d’une organisation.
Nombre CI CMDB	Score unique 	Nombre de CI de l’organisation qui sont enregistrés et suivis dans le Base de données de gestion des configurations (CMDB). Fournit une répartition des CI suivants : • CI analysés : nombre de CI analysés • Exploit : nombre d’exploits disponibles • Accessible sur Internet : nombre de CI accessibles sur Internet
Ressource dans le cloud	Score unique 	Nombre de CI avec une catégorie d’actifs telle que le cloud. Fournit une répartition des actifs cloud suivants : • AWS • Azure • GCP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble des actifs (suite)

Titre	Type	Description
Image de Docker	Score unique 	Nombre d'images Docker incluant le nombre d'images de base.
Applications	Score unique 	Nombre d'applications dans l'organisation.

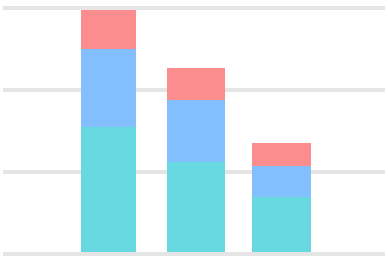
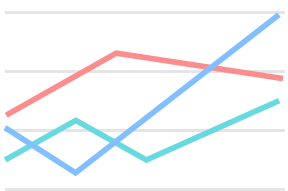
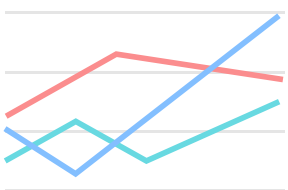
Onglet Vue d'ensemble de la vulnérabilité

Titre	Type	Description
KEV CISA	Graphique à secteurs	Nombre de vulnérabilités associées au catalogue et au CISA marqueur CISA comme vrai. Fournit une répartition basée sur les éléments suivants : • Vulnérabilité CISA : types de vulnérabilités avec le marqueur CISA comme vrai • CI hôte : accessible sur Internet : CI accessibles sur Internet • VIT non affectés : VIT non affectés avec le marqueur CISA comme vrai • Cible VIT manquée : VIT dont la cible a manqué le marqueur CISA comme vrai

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble de la vulnérabilité (suite)

Titre	Type	Description
Vulnérabilités actives par criticité	Barre 	Nombre de VIT, AVIT et CVIT actifs en fonction de la criticité.
Tendance de création et de fermeture de vulnérabilité	Ligne multiple 	Nombre de vulnérabilités nouvelles et fermées pour toutes les applications. Fournit une tendance pour les trois derniers mois.
Mauvaise configuration par plateforme cloud	Ligne multiple 	Nombre de problèmes de configuration basés sur la cote de risque pour chaque actif dans le cloud.
Conformité du cloud	Table	Liste des ressources dont la catégorie d'actifs est cloud avec les détails suivants : • Nom de la ressource • Classe • Problèmes de vulnérabilité : nombre de problèmes présents dans la ressource qui sont regroupés en fonction de l'évaluation du risque. • Problèmes de configuration : nombre de ressources présentant des problèmes de configuration ainsi que l'évaluation du risque.

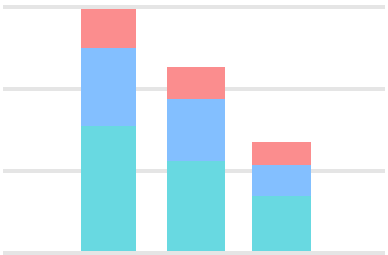
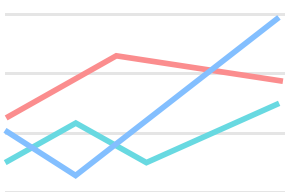
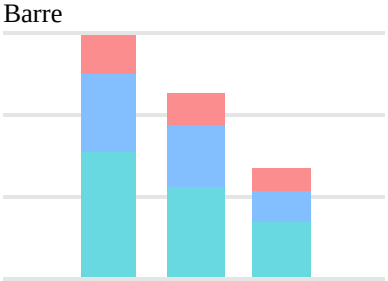
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble de la vulnérabilité (suite)

Titre	Type	Description
		• Compte dans le cloud : ID de compte dans le cloud. • Région du cloud : emplacement des ressources dans le cloud. • Fournisseur dans le cloud : nom du fournisseur dans le cloud.

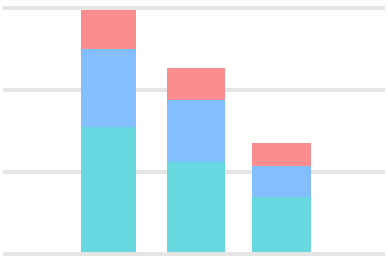
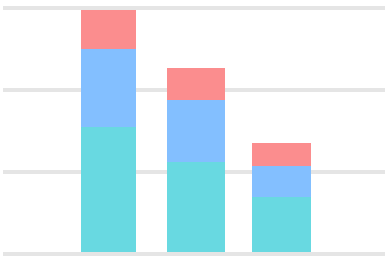
Onglet Vue d'ensemble de l'affectation

Titre	Type	Description
VIT non attribués	Barre 	Nombre de vulnérabilités qui ne sont affectées à aucun groupe ou individu avec l'évaluation du risque.
MTTR par groupe d'affectation - 10 premiers	Ligne multiple 	Temps moyen nécessaire à un groupe d'affectation pour identifier et corriger les vulnérabilités ou les problèmes de sécurité. Les 10 premiers groupes d'affectation ayant le temps moyen de rattrapage le plus élevé sont affichés.
10 principaux groupes d'affectation sans SLA (critique et vulnérabilité élevée)	Barre 	10 principaux groupes d'affectation qui n'ont pas respecté la date cible de rattrapage des vulnérabilités critiques et élevées.

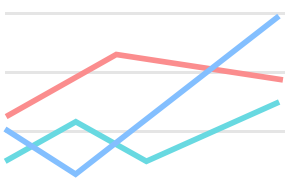
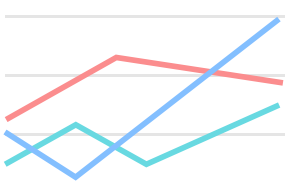
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Gestion des exceptions

Titre	Type	Description
VIT différés	Barre 	Nombre de vulnérabilités dans l'état différé en fonction de l'évaluation du risque.
VIT critiques et différés élevés par groupe d'affectation	Barre 	Nombre de vulnérabilités avec des cotes de risque critique et élevé à l'état différé, classées en fonction des groupes d'affectation.

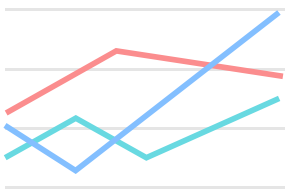
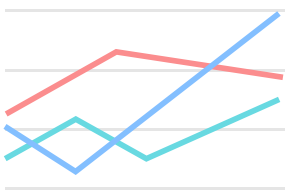
Onglet Accord sur les niveaux de service (SLA)

Titre	Type	Description
Vulnérabilité de l'hôte : exécution de SLA par groupe d'affectation	Ligne multiple 	Temps nécessaire à un groupe d'affectation pour corriger les vulnérabilités de l'hôte. Fournit une tendance pour les 10 derniers mois.
Problèmes de conformité : exécution de SLA par groupe d'affectation	Ligne multiple 	Temps nécessaire à un groupe d'affectation pour corriger les problèmes de conformité. Fournit une tendance pour les 10 derniers mois.

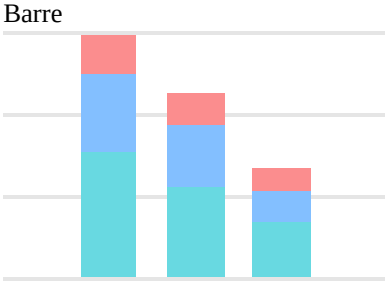
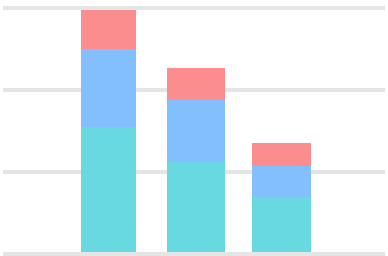
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Accord sur les niveaux de service (SLA) (suite)

Titre	Type	Description
Vulnérabilité de l'application : exécution de SLA par groupe d'affectation	Ligne multiple 	Temps nécessaire à un groupe d'affectation pour corriger les vulnérabilités de l'application. Fournit une tendance pour les 10 derniers mois.
Vulnérabilité de conteneur : exécution de SLA par groupe d'affectation	Ligne multiple 	Temps nécessaire à un groupe d'affectation pour corriger les vulnérabilités du conteneur. Fournit une tendance pour les 10 derniers mois.

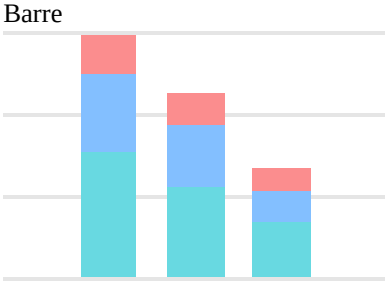
Onglet Vue d'ensemble de l'exclusion

Titre	Type	Description
Règles d'exclusion	Table	Liste de toutes les règles d'exclusion que vous avez créées.
Règles d'exclusion par rapport à accessible sur Internet	Barre 	Règles d'exclusion impactant les détections qui appartiennent aux actifs accessibles sur Internet.
Règles d'exclusion et existence de l'exploit	Barre 	Règles d'exclusion impactant les détections qui sont vulnérables aux exploits existants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

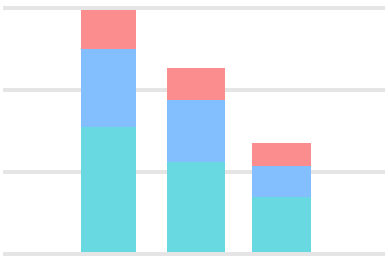
Onglet Intelligence sur les vulnérabilités

Titre	Type	Description
Vulnérabilités avec Score EPSS>= 0,9	Table	Complétez la vue de liste de toutes les entrées vulnérables (CVE ou TPE) dont le score EPSS est supérieur ou égal à 0,9, ainsi que les détails suivants. • ID : ID CVE de la vulnérabilité • Score de l'EPSS • Dernière modification de l'EPSS • CISA KEV BOD 22-01 : Indique si l'entrée existe dans la CISA KEV BOD (Binding Operational Directive 22-01) • VI totaux : nombre total de VI existants pour cette entrée de vulnérabilité. • Total des VI de conteneurs : nombre total d'EV de conteneurs qui existent pour cette entrée de vulnérabilité. • Gravité
Éléments vulnérables d'hôte externes avec un score EPSS >= 0,9	Score unique 	Nombre indiquant le nombre agrégé d'éléments vulnérables d'hôte orientés vers l'extérieur avec un score EPSS supérieur ou égal à 0,9. Fournit des scores uniques triés par gravité de la cote de risque.
Éléments vulnérables de l'hôte orientés vers l'extérieur, par niveau de risque	Barre 	Nombre d'éléments vulnérables de l'hôte orientés vers l'extérieur, par cote de risque. Les barres de la pile sont classées par score EPSS >=0,9 et CISA KEV = vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Intelligence sur les vulnérabilités (suite)

Titre	Type	Description
Éléments vulnérables avec un score EPSS >= 0,9 par niveau de risque	Barre 	Nombre de vulnérabilités avec un score EPSS supérieur ou égal à 0,9, triés par cote de risque. Fournit une répartition par éléments vulnérables d'hôte, d'applications et de conteneurs.

Travaux planifiés pour la collecte de données

Travaux de collecte de données permet de collecter automatiquement les scores d'indicateurs et de répartitions automatisés. Les travaux planifiés suivants sont exécutés pour collecter automatiquement des scores sur de nouvelles données.

Avertissement : Par défaut, les travaux de collecte de données suivants sont désactivés dans le système de base :

- Collecte de données quotidienne du tableau de bord unifié
- Collecte de données hebdomadaire du tableau de bord unifié
- Collecte de données historiques du tableau de bord unifié

Avant d'activer les tâches, consultez la base de connaissances .

Tâche planifiée	Fréquence	Description
Collecte de données historiques du tableau de bord unifié	Une fois	Collecte les scores et les instantanés des enregistrements existants.
Collecte de données hebdomadaire du tableau de bord unifié	Hebdomadaire	Collecte des données chaque semaine.
Collecte de données quotidienne du tableau de bord unifié	Quotidien	Collecte des données tous les jours.
Déployer les scores de risque sur l'organisation	Quotidien	Collecte le score de risque agrégé pour une organisation.
Renseigner les nombres quotidiens de conformité au cloud	Quotidien	Collecte des données pour la conformité au cloud.
Tâche quotidienne de l'EPSS	Quotidien	Collecte les données de l'EPSS à partir de First.org.

Une nouvelle table Déployer le score de risque de l'application [sn_vul_cmn_rollup_app_risk_score] est créée dans le périmètre commun de vulnérabilité. Cette table est renseignée à l'aide des calculateurs de déploiement suivants via les travaux planifiés quotidiens.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du calculateur de déploiement	Description
Déploiement du score de risque de l'organisation	Cumule les scores de risque pour tous les éléments vulnérables et les problèmes de configuration dans une organisation. Il fournit un score de risque global pour une organisation.
Déploiement de l'élément vulnérable	Cumule les scores de risque pour tous les éléments vulnérables dans une organisation afin de contribuer au score de risque global d'une organisation.
Déploiement de l'élément vulnérable d'application	Cumule les scores de risque pour tous les éléments vulnérables de l'application dans une organisation afin de contribuer au score de risque global d'une organisation.
Déploiement de l'élément vulnérable de conteneur	Cumule les scores de risque pour tous les éléments vulnérables du conteneur dans une organisation afin de contribuer au score de risque global d'une organisation.
Déploiement du résultat de test	Regroupe les scores de risque pour tous les résultats de test d'une organisation afin de contribuer au score de risque global d'une organisation.
Cumul des scores de l'EPSS des NVD aux TPE	Regroupe les scores EPSS des NVD aux TPE pour contribuer au score de risque global d'une organisation.

Surveillance et gestion des éléments vulnérables et des résultats des tests dans le Espace de travail du gestionnaire de vulnérabilités

Cela Espace de travail du gestionnaire de vulnérabilités vous permet de surveiller les éléments vulnérables (VIT, AVIT et CVIT) et les résultats des tests (TR) à l'aide de rubriques de visualisation, et de suivre et gérer leur progression du rattrapage en créant des efforts de rattrapage.

Ouvrir les résultats de recherche dans Espace de travail du gestionnaire de vulnérabilités

Ouvrez les résultats de recherche dans au Espace de travail du gestionnaire de vulnérabilités lieu de l'interface utilisateur classique en modifiant le périmètre de l'application.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin ou sn_vul.read_all pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager ou sn_vul.app_read_all pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst, sn_vul_container.vulnerability_admin ou sn_vul_container.read_all pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin ou sn_vulc.read pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

Exemple : si vous recherchez un élément vulnérable d'hôte avec son numéro dans le champ **Rechercher** en définissant le périmètre Espace de travail du gestionnaire de vulnérabilités de l'application sur , le VIT s'ouvre dans sa vue d'enregistrement dans le Espace de travail du gestionnaire de vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans la barre de navigation unifiée, sélectionnez l'icône Globe .
2. **Sélectionnez le périmètre de l'application**.
3. Définissez le champ d'application sur **Espace de travail du gestionnaire de vulnérabilité**.

Que faire ensuite

Lorsque vous recherchez des enregistrements tels que des VIT, des tâches de rattrapage, des approbations de changement d'état, etc., dans le champ **Rechercher** de la barre de navigation unifiée, les enregistrements s'ouvrent dans le champ .Espace de travail du gestionnaire de vulnérabilités

Lorsque le périmètre n'est pas Global, l'icône Globe s'affiche avec un anneau rouge . Sélectionnez-le à nouveau pour changer le champ d'application.

Créer et appliquer des filtres pour le résumé des enregistrements actifs (VIT, AVIT, CVIT et CTR)

En tant que gestionnaire et analyste des vulnérabilités, vous pouvez filtrer les enregistrements souhaités pour visualiser leur résumé sur la page d'accueil du Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Page d'accueil**.
2. Sélectionnez l'icône , puis sélectionnez **Créer un filtre** dans les onglets Vulnérabilités de l'hôte, Vulnérabilités du conteneur, Vulnérabilités de l'application ou Résultats des tests de configuration.
3. Renseignez les champs de la fenêtre contextuelle Créer un filtre.

Fenêtre contextuelle Créer des filtres

Champ	Description
Nom du filtre	Nom à donner au filtre.
Conditions	Condition permettant d'afficher uniquement les enregistrements pour lesquels vous souhaitez afficher des visualisations.
Actualiser quotidiennement	Mettez à jour les informations de visualisation tous les jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Enregistrer**.
5. Affichez les visualisations des enregistrements filtrés en sélectionnant le nouveau filtre dans le champ **Afficher par** .
   Pour plus d'informations sur les widgets, consultez Page d’accueil dans Espace de travail du gestionnaire de vulnérabilités.
6. Pour mettre à jour ou supprimer un filtre :

   a. Sélectionnez l’icône , puis Modifier le **filtre**.

   b. Dans la fenêtre contextuelle Filtres enregistrés, sélectionnez le filtre que vous souhaitez mettre à jour ou supprimer.

   c. Mettez à jour ou supprimez le filtre.

Action	Étapes
Supprimez le filtre.	Sélectionnez **Supprimer**.
Modifier le nom du filtre	Modifiez le nom du filtre et sélectionnez **Mettre à jour**.
Modifier les conditions de filtre	Modifiez la condition pour afficher uniquement les informations de certains enregistrements et sélectionnez **Mettre à jour**.
Actualiser quotidiennement	Déterminez s’il faut actualiser les informations de visualisation tous les jours et sélectionnez **Mettre à jour**.

Information associée

Page d’accueil dans Espace de travail du gestionnaire de vulnérabilités

Utiliser des rubriques de visualisation dans le Espace de travail du gestionnaire de vulnérabilités

Utilisez les rubriques de surveillance dans le pour afficher les Espace de travail du gestionnaire de vulnérabilités vulnérabilités et les erreurs de configuration filtrées à partir de vos données importées à partir des critères que vous avez définis. Utilisez ces informations pour déterminer l’impact des vulnérabilités et des erreurs de configuration de chaque rubrique de surveillance sur votre environnement.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d’hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l’application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

À partir de la page Rubriques de visualisation, vous pouvez effectuer les tâches suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Surveillez le nombre d'efforts et d'enregistrements de rattrapage (VIT, AVIT, CVIT et TR) pour suivre l'évolution de votre rattrapage de vulnérabilité.
- Modifiez ou supprimez vos rubriques de visualisation existantes et créez des rubriques de visualisation.
- Créez les efforts de rattrapage et transférez automatiquement les tâches de rattrapage à vos équipes informatiques uniquement pour les vulnérabilités que vous souhaitez corriger.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

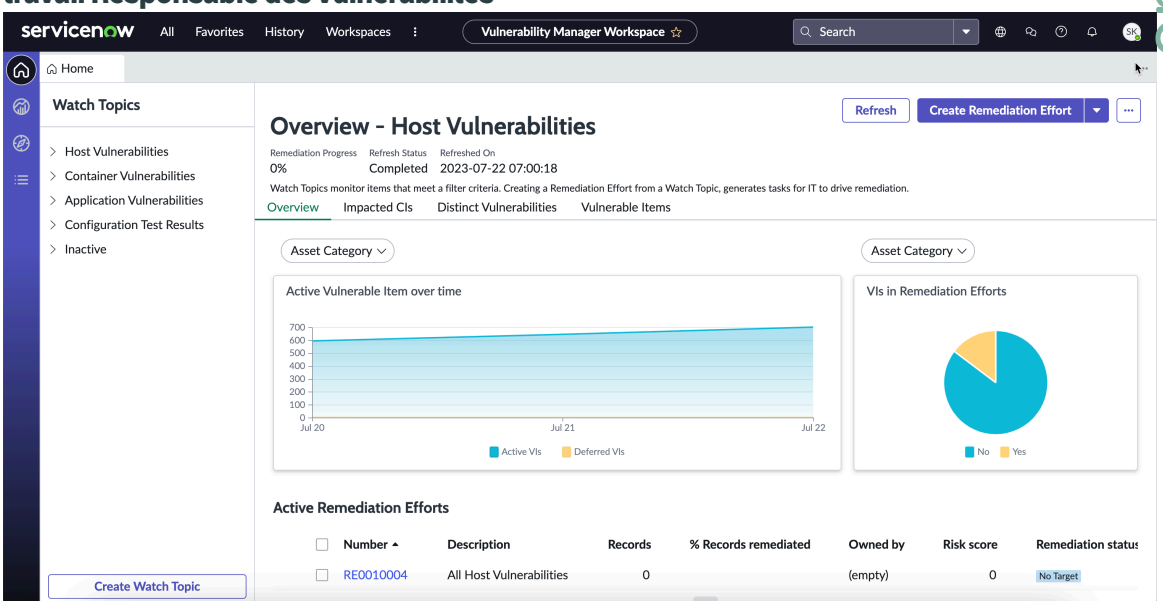
Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sélectionnez l'icône des rubriques de surveillance.
3. Sélectionnez une rubrique de visualisation dans les onglets Vulnérabilités de l'hôte, Vulnérabilités du conteneur, Vulnérabilités de l'application ou Résultats des tests de configuration de la page Rubriques de visualisation.

   Lorsque vous sélectionnez une rubrique de visualisation, l'onglet **Vue d'ensemble** s'affiche par défaut.

   Pour plus d'informations sur les rubriques relatives à la montre, reportez-vous à la section Page Rubriques de surveillance dans le Espace de travail du gestionnaire de vulnérabilités.

Onglet Vue d'ensemble de la version 19.0 sur la page d'accueil de l'espace de travail Responsable des vulnérabilités



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les tableaux de bord sont dynamiques et les nouvelles données de vulnérabilité sont mises à jour lors de l'importation.

4. Sélectionnez un **onglet Éléments connexes** pour afficher plus de données.

   Pour plus d'informations sur la liste des éléments connexes et les visualisations d'une rubrique de visualisation, reportez-vous à la section Liste et visualisations d'éléments connexes dans une rubrique de surveillance.

5. Effectuez les actions d'interface utilisateur sur la page Rubriques de visualisation.

Action d'interface utilisateur	Description
Créer une rubrique de surveillance	Créez votre propre rubrique de surveillance à l'aide de votre propre ensemble de conditions pour les vulnérabilités et les mauvaises configurations que vous jugez importantes. Pour plus d'informations sur la création d'une rubrique de visualisation, reportez-vous à la section Créer une rubrique de surveillance dans le Espace de travail du gestionnaire de vulnérabilités.
Modifier ou supprimer une rubrique de surveillance existante	Pour plus d'informations sur la modification ou la suppression d'une rubrique de surveillance, reportez-vous à la section Modifier ou supprimer une rubrique de surveillance dans Espace de travail du gestionnaire de vulnérabilités.
Désactiver ou activer une rubrique de surveillance	Vous pouvez désactiver ou activer une rubrique de visualisation. Pour plus d'informations sur la désactivation ou l'activation d'une rubrique de montre, consultezDésactiver ou activer une rubrique de surveillance .
Actualiser une rubrique de surveillance	Vous pouvez obtenir les derniers détails d'une rubrique de surveillance en sélectionnant le bouton **Actualiser** . Le dernier état d'actualisation et l'horodatage sont affichés sous le nom de la rubrique de visualisation. ○ Une rubrique de visualisation est actualisée automatiquement lorsqu'elle est créée ou mise à jour. ○ Lorsque vous actualisez une rubrique de visualisation, tous les détails de la rubrique de visualisation, y compris les graphiques et les efforts de rattrapage sont mis à jour. **Remarque :** Étant donné que vous ne pouvez pas actualiser une rubrique de visualisation inactive, le bouton **Actualiser** est inactif pour une rubrique de surveillance inactive.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
Créer un effort de rattrapage	○ Créez un effort de rattrapage. Un effort de rattrapage contient les tâches de rattrapage qui sont affectées à vos équipes informatiques. Vous pouvez utiliser cet outil pour piloter et suivre la progression du rattrapage, de l'affectation à la résolution. ○ Lorsque vous créez un effort de rattrapage, tous les éléments vulnérables actifs sont automatiquement extraits s'ils ne font pas déjà partie d'un effort de rattrapage existant pour cette rubrique de visualisation. ○ Les tâches de rattrapage sont affectées automatiquement aux équipes informatiques en fonction du groupe d'affectation des VI. ○ Un exemple d'effort de rattrapage de la rubrique de surveillance *Vulnérabilités sur serveurs Windows pourrait* être *Vulnérabilités sur serveurs Windows au 2e trimestre 2021*. Les tâches de rattrapage de cet effort sont ensuite affectées aux groupes d'affectation répertoriés dans les enregistrements associés.
Créer un effort récurrent	Créez des efforts de rattrapage récurrents selon un calendrier qui vous aide à suivre les vulnérabilités susceptibles de nécessiter votre attention immédiate et continue. Pour plus d'informations sur la création d'un effort récurrent, reportez-vous à la section Créer un effort de rattrapage récurrent dans le Espace de travail du gestionnaire de vulnérabilités. **Remarque :** Vous ne pouvez pas créer d'effort récurrent pour une rubrique de surveillance inactive.
Affiner les filtres pour une colonne d'une liste	Passez la souris sur le titre d'une colonne et cliquez sur le menu à trois points verticaux pour définir les filtres de cette colonne. Par exemple, supposons que vous souhaitiez filtrer davantage vos éléments de configuration qui sont associés aux enregistrements. Vous pouvez sélectionner la colonne Élément de configuration pour afficher les conditions de filtre disponibles. Vous pouvez définir des conditions pour filtrer vos actifs afin de ne voir que les actifs qui contiennent des données PCI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Filtrez les éléments ou faites correspondre les éléments d'une ligne dans une colonne. Par exemple, supposons que vous souhaitiez afficher uniquement les enregistrements qui présentent une vulnérabilité spécifique. Une fois l'onglet de liste Éléments connexes Éléments vulnérables sélectionné, dans la liste des enregistrements, sélectionnez la ligne d'un enregistrement dans la colonne Résumé. Sélectionnez le menu à trois points verticaux qui s'affiche, puis sélectionnez l'une des options suivantes : ○ **Afficher la correspondance** : affiche tous les autres enregistrements qui présentent cette vulnérabilité. ○ **Filtrer** : affiche tous les enregistrements qui n'ont pas cette vulnérabilité.

6. **Facultatif :** Sélectionnez un enregistrement pour afficher plus de détails.

Créer une rubrique de surveillance dans le Espace de travail du gestionnaire de vulnérabilités

Les gestionnaires de vulnérabilité et les analystes peuvent créer des rubriques de surveillance à l'aide d'un ensemble de conditions pour filtrer les sous-ensembles d'enregistrements (VIT, AVIT, CVIT ou CTR) qu'ils souhaitent surveiller.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Dans l'onglet Vue d'ensemble des rubriques de visualisation, un rapport de tendance mis à jour tous les soirs, ainsi que d'autres rapports, affichent l'état actuel des enregistrements de cette rubrique de visualisation.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité** > **Rubriques de surveillance**.
2. **Facultatif :** Sinon, à droite du bouton Créer un effort de rattrapage, cliquez sur des trois points , puis modifiez pour modifier une rubrique de surveillance existante.

   Remarque : Vous remarquerez peut-être un délai avant que les données actuelles ne s'affichent pour une rubrique de surveillance après avoir modifié le filtrage.

3. En bas à gauche de la page, sélectionnez **Créer une rubrique de visualisation**.
4. Renseignez les champs dans le modal qui s'affiche.
   Pour plus d'informations sur les champs du modal Créer une rubrique de visualisation, voirChamps du formulaire Créer une rubrique de visualisation.
5. Définissez des conditions pour la catégorie d'enregistrement sélectionnée.

Option dans la liste déroulante Catégorie	Étapes
Vulnérabilités d'hôte	Dans la **condition d'élément vulnérable**, définissez les conditions pour identifier les vulnérabilités de l'hôte. Les vulnérabilités de l'hôte sont détectées en fonction des conditions définies.
Vulnérabilités d'applications	Dans la **condition d'élément vulnérable d'application**, définissez les conditions pour identifier les vulnérabilités de l'hôte. Les vulnérabilités de l'application (ou AVIT) sont détectées en fonction des conditions définies.
Vulnérabilités du conteneur	Dans la **condition d'élément vulnérable de conteneur**, définissez les conditions pour identifier les vulnérabilités de l'hôte. Les vulnérabilités de conteneur (CVIT) sont détectées en fonction des conditions définies.
Résultats des tests de configuration	Dans la **condition Résultats des tests de configuration**, définissez les conditions pour identifier les problèmes de configuration. Les résultats des tests de configuration sont détectés en fonction des conditions définies.

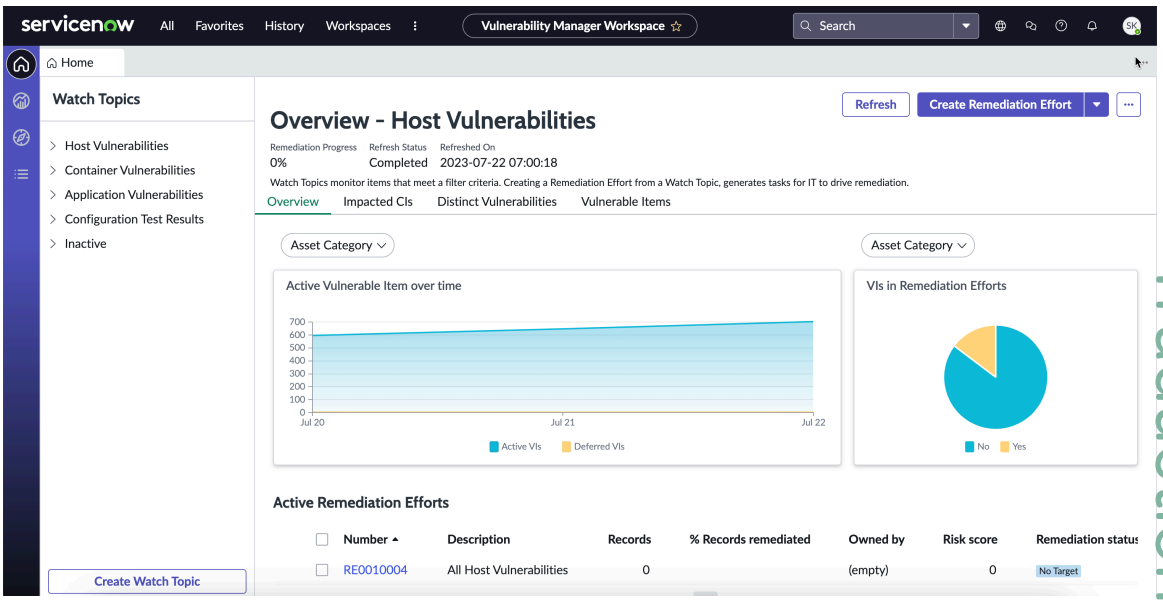
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous ne définissez aucune condition dans votre rubrique de surveillance, aucune donnée n'est transférée vers le tableau de bord.

6. Cliquez sur **Envoyer**.
   Votre nouveau sujet de visualisation s'affiche sur la page de destination Accueil. Lesrubriques de surveillance sont classées par type d'enregistrement dans le volet de navigation.

Page d'accueil de la version 19.0 Espace de travail du gestionnaire de vulnérabilités



Que faire ensuite

Créez un effort de rattrapage.

Modifier ou supprimer une rubrique de surveillance dans Espace de travail du gestionnaire de vulnérabilités

Vous pouvez modifier ou supprimer une rubrique de surveillance existante dans le Espace de travail du gestionnaire de vulnérabilités fichier .

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Si vous modifiez une rubrique de surveillance existante :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les données du tableau de bord sont mises à jour pour refléter vos changements.
- Les enregistrements qui font actuellement partie des efforts de rattrapage existants restent inchangés.
- Les enregistrements qui ne font pas actuellement l'objet d'efforts de rattrapage s'affichent en fonction des critères que vous saisissez dans le générateur de conditions.

Si vous supprimez une rubrique de visualisation avant que tous ses enregistrements associés ne soient corrigés, les enregistrements qui s'affichent avec cette rubrique de surveillance ne sont pas affectés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Rubriques de surveillance**.
2. Ouvrez la rubrique de surveillance que vous souhaitez modifier.
3. Cliquez sur Plus à trois points, puis sur **Modifier**.

   Remarque : Vous ne pouvez pas modifier une rubrique de surveillance inactive.

4. Dans le modal Modifier la rubrique de visualisation, modifiez les champs.
5. Cliquez sur **Envoyer**.

   Remarque : Vous remarquerez peut-être un délai avant que les données actuelles ne s'affichent pour une rubrique de surveillance après avoir modifié le filtrage.

   Vous pouvez également modifier les efforts de rattrapage récurrents existants. S'il existe un effort de rattrapage récurrent pour une rubrique de visualisation, Modifier **l'effort récurrent** est disponible dans le menu. Sélectionnez cette option pour modifier l'effort récurrent.

   Les modifications que vous apportez et enregistrez dans l'enregistrement de l'effort de rattrapage n'affectent aucun des autres efforts de rattrapage que vous avez déjà créés à partir de la rubrique de visualisation.

6. **Facultatif :** Pour supprimer une rubrique de visualisation, sélectionnez du menu à trois points sur la rubrique de surveillance et sélectionnez **Supprimer**.

Désactiver ou activer une rubrique de surveillance

Vous pouvez désactiver ou activer une rubrique de surveillance dans l'espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

- Toutes les rubriques de surveillance inactives sont affichées dans le module **Inactif** du volet de navigation.
- Vous ne pouvez pas créer d'effort de rattrapage ou d'effort de rattrapage récurrent pour une rubrique de surveillance inactive.
- Vous ne pouvez pas actualiser une rubrique de surveillance inactive.
- Les détails d'une rubrique de surveillance inactive et ses efforts de rattrapage associés ne sont pas mis à jour.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Rubriques de surveillance**.
2. Ouvrez la rubrique de surveillance que vous souhaitez désactiver.
3. Cliquez sur les trois points, puis sur **Désactiver**.
   La rubrique de surveillance apparaît dans le module Inactif.
4. Pour activer une rubrique de visualisation, sélectionnez-la dans le module Inactif, sélectionnez le menu à trois points, puis sélectionnez **Activer**.
   La rubrique de surveillance activée se déplace vers le module approprié dans le volet de navigation.

Utiliser les enregistrements d'effort de rattrapage

Lorsque les gestionnaires et les analystes de vulnérabilité créent des efforts de rattrapage, les tâches de rattrapage (VUL, AVUL, CVIL et CRG) sont automatiquement affectées aux équipes informatiques pour remédiation.

Avant de commencer

Vous devez créer un effort de rattrapage avant de pouvoir l'utiliser pour surveiller la progression du rattrapage sur les tâches de rattrapage.

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Procédure

1. Si elle n'est pas sélectionnée, cliquez sur l'icône Liste en haut à gauche.

   La vue de liste contenant les enregistrements d'effort de rattrapage actifs s'affiche.

2. Dans la colonne Type d'enregistrement, sélectionnez le menu à trois points et sélectionnez **Grouper par type d'enregistrement**.
   Les efforts de rattrapage classent en éléments vulnérables d'hôte, éléments vulnérables d'applications, éléments vulnérables de conteneurs et résultats des tests de configuration.
3. À partir de la page de destination de la vue de liste, avec des efforts de rattrapage actifs sélectionnés dans les listes filtrées, cliquez sur un enregistrement pour l'ouvrir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’enregistrement s’affiche. Vous pouvez afficher les tâches et les enregistrements de rattrapage associés à l’effort de rattrapage sélectionné.

4. Reportez-vous à la table suivante pour connaître les actions que vous pouvez effectuer sur l’enregistrement de l’effort de rattrapage.

   Une fois l’enregistrement créé, l’affichage des tâches de rattrapage et un grand nombre d’enregistrements peuvent prendre quelques minutes.

Action d'interface utilisateur	Description
Ajouter une balise	À droite de l’en-tête, cliquez sur la petite icône de balise. Vous voudrez peut-être ajouter du texte pour vous aider davantage à identifier cet enregistrement. Par exemple, vous pouvez ajouter une balise indiquant que cet enregistrement contient des données PCI ou d’autres données critiques.
Ajouter une note de travail à l’enregistrement	Tout à droite de l’écran, cliquez sur l’icône **Activité** (icône d’éclair) et entrez une note de travail. Cliquez sur l’icône pour activer/désactiver le panneau.
Mettre à jour l'enregistrement	Dans l’onglet **Détails** , pour tous les champs modifiables, cliquez sur un champ pour le sélectionner, apportez vos modifications, puis cliquez sur **Enregistrer** pour mettre à jour l’enregistrement.
Lorsqu’il est affiché, cliquez sur l’icône de filtre pour affiner les données sur la page affichée	Avec l’un des onglets Tâches de rattrapage, Éléments vulnérables ouRésultats des tests de configuration sélectionnés, cliquez sur l’icône de filtre pour afficher les filtres qui s’appliquent à l’onglet, tout à droite. Dans le panneau qui s’affiche, cliquez sur **Vue avancée** pour ajouter ou modifier des conditions de filtre pour les éléments de la page. Cliquez sur **Mettre à jour** pour enregistrer vos modifications. Par exemple, dans l’onglet **Éléments vulnérables** , vous préférerez peut-être ajouter le champ Âge et saisir une plage pour afficher uniquement les enregistrements d’une période spécifique. Les enregistrements qui correspondent aux conditions que vous définissez sont affichés dans la liste.
Affiner les filtres pour les éléments d’une colonne	Sélectionnez une colonne, puis cliquez sur le menu à trois points verticaux, développez-la et entrez des conditions pour affiner et regrouper les données dans la colonne.
Filtrer les éléments ou faire correspondre les éléments d’une ligne dans une colonne	Imaginons, par exemple, que vous souhaitiez afficher uniquement les enregistrements qui présentent une vulnérabilité spécifique. Dans la liste des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
	enregistrements, sélectionnez la ligne de l'enregistrement dans la colonne **Résumé** . Cliquez sur le menu à points vertical qui s'affiche et choisissez-en un : ○ **Afficher la correspondance** : affichez tous les autres enregistrements qui présentent cette vulnérabilité. ○ **Filtrer** : afficher tous les enregistrements qui n'ont pas cette vulnérabilité.

5. Dans les onglets Tâches de rattrapage, Éléments vulnérables et Résultats des tests de configuration, vous pouvez explorer dans le détail les enregistrements d'une tâche de rattrapage (VUL, AVUL, CVIL ou CRG), d'un élément vulnérable (VIT, AVIT ou CVIT) et d'un résultat de test (CTR) individuels, respectivement.

Que faire ensuite

Si vous souhaitez créer une tâche de rattrapage sur demande à partir d'un effort de rattrapage, reportez-vous à la section Créer une tâche de rattrapage sur demande à partir de Effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités. Vous pouvez également Créer une liste personnalisée des enregistrements vous aider à surveiller la progression du rattrapage.

Créer un effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités

Un enregistrement d'effort de rattrapage est une liste statique d'enregistrements que vous créez à partir d'une rubrique de surveillance dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Vous utilisez des efforts de rattrapage pour transférer les tâches que les équipes informatiques utilisent pour corriger les vulnérabilités et les erreurs de configuration.

- Vous pouvez modifier les efforts de rattrapage existants.
- Créez des efforts de rattrapage qui sont créés automatiquement aux dates et heures que vous définissez.
- Transférer des enregistrements d'efforts de rattrapage existants vers un nouvel effort de rattrapage.

À partir de la version 18.0, comme vous ne pouvez pas créer un effort de rattrapage pour une rubrique de surveillance inactive, le bouton **Créer un effort de rattrapage** est inactif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité** > **Rubriques de surveillance**.
2. Sur la page Rubriques de visualisation, sélectionnez une rubrique de visualisation pour laquelle vous souhaitez créer un effort de rattrapage.
3. Pour afficher les enregistrements associés à la rubrique de visualisation sélectionnée, sous l'en-tête de l'enregistrement, cliquez sur l'onglet **Éléments vulnérables**, **Éléments vulnérables de l'application**, **Éléments vulnérables de conteneurs** ou **Résultats des tests de configuration** dans leurs rubriques de visualisation respectives.

   Les enregistrements s'affichent.

   Par exemple, dans l'en-tête sous l'onglet Éléments vulnérables, vous pouvez afficher le nombre total d'enregistrements de cette rubrique de visualisation.

   Les colonnes et données suivantes s'affichent :

Colonnes de l'onglet Éléments vulnérables

Colonne	Description
Numéro	Numéro d'enregistrement.
Résumé	Description de la vulnérabilité.
Élément de configuration	L'actif associé à la vulnérabilité.
Cote de risque	Score de risque quantifié séparant les enregistrements en critiques, élevés, moyens, faibles et aucun.
État	État de l'enregistrement.
Statut de la remédiation	État du rattrapage d'un enregistrement.
Groupe d'affectation	Groupes d'affectation responsables du rattrapage. L'affectation d'enregistrements à des groupes est basée sur les règles d'affectation que vous créez.
Effort de rattrapage	S'il est affecté à un effort de rattrapage, chaque enregistrement répertorie l'effort de rattrapage qui lui est affecté. Une fois ajouté à un effort de rattrapage, un enregistrement n'est ajouté à aucun autre effort de rattrapage que vous créez.
Groupe d'affectation	Groupes d'affectation responsables du rattrapage. L'affectation d'enregistrements à des groupes est basée sur les règles d'affectation que vous créez.
Effort de rattrapage	S'il est affecté à un effort de rattrapage, chaque enregistrement répertorie l'effort de rattrapage qui lui est affecté. Une fois ajouté à un effort de rattrapage, un enregistrement n'est ajouté à aucun autre effort de rattrapage que vous créez.
Dans une tâche de remédiation	Si vrai, cette valeur indique qu'un enregistrement est déjà dans une tâche de rattrapage. Les enregistrements peuvent se trouver dans plusieurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
	tâches de rattrapage, mais un enregistrement ne peut être ajouté qu'à un seul effort de rattrapage.
Existence de l'exploit	Indique s'il existe un exploit connu pour un enregistrement.
Dernières ouvertures	Date de la dernière ouverture de l'enregistrement dans votre ServiceNow AI Platform. Si l'enregistrement a été fermé puis rouvert, il s'agit de la dernière fois que l'enregistrement a été rouvert.

4. Pour créer un effort de rattrapage, cliquez sur **Créer un effort de rattrapage**.

   Lorsque vous créez un effort de rattrapage, les enregistrements déjà présents dans des efforts de rattrapage existants ne sont pas ajoutés aux nouveaux efforts de rattrapage que vous créez à partir de cette rubrique de visualisation.

   À mesure que des enregistrements sont mis à jour ou que de nouveaux enregistrements sont créés dans des rubriques de surveillance, vous pouvez créer des efforts de rattrapage.

5. Vous pouvez Créer un effort de rattrapage récurrent dans le Espace de travail du gestionnaire de vulnérabilitéségalement .

   Le bouton **Modifier** est disponible dans le menu pour les efforts de rattrapage existants. Vous pouvez modifier les champs et les conditions à partir d'une fenêtre modale qui s'affiche. Les modifications que vous apportez et enregistrez dans l'enregistrement de l'effort de rattrapage n'affectent aucun des autres efforts de rattrapage que vous avez déjà créés à partir de la rubrique de visualisation.

6. À l'étape 1 du modal Créer un effort de rattrapage, renseignez les champs.

   Dans le champ Brève description, saisissez un texte qui décrit l'effort de rattrapage récurrent et vous aide à le localiser et à le suivre dans la liste des efforts.

   Dans le champ Description, saisissez plus de texte sur le contexte de l'effort qui vous aide à le localiser facilement dans la liste des efforts de rattrapage.

7. À l'étape 2, Génération de tâches, choisissez une méthode dans la liste pour regrouper les enregistrements dans les tâches de rattrapage que vous générez à partir de cet effort de rattrapage après sa création.

Option	Description
Par groupe d'affectation	Les enregistrements avec le même groupe d'affectation sont regroupés en une seule tâche de rattrapage.
Par groupe d'affectation et élément de configuration	Les enregistrements avec le même groupe d'affectation et le même élément de configuration sont regroupés en une seule tâche de rattrapage.
Par groupe d'affectation et (vulnérabilité ou test de configuration)	Les enregistrements avec le même groupe d'affectation et le même élément de configuration sont regroupés en une seule tâche de rattrapage.
Aucune (aucune tâche de rattrapage n'est créée).	Utilisez cette méthode si vous souhaitez ajouter des enregistrements manuellement à une tâche de rat-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	trapage pour cet effort. Consultez Créer une tâche de rattrapage sur demande à partir de Effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités.

8. Pour actualiser automatiquement les éléments vulnérables en double de l'hôte, vous devez cocher la case **Actualiser automatiquement les éléments vulnérables en double pour les tâches de rattrapage créées** .

   Remarque : Cette case à cocher est disponible uniquement pour les vulnérabilités d'hôte.

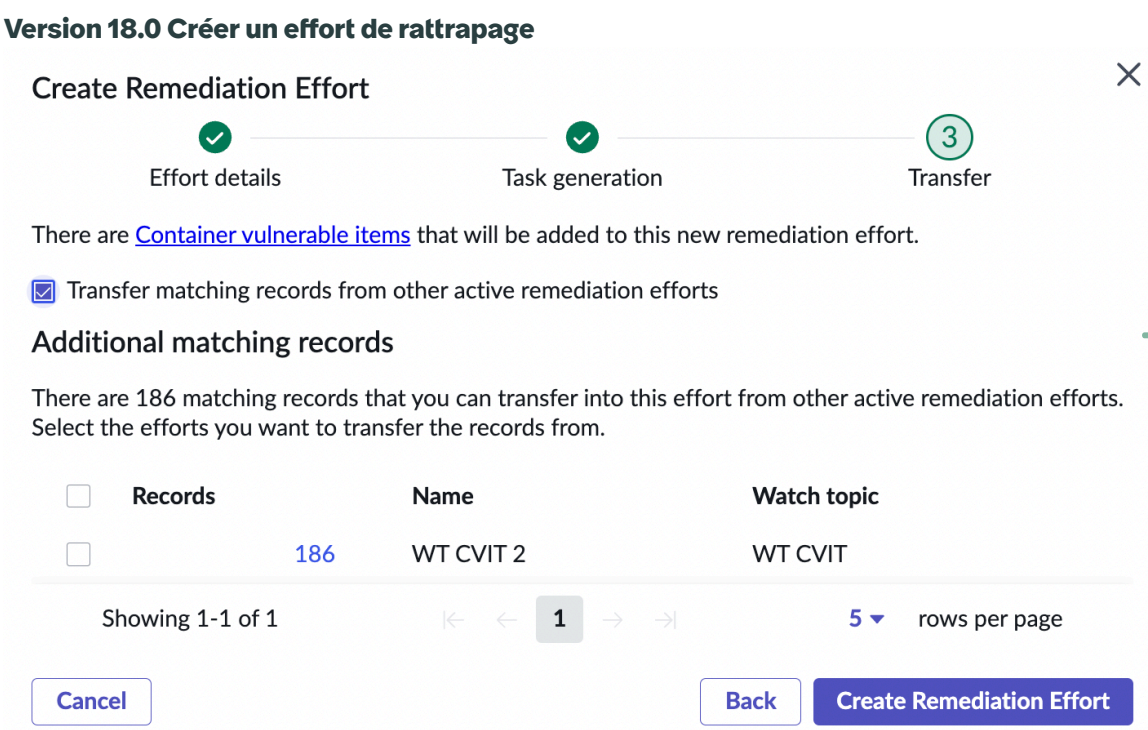
9. À l'étape 3, Transférer, vérifiez le nombre d'enregistrements que vous souhaitez ajouter à l'effort de rattrapage et voyez combien d'enregistrements sont disponibles pour le transfert à partir d'autres efforts de rattrapage actifs.

   S'il n'existe aucun nouvel enregistrement actif à ajouter, le texte suivant s'affiche :

   Il n'existe aucun enregistrement actif disponible à ajouter à ce nouvel effort de rattrapage.

   Tous les enregistrements supplémentaires disponibles pour le transfert vers cet effort sont répertoriés sous Enregistrements correspondants supplémentaires .

   Cochez la case **Transférer les enregistrements correspondants à partir d'autres efforts de rattrapage actifs** , puis cochez les cases en regard des enregistrements que vous souhaitez transférer à partir d'autres efforts de rattrapage actifs.



   Après avoir cliqué sur **Créer un effort de rattrapage**, le nouvel effort de rattrapage s'affiche au bout de quelques instants. Selon le nombre d'enregistrements, le remplissage du nouvel enregistrement peut prendre un certain temps. Un message indique si l'enregistrement est toujours en cours de remplissage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le nouvel effort de rattrapage est créé avec tous les enregistrements disponibles dans la rubrique de surveillance utilisée pour le créer, en plus de tous les enregistrements que vous avez sélectionnés pour le transfert à partir d'efforts existants.

Si vous sélectionnez des enregistrements à transférer à partir d'un effort existant, et que l'effort existant transfère tous ses enregistrements dans votre nouvel effort, l'effort de rattrapage à partir duquel vous avez déplacé les enregistrements est fermé. Pour en savoir plus sur l'impact du transfert d'enregistrements sur les tâches de rattrapage associées aux efforts de rattrapage, reportez-vous à la section Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Réponse aux vulnérabilités.

Remarque : S'il n'y a pas d'enregistrements disponibles dans la rubrique de surveillance ou des enregistrements sélectionnés pour le transfert, le bouton **Créer un effort de rattrapage** est désactivé.

La *`Populate Efforts`* tâche planifiée s'exécute toutes les 10 minutes pour renseigner les données dans les widgets en fonction de la condition sélectionnée.

Cliquez sur l'onglet Progression du rattrapage pour afficher la progression du rattrapage. Cliquez sur n'importe quel élément pour afficher les détails, y compris le type d'enregistrement, le score de risque, la cote de risque, le pourcentage d'enregistrements rattrapés, les enregistrements à l'état différé et non différé et le nombre total d'enregistrements, les conditions utilisées dans la rubrique de surveillance et l'état du rattrapage. Les informations sur l'état du rattrapage, telles que la cible de rattrapage et l'état du rattrapage, sont déployées à partir de la table Éléments vulnérables. Le score de risque d'enregistrement le plus élevé est déployé à partir de la table Calculateurs de vulnérabilité tandis que le score de risque est déployé à partir du **Calculateurs de déploiement de vulnérabilité** > **Déploiement d'effort de correction**.

L'onglet Tâches de remédiation affiche les tâches de tous les types de problèmes. Les champs sont renseignés lorsque les travaux planifiés suivants s'exécutent. Elles sont exécutées automatiquement toutes les 15 minutes :

- Redéployer les valeurs des éléments vulnérables de l'application sur la vulnérabilité et le groupe.
- Déployer les valeurs d'éléments vulnérables du conteneur sur la vulnérabilité et le groupe.
- Déployer les valeurs des résultats des tests dans le groupe de résultats des tests et les tests de configuration.
- Redéployer les valeurs des éléments vulnérables sur la vulnérabilité et le groupe.

Dans la vue Listes, vous pouvez afficher les efforts de rattrapage, les tâches de rattrapage, les éléments vulnérables, les résultats des tests de configuration, etc. Vous pouvez ouvrir une tâche de rattrapage ou un élément vulnérable et afficher la page Détails. Cliquez sur les ellipses Actions supplémentaires, puis sur **Démarrer l'examen** pour résoudre une tâche de rattrapage.

10. **Facultatif :** Vous pouvez également modifier les efforts de rattrapage récurrents existants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(Optional) S'il existe un effort de rattrapage récurrent pour une rubrique de visualisation, Modifier **l'effort récurrent** est disponible dans le menu en haut à droite d'une rubrique de visualisation. Choisissez cette option pour modifier l'effort récurrent.

Les modifications que vous apportez et enregistrez dans l'enregistrement de l'effort de rattrapage n'affectent aucun des autres efforts de rattrapage que vous avez déjà créés à partir de la rubrique de visualisation.

Créer une tâche de rattrapage sur demande à partir de Effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités

Créez une tâche de rattrapage sur demande à partir d'un effort de rattrapage. Si vous créez une tâche de rattrapage sur demande, vous choisissez les enregistrements que vous souhaitez ajouter manuellement.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Pour la version 18.0 de Réponse aux vulnérabilités, vous ne pouvez pas créer une tâche de rattrapage à partir de la vue d'enregistrement d'un effort de rattrapage.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. En haut à gauche de l'espace de travail avec la page d'accueil affichée, cliquez sur l'icône Vue **de listes** pour afficher la page de destination Liste.
3. Sous Efforts de rattrapage, cliquez sur **Actif** ou **Tous**.
4. Dans la liste qui s'affiche, cliquez sur un enregistrement pour l'ouvrir.
   L'onglet Vue d'ensemble de l'enregistrement s'affiche.
5. Cliquez sur l'onglet **Éléments vulnérables** .
   La liste des enregistrements s'affiche.
6. Pour créer une nouvelle tâche de rattrapage, dans la colonne Numéro, sélectionnez les enregistrements que vous souhaitez ajouter.
7. Cliquez sur **Créer une tâche de rattrapage**.
8. Renseignez les champs du modal qui s'affiche.

Champ	Description
Description brève	Saisissez un texte qui peut vous aider à identifier facilement ces tâches de rattrapage à partir de vos tâches de rattrapage existantes.
Groupe d'affectation	Choisissez un groupe d'affectation pour les tâches. Utilisez le filtre pour vous aider à localiser le groupe souhaité.

9. Cliquez sur **Créer**.
10. La nouvelle tâche de rattrapage s'affiche avec les enregistrements actifs que vous avez sélectionnés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un effort de rattrapage récurrent dans le Espace de travail du gestionnaire de vulnérabilités

Vous pouvez créer et planifier des efforts de rattrapage récurrents qui sont générés automatiquement aux dates et heures que vous définissez.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Vous pouvez créer automatiquement des efforts de rattrapage récurrents selon un calendrier qui vous aide à suivre les vulnérabilités susceptibles de survenir et nécessitant une attention immédiate et continue.

À partir de la version 18.0, comme vous ne pouvez pas créer un effort de rattrapage récurrent pour une rubrique de surveillance inactive, l'option **Créer un effort récurrent** est inactive. Si vous désactivez une rubrique de surveillance qui a un effort récurrent déjà planifié, un nouvel effort de rattrapage n'est pas créé tant que la rubrique de surveillance n'est pas activée. En outre, les détails de la **récurrence de l'effort** et de la **date de la prochaine récurrence** disparaissent en haut à droite. Après avoir activé la rubrique de visualisation, un effort de rattrapage est créé au calendrier à venir.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité** > **Rubriques de surveillance**.
2. Sur la page Rubriques de visualisation, sélectionnez une rubrique de visualisation pour laquelle vous souhaitez créer un effort de rattrapage récurrent.

   Vous pouvez créer un effort de rattrapage récurrent par rubrique de visualisation.

   Remarque : Vous ne pouvez pas transférer les enregistrements d'efforts de rattrapage récurrents vers de nouveaux efforts de rattrapage. Toutefois, vous pouvez transférer des enregistrements d'efforts de rattrapage existants et non récurrents vers de nouveaux efforts de rattrapage. Pour en savoir plus sur le transfert d'enregistrements, reportez-vous Transférer des enregistrements aux efforts de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités à la section .

3. Dans une rubrique de visualisation, en haut à droite de la liste Créer un effort de rattrapage, sélectionnez **Créer un effort récurrent**.

   Le modal Créer un effort récurrent s'affiche.

4. À l'étape 1, Détails de l'effort, renseignez les champs requis.

   Dans le champ Brève description, saisissez le texte qui décrit l'effort de rattrapage récurrent qui vous aide à le localiser et à le suivre dans la liste des efforts.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le champ Description, saisissez plus de texte sur le contexte de l'effort qui vous aide à le localiser facilement dans la liste des efforts de rattrapage. Par exemple, les vulnérabilités des actifs orientés vers l'extérieur.

5. Cliquez sur **Suivant**.
   Les détails de la génération de tâches s'affichent.
6. À l'étape 2, Génération de tâches, choisissez une méthode dans la liste pour regrouper les éléments vulnérables dans les tâches de rattrapage que vous générez à partir de cet effort de rattrapage après sa création.
   - Par groupe d'affectation
   - Par groupe d'affectation et élément de configuration
   - Par groupe d'affectation et vulnérabilité
   - Aucune (aucune tâche de rattrapage n'est créée). Utilisez cette méthode si vous souhaitez ajouter des enregistrements manuellement à une tâche de rattrapage pour cet effort. Consultez Créer une tâche de rattrapage sur demande à partir de Effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités.
7. Pour actualiser automatiquement les éléments vulnérables en double de l'hôte, vous devez sélectionner l'option **Actualiser automatiquement les éléments vulnérables en double pour les tâches de rattrapage créées** .

   Remarque : Cette case à cocher est disponible uniquement pour les vulnérabilités d'hôte.
8. Cliquez sur **Suivant** pour continuer.
9. À l'étape 3, Récurrence, sélectionnez la fréquence.

Option	Description
Par trimestre (tous les 3 mois)	Planifie l'effort de rattrapage une fois tous les trois mois. **Remarque :** Si le mois que vous sélectionnez ne compte que 30 jours, l'effort de rat–trapage est créé à cette dernière date du mois.
Mensuel	Planifie l'effort de rattrapage une fois par mois.
Hebdomadaire	Planifie l'effort de rattrapage une fois par semaine. **Remarque :** Cette option est disponible à partir de la version 19.0 de Réponse aux vulné-rabilités.
Quotidien	Planifie l'effort de rattrapage tous les jours. **Remarque :** Cette option est disponible à partir de la version 19.0 de Réponse aux vulné-rabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Définissez le calendrier de récurrence.

Utilisez les listes pour sélectionner le mois/jour/heure/minute dans lequel vous souhaitez créer l'effort de rattrapage. Le fuseau horaire pour la planification est par défaut votre fuseau horaire.

Remarque : Si vous avez de nombreuses vulnérabilités, vous préférerez peut-être définir la création en dehors des heures de travail.

Si vous souhaitez que la tâche soit créée le dernier jour du mois, la tâche planifiée crée l'effort de rattrapage récurrent le dernier jour du mois. Un message s'affiche si le mois ne dispose pas de 31 jours.

b. **Facultatif :** Sélectionnez **Transférer les vulnérabilités** vers les vulnérabilités actives dans cet effort de rattrapage pour les poursuivre dans chaque effort de rattrapage ultérieur créé.

10. Cliquez sur **Planifier la récurrence**.
Un message s'affiche indiquant que l'enregistrement de rattrapage récurrent a été créé. Le nouvel effort de rattrapage ne s'affiche pas immédiatement, il est créé lorsque vous l'avez planifié. Il s'affiche dans vos listes après sa création par la tâche planifiée.

La date de création de l'effort de rattrapage est affichée sur la rubrique de surveillance correspondante. Pour en savoir plus sur la façon dont les tâches de rattrapage associées aux efforts de rattrapage sont impactées par le transfert d'enregistrements, reportez-vous à la section Cycles de vie des efforts de rattrapage, des tâches de rattrapage et des enregistrements dans les espaces de travail Réponse aux vulnérabilités.

Transférer des enregistrements aux efforts de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités

Vous pouvez transférer des enregistrements d'efforts de rattrapage existants vers de nouveaux efforts de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Si vous êtes confronté à une menace zero-day ou à une vulnérabilité très critique que vous souhaitez résoudre rapidement, vous pouvez consolider tous les enregistrements actifs que vous avez déjà pour cette vulnérabilité en un seul effort de rattrapage. Toutefois, chaque enregistrement ne peut faire partie que d'un seul effort et les enregistrements peuvent se chevaucher entre les rubriques de surveillance. Pour les rassembler tous, vous devez donc transférer ces enregistrements de plusieurs efforts existants en un seul effort de rattrapage.

Imaginons, par exemple, que vous ayez créé un effort de rattrapage qui contient une vulnérabilité hautement prioritaire. Étant donné que cette vulnérabilité est répandue et a potentiellement un impact sur d'autres zones de votre environnement, vous pouvez avoir des enregistrements qui sont déjà associés à cette vulnérabilité dans des efforts de rattrapage existants. Pour combiner ces enregistrements afin qu'ils soient tous dans un seul effort de rattrapage, vous pouvez transférer tous les enregistrements d'efforts de rattrapage existants dans un nouvel effort de rattrapage.

Remarque : Vous ne pouvez pas transférer les enregistrements d'efforts de rattrapage récurrents vers de nouveaux efforts de rattrapage. Pour plus d'informations, consultez Créer un effort de rattrapage récurrent dans le Espace de travail du gestionnaire de vulnérabilités.

Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sélectionnez l'icône des rubriques de surveillance.
3. Sur la page Rubriques de visualisation, sélectionnez une rubrique de visualisation pour laquelle vous souhaitez créer un effort de rattrapage récurrent.
4. Cliquez sur **Créer un effort de rattrapage**.
   Le modal Créer un effort de rattrapage s'affiche.
5. À la première étape, Détails de l'effort, renseignez les champs requis.

   Dans le champ Description brève, saisissez un texte qui décrit l'effort de rattrapage récurrent qui vous aide à le localiser et à le suivre dans la liste des efforts.

   Dans le champ Description, saisissez plus de texte sur le contexte de l'effort qui vous aide à le localiser facilement dans la liste des efforts de rattrapage. Par exemple, les vulnérabilités Log4J actives.

   a. Dans le champ Nom, saisissez un nom pour votre nouvel effort de rattrapage.
      Par défaut, le nom de la rubrique de surveillance s'affiche.

   b. Dans le champ Description, saisissez un texte qui vous aidera à localiser facilement cet effort de rattrapage à partir de la liste des efforts de rattrapage.

6. Cliquez sur **Suivant**.
   Les détails de la génération de tâches s'affichent.
7. À l'étape 2, Génération de tâches, choisissez une méthode dans la liste pour regrouper les enregistrements dans les tâches de rattrapage que vous générez à partir de cet effort de rattrapage après sa création.
   - Par groupe d'affectation
   - Par groupe d'affectation et élément de configuration
   - Par groupe d'affectation et vulnérabilité
   - Aucune (aucune tâche de rattrapage n'est créée). Utilisez cette méthode si vous souhaitez ajouter des enregistrements manuellement à une tâche de rattrapage pour cet effort. Consultez Créer une tâche de rattrapage sur demande à partir de Effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités.
8. Pour actualiser automatiquement les éléments vulnérables en double, vous devez sélectionner l'option **Actualiser automatiquement les éléments vulnérables en double pour les tâches de rattrapage créées** .
9. Cliquez sur **Suivant**.

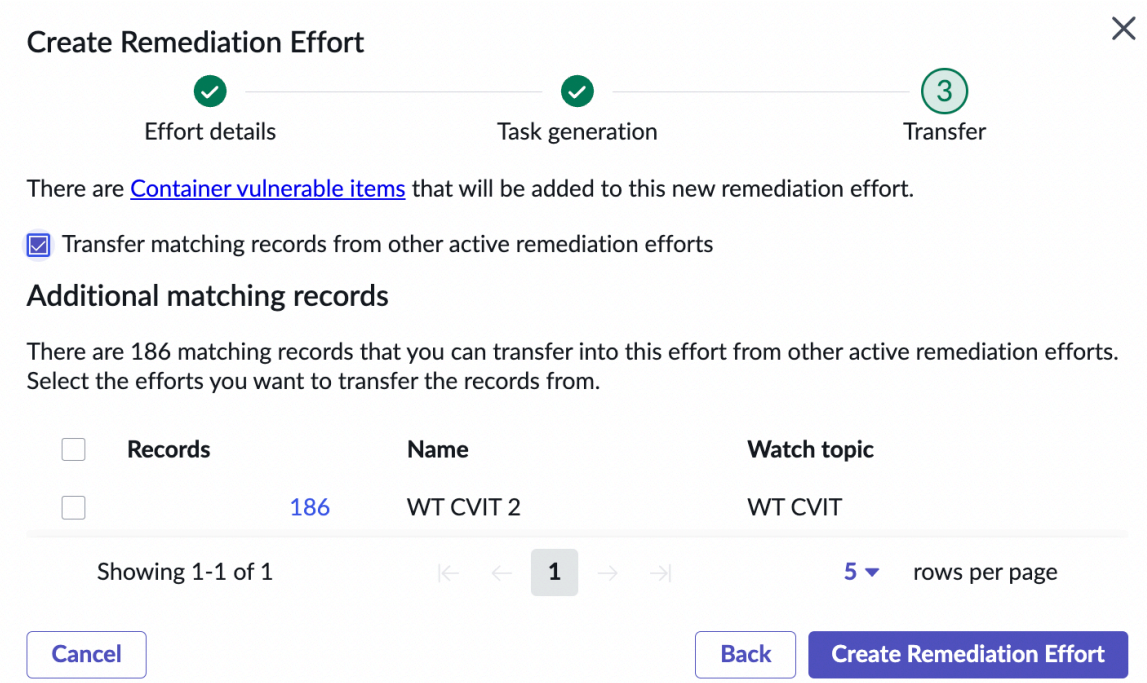
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. À l'étape 3, Transférer, vérifiez combien d'enregistrements seront ajoutés à l'effort de rattrapage et combien d'enregistrements sont disponibles pour le transfert à partir d'autres efforts de rattrapage actifs.
11. Pour transférer des enregistrements à partir d'autres efforts, dans la liste, cochez les cases correspondant aux enregistrements souhaités.

    Cochez la case **Transférer les enregistrements correspondants à partir d'autres efforts de rattrapage actifs** , puis cochez les cases en regard des enregistrements que vous souhaitez transférer à partir d'autres efforts de rattrapage actifs.

Version 18.0 Créer un effort de rattrapage



12. Cliquez sur **Créer un effort de rattrapage**.

    Après quelques instants, le nouvel effort de rattrapage s'affiche. Selon le nombre d'enregistrements, cela peut prendre un certain temps. Un message indique que l'enregistrement est en cours de remplissage.

    Le nouvel effort de rattrapage est créé avec tous les enregistrements disponibles dans la rubrique de surveillance utilisée pour le créer, en plus de tous les enregistrements que vous avez sélectionnés pour le transfert à partir d'efforts existants.

    Si vous sélectionnez des enregistrements à transférer à partir d'un effort existant, et que l'effort existant transfère tous ses enregistrements dans votre nouvel effort, l'effort de rattrapage à partir duquel vous avez déplacé les enregistrements est fermé.

    Remarque : S'il n'y a aucun enregistrement disponible dans la rubrique de surveillance ni aucun enregistrement sélectionné pour le transfert, le bouton **Créer un effort de rattrapage** est désactivé.

    Pour plus d'informations sur l'impact du transfert d'enregistrements sur les tâches de rattrapage associées aux efforts de rattrapage, consultez Transfert d'enregistrements ou Report d'enregistrements.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter un contrôle de compensation à la bibliothèque

En tant que gestionnaire des vulnérabilités ou analyste, ajoutez une liste de contrôles compensatoires à la bibliothèque de contrôles compensatoires dans le Espace de travail du gestionnaire de vulnérabilités, qui peuvent être appliqués pour la réduction des risques liés aux éléments vulnérables de l'hôte et aux tâches de remédiation.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

Certaines commandes compensatoires couramment utilisées sont livrées avec le système de base. Vous pouvez afficher ces contrôles de compensation en accédant à **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Listes** > **Bibliothèques** > **Contrôles de compensation**. Vous pouvez activer ou désactiver ces contrôles de compensation selon vos besoins.

Remarque : La fonctionnalité de contrôles de compensation est disponible uniquement pour les vulnérabilités de l'hôte.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Dans la page Liste, sous Bibliothèques, sélectionnez **Contrôles de compensation**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire Créer des contrôles de compensation.

Champs de formulaire Créer des contrôles de compensation

Champ	Description
Nom	Nom du contrôle de compensation, qui apparaît en tant qu'option dans la liste déroulante **Contrôles de compensation** du modal Demande d'exception.
Description	Informations brèves qui fournissent des détails sur le contrôle compensatoire.
Actif	État du contrôle de compensation. Seuls les contrôles actifs apparaissent dans la liste **déroulante Contrôles de compensation** du modal Demande d'exception.

5. Sélectionnez **Enregistrer**.
6. Dans la liste Contrôles de compensation sous Bibliothèques, sélectionnez le contrôle de compensation souhaité et sélectionnez **Modifier**, activer ou désactiver un contrôle de compensation et cliquez sur **Enregistrer** pour modifier les contrôles de compensation.
   Tous les contrôles compensatoires actifs apparaissent sous forme d'option dans la liste **déroulante Contrôles compensatoires** du modal Demander une exception pour les demandes de réduction des risques.

Que faire ensuite

À partir de la version 21.0 de Réponse aux vulnérabilités, vous pouvez associer des contrôles de compensation à des CVE ou des TPE après avoir ajouté un contrôle de compensation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à la bibliothèque. Pour plus d'informations sur l'association de contrôles compensatoires, reportez-vous à la section Associer des contrôles compensatoires à des CVE ou des TPE pour les demandes de réduction des risques.

Information associée

Comprendre les contrôles compensatoires pour la réduction des risques

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

Associer des contrôles compensatoires à des CVE ou des TPE pour les demandes de réduction des risques

Impact des contrôles compensatoires sur le score de risque et la date d'expiration

Associer des contrôles compensatoires à des CVE ou des TPE pour les demandes de réduction des risques

En tant que gestionnaire ou analyste des vulnérabilités, vous pouvez associer les contrôles compensatoires pertinents à une entrée de vulnérabilité commune (CVE) ou à une entrée tierce (TPE) dans , Espace de travail du gestionnaire de vulnérabilités qui peut être utilisée pour réduire le risque posé par une vulnérabilité.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche

- Si vous n'associez pas de contrôles de compensation à une CVE ou à une TPE, tous les contrôles actifs apparaissent dans le champ Sélectionner les contrôles de compensation du formulaire Demande d'exception.
- Si vous associez un contrôle de compensation à une CVE, ce contrôle de compensation est automatiquement associé au TPE, qui est mappé sur le CVE.

Remarque : La fonctionnalité de contrôles de compensation est disponible uniquement pour les vulnérabilités de l'hôte.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Listes, sous Bibliothèques, ouvrez l'un des éléments suivants pour lequel vous souhaitez associer les contrôles :
   - **CVE** dans la liste CVE.
   - **TPE** dans la liste des TPE.
3. Sélectionnez **Associer des contrôles**.

   Remarque : Le bouton **Associer les contrôles** n'apparaît que lorsque la réduction du risque est activée pour une CVE ou une TPE. En d'autres termes, vous pouvez associer des contrôles compensatoires uniquement lorsque la réduction du risque est activée pour une CVE ou une TPE. Si le bouton **Associer les contrôles** n'est pas visible, sélectionnez **Activer la réduction du risque**.

4. Dans le modal Associer les contrôles, sélectionnez les contrôles de compensation qui peuvent être appliqués aux vulnérabilités associées aux CVE ou TPE pour réduire les risques.
5. Sélectionnez **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les contrôles de compensation associés apparaissent dans l'onglet Contrôles de compensation applicables dans la vue d'enregistrement des CVE et TPE.
- Lorsqu'un propriétaire de rattrapage demande une réduction des risques, ces contrôles de compensation associés apparaissent dans le champ Sélectionner les contrôles de compensation du modal Demande d'exception.

Information associée

Comprendre les contrôles compensatoires pour la réduction des risques

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

Ajouter un contrôle de compensation à la bibliothèque

Impact des contrôles compensatoires sur le score de risque et la date d'expiration

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

En tant que responsable et analyste des vulnérabilités, vous pouvez désactiver ou activer les demandes de réduction des risques pour les vulnérabilités de l'hôte associées à une entrée de vulnérabilité commune (CVE) ou à une entrée tierce (TPE) dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

La réduction du risque pour les CVE et TPE est activée par défaut.

Remarque : La fonctionnalité de contrôles de compensation est disponible uniquement pour les vulnérabilités de l'hôte.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
   Sur la page Listes, sous Bibliothèques, ouvrez l'un des éléments suivants pour lequel vous souhaitez désactiver les demandes de réduction des risques :
   - **CVE** dans la liste CVE.
   - **TPE** de la liste TPE.
2. Sélectionnez **Désactiver la réduction du risque**.
   Le propriétaire du rattrapage ne peut pas demander de réduction du risque pour les éléments vulnérables de l'hôte associés à cette CVE ou TPE. En d'autres termes, la case à cocher Demande de réduction des risques n'apparaît pas lorsque le **motif** est sélectionné en tant que Contrôle d'atténuation en place dans le modal de demande d'exception.
3. Pour activer les demandes de réduction des risques pour les éléments vulnérables de l'hôte, sélectionnez **Activer la réduction des risques**.

Information associée

Comprendre les contrôles compensatoires pour la réduction des risques

Ajouter un contrôle de compensation à la bibliothèque

Associer des contrôles compensatoires à des CVE ou des TPE pour les demandes de réduction des risques

Impact des contrôles compensatoires sur le score de risque et la date d'expiration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyser de nouveau les enregistrements et les tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités

Pour vérifier que vos tâches et enregistrements de rattrapage ont été résolus entre les cycles d'analyse planifiés, lancez de nouvelles analyses à partir de votre ServiceNow AI Platform examen à la demande.

Rôle requis : sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin.

Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, correctifs et autres actions ont correctement corrigé des vulnérabilités spécifiques sur vos éléments de configuration (CI).

Les Rapid7 scanners et Qualys sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Analyser de nouveau** n'est pas disponible.

Pour activer ces scanners, en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin :

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Recherchez le produit de scanner que vous souhaitez activer et cliquez sur l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher Activé.
4. Cliquez sur **Mettre à jour**.

   Le produit que vous avez activé s'affiche dans le champ Source sur les enregistrements d'élément vulnérable et de tâche de rattrapage après la prochaine importation, et **Analyser à nouveau** est disponible en tant qu'action d'interface utilisateur.

La nouvelle analyse est prise en charge pour les enregistrements et les tâches de rattrapage avec les intégrations suivantes dans le Espace de travail du gestionnaire de vulnérabilités. Consultez les rubriques suivantes pour plus d'informations :

- Analyser Rapid7 de nouveau les Réponse aux vulnérabilités éléments vulnérables à partir des espaces de travail
- Analyser Qualys de nouveau les Réponse aux vulnérabilités éléments vulnérables à partir des espaces de travail
- Analyser Tenable.io de nouveau et Tenable.sc les éléments vulnérables à partir des espaces de Réponse aux vulnérabilités travail

Pour lancer de nouvelles analyses dans les enregistrements d'élément Espace de travail du gestionnaire de vulnérabilités vulnérable et de tâche de rattrapage, les enregistrements nécessitent un scanner pris en charge comme source.

Vous préférez peut-être créer une liste filtrée qui affiche les enregistrements selon leur source. Consultez Créer une liste personnalisée des enregistrements un exemple de création de liste.

Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités

Évaluez les affectations, la date cible de rattrapage, les tâches de rattrapage, les exceptions et le score de risque pour un ensemble d'enregistrements (VIT, AVIT, CVIT ou TR) dans le Espace de travail du gestionnaire de vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Avant la version 23.0 de Vulnerability Response, il était nécessaire d'appliquer les règles à tous les enregistrements pour obtenir les dernières affectations, dates cibles de rattrapage, scores de risque et tâches de rattrapage, ce qui était un processus chronophage. À partir de la version 23.0, vous pouvez évaluer et mettre à jour de manière sélective ces propriétés pour des enregistrements spécifiques, réduisant ainsi le temps de traitement. En outre, vous pouvez affiner le processus de rattrapage en fonction de ces propriétés mises à jour. À partir de la version 24.0.6 de Vulnerability Response, vous pouvez évaluer les règles d'exception pour les enregistrements sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, ouvrez la liste Actif ou Tous dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de l'application
   - Éléments vulnérables de conteneurs
   - Résultats des tests de configuration
3. **Facultatif :** Cochez la case des enregistrements souhaités pour mettre à jour uniquement les enregistrements sélectionnés en sélectionnant l'option Éléments sélectionnés dans le modal.
4. Sélectionnez le bouton **Réévaluer** .
5. Dans le modal Réévaluer et mettre à jour les propriétés de rattrapage, sélectionnez les propriétés que vous souhaitez mettre à jour pour les enregistrements sélectionnés.

Champ	Description
Sélection d'enregistrement	○ **Éléments sélectionnés** : met à jour uniquement les enregistrements sélectionnés. ○ **Tous les éléments** : met à jour tous les enregistrements de la liste.
Affectations	Met à jour les affectations dans le champ **Groupe d'affectation** en fonction des dernières règles d'affectation.
Score du risque	Met à jour le score de risque dans le champ de **score de risque** conformément aux dernières règles de score de risque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Tâches de rattrapage	Met à jour les tâches de rattrapage en fonction des dernières règles de tâche de rattrapage.
Exceptions	Met à jour l'état de report des enregistrements en fonction des dernières règles d'exception. Pour en savoir plus sur la façon dont le statut de report des enregistrements est mis à jour, reportez-vous à la section Réévaluation des exceptions pour les enregistrements sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités.
Date de la cible de remédiation	Met à jour la date cible de rattrapage en fonction des dernières règles de cibles de rattrapage.

Remarque : Lorsque vous sélectionnez une propriété, ses propriétés dépendantes sont sélectionnées automatiquement.

6. Sélectionnez **Appliquer**.

Résultats

Les propriétés sont mises à jour pour les enregistrements sélectionnés. Vous pouvez consulter les **notes de travail** des enregistrements pour connaître les valeurs précédentes et les plus récentes des propriétés de rattrapage mises à jour.

Report direct des éléments vulnérables (VIT) par des règles d'exception sans création de tâche de rattrapage

Les règles d'exception sont appliquées directement aux éléments vulnérables (VIT), éliminant ainsi le processus de création d'une tâche de rattrapage. La colonne Règle d'exception automatique est ajoutée à la vue de formulaire, qui remplit la règle d'exception actuelle appliquée sur l'élément vulnérable (VIT)

Approbation de la règle d'exception/Réappliquer :

Une règle d'exception est créée pour un élément vulnérable (VIT) particulier, qui est dans un état **ouvert, en cours d'examen, en attente d'implémentation** initialement. Une fois la règle approuvée, elle est traitée par une tâche planifiée quotidienne et nocturne qui réapplique la règle d'exception.

Lorsque la tâche planifiée s'exécute, au cas où le VIT est différé (reporté) en raison du mappage incorrect du VIT à la règle d'exception, le travail planifié rouvre le VIT pour réappliquer une nouvelle règle d'exception.

Une nouvelle règle avec un ordre d'exécution ultérieur peut également être activée pour remplacer la précédente.

Remarque : La date de fin de report est définie sur 12 mois par défaut et vous pouvez la modifier au besoin à partir de la page des paramètres de configuration de gestion des exceptions. Si vous essayez de sélectionner une date de report postérieure à la date par défaut, le système génère une erreur.

Gestion des règles d'exception annulées ou supprimées :

Si l'ancienne règle d'exception est annulée ou supprimée, elle déclenche une tâche en arrière-plan pour :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Ouvrez tous les VIT associés.
- Passez la règle d'exception à l'état de brouillon lorsque la règle est annulée.
- Appliquez une nouvelle règle d'exception aux VIT. (S'il existe une règle d'exception applicable, le VIT lui sera associé et le statut VIT sera reporté).

Création d'un nouveau VIT (insertion) :

Lorsqu'un nouveau VIT est créé (tel qu'une ingestion), il est automatiquement affecté à la règle d'exception. La nouvelle VIT sera également reportée avec le même raisonnement et jusqu'à la même date, en suivant le même processus que lorsqu'une règle d'exception est annulée.

Un lien cliquable est disponible dans l'espace de travail du gestionnaire de VM pour accéder directement à la règle d'exception, permettant à l'utilisateur de voir quelle règle d'exception affecte un VIT donné.

Utiliser la vue de liste dans le Espace de travail du gestionnaire de vulnérabilités

La vue de liste dans le Espace de travail du gestionnaire de vulnérabilités permet aux gestionnaires et analystes de vulnérabilité et de sécurité de voir la progression du rattrapage sur les enregistrements, d'explorer les enregistrements de Vulnerability Response et d'afficher l'état de leurs demandes d'approbation et exceptions.

Avant de commencer
Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail du gestionnaire de vulnérabilité**.
2. En haut à gauche de l'espace de travail avec la page d'accueil affichée, cliquez sur l'icône **Liste** .
3. **Facultatif :** Cliquez sur **Mes listes** pour créer une liste.
   Pour en savoir plus sur la création d'une liste, reportez-vous à la section Créer une liste personnalisée des enregistrements.
4. Reportez-vous à la table suivante pour connaître les actions que vous pouvez effectuer sur la page Liste.

Action d'interface utilisateur	Description
Ouvrir un effort de rattrapage	Avec **Actif** sélectionné dans la liste **Efforts de rattrapage** , cliquez sur un lien d'effort de rattrapage pour l'ouvrir. Un effort de rattrapage est un ensemble d'enregistrements associés à une rubrique de visualisation. Les enregistrements

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
	répertoriés dans un effort de rattrapage sont statiques. Elles ne sont pas mises à jour par les nouvelles données d'importation ou les modifications que vous apportez aux rubriques de visualisation. Les éléments de liste connexes de l'enregistrement de l'effort de rattrapage vous permettent de visualiser la progression globale du rattrapage et l'état des enregistrements qui lui sont associés. Pour plus de détails et les actions d'interface utilisateur que vous pouvez effectuer à partir d'un effort de rattrapage, reportez-vous à la section Utiliser les enregistrements d'effort de rattrapage.
À gauche de la colonne Numéro avec une liste affichée, passez la souris sur une ligne et cliquez sur la petite icône d'informations **(i)** pour enregistrer un enregistrement.	Les détails relatifs aux enregistrements sont affichés dans le panneau latéral droit de la page. Les détails incluent : ○ Groupe d'affectation ○ Vulnérabilité ○ Affecté à ○ Brève description ○ Description Vous pouvez modifier les champs. Si la case à cocher Actif s'affiche, vous pouvez activer ou désactiver l'enregistrement. Cliquez sur Mettre **à jour** pour enregistrer vos modifications.
Actualiser la liste	Avec l'icône d'actualisation en haut à droite de la page, rechargez la page actuelle.
Rétablir la largeur des colonnes	Cliquez sur l'icône Engrenage pour ajuster la largeur des colonnes de vos listes. Une copie de la liste d'origine est enregistrée sous **Vos listes**.
Copier l'URL de la page affichée	Copiez l'URL pour l'utiliser ailleurs.
Exporter la page	Dans la fenêtre modale, saisissez le fichier et les types de diffusion, puis cliquez sur **Exporter**.
Affinez les filtres pour les données de la page.	Sélectionnez une colonne et développez le menu à trois points verticaux pour afficher les options qui filtrent davantage les données de la colonne. Par exemple, vous préférez peut-être filtrer la colonne Groupe d'affectation de la liste des tâches de rattrapage actives par un groupe d'affectation spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action d'interface utilisateur	Description
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ○ Afficher la correspondance : affiche uniquement les éléments qui correspondent à la cellule sélectionnée dans la colonne. ○ Filtrer : filtre les éléments de la colonne qui correspondent à la cellule sélectionnée dans la colonne.

5. Créez un élément vulnérable d'application à partir de la liste **Actif** ou **Tous** ci-dessous *Application Vulnerable items* en cliquant sur le bouton **Nouveau** en haut à droite.

Créer une liste personnalisée des enregistrements

Vous pouvez créer une liste personnalisée dans le Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sélectionnez l'icône **Liste** , puis cliquez sur **Mes listes**.
3. Sélectionnez **Nouvelle liste**.
4. Dans le modal Nouvelle liste, cliquez sur **Démarrer à partir d'une liste existante** et recherchez une liste existante à utiliser comme modèle dans la liste de choix Liste.
5. Modifiez le nom de la liste.
6. Ajoutez des filtres.
   Par exemple, vous pouvez créer une liste des enregistrements actifs pour un scanner particulier que vous souhaitez surveiller pour les nouvelles analyses. Vous pouvez utiliser les filtres : actif est vrai et source contient (nom de votre scanner).
7. Modifiez les colonnes que vous souhaitez afficher dans votre liste.
8. Cliquez sur **Créer**.
   Votre nouvelle liste s'affiche.
9. Vous pouvez également cliquer sur **Créer votre propre** nom, entrer un nom, puis **sélectionner la source**.
10. Commencez à taper dans le champ et sélectionnez parmi les sources qui s'affichent pour votre nouvelle liste.
11. Cliquez sur **Créer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Votre nouvelle liste s'affiche.

Remarque : Si vous quittez le module de liste, la liste affichée lorsque vous quittez est la liste que vous voyez lorsque vous revenez.

12. Pour supprimer une liste, avec la liste affichée, cliquez sur l'icône d'engrenage en haut à droite de la page.

Créer une tâche de rattrapage manuellement dans le Espace de travail du gestionnaire de vulnérabilités

À partir de la version 25.0.4 de , vous pouvez créer manuellement des tâches de Réponse aux vulnérabilités rattrapage à partir des listes Éléments vulnérables d'hôte, Éléments vulnérables d'applications, Éléments vulnérables de conteneurs et Résultats des tests de configuration sur la page Liste de Espace de travail du gestionnaire de vulnérabilités. Vous pouvez également créer des tâches de rattrapage à partir des listes d'exploration qui s'affichent lorsque vous cliquez sur les visualisations de la page d'accueil.

Avant de commencer

Rôle requis :

- sn_vul.write_all, sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_write_all ou sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.write_all, sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.write ou sn_vulc.admin pour les résultats des tests de configuration (TR)

Pourquoi et quand exécuter cette tâche

La création manuelle de tâches de rattrapage (RT) dans Espace de travail du gestionnaire de vulnérabilités offre un contrôle granulaire sur la gestion des tâches de rattrapage en vous permettant de regrouper les enregistrements (VIT, CVIT, AVIT ou TR) en tâches de rattrapage de manière dynamique et en temps réel.

Vous pouvez créer une tâche de rattrapage manuellement lorsque vous voulez :

- Regrouper les éléments vulnérables par autre fonction que les critères des règles de la tâche de rattrapage. Par exemple, vous pouvez créer des tâches de rattrapage pour un gestionnaire particulier ou pour de nouveaux exploits actifs, tels qu'un ransomware qui inclut différentes vulnérabilités.
- Regrouper les enregistrements dissociés.
- Les règles de tâche de rattrapage sont inactives.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste**.
2. Sur la page Liste, ouvrez la liste **Actif** ou **Tous** dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de l'application
   - Éléments vulnérables de conteneurs
   - Résultats des tests de configuration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. **Facultatif :** Cochez la case des enregistrements que vous souhaitez mettre à jour, puis sélectionnez l'option Éléments sélectionnés dans le champ Sélection d'enregistrement du modal Créer une tâche de rattrapage.
4. Sélectionnez **Créer une tâche de rattrapage**.
5. Renseignez les champs suivants du modal Créer une tâche de rattrapage.

Créer un modal de tâche de rattrapage

Champ	Description
Sélection d'enregistrement	○ **Éléments sélectionnés** : met à jour uniquement les enregistrements sélectionnés. ○ **Tous les éléments** : met à jour tous les enregistrements de la liste.
Description brève	Brève note sur les tâches de rattrapage.
Critères de regroupement	Les choix possibles sont les suivants : ○ **Groupe d'affectation** : les enregistrements avec le même groupe d'affectation sont regroupés en une seule tâche de rattrapage. ○ **Groupe d'affectation et élément de configuration** : les enregistrements avec le même groupe d'affectation et le même élément de configuration sont regroupés en une seule tâche de rattrapage. ○ **Groupe d'affectation et vulnérabilité** : les enregistrements avec le même groupe d'affectation et la même vulnérabilité sont regroupés en une seule tâche de rattrapage. ○ **Groupe d'affectation et cote de risque** : les enregistrements ayant le même groupe d'affectation et la même cote de risque sont regroupés en une seule tâche de rattrapage.
Gestion des enregistrements dans d'autres tâches de remédiation	Les choix possibles sont les suivants : ○ **Ignorer les enregistrements pour les nouvelles tâches de rattrapage** : aucune action n'est effectuée sur les enregistrements qui font partie d'autres tâches de rattrapage. ○ **Déplacer vers les nouvelles tâches de rattrapage** : les enregistrements qui font partie d'autres tâches de rattrapage sont transférés vers les nouvelles tâches de rattrapage. ○ **Conserver les tâches de rattrapage actuelles et nouvelles** : les enregistrements qui font partie d'autres

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	tâches de rattrapage sont conservés dans les anciennes et les nouvelles tâches de rattrapage.

6. Sélectionnez **Créer une tâche de rattrapage**.

Résultats

Les tâches de remédiation sont créées en fonction des critères de regroupement. Une notification par e-mail est envoyée aux propriétaires de rattrapage du groupe d'affectation, les informant qu'une tâche de rattrapage a été créée et affectée à leur groupe. Pour obtenir des exemples sur la façon dont les tâches de rattrapage sont créées en fonction des critères de regroupement, reportez-vous à la section Exemples de création de tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT.

Activer ou désactiver l'importation de résultats de tests pour un Qualys groupe de tests

À partir de la version 23.0 de Réponse aux vulnérabilités, contrôlez l'importation des résultats des tests pour les tests d'un groupe de Qualys tests à l'aide du bouton **Activer/désactiver l'importation** , disponible dans la vue d'enregistrement du groupe de tests.

Avant de commencer

Rôle requis : sn_vulc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Listes**.
2. Dans les bibliothèques, sous la liste Groupes de tests, ouvrez un groupe de Qualys tests dans la vue d'enregistrement.
3. Désactivez l'importation des résultats des tests associés à un groupe de Qualys tests en sélectionnant le bouton **Désactiver l'importation** .
   À partir de l'ingestion de données à venir, les résultats des tests ne sont pas importés pour le groupe de Qualys tests.
   La valeur du champ **Est une importation désactivée** devient *vrai*.
4. **Facultatif :** Activez l'importation des résultats des tests en sélectionnant le bouton **Activer l'importation** .

Modifier la gravité d'une CVE ou d'une TPE

En tant que responsable des vulnérabilités ou analyste, vous pouvez modifier le niveau de gravité de l'entrée de vulnérabilité commune (CVE) ou de l'entrée tierce (TPE) dans l'espace de travail du gestionnaire de vulnérabilité.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager, sn_vul.app_developer pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Listes** > **Bibliothèques**.
2. Ouvrez l'entrée appropriée :
   - **CVE (NVD)** : pour modifier la gravité d'une CVE.
   - **TPE** : pour modifier la gravité d'un TPE.
3. Sélectionnez **Modifier la gravité** dans l'icône Actions **supplémentaires**
4. Sélectionnez le nouveau niveau de gravité dans la liste déroulante.
5. Fournissez une justification pour votre mise à jour.
6. Sélectionnez **Soumettre**.

Remarque :

- Vous pouvez revenir à la gravité source d'origine à l'aide de l'option **Réinitialiser la gravité** du menu **Actions supplémentaires** . Cette option s'affiche uniquement après avoir modifié la gravité.
- Le champ **Gravité modifiée** s'affiche uniquement lorsque vous modifiez la gravité de la source. Si vous réinitialisez la valeur d'origine, le champ est supprimé.
- Le système utilisera la **gravité modifiée** pour les calculs de risque à partir de la prochaine tâche planifiée. Si la gravité est réinitialisée, la gravité source d'origine est appliquée à la place.

Approuver ou rejeter les demandes dans le Espace de travail du gestionnaire de vulnérabilités

Approuvez ou rejetez les demandes soumises par les propriétaires de rattrapages.

Avant de commencer

Rôles requis :

Rôles d'approbateur requis pour diverses demandes d'approbation

Type d'approbation	Niveaux d'approbation requis	Rôles d'approbateur	Informations supplémentaires
Approbations de faux positifs	Un	• Rôle granulaire sn_vul.false_positive_approver pour les éléments vulnérables (VIT). • Rôle sn_vul.app_false_positive_approver pour les éléments vulnérables de l'application (AVIT) • Rôle sn_vul_container.false_positive_approver pour les éléments vulnérables de conteneur (CVIT)	-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles d’approbateur requis pour diverses demandes d’approbation (suite)

Type d'approbation	Niveaux d’approbation requis	Rôles d'approbateur	Informations supplémentaires
		• sn_vulc.false_positive_approver pour les résultats des tests de configuration Ou Les approbateurs doivent faire partie du groupe d’utilisateurs Approbateurs de faux positifs.	
Approbations d’exception (reports)	Deux	• Un approbateur est requis dans le groupe Approbateur - Niveau 1 • Un approbateur est requis dans le groupe d’approbateurs de niveau 2	Une demande d’exception pour un enregistrement ou une tâche de rattrapage est approuvée à l’aide d’un workflow d’approbation à deux niveaux par défaut. La demande d’exception nécessite deux niveaux d’approbateurs. Une fois la demande approuvée par l’approbateur de niveau 1, elle est envoyée à l’approbateur de deuxième niveau et est ensuite visible dans la file d’attente de l’approbateur 2.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles d’approbateur requis pour diverses demandes d’approbation (suite)

Type d'approbation	Niveaux d’approbation requis	Rôles d'approbateur	Informations supplémentaires
Annuler l’affectation des approbations	Un approbateur est requis dans le groupe Approbateur – Niveau 1	• sn_vul.unassign_appr pour AVIT et VIT • sn_vul_container.unas pour CVIT • sn_vulc.unassign_app pour les problèmes de configuration (CI)	**Remarque :** Par défaut, une configuration d’approbation est fournie et un groupe d’approbation de désaffectation est créé. Les utilisateurs (Annuler l’affectation de l’approbateur : niveau 1) de ce groupe peuvent approuver la demande. Ce groupe contient un rôle d’approbateur de désaffectation, sn_vul.unassign_approver, par défaut. Vous pouvez modifier ou créer un nouveau groupe et mettre à jour la configuration de l’approbation. Pour configurer des règles d’approbation, accédez au module Règles d’approbation respectif, sélectionnez l’une des règles d’approbation suivantes, puis accédez à la configuration de l’approbation dans l’onglet **Configurations d’approbation** : • *Vulnerable item field change request* pour un élément vulnérable. • *Vulnerability field*

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles d'approbateur requis pour diverses demandes d'approbation (suite)

Type d'approbation	Niveaux d'approbation requis	Rôles d'approbateur	Informations supplémentaires
Approbations de réduction des risques	Deux	• Un approbateur est requis dans le groupe Approbateur - Niveau 1 • Un approbateur est requis dans le groupe d'approbateurs de niveau 2	Le flux d'approbation pour la réduction du risque est le même que pour les approbations d'exception (reports).

Consultez Réponse aux vulnérabilités Profils et rôles granulaires et Affecter les rôles de personnage à l'aide de l'assistant Réponse aux vulnérabilités de configuration pour plus d'informations sur l'affectation de rôles de profil aux utilisateurs et d'utilisateurs à des groupes.

Remarque : Ajoutez des utilisateurs aux groupes d'approbation avant d'envoyer des demandes d'approbation. Si vous créez des demandes avant d'ajouter des utilisateurs aux groupes d'approbation, les demandes peuvent ne pas être visibles par les utilisateurs qui ont l'autorisation d'approbation.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
   Si un approbateur n'a pas accès à l'espace de travail, les approbations peuvent être traitées à **Réponse aux vulnérabilités** > **Mes approbations** dans l'environnement classique.
2. Sélectionnez l'icône de vue de liste ( ).
   La page Liste s'affiche.
3. Dans la liste filtrée des approbations, sélectionnez **Mes affectations**.
4. Localisez la demande que vous souhaitez traiter, puis sélectionnez le lien dans la colonne État.
   L'enregistrement de l'approbation de changement d'état de la vulnérabilité (VCA#) s'affiche.
5. Choisissez l'une des options suivantes pour approuver ou rejeter la demande.

Option	Description
Cliquez sur l'onglet Détails, saisissez du texte dans le champ Commentaires, puis cliquez sur Rejeter	○ Un message s'affiche, indiquant que l'enregistrement Approbation du chan–gement d'état de la vulnérabilité a été rejeté. ○ L'état de l'enregistrement Approbation du changement d'état de la vulnérabilité passe à Rejeté. ○ L'état de la tâche de rattrapage ou de l'enregistrement reste le même.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	○ L'enregistrement d'approbation de changement d'état de vulnérabilité n'est plus affiché dans votre vue de liste Approbations dans l'espace de travail.
Dans les onglets Demande ou Détails , cliquez sur Approuver	○ Un message s'affiche indiquant que l'enregistrement d'approbation de changement d'état de la vulnérabilité est approuvé. ○ L'état de la tâche de rattrapage ou de l'enregistrement passe à Différé. ○ Les enregistrements actifs sur la transition des tâches de rattrapage vers Différé. ○ L'enregistrement de l'approbation du changement d'état de la vulnérabilité n'est plus affiché dans votre vue de liste Approbations.

Configurer des notifications par e-mail dans les Réponse aux vulnérabilités espaces de travail

Identifiez les utilisateurs pour les rappels automatiques par e-mail envoyés aux utilisateurs du groupe d'utilisateurs Propriétaire de rattrapage.

Avant de commencer

Rôle requis : admin

Cette fonctionnalité génère automatiquement une synthèse d'e-mail pour les utilisateurs du groupe d'utilisateurs Propriétaire de rattrapage. Ajoutez tous les utilisateurs pour lesquels vous souhaitez recevoir des notifications par e-mail, comme décrit dans Utiliser la synthèse d'e-mail dans les espaces de travail Réponse aux vulnérabilités.

Vérifiez que les utilisateurs ont une adresse e-mail active saisie dans leur enregistrement utilisateur et que vous les avez ajoutés au groupe d'utilisateurs Propriétaire de rattrapage.

Si vous souhaitez modifier la fréquence de livraison, le jour ou l'heure des e-mails, ou désactiver la fonctionnalité, procédez comme suit.

Procédure

1. Accédez à la **Tous** > **Travaux planifiés**.
2. Localisez **Générer une synthèse de rattrapage** et cliquez dessus pour ouvrir l'enregistrement.

   Vous préférez peut-être laisser les champs dans leurs paramètres par défaut jusqu'à ce que vous vérifiiez que les notifications sont envoyées. Par défaut, les e-mails sont envoyés chaque semaine, le lundi matin à 9h00 dans le fuseau horaire de l'instance qui exécute la tâche.

3. Modifiez les champs dans le formulaire.
   Pour plus d'informations sur les champs de formulaire, consultez Générer des champs de formulaire de synthèse de rattrapage.
4. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Si vous avez vérifié que toutes les informations répertoriées précédemment sont correctes et que vous avez des utilisateurs dans le groupe d'utilisateurs Propriétaire de rattrapage, mais que les e-mails ne sont pas envoyés comme prévu, vérifiez qu'il existe des canaux activés pour recevoir des notifications par e-mail. Consultez Créer des canaux de notification .

Rattrapage des éléments vulnérables et résultats des tests dans le Espace de travail de Security Exposure Management

Dans , Espace de travail du gestionnaire de vulnérabilités vous pouvez corriger les éléments vulnérables et les résultats des tests dans une rubrique de visualisation en définissant une condition et vous pouvez suivre leur progression en créant des efforts de rattrapage.

Utilisation de la modification en bloc dans le Espace de travail du gestionnaire de vulnérabilités

Dans , Espace de travail du gestionnaire de vulnérabilités vous pouvez mettre à jour l'état des enregistrements, demander des exceptions et des faux positifs, et affecter des enregistrements à un groupe d'affectation avec plusieurs éléments vulnérables (VIT, AVIT ou CVIT) simultanément à l'aide de la fonctionnalité de modification en bloc.

La fonctionnalité de modification en bloc est disponible pour :

- éléments vulnérables d'hôte (VIT) à partir de la version 21.0 de Réponse aux vulnérabilités.
- éléments vulnérables de l'application (AVIT) et éléments vulnérables de conteneur (CVIT) à partir de la version 22.0 du Réponse aux vulnérabilités.
- résultats des tests à partir de la version 23.0 de Réponse aux vulnérabilités.

Mettre à jour l'état des enregistrements en bloc dans le Espace de travail du gestionnaire de vulnérabilités

Mettez à jour l'état de plusieurs enregistrements (VIT, AVIT ou CVIT) simultanément en fonction de leur progression dans le rattrapage à l'aide de la fonction de modification en bloc du Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste**.
2. Sur la page Liste, ouvrez la liste Actif ou Tous dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
3. Effectuez l'une des actions suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Uniquement les éléments sélectionnés** dans le champ **Sélection d'enregistrement** .
- Appliquez des filtres si vous souhaitez utiliser l'option de **filtre Tous les éléments vulnérables qui correspondent** dans le champ **Sélection d'enregistrement** .

4. Sélectionnez le bouton **Modifier en bloc** .
5. Sur la fenêtre modale Modifier en bloc, renseignez les champs suivants pour mettre à jour l'état des enregistrements.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ○ Éléments sélectionnés uniquement : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ○ Tous les éléments vulnérables qui correspondent au filtre : Sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ○ Tâche de rattrapage : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ○ Entrée de vulnérabilité : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une entrée vulnérable commune (CVE), puis sélectionnez la CVE dans le champ **Entrée de vulnérabilité** . **Remarque :** Les enregistrements avec un CI non valide ou CI désactivé ne sont pas mis à jour.
État	Changement de **l'état** dans l'enregistrement. Les choix possibles sont les suivants : ○ Ne pas mettre à jour ○ Ouvert ○ En cours d'examen ○ En attente d'implémentation ○ Différé Pour plus d'informations, consultezDemander une exception en bloc dans l'espace de travail du gestionnaire de vulnérabilité. ○ Fermé Pour plus d'informations, voir Modifier en bloc le faux positif dans l'espace de travail du gestionnaire de vulnérabilité ○ Résolu

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Seuls les enregistrements pour lesquels la transition d'état est valide sont mis à jour.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Sélectionnez **Modifier**.

   Une tâche de modification en bloc asynchrone met à jour les enregistrements sélectionnés.

Modifier en bloc les éléments vulnérables de l'hôte avec des correctifs et des solutions

Recommandez un correctif ou une solution pour plusieurs éléments vulnérables d'hôte simultanément à l'aide de la fonction de modification en bloc du Espace de travail du gestionnaire de vulnérabilités.

Avant de commencer

Rôle requis : sn_vul.vulnerability_analyst, sn_vul.vulnerability_admin et tout rôle ayant un rôle granulaire sn_vul.bulk_edit.

Pourquoi et quand exécuter cette tâche

Dans la fenêtre modale Modifier en bloc, tout en ajoutant une solution et un correctif préférés, vous pouvez également annuler l'affectation ou affecter plusieurs éléments vulnérables d'hôte (VIT) à un groupe d'affectation simultanément.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.

   Remarque : Les enregistrements sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.

2. Sur la page Liste, sous Éléments vulnérables d'hôte, ouvrez la liste Actif ou Tous.
3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Uniquement les éléments sélectionnés** dans le champ **Sélection d'enregistrement** .
   - Appliquez des filtres si vous souhaitez utiliser l'option de **filtre Tous les éléments vulnérables qui correspondent** dans le champ **Sélection d'enregistrement** .
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Uniquement les éléments sélectionnés** dans le champ Sélection d'enregistrement de la fenêtre modale Modifier en bloc.
   - Appliquez des filtres si vous souhaitez utiliser l'option de **filtre Tous les éléments vulnérables qui correspondent au filtre** dans le champ Sélection d'enregistrement de la fenêtre modale Modifier en bloc.
4. Sélectionnez le bouton **Modifier en bloc** .
5. Sur la fenêtre modale Modifier en bloc, renseignez les champs pour recommander un correctif ou une solution pour plusieurs éléments vulnérables d'hôte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ Éléments sélectionnés uniquement : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ Tous les éléments vulnérables qui correspondent au filtre : Sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ Tâche de rattrapage : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ Entrée de vulnérabilité : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une entrée vulnérable commune (CVE), puis sélectionnez la CVE dans le champ **Entrée de vulnérabilité** . **Remarque :** ◦ Les enregistrements avec un CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements (VIT) à l'état Ouvert, En cours d'examen ou En attente d'implémentation sont mis à jour.
État	Changement pour **l'état** des éléments vulnérables de l'hôte. Vous pouvez ajouter la solution et le correctif préférés uniquement lorsque vous choisissez les états suivants. ◦ Ne pas mettre à jour ◦ Ouvert ◦ En cours d'examen ◦ En attente d'implémentation
Solution privilégiée	Solution ciblée pour corriger tous les éléments vulnérables sélectionnés pour une modification en bloc. Sélectionnez le changement pour le champ **Solution privilégiée** dans l'élément vulnérable. Les choix proviennent d'une liste de recherche de solutions privilégiées disponibles pour les VIT sélectionnés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ◦ L'ensemble des solutions privilégiées disponibles est une intersection de toutes les solutions potentielles des vulnérabilités dans tous les VIT sélectionnés. ◦ Lors de la sélection de **Sélection d'enregistrement** > **Entrée de vulnérabilité** pour une modification en bloc, tous les VIT pour la vulnérabilité seront définis sur la solution privilégiée sélectionnée. **Remarque :** Cette opération ne définit pas la **solution privilégiée** au niveau d'entrée de vulnérabilité. Définir la **solution privilégiée** au niveau d'entrée de vulnérabilité définirait la **solution privilégiée** pour tous les nouveaux VIT à l'avenir. La modification en bloc ne modifie que l'ensemble actuel des VIT. ◦ Les vulnérabilités distinctes dans les critères de sélection sont limitées à 500. S'il existe plus de 500 vulnérabilités distinctes, un message d'avertissement s'affiche vous demandant de sélectionner des VIT avec des critères différents pour définir la **solution privilégiée**. ◦ Le nombre total de solutions pouvant être affichées dans la liste de recherche est limité à 170. S'il y a plus de 170 solutions, un message d'avertissement s'affiche. La valeur mise à jour est affichée dans la vue de liste Élément vulnérable.
Correctif préféré	Correctif destiné à corriger tous les éléments de vulnérabilité sélectionnés pour une modification en bloc. **Remarque :** ◦ Vous devez installer Patch Orchestration pour afficher la liste des correctifs préférés. ◦ L'ensemble des correctifs préférés disponibles est une intersection de tous les correctifs potentiels dans tous les VIT sélectionnés. ◦ Les vulnérabilités distinctes dans les critères de sélection sont limitées à 500. S'il existe plus de 500 vulnérabilités distinctes, un message d'avertissement s'affiche vous demandant de sélectionner des VIT avec des critères différents pour définir le **correctif préféré**. ◦ Le nombre total de correctifs pouvant être affichés dans la liste de recherche est limité à 170. S'il y a plus de 170 correctifs, un message d'avertissement s'affiche.
Annuler l'affectation	Tous les éléments sélectionnés sont désaffectés pour le groupe d'affectation et le propriétaire de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ◦ Ce champ s'affiche lorsque vous sélectionnez l'état Ne pas mettre à jour. ◦ Lorsque vous annulez l'affectation d'enregistrements, une tâche de rattrapage est créée et envoyée pour approbation. Pour plus d'informations, voir Supprimer les affectations pour les éléments vulnérables d'hôte en bloc
Groupe d'affectation	Groupe d'affectation pour les enregistrements. Tous les groupes d'affectation actifs apparaissent dans ce champ. **Remarque :** Ce champ est désactivé lorsque vous cochez la case Annuler l'affectation.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Sélectionnez **Modifier**.

Résultats
Une tâche de modification en bloc asynchrone met à jour les éléments vulnérables de l'hôte (VIT) sélectionnés. La solution et le correctif préférés sont ajoutés aux éléments vulnérables de l'hôte (VIT) appropriés. Ouvrez un élément vulnérable d'hôte et affichez la solution et le correctif préférés dans la section Rattrapage de l'onglet Détails.

Affecter des enregistrements à un groupe d'affectation en bloc

Affectez simultanément plusieurs enregistrements (VIT, AVIT, CVIT ou TR) à un groupe d'affectation à l'aide de la fonction de modification en bloc du Espace de travail du gestionnaire de vulnérabilités fichier .

Avant de commencer
Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste**.
2. Sur la page Liste, ouvrez la liste Actif ou Tous dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
   - Résultats des tests de configuration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Uniquement les éléments sélectionnés** dans le champ de sélection d'enregistrement .
   - Appliquez des filtres si vous souhaitez utiliser l'option de **filtre Tous les enregistrements qui correspondent dans** le champ de sélection d'enregistrement .
4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs du formulaire pour affecter les enregistrements à un groupe d'affectation.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ *Éléments sélectionnés uniquement* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ *Tous les enregistrements qui correspondent au filtre* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ *Tâche de rattrapage* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ *Entrée de vulnérabilité* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une vulnérabilité, puis sélectionnez une CVE ou une TPE dans le champ **Entrée de vulnérabilité**. **Remarque :** Ce champ s'affiche pour les éléments vulnérables d'hôte, d'applications et de conteneurs. ◦ *Test de configuration* : sélectionnez cette option si vous souhaitez mettre à jour les résultats des tests spécifiques à un test, puis sélectionnez un test dans le champ **Test de configuration** . **Remarque :** Cette option s'affiche uniquement pour les résultats des tests de configuration. **Remarque :** ◦ Les enregistrements avec un CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements à l'état Ouvert, En cours d'examen, En attente d'implémentation ou Différé sont mis à jour.
Groupe d'affectation	Groupe d'affectation pour les enregistrements. Tous les groupes d'affectation actifs apparaissent dans ce champ. **Remarque :** Ce champ est désactivé lorsque vous cochez la case Annuler l'affectation pour les VIT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.

Résultats
Ouvrez un enregistrement dont vous avez mis à jour le groupe d'affectation et accédez à l'onglet Vue d'ensemble. Le groupe d'utilisateurs auquel l'enregistrement est affecté apparaît dans le champ **Groupe d'affectation** .

Supprimer les affectations pour les éléments vulnérables d'hôte en bloc

Retirez-vous ou vos groupes des champs **Affecté à** et **Groupe d'affectation** sur les éléments vulnérables d'hôte (VIT) ou les tâches de rattrapage (VUL) si vous déterminez que les enregistrements ne se trouvent pas dans votre périmètre pour le rattrapage, ou si vous pensez que les enregistrements vous ont été incorrectement affectés à vous ou à vos groupes.

Avant de commencer
Rôle requis : sn_vul.vulnerability_analyst et sn_vul.vulnerability_admin

Pourquoi et quand exécuter cette tâche
La fonctionnalité Annuler l'affectation s'applique aux enregistrements dont l'état n'est pas Fermé ou Résolu. Lorsque vous supprimez les affectations pour les éléments vulnérables d'hôte à l'aide de la fonctionnalité de modification en bloc, seuls les enregistrements pertinents sont mis à jour.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, sous Éléments vulnérables d'hôte, ouvrez la liste Actif ou Tous.
3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option **Uniquement les éléments sélectionnés** dans le champ Sélection d'enregistrement .
   - Appliquez des filtres si vous souhaitez utiliser l'option de **filtre Tous les éléments vulnérables qui correspondent** dans le champ Sélection d'enregistrement .
4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs du formulaire pour supprimer les affectations en bloc.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ○ Éléments sélectionnés uniquement : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ○ Tous les éléments vulnérables qui correspondent au filtre : Sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ○ Tâche de rattrapage : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ○ Entrée de vulnérabilité : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une entrée vulnérable commune (CVE), puis sélectionnez la CVE dans le champ **Entrée de vulnérabilité** . **Remarque :** ○ Les enregistrements avec un CI non valide ou CI désactivé ne sont pas mis à jour. ○ Seuls les enregistrements à l'état Ouvert, En cours d'examen, En attente d'implémentation ou Différé sont mis à jour.
État	Sélectionnez l'état Ne pas mettre à jour.
Annuler l'affectation	L'affectation de tous les éléments vulnérables sélectionnés est annulée au groupe d'affectation et au propriétaire du rattrapage. **Remarque :** ○ Ce champ s'affiche lorsque vous sélectionnez l'état Ne pas mettre à jour. ○ Lorsque vous annulez l'affectation d'enregistrements, une tâche de rattrapage est créée et envoyée pour approbation.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.
   Une tâche de rattrapage est créée avec les éléments vulnérables de l'hôte (VIT) sélectionnés.

   Votre demande est soumise pour approbation et l'approbateur reçoit une notification par e-mail concernant votre demande.

   L'état des éléments vulnérables de l'hôte (VIT) et de la tâche de rattrapage (VUL) passe à l'état En cours de révision. Si une tâche de rattrapage est mise à jour avec cette fonctionnalité, les champs **Affecté à** et **Groupe d'affectation** de tous ses VIT associés sont également effacés lors de l'approbation de votre demande.

Résultats

Dans l'espace de travail du gestionnaire de vulnérabilités, sur la page Liste, accédez à **Demandes d'exception** > **Tous** et ouvrez l'enregistrement d'approbation de changement d'état correspondant (VCA#) et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Résultat
Approuvé	Les champs **Affecté à** et **Groupe d'affectation** de tous les éléments vulnérables d'hôte sont effacés.
Rejeté	Les champs **Affecté à** et **Groupe d'affectation** de tous les éléments vulnérables d'hôte ne sont pas mis à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le **flux d'activité** d'un enregistrement ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de votre demande.

Demander une exception en bloc dans l'espace de travail du gestionnaire de vulnérabilité

Demander une exception pour plusieurs enregistrements (VIT, AVIT, CVIT ou TR) simultanément à l'aide de la fonctionnalité de modification en bloc au lieu de sélectionner manuellement chaque enregistrement.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Lorsque vous demandez une exception pour un ou plusieurs enregistrements à partir de la fenêtre modale Modifier en bloc, une tâche de rattrapage est créée avec les enregistrements sélectionnés.

Remarque : Les éléments vulnérables de l'application (AVIT) des scanners dont le paramètre **Gérer les exceptions dans ServiceNow** est défini sur faux ne sont pas mis à jour.

- Si vous sélectionnez des AVIT à partir de différents scanners, certains avec le paramètre **Gérer les exceptions dans ServiceNow** défini sur vrai et d'autres sur faux, les AVIT liés aux scanners avec le paramètre **Gérer les exceptions dans ServiceNow** défini sur faux ne sont pas mis à jour.
- Si vous sélectionnez AVIT à partir des scanners uniquement avec le paramètre **Gérer les exceptions dans ServiceNow** défini sur faux, l'option *Différer* n'apparaît pas dans le champ **État** de la fenêtre modale Modifier en bloc.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité**.
2. Sur la page Liste, ouvrez la liste Actif ou Tous dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
   - Résultats des tests de configuration
3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option *Uniquement les éléments sélectionnés* dans le champ de sélection d'enregistrement .
   - Appliquez des filtres si vous souhaitez utiliser l'option de *filtre Tous les enregistrements qui correspondent dans* le champ de sélection d'enregistrement .
4. Sélectionnez le bouton **Modifier en bloc** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Renseignez les champs suivants sur le formulaire pour demander une exception pour plusieurs enregistrements (VIT, AVIT, CVIT ou TR) simultanément.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ○ *Éléments sélectionnés uniquement* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ○ *Tous les enregistrements qui correspondent au filtre* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ○ *Tâche de rattrapage* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ○ *Entrée de vulnérabilité* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une vulnérabilité , puis sélectionnez un CVE ou un TPE dans le champ **Entrée de vulnérabilité** . **Remarque :** Ce champ s'affiche pour les éléments vulnérables d'hôte, d'applications et de conteneurs. ○ *Test de configuration* : sélectionnez cette option si vous souhaitez mettre à jour les résultats des tests spécifiques à un test, puis sélectionnez un test dans le champ **Test de configuration** . **Remarque :** Cette option s'affiche uniquement pour les résultats des tests de configuration. **Remarque :** ○ Les enregistrements avec un CI non valide ou CI désactivé ne sont pas mis à jour. ○ Seuls les enregistrements à l'état Ouvert, En cours d'examen ou En attente d'implémentation sont mis à jour.
État	Sélectionnez l'état *Différé* pour demander une exception pour les enregistrements sélectionnés. **Remarque :** ○ Lorsque vous sélectionnez cette option, les champs Motif, Description brève, Jusqu'à et Informations supplémentaires s'affichent. ○ Lorsque vous différez des enregistrements, une tâche de rattrapage est créée et cette tâche est envoyée pour approbation.
Motif	Motif du report des enregistrements :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre **Remarque :** Le champ **Motif** s'affiche lorsque vous sélectionnez l'état Différé.
Description brève	Brève note décrivant les motifs de la demande de report. Ces informations sont reflétées dans le champ **Description** de la tâche de rattrapage créée pour une demande de report. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé et Fermé-Faux positif.
Jusqu'à	Date jusqu'à laquelle l'enregistrement reste reporté. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé.
Informations supplémentaires	Toute autre information nécessaire. Ces informations sont reflétées dans le champ Informations supplémentaires de l'onglet Vue d'ensemble de la tâche de rattrapage créée pour les demandes de report et de faux positifs fermés. Si votre demande de report est approuvée, ces informations supplémentaires apparaissent sous forme de notes de report pour VIT et la tâche de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé et Fermé-Faux positif.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.
7. Dans la fenêtre modale Répondre au questionnaire, répondez aux questions et cliquez sur **Soumettre**.

Une tâche de rattrapage contenant les enregistrements que vous avez sélectionnés est créée. Votre demande est soumise pour approbation et l'état des enregistrements passe à En cours de révision.

Remarque : Le modal **Répondre au questionnaire** s'affiche uniquement lorsque le questionnaire est activé pour les demandes d'exception dans le formulaire Gestion des exceptions. Pour plus d'informations sur la configuration d'un questionnaire pour les demandes d'exception, reportez-vous à la rubrique Configurer la gestion des exceptions pour Réponse aux vulnérabilités, Configurer la gestion des exceptions pour Réponse aux vulnérabilités des applications et Configurer la gestion des exceptions pour Réponse aux vulnérabilités pour conteneurs, et .Conformité de la configuration Vue d'ensemble de la gestion des exceptions

L'approbateur reçoit une notification par e-mail concernant votre demande.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Dans l'espace de travail du gestionnaire de vulnérabilités, sur la page Liste, accédez à **Exceptions** > **Tous**, ouvrez l'enregistrement d'approbation de changement d'état correspondant (VCA#) et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Résultat
Approuvé	L'état de la tâche de rattrapage passe à Différé avec le motif donné comme sous-état. L'état et le motif sont affichés dans les dossiers.
Rejeté	L'état de la tâche de rattrapage et de ses enregistrements ne change pas.

Dans le **flux d'activité** d'un enregistrement ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de votre demande.

Modifier en bloc le faux positif dans l'espace de travail du gestionnaire de vulnérabilité

Marquez un ou plusieurs enregistrements (VIT, AVIT, CVIT ou TR) comme faux positifs en utilisant simultanément la fonctionnalité de modification en bloc à partir de l'espace de travail Responsable des vulnérabilités au lieu de sélectionner manuellement chaque élément.

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Lorsque vous émettez une demande de faux positif pour un ou plusieurs enregistrements à partir de la fenêtre modale Modifier en bloc, une tâche de rattrapage est créée avec les enregistrements sélectionnés.

Remarque : Lorsque vous émettez une demande de faux positif pour les éléments vulnérables de l'application (AVIT) à l'aide de la fonctionnalité de modification en bloc, les AVIT des scanners dont le paramètre **Gérer les faux positifs avec ServiceNow** est défini sur faux ne sont pas mis à jour.

- Si vous sélectionnez les AVIT à partir de différents scanners, certains dont le paramètre **Gérer les faux positifs avec ServiceNow** est défini sur vrai et d'autres sur faux, les AVIT liés aux scanners dont le paramètre **Gérer les faux positifs avec ServiceNow** est défini sur faux ne sont pas mis à jour.
- Si vous sélectionnez AVIT à partir des scanners uniquement avec le paramètre **Gérer les faux positifs avec ServiceNow** défini sur faux, l'option *Faux positif* n'apparaît pas dans le champ **Motif** de la fenêtre modale Modifier en bloc.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste**.

   Remarque : Les enregistrements sélectionnés doivent être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.

2. Sur la page Liste, ouvrez la liste Actif ou Tous dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
   - Résultats des tests de configuration
3. Effectuez l'une des actions suivantes :
   - Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option *Uniquement les éléments sélectionnés* dans le champ de **sélection d'enregistrement** .
   - Appliquez des filtres si vous souhaitez utiliser l'option de *filtre Tous les enregistrements qui correspondent dans* le champ **de sélection d'enregistrement** .
4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs du formulaire pour demander un faux positif pour plusieurs enregistrements.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ○ *Éléments sélectionnés uniquement* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ○ *Tous les enregistrements qui correspondent au filtre* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ○ *Tâche de rattrapage* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ○ *Entrée de vulnérabilité* : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une vulnérabilité , puis sélectionnez un CVE ou un TPE dans le champ **Entrée de vulnérabilité** . **Remarque :** Ce champ s'affiche pour les éléments vulnérables d'hôte, d'applications et de conteneurs. ○ *Test de configuration* : sélectionnez cette option si vous souhaitez mettre à jour les résultats des tests spécifiques à un test, puis sélectionnez un test dans le champ **Test de configuration** . **Remarque :** Cette option s'affiche uniquement pour les résultats des tests de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ◦ Les enregistrements avec un CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements à l'état Ouvert, En cours d'examen ou En attente d'implémentation sont mis à jour.
État	Sélectionnez l'état **Fermé** .
Motif	Sélectionnez le motif comme faux positif. **Remarque :** ◦ Lorsque vous sélectionnez cette option, les champs Brève description et Informations supplémentaires s'affichent. ◦ Une tâche de rattrapage est créée lorsque vous marquez les enregistrements comme faux positifs et que cette tâche est envoyée pour approbation. **Remarque :** Le champ **Motif** s'affiche lorsque vous sélectionnez l'état Différé ou Fermé.
Description brève	Brève note décrivant les raisons de la demande de faux positif fermé. Ces informations sont reflétées dans le champ **Description** de la tâche de rattrapage créée pour une demande de faux positif fermé. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé ou Fermé-Faux positif.
Informations supplémentaires	Toute autre information nécessaire. Ces informations sont reflétées dans le champ Informations supplémentaires de l'onglet Vue d'ensemble de la tâche de rattrapage créée pour la demande de faux positif fermé. Si votre demande de faux positif est approuvée, ces informations supplémentaires apparaissent sous forme de notes pour la VIT et la tâche de rattrapage. **Remarque :** Ce champ s'affiche lorsque vous sélectionnez l'état Différé ou Fermé-Faux positif.
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.
7. Dans la fenêtre modale Répondre au questionnaire, répondez aux questions et sélectionnez **Soumettre**. Une tâche de rattrapage est créée avec les enregistrements sélectionnés. Votre demande est soumise pour approbation et l'état de la tâche de rattrapage devient En cours de révision.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le modal **Répondre au questionnaire** s'affiche uniquement lorsque le questionnaire est activé pour les demandes de faux positif dans le formulaire Gestion des exceptions. Pour plus d'informations sur la configuration d'un questionnaire pour les demandes de faux positif, reportez-vous aux sections Configurer la gestion des exceptions pour Réponse aux vulnérabilités, Configurer la gestion des exceptions pour Réponse aux vulnérabilités des applications et Configurer la gestion des exceptions pour Réponse aux vulnérabilités pour conteneurs.

L'approbateur reçoit une notification par e-mail concernant votre demande.

Résultats

Dans l'espace de travail du gestionnaire de vulnérabilités, sur la page Liste, accédez à **Exceptions** > **Tous**, ouvrez l'enregistrement d'approbation de changement d'état correspondant (VCA#) et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Résultat
Approuvé	L'état de la tâche de rattrapage passe à Fermé avec le motif Faux positif. L'état et le motif sont affichés dans les dossiers.
Rejeté	L'état de la tâche de rattrapage et de ses enregistrements ne change pas.

Dans le **flux d'activité** d'un enregistrement ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de votre demande.

Fermer les enregistrements en bloc dans le Espace de travail du gestionnaire de vulnérabilités

Fermez plusieurs enregistrements (VIT, AVIT ou CVIT) simultanément à l'aide de la fonction de modification en bloc du Espace de travail du gestionnaire de vulnérabilités fichier .

Avant de commencer

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail du gestionnaire de vulnérabilité** > **Liste**.
2. Sur la page Liste, ouvrez la liste Actif ou Tous dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de conteneurs
   - Éléments vulnérables d'applications
3. Effectuez l'une des actions suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cochez la case en regard de chaque élément si vous souhaitez utiliser l'option Uniquement les éléments sélectionnés dans le champ **Sélection d'enregistrement** .
- Appliquez des filtres si vous souhaitez utiliser l'option de filtre Tous les éléments vulnérables qui correspondent dans le champ **Sélection d'enregistrement** .

4. Sélectionnez le bouton **Modifier en bloc** .
5. Renseignez les champs du formulaire pour fermer les enregistrements sélectionnés.

Modifier en bloc les champs modaux

Champ	Description
Sélection d'enregistrement	Enregistrements à mettre à jour. Les choix possibles sont les suivants : ◦ Éléments sélectionnés uniquement : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements que vous avez sélectionnés à l'aide de la case à cocher. ◦ Tous les éléments vulnérables qui correspondent au filtre : Sélectionnez cette option si vous souhaitez mettre à jour les enregistrements filtrés. ◦ Tâche de rattrapage : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements d'une tâche de rattrapage, puis sélectionnez la tâche de rattrapage souhaitée dans le champ **Tâche de rattrapage** . ◦ Entrée de vulnérabilité : sélectionnez cette option si vous souhaitez mettre à jour les enregistrements spécifiques à une entrée vulnérable commune (CVE), puis sélectionnez la CVE dans le champ **Entrée de vulnérabilité** . **Remarque :** ◦ Les enregistrements avec un CI non valide ou CI désactivé ne sont pas mis à jour. ◦ Seuls les enregistrements à l'état Ouvert, En cours d'examen ou En attente d'implémentation sont mis à jour.
État	Sélectionnez l'état Fermé.
Motif	Motif de la fermeture des dossiers : ◦ Faux positif **Remarque :** Lorsque vous sélectionnez cette option pour marquer les enregistrements comme faux positifs, les champs Motif, Description brève et Informations supplémentaires s'affichent. Pour plus d'informations sur la modification en bloc des faux positifs, reportez-vous à la section Modifier en bloc le faux positif dans l'espace de travail du gestionnaire de vulnérabilité. ◦ Annulé ◦ Fixe **Remarque :** Les motifs Annulé et Corrigé ne s'appliquent pas aux CVIT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Notes de travail	Texte que vous saisissez pour décrire les changements.

6. Cliquez sur **Modifier**.

Une tâche de modification en bloc asynchrone met à jour les enregistrements pertinents.

Demander des exceptions pour les tâches et les enregistrements de rattrapage dans Espace de travail du gestionnaire de vulnérabilités

À partir du Espace de travail du gestionnaire de vulnérabilités, les gestionnaires de vulnérabilité et les analystes peuvent demander des exceptions et des faux positifs pour une tâche de rattrapage (VUL, AVUL, CVUL ou CRG) et un enregistrement (VIT, CVIT, AVIT ou CTR). Vous pouvez également diviser une tâche de rattrapage et créer des demandes de changement.

Rôle requis :

- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_sec_manager pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.vulnerability_analyst ou sn_vul_container.vulnerability_admin pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.admin pour les résultats des tests de configuration (CTR)

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

Dans le Espace de travail du gestionnaire de vulnérabilités, vous pouvez effectuer les actions suivantes sur les enregistrements et les tâches de rattrapage :

- Divisez une tâche de rattrapage (VUL, AVUL, CVUL et CRG).
- Demander une exception pour un enregistrement (VIT, AVIT ou CVIT) ou une tâche de rattrapage (VUL, AVUL, CVIL ou CRG).
- Demandez une exception de politique pour des enregistrements (VIT, AVIT ou CVIT) ou une tâche de rattrapage (VUL, AVUL, CVIL ou CRG).
- Demander une réduction du risque pour un élément vulnérable de l'hôte (VIT) et une tâche de rattrapage (VUL)
- Créez une demande de changement pour une tâche de rattrapage (VUL, CVUL ou CRG).
- Demander un faux positif pour un enregistrement (VIT, AVIT ou CVIT) ou une tâche de rattrapage (VUL, AVUL, CVUL ou CRG).

Remarque : Vous pouvez émettre des demandes de faux positif pour un ensemble de résultats de test à partir d'une tâche de rattrapage (CRG).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous lancez ces actions d'interface utilisateur à partir d'enregistrements dans le Espace de travail du gestionnaire de vulnérabilités, de la même manière que les propriétaires de rattrapage effectuent ces tâches dans le Espace de travail de remédiation IT.

Consultez les rubriques suivantes pour plus d'informations :

- Demander un faux positif pour un élément vulnérable ou une tâche de rattrapage
- Demander une exception dans le Espace de travail de remédiation IT
- Demander une réduction du risque pour un élément vulnérable ou une tâche de rattrapage
- Fractionner une tâche de rattrapage dans le Espace de travail de remédiation IT
- Créer une demande de changement dans Espace de travail de remédiation IT
- Demander une exception à l'aide de GRC : Gestion de la politique et de la conformitéEspace de travail de remédiation IT
- Demander un faux positif pour un ensemble de résultats des tests

Information associée

Vue d'ensemble de la gestion des exceptions

Conformité de la configuration Vue d'ensemble de la gestion des exceptions

Demander une exception en bloc dans l'espace de travail du gestionnaire de vulnérabilité

Modifier en bloc le faux positif dans l'espace de travail du gestionnaire de vulnérabilité

Demander une extension pour un élément vulnérable différé dans l'espace de travail du gestionnaire de vulnérabilité

Demandez une extension pour un élément vulnérable différé avant qu'il n'atteigne sa date d'échéance différée. En tant que propriétaire du rattrapage, vous n'êtes plus obligé d'attendre la date d'échéance différée pour effectuer cette demande.

Avant de commencer

Rôle requis : sn_vul.vulnerability_admin ou sn_vul.admin (déconseillé)

Pourquoi et quand exécuter cette tâche

Vous pouvez également demander une extension à partir de l'environnement classique.

Utilisez la même procédure pour demander une extension pour un élément vulnérable d'application, un élément vulnérable de conteneur, un groupe de résultats de test et une tâche de rattrapage.

Procédure

1. Accédez à la **Espaces de travail** > **Espaces de travail du gestionnaire de vulnérabilité**.
2. Sélectionnez Listes.
3. Sous Éléments vulnérables d'hôte, sélectionnez **Tous**.
4. Filtrez la liste en sélectionnant Différé dans la colonne État.
5. Sélectionnez un élément vulnérable différé.

   Remarque : Le bouton Demande d'extension n'est visible que lorsque l'état de l'élément vulnérable est Différé.

6. Sélectionnez le bouton **Demande d'extension** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Renseignez les champs du formulaire comme il convient.

Champ	Description
Prolonger jusqu'au	Sélectionnez la date à laquelle l'élément vulnérable différé doit être prolongé pour correction.
Motif	Entrez le motif pour lequel le problème est reporté. Les choix sont les suivants : ○ En attente de fenêtre de maintenance ○ Correctif non disponible ○ Risque accepté ○ Contrôle d'atténuation en place ○ Autre
Informations supplémentaires	Entrez toute autre information pertinente.

8. Sélectionnez **Demande d'extension**.
Un e-mail est déclenché lors de la soumission de la demande et de l'action ultérieure par l'approbateur.

Remarque :

- La demande passe par deux niveaux d'approbation.
- Si un élément vulnérable différé est prolongé à nouveau, le nombre de reports d'extension augmente dans le back-end.

9. Une fois la demande approuvée, les notes Jusqu'à, Motif et Report sont mises à jour.

Espace de travail du gestionnaire de vulnérabilités Informations de référence

Les rubriques suivantes vous fournissent des liens, des informations de référence, en plus des données de champ sur les formulaires et les enregistrements trouvés dans Espace de travail du gestionnaire de vulnérabilités.

Champs du formulaire Créer une rubrique de visualisation

Le tableau suivant décrit les champs du formulaire Créer une rubrique de visualisation dans le Espace de travail du gestionnaire de vulnérabilités.

Champ	Description
Nom	Nom de la rubrique de votre montre, par exemple VI critiques.
Propriété de	Nom de l'utilisateur propriétaire de la rubrique de surveillance.
Ordre d'affichage	Entrez une valeur comprise entre 100 et 1 000. 100 est la valeur par défaut. Les valeurs inférieures commençant par 100 sont affichées par ordre croissant sur les listes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Groupe propriétaire	Nom du groupe propriétaire de la rubrique de surveillance.
Actif	Activer ou désactiver la rubrique de surveillance. La valeur par défaut est sélectionnée (Actif).
Liste de surveillance	Ajoutez les noms des utilisateurs qui reçoivent des notifications et peuvent afficher la rubrique de visualisation.
Description	Texte qui décrit la rubrique de votre montre. Ce texte s'affiche dans le champ Description lorsque vous créez un effort de rattrapage à partir de cette rubrique de visualisation.
Catégorie	Type d'enregistrement pour lequel la rubrique de surveillance est créée.

Information associée

Créer une rubrique de surveillance dans le Espace de travail du gestionnaire de vulnérabilités

Champs du formulaire de demande d'exception GRC

La table suivante présente la description des champs du formulaire d'exception de demande GRC.

Formulaire de demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commence. La valeur par défaut est la date actuelle. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert. **Remarque :** Le nombre de jours pendant lesquels l'exception de politique est valide ne peut pas dépasser la **durée maximale de l'exception (jours)** que vous définissez pour la politique dans Politique et conformité. Pour plus d'informations, consultez Créer une politique .
Motif	Motif de la demande d'exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de demande d'exception (suite)

Champ	Description
Justification	Détails liés au motif pour lequel cette demande est effectuée. Ce champ doit être renseigné par le propriétaire du rattrapage.

Générer des champs de formulaire de synthèse de rattrapage

La table suivante présente les champs du formulaire Générer une synthèse de rattrapage.

Générer des champs de synthèse de rattrapage

Champ	Description
Case à cocher Actif	Cette case à cocher est activée par défaut. Si vous ne souhaitez pas envoyer de notifications par e-mail, désactivez ce champ.
Exécuter	Hebdomadaire est la valeur par défaut. Choisissez une option dans la liste.
Jour	Lundi est la valeur par défaut. Choisissez une option dans la liste.
Heure	Fixez une heure pour la livraison des e-mails. Sélectionnez un fuseau horaire si vous souhaitez utiliser un fuseau horaire autre que celui utilisé par l'instance exécutant la tâche.

Impact des contrôles compensatoires sur le score de risque et la date d'expiration

En tant que propriétaire du rattrapage, vous pouvez demander une réduction du risque pour un élément vulnérable d'hôte ou une tâche de rattrapage. Le responsable ou l'analyste des vulnérabilités peut également approuver ces demandes de réduction des risques.

Pour plus d'informations sur la façon de demander la réduction des risques et d'approuver l'approbation de réduction des risques, consultez Demander une réduction du risque pour un élément vulnérable ou une tâche de rattrapage et Approuver ou rejeter les demandes dans le Espace de travail du gestionnaire de vulnérabilités respectivement.

Lorsqu'une demande de réduction des risques est approuvée, le score des risques est réduit en fonction de la **valeur souhaitée** (cote de risque) dans l'enregistrement d'approbation de changement d'état (VCA#). Le score de risque le plus élevé de la cote de risque souhaitée est affecté à l'enregistrement lorsque votre demande de réduction des risques est approuvée. L'exemple suivant montre comment le score de risque et le score de risque d'origine sont mis à jour lorsque des contrôles de compensation sont appliqués. Les scores de risque les plus élevés par défaut des évaluations de risque sont utilisés dans l'exemple suivant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Impact des contrôles compensatoires sur le score de risque et le score de risque initial

Scénario	Cote de risque	Score du risque	Score de risque d'origine (score de risque calculé)
Données antérieures à la version 20.0	2 - Élevée	80	Ce champ n'était plus disponible avant la version 20.0.
Après la mise à niveau vers la version 20.0	2 - Élevée	80	Zéro
Le score de risque calculé passe à 90 pendant l'ingestion	1 – Critique	90.0	Zéro
Lorsque vous appliquez des contrôles de compensation	3 : moyen	69	90.0
Le score de risque calculé passe à 70 pendant l'ingestion	3 : moyen	69	70
Le score de risque calculé passe à 50 pendant l'ingestion	3 : moyen	50	50
Le score de risque calculé passe à 80 pendant l'ingestion	3 : moyen	50	80
Quand les contrôles de compensation expirent le **Date de fin pour la réduction du risque**	2 - Élevée	80	Zéro

Impact des contrôles compensatoires sur une tâche de rattrapage

Lorsque votre demande de réduction des risques est approuvée pour une tâche de rattrapage, l'impact des contrôles compensatoires sur ses éléments vulnérables est le suivant :

- Les contrôles de compensation appliqués à la tâche de rattrapage sont appliqués à ses éléments vulnérables (autres que ceux à l'état Fermé) dont le score de risque est supérieur au score de risque correspondant à la **valeur souhaitée** dans l'approbation de changement d'état d'une tâche de rattrapage. De plus, le score de risque de ces éléments vulnérables est réduit en fonction de la **valeur souhaitée**.
- La **date de fin pour la réduction du risque** reste inchangée pour les éléments vulnérables sur lesquels un contrôle de compensation est déjà appliqué. Elle n'est pas mise à jour **avec la date de fin de** réduction des risques de la tâche de rattrapage.
- La **date de fin pour la réduction du risque** est reportée aux éléments vulnérables uniquement lorsqu'un contrôle compensatoire n'est appliqué à aucun élément vulnérable auparavant. Si vous appliquez à nouveau les contrôles compensatoires à la tâche de rattrapage, la **date de fin pour la réduction du risque** n'est pas reportée sur les éléments

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérables, car la date de fin existante pour la réduction du **risque** des éléments vulnérables est prioritaire.

- Lorsqu'un nouvel élément vulnérable est ajouté à une tâche de rattrapage à laquelle des contrôles compensatoires sont déjà appliqués, le risque n'est pas transféré à l'élément vulnérable.

Impact d'un contrôle compensatoire sur un élément vulnérable

Lorsque votre demande de réduction des risques est approuvée pour un élément vulnérable :

- Son nouveau score de risque s'affiche dans le champ de **score de risque** et l'ancien score de risque (score de risque calculé) est déplacé vers le champ de **score de risque d'origine** . Ce changement est valable jusqu'à la date spécifiée dans le champ Date de **fin pour la réduction du risque** .
- Lorsqu'un élément vulnérable a déjà des contrôles de compensation appliqués, lors de l'ingestion :
  - Si le score de risque calculé est supérieur au score de risque, le score de risque reste le même et le score de risque d'origine est mis à jour avec le score de risque calculé.
  - Si le score de risque calculé est inférieur au score de risque, le score de risque et le score de risque d'origine sont mis à jour avec le score de risque calculé.
- Si un élément de configuration (CI) est modifié pour un élément vulnérable sur lequel un contrôle de compensation est déjà appliqué :
  - Le CI est mis à jour pour un élément vulnérable par défaut, car la `sn_sec_cmn.update_on_ci_change` propriété système est définie sur vrai.

    Le contrôle de compensation est toujours applicable pour l'élément vulnérable.
  - L'élément vulnérable est fermé et un nouvel élément vulnérable est créé si la `sn_sec_cmn.update_on_ci_change` propriété système est définie sur faux.

    Le contrôle de compensation appliqué à l'ancien élément vulnérable est appliqué au nouvel élément vulnérable et la **date de fin pour la réduction du risque**, le **score de risque d'origine** et le **score de risque** restent les mêmes.
- Lorsqu'un élément vulnérable est rouvert par le scanner et qu'un contrôle de compensation lui est déjà appliqué, le même contrôle de compensation est appliqué après sa réouverture.

Information associée

Comprendre les contrôles compensatoires pour la réduction des risques

Ajouter un contrôle de compensation à la bibliothèque

Associer des contrôles compensatoires à des CVE ou des TPE pour les demandes de réduction des risques

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

#unique_158_Connect_42_li-risk-reduction-vmws

Exemples de création de tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT

Lorsque vous créez manuellement des tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT, les enregistrements sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

regroupés dans une tâche de rattrapage en fonction des critères de regroupement que vous sélectionnez.

Prenons l'exemple suivant où 10 enregistrements sont sélectionnés pour la création d'une tâche de rattrapage. Après avoir fourni les détails de la sélection d'enregistrements et une brève description, sélectionnez les **critères de regroupement** en fonction de vos besoins, puis sélectionnez la façon dont vous souhaitez gérer les enregistrements qui font déjà partie des tâches de rattrapage existantes.

Example: Création d'une tâche de rattrapage en fonction des critères de regroupement

Éléments vulnérables sélectionnés pour la création de la tâche de rattrapage

ID d'élément vulnérable	Tâches de rattrapage existantes	Groupe d'affectation	Élément de configuration	Vulnérabilité	Cote de risque
VIT10001	VUL10021, VUL10022	Gestionnaire de rattrapage	APSVR-NY-1672	CVE-2018-9020	4
VIT10002	-	Réponse aux vulnérabilités	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10003	VUL10021	Administrateurs LDAP	DEV-IBM-NY-682	CVE-2012-5357	1
VIT10004	-	Gestionnaire de rattrapage	CRMBK-SD-4210	CVE-2013-1710	4
VIT10005	VUL10022	Réponse aux vulnérabilités	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10006	-	Gestionnaire de rattrapage	CRMBK-SD-4210	CVE-2013-1710	2
VIT10007	-	Administrateurs LDAP	DEV-SAP-SD-9388	CVE-2013-3906	1
VIT10008	-	Administrateurs LDAP	DEV-IBM-NY-682	CVE-2013-3906	1
VIT10009	-	Gestionnaire de rattrapage	CRMBK-SD-4210	CVE-2013-1710	2
VIT10010	-	Administrateurs LDAP	DEV-SAP-SD-9388	CVE-2013-3906	4

La liste suivante montre comment les enregistrements sont regroupés en tâches de rattrapage en fonction des critères de regroupement sélectionnés lors de la création de la tâche de rattrapage.

Scénario 1 : les critères de regroupement sont sélectionnés en tant que « Groupe d'affectation » et la gestion des enregistrements dans d'autres tâches de rattrapage est sélectionnée en tant que « Ignorer les enregistrements pour les nouvelles tâches de rattrapage »

Les enregistrements avec le même groupe d'affectation sont regroupés en une seule tâche de rattrapage. Les enregistrements qui font déjà partie des tâches de rattrapage existantes ne sont pas ajoutés aux nouvelles tâches de rattrapage. Ici, trois tâches de rattrapage sont créées, chacune contenant les enregistrements qui sont affectés au **gestionnaire de rattrapage**, aux **administrateurs LDAP** et aux groupes **d'affectation de Vulnerability Response** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de rattrapage créée dans le scénario 1

Tâches de rattrapage créées	Enregistrements dans la tâche de rattrapage
Tâche de rattrapage 1 - VUL10001	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe d'affectation du **gestionnaire de rattrapage** : • VIT10004 • VIT10006 • VIT10009 L'enregistrement VIT10001 ne sera pas déplacé vers la tâche de rattrapage VUL10001.
Tâche de rattrapage 2 - VUL10002	Cette tâche de rattrapage contient l'enregistrement VIT10002 affecté au groupe d'affectation **Réponse aux vulnérabilités** . L'enregistrement VIT10005 ne sera pas déplacé vers la tâche VUL10002.
Tâche de rattrapage 3 - VUL10003	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe **d'affectation Administrateurs LDAP** : • VIT10007 • VIT10008 • VIT10010 L'enregistrement VIT10003 ne sera pas déplacé vers la tâche de rattrapage VUL10003.

Scénario 2 : les critères de regroupement sont sélectionnés en tant que « Groupe d'affectation et élément de configuration » et la gestion des enregistrements dans d'autres tâches de rattrapage est sélectionnée en tant que « Transférer les enregistrements aux nouvelles tâches de rattrapage »

Les enregistrements avec le même élément de configuration qui sont affectés au même groupe d'affectation sont regroupés dans une tâche de rattrapage. Les enregistrements VIT10001, VIT10003 et VIT10005 sont supprimés de leurs anciennes tâches de rattrapage et déplacés vers les nouvelles tâches de rattrapage. Ici, cinq tâches de rattrapage sont créées.

Tâches de rattrapage créées dans le scénario 2

Tâches de rattrapage créées	Les enregistrements font partie de la tâche de rattrapage
Tâche de rattrapage 1 - VUL10004	Cette tâche de rattrapage contient les enregistrements affectés au groupe d'affectation du **propriétaire de**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de rattrapage créées dans le scénario 2 (suite)

Tâches de rattrapage créées	Les enregistrements font partie de la tâche de rattrapage
	rattrapage et avec l'élément **de configuration APSVR-NY-1672** . • VIT10001 L'enregistrement VIT10001 sera supprimé de la VUL10021 et VUL10022 tâches de rattrapage.
Tâche de rattrapage 2 - VUL10005	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe d'affectation **Réponse aux vulnérabilités** et avec l'élément **de configuration DEV-IBM-NY-682** . • VIT10002 • VIT10005 L'enregistrement VIT10005 sera supprimé de la tâche de rattrapage VUL10022.
Tâche de rattrapage 3 : VUL10006	Cette tâche de rattrapage contient les enregistrements affectés au groupe **d'affectation des administrateurs LDAP** et à l'élément **de configuration DEV-IBM-NY-682** . • VIT10003 • VIT10008 L'enregistrement VIT10003 sera supprimé de la tâche de rattrapage VUL10021.
Tâche de rattrapage 4 - VUL10007	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe d'affectation du **gestionnaire de rattrapage** et avec l'élément de configuration **CRMBK-SD-4210** . • VIT10004 • VIT10006 • VIT10009
Tâche de rattrapage 5 - VUL10008	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe **d'affectation des administrateurs LDAP** et qui possèdent l'élément **de configuration DEV-SAP-SD-9388** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de rattrapage créées dans le scénario 2 (suite)

Tâches de rattrapage créées	Les enregistrements font partie de la tâche de rattrapage
	• VIT10007 • VIT10010

Scénario 3 : les critères de regroupement sont sélectionnés comme « Groupe d'affectation et vulnérabilité » et la gestion des enregistrements dans d'autres tâches de rattrapage est sélectionnée comme « Conserver les enregistrements dans les tâches de rattrapage actuelles et nouvelles »

Les enregistrements avec la même vulnérabilité qui sont affectés au même groupe d'affectation sont regroupés dans une tâche de rattrapage. Les enregistrements VIT10001, VIT10003 et VIT10005 seront ajoutés à leurs nouvelles tâches de rattrapage respectives sans être supprimés de leurs anciennes tâches de rattrapage. Ici, cinq tâches de rattrapage sont créées.

Tâches de rattrapage créées dans le scénario 3

Tâches de rattrapage créées	Les enregistrements font partie de la tâche de rattrapage
Tâche de rattrapage 1 - VUL10009	Cette tâche de rattrapage contient les enregistrements affectés au groupe d'affectation du **propriétaire de rattrapage** et présentant la vulnérabilité **CVE-2018-9020** . • VIT10001 L'enregistrement VIT10001 continuera de faire partie de VUL10021 et VUL10022 également des tâches de rattrapage.
Tâche de rattrapage 2 - VUL10010	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe d'affectation **Réponse aux vulnérabilités** et qui présentent la vulnérabilité **CVE-2018-9020** . • VIT10002 • VIT10005 L'enregistrement VIT10005 continuera également de faire partie de VUL10022 tâche de rattrapage.
Tâche de rattrapage 3 - VUL10011	Cette tâche de rattrapage contient les enregistrements affectés au groupe **d'affectation des administrateurs LDAP** et présentant la vulnérabilité **CVE-2012-5357** . • VIT10003

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de rattrapage créées dans le scénario 3 (suite)

Tâches de rattrapage créées	Les enregistrements font partie de la tâche de rattrapage
	L'enregistrement VIT10003 continuera également de faire partie de la tâche de rattrapage de VUL10021.
Tâche de rattrapage 4 - VUL10012	Cette tâche de rattrapage contient les enregistrements affectés au groupe d'affectation **du gestionnaire de rattrapage** et présentant la vulnérabilité **CVE-2013-1710** . • VIT10004 • VIT10006 • VIT10009
Tâche de rattrapage 5 - VUL10013	Cette tâche de rattrapage contient les enregistrements affectés au groupe **d'affectation des administrateurs LDAP** et présentant la vulnérabilité **CVE-2013-3906** . • VIT10007 • VIT10008 • VIT10010

Scénario 4 : Regroupement des critères en tant que « Groupe d'affectation et cote de risque » et Gestion des enregistrements dans d'autres tâches de rattrapage sélectionnée en tant que « Conserver les enregistrements dans les tâches de rattrapage actuelles et nouvelles »

Les enregistrements ayant la même cote de risque qui sont affectés au même groupe d'affectation sont regroupés dans une tâche de rattrapage. Les enregistrements VIT10001, VIT10003 et VIT10005 seront ajoutés à leurs nouvelles tâches de rattrapage respectives sans être supprimés de leurs anciennes tâches de rattrapage. Ici, cinq tâches de rattrapage sont créées.

Tâche de rattrapage créée dans le scénario 4

Tâches de rattrapage créées	Les enregistrements font partie de la tâche de rattrapage
Tâche de rattrapage 1 - VUL10014	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe d'affectation du **propriétaire de rattrapage** et avec une cote de risque **de 4** . • VIT10001 • VIT10004 L'enregistrement VIT10001 continuera de faire partie des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de rattrapage créée dans le scénario 4 (suite)

Tâches de rattrapage créées	Les enregistrements font partie de la tâche de rattrapage
	tâches de rattrapage VUL10021 et VUL10022.
Tâche de rattrapage 2 VUL10015	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe d'affectation **Réponse aux vulnérabilités** et avec **2** cotes de risque. • VIT10002 • VIT10005 L'enregistrement VIT10005 continuera de faire partie de VUL10022 tâche de rattrapage.
Tâche de rattrapage 3 - VUL10016	Cette tâche de rattrapage contient les enregistrements affectés au groupe **d'affectation des administrateurs LDAP** et avec **une** cote de risque 1. • VIT10003 • VIT10007 • VIT10008 L'enregistrement VIT10003 continuera de faire partie de VUL10021 tâche de rattrapage.
Tâche de rattrapage 4 - VUL10017	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe d'affectation **du gestionnaire de rattrapage** et avec **2** cotes de risque. • VIT10006 • VIT10009
Tâche de rattrapage 5 - VUL10018	Cette tâche de rattrapage contient les enregistrements qui sont affectés au groupe **d'affectation des administrateurs LDAP** et avec une cote de risque **de 4** . • VIT10010

Information associée

Créer une tâche de rattrapage manuellement dans le Espace de travail du gestionnaire de vulnérabilités

Créer une tâche de rattrapage manuellement dans le Espace de travail de remédiation IT

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réévaluation des exceptions pour les enregistrements sélectionnés dans le Espace de travail du gestionnaire de vulnérabilités

Dans , Espace de travail du gestionnaire de vulnérabilités lorsque vous évaluez les règles d'exception d'un ensemble d'enregistrements dans le modal Réévaluer et mettre à jour les propriétés de rattrapage, leur état de report et leur date de fin de report sont mis à jour conformément aux dernières règles d'exception.

Scénarios

Vous pouvez rencontrer les scénarios suivants, lorsque vous évaluez les exceptions pour un ensemble sélectionné d'enregistrements dans le modal Réévaluer et mettre à jour les propriétés de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités:

Scénario 1 : Lorsque les enregistrements sélectionnés sont déjà différés manuellement et qu'ils correspondent à la condition d'une règle d'exception, ces enregistrements restent à l'état Différé sans aucun changement.

Scénario 2 : Lorsque les enregistrements sélectionnés correspondent à la condition des règles d'exception et que ces enregistrements sont dans un état de non-report (par exemple, ouvert, en cours de révision, en cours d'examen), ces enregistrements sont différés jusqu'à la date définie dans la règle d'exception.

Scénario 3 : Lorsque les enregistrements sélectionnés sont déjà à l'état Différé (ceux qui sont différés à l'aide de la règle d'exception A), ils restent à l'état Différé dans les scénarios suivants :

- La règle d'exception expire et les enregistrements ne correspondent pas à la condition
- La règle d'exception expire et les enregistrements correspondent à la condition
- la règle d'exception A expire et les enregistrements correspondent à la condition d'une autre règle d'exception B.

Scénario 4 : Considérez que les enregistrements sont différés à l'aide d'une règle d'exception. Lorsque vous modifiez la condition de la règle d'exception de sorte que l'état Différé des enregistrements n'est plus valide, puis réévaluez les règles d'exception pour ces enregistrements :

- les enregistrements passent à l'état Ouvert
- Les champs Date de fin, Date du report, Nombre de reports et autres sont mis à jour.

Example: Considérez que vous évaluez les exceptions pour les éléments vulnérables de l'hôte (VIT) suivants.

Considérez la règle d'exception avec les détails suivants :

Détails de la règle d'exception

Champ	Description	Valeur
Nom	Nom de la règle d'exception.	Différer les VIT critiques
Début de validité	Date à partir de laquelle cette règle est active pour différer les VI.	20-08-2024
Date de fin de validité	Date à partir de laquelle la tâche de rattrapage arrête d'accepter de nouveaux VI.	30-11-2024

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de la règle d'exception (suite)

Champ	Description	Valeur
Motif	Raison de la création de cette règle d'exception.	Risque accepté
Groupe d'affectation	Groupe auquel la tâche de rattrapage créée pour le suivi des VI différés est affectée.	Groupe de rattrapage 1
Informations supplémentaires	Informations supplémentaires que le demandeur souhaite fournir à l'approbateur. Ces informations sont renseignées dans le champ Description de la tâche de rattrapage.	Cette règle a été créée pour différer automatiquement les VIT critiques.
Condition	Condition de filtre pour les éléments vulnérables qui peut être définie lors du traitement des éléments vulnérables.	Cote de risque = 5 – Critique
Exécuter sur les données existantes	Option qui vous permet d'exécuter cette règle sur des données existantes la première fois que cette règle est exécutée.	Oui
État	État de la règle d'exception.	Approuvé
Ordre d'exécution	Ordre unique pour chaque règle d'exception	100
Reporté jusqu'à	Date à laquelle les VUL et les VI sont reportés. À cette date, la VUL créée est fermée, tous les VI sont déplacés hors du groupe et les règles de groupe sont réappliquées.	2024-12-23 16:10:29

Le tableau suivant montre comment l'état change lorsque les règles d'exception sont réévaluées pour plusieurs VIT simultanément :

Enregistrements pour lesquels les exceptions sont réévaluées

Numéro VIT	État	Cotes de risque	État mis à jour après réévaluation des exceptions -1	Date de fin : 1
VIT120067	Ouvert	2 - Faible	Ouvert	-
VIT120068	En cours de révision	3 : moyen	En cours de révision	-
VIT120069	En cours d'examen	5 - Critique	Différé	2024-12-23 16:10:29
VIT120070	Différé	5 - Critique	Différé	2024-12-23 16:10:29
VIT120071	Différé	2 - Faible	Différé	2024-10-02 16:10:29 (Différé manuellement)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements pour lesquels les exceptions sont réévaluées (suite)

Numéro VIT	État	Cotes de risque	État mis à jour après réévaluation des exceptions -1	Date de fin : 1
VIT120072	Fermé	5 - Critique	Fermé	-

Lorsque la condition de la règle d'exception précédente est modifiée en `Cote de risque = 2 - Faible` et **Reporté jusqu'à** est modifié en `2024-12-31 14:10:23` , les enregistrements sont mis à jour comme suit :

Enregistrements pour lesquels les exceptions sont réévaluées

Numéro VIT	État mis à jour après réévaluation des exceptions -1	Cote de risque	État mis à jour après réévaluation des exceptions : 2	Jusqu'à la date : 2
VIT120067	Ouvert	2 - Faible	Différé	2024-12-31 14:10:23
VIT120068	En cours de révision	3 : moyen	En cours de révision	-
VIT120069	Différé	5 - Critique	Différé	2024-12-23 16:10:29
VIT120070	Différé	5 - Critique	Différé	2024-12-23 16:10:29
VIT120071	Différé	2 - Faible	Différé (aucun changement dans l'état)	2024-10-02 16:10:29 (Aucun changement dans la date de fin)
VIT120072	Fermé	5 - Critique	Fermé	-

Information associée

Réévaluer les propriétés de rattrapage des enregistrements dans le Espace de travail du gestionnaire de vulnérabilités

Vue d'ensemble des règles d'exception

Conformité de la configuration Vue d'ensemble de la gestion des exceptions

Espace de travail de remédiation IT

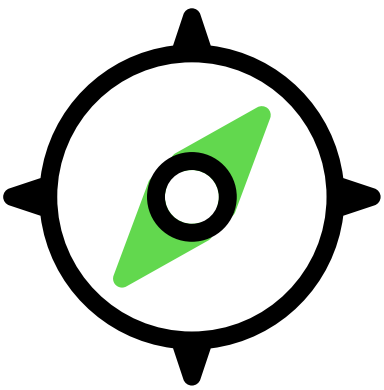
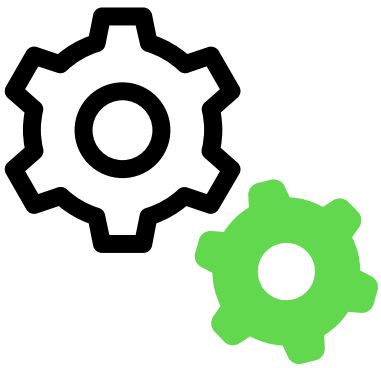
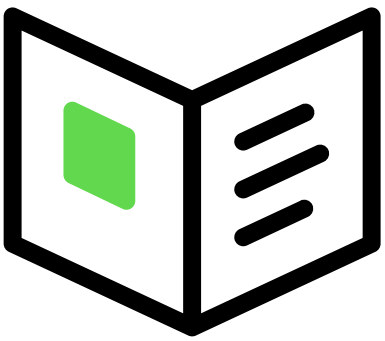
Les équipes informatiques peuvent gagner du temps dans la résolution des vulnérabilités liées aux technologies de l'information en créant facilement des demandes de changement, en analysant à nouveau les éléments vulnérables et en soumettant des demandes d'exception Espace de travail de remédiation ITà partir du .

Démo de l'espace de travail de remédiation informatique v18.0

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Premiers pas

Explorer	Corriger	Référence
		
En savoir plus sur le Espace de travail de remédiation IT	Découvrez comment corriger les vulnérabilités et les erreurs de configuration à partir du Espace de travail de remédiation IT	Obtenir des informations supplémentaires pour configurer et administrer Espace de travail de remédiation IT

Dépannage et demande d'aide

- Security Operations sur ServiceNow Community
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Exploration de l'Espace de travail de remédiation IT

Il Espace de travail de remédiation IT est destiné aux propriétaires de rattrapages informatiques et aux groupes informatiques. Il est composé de vues d'accueil et de listes, ainsi que de visualisations de données sur lesquelles vous pouvez cliquer et qui vous permettent de voir les tâches de rattrapage qui vous ont été affectées et le nombre d'enregistrements qui vous sont affectés et qui ont des solutions.

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

Le se Espace de travail de remédiation IT compose des pages, listes et formulaires suivants :

Page de destination (accueil)

La page d'accueil comprend la carte Tâches de rattrapage affectées, la carte Solutions préférées sur les VI, la carte CI impactés, la carte Correctifs préférés sur les VI et la liste des tâches de rattrapage. Pour en savoir plus sur la page d'accueil, reportez-vous à Page d'accueil dans Espace de travail de remédiation IT.

Page Tableaux de bord

La page Tableaux de bord contient le tableau de bord Rattrapage de vulnérabilité. Pour en savoir plus sur la page Tableaux de bord, reportez-vous à la section Page Tableaux de bord dans Espace de travail de remédiation IT.

Page de liste

Cette vue se compose de listes par défaut et personnalisées des tâches de remédiation, des éléments vulnérables d'hôte, des éléments vulnérables d'applications, des éléments vulnérables de conteneur, des résultats des tests de configuration qui vous sont affectés et des solutions, des demandes d'exceptions, etc. Pour plus d'informations sur la page Liste, reportez-vous à Page de liste dans Espace de travail de remédiation IT. Pour en savoir plus sur ce que vous pouvez faire à partir de cette page, reportez-vous à la section Créer une liste dans le Espace de travail de remédiation IT.

Afficher un exemple de workflow dans le Espace de travail de remédiation IT

Consultez un exemple de workflow de bout en bout dans le Espace de travail de remédiation IT. Découvrez comment les spécialistes informatiques peuvent utiliser l'espace de travail pour surveiller les éléments vulnérables critiques (VIT, AVIT et CVIT) et les résultats des tests (TR) et corriger les vulnérabilités qui leur sont affectées.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Procédure

Cliquez sur l'image suivante pour afficher les étapes du workflow.
Démo de l'espace de travail de remédiation informatique

L'image comprend les tâches suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- À partir de la page d'accueil (page de destination du propriétaire de rattrapage informatique), affichez les tâches de rattrapage qui vous sont affectées. Basculez entre les tâches qui vous sont affectées et celles de votre groupe. Affichez les tâches de rattrapage d'hôte dotées de solutions. Pour en savoir plus sur la page d'accueil, reportez-vous à Page d'accueil dans Espace de travail de remédiation IT.
- Sélectionnez la vue **Liste** pour afficher les listes de vos tâches affectées.
- Dans la vue de liste avec la liste **Affecté à mon groupe** sélectionnée dans la liste Tâches de rattrapage, identifiez et affectez-vous le travail. Pour plus d'informations sur la page Liste, reportez-vous à Page de liste dans Espace de travail de remédiation IT.
- Regroupez les tâches de rattrapage par type d'enregistrement : sélectionnez le menu à trois points dans la colonne **Type d'enregistrement** , puis sélectionnez **Grouper par type d'enregistrement**.
- Sur une tâche de rattrapage ouverte (VUL, AVUL, CVUL et CRG) :
  - Sélectionnez l'onglet **Vue d'ensemble** pour afficher les enregistrements (VIT, AVIT, CVIT et TR) et les éléments de configuration (CI) affectés qui sont associés à l'enregistrement.
  - Sélectionnez l'onglet **Solutions** pour afficher les solutions préférées et potentielles pour une tâche de rattrapage d'hôte.
  - Sélectionnez l'onglet **Détails** pour modifier les champs modifiables tels que État, Groupe d'affectation, Affecté à et Description brève et afficher les actions effectuées sur une tâche de rattrapage.
  - Sélectionnez l'onglet **Approbation de changement d'état** pour afficher les enregistrements d'approbation de changement d'état (CA#), ce qui vous aide à suivre le workflow d'approbation.
  - Sélectionnez l'onglet **Demandes de changement** pour afficher l'état d'approbation des demandes de changement et créer une nouvelle demande de changement en sélectionnant le bouton **Nouveau** .
  - Sélectionnez les actions d'interface utilisateur : **Marquer comme faux positif**, **Créer un changement**, **Fractionner la tâche**, **Mettre à jour l'état**, **Demande d'exception**, **Supprimer**, etc. Suivez les invites des boîtes de dialogue pour vous aider dans votre correction.

Page d'accueil dans Espace de travail de remédiation IT

La page d'accueil de fournit Espace de travail de remédiation IT une liste consolidée des tâches de rattrapage d'hôtes, d'applications, de conteneurs et de résultats de tests qui vous sont affectées, à vous et à vos groupes d'affectation.

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

La page d'accueil se compose des cartes suivantes et de la liste des tâches de rattrapage qui vous sont affectées et qui sont affectées à vos groupes d'affectation, ainsi que des enregistrements qui vous sont affectés et qui ont des solutions.

Carte des tâches de rattrapage affectées

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nombre de tâches de rattrapage actives qui vous sont affectées. Sélectionnez la tuile pour afficher la liste des tâches de rattrapage.

Solutions privilégiées sur la carte des VI

Nombre de solutions privilégiées disponibles pour corriger les éléments vulnérables de l'hôte. La liste des solutions s'affiche si l'application Gestion des solutions de vulnérabilité est installée. Cette carte vous montre les données de solution, les solutions potentielles et préférées des fournisseurs tiers concernant vos éléments vulnérables.

Carte des CI impactés

Le nombre d'éléments de configuration qui ont des VI qui sont affectés à vous ou à vos groupes. Pour plus d'informations, consultez Afficher les éléments de configuration présentant des vulnérabilités dans Espace de travail de remédiation IT.

Correctifs préférés sur la carte des VI

Nombre de correctifs préférés disponibles qui peuvent être utilisés pour corriger les éléments vulnérables de l'hôte.

Liste des tâches de rattrapage

Liste des tâches de rattrapage qui vous sont affectées et qui sont affectées à vos groupes d'affectation. Vous pouvez filtrer les enregistrements en sélectionnant les options **Affecté à moi** et **Affecté à mes groupes** .

Vous pouvez cliquer sur une tâche de rattrapage pour en afficher les détails et démarrer une enquête. Dans la vue Listes, vous pouvez afficher les tâches de rattrapage, les éléments vulnérables, les résultats des tests de configuration, etc. Vous pouvez ouvrir une tâche de rattrapage et cliquer sur **Me l'affecter** pour vous affecter la tâche et commencer l'examen.

Remarque : Si vous ne vous affectez pas la tâche dans la tâche de rattrapage, vous ne pouvez afficher aucune action d'interface utilisateur au niveau de l'enregistrement.

Cliquez sur les ellipses Actions supplémentaires, puis sur **Démarrer l'examen** pour résoudre une tâche de rattrapage.

Pour plus d'informations sur ce que vous pouvez faire sur la page d'accueil, reportez-vous à la section Utiliser des enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT.

Page Tableaux de bord dans Espace de travail de remédiation IT

La page Espace de travail de remédiation IT Tableaux de bord de fournit le tableau de bord de rattrapage de vulnérabilité dans l'interface Next Experience utilisateur qui peut être utilisé pour se concentrer sur les tâches de rattrapage et les éléments vulnérables.

En tant que propriétaire du rattrapage (sn_vul.remediation_owner), vous pouvez accéder au tableau de bord **Rattrapage des vulnérabilités** en accédant à **Espaces de travail** > **Espace de travail de remédiation informatique** et en sélectionnant l'icône Tableaux de bord. Pour en savoir plus sur le tableau de bord Rattrapage des vulnérabilités, reportez-vous à la section Utilisation des tableaux de bord par défaut Réponse aux vulnérabilités.

Vous pouvez créer un tableau de bord personnalisé en sélectionnant l'icône ⋮ et en sélectionnant **Créer**.

Page de liste dans Espace de travail de remédiation IT

La vue de liste dans la vue de rattrapage Espace de travail de remédiation IT permet aux propriétaires de rattrapage d'afficher les enregistrements (VIT, AVIT, CVIT et TR) qui leur sont affectés et qui sont affectés à leurs groupes d'affectation, et de corriger ces vulnérabilités et erreurs de configuration. Vous pouvez également consulter la liste des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

solutions préférées recommandées pour corriger les éléments vulnérables de l'hôte (VIT). Outre ces listes, vous pouvez afficher la liste des demandes d'exception et des demandes d'évaluation de test de pénétration que vous avez soumises, les conclusions du test de pénétration associées à vos demandes d'évaluation de test de pénétration, les bibliothèques prises en charge et d'autres données prises en charge.

Rôles requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Les listes et les liens de la page Liste vous permettent d'accéder facilement aux enregistrements et aux tâches. Il contient deux onglets :

- **Onglet Listes** : affiche les listes par défaut pour les efforts de rattrapage, les tâches de rattrapage, les éléments vulnérables (VIT, AVIT ou CVIT), les solutions, les exceptions et les résultats des tests de configuration (TR), entre autres. Pour plus d'informations, consultez le tableau suivant.
- **Onglet Mes listes** : affiche toute liste que vous avez renommée à partir de l'onglet Liste et toute liste que vous créez.

  Vous pouvez également créer votre propre liste d'enregistrements. Pour plus d'informations, consultez Créer une liste dans le Espace de travail de remédiation IT.

Conseil :

Si l'administrateur définit la *sn_vul_cmn_ws.navigate_to_workspace* propriété système sur true , lors de la sélection des liens de filtre prédéfinis dans le Réponse aux vulnérabilités module , Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs et Résultats des tests dans Conformité de la configuration le menu **Tout** , ces liens s'ouvrent dans la page Liste du Espace de travail de remédiation IT.

Par exemple, si vous sélectionnez **Affecté à mes groupes** en accédant à **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation** > **Affecté à mes groupes**, ce lien est redirigé vers le Espace de travail de remédiation IT fichier . La liste Affecté à mon groupe du module Tâches de remédiation s'ouvre dans la page Liste de l'espace de travail de remédiation informatique si vous disposez du rôle de propriétaire de remédiation. Pour afficher les tâches de rattrapage de l'hôte, regroupez les tâches par **type d'enregistrement**.

Vous pouvez masquer le nombre d'enregistrements dans une liste à l'aide de la *glide.ui.list.seismic.omit.count* propriété système. Pour plus d'informations sur la façon de désactiver/d'activer l'affichage du nombre d'enregistrements sur une liste, consultez l'article de la base de connaissances KBB0010402 .

Onglet Listes

Les listes suivantes s'affichent :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes

Élément de liste	Description	Applications requises	Rôle requis
Tâches de rattrapage	Affichez la liste des tâches de rattrapage et accédez à la tâche souhaitée pour commencer à travailler dessus. Les listes suivantes sont disponibles : • **Affecté à vous** : répertorie toutes les tâches de rattrapage d'hôtes, d'applications, de conteneurs et de résultats de tests qui vous sont affectées. • **Affecté à mon groupe** : répertorie toutes les tâches de rattrapage d'hôtes, d'applications, de conteneurs et de résultats de tests qui sont affectées aux groupes d'affectation auxquels vous appartenez. Regroupez les tâches par type d'enregistrement pour les classer en tâches de rattrapage des résultats des tests d'hôte, d'application, de conteneur et de configuration. Les tâches de rattrapage créées par les règles de tâche de rattrapage dans l'interface utilisateur classique ont un effort de rattrapage vide.	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.remediation_owne pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Applications requises	Rôle requis
Actifs concernés	Affichez la liste des actifs impactés. Les listes suivantes sont disponibles : • **Affecté à vous** : liste des éléments de configuration impactés qui vous sont affectés • **Affecté à mon groupe** : liste des éléments de configuration impactés affectés à vos groupes d'affectation.	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.remediation_owne pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)
Éléments vulnérables d'hôte	Affichez la liste des éléments vulnérables de l'hôte et accédez à l'élément souhaité pour commencer à travailler dessus. Les listes suivantes sont disponibles : • **Mes affectations** : liste des éléments vulnérables d'hôte qui vous sont affectés pour correction. • **Affecté à mon groupe** : liste des éléments vulnérables d'hôte affectés aux groupes d'affectation auxquels vous appartenez.	Réponse aux vulnérabilités	sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
Éléments vulnérables de l'application	Affichez la liste des éléments vulnérables de l'hôte et accédez à l'élément souhaité pour commencer à travailler dessus. Les	Réponse aux vulnérabilités des applications	sn_vul.app_champion_sécurité_

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Applications requises	Rôle requis
	listes suivantes sont disponibles : • **Mes affectations** : liste des éléments vulnérables d'applications qui vous sont affectés pour le rattrapage. • **Affecté à mon groupe** : liste des éléments vulnérables d'applications affectés aux groupes d'affectation auxquels vous appartenez.		
Éléments vulnérables de conteneurs	Affichez la liste des éléments vulnérables du conteneur et accédez à l'élément souhaité pour commencer à travailler dessus. Cette vue de liste contient : • **Affectés à moi** : liste des éléments vulnérables de conteneurs qui vous sont affectés pour correction. • **Affecté à mon groupe** : liste des éléments vulnérables de conteneurs affectés aux groupes d'affectation auxquels vous appartenez.	Réponse aux vulnérabilités pour conteneurs	sn_vul_container.remediation_owner Affichez la liste des évaluations nécessaires pour effectuer une revue post-incident.
Résultats des tests de configuration	Affichez la liste des résultats des tests et accédez à l'enregistrement souhaité pour commencer à	Conformité de la configuration	sn_vulc.remediation_owner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Applications requises	Rôle requis
	travailler dessus. Cette vue de liste contient : • **Mes affectations** : liste des résultats des tests de configuration qui vous sont affectés pour correction. • **Affecté à mon groupe** : liste des résultats des tests de configuration affectés aux groupes d'affectation auxquels vous appartenez.		
Solutions	Répertorie les solutions de l'application Solution Management. La liste des solutions s'affiche si l'application Gestion des solutions de vulnérabilité est installée. • **Tout** : affiche toutes les solutions disponibles que vous utilisez pour corriger les éléments vulnérables de l'hôte. • **Priorité la plus élevée** : affiche toutes les solutions utilisées pour renseigner les solutions préférées. • **Avec éléments vulnérables** : affiche les solutions qui sont utilisées en	Réponse aux vulnérabilités	sn_vul.remediation_owner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Applications requises	Rôle requis
	tant que solution préférée pour les éléments vulnérables.		
Demandes d'exception	• **Mes demandes** : liste de toutes les demandes d'approbation d'exception, de faux positif et de désaffectation que vous avez émises pour les éléments vulnérables d'hôte, d'application ou de conteneur, ainsi que leurs tâches de rattrapage. • **Mes demandes (Conformité de la configuration)** : liste de toutes les demandes d'approbation d'exception, de faux positif et de désaffectation que vous avez émises pour les résultats des tests et leurs tâches de rattrapage sur lesquelles vous travaillez.	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.remediation_owne pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)
Bibliothèques	Contient les listes suivantes : • **NVD** : une bibliothèque complète de renseignements sur les vulnérabilités gérée par le National Institute of Standards and Technology (NIST). Liste des vulnérabilités	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.remediation_owne pour les éléments vulnérables de conteneurs (CVIT)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Applications requises	Rôle requis
	trouvées par NVD et comprend des listes de vérification de sécurité, des failles logicielles liées à la sécurité, des erreurs de configuration, des noms de produits et des mesures d'impact, y compris les exploits. • **CWE** : liste des types de faiblesses logicielles développés par la communauté. Chaque enregistrement CWE comprend également un article de la base de connaissances associé qui décrit la faiblesse. • **Vulnérabilités de l'application** : liste de toutes les entrées de vulnérabilité de l'application tierce. • **TPE** : liste des vulnérabilités tierces importées dans votre instance. Contient une liste des références, des éléments vulnérables, des exploits et des CVE connexes. • **Tests** : tests importés à partir des intégrations tierces auxquelles les résultats des tests doivent être conformes.		• sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Applications requises	Rôle requis
	• **Groupes de tests** : liste des groupes/ politiques de tests importés à partir des intégrations tierces. Un groupe de tests contient un ensemble de tests.		
CMDB	• **Éléments détectés** : liste de tous les éléments détectés. • **Images du conteneur détectées** :	Réponse aux vulnérabilités, Réponse aux vulnérabilités des applications, Réponse aux vulnérabilités pour conteneurs, et Conformité de la configuration	• sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT) • sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT) • sn_vul_container.remediation_owne pour les éléments vulnérables de conteneurs (CVIT) • sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)
Demandes d'évaluation de test de pénétration	Les demandes d'évaluation des tests de pénétration que vous avez soumises à l'équipe de sécurité pour effectuer une évaluation de sécurité de toute application d'entreprise. Cette liste contient : • **Affecté à moi** : liste des demandes d'évaluation de test de pénétration que vous avez émises. • **Affecté à mes groupes** : liste des demandes d'évaluation de test de pénétration	Réponse aux vulnérabilités des applications	sn_vul.app_champion_sécurité_

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Applications requises	Rôle requis
	émises par les utilisateurs de vos groupes d'affectation.		
Conclusions du test de pénétration	Liste des vulnérabilités identifiées lors de l'évaluation du test de pénétration effectuée par l'équipe de sécurité : • **Affecté à moi** : liste des conclusions du test de pénétration qui vous sont affectés pour correction. • **Affecté à mes groupes** : liste des conclusions du test de pénétration affectés à vos groupes d'affectation pour correction.	Réponse aux vulnérabilités des applications	sn_vul.app_champion_sécurité_
Données associées	Cette vue de liste contient : • **Sources faisant autorité** : liste des sources faisant autorité qui fournissent des informations récapitulatives utiles pour rechercher les publications sources qui ont été utilisées pour créer l'enregistrement. • **Technologies** : liste des technologies qui fournissent les informations récapitulatives sur chaque source et citation faisant autorité (également	Conformité de la configuration	sn_vulc.remediation_owner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Applications requises	Rôle requis
	appelée, dans Qualys, cadre de travail).		

Information associée

Utiliser la vue de liste dans le Espace de travail du gestionnaire de vulnérabilités

Utilisation du Espace de travail de remédiation IT

Le Espace de travail de remédiation IT fournit une liste consolidée des vulnérabilités d'hôte, d'application, de conteneur et de configuration incorrecte qui vous sont affectées, à vous et à votre groupe. Vous pouvez utiliser cet espace de travail pour corriger et demander des exceptions pour les vulnérabilités et les erreurs de configuration.

Ouvrir les résultats de recherche dans Espace de travail de remédiation IT

Définissez le périmètre de l'application pour Espace de travail de remédiation IT ouvrir vos résultats de recherche dans l'interface utilisateur plutôt que dans l'interface Espace de travail de remédiation IT utilisateur classique en modifiant le périmètre de l'application.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Par exemple, si vous recherchez un élément vulnérable d'hôte avec son numéro dans le champ **Rechercher** en définissant le périmètre de l'application sur Espace de travail de remédiation IT, le VIT s'ouvre dans sa vue d'enregistrement dans le Espace de travail de remédiation IT.

Procédure

1. Dans la barre de navigation unifiée, sélectionnez l'icône globe .
2. Sélectionnez **le périmètre de l'application**, puis définissez le périmètre sur **Espace de travail de remédiation informatique**.

Résultats

Lorsque vous recherchez des enregistrements tels que des VIT, des tâches de rattrapage, des approbations de changement d'état, etc., dans le champ **Rechercher** de la barre de navigation unifiée, les enregistrements s'ouvrent dans le champ .Espace de travail de remédiation IT

Lorsque le périmètre n'est pas Global, l'icône globe s'affiche avec un anneau rouge . Sélectionnez-le à nouveau pour changer le champ d'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser la synthèse d'e-mail dans les espaces de travail Réponse aux vulnérabilités

Utilisez les notifications par e-mail pour afficher la progression de votre rattrapage et vous rappeler quand les tâches approchent ou dépassent le SLA.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

En tant que propriétaire de rattrapage, venez dans votre espace de travail et voyez votre notification par e-mail comme un résumé de votre travail. Voyez ce que vous avez accompli, ce qui approche et ce qui est en retard. Utilisez la notification pour vous aider à organiser et à hiérarchiser vos actions de rattrapage critiques. Cliquez sur un lien dans l'e-mail pour accéder directement à votre espace de travail. Les notifications peuvent aider les spécialistes informatiques à obtenir un aperçu de l'état de leur travail. En tant que responsable des vulnérabilités, aidez vos spécialistes informatiques à accéder à la plateforme directement à partir de leur service de messagerie pour les tâches de correction.

Consultez la rubrique Configurer des notifications par e-mail dans les Réponse aux vulnérabilités espaces de travail pour en savoir plus sur la configuration de cette fonctionnalité.

L'e-mail affiche par défaut les tâches que vous avez fermées, le nombre total de tâches actives qui vous sont affectées, à vous et à vos groupes, les tâches nouvellement affectées, les VIT fermés, ainsi que d'autres informations.

Procédure

1. Accédez à votre e-mail, localisez une notification et cliquez pour l'ouvrir.
   La notification s'affiche avec des informations sur l'état de votre travail.
2. Cliquez sur **Accéder à l'espace de travail** pour accéder à votre espace de travail.

Créer une liste dans le Espace de travail de remédiation IT

Avec la vue de liste dans , Espace de travail de remédiation IT vous pouvez afficher les tâches de rattrapage et les enregistrements qui vous sont affectés, à vous et à vos groupes. Vous pouvez également suivre vos demandes d'exception et de faux positifs pour les tâches de rattrapage (VUL, AVUL, CVIL et CRG), les éléments vulnérables (VIT, AVIT et CVIT) et les résultats des tests (TR) et afficher les solutions.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
2. Cliquez sur l'icône Liste ( ).
   La vue de liste s’affiche.
   - Cliquez sur une liste filtrée pour afficher le nombre total de tâches de rattrapage actives ou d’enregistrements affectés à vous ou à votre groupe. Consultez la rubrique Utiliser des enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT pour plus d’informations sur ce que vous pouvez faire à partir de ces enregistrements.
   - Affichez le nombre total de VI qui vous sont affectés ou qui sont affectés à vos groupes et qui disposent de solutions. Cliquez sur la carte **Solutions préférées sur les VI** pour afficher la liste.
   - Consultez les CI vulnérables qui vous sont affectés, ainsi qu’à vos groupes, qui présentent des vulnérabilités dans l’onglet **CI vulnérables** ou dans la liste des CI vulnérables qui vous sont affectés et qui sont affectés à votre groupe dans la vue de liste.
3. Sélectionnez l'onglet **Mes listes**.
4. Sélectionnez **Ajouter une nouvelle liste**.
5. Créez la liste en fonction d’une liste existante ou de votre propre configuration.

Type de création	Actions
Liste basée sur une liste existante	**a.** Sélectionnez l’onglet **Démarrer à partir de** l’onglet existant. **b.** Dans le champ **Liste** , sélectionnez la liste existante à utiliser comme modèle pour la liste déroulante. **c.** Nommez la liste dans le champ**Nom de** la liste.
Liste nouvellement créée	**a.** Sélectionnez **Créer votre propre** **b.** Nommez la liste dans le champ**Nom de** la liste. **c.** Sélectionnez la source dont vous souhai–tez filtrer les données dans la liste.

6. **Facultatif :** Créez une liste filtrée.
   a. Dans le champ **Sélectionner des colonnes** , déterminez les colonnes qui apparaîtront dans la liste en supprimant les champs que vous ne souhaitez pas afficher.
   b. Fournissez des conditions pour filtrer la liste.
   (Optional) Pour ajouter plus d’une condition, sélectionnez **Nouvel ensemble de conditions**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, si vous souhaitez créer une liste d'éléments vulnérables actifs pour un scanner que vous souhaitez surveiller, vous pouvez entrer les conditions **[Active][is][true]** et **[Source][contains][scanner-name].**

c. Sélectionnez **Créer**.
Votre nouvelle liste s'affiche.

Remarque : Si vous quittez le module de liste, la liste affichée lorsque vous quittez est la liste que vous voyez lorsque vous revenez. Pour supprimer les listes personnalisées que vous créez, avec la liste affichée, à droite du volet, sélectionnez l'icône d'engrenage, puis sélectionnez **Supprimer**.

7. Reportez-vous au tableau suivant pour savoir ce que vous pouvez faire à partir de la vue de liste.

Tâche	Description
Cliquez sur Mes listes	Créez des listes et affichez celles que vous avez créées. Dans le modal qui s'affiche, créez une autre version d'une liste existante ou une nouvelle liste. Les listes que vous créez sont affichées dans l'onglet Ma liste. Pour supprimer une liste, avec la liste affichée, à l'extrême droite de la page, cliquez sur l'icône d'engrenage.
Vous affecter des enregistrements de tâches de rattrapage	Dans l'onglet Listes avec **Affecté à mon groupe** sélectionné, cliquez sur un enregistrement de tâche de rattrapage (VUL) pour l'ouvrir. Dans l'enregistrement qui s'affiche, cliquez sur **Me l'affecter**. Cette option n'est disponible que si aucune tâche de rattrapage ne vous n'est déjà affectée.
Ouvrir une tâche de rattrapage (VUL)	Avec un enregistrement de tâche de rattrapage affiché, cliquez sur un élément de liste connexe pour ouvrir et afficher les détails suivants : ○ Vue d'ensemble : affichez la progression du rattrapage et d'autres détails de la tâche de rattrapage. ○ Solutions : affichez les solutions préférées et potentielles que vous pouvez utiliser pour corriger la vulnérabilité. Dans l'onglet Solutions, les éléments de liste connexes enfants affichent les solutions préférées et les solutions potentielles. ○ Détails : plus d'informations sur la vulnérabilité associée. Vous pouvez modifier ces champs. ○ Demandes de changement : affichez les demandes de changement associées à l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	○ Approbations demandées : affichez les approbations demandées. s'il n'y a aucune approbation de demande de changement, cet élément de liste connexe n'est pas affiché. ○ Approbations de changement de l'état : affichez les faux positifs et les demandes d'exception associés à cet enregistrement. En l'absence de demandes, cet élément de liste connexe n'est pas affiché. Les enregistrements ouverts restent affichés sous forme d'onglets jusqu'à ce que vous les fermiez. Voyez Utiliser des enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT ce que vous pouvez faire à partir de l'enregistrement de la tâche de rattrapage.
Ouvrir un enregistrement d'élément vulnérable (VIT)	Avec un enregistrement d'élément vulnérable affiché, cliquez sur un élément de liste connexe pour ouvrir et afficher les détails suivants : ○ Vue d'ensemble : l'actif affecté, la vulnérabilité associée, la détection initiale et d'autres détails sur l'état et la date cible. ○ Détails : plus d'informations de vue d'ensemble, y compris la solution préférée le cas échéant. Vous pouvez modifier ces champs. ○ Détections : premier trouvé, dernier trouvé, adresse IP, port, protocole et informations de preuve, le cas échéant. ○ Services concernés : criticité opérationnelle, groupe de support et service ○ Tâches de remédiation : tâches de remédiation auxquelles ce VI est associé. Les enregistrements VIT ouverts restent affichés sous forme d'onglets jusqu'à ce que vous les fermiez. Voyez Utiliser des enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT ce que vous pouvez faire à partir de l'enregistrement de la tâche de rattrapage.
Définir des filtres pour une colonne d'une liste	Sélectionnez une colonne et développez le menu de points verticaux pour afficher les options qui filtrent davantage les données de la colonne. Par exemple, dans une liste d'éléments vulnérables sélectionnés, vous préfére–

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	rez peut-être trier la colonne d'évaluation des risques afin que seuls les éléments cri–tiques soient affichés.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ○ Afficher la correspondance : affiche uni–quement les éléments qui correspondent à la cellule sélectionnée dans la colonne. ○ Filtrer : filtre les éléments de la colonne qui correspondent à la cellule sélection–née dans la colonne.
Dans la vue Liste, à gauche de la colonne Numéro avec une liste affichée, passez la souris sur une ligne et cliquez sur la petite icône d'informations (i) pour un enregistrement.	Les détails relatifs aux enregistrements sont affichés dans le panneau latéral droit de la page.

Utiliser des enregistrements dans le Espace de travail de remédiation IT

Utilisez des enregistrements pour vous aider à afficher la progression du rattrapage et l'impact des éléments vulnérables sur vos actifs.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Procédure

1. Dans votre ServiceNow AI Platform instance, accédez à **Espaces de travail** > **Espace de travail de remédiation informatique**.
   La page de destination Accueil s'affiche.
2. Accédez à un enregistrement d'élément vulnérable et ouvrez-le à partir de la page de destination d'accueil ou de la vue de liste.

   L'onglet Détails comprend des informations dans l'en-tête du formulaire en haut qui se rapportent à la nature de la vulnérabilité, par exemple, CVE-2013-5014 détectée sur LINUX-DAL-4331. Sous l'en-tête du formulaire, les valeurs pour l'état, la cote de risque et la date cible de rattrapage sont affichées.
3. Reportez-vous à la table suivante pour connaître les actions d'interface utilisateur que vous pouvez effectuer sur l'enregistrement de tâche de rattrapage.

Tâche	Description
Cliquer sur un lien d'éléments connexes	○ Vue d'ensemble : affichez des détails tels que l'état, la cote de risque, le score de risque, la source, le dernier trouvé, l'état

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	du rattrapage, la vulnérabilité associée, l'élément de configuration affecté et les informations de détection initiale. ○ Détails : plus d'informations sur la vue d'ensemble, y compris la solution privilégiée. Vous pouvez modifier ces champs. ○ Détections : affichez les informations de détection importées à partir de vos scanners. ○ Services impactés : affichez les services impactés par la vulnérabilité. ○ Tâches de rattrapage : affichez les autres tâches de rattrapage associées à cet élément vulnérable. Les enregistrements ouverts à partir du VIT restent affichés sous forme d'onglets sous les onglets d'enregistrement jusqu'à ce que vous les fermiez.
Cliquez sur un lien pour ouvrir un enregistrement	Dans la liste affichée sur les enregistrements ouverts à partir des liens Éléments connexes, affichez plus de détails sur les tâches de rattrapage, les détections et les services impactés.
Cliquer sur une action d'interface utilisateur	○ Me l'affecter : cette option s'affiche uniquement si la tâche de rattrapage ne vous est pas déjà affectée. ○ Marquer comme faux positif : signale lorsqu'un scanner trouve une vulnérabilité mais que vous déterminez qu'aucune vulnérabilité n'existe. Envoyez une demande. ○ Si l'élément vulnérable vous est affecté, vous pouvez analyser à nouveau le VI. ○ Résoudre : résoudre cet élément vulnérable. Les tâches de rattrapage associées passent à l'état Résolu lorsque tous ses VI sont résolus. ○ Demande d'exception : si une date cible est dépassée et que vous savez que vous avez besoin de plus de temps pour résoudre la vulnérabilité, soumettez une demande. ○ Enregistrer : enregistre les changements et met à jour l'enregistrement.
Ajouter une note de travail ou joindre un fichier	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'éclair) et entrez une note de travail. Cliquez sur l'icône pour activer/désactiver le panneau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	Vous pouvez également charger un fichier.
Définir des filtres pour une colonne d'une liste	Sélectionnez une colonne et développez le menu de points verticaux pour afficher les options qui filtrent davantage les données de la colonne. Par exemple, avec l'élément connexe Détections sélectionné, vous préférerez peut-être trier la colonne de sorte que seules les dernières détections trouvées à une certaine date soient affichées.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ○ Afficher la correspondance : affiche uniquement les éléments qui correspondent à la cellule sélectionnée dans la colonne. ○ Filtrer : filtre les éléments de la colonne qui correspondent à la cellule sélectionnée dans la colonne.

Créer une tâche de rattrapage manuellement dans le Espace de travail de remédiation IT

À partir de la version 25.0.4 de Réponse aux vulnérabilités, vous pouvez créer manuellement des tâches de rattrapage à partir des listes Éléments vulnérables d'hôte, Éléments vulnérables d'application, Éléments vulnérables de conteneurs et Résultats des tests de configuration sur la page Liste de Espace de travail de remédiation IT.

Avant de commencer

Rôle requis :

- sn_vul.write_assigned ou sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_write_assigned ou sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.writer_assigned ou sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique** > **Liste**.
2. Sur la page Liste, ouvrez la liste Actif ou Tous dans l'une des listes suivantes :
   - Éléments vulnérables d'hôte
   - Éléments vulnérables de l'application
   - Éléments vulnérables de conteneurs
   - Résultats des tests de configuration
3. Cochez la case des enregistrements que vous souhaitez mettre à jour, puis sélectionnez l'option Éléments sélectionnés dans le champ Sélection d'enregistrement du modal Créer une tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Créer une tâche de rattrapage**.
5. Renseignez les champs suivants du modal Créer une tâche de rattrapage.

Créer un modal de tâche de rattrapage

Champ	Description
Sélection d'enregistrement	**Éléments sélectionnés** : met à jour uniquement les enregistrements sélectionnés.
Description brève	Brève note sur les tâches de rattrapage.
Critères de regroupement	Les choix possibles sont les suivants : ○ **Groupe d'affectation** : les enregistrements avec le même groupe d'affectation sont regroupés en une seule tâche de rattrapage. ○ **Groupe d'affectation et élément de configuration** : les enregistrements avec le même groupe d'affectation et le même élément de configuration sont regroupés en une seule tâche de rattrapage. ○ **Groupe d'affectation et vulnérabilité** : les enregistrements avec le même groupe d'affectation et la même vulnérabilité sont regroupés en une seule tâche de rattrapage. ○ **Groupe d'affectation et cote de risque** : les enregistrements ayant le même groupe d'affectation et la même cote de risque sont regroupés en une seule tâche de rattrapage.
Gestion des enregistrements dans d'autres tâches de remédiation	Les choix possibles sont les suivants : ○ **Ignorer les enregistrements pour les nouvelles tâches de rattrapage** : aucune action n'est effectuée sur les enregistrements qui font partie d'autres tâches de rattrapage. ○ **Déplacer vers les nouvelles tâches de rattrapage** : les enregistrements qui font partie d'autres tâches de rattrapage sont transférés vers les nouvelles tâches de rattrapage. ○ **Conserver les tâches de rattrapage actuelles et nouvelles** : les enregistrements qui font partie d'autres tâches de rattrapage sont conservés dans les anciennes et les nouvelles tâches de rattrapage.

6. Sélectionnez **Créer une tâche de rattrapage**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Les tâches de remédiation sont créées en fonction des critères de regroupement. Une notification par e-mail est envoyée aux propriétaires de rattrapage du groupe d'affectation, les informant qu'une tâche de rattrapage a été créée et affectée à leur groupe. Pour obtenir des exemples sur la façon dont les tâches de rattrapage sont créées en fonction des critères de regroupement et des critères de gestion des enregistrements, reportez-vous à la section Exemples de création de tâches de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités et Espace de travail de remédiation IT.

Utiliser des enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT

Les tâches de rattrapage sont créées et affectées automatiquement à partir des efforts de rattrapage. Les équipes informatiques et les propriétaires de rattrapage peuvent afficher les tâches de rattrapage dans le Espace de travail de remédiation IT.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Lorsque les gestionnaires et les analystes de vulnérabilité créent des efforts de correction pour favoriser la correction, les tâches de correction sont créées automatiquement et affectées aux équipes informatiques en fonction du groupe associé aux enregistrements dans un effort de correction.

Consultez les CI vulnérables qui vous sont affectés, ainsi qu'à vos groupes, qui présentent des vulnérabilités dans l'onglet **CI vulnérables** ou dans la liste des CI vulnérables qui vous sont affectés et qui sont affectés à votre groupe dans la vue de liste.

Procédure

1. Dans votre ServiceNow AI Platform instance, accédez à **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
   La page de destination Accueil s'affiche.
2. Dans la section Tâches de rattrapage, cliquez sur une tâche de rattrapage pour l'ouvrir.
3. **Facultatif :** Vous pouvez également cliquer sur l'icône Liste en haut à gauche de la page d'accueil pour afficher toutes les tâches de rattrapage (VUL, AVUL, CVUL et CRG) et les enregistrements (VIT, AVIT, CVIT et TR) affectés à vous et à vos groupes.
   Pour plus d'informations sur l'utilisation de la vue de liste, reportez-vous à la section Créer une liste dans le Espace de travail de remédiation IT.
4. À partir de la page d'accueil ou de la vue de liste, cliquez sur une tâche de rattrapage pour l'ouvrir.

   Dans l'onglet **Détails** , vous pouvez mettre à jour certaines informations de l'enregistrement, telles que le groupe d'affectation, l'état, la description brève, etc. Cliquez sur **Enregistrer** pour appliquer vos modifications.
5. Reportez-vous à la table suivante pour connaître les actions d'interface utilisateur que vous pouvez effectuer à partir de l'enregistrement de tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
Cliquer sur un lien d'éléments connexes	○ Vue d'ensemble : affichez la progression de votre rattrapage avec le % de VI rattrapés, l'état, la cote de risque, le groupe d'affectation, les CI affectés et d'autres détails sur les tâches. Pour voir les CI affectés, reportez-vous à l'image suivant le tableau. ○ Solutions : affichez les solutions préférées et potentielles que vous pouvez utiliser pour corriger la vulnérabilité. Sur l'enregistrement qui s'affiche, les éléments de liste connexes enfants affichent les solutions privilégiées et les solutions potentielles. Voir les images sous le tableau. ○ Détails : plus d'informations sur la vulnérabilité associée. Vous pouvez modifier ces champs. ○ Demandes de changement : affichez les demandes de changement associées à l'enregistrement. ○ Approbations demandées : affichez les soumissions de demandes de changement. s'il n'existe aucune demande d'approbation de demande de changement, cet élément de liste connexe n'est pas affiché. ○ Approbations de changement de l'état : affichez les faux positifs et les demandes d'exception associés à cet enregistrement. En l'absence de demandes, cet élément de liste connexe n'est pas affiché. Les enregistrements ouverts restent affichés sous forme d'onglets jusqu'à ce que vous les fermiez.
Cliquez sur un lien pour ouvrir un enregistrement	Dans la liste affichée sur les enregistrements ouverts à partir des liens Éléments connexes, affichez plus de détails sur les enregistrements, les vulnérabilités associées, les CI affectés (actifs), les données de détection, les services impactés et les enregistrements associés.
Cliquer sur une action d'interface utilisateur	○ Me l'affecter : cette option s'affiche uniquement si la tâche de rattrapage ne vous est pas déjà affectée. ○ Marquer comme faux positif : soumettez une demande si, par exemple, un scanner détecte une vulnérabilité mais que

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	vous déterminez qu'aucune vulnérabilité n'existe. ○ Créer un changement : vous pouvez créer une nouvelle demande de changement ou ajouter cette tâche de rattrapage à une demande de changement existante. ○ Fractionner la tâche : identifiez un sous-ensemble de VI que vous souhaitez inclure dans une nouvelle tâche de rattrapage ○ Demande d'exception : soumettez une demande si une date cible est dépassée et que vous savez avoir besoin de plus de temps pour résoudre la vulnérabilité. ○ Résoudre : résoudre ce RT. La tâche de rattrapage passe à l'état Résolu et tous ses VI passent à Résolu. ○ Enregistrer : enregistre les changements et met à jour l'enregistrement.
Ajouter une note de travail ou joindre un fichier	Tout à droite de l'écran, cliquez sur l'icône **Activité** (icône d'éclair) et entrez une note de travail. Cliquez sur l'icône pour activer/désactiver le panneau. Vous pouvez également charger un fichier.
Définir des filtres pour une colonne d'une liste	Sélectionnez une colonne et développez le menu vertical à trois points pour afficher les options qui filtrent davantage les données de la colonne. Par exemple, une fois l'élément associé à la vue d'ensemble sélectionné, vous préférerez peut-être trier la colonne de cote de risque afin que seuls les éléments critiques s'affichent.
Filtrer une colonne par une ligne sélectionnée	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ○ Afficher la correspondance : affiche uniquement les éléments qui correspondent à la cellule sélectionnée dans la colonne. ○ Filtrer : filtrer les éléments de la colonne qui correspondent à la cellule sélectionnée dans la colonne.

L'onglet Solutions d'une tâche de rattrapage de l'hôte vous montre les informations sur les solutions préférées et potentielles qui correspondent le mieux à la vulnérabilité associée à la tâche de rattrapage. Les solutions sont des correctifs que vos équipes informatiques appliquent pour résoudre les vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si l'application Gestion des solutions de vulnérabilité est installée, les *solutions privilégiées* sont celles qui sont appliquées aux éléments vulnérables. La liste des solutions est basée sur les éléments vulnérables de la tâche de rattrapage de l'hôte.

Les solutions potentielles sont la liste de toutes les solutions disponibles pour les VIT dans une tâche de rattrapage d'hôte.

Vous pouvez afficher les CI (actifs) affectés par cette vulnérabilité sur la tâche de rattrapage en accédant à **Vue d'ensemble** > **CI affectés**.

Vous affecter une tâche ou un enregistrement de rattrapage dans Espace de travail de remédiation IT

Affectez-vous une tâche de rattrapage (VUL, AVUL, CVIL ou CRG) ou un enregistrement (VIT, AVIT, CVIT ou TR) à partir de la page Liste de l'espace de Espace de travail de remédiation IT travail.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique** > **Liste** > **Tâches de rattrapage** > **Affecté à mon groupe**.
2. Ouvrez une tâche de rattrapage (VUL, AVUL, CVUL ou CRG) à partir de la liste des tâches de rattrapage.
3. Dans les boutons d'action d'interface utilisateur à droite, cliquez sur **Me l'affecter**.

   Le bouton **Me l'affecter n'est** disponible que si l'enregistrement ne vous est pas déjà affecté.

   La tâche de rattrapage s'affiche dans la liste Mes affectations sous Tâches de rattrapage.
4. Vous pouvez également vous affecter un enregistrement (VIT, AVIT, CVIT ou TR) en suivant les mêmes étapes qu'un enregistrement ouvert.
   Le bouton **Me l'affecter n'est** disponible que si l'enregistrement ne vous est pas déjà affecté.

Afficher les éléments de configuration présentant des vulnérabilités dans Espace de travail de remédiation IT

Les améliorations suivantes ont été ajoutées aux tâches de rattrapage avec la version 16.1 de l'application Réponse aux vulnérabilités .

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le rôle itil ou cmdb_read est également requis si vous souhaitez afficher les données CI dans les espaces de travail.

Pourquoi et quand exécuter cette tâche

Consultez les éléments de configuration (CI) qui vous sont affectés et qui présentent des vulnérabilités. Cliquez sur **Tableau de résultats des CI impactés** . Cliquez sur la liste Filtre en haut à gauche pour basculer entre **Affecté à moi-même** et **Affecté à mes groupes**. À partir de la vue de liste, cliquez sur les liens.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
   La page de destination Accueil s'affiche.
2. Vous pouvez également afficher ces listes à partir des liens de la vue de liste ou en accédant à leurs modules, par exemple : **Tous** > **Réponse aux vulnérabilités** > **Tâches de remédiation**.
3. Choisissez-en un pour continuer.
   En fonction de ce qui est sélectionné dans l'activation/désactivation du filtre, affichez les listes des enregistrements suivants qui vous sont affectées ou qui sont affectées à vous et à vos groupes.

Option	Description
Tâche de rattrapage affectée	Tâches de rattrapage (RT). Pour plus d'informations sur les actions que vous pouvez effectuer à partir d'un RT, reportez-vous à la section Utiliser des enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT.
Solution privilégiée sur les VI	Enregistrements (VIT) auxquels des solutions préférées sont mappées. Si l'application Gestion des solutions de vulnérabilité est installée, les solutions privilégiées sont les solutions de remplacement les plus élevées appliquées aux enregistrements. La liste des solutions est basée sur les enregistrements de l'enregistrement de la tâche de rattrapage. Pour voir ce que vous pouvez faire à partir des enregistrements de solution, reportez-vous à la section Utiliser des enregistrements de tâche de rattrapage dans le Espace de travail de remédiation IT.
CI impactés	(CI) avec des vulnérabilités. Une fois son remplissage initial, ce tableau de résultats affiche les nombres mis à jour de vos CI vulnérables après l'ajout de nouveaux VI présentant des vulnérabilités, ou lorsque des changements d'état sont apportés aux VI existants. Consultez les étapes suivantes pour savoir comment afficher cet enregistrement et ce que vous pouvez faire à partir de cette liste.

4. Cliquez sur le tableau **de résultats CI impactés** .

   La liste des enregistrements de CI s'affiche.
5. Cliquez sur un élément de configuration pour ouvrir son enregistrement.
   L'enregistrement s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les listes connexes vous permettent d'afficher les détails et divers enregistrements associés. Les nouvelles données disponibles sur cet enregistrement avec cette version comprennent :

- Une chronologie qui affiche l'activité récente sur cet enregistrement.
- Toutes les demandes de changement associées à ce CI.
- Accédez facilement aux tableaux de résultats et affichez les tâches de rattrapage, les éléments vulnérables et les solutions privilégiées associés à ce CI.
- Vous pouvez accéder aux tableaux de résultats et afficher les correctifs préférés associés à ce CI. Les correctifs préférés sont les correctifs associés aux éléments vulnérables. L'onglet Correctifs de la liste connexe affiche les correctifs installés et manquants pour les CI.
- Informations sur le CI, notamment la classe, l'emplacement, l'orientation vers Internet, l'environnement et le calendrier de maintenance.

Créer une demande de changement dans Espace de travail de remédiation IT

Depuis une tâche de rattrapage (VUL, AVUL, CVUL ou CRG), créez une demande de changement. Vous pouvez également ajouter une tâche de rattrapage à une demande de changement existante.

Avant de commencer
Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Remarque : Le rôle itli est requis si vous souhaitez soumettre des demandes de changement à partir du Espace de travail de remédiation IT.

Pourquoi et quand exécuter cette tâche
Il peut y avoir plusieurs raisons pour lesquelles vous voulez créer une demande de changement pour une tâche de rattrapage. En général, c'est parce que votre enquête nécessite une intervention manuelle pour corriger les vulnérabilités.

Pour plus d'informations sur les demandes de changement et la création de demandes de changement à partir de l'environnement classique, reportez-vous à la section Change Management pour Réponse aux vulnérabilités.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Sélectionnez l'icône Liste.
3. Sur la page Liste, dans la liste Tâches de rattrapage, localisez une tâche de rattrapage (VUL, AVUL, CVUL ou CRG) pour laquelle vous souhaitez créer une demande de changement.
4. Dans les boutons d'action d'interface utilisateur situés à droite, développez la liste et choisissez-en un :
   - Cliquer sur **Créer un changement**
   - **Ajouter au changement existant**
5. Pour créer une nouvelle demande de changement, renseignez les champs du modal qui s'affiche.
   Pour en savoir plus sur les champs du formulaire, reportez-vous à la rubrique Champs de formulaire de demande de création de changement.
6. Sélectionnez **Créer une demande de changement**.
   L'enregistrement de la tâche de rattrapage s'affiche et un message indique que la demande de changement a été créée avec succès.

   Cliquez sur le lien connexe Demandes de changement sur un enregistrement pour afficher toutes les demandes de changement associées à l'enregistrement.
7. Pour ajouter cette tâche de rattrapage à une demande de changement existante, procédez comme suit.

   a. Cliquez sur la flèche vers le bas pour développer la liste sur le bouton **Créer un changement** .

   b. Sélectionnez **Ajouter au changement existant**.

   c. Dans la fenêtre modale qui s'affiche, cliquez sur l'icône de recherche pour afficher la liste des demandes de changement existantes.

   d. Pour ajouter des conditions à la liste afin de cibler la liste des demandes de changement, dans l'angle supérieur droit de la fenêtre modale, cliquez sur l'icône de filtre (entonnoir).

   e. Dans le nouveau volet qui s'affiche, cliquez sur **Vue avancée**.

   f. Utilisez le générateur de conditions pour créer vos conditions.

   g. Sélectionnez **Mettre à jour**.

   h. Dans la liste, cliquez sur une demande de changement pour la sélectionner.
   Une fenêtre modale mise à jour s'affiche avec votre choix.

   i. **Facultatif :** Dans le modal, cochez la case Ajouter des CI au CR pour ajouter des éléments de configuration à partir de tous les éléments vulnérables actifs à la demande de changement.

   j. Sélectionnez **Ajouter un changement**.
   L'enregistrement de rattrapage s'affiche et un message indique que la demande de changement a été créée et soumise pour approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cliquez sur le lien **Afficher le changement** dans le message pour ouvrir l'enregistrement de la demande de changement (CHG).
- Sélectionnez le lien de menu d'élément connexe **Demandes de changement** sur l'enregistrement de tâche de rattrapage pour afficher toutes les demandes de changement associées à l'enregistrement.

Dans l'environnement classique, vous pouvez également accéder à **Libre-service** > **Mes demandes**. Une fois que vous avez soumis le changement et qu'il est implémenté, si la synchronisation d'état est activée, la tâche de rattrapage passe automatiquement à Résolu. Pour plus d'informations sur les états et la synchronisation des états dans les demandes de changement, reportez-vous à la section Créer une demande de changement à partir d'une tâche de rattrapage.

Fractionner une tâche de rattrapage dans le Espace de travail de remédiation IT

Depuis une tâche de rattrapage (VUL, AVUL, CVIL ou CRG), identifiez un sous-ensemble d'enregistrements et créez une nouvelle tâche de rattrapage pour eux.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Vous pouvez sélectionner des enregistrements individuels dans l'onglet Vue d'ensemble d'une tâche de rattrapage et les déplacer vers une nouvelle tâche de rattrapage.

Les cas d'utilisation permettant de diviser des enregistrements (VIT, AVIT, CVIT ou CTR) de tâches de rattrapage existantes en nouvelles tâches peuvent inclure les exemples suivants :

- Vous souhaitez créer une ou plusieurs demandes de changement pour une tâche fractionnée.
- Vous souhaitez réaffecter une tâche fractionnée à un autre utilisateur de votre groupe d'affectation.
- Vous demandez un report ou une exception pour une tâche fractionnée, car vous savez que certaines vulnérabilités sur des éléments de configuration (CI) spécifiques ne peuvent pas être corrigées à la date cible.

Pour plus d'informations sur les demandes de changement et le fractionnement d'une tâche de rattrapage dans l'environnement classique et pour les versions antérieures Réponse aux vulnérabilités à la version 15.0, reportez-vous à la section Fractionner une tâche de rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Ouvrez une tâche de rattrapage (VUL, AVUL, CVIL ou CRG) à partir de la page d'accueil ou de la page de liste.
3. Dans l'onglet Vue d'ensemble, sélectionnez les enregistrements (VIT, AVIT, CVIT ou CTR) que vous souhaitez déplacer vers une nouvelle tâche de rattrapage.
4. Cliquez sur **Fractionner la tâche**.
5. Dans la boîte de dialogue qui s'affiche, le nombre d'enregistrements (VIT, AVIT, CVIT ou CTR) que vous avez sélectionnés dans la liste s'affiche.
6. Cliquez à nouveau sur **Fractionner la tâche** .
   Un message de confirmation s'affiche avec un lien vers la nouvelle tâche de rattrapage.

   Vous pouvez également utiliser le générateur de conditions pour filtrer les enregistrements (VIT, AVIT, CVIT ou CTR).
7. Localisez la tâche de rattrapage que vous souhaitez diviser.
8. Dans les boutons d'action d'interface utilisateur situés à droite, cliquez sur **Fractionner la tâche**.
   Après quelques instants, le générateur de conditions s'affiche.
9. Dans la fenêtre modale qui s'affiche, utilisez le générateur de conditions pour identifier le sous-ensemble d'enregistrements (VIT, AVIT, CVIT ou CTR) que vous souhaitez ajouter à une nouvelle tâche de rattrapage.
10. Cliquez sur **Fractionner la tâche**.
    Si un message indique qu'aucun enregistrement ne correspond à vos conditions, vous devez ajuster vos critères et cliquer à nouveau sur **Fractionner la tâche** . Modifiez le champ Description brève selon vos besoins. Ce champ peut vous aider à trouver votre nouvelle tâche de rattrapage après sa création.

    Si les enregistrements correspondent à vos conditions, le nombre d'enregistrements correspondants s'affiche dans un message.
11. **Facultatif :** Cliquez sur le lien **Prévisualiser les éléments** pour afficher les enregistrements qui correspondent à vos conditions de filtre.
    La nouvelle tâche de rattrapage s'affiche sous la forme d'un nouvel onglet.

Demander un faux positif pour un élément vulnérable ou une tâche de rattrapage

Indiquez une demande de faux positif pour un élément vulnérable d'hôte (VIT), un élément vulnérable d'application (AVIT), un élément vulnérable de conteneur (CVIT) ou une tâche de rattrapage (VUL, AVUL, CVUL ou CRG) dans le Espace de travail de remédiation IT. Un faux positif est une condition dans laquelle un scanner signale de manière incorrecte l'existence

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'une vulnérabilité dans le système en raison de situations telles qu'une classification incorrecte, une logique incorrecte ou un algorithme dans le scanner.

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Pour en savoir plus sur la procédure de demande d'un faux positif pour un ensemble de résultats de test, reportez-vous à la section Demander un faux positif pour un ensemble de résultats des tests.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Sélectionnez l'icône Liste (icône).
3. Sélectionnez la tâche de rattrapage (VUL, AVUL, CVUL ou CRG) ou l'élément vulnérable (VIT, AVIT ou CVIT).
4. Sélectionnez **Marquer comme faux positif**.
5. Saisissez des informations sur la demande.
6. Sélectionnez **Demander l'approbation**.
7. Fournissez des informations supplémentaires sur votre demande à l'approbateur et sélectionnez **Soumettre**.

> **Remarque :** Le modal Répondre au questionnaire s'affiche uniquement lorsque la case **Activer le questionnaire pour marquer comme faux positif** est cochée dans le formulaire Configuration de gestion des exceptions. Pour plus d'informations, consultez Configurer la gestion des exceptions pour Réponse aux vulnérabilités,Configurer la gestion des exceptions pour Réponse aux vulnérabilités des applications, Configurer la gestion des exceptions pour Réponse aux vulnérabilités pour conteneurs et Configurer la gestion des exceptions pour Conformité de la configuration.

Résultats

L'état de l'élément vulnérable (VIT, AVIT ou CVIT) ou de la tâche de rattrapage (VUL, AVUL ou CVUL) passe à l'état En cours de révision.

Votre demande est soumise pour approbation et l'approbateur reçoit une notification par e-mail concernant votre demande.

Vous recevrez une notification par e-mail lors de l'approbation ou du rejet de votre demande.

Que faire ensuite

Dans l'espace de travail Rattrapage informatique, sur la page Liste, accédez à **Demandes d'exception** > **Mes demandes** et ouvrez l'enregistrement d'approbation de changement d'état correspondant (VCA#) et vérifiez l'état de votre demande dans la colonne État d'approbation :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État d'approbation	Enregistrement (VIT, AVIT ou CVIT)	Tâche de rattrapage (VUL, AVUL, CVIL ou CRG)
Approuvé	L'état de l'enregistrement passe à Fermé avec le motif Faux positif.	L'état de la tâche de rattrapage passe à Fermé avec le motif Faux positif. En conséquence, l'état est transmis aux enregistrements dans la tâche de rattrapage. Accédez à l'onglet Détails d'une tâche de rattrapage et définissez la date d'expiration du faux positif dans le champ **Jusqu'à** si nécessaire. La tâche de rattrapage revient à l'état Ouvert après la date spécifiée et l'état est réduit aux résultats des tests.
Rejeté	L'état de l'enregistrement ne change pas.	L'état de la tâche de rattrapage et de ses enregistrements revient à l'état précédent.

Dans le **flux d'activité** d'un enregistrement ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de la demande de faux positif.

Information associée

Vue d'ensemble des faux positifs

Demander un faux positif pour un ensemble de résultats des tests

Émettez une demande de faux positif pour un ensemble de résultats de tests dans une tâche de rattrapage dans le Espace de travail de remédiation IT.

Pourquoi et quand exécuter cette tâche

Les conditions suivantes doivent être remplies pour que vous puissiez demander un faux positif pour un ensemble de résultats de tests dans une tâche de rattrapage :

- La version 22.0 de Réponse aux vulnérabilités doit être installée.
- Au moins un résultat de test sélectionné doit être à l'état actif
- La tâche de rattrapage doit avoir au moins deux résultats des tests
- Au moins un résultat de test n'est pas sélectionné

Avant de commencer

Rôle requis : sn_vulc.remediation_owner

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Cliquez sur l'icône Liste ( ).
3. Sur la page Liste, sélectionnez la tâche de Conformité de la configuration rattrapage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la liste connexe Vue d'ensemble, sous l'onglet Résultats des tests, sélectionnez les résultats des tests que vous souhaitez marquer comme faux positifs.
5. Sélectionnez le bouton **Marquer comme faux positif** dans l'onglet Résultats des tests de configuration.
6. Dans la boîte de dialogue qui s'affiche, entrez des informations sur la demande et sélectionnez **Demander l'approbation**.
7. Dans la fenêtre modale Répondre au questionnaire, répondez aux questions pour fournir des informations supplémentaires sur votre demande à l'approbateur et sélectionnez **Soumettre**.

> **Remarque :** Le modal Répondre au questionnaire s'affiche uniquement lorsque la case **Activer le questionnaire pour marquer comme faux positif** est cochée dans le formulaire Configuration de gestion des exceptions. Pour en savoir plus sur la configuration d'un questionnaire, reportez-vous à la section Configurer la gestion des exceptions pour Conformité de la configuration.

Résultats

Les résultats des tests sélectionnés sont déplacés vers une nouvelle tâche de rattrapage et votre demande est soumise pour approbation. Le numéro de tâche apparaît dans le **flux d'activité** de l'ancienne tâche de rattrapage. L'approbateur reçoit une notification par e-mail concernant votre demande.

Vous recevrez une notification par e-mail concernant l'approbation ou le rejet de votre demande. Dans le **flux d'activité** d'un résultat de test ou d'une tâche de rattrapage, vous pouvez afficher l'ensemble du workflow de la demande de faux positif.

Que faire ensuite

1. Dans le Espace de travail de remédiation IT, sur la page Liste, accédez à **Demandes d'exception** > **Mes demandes**.
2. Ouvrez l'enregistrement d'approbation de changement d'état correspondant (VCA#) et vérifiez l'état de votre demande dans la colonne État d'approbation :

État d'approbation	Résultat
Approuvé	L'état de la nouvelle tâche de rattrapage passe à Fermé avec un motif de faux positif.
Rejeté	L'état de la nouvelle tâche de rattrapage devient Ouvert.

3. Une fois la demande approuvée, accédez à l'onglet Détails de la nouvelle tâche de rattrapage et définissez la date d'expiration du faux positif dans le champ **Jusqu'à** si nécessaire.

   La tâche de rattrapage revient à l'état Ouvert après la date spécifiée et l'état est réduit aux résultats des tests.

Demander une exception dans le Espace de travail de remédiation IT

Demander une exception pour l'élément vulnérable d'hôte (VIT), l'élément vulnérable d'application (AVIT), l'élément vulnérable de conteneur (CVIT) et la tâche de rattrapage (VUL, AVUL, CVIL ou CRG) à partir Espace de travail de remédiation IT du .

Avant de commencer

Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Certaines vulnérabilités peuvent ne pas avoir de correctif, de correctif ou de solution existant. Vous pouvez également déterminer qu'une tâche de rattrapage ne peut pas être résolue à la date cible. Lorsque votre rattrapage ne peut pas être conforme à une politique, une norme ou une directive publiée en matière de gestion des vulnérabilités ou de sécurité, vous pouvez demander une exception.

Vous pouvez demander des exceptions pour les tâches de Espace de travail de remédiation IT rattrapage (VUL, AVUL, CVIL ou CRG) et les éléments vulnérables (VIT, AVIT ou CVIT) qui vous sont affectés.

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

À partir de la version 18.0, vous pouvez demander des exceptions pour les éléments de vulnérabilité d'application et les éléments de vulnérabilité de conteneur.

Pour plus d'informations sur la demande d'exceptions dans l'environnement classique, reportez-vous à la section Demander une exception pour une tâche de rattrapage.

Procédure

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Espace de travail de remédiation informatique**.
2. Sélectionnez l'icône Liste.
3. Dans la liste des tâches de rattrapage, ouvrez une tâche de rattrapage (VUL, AVUL, CVIL ou CRG) ou un enregistrement (VIT, AVIT ou CVIT) pour lequel vous souhaitez demander une exception.
4. Dans les boutons d'action d'interface utilisateur situés à droite, cliquez sur **Demande d'exception**.
5. Dans la boîte de dialogue qui s'affiche, renseignez la date de fin de l'exception, sélectionnez un motif dans la liste et ajoutez toute autre information requise.
6. Cliquez sur **Demande d'exception**.
7. Dans la fenêtre modale **Répondre au questionnaire** , répondez aux questions et cliquez sur **Soumettre**.

Remarque : Le modal **Répondre au questionnaire** s'affiche uniquement lorsque la case **à cocher Activer le questionnaire pour demander une exception** est cochée dans le formulaire **Configuration de gestion des exceptions** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un message indique que votre demande est soumise avec succès pour approbation.

Une demande d'exception pour une tâche de rattrapage est approuvée à l'aide d'un workflow d'approbation par défaut à deux niveaux. Une fois que la demande est approuvée par l'approbateur de niveau 1, elle est envoyée à l'approbateur de niveau 2.

- La tâche ou l'enregistrement de rattrapage passe à En cours de révision lorsque la demande d'exception est ouverte.
- La tâche ou l'enregistrement de rattrapage passe à l'état Différé si la demande est approuvée.
- L'enregistrement de demande d'exception (VCA#) est fermé une fois votre demande d'exception approuvée.

Pour afficher l'état de vos demandes d'approbation, cliquez sur Mes demandes sous Demandes d'exception de la page **Liste**. Le numéro de la demande (VCA#) s'affiche lorsque vous ouvrez l'enregistrement ou la tâche de rattrapage dans la liste.

- Si la demande est rejetée, l'enregistrement de demande (VCA#) affiche **Rejeté** dans la colonne État d'approbation de votre vue de liste sous Mes demandes.
- Vous devez soumettre une nouvelle demande d'exception si vous souhaitez toujours différer cet élément.

Demander une exception à l'aide de GRC : Gestion de la politique et de la conformitéEspace de travail de remédiation IT

Demander une exception de politique pour l'élément vulnérable de l'hôte (VIT), l'élément vulnérable de l'application (AVIT), l'élément vulnérable du conteneur (CVIT) ou la tâche de rattrapage (VUL, AVUL, CVIL ou CRG) à partir Espace de travail de remédiation IT du .

Avant de commencer

Rôle requis :

- sn_vul.remediation_owner pour les éléments vulnérables d'hôte (VIT)
- sn_vul.app_security_champion pour les éléments vulnérables de l'application (AVIT)
- sn_vul_container.remediation_owner pour les éléments vulnérables de conteneurs (CVIT)
- sn_vulc.remediation_owner pour les résultats des tests de configuration (CTR)

Pourquoi et quand exécuter cette tâche

Remarque : À partir de la version 19.0 de Réponse aux vulnérabilités, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 19.0	Terminologie v19.0 et ultérieures
Groupes de résultats des tests	Tâches de remédiation
Problèmes de configuration	Résultats des tests de configuration
Politique	Groupe de test

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Dans le navigateur d'application, sélectionnez l'icône Liste (icône ).
3. Sur la page Liste, sous Éléments vulnérables d'hôte, Éléments vulnérables d'applications, Éléments vulnérables de conteneurs ou Tâches de rattrapage (VUL, AVUL, CVIL ou CRG), sélectionnez l'enregistrement pour lequel vous souhaitez demander une exception.
   L'enregistrement que vous sélectionnez doit être à l'état Ouvert, En cours d'examen ou En attente d'implémentation.
4. Sélectionnez le bouton **Demande d'exception** .
5. Remplissez les champs du formulaire.
   Pour plus d'informations sur les champs de formulaire, consultez Champs de formulaire de demande d'exception pour les exceptions de politique.
6. Sélectionnez **Demander une exception**.
7. Dans la fenêtre modale Répondre au questionnaire, répondez aux questions pour fournir des informations supplémentaires sur votre demande et sélectionnez **Soumettre**.

   Remarque : Le modal Répondre au questionnaire s'affiche uniquement lorsque les détails du questionnaire sont ajoutés au registre d'intégration respectif.

   Un message indique que votre demande est soumise avec succès pour approbation.

   Pour plus d'informations sur l'intégration des exceptions de politique et le transfert entre le propriétaire du rattrapage et le gestionnaire de conformité, consultez Configuration facultative de Policy and Compliance Management .

Demander une réduction du risque pour un élément vulnérable ou une tâche de rattrapage

Demandez une réduction du risque pour un élément vulnérable de l'hôte ou une tâche de rattrapage dans le Espace de travail de remédiation IT.

Avant de commencer

Rôle requis : sn_vul.remediation_owner

Pourquoi et quand exécuter cette tâche

À partir de la version 21.0 de , vous ne pouvez demander une réduction du Réponse aux vulnérabilitésrisque que pour les éléments suivants :

- Une tâche de rattrapage uniquement si tous ses éléments vulnérables sont associés à la même entrée de vulnérabilité commune (CVE), que sa réduction du risque soit activée ou non pour les CVE.
- Un tiers (TPE) pour lequel la réduction du risque est activée.

Remarque : La fonctionnalité de contrôles de compensation est disponible uniquement pour les vulnérabilités de l'hôte.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de remédiation informatique**.
2. Cliquez sur l'icône Liste ().
3. Sur la page Liste, ouvrez un élément vulnérable d'hôte ou une tâche de rattrapage.
4. Sélectionnez l'icône Autres options, puis Demande **d'exception**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Renseignez les champs du formulaire Demande d'exception.
   Pour obtenir une description des valeurs de champ, consultez Formulaire de demande d'exception pour la réduction du risque.
6. Sélectionnez **Demander une exception**.
7. Si un modal Répondre au questionnaire s'affiche, répondez aux questions pour fournir des informations supplémentaires sur votre demande et sélectionnez **Soumettre**.

> **Remarque :** Le modal Répondre au questionnaire s'affiche uniquement lorsque le questionnaire est activé pour la gestion des exceptions. Pour plus d'informations, consultez Configurer la gestion des exceptions pour Réponse aux vulnérabilités.

Résultats
Un message s'affiche indiquant que votre demande a été soumise avec succès pour approbation. Une notification concernant votre demande est envoyée à l'approbateur.

- Si votre demande porte sur un report et une réduction des risques :
  - Deux approbations de changement d'état (VCA#) sont créées pour le report et la réduction des risques.
  - L'état de l'enregistrement est défini sur En cours de révision.
- Si votre demande vise uniquement la réduction des risques :
  - Une approbation de changement d'état (VCA#) est créée.
  - L'état ne change pas.

Lors de l'approbation ou du rejet de votre demande, vous recevrez une notification. Pour plus d'informations sur le processus d'approbation, reportez-vous à Approuver ou rejeter les demandes dans le Espace de travail du gestionnaire de vulnérabilités.

Pour plus d'informations sur la façon dont la **date de fin de la réduction du risque** est mise à jour pour une tâche de rattrapage et un élément vulnérable lorsqu'une demande de réduction du risque est approuvée, reportez-vous à la section Impact des contrôles compensatoires sur le score de risque et la date d'expiration.

Information associée

Comprendre les contrôles compensatoires pour la réduction des risques

Désactiver ou activer la réduction du risque pour une CVE ou une TPE

Ajouter un contrôle de compensation à la bibliothèque

Impact des contrôles compensatoires sur le score de risque et la date d'expiration

Analyser de nouveau les éléments vulnérables et les tâches de rattrapage dans le Espace de travail de remédiation IT

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Lancez de nouvelles analyses à partir de dans Espace de travail de remédiation IT votre ServiceNow AI Platform On-demand.

Les nouvelles analyses vous permettent de vérifier que vos activités de rattrapage, correctifs et autres actions ont correctement corrigé des vulnérabilités spécifiques sur vos éléments de configuration (CI).

La nouvelle analyse est prise en charge pour les intégrations suivantes dans le Espace de travail de remédiation IT. Consultez les rubriques suivantes pour plus d'informations :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Analyser Qualys de nouveau les Réponse aux vulnérabilités éléments vulnérables à partir des espaces de travail
- Analyser Rapid7 de nouveau les Réponse aux vulnérabilités éléments vulnérables à partir des espaces de travail
- Analyser Tenable.io de nouveau et Tenable.sc les éléments vulnérables à partir des espaces de Réponse aux vulnérabilités travail

Rôles requis : sn_vul.remediation_owner pour le Espace de travail de remédiation IT

Analyser Qualys de nouveau les Réponse aux vulnérabilités éléments vulnérables à partir des espaces de travail

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Lancez de nouvelles analyses du produit à Qualys la demande à partir de Espace de travail de remédiation IT votre ServiceNow AI Platform instance.

Avant de commencer

Pour lancer une nouvelle analyse du produit à Qualys partir de l'environnement classique, reportez-vous à la section Lancer une nouvelle analyse pour le Qualys Vulnerability Integration.

Les Qualys scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont ces applications comme source, le bouton **Analyser de nouveau** n'est pas disponible.

Pour activer ces scanners, en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin :

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Recherchez le produit de scanner que vous souhaitez activer et cliquez sur l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher Activé.
4. Cliquez sur **Mettre à jour**.

   Le produit que vous avez activé s'affiche dans le champ Source sur les enregistrements d'élément vulnérable et de tâche de rattrapage après la prochaine importation, et **Analyser à nouveau** est disponible en tant qu'action d'interface utilisateur.

Pour plus d'informations sur la configuration de votre Qualys scanner, reportez-vous aux sections Configurer les dispositifs de scanner et Configurations et modifications avancées Qualys.

- Vous pouvez lancer de nouvelles analyses à la demande pour les éléments vulnérables et les tâches de rattrapage qui ont le Qualys produit comme source à partir de votre Espace de travail de remédiation ITServiceNow AI Platform.
- Sur un enregistrement de tâche de rattrapage, l'enregistrement peut être dans n'importe quel état autre que **Fermé** et tous les VI associés doivent provenir du Qualys produit.
- Pour lancer de nouvelles analyses dans l'espace de travail de rattrapage informatique à partir d'enregistrements d'éléments vulnérables et de tâches de rattrapage, ces enregistrements doivent vous être affectés.

Rôles requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_vul.remediation_owner pour le Espace de travail de remédiation IT fichier .
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin à partir de l'espace de travail Responsable des vulnérabilités.

Procédure

1. Accédez à un élément vulnérable ou à une tâche de rattrapage qui vous a été affectée et ouvrez-le.

   Remarque : Si vous choisissez un effort de rattrapage pour lancer une nouvelle analyse, tous les éléments vulnérables associés à cet enregistrement sont analysés.

2. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**.
3. Dans la fenêtre modale Ré-analyser, choisissez un profil d'option.
   Un profil d'option est requis lorsque vous lancez une Qualys analyse à partir de votre ServiceNow AI Platform®. Les profils d'option contiennent Qualys des paramètres d'analyse.

Option	Description
Utiliser le profil d'option par défaut	Il s'agit du profil d'option défini par défaut pour l'instance d'intégration. Vous sélectionnez ce profil lors de la configuration de votre Qualys scanner. Consultez Configurer les dispositifs de scanner pour plus d'informations.
Spécifier le profil d'option	Dans la liste Profil d'option, choisissez un profil à utiliser pour l'analyse. Vous pouvez sélectionner le profil d'option que vous souhaitez utiliser pour les analyses afin de faire correspondre les éléments de configuration.

4. Dans la fenêtre modale Analyser à nouveau, cliquez sur **Demander une nouvelle analyse**.
   Le message La demande d'analyse est en cours de traitement s'affiche.
5. Cliquez sur le lien **Afficher l'état** dans le message pour afficher la progression de l'analyse.

   L'enregistrement d'analyse (VSCAN#) s'affiche. Sous l'en-tête d'enregistrement avec le numéro d'analyse, les listes d'éléments connexes affichent les informations suivantes :

   - La liste Détails affiche le numéro d'analyse de l'analyse parente, la source du scanner et l'état. Affichez les analyses terminées et échouées dans la section Synthèse de l'analyse.
   - La liste Analyses affiche toutes les analyses enfants et leurs états. Lorsque toutes les analyses enfants sont terminées, l'état de l'analyse parente passe à Terminé.
   - La liste Source affiche l'élément vulnérable utilisé pour l'analyse, l'élément de configuration et la vulnérabilité associés, l'état du VI et son état de rattrapage.

   Votre ServiceNow AI Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform® votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée.

Tous les VI qui sont passés ou passeront à l'état Fermé/Corrigé sont importés lors de la prochaine importation planifiée des Qualys intégrations.

Analyser Rapid7 de nouveau les Réponse aux vulnérabilités éléments vulnérables à partir des espaces de travail

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Lancez de nouvelles analyses dans le Rapid7 produit sur demande à partir de l'espace de travail de remédiation informatique de votre ServiceNow AI Platform instance.

Avant de commencer

Pour lancer une nouvelle analyse du produit à partir de l'environnement classique, reportez-vous à la section Lancer une nouvelle analyse pour l'intégration de vulnérabilité Rapid7. Cette rubrique comprend également des informations sur la planification des analyses avec les paramètres d'intégration sur l'instance d'intégration Rapid7 .

Les Rapid7 scanners sont désactivés par défaut dans l'application Réponse aux vulnérabilités . Si vous tentez d'effectuer une nouvelle analyse à partir des éléments vulnérables ou des tâches de rattrapage qui ont Rapid7 l'application comme source, le bouton **Analyser de nouveau** n'est pas disponible.

Pour activer ces scanners, en tant qu'utilisateur disposant du rôle sn_vul.vulnerability_admin :

1. Accédez à la **Tous** > **Réponse aux vulnérabilités** > **Analyse de la vulnérabilité** > **Scanners**.
2. Recherchez le produit de scanner que vous souhaitez activer et cliquez sur l'enregistrement pour l'ouvrir.
3. Sélectionnez la case à cocher Activé.
4. Cliquez sur **Mettre à jour**.

Le produit que vous avez activé s'affiche dans le champ Source sur les enregistrements d'élément vulnérable et de tâche de rattrapage après la prochaine importation, et **Analyser à nouveau** est disponible en tant qu'action d'interface utilisateur.

- Vous pouvez lancer de nouvelles analyses à la demande pour les éléments vulnérables et les tâches de rattrapage qui ont le produit comme source à partir de l'espace Rapid7 InsightVM de travail de remédiation informatique de votre ServiceNow AI Platform.
- Sur un enregistrement de tâche de rattrapage, l'enregistrement peut être dans n'importe quel état autre que **Fermé** et tous les VI associés doivent provenir du Rapid7 produit.
- Pour lancer de nouvelles analyses dans l'espace de travail de rattrapage informatique à partir d'enregistrements d'éléments vulnérables et de tâches de rattrapage, ces enregistrements doivent vous être affectés.

Rôles requis :

- sn_vul.remediation_owner pour l'espace de travail de remédiation informatique
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin à partir de l'espace de travail du gestionnaire de vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à un élément vulnérable ou à une tâche de rattrapage qui vous a été affectée et ouvrez-le.

   Remarque : Si vous choisissez un effort de rattrapage pour lancer une nouvelle analyse, tous les éléments vulnérables associés à cet enregistrement sont analysés.

2. Dans l'angle supérieur droit de l'enregistrement, cliquez sur **Analyser à nouveau**.
3. Dans la fenêtre modale Confirmer la nouvelle analyse, cliquez sur **Demander une nouvelle analyse**. Le message La demande d'analyse est en cours de traitement s'affiche.
4. Cliquez sur le lien **Afficher l'état** dans le message pour afficher la progression de l'analyse.

   L'enregistrement d'analyse (VSCAN#) s'affiche. Sous l'en-tête d'enregistrement avec le numéro d'analyse, les listes d'éléments connexes affichent les informations suivantes :

   - La liste Détails affiche le numéro d'analyse de l'analyse parente, la source du scanner et l'état. Affichez les analyses terminées et échouées dans la section Synthèse de l'analyse.
   - La liste Analyses affiche toutes les analyses enfants et leurs états. Lorsque toutes les analyses enfants sont terminées, l'état de l'analyse parente passe à Terminé.
   - La liste Source affiche l'élément vulnérable utilisé pour l'analyse, l'élément de configuration et la vulnérabilité associés, l'état du VI et son état de rattrapage.

   Votre ServiceNow AI Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité.

   Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform® votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée.

   Tous les VI qui sont passés ou passeront à l'état Fermé/Corrigé sont importés lors de la prochaine importation planifiée des Rapid7 intégrations.

Analyser Tenable.io de nouveau et Tenable.sc les éléments vulnérables à partir des espaces de Réponse aux vulnérabilités travail

Vérifiez que vos éléments vulnérables ont été corrigés entre les cycles d'analyse planifiés. Lancez de nouvelles analyses dans le Tenable.io et Tenable.sc les produits sur demande à partir de l'espace de travail de remédiation informatique de votre ServiceNow AI Platform instance.

Avant de commencer

Pour lancer une nouvelle analyse des produits de l'environnement Tenable.ioTenable.sc classique de Réponse aux vulnérabilités, reportez-vous à la section Lancer une nouvelle analyse pour l'intégration Tenable.sc et Lancer une nouvelle analyse pour l'intégration Tenable.io.

Pour effectuer de nouvelles analyses à partir de votre ServiceNow AI Platform, vous avez besoin de vos informations d'identification Tenable. Pour plus d'informations sur la configuration de vos Tenable.io scanners AND Tenable.sc et sur l'importation de vos informations d'identification à partir de Tenable, reportez-vous à la section Configurer l'intégration de vulnérabilité Tenable à l'aide de l'assistant de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous pouvez lancer de nouvelles analyses à la demande pour les éléments vulnérables et les tâches de rattrapage qui ont le ou Tenable.sc le Tenable.io produit comme source à partir de l'espace de travail de remédiation informatique de votre ServiceNow AI Platform.
- Sur un enregistrement de tâche de **rattrapage**, l'enregistrement peut être dans n'importe quel état autre que Fermé, et tous les VI associés doivent provenir du Tenable.io ou du Tenable.sc produit.
- Pour lancer de nouvelles analyses dans les enregistrements d'élément Espace de travail de remédiation IT vulnérable et de tâche de rattrapage, ces enregistrements doivent vous être affectés.

Rôles requis :

- sn_vul.remediation_owner pour le champ Espace de travail de remédiation IT
- sn_vul.vulnerability_analyst ou sn_vul.vulnerability_admin à partir de l'espace de travail du gestionnaire de vulnérabilité

Procédure

1. Accédez à un élément vulnérable ou à une tâche de rattrapage qui vous a été affectée et ouvrez-le.

   Remarque : Si vous choisissez un effort de rattrapage pour lancer une nouvelle analyse, tous les éléments vulnérables associés à cet enregistrement sont analysés.

2. Dans l'angle supérieur droit d'un enregistrement, cliquez sur **Analyser à nouveau**.
   Vous êtes invité à choisir l'instance ou les instances pour la nouvelle analyse et les informations d'identification du scanner que vous souhaitez utiliser pour accéder au scanner. Les informations d'identification affichées sont celles importées par les intégrations d'informations d'identification d'analyse Tenable.io and Tenable.sc .
3. Dans la fenêtre modale, cliquez sur l'icône de recherche.

   Dans le modal Sélectionner une information d'identification de numérisation qui s'affiche, utilisez les filtres dans les en-têtes de colonne pour sélectionner le nom, l'instance et/ou les instances, ainsi que les types d'informations d'identification que vous souhaitez utiliser.

   Consultez le tableau suivant pour plus d'informations.

Colonne	Description
Nom	Choisissez le nom des informations d'identification que vous souhaitez. Passez la souris sur le titre de la colonne. Utilisez le menu vertical à trois points dans le titre de la colonne pour filtrer les noms de vos informations d'identification.
Instance d'intégration	Choisissez un ou si Tenable.io pour Tenable.sc l'instance d'intégration Tenable.sc à partir de laquelle vous souhaitez lancer une nouvelle analyse. Toutes vos instances d'intégration pour Tenable.io ou Tenable.sc sont affichées. Si un élément vulnérable existe dans plusieurs instances d'intégration, vous pouvez utili–

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
	ser ce filtre pour limiter ou développer les instances que vous souhaitez analyser. **Remarque :** Si vous choisissez d'analyser à nouveau les éléments vulnérables à partir d'un enregistrement de tâche de rattrapage pour une seule instance d'intégration, seuls les éléments vulnérables actifs associés à cette tâche de rattrapage, pour cette instance, à l'aide des informations d'identification que vous sélectionnez sont analysés.
Type	Il s'agit des informations d'identification de scanner disponibles importées à partir des Tenable.io produits OR Tenable.sc . Passez la souris sur le titre de la colonne. Utilisez le menu vertical à trois points dans le titre de la colonne pour ouvrir le modal et sélectionner les types d'informations d'identification souhaités.

4. Dans la fenêtre modale Analyser de nouveau mise à jour, cliquez sur **Demander une nouvelle analyse**. Le message La demande d'analyse est en cours de traitement s'affiche.
5. Cliquez sur le lien **Afficher l'état** dans le message pour afficher la progression de l'analyse.

   L'enregistrement d'analyse (VSCAN#) s'affiche. Sous l'en-tête d'enregistrement avec le numéro d'analyse, les listes d'éléments connexes affichent les informations suivantes :
   - La liste Détails affiche le numéro d'analyse de l'analyse parente, la source du scanner et l'état. Affichez les analyses terminées et échouées dans la section Synthèse de l'analyse.
   - La liste Analyses affiche toutes les analyses enfants et leurs états. Lorsque toutes les analyses enfants sont terminées, l'état de l'analyse parente passe à Terminé.
   - La liste Source affiche l'élément vulnérable utilisé pour l'analyse, l'élément de configuration et la vulnérabilité associés, l'état du VI et son état de rattrapage.

   Votre ServiceNow AI Platform® instance suit l'état de la nouvelle analyse jusqu'à ce qu'elle se termine avec succès ou jusqu'à ce que la période de suivi définie expire, selon la première éventualité.

   Le délai d'expiration n'arrête pas l'analyse. Le délai d'expiration fait référence au moment où le suivi de l'état de ServiceNow AI Platform® votre nouvelle analyse a cessé, et non au moment où la nouvelle analyse réelle s'est arrêtée.

   Tous les VI qui sont passés, ou passeront à l'état Fermé/Corrigé, sont importés avec la prochaine importation planifiée des Tenable.io intégrations OU Tenable.sc .

Espace de travail de remédiation IT Informations de référence

Les rubriques suivantes vous fournissent des liens, des informations de référence, en plus des données de champ sur les formulaires et les enregistrements trouvés dans Espace de travail de remédiation IT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire de demande de création de changement

La table suivante répertorie les champs et leur description dans le formulaire Créer une demande de changement.

Champ	Description
Type de changement	Normal : normal est la valeur par défaut. Standard : deux champs supplémentaires s'affichent : Catégorie de changement standard : sélectionnez une catégorie dans la liste Modèle de changement standard : sélectionnez un modèle dans la liste de choix à utiliser pour cette demande de changement Urgence : priorité critique
Ajouter des CI à la demande de changement	Activé par défaut. Si cette option est activée, la demande de changement ajoute tous les éléments de configuration (CI) qui appartiennent aux éléments vulnérables actifs dans cet effort de rattrapage.
Priorité	Élevé est la valeur par défaut. Sélectionnez une priorité dans la liste.
Groupe d'affectation	Le groupe d'affectation est par défaut extrait de la rubrique de visualisation. Cliquez sur l'icône de recherche puis, dans le modal, choisissez un autre groupe d'affectation.
Date de fin prévue	Cliquez sur l'icône Calendrier pour sélectionner une date de fin planifiée.
Affecté à	Par défaut, l'utilisateur actuel est affecté à la tâche de rattrapage. Cliquez sur l'icône de recherche et choisissez un autre utilisateur dans le modal.
Description brève	La brève description est extraite de la tâche de rattrapage. Cliquez sur le texte pour le modifier.
Description	La description est extraite de la tâche de rattrapage. Cliquez sur le texte pour le modifier.
Justification	Justification tirée de la tâche de rattrapage. Cliquez sur le texte pour le modifier.
Plan d'implémentation	Prérempli avec les informations sur la solution préférée si elles sont disponibles. Affichez la solution ou saisissez un plan de justification.

Information associée

Créer une demande de changement dans Espace de travail de remédiation IT

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire de demande d'exception pour les exceptions de politique

La table suivante répertorie les champs que vous devez remplir dans le formulaire Demande d'exception pour les exceptions de politique.

Formulaire de demande d'exception

Champ	Description
Politique	Politique de gestion de la vulnérabilité pour laquelle vous demandez une exception.
Objectif du contrôle	Objectifs de contrôle associés à la politique que vous avez sélectionnée. Si une politique n'est pas sélectionnée, tous les objectifs de contrôle sont répertoriés.
Début de validité	Date à laquelle l'exception commence. La valeur par défaut est la date actuelle. Cette date ne peut pas être dans le passé.
Valide jusqu'au	Date à laquelle l'exception de politique expire et où l'état de l'élément ou du groupe vulnérable passe de Différé à Ouvert. **Remarque :** Le nombre de jours de validité de l'exception de politique ne peut pas dépasser la valeur du champ **Durée maximale de l'exception (jours)** que vous définissez pour la politique. Pour plus d'informations, consultez Créer une politique .
Motif	Motif de la demande d'exception.
Justification	Détails relatifs à la raison pour laquelle cette exception est demandée. Ce champ doit être renseigné par le propriétaire du rattrapage.

Information associée

Demander une exception à l'aide de GRC : Gestion de la politique et de la conformitéEspace de travail de remédiation IT

Formulaire de demande d'exception pour la réduction du risque

La table suivante indique les champs du formulaire Demande d'exception pour les demandes de réduction des risques.

Formulaire de demande d'exception

Champ	Description
Motif	Raison de votre demande d'exception. Sélectionnez *Contrôle d'atténuation en place pour la demande de* réduction des risques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de demande d'exception (suite)

Champ	Description
	Pour savoir comment ajouter de nouveaux choix de motifs, reportez-vous à la section Définir le mappage du motif de la politique.
Demande de report	Différez le disque. Ce champ est sélectionné par défaut. **Remarque :** Ce champ s'affiche uniquement lorsque l'option *Contrôle d'atténuation en place* est sélectionnée dans le champ **Motif** .
Demande de réduction des risques	Vous permet de demander la réduction du score de risque. **Remarque :** Cette case à cocher n'apparaît que lorsque l'option *Contrôle d'atténuation en place* est sélectionnée dans le champ **Motif** .
Cote de risque actuelle	Gravité actuelle du risque. **Remarque :** Ce champ est disponible uniquement si la case Demande **de réduction des risques** est cochée.
Cote de risque souhaitée	Nouvelle cote de risque que vous souhaitez affecter à l'enregistrement. Le score de risque le plus élevé dans cette plage d'évaluation des risques est appliqué à l'enregistrement lorsque votre demande est approuvée. **Remarque :** Ce champ est disponible uniquement si la case Demande **de réduction des risques** est cochée.
Sélectionner les contrôles de compensation	Motif de votre demande de réduction de la cote de risque.
Jusqu'à	Date d'expiration de la demande de report ou de réduction du risque. Lorsque la demande d'exception expire : • L'enregistrement revient à l'état Ouvert. • Les contrôles de compensation expirent. • Le score calculé remplacera un score réduit.
Notes de justification	Détails liés au motif pour lequel cette demande est effectuée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Demander une réduction du risque pour un élément vulnérable ou une tâche de rattrapage

Explorer l'espace de travail de l'évaluation de la vulnérabilité

L'espace de travail Évaluation de la vulnérabilité est conçu pour permettre au gestionnaire d'événements de vulnérabilité d'effectuer une évaluation de l'exposition et de gérer de manière proactive les événements de vulnérabilité critiques, en particulier lors d'événements de vulnérabilité critiques tels qu'un événement zero-day.

Une fois qu'une vulnérabilité critique est identifiée, les gestionnaires d'événements de vulnérabilité peuvent évaluer l'impact potentiel et le risque associés à la vulnérabilité. Les analystes peuvent analyser le système, les applications ou les composants réseau affectés pour comprendre la gravité et les vecteurs d'attaque possibles au sein de l'organisation.

L'espace de travail Évaluation de la vulnérabilité contient :

Page d'évaluation de l'exposition

Fournit une visibilité détaillée des actifs exposés aux vulnérabilités et aux logiciels vulnérables. La fonctionnalité d'évaluation de l'exposition fournit :

- Visibilité des actifs impactés pour détecter les vulnérabilités et les logiciels affectés
- Capacité à effectuer des évaluations autonomes pour un seul CVE ou un logiciel vulnérable
- Visibilité sur les actifs impactés pour les CVE de vulnérabilité exploitée connue de CISA
- Visibilité de l'exposition à partir d'un modèle de détection et d'actifs supplémentaires.
- Capacité à créer des éléments vulnérables

Page d'évaluation de la vulnérabilité

Page Évaluation de vulnérabilité dans laquelle vous pouvez gérer les événements de crise de vulnérabilité de l'évaluation à la résolution à l'aide du workflow Gestion de crise de vulnérabilité. Le workflow vous permet de suivre les événements de vulnérabilité qui vous intéressent, d'analyser les risques qui leur sont associés, d'évaluer l'exposition de plusieurs inventaires (par exemple, l'inventaire des installations logicielles) et de les déclarer comme une crise pour un engagement de réponse élevé. Vous pouvez ensuite associer l'enregistrement de l'évaluation des vulnérabilités à un incident de sécurité majeur et permettre à l'équipe de Security Incident Response de répondre à la crise.

- Créer et modifier des évaluations de vulnérabilité pour les événements de vulnérabilité critiques
- Enregistrez les attributs clés de la vulnérabilité pour calculer le risque
- Effectuer une évaluation de la vulnérabilité pour déterminer le niveau et la priorité d'exposition
- Déclarer l'évaluation de vulnérabilité comme un événement critique
- Associez l'évaluation de la vulnérabilité à un incident de sécurité majeur en liant, en proposant ou en promouvant l'évaluation de la vulnérabilité à un incident de sécurité majeur.

Page de liste

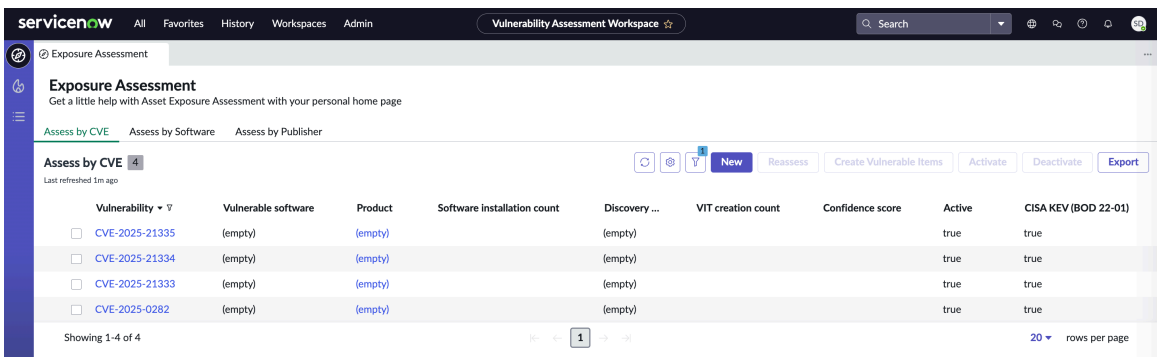
La page Liste comprend une bibliothèque contenant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- CVE
- TPE
- CWE

L'image suivante vous montre la page d'accueil de l'espace de travail Évaluation de la vulnérabilité.



Explorer l'évaluation de l'exposition

L'évaluation de l'exposition utilise le cadre de travail CPE (Common Platform Enumeration), qui fait partie du système CVE (Common Vulnerabilities and Exposures), pour évaluer l'exposition de vos actifs aux logiciels de vulnérabilité. Cette évaluation est réalisée à l'aide d'un modèle de détection de logiciels.

En utilisant un algorithme d'appariement, les CPE pertinents sont associés et mappés au modèle de détection de logiciels, ce qui permet d'identifier les expositions potentielles.

Vous pouvez utiliser l'évaluation de l'exposition par CVE ou un logiciel pour identifier l'exposition à des vulnérabilités potentielles pour les scénarios suivants :

- Vulnérabilités qui peuvent ne pas être identifiées par les scanners traditionnels
- Vulnérabilités zero-day avant que le scanner ne fournisse la signature pour la détection des vulnérabilités

L'évaluation de l'exposition fournit un avertissement précoce pour corriger ces vulnérabilités et améliorer la maturité du programme de gestion des vulnérabilités.

Conditions préalables à l'évaluation de l'exposition

Versions disponibles

Application	Version
Module d'extension Vulnerability Crisis Management	1.0
Réponse aux vulnérabilités	20.0
Réponse aux vulnérabilités avec NVD	1.3
Vulnerability Response integration with CISA	1.2
Intégration de Vulnerability Response avec NVD	1.3

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Versions disponibles (suite)

Application	Version
Remarque : Pour plus d'informations, consultez Présentation des intégrations NVD.	
Gestion des actifs logiciels	Module d'extension Software Asset Management Foundation ou Gestion des actifs logiciels - Professional module d'extension

Cas d'utilisation

Pour obtenir des exemples sur la façon dont l'organisation des analystes de vulnérabilité utiliserait l'espace de travail Évaluation de l'exposition à la vulnérabilité, consultez ces cas d'utilisation.

Type d'évaluation	Utiliser
Évaluer par CVE	Évaluez les vulnérabilités par CVE afin de bien comprendre l'impact et l'exposition des systèmes affectés à l'aide Gestion des actifs logiciels de (SAM) et Découverte des données. Prenez des mesures de rattrapage rapides en créant des VIT manuels et en les affectant aux propriétaires de rattrapage. L'évaluation par CVE est utile car les scanners peuvent ne pas détecter tous les systèmes affectés, alors qu'ils Découverte identifient généralement la plupart des logiciels sur la surface d'attaque.
Évaluer par logiciel	Évaluez l'impact par logiciel lorsque CVE n'est pas disponible pour identifier le nombre de CI sur lesquels le logiciel est installé. Grâce à l'évaluation par logiciel, vous pouvez agir de manière proactive sur les vulnérabilités critiques ou de type « zero-day » en créant un VIT manuel et en l'affectant au propriétaire de la correction avant qu'elles ne soient officiellement publiées ou avant que les scanners ne les identifient.
Évaluer par éditeur	Évaluez les vulnérabilités d'un fournisseur de logiciel afin de comprendre l'impact et l'exposition des systèmes affectés pour les CVE publiées par le fournisseur dans un délai donné. L'évaluation par éditeur vous aide à évaluer le risque et les vulnérabilités critiques du fournisseur, ce qui permet une correction proactive.

Compatibilité et configuration requise

L'application Réponse aux vulnérabilités est disponible sur le ServiceNow Store. L'application Gestion des actifs logiciels ITSM (com.snc.asset_management) est requise pour le module

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d’évaluation de l’exposition. Cette application gère l’ensemble de vos actifs et licences logicielles, et la SAM Foundation version de cette application fait partie de l’application Réponse aux vulnérabilités que vous téléchargez à partir du ServiceNow Store.

Important : L’application d’évaluation de l’exposition fonctionne avec les modules d’extension suivants :

- Module d'extension Software Asset Management Foundation (com.snc.sams)
- Gestion des actifs logiciels - Professional (com.snc.pa.samp)
- Module d'extension de gestion des actifs logiciels (com.snc.software_asset_management)

Pour vérifier que l’application SAM Foundation est installée sur votre instance, accédez à **Applications système** > **Toutes les applications disponibles** > **Tous** et recherchez com.snc.asset_management. Si l’application n’est pas installée, sélectionnez **Installer**. Étant donné que l’application d’évaluation de l’exposition aux vulnérabilités nécessite l’accès aux données d’actif sur votre ServiceNow AI Platform® instance, les applications de gestion des actifs doivent disposer de données à référencer. La table Modèles de détection de logiciels (cmdb_sam_sw_discovery_model) et les installations de logiciels (cmdb_sam_sw_install) exigent des données.

Champs d’algorithme de correspondance pour les modèles de détection de logiciels

L’application Gestion des actifs logiciels - Professional vous permet de modifier un modèle de détection de logiciels afin de normaliser manuellement les logiciels détectés qui n’ont pas été entièrement normalisés (partiellement normalisés, normalisés par l’éditeur ou correspondance introuvable) sur le formulaire des modèles de découverte de logiciels afin qu’il puisse être rapproché. À partir de la version 20.0 de Réponse aux vulnérabilités prend en charge le modèle de détection normalisé qui provient de Gestion des actifs logiciels - Professional. Les champs suivants sont utilisés pour l’algorithme de correspondance des modèles de détection de logiciels.

CPE (modèle logiciel)	Fondations SAM	SAM professionnel
Fournisseur	Clé primaire	Clé primaire
Produit	Nom d'affichage	Nom d'affichage
Version	Éditeur détecté	Éditeur détecté
Édition	Produit détecté	Produit détecté
	Version détectée	Version détectée
		Éditeur normalisé
		Produit normalisé
		Version normalisée

Remarque : L’application SAM Professional ne fait pas partie du produit principal Réponse aux vulnérabilités de et ServiceNow Store nécessite un abonnement distinct.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété système

Pour traiter automatiquement les vulnérabilités exploitées par CISA pour l'évaluation de l'exposition, définissez la propriété *sn_vul_analyst.enable_exposure_for_cisa* système sur *true*. La valeur par défaut est *false*.

Travaux planifiés

Voici les travaux planifiés.

Nom de la tâche planifiée	Description
Vérifier l'exposition potentielle à la vulnérabilité	Traite les CVE delta, les logiciels et les installations pour obtenir l'exposition. **Remarque :** Cette tâche planifiée s'exécute toutes les 12 heures. Il s'exécute pendant une période plus longue que les autres travaux planifiés.
Insérer un CVE exploité par CISA dans la configuration d'exposition	Sur demande. Insère les CVE CISA dans la table Configuration de l'exposition pour calculer l'exposition.
Exécuter l'évaluation de l'exposition pour les CVE configurés	Sur demande. Calcule l'exposition pour tous les enregistrements CVE dans la table Configuration de l'exposition.
Exécuter l'exposition logicielle	Sur demande. Calcule l'exposition pour tous les enregistrements logiciels dans la table Configuration de l'exposition.

Termes clés

- **Score de confiance :** Un score de confiance est une mesure de la fiabilité de la fourniture d'une recommandation pour un champ. Plus le score est élevé, plus la recommandation est fiable. Pour des exemples de calculs, reportez-vous à la section Exemple de calcul du score de confiance.
- **Nombre d'installations logicielles :** Nombre d'actifs logiciels impactés par la vulnérabilité.
- **Modèle logiciel :** Modèle logiciel associé au produit. Explorez le modèle logiciel pour voir le résultat du modèle logiciel. Pour plus d'informations, consultez Modèles de détection et installations de logiciels Module d'extension Software Asset Management Foundation .

Le champ **Nombre d'installations de logiciels** fournit le nombre total d'installations de logiciels, quel que soit leur état actif ou inactif sur le modèle de détection. À partir de la version 22.0 de , une nouvelle propriété système, , a été introduite pour déterminer si les installations logicielles inactives doivent être filtrées pour l'évaluation de l'exposition Réponse aux vulnérabilités*sn_vul.filter_inactive_sw_installs* Par défaut, la propriété est activée dans le système de base. Lorsque le filtre est activé, seules les installations actives sont affichées.

Le champ **Modèle de détection** indique spécifiquement le nombre d'installations de logiciels actives, car les installations inactives sont filtrées en fonction du filtre par défaut actif=vrai dans la table Modèle de découverte de logiciels. Le nombre de ce champ doit correspondre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

au nombre filtré affiché dans le champ **Nombre d'installation de logiciel** . Le nombre indiqué dans le champ **Installation de logiciel** persiste même si vous mettez à jour la propriété système. Pour obtenir le nombre mis à jour, vous devez exécuter les travaux *`Run exposure assessment for configured CVEs`* planifiés et *`Run software exposure that updates the count`*.

Évaluation de l'exposition par CVE

L'évaluation de l'exposition utilise les vulnérabilités et les expositions communes (CVE) pour évaluer l'exposition de vos actifs à l'aide du modèle de détection de logiciels. Vous pouvez utiliser l'évaluation de l'exposition par CVE pour identifier l'exposition aux vulnérabilités potentielles.

Pour plus d'informations sur l'évaluation de l'exposition par CVE, voir :

- Ajouter des CVE pour évaluer l'exposition
- Créer des VI pour les CVE pour l'évaluation de l'exposition
- Activer ou désactiver les CVE pour l'évaluation de l'exposition
- Exporter les CI impactés pour l'évaluation de l'exposition
- Exemple de calcul du score de confiance

Ajouter des CVE pour évaluer l'exposition

Ajoutez les vulnérabilités et expositions courantes (CVE) à la liste de configuration de l'exposition des CVE dans l'évaluation de l'exposition pour évaluer l'impact d'une nouvelle vulnérabilité ou d'une vulnérabilité zero-day.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par CVE**.
2. Sélectionnez **Ajouter**.
3. Dans la boîte de dialogue Ajouter un CVE, sélectionnez les CVE que vous souhaitez ajouter à la liste et sélectionnez l'option **Ajouter** .
   Les CVE qui figurent déjà dans la liste ne sont pas ajoutées à nouveau. Les autres sont ajoutés à la liste des CVE.

   Remarque : Sélectionnez l'icône de filtre pour accéder à la **vue avancée** et spécifiez les CVE que vous souhaitez afficher.

4. Pour évaluer l'impact des CVE qui figurent déjà dans la liste :

   a. Cochez la case des CVE que vous souhaitez réévaluer.

   b. Sélectionnez le bouton **Réévaluer** .
   Les détails mis à jour apparaissent dans leurs colonnes respectives.

Créer des VI pour les CVE pour l'évaluation de l'exposition

Créez des éléments vulnérables (VI) à partir de la page Évaluation de l'exposition. Les gestionnaires d'événements de vulnérabilité analysent ensuite cette liste d'éléments

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vulnérables et recommandent des solutions et des correctifs qui aident l'équipe informatique à corriger ces vulnérabilités.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Une fois l'exposition évaluée, la liste de l'évaluation potentielle s'affiche dans l'enregistrement d'évaluation de l'exposition avec le nombre d'éléments de configuration (CI). Vous pouvez sélectionner les enregistrements et, dans l'action de liste, sélectionner **Créer des éléments vulnérables** pour créer des éléments vulnérables (VI) pour les CI où le logiciel vulnérable est présent et sur les vulnérabilités et expositions communes (CVE). Les VI sont créés en arrière-plan. Ce processus peut prendre un certain temps. Une fois les éléments créés, vous pouvez naviguer vers la table des VI pour afficher les enregistrements créés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par CVE**.
2. Sélectionnez les CVE requis et sélectionnez l'option **Créer des éléments vulnérables** .
3. Dans la boîte de dialogue Créer des éléments vulnérables, sélectionnez l'option **Créer des éléments vulnérables** .
4. Sélectionnez le lien **Afficher l'état** pour afficher l'état de la tâche d'arrière-plan utilisée pour créer les VI.

Activer ou désactiver les CVE pour l'évaluation de l'exposition

Pour le traitement delta d'une CVE, vous pouvez l'activer, l'ajoutant ainsi à la liste active des CVE.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Remarque : À partir de la version 4.0.1 de Vulnerability Exposure Assessment, si une entrée de vulnérabilité commune (CVE) n'a pas été mise à jour ou si des éléments vulnérables (VIT) ont été créés au cours des 30 derniers jours, l'enregistrement d'évaluation de l'exposition pour cette CVE est automatiquement marqué comme inactif. Toutefois, vous pouvez activer ou désactiver manuellement ces enregistrements. En outre, la tâche `Check potential vulnerability exposure` planifiée s'exécute en continu pour rechercher ces CVE afin de les désigner comme inactifs.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par CVE**.
2. Sélectionnez les CVE actifs requis, puis sélectionnez l'option **Désactiver** .
   Les CVE sont désactivés.

   Remarque : Pour activer un logiciel, suivez le même processus et sélectionnez l'option **Activer** .
3. Actualisez la page pour afficher l'état mis à jour (faux) dans la colonne Actif.

Exporter les CI impactés pour l'évaluation de l'exposition

Vous pouvez suivre la liste des actifs impactés pour une nouvelle CVE en exportant les éléments de configuration (CI) liés à un enregistrement d'évaluation de l'exposition vers

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

une feuille Excel. Cette feuille permet de partager les détails des actifs et de créer des propriétaires d'incidents avec les actifs impactés connus pour les vulnérabilités zero-day.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par CVE**.
2. Sélectionnez le modèle de détection de l'enregistrement dont vous souhaitez exporter les CI. L'onglet Installations de logiciels contient les CI actifs associés à l'enregistrement de logiciel. Ces CI sont stockés dans la colonne **Installé sur** .
3. Sélectionnez l'option **Exporter** .
4. Dans la boîte de dialogue Exporter, sélectionnez le type de fichier et le type de livraison pour exporter les CI associés.
5. Sélectionnez l'option **Exporter** .

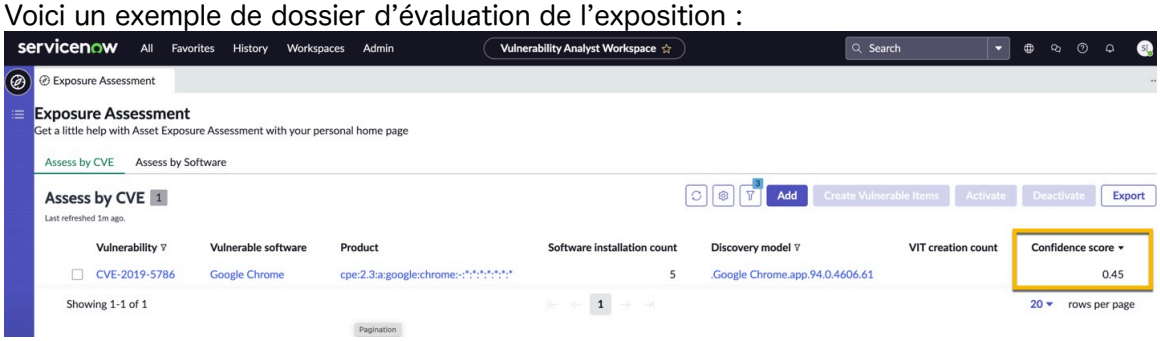
Exemple de calcul du score de confiance

Exemple de calcul de la fiabilité d'une vulnérabilité zero-day en fonction de ses informations CVE (Common Vulnerabilities and Exposures).

Voici un exemple de calcul du score de confiance à partir des informations CPE (Common Platform Enumeration) de **CVE-2019-5786**.

Remarque : Pour afficher les CPE, vous pouvez regrouper la colonne Vulnérabilité par vulnérabilité. Pour en savoir plus sur l'affichage des détails relatifs aux logiciels vulnérables, reportez-vous à la section Afficher les détails des logiciels vulnérables.

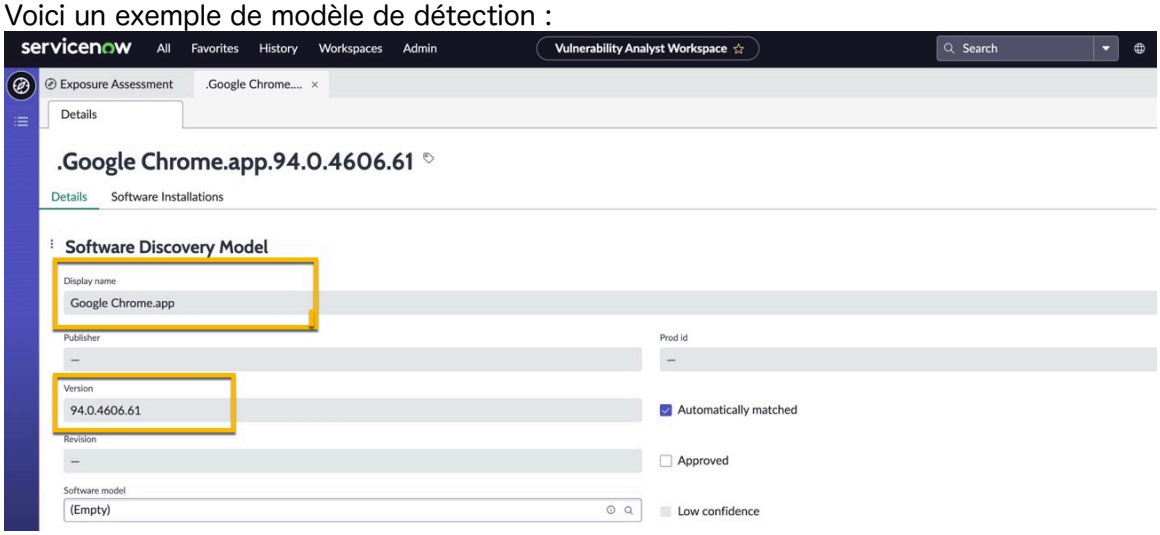
Voici un exemple de dossier d'évaluation de l'exposition :



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voici un exemple de modèle de détection :



Comment calculer le score de confiance

La plage du score de confiance est de 0 à 1. Sur la base des informations CPE, le score de confiance est calculé à l'aide de la formule suivante :

```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) +
 (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

```
.45
```

Remarque : Pour vous référer aux valeurs utilisées pour calculer le score de confiance, reportez-vous à la section Tables de référence du score de confiance pour l'évaluation de l'exposition.

Calcul du score de confiance lorsque le modèle logiciel est mis en correspondance avec le modèle de détection normalisé

Si vous utilisez le modèle de détection normalisé, les informations supplémentaires disponibles pour le modèle de détection de logiciels fournissent un score de confiance amélioré. Voici l'exemple de calcul :

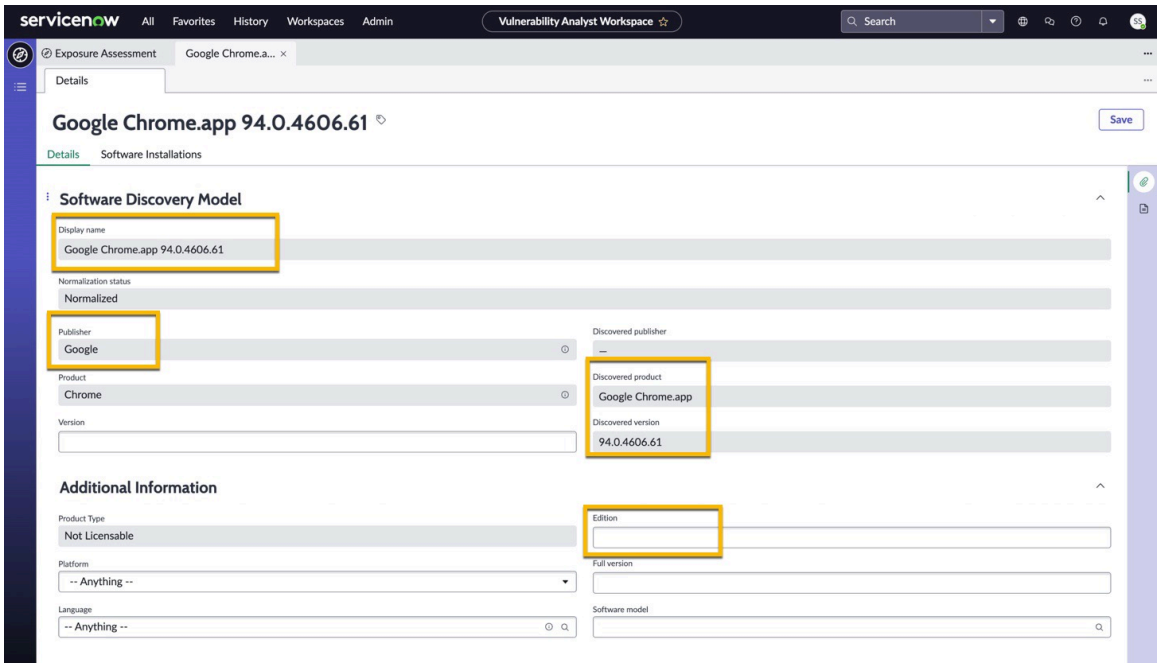
Voici un exemple d'enregistrement d'évaluation de l'exposition normalisée.



Voici un exemple de modèle de découverte normalisé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.




```
((BASE SCORE) + (publisher score) + (product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (20) + (15) + (15) + (0) + (10)) / 100
```

=

```
85 / 100
```

=

```
.85
```

Remarque : Pour vous référer aux valeurs utilisées pour calculer le score de confiance, reportez-vous à la section Tables de référence du score de confiance pour l'évaluation de l'exposition.

Afficher les détails des logiciels vulnérables

Affichez les détails du logiciel vulnérable, dans ce cas, Google Chrome. Il est comparé au modèle de détection et au CPE (Common Platform Enumeration). Cette version CPE impacte toutes les versions de Google Chrome.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à **Tout** et saisissez *sn_vul_software.LIST*.
2. Dans la liste des logiciels vulnérables, recherchez **cpe :2.3 :a :google :chrome :-:*:*:*:*:*:*:*** pour afficher les informations.

Tables de référence du score de confiance pour l'évaluation de l'exposition

Valeurs de référence utilisées pour calculer le score de confiance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables de référence

Table de référence pour le calcul du score de confiance

Segment logiciel vulnérable	Segment de modèle de découverte	Score	Segment de correspondance exacte du modèle de découverte	Score de correspondance exacte
Éditeur	Nom complet	15	Éditeur	5
Modèle	Nom complet	15	Modèle	5
Version	Nom complet	10	Version	5
Édition	Nom complet	3	Édition normalisée	2
Nom complet	Nom complet	10	Nom complet	5

Table récapitulative du score de confiance

Score	Valeur
Somme de tous les scores	75
Score de base **Remarque :** Score minimum attribué à tous les modèles de détection appariés.	25
Score total	100

Évaluation de l'exposition par logiciel

Évaluation de l'exposition des vulnérabilités zero-day, lorsque les vulnérabilités et les expositions communes (CVE) pour l'actif ou l'élément de configuration ne sont pas disponibles. Elle utilise les informations logicielles pour évaluer l'exposition, à l'aide du modèle de détection de logiciels.

Pour plus d'informations sur l'évaluation de l'exposition par logiciel, voir :

- Ajouter un logiciel pour l'évaluation de l'exposition
- Créer des VI pour les logiciels pour l'évaluation de l'exposition
- Activer ou désactiver le logiciel pour l'évaluation de l'exposition
- Exporter les CI impactés pour les logiciels dans l'espace de travail Évaluation de la vulnérabilité

Ajouter un logiciel pour l'évaluation de l'exposition

Ajoutez un nouveau logiciel au module d'évaluation de l'exposition pour évaluer l'impact d'une nouvelle vulnérabilité ou d'une vulnérabilité zero-day.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par logiciel** > **Ajouter**.
2. Remplissez les champs du formulaire.

Champ	Description
Éditeur	Éditeur du logiciel.
Produit	Nom du produit du logiciel.
Version	Version du produit logiciel.
Édition	Édition du logiciel.

Remarque : Si vous essayez d'ajouter une exposition pour un logiciel qui existe dans la table avec le statut « faux », un enregistrement en double n'est pas créé. L'état du logiciel existant est mis à jour sur « vrai ».

3. Sélectionnez l'option **Ajouter** .
4. Pour évaluer l'impact des logiciels qui figurent déjà dans la liste :
   a. Cochez la case du logiciel que vous souhaitez réévaluer.
   b. Sélectionnez le bouton **Réévaluer** .
   Les détails mis à jour apparaissent dans leurs colonnes respectives.

Créer des VI pour les logiciels pour l'évaluation de l'exposition

Créez des éléments vulnérables (VI) à partir de la page Évaluation de l'exposition. Les gestionnaires d'événements de vulnérabilité analysent ensuite cette liste d'éléments vulnérables et recommandent des solutions et des correctifs qui aident l'équipe informatique à corriger ces vulnérabilités.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par logiciel**.
2. Sélectionnez les enregistrements pour lesquels vous souhaitez créer des VI.
3. Sélectionnez l'option **Créer des éléments vulnérables** .
4. Dans la boîte de dialogue Créer des éléments vulnérables, sélectionnez l'une des options suivantes :
   - Vulnérabilité existante
   - Nouvelle vulnérabilité
5. Sélectionnez l'option **Créer des éléments vulnérables** .

Activer ou désactiver le logiciel pour l'évaluation de l'exposition

Pour arrêter tout traitement delta ultérieur du logiciel, vous pouvez choisir de le désactiver, le supprimant ainsi de la liste active des logiciels.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par logiciel**.
2. Pour le désactiver, sélectionnez le logiciel actif requis et sélectionnez l'option **Désactiver** .
   Le logiciel est désactivé.

   Remarque : Pour activer un logiciel, suivez le même processus et sélectionnez l'option **Activer** .
3. Actualisez la page pour afficher l'état mis à jour (faux) dans la colonne Actif.

Exporter les CI impactés pour les logiciels dans l'espace de travail Évaluation de la vulnérabilité

Vous pouvez suivre la liste des actifs impactés pour les nouveaux logiciels en exportant les éléments de configuration (CI) liés à un enregistrement d'évaluation de l'exposition vers une feuille Excel. Cette feuille permet de partager les détails des actifs et de créer des propriétaires d'incidents avec les actifs impactés connus pour les vulnérabilités zero-day.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par logiciel**.
2. Sélectionnez le modèle de détection de l'enregistrement dont vous souhaitez exporter les CI.
   L'onglet Installations de logiciels contient les CI actifs associés à l'enregistrement de logiciel. Ces CI sont stockés dans la colonne **Installé sur** .
3. Sélectionnez l'option **Exporter** .
4. Dans la boîte de dialogue Exporter, sélectionnez le **type de fichier** et le **type de livraison** pour exporter les CI associés.
5. Sélectionnez l'option **Exporter** .

Évaluation de l'exposition par le logiciel de l'éditeur

Évaluez l'exposition aux vulnérabilités zero-day lorsque les vulnérabilités et expositions communes (CVE) pour l'actif ou l'élément de configuration ne sont pas disponibles. Elle utilise les informations logicielles pour évaluer l'exposition, à l'aide du modèle de détection de logiciels.

Pour plus d'informations sur l'évaluation de l'exposition par logiciel, voir :

- Ajouter un logiciel d'un éditeur pour l'évaluation de l'exposition
- Créer des VI pour les logiciels d'un éditeur pour l'évaluation de l'exposition
- Activer ou désactiver un logiciel d'un éditeur pour l'évaluation de l'exposition
- Exporter les CI impactés pour les logiciels par un éditeur dans l'espace de travail Évaluation de la vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter un logiciel d'un éditeur pour l'évaluation de l'exposition

Ajoutez un logiciel d'un éditeur au module d'évaluation de l'exposition pour évaluer l'impact d'une nouvelle vulnérabilité ou d'une vulnérabilité de type « zero-day ».

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par éditeur** > **Nouveau**.
2. Dans la fenêtre Nouvelle évaluation , sélectionnez l'éditeur pour lequel vous souhaitez effectuer l'évaluation.
3. Sélectionnez une date dans le champ **Publié à partir de CVE** .
   Si l'une des entrées de vulnérabilité courantes (CVE) associées au logiciel est modifiée après la date sélectionnée, ce logiciel est pris en compte pour l'évaluation de l'exposition.
4. Sélectionnez le niveau de gravité des CVE dans la section **Gravité CVE** .
5. Sélectionnez **Commencer l'évaluation**.
   Une fois la tâche terminée, les enregistrements sélectionnés sont créés.

Créer des VI pour les logiciels d'un éditeur pour l'évaluation de l'exposition

Créez des éléments vulnérables (VI) à partir de la page Évaluation de l'exposition pour analyser la liste des VI et recommander des solutions et des correctifs qui peuvent aider l'équipe informatique à corriger les vulnérabilités.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par éditeur**.
2. Sélectionnez les enregistrements pour lesquels vous souhaitez créer des VI.
3. Sélectionnez l'option **Créer des éléments vulnérables** .
4. Dans la boîte de dialogue Créer des éléments vulnérables, sélectionnez l'une des options suivantes :
   - Vulnérabilité existante
   - Nouvelle vulnérabilité
5. Sélectionnez l'option **Créer des éléments vulnérables** .

Activer ou désactiver un logiciel d'un éditeur pour l'évaluation de l'exposition

Activez ou désactivez un logiciel d'un éditeur pour arrêter le traitement delta du logiciel et le supprimer de la liste active des logiciels.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par éditeur**.
2. Pour le désactiver, sélectionnez le logiciel actif requis par un éditeur et sélectionnez l'option **Désactiver** sous le bouton **Réévaluer** .
   L'éditeur est désactivé.

   Remarque : Pour activer le logiciel par un éditeur, suivez le même processus et sélectionnez l'option **Activer** .
3. Actualisez la page pour afficher l'état mis à jour (faux) dans la colonne Actif.

Exporter les CI impactés pour les logiciels par un éditeur dans l'espace de travail Évaluation de la vulnérabilité

Vous pouvez suivre la liste des actifs impactés pour les nouveaux logiciels en exportant les éléments de configuration (CI) liés à un enregistrement d'évaluation de l'exposition vers une feuille Excel. Cette feuille permet de partager les détails des actifs et de créer des propriétaires d'incidents avec les actifs impactés connus pour les vulnérabilités zero-day.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de l'exposition** > **Évaluer par éditeur**.
2. Sélectionnez le modèle de détection de l'enregistrement dont vous souhaitez exporter les CI.
   L'onglet Installations de logiciels contient les CI actifs associés à l'enregistrement de logiciel. Ces CI sont stockés dans la colonne **Installé sur** .
3. Sélectionnez l'option **Exporter** .
4. Dans la boîte de dialogue Exporter, sélectionnez le **type de fichier** et le **type de livraison** pour exporter les CI associés.
5. Sélectionnez l'option **Exporter** .

Explorer l'évaluation des vulnérabilités

L'espace de travail Évaluation de la vulnérabilité est conçu pour permettre au gestionnaire des événements de vulnérabilité de créer un événement de vulnérabilité et d'effectuer une évaluation de la vulnérabilité, en particulier pendant l'analyse de vulnérabilité zero-day.

Vous pouvez utiliser l'espace de travail Évaluation de la vulnérabilité pour gérer les vulnérabilités critiques, telles que :

- Vulnérabilités zero-day de gravité critique ou élevée
- Nouvelles informations sur les menaces identifiées pour une vulnérabilité
- Exploitation rapide d'une vulnérabilité de gravité critique ou élevée.

Espace de travail Évaluation de la vulnérabilité et Gestion de crise de vulnérabilité

En tant que gestionnaire d'événements de vulnérabilité, identifiez et créez un enregistrement d'événement de vulnérabilité pour les vulnérabilités d'intérêt. Une fois

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'événement vulnérable créé, vous pouvez effectuer une évaluation des risques, mettre à jour manuellement les attributs de risque et calculer automatiquement le score de risque. À l'aide de l'espace de travail Évaluation de la vulnérabilité, vous pouvez effectuer les actions suivantes pour gérer un événement de crise de vulnérabilité du début à la résolution.

- Créer un enregistrement d'évaluation de vulnérabilité
- Modifier l'enregistrement de l'évaluation des vulnérabilités
- Effectuer une évaluation de vulnérabilité
- Examiner les détails de l'évaluation
- Affecter une priorité et un niveau d'exposition à l'enregistrement d'évaluation de vulnérabilité
- Ajouter les CI affectés à l'enregistrement de l'évaluation
- Créer des éléments vulnérables pour le CI affecté ou le composant logiciel affecté
- Lier l'enregistrement de l'évaluation des vulnérabilités à un incident de sécurité majeur dans Gestion des incidents de sécurité majeurs

Conditions préalables à l'évaluation de la vulnérabilité

Versions disponibles

Application	Version
Module d'extension Vulnerability Crisis Management	1.0
Réponse aux vulnérabilités	20.0
Réponse aux vulnérabilités avec NVD **Remarque :** Pour plus d'informations, consultez Présentation des intégrations NVD.	1.4.2
Vulnerability Response integration with CISA	1.2
Modèle de données pour SBOM	1.1.2
Nomenclature logicielle Core	2.0.2
Gestion des actifs logiciels	Module d'extension Software Asset Management Foundation ou Gestion des actifs logiciels - Professional module d'extension
Gestion des incidents de sécurité majeurs	2.2.5

Travaux planifiés

Voici les travaux planifiés.

Nom de la tâche planifiée	Description
Évaluation de la vulnérabilité	Met à jour la table des éléments de configuration affectés et la source du CI si des éléments vulnérables (VIT ou AVIT) sont créés après l'évaluation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la tâche planifiée	Description
	Remarque : Cette tâche planifiée s'exécute quotidiennement. Il s'exécute pendant une période plus longue que les autres travaux planifiés.

Information associée

Gestion de crise de vulnérabilité

Créer un enregistrement d'évaluation de vulnérabilité

Créez des enregistrements d'évaluation pour les vulnérabilités d'intérêt. Après avoir créé l'évaluation, vous pouvez lancer l'évaluation initiale des risques, mettre à jour manuellement l'enregistrement et calculer automatiquement le score de risque.

Avant de commencer

Vous devez faire partie du groupe d'affectation du gestionnaire d'événements d'évaluation de la vulnérabilité du système de base pour pouvoir effectuer les tâches associées à l'évaluation de la vulnérabilité.

Rôle requis : sn_vul_analyst.vul_event_manager, sn_vul_analyst.emergency_response

Pourquoi et quand exécuter cette tâche

Vous pouvez créer un enregistrement d'évaluation de vulnérabilité pour les vulnérabilités d'intérêt en associant l'enregistrement d'événement à un CVE primaire ou à un produit affecté.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez l'icône **Évaluation de vulnérabilité** .
3. Sélectionnez **Nouveau**.
4. Entrez un titre approprié dans le champ **Titre** .
5. **Facultatif :** Sélectionnez un CVE primaire à associer au nouvel enregistrement d'évaluation dans le champ **CVE primaire** .

   Remarque : Tous les détails préliminaires de l'enregistrement d'évaluation sont renseignés en fonction du produit que vous sélectionnez ou créez ou du CVE primaire que vous associez à l'enregistrement.

6. Sélectionnez **Soumettre**.
   L'enregistrement de l'évaluation de vulnérabilité avec le titre que vous avez saisi est créé et s'affiche dans un nouvel onglet d'évaluation de vulnérabilité. Par défaut, l'enregistrement de l'évaluation de vulnérabilité s'affiche dans l'onglet **Détails** .

   Remarque : Par défaut, les détails des CVE primaires associés/mappés sont affichés.

   - Si aucun CVE primaire n'est sélectionné lors de la création de l'enregistrement de l'événement d'évaluation de la vulnérabilité, un enregistrement par défaut est créé.
   - Si le CVE principal a des CVE associés, les CVE connexes sont renseignés dans l'onglet **Entrées de vulnérabilité** . Vous pouvez ajouter d'autres CVE associés à partir de l'onglet **Entrées de vulnérabilité** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Accédez à l'onglet **Produits affectés** .

   a. Sélectionnez **Nouveau**.

   b. Renseignez les champs du formulaire.

Champ	Description
Éditeur	Éditeur du logiciel. Il s'agit d'un champ obligatoire.
Produit	Nom du produit du logiciel. Il s'agit d'un champ obligatoire.
Version	Version du produit logiciel.
Édition	Édition du logiciel.

   Remarque : Si vous essayez d'ajouter une vulnérabilité pour un logiciel qui existe dans la table avec le statut « faux », aucun enregistrement en double n'est créé. L'état du logiciel existant est mis à jour sur « vrai ».

   c. Sélectionnez **OK**.

8. Sélectionnez **Enregistrer**.

Mettre à jour l'enregistrement de l'effacement automatique de l'évaluation des vulnérabilités

Mettez à jour l'enregistrement de purge automatique de l'évaluation de vulnérabilité.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Dans le système de base, la période de conservation des enregistrements d'évaluation de vulnérabilité est fixée à 6 mois. Si l'état d'un enregistrement d'évaluation de vulnérabilité est fermé, les enregistrements d'évaluation de vulnérabilité sont stockés uniquement jusqu'à la période de conservation définie et les enregistrements connexes de cette évaluation sont supprimés après 6 mois de toutes les tables connexes.

Procédure

1. Accédez à la **Tous** > **Purges automatiques**.
2. Ouvrez l'enregistrement avec la table, sn_vul_analyst_vulnerability_assessment.
3. Cochez la case **Actif** pour activer l'option de purge automatique de l'enregistrement d'évaluation de vulnérabilité.
4. Cliquez sur **Mettre à jour**.

Modifier l'enregistrement de l'évaluation des vulnérabilités

Mettez à jour l'enregistrement de l'évaluation de vulnérabilité, publiez sa création. En fonction des valeurs du champ, vous pouvez calculer le score de risque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Une fois que le CVE principal est ajouté à l'évaluation des vulnérabilités, l'enregistrement passe à l'état En attente d'évaluation. Vous pouvez également ajouter d'autres CVE connexes dans l'onglet **Entrées de vulnérabilité**ou ajouter les produits affectés par cette vulnérabilité à partir de l'onglet **Produits affectés** . Vous pouvez apporter d'autres modifications aux champs **d'évaluation des risques** et le **score de risque** de l'enregistrement d'évaluation est automatiquement mis à jour en conséquence.

Procédure
1. Accédez à la **Tous** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de la vulnérabilité**.
2. Dans l'onglet **Détails** , mettez à jour les champs.

Champ	Description
Titre	Titre décrivant l'enregistrement de l'événement de vulnérabilité.
CVE primaire	CVE primaire que vous avez associé à l'enregistrement d'événement.
État	État actuel de l'enregistrement d'événement.
Priorité	Priorité de l'enregistrement de l'événement sur une échelle de 1 à 5.
Sources d'alerte	Source de l'événement de vulnérabilité potentielle.
Score du risque	Score de risque calculé automatiquement. Non modifiable par défaut.
Niveau d'exposition	Niveau d'exposition de l'événement de vulnérabilité sur une échelle de 1 à 5.
Groupe d'affectation	Groupe d'affectation auquel l'enregistrement d'événement est affecté.
Affecté à	Utilisateur auquel l'enregistrement d'événement est affecté.
Description	Description détaillée de l'enregistrement de l'événement.

3. Accédez à l'onglet **Entrées de vulnérabilité** pour ajouter des CVE associées ou connexes.
   a. Sélectionnez **Nouveau**.
   b. Recherchez l'enregistrement dans le champ **Entrée de vulnérabilité** .
   c. Sélectionnez l'enregistrement de vulnérabilité que vous souhaitez associer à l'enregistrement d'évaluation.
   d. **Facultatif :** Sélectionnez **Parcourir** pour parcourir et joindre un fichier.
   e. Sélectionnez **Enregistrer**.

   Les enregistrements de vulnérabilité que vous avez sélectionnés sont ajoutés à l'enregistrement d'évaluation et s'affichent dans l'onglet **Entrées de vulnérabilité** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. **Facultatif :** Ajouter les produits affectés.
5. Ajouter le lien connexe à l'enregistrement de l'évaluation.
6. Modifiez les **attributs de risque** pour les CVE primaires associés à l'enregistrement de l'événement d'évaluation de vulnérabilité.

Champ	Description
Corruption de la mémoire	Indique si cet enregistrement d'événement peut corrompre la mémoire.
Exécutable de code distant	Indique si l'exécution du code à distance est possible.
Escalade de privilèges locaux	Indique s'il existe une vulnérabilité d'escalade de privilège local.
Accès non autorisé	Indique s'il existe une vulnérabilité d'accès non autorisé.
DDOS	Indique si l'événement potentiel pourrait impliquer un déni de service distribué.
Complexité de l'attaque	Indique la complexité de la pièce jointe. Les options sont faible, moyenne ou élevée.
Vecteur d'attaque	Indique la voie ou la méthode d'attaque potentielle. Les options sont : réseau, réseau adjacent, local, physique, aucun.
Privilèges requis	Indique le niveau de privilèges requis par un attaquant pour exploiter la vulnérabilité. Les options sont Aucun, Faible ou Élevé.
Interaction de l'utilisateur	Indique si une interaction de l'utilisateur est nécessaire ou non pour exploiter la vulnérabilité.
Impact de la confidentialité	Indique la mesure de l'impact potentiel de la vulnérabilité sur la confidentialité. Les options sont Aucun, Faible ou Élevé
Changement du périmètre	Indique si le périmètre de l'évaluation a changé.
Impact sur la disponibilité	Indique l'impact potentiel sur la disponibilité d'une vulnérabilité d'utilisation abusive exploitée avec succès. La disponibilité fait référence à l'accessibilité des ressources d'information. Les options sont Aucun, Faible ou Élevé
Impact sur l'intégrité	Indique l'impact potentiel sur l'intégrité d'une vulnérabilité d'utilisation abusive exploitée avec succès. L'intégrité fait référence à la fiabilité et à la véracité garantie de l'information.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Les options sont Aucun, Faible ou Élevé
Niveau de rattrapage	Indique l'état ou la disponibilité du rattrapage de la vulnérabilité. Les options sont Réparation officielle, Réparation temporaire, Solution de contournement, Non disponible, Non défini.
Maturité du code d'exploitation	Indique la probabilité d'exploitation de la vulnérabilité en fonction de l'état existant des techniques d'exploitation et de la disponibilité du code. Les options sont Non prouvées, Preuve de concept, Fonctionnelles, Élevées et Non définies.
Fiabilité du rapport	Indique votre degré de confiance dans l'existence de la vulnérabilité.

7. Saisissez les commentaires pertinents dans le champ **Composer** .
   - Saisissez vos notes de travail dans le champ **Notes de travail (privées).**
   - Saisissez vos commentaires (visibles par tout le monde) dans le champ **Commentaires** .
8. **Enregistrez** l'enregistrement de l'évaluation.
   En fonction des mises à jour que vous avez apportées aux champs **d'attribut de risque** pour le CVE principal ou le produit affecté associé à l'enregistrement d'évaluation, le champ de **score de risque** est automatiquement mis à jour.

   Remarque : Pour modifier les règles ou les critères du calculateur de score de risque du système de base, accédez à **Tous** > **Calculateurs de l'évaluation de la vulnérabilité** > **Calculateur du risque de l'évaluation de la vulnérabilité** > **Règle de risque pour l'évaluation de la vulnérabilité**. Vous pouvez ajouter des critères et modifier la pondération au niveau du champ en fonction des critères existants, si nécessaire.

Que faire ensuite
Effectuez une évaluation initiale de l'enregistrement de l'événement.

Supprimer les CVE associés ou les produits affectés de l'enregistrement d'évaluation de la vulnérabilité

Supprimez un enregistrement d'événement de vulnérabilité s'il n'est plus nécessaire.

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche
Vous pouvez supprimer les CVE ou les produits concernés associés à l'enregistrement d'évaluation de vulnérabilité. Vous ne pouvez supprimer les entrées de vulnérabilité/les CVE associés ou les produits affectés que s'ils ont l'état **Nouveau** ou **En attente d'évaluation** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Évaluation de la vulnérabilité**.
2. Sélectionnez l'enregistrement de l'évaluation de vulnérabilité.
3. Sélectionnez l'onglet **Entrées de vulnérabilité** ou l'onglet **Produits affectés** .
4. Sélectionnez l'enregistrement CVE associé ou le produit affecté.
5. Sélectionnez **Supprimer**.

> **Remarque :** Le bouton **Supprimer** s'affiche uniquement pour un enregistrement d'évaluation lorsqu'il a l'état **Nouvelle** ou **En attente d'évaluation** .

Ajouter le lien connexe à l'enregistrement de l'évaluation

Ajoutez des liens et des informations supplémentaires relatifs à l'enregistrement de l'évaluation.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez l'entrée d'enregistrement de l'évaluation.
3. Sélectionnez l'onglet **Liens connexes** .
4. Saisissez une description pertinente dans le champ **Description** .
5. Entrez l'URL dans le champ **Lien** .
6. Sélectionnez **OK**.
   Le lien connexe est ajouté et répertorié dans l'onglet Liens connexes.

Effectuer une évaluation

Une fois que vous avez créé l'enregistrement d'évaluation de vulnérabilité et mis à jour les champs d'attribut de risque, exécutez une évaluation de l'enregistrement d'événement.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche

Effectuez une évaluation initiale après la création d'un événement de vulnérabilité d'intérêt et déterminez qu'elle présente un risque pour les systèmes et les données. Le but de cette activité est d'analyser plus en détail la menace en mettant à jour l'évaluation des risques par une évaluation approfondie de l'exposition.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluation de la vulnérabilité**.
2. Sélectionnez l'enregistrement approprié dans la liste des enregistrements d'événements d'évaluation de vulnérabilité.
3. Sélectionnez **Évaluer** pour exécuter l'évaluation de vulnérabilité.
   La tâche Réponse aux vulnérabilités : traiter l'événement d'évaluation de la vulnérabilité en arrière-plan est lancée et une notification pertinente s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Afficher l'état** sur la notification pour afficher l'état de la tâche en cours d'exécution.
5. Sélectionnez **Enregistrer**.

L'onglet **Évaluations** affiche les détails de l'évaluation. Lorsque l'évaluation est traitée, les VIT ou AVIT associés aux entrées vulnérables ou aux CVE s'affichent dans l'onglet **Éléments vulnérables** ou **Éléments vulnérables de l'application** .

Résultats

- Les éléments vulnérables ou les TPE associés aux CVE associés sont récupérés lors de l'évaluation. Les CI associés aux éléments vulnérables sont également identifiés et affichés dans la table Éléments de configuration affectés.
- Si les CI associés n'existent pas dans la table CI affectés, les CI identifiés sont ajoutés à la table et la valeur du champ **A un élément vulnérable** est définie sur **Vrai**, et la valeur du champ **Source** est définie sur Scanner.
- Si le CI existe déjà dans la table des CI affectés, seule la valeur **du champ A un élément vulnérable** est définie sur **Vrai** et la valeur des champs **Source** pour le CI reste la même que lors de la création de l'enregistrement de l'évaluation.
- Si des éléments vulnérables sont créés après l'évaluation, une tâche planifiée d'évaluation de vulnérabilité est exécutée pour mettre à jour la table des CI affectés et la source du CI.

Que faire ensuite

- Affecter une priorité et un niveau d'exposition à l'enregistrement d'évaluation de vulnérabilité
- Ajouter les CI affectés à l'enregistrement de l'évaluation
- Créer des éléments vulnérables pour le CI affecté ou le composant logiciel affecté
- Ajouter le lien connexe à l'enregistrement de l'évaluation

Information associée

Onglet Évaluation

Onglet Vue d'ensemble

Onglet Évaluation

Examinez les résultats de l'évaluation dans l'onglet Évaluation. Une fois que vous avez effectué une évaluation de l'événement de vulnérabilité, l'enregistrement est corrélé aux données provenant de Nomenclature logicielle et Gestion des actifs logiciels affiché avec des visualisations.

L'onglet Évaluation renseigne les données (le cas échéant) en fonction de l'enregistrement d'évaluation que vous créez et met en corrélation les détails avec les évaluations à partir des données de Gestion des actifs logiciels composant dans Nomenclature logicielle la CMDB.

Fonctionnement de l'évaluation

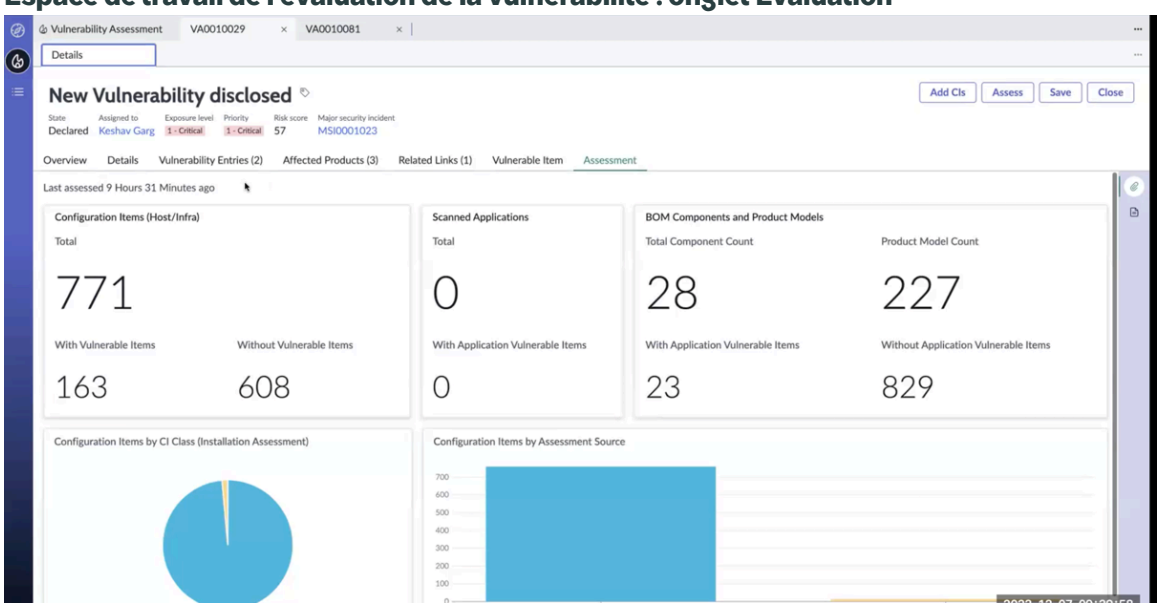
En sélectionnant le bouton **Évaluer** , une évaluation de toutes les CVE associées et des produits affectés à l'aide des données Gestion des actifs logiciels AND SBOM est lancée. Un travail en arrière-plan est déclenché et, lorsque l'évaluation est traitée, les VIT ou AVIT associés aux entrées vulnérables ou aux CVE s'affichent dans les onglets **Vulnerable Items (Éléments vulnérables**) et **Éléments vulnérables de l'application** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Tous les éléments vulnérables ou TPE associés aux CVE sont identifiés.
- Les éléments de configuration (CI) associés aux éléments vulnérables sont également identifiés et affichés dans la table des éléments de configuration affectés.
- Si les CI ne sont pas présents dans la table CI affectés, les CI identifiés sont ajoutés à la table et le marqueur **A un élément vulnérable** est tourné sur vrai et la valeur du champ **Source** est définie sur Scanner.
- Si le CI existe déjà dans la table des éléments de configuration affectés, seul le marqueur **A un élément vulnérable** est défini sur vrai et la **source** reste inchangée depuis la création de l'enregistrement d'évaluation.
- Si des éléments vulnérables sont créés après l'évaluation, une tâche planifiée d'évaluation de vulnérabilité est exécutée pour mettre à jour la table des CI affectés et la source du CI.
- Dans l'espace de travail Évaluation, vous pouvez afficher les horodatages pour voir la dernière évaluation des événements. L'onglet **Évaluation n'est** visible que lorsque les nouvelles évaluations sont créées. Si l'état de l'évaluation est en cours, le dernier état de l'évaluation s'affiche au fur et à mesure de l'évaluation en cours. Pour afficher l'état de l'évaluation mis à jour, vous devez actualiser la page. Une fois l'évaluation terminée, l'utilisateur sera en mesure de voir tous les onglets connexes pour cette évaluation.

Espace de travail de l'évaluation de la vulnérabilité : onglet Évaluation



Les détails de l'évaluation s'affichent pour les widgets suivants.

- Éléments de configuration (Hôte/Infra)
- Applications numérisées
- Composants de nomenclature et modèles de produits
- Éléments de configuration par classe CI (évaluation de l'installation)
- Éléments de configuration par source d'évaluation : affiche la liste des éléments de configuration affectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations des données

Nom	Type	Description
Éléments de configuration (Hôte/ Infra)	Score unique	Affiche le nombre de CI avec et sans VI. Le widget Éléments de configuration affiche le nombre total de CI associés à l'enregistrement d'évaluation. Le widget affiche également les éléments de configuration avec et sans éléments vulnérables.
Applications numérisées	Nombre	Nombre total d'applications analysées avec AVIT. **Remarque :** Vous pouvez afficher le nombre d'applications analysées pour les CVE primaires et secondaires.
Composants de nomenclature et modèles de produits	Score unique	Nombre total de composants, nombre de modèles de produits, avec nombre d'éléments vulnérables de l'application, sans le nombre d'éléments vulnérables de l'application.
Éléments de configuration par source d'évaluation	Barre empilée	Éléments de configuration affectés empilés par source d'évaluation.
Éléments de configuration par classe CI (évaluation de l'installation)	Graphique à secteurs	Éléments de configuration empilés par classe CI.

Onglet Vue d'ensemble

Vue d'ensemble des détails de l'évaluation affichés dans l'onglet Vue d'ensemble. Une fois l'évaluation initiale effectuée, l'enregistrement est corrélé aux données de Nomenclature logicielle et Gestion des actifs logiciels affiché avec des visualisations.

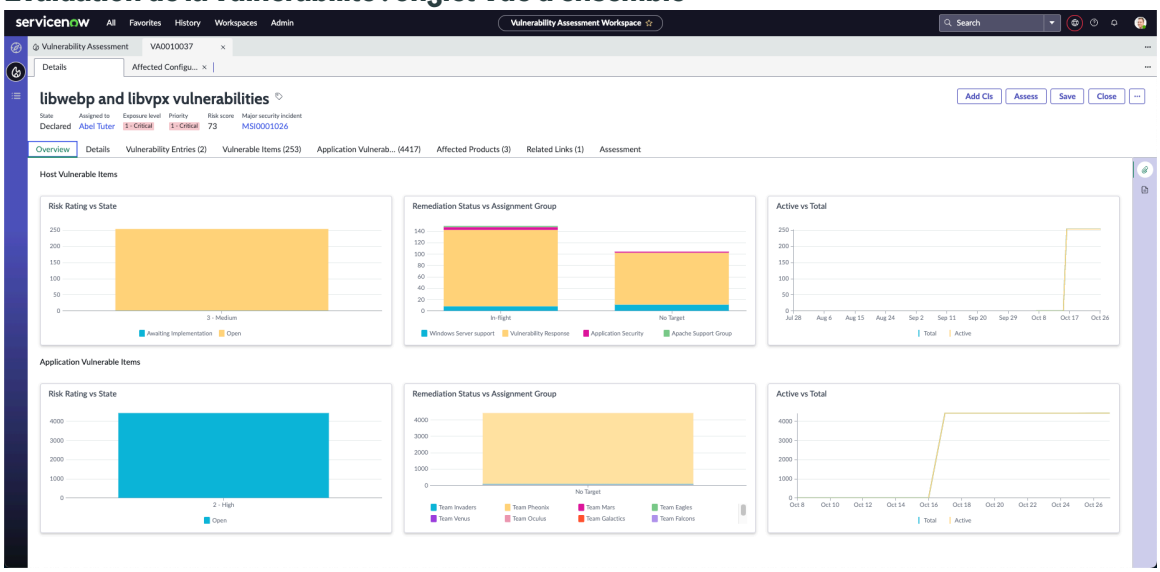
Onglet Vue d'ensemble

L'onglet Vue d'ensemble renseigne les données (le cas échéant) en fonction de l'enregistrement d'évaluation que vous créez et met en corrélation les détails avec les évaluations et Nomenclature logicielle les données de Gestion des actifs logiciels la CMDB. Le champ

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluation de la vulnérabilité : onglet Vue d'ensemble



Les détails de l'évaluation s'affichent pour les widgets suivants.

- Éléments vulnérables d'hôte (hôte/infra)
  - Cote de risque par rapport à l'état
  - État du rattrapage par rapport au groupe d'affectation
  - Actif par rapport à total
- Éléments vulnérables de l'application
  - Cote de risque par rapport à l'état
  - État du rattrapage par rapport au groupe d'affectation
  - Actif par rapport à total

Visualisations des données

Éléments vulnérables d'hôte

Nom	Type	Description
Cote de risque par rapport à l'état	Barre empilée	État des éléments vulnérables empilés par leur cote de risque.
État du rattrapage par rapport au groupe d'affectation	Barre empilée	État du rattrapage de l'élément vulnérable empilé par son groupe d'affectation.
Actif par rapport à total	Liste et ligne	Nombre total d'éléments vulnérables associés à cette entrée par rapport aux éléments vulnérables actifs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Éléments vulnérables de l'application

Nom	Type	Description
Cote de risque par rapport à l'état	Barre empilée	État des éléments vulnérables de l'application empilés par leur cote de risque.
État du rattrapage par rapport au groupe d'affectation	Barre empilée	État du rattrapage de l'élément vulnérable de l'application empilé par son groupe d'affectation.
Actif par rapport à total	Liste et ligne	Nombre total d'éléments vulnérables de l'application associés à cette entrée par rapport aux éléments vulnérables actifs.

Affecter une priorité et un niveau d'exposition à l'enregistrement d'évaluation de vulnérabilité

Affectez manuellement une priorité et un niveau d'exposition à l'enregistrement d'évaluation de vulnérabilité.

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez un enregistrement d'évaluation de vulnérabilité.
3. Accédez aux **attributs de risque** dans l'onglet **Détails** .
4. Sélectionnez une **priorité** dans la liste des options.
5. Sélectionnez un **niveau d'exposition** dans la liste des options.
6. Sélectionnez **Enregistrer**.

Ajouter les CI affectés à l'enregistrement de l'évaluation

Ajoutez manuellement les CI dans votre organisation qui, selon vous, devraient être associés à l'enregistrement d'évaluation des vulnérabilités, mais qui ne s'affichent pas dans les CI affectés après l'évaluation initiale .

Avant de commencer

Rôle requis : sn_vul_analyst.vul_event_manager

Pourquoi et quand exécuter cette tâche

Ajoutez des CI dont vous savez qu'ils peuvent avoir été impactés, mais qui ne s'affichent pas une fois l'évaluation terminée. Vous ne pouvez ajouter des CI que lorsque l'enregistrement de l'évaluation est dans l'état **Déclaré** ou **En attente d'évaluation** .

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez l'enregistrement d'évaluation requis dans la liste.
3. Sélectionnez **Ajouter des CI**.
4. Sélectionnez les éléments de configuration dans la boîte de dialogue Éléments de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez **Ajouter des CI**.
   La tâche d'arrière-plan Réponse aux vulnérabilités - Ajouter des éléments de configuration à l'événement est initiée et une notification pertinente s'affiche.
6. Sélectionnez **Afficher l'état** sur la notification pour afficher l'état de la tâche en cours d'exécution.

Résultats
Les enregistrements sont ajoutés à la table Éléments de configuration affectés avec la **source** sur `Manuel`.

Que faire ensuite
Accédez à l'onglet **Évaluation** et actualisez le widget **Éléments de configuration (hôte/infra)** pour afficher les CI que vous avez ajoutés.

Créer des éléments vulnérables pour le CI affecté ou le composant logiciel affecté

Créez des éléments vulnérables (VI) ou des éléments vulnérables de l'application (AVIT) à partir de l'espace de travail Évaluation de la vulnérabilité. Les analystes de vulnérabilité analysent la liste des VI et recommandent des solutions et des correctifs qui aident l'équipe informatique à corriger ces vulnérabilités.

Le gestionnaire d'événements de vulnérabilité doit être en mesure de sélectionner un, plusieurs ou tous les résultats de recherche d'exposition pour créer des éléments de vulnérabilité.

- Élément vulnérable de l'application pour les résultats d'évaluation SBOM auxquels aucun AVIT n'est associé
- Éléments vulnérables pour les éléments de configuration auxquels aucun VIT n'est associé
- Associez les CVE primaires aux éléments de vulnérabilité.

Créer des VI pour des éléments de configuration sans éléments vulnérables associés

Créer des éléments vulnérables VIT pour les éléments de configuration identifiés via l'évaluation de la vulnérabilité mais qui n'ont pas de VIT associés à l'enregistrement.

Avant de commencer
Rôle requis : admin

Procédure
1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluations**.
2. Sélectionnez l'enregistrement d'évaluation dont vous avez besoin pour créer le VIT.
3. Sélectionnez l'onglet **Évaluation** .
4. Sélectionner **sans nombre d'éléments de configuration** à partir du widget **Éléments de configuration (infra hôte).**
5. Sélectionnez les éléments de configuration pour lesquels vous souhaitez créer des VIT à partir de la liste **Éléments de configuration affectés** .
6. Sélectionnez **Créer un élément vulnérable**.
   La tâche d'arrière-plan de l'évaluation des vulnérabilités de Vulnerability Response - Créer des VIT manuels est lancée et une notification pertinente s'affiche.
7. Sélectionnez **Afficher l'état** sur la notification pour afficher l'état de la tâche en cours d'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les éléments vulnérables des éléments de configuration affectés que vous avez sélectionnés sont créés.

Le widget **Éléments de configuration (infra hôte)** affiche désormais le même CI dans le nombre Avec **éléments vulnérables** .

Créez des éléments vulnérables de l'application (AVIT) pour les produits, modèles ou composants affectés sans éléments vulnérables de l'application associés

Créez des éléments vulnérables de l'application (AVIT) pour les produits ou composants affectés, les éléments identifiés via l'évaluation des vulnérabilités, mais qui n'ont pas d'AVIT associés à l'enregistrement.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité** > **Évaluations**.
2. Sélectionnez l'enregistrement d'évaluation dont vous avez besoin pour créer le VIT.
3. Sélectionnez l'onglet **Évaluation** .
4. Sélectionnez **Sans nombre d'éléments vulnérables d'application** dans le widget **Composants de nomenclature et Modèles de produits** .
5. Sélectionnez les modèles de produits affectés pour lesquels vous souhaitez créer des AVIT à partir de la liste **Modèles de produits affectés** .
6. **Sélectionnez Créer un élément vulnérable de l'application**.
   La tâche d'arrière-plan de l'évaluation des vulnérabilités de Vulnerability Response - Créer des VIT manuels est lancée et une notification pertinente s'affiche.
7. Sélectionnez **Afficher l'état** sur la notification pour afficher l'état de la tâche en cours d'exécution.
   Les éléments vulnérables de l'application pour les modèles de produits affectés, les éléments que vous avez sélectionnés sont créés. pour les CVE primaires associées à l'enregistrement.

   Le widget **Composants de nomenclature et Modèles de produit** affiche désormais le même modèle de produit ou composant dans le nombre **d'éléments vulnérables de l'application** .

Lier l'enregistrement de l'évaluation des vulnérabilités à un incident de sécurité majeur dans Gestion des incidents de sécurité majeurs

Vous pouvez lier, proposer ou promouvoir l'enregistrement de l'évaluation à Incident de sécurité majeur condition d'avoir accès à l'application Gestion des incidents de sécurité majeurs .

Avant de commencer
Rôle requis : sn_vul_analyst.vul_event_manager, sn_si.analyst sn_msi.workspace_admin

Pourquoi et quand exécuter cette tâche
Vous pouvez déplacer l'enregistrement de l'évaluation pour l'associer à un incident de sécurité majeur existant, créer un nouveau MSI à partir de l'enregistrement d'évaluation ou promouvoir l'enregistrement de l'évaluation de la vulnérabilité en incident de sécurité majeur. Tirez parti des Gestion des incidents de sécurité majeurs fonctionnalités telles que les intégrations avec Microsoft Teams et Microsoft SharePoint.

Vous pouvez également afficher le lien vers les incidents de sécurité majeurs dans l'espace de travail du gestionnaire de vulnérabilité pour les éléments vulnérables. Le MSIM lien sera

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

associé à l'évaluation de vulnérabilité qui sera affichée sur les éléments de vulnérabilité ainsi que sur les autres espaces de travail de Réponse aux vulnérabilités.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail de l'évaluation de la vulnérabilité**.
2. Sélectionnez l'enregistrement d'évaluation que vous souhaitez lier à un incident de sécurité majeur.
3. Sélectionnez l'icône Actions **supplémentaires** , dans l'onglet **Détails** .
4. Sélectionnez l'une des options suivantes :

Option	Description
Lier à l'incident de sécurité majeur	Sélectionnez l'enregistrement MSI existant dans la liste des incidents de sécurité majeurs. L'enregistrement de l'évaluation de la vulnérabilité est lié à l'incident de sécurité majeur existant.
Proposer comme incident de sécurité majeur	Saisissez les détails suivants et sélectionnez **Proposer**. ○ Date de détection ○ Justification ○ Impact potentiel
Promouvoir comme incident de sécurité majeur	Entrez les détails suivants et sélectionnez **Promouvoir**. ○ Date de détection ○ Date de résolution estimée ○ Justification ○ Impact potentiel

5. Sélectionnez **Enregistrer**.

Que faire ensuite

Sélectionnez l'enregistrement MSI pour ouvrir l'enregistrement dans la Gestion des incidents de sécurité majeurs vue.

Information associée

Lier à Incident de sécurité majeur

Proposer en tant que Incident de sécurité majeur

Promouvoir à Incident de sécurité majeur

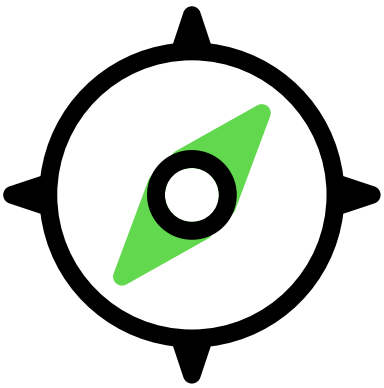
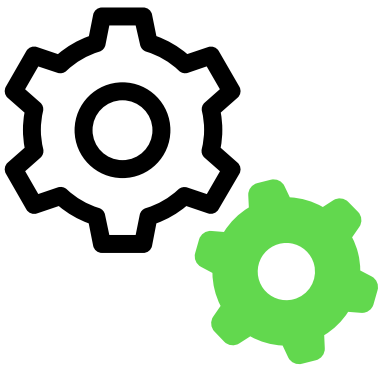
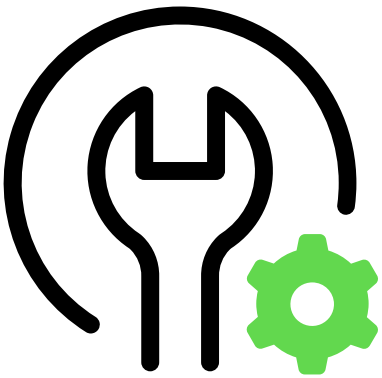
Nomenclature logicielle

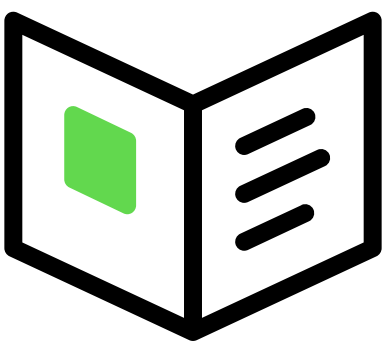
Affichez une liste des composants logiciels open source et tiers que vous utilisez dans le développement de vos applications. Obtenez des informations sur les licences logicielles, les informations de version et les vulnérabilités connues de vos composants dans les Nomenclature logicielle fichiers (SBOM) que vous chargez dans votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Premiers pas

Explorer	Configurer	Utiliser
		
En savoir plus sur les concepts et les SBOM fonctionnalités.	Configurer les SBOM applications.	Découvrez comment importer SBOM des composants et afficher des données dans l’espace de travail.

Référence

Obtenez des détails sur SBOM les formulaires, les champs, les tables et les propriétés.

Dépannage et demande d'aide

- Communauté Security Operations
- CycloneDX - Nomenclature logicielle (SBOM).
- SPDX .
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues .
- Contact Service client et assistance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer Nomenclature logicielle

Identifiez les composants utilisés dans les applications de votre organisation à partir des Nomenclature logicielle fichiers queSBOM vous chargez dans votre instance. Comprenez tous les risques associés à l'utilisation de logiciels open source pour vous aider à déterminer votre exposition potentielle, à consulter la conformité des licences et à corriger les vulnérabilités.

Vue d'ensemble de Nomenclature logicielle

Les composants tiers et open source vous offrent de nombreux avantages pour la création et la mise en production rapides de vos projets logiciels. Cependant, dans certains cas, il existe des risques associés à l'utilisation de composants accessibles au public, tels que les suivants :

- Manque de visibilité sur l'intégrité des composants
- Vulnérabilités dans les logiciels open source
- Package Intelligence pour les logiciels open source
- Licences de logiciels non conformes

Vous pouvez charger vos fichiers de nomenclature logicielle via une API ou manuellement. Affichez les fichiers que vous importez en tant qu'entités, qui sont des inventaires des bibliothèques de composants tiers utilisées dans votre logiciel, y compris les dépendances transitives et les informations de gestion des licences disponibles.

Pour plus d'informations sur ce qui est inclus dans les inventaires de logiciels dans les nomenclatures logicielles CycloneDX et SPDX, voir CycloneDX - nomenclature logicielle (SBOM) et SPDX .

Nomenclature logicielle utilisateurs

Utilisateurs

Utilisateur	Description
Responsables et analystes des vulnérabilités	Affichez les fichiers de nomenclature logicielle chargés dans les enregistrements, les visualisations de données, ainsi que des renseignements améliorés sur les vulnérabilités dans l'espace Nomenclature logicielle de travail (SBOM). Les responsables des vulnérabilités et les analystes utilisent ces informations pour déterminer la conformité de vos licences logicielles et l'exposition potentielle aux risques liés à l'utilisation de logiciels open source.
Utilisateurs qui peuvent inclure, mais sans s'y limiter : • Avocats spécialisés dans la technologie ou les logiciels • Responsables IT	Affichez les licences de logiciels propriétaires et open source téléchargées pour les composants de vos fichiers téléchargés SBOM . Créez une base de données de licences logicielles propriétaires et open source pour les composants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs (suite)

Utilisateur	Description
• Auditeurs • Gestionnaires et équipes des actifs logiciels	Examinez et classez les licences avec des informations manquantes en fonction de vos politiques internes ou réglementaires. Faites correspondre vos composants aux licences, déterminez la conformité globale de votre licence et voyez votre exposition potentielle aux risques liés aux licences interdites, restreintes ou manquantes.

Workflow Nomenclature logicielle

Les applications SBOM vous permettent de charger des fichiers et d'afficher les détails des entités, les inventaires de composants, les vulnérabilités et les informations de licence de logiciel dans l'espace de travail Nomenclature logicielle (SBOM).

- Chargez SBOM des fichiers avec une API ou manuellement.
- Examinez les composants du SBOM fichier que vous avez chargé dans l'espace de SBOM travail.
- Examinez les informations de licence de composant à partir des fichiers chargés SBOM et classez-les pour vous aider à identifier votre exposition aux licences restreintes ou interdites.
- Évaluez votre exposition au risque et créez des éléments vulnérables pour les composants qui présentent des vulnérabilités associées.
- Affichez les rapports et les tableaux de bord, ainsi que la conformité globale de votre licence pour les composants chargés SBOM sur la page d'accueil de l'espace SBOM de travail.

Nomenclature logicielle avantages

Trois applications de nomenclature logicielle vous permettent d'afficher un inventaire précis de vos composants logiciels et des risques associés :

- Modèle de données pour SBOM
- SBOM Core
- SBOM Réponse

Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response .

SBOM avantages

Avantage	Application	Versions prises en charge
Cette application fournit les tables utilisées pour stocker SBOM les données. Cette application est requise. Elle comprend les tables, les ACL et les rôles requis pour lire SBOM les données.	Modèle de données pour SBOM	v4.0, v3.0, v2.0

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

SBOM avantages (suite)

Avantage	Application	Versions prises en charge
Cette application est requise. Elle comprend l'API requise pour charger SBOM des documents et la logique métier requise pour analyser et importer les données de ces documents dans votre instance. Vous pouvez afficher un inventaire de vos composants logiciels dans SBOM l'espace de travail, mais vous ne pouvez pas afficher les visualisations de données sur la page de destination. Téléchargez, analysez et traitez vos fichiers de nomenclature logicielle dans les normes CycloneDX et SPDX. Consultez la colonne Versions prises en charge pour connaître les formats de fichier et les versions pris en charge pour ces produits. Affichez les entités de nomenclature (BOM) et un inventaire de vos composants logiciels. Une entité BOM est le composant de niveau racine d'un fichier SBOM. Par exemple, pour un CycloneDX SBOM, le composant répertorié dans les métadonnées est considéré comme l'entité BOM.	SBOM Core	v6.0, v5.0, v4.0 À partir de la version 4.0, SBOM Core prend en charge : • XML et JSON versions 1.0 à 1.6 de CycloneDX. • JSON versions 2.2 à 2.3 de SPDX.
• SBOM Une réponse est requise si vous souhaitez accéder aux fonctionnalités et aux visualisations de données sur la page de destination dans l'espace de travail SBOM . • Nomenclature logicielle La réponse nécessite l'application Réponse aux vulnérabilités . • Affichez l'inventaire de vos composants et évaluez votre exposition au risque dans l'espace de SBOM travail. Configurez des règles pour créer automatiquement des éléments vulnérables de l'application (AVIT) et corrigez-les avec le Réponse aux vulnérabilités des applications workflow. • Affichez les informations de licence de composant téléchargées avec vos SBOM fichiers dans le module Administration de licences. Classez et résolvez (associez) les composants que vous chargez dans vos Réponse aux vulnérabilités des applications fichiers aux licences afin de voir l'état de conformité global de votre licence. • À partir de la version 4.0 de Réponse aux vulnérabilités des applications Response, vous pouvez afficher les composants identifiés comme périmés ou abandonnés comme	SBOM Réponse	v6.0, v5.0, v4.0

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

SBOM avantages (suite)

Avantage	Application	Versions prises en charge

« non conformes » dans l'interface Policy as Code Engine (PaCE) disponible dans l'espace de SBOM travail.
 	
• Les intégrations OSV.dev et Deps.dev sont incluses lorsque vous installez SBOM Response.
  ◦ OSV.dev s'agit d'une API open source qui fournit des informations de veille sur les vulnérabilités pour une version donnée d'un package ou d'une bibliothèque.
  ◦ Deps.dev est une API open source qui fournit une liste des versions pour un package ou une bibliothèque donnée et identifie les composants qui sont à **l'état périmé** et **abandonné** .
 	
Consultez Configuration des intégrations Deps.dev, OSV.dev et PaCE pour Nomenclature logicielle pour plus d'informations.
 	
Consultez la section Intégrer PaCE avec d'autres applications pour plus d'informations sur PaCE et les politiques PaCE.		

Générez et chargez (Nomenclature logicielleSBOM) des fichiers pour les logiciels tout au long de leurs cycles de développement d'intégration et de déploiement continus.	SBOM Réponse	• Modèle de données pour SBOM: v1.4 et versions ultérieures. • SBOM Core : v3.0 et versions ultérieures. • SBOM Réponse : v4.0 et versions ultérieures.

Réponse aux vulnérabilités applications et CSDM tables

Réponse aux vulnérabilités des applications Les Réponse aux vulnérabilités intégrations et Nomenclature logicielle applications de vulnérabilité tierces gèrent les tables (y contribuent des données). CSDM Ces applications utilisent également des données provenant de CSDM tables générées par d'autres applications. Plusieurs ServiceNow produits bénéficient donc de ces Opérations de sécurité applications et y ajoutent de la valeur. Consultez Réponse aux vulnérabilités applications et CSDM tables pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce qu'il faut explorer ensuite

Pour en savoir plus sur la configuration et l'utilisation de Nomenclature logicielle, consultez :

- Explorer les applications prises en charge pour Nomenclature logicielle
- Configurer Nomenclature logicielle
- Chargement et affichage de vos SBOM fichiers dans l'espace de SBOM travail
- Afficher des rapports et des tableaux de bord dans l'espace de Nomenclature logicielle travail

Explorer les applications prises en charge pour Nomenclature logicielle

Les renseignements sur les vulnérabilités tiers et d'autres intégrations avec les Nomenclature logicielle applications peuvent améliorer les données de vos fichiers chargés.

Avantages des applications prises en charge

Les renseignements sur les vulnérabilités tiers et d'autres intégrations aux applications vous permettent d'afficher les Nomenclature logicielle nombres de composants considérés comme périmés et abandonnés, ainsi que des informations indiquant si vous pouvez corriger les vulnérabilités associées aux composants.

Les ServiceNow® applications et les intégrations tierces répertoriées dans le tableau suivant sont prises en charge par les SBOM applications. Ces applications vous fournissent des données de vulnérabilité enrichies, des renseignements sur la vulnérabilité et d'autres informations clés qui peuvent vous aider à visualiser et à hiérarchiser les vulnérabilités associées aux fichiers SBOM. Toutes ces applications et intégrations sont disponibles à partir du ServiceNow® Store.

Applications et intégrations tierces prises en charge

Avantage	Application	Versions prises en charge	Utilisateurs
Réponse aux vulnérabilités est nécessaire si vous installez l'application SBOM Response. Installez l'application Réponse aux vulnérabilités avant d'installer SBOM Response. Réponse aux vulnérabilités des applications fonctionnalités sont installées avec Réponse aux vulnérabilités. Ces fonctionnalités permettent d'accéder à l'espace	Réponse aux vulnérabilités	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response .	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications et intégrations tierces prises en charge (suite)

Avantage	Application	Versions prises en charge	Utilisateurs
de travail du gestionnaire de vulnérabilités dans l'application et au workflow de vulnérabilité pour vous aider à corriger les éléments vulnérables de l'application Réponse aux vulnérabilités (AVIT).			
Affichez les données améliorées de vulnérabilité et de gravité NVD. Affichez les données importées à partir des intégrations NVD et CWE pour enrichir toutes les données de vulnérabilité que vous pourriez trouver dans vos données SBOM. Consultez Importation de données avec les intégrations NVD et CWE et gestion de bibliothèques tierces pour plus d'informations.	Vulnerability Response Integration avec NVD et SBOM Response	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response .	
Importez des fichiers de nomenclatures logicielles avec le Veracode Vulnerability Integration fichier . Cela Veracode Vulnerability Integration inclut les améliorations suivantes avec Veracode les fichiers SBOM : • Si vous avez installé SBOM Response, vous avez la possibilité d'inclure les vulnérabilités trouvées pour SBOM les SBOM	Intégration de vulnérabilité Veracode et réponse SBOM	À partir de la version 4.3 du .Veracode Vulnerability Integration Si vous avez déjà installé, vous pouvez également télécharger les données importées Veracode SBOM aux formats CycloneDX (JSON et XML) et SPDX (XML) à partir de la Veracode Vulnerability Integration version v3.0 de SBOM Core.	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications et intégrations tierces prises en charge (suite)

Avantage	Application	Versions prises en charge	Utilisateurs
fichiers que vous chargez. • SBOM est mappé au champ Source pour les enregistrements de la table Nomenclature [sn_sbom_doc] pour les SBOM SBOM fichiers que vous chargez. Consultez Veracode Vulnerability Integration pour plus d'informations.		Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response .	
Chargez SBOM des ServiceNow AI Platform fichiers à partir de vos référentiels GitHub. Déterminez si SBOM les fichiers générés dans vos pipelines CI/CD (intégration continue et livraison/déploiement continus) ont été mis en file d'attente avec succès dans votre ServiceNow AI Platform instance. Protégez vos environnements contre les composants potentiellement dangereux pendant les cycles de développement logiciel avec GitHub Actions que vous lancez à partir de votre environnement GitHub.	Obtenez toutes les actions GitHub requises pour SBOM le chargement dans GitHub Marketplace.	À partir de la version 4.0 de SBOM Core.	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Nomenclature logicielle

Téléchargez et activez les applications requises pour l'application Nomenclature logicielle (SBOM) avant de charger les SBOM fichiers.

Vue d'ensemble de la configuration

1. Téléchargez les applications requises SBOM et toutes les applications et intégrations prises en charge supplémentaires que vous souhaitez à partir de ServiceNow Store dans votre instance ServiceNow. Consultez Explorer Nomenclature logicielle et Télécharger une application à partir de ServiceNow Store pour la première fois pour plus d'informations sur les applications prises en charge.

   L'application Vulnerability Response est requise pour SBOM Response. Installez l'application Vulnerability Response avant d'installer SBOM Response.

2. Localisez les applications SBOM que vous avez téléchargées et sélectionnez Installer pour les activer ainsi que leurs dépendances dans l'ordre suivant. Consultez Installer les applications prises en charge pour Nomenclature logicielle.

   - Vulnerability Response et ses dépendances
   - Intégration de Vulnerability Response avec NVD
   - Modèle de données pour SBOM
   - SBOM Core
   - SBOM Réponse, qui inclut les intégrations OSV.dev et Deps.dev et l'accès aux options de Policy as Code Engine (PaCE) dans l'espace de travail SBOM.

3. Configurez les intégrations Deps.dev et OSV.dev. Ces intégrations sont incluses dans l'application SBOM Response et sont installées et activées automatiquement. Vous devez lancer l'intégration OSV.dev : complète sur demande à partir de son enregistrement d'intégration. Voir Configuration des intégrations Deps.dev, OSV.dev et PaCE pour Nomenclature logicielle et Explorer Nomenclature logicielle pour plus d'informations.

   L'intégration Deps.dev vous fournit des informations sur les composants qui sont à **l'état périmé** et **abandonné** pour une version donnée d'un package ou d'une bibliothèque que vous chargez dans vos SBOM fichiers.

   OSV.dev extrait les données de vulnérabilité d'une base de données open source pour une version d'un package ou d'une bibliothèque que vous chargez dans vos SBOM fichiers.

4. Consultez la documentation produit pour configurer toutes les applications et intégrations prises en charge supplémentaires que vous avez installées. Consultez Intégrations de Réponse aux vulnérabilités et Intégrer Réponse aux vulnérabilités des applications avec d'autres applications.

Installer les applications prises en charge pour Nomenclature logicielle

Téléchargez et activez les applications requises pour l'application Nomenclature logicielle (SBOM) avant de charger les fichiers.

Avant de commencer
Rôles requis : administrateur pour le téléchargement, l'installation et l'activation de toutes les applications et les affectations de rôles dans votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Procédure

1. Téléchargez les applications requises SBOM à partir de dans ServiceNow Store votre ServiceNow instance.

   Ces applications vous permettent de charger et d'importer SBOM des fichiers dans votre instance. Vous pouvez afficher les données d'entité et de composant BOM dans l'espace de SBOM travail si vous avez SBOM installé Core.

   Vous pouvez afficher l'entité BOM, les données des composants et les visualisations de données dans l'espace de SBOM travail si Response est SBOM installé.

   - Modèle de données pour SBOM
   - SBOM Core

   Pour plus d'informations sur le téléchargement et l'activation des applications, consultez les rubriques suivantes :

   - Installer une ServiceNow Store application
   - Installer une mise à jour dans une ServiceNow Store application

2. **Facultatif :** Si vous souhaitez afficher vos SBOM données dans l'espace de travail, afficher les renseignements sur les SBOM vulnérabilités tiers importés, évaluer votre exposition aux risques et corriger les vulnérabilités avec les Réponse aux vulnérabilités des applications workflows and Réponse aux vulnérabilités , téléchargez les applications suivantes :

   - Réponse aux vulnérabilités et ses dépendances
   - Intégration de Vulnerability Response avec NVD
   - SBOM Réponse

   Pour plus d'informations sur ces applications et d'autres applications prises en charge SBOM , reportez-vous à la section Explorer Nomenclature logicielle.

3. Une fois les applications téléchargées, accédez à **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.
4. Localisez les SBOM applications que vous avez téléchargées et sélectionnez **Installer** pour les activer ainsi que leurs dépendances.

   Un message s'affiche après l'activation réussie d'une application. Activez les applications dans l'ordre suivant :

   - Réponse aux vulnérabilités et ses dépendances
   - Intégration de Vulnerability Response avec NVD
   - Modèle de données pour SBOM
   - SBOM Core
   - SBOM Réponse, qui inclut les intégrations OSV.dev et Deps.dev et prend en charge l'interface Policy as Code Engine (PaCE) dans l'espace de SBOM travail.

   Reportez-vous à la section Configuration des intégrations Deps.dev, OSV.dev et PaCE pour Nomenclature logicielle pour plus d'informations sur la configuration de ces applications d'intégration après avoir installé SBOM Response.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Facultatif :** Activer les intégrations en accédant à **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous** et en sélectionnant **Installer**.

   (Optional) Pour en savoir plus sur ces intégrations et les options qu'elles offrent, reportez-vous à la section Explorer Nomenclature logicielle.

   - Intégration de Vulnerability Response avec Veracode. Consultez Installer l'intégration ServiceNow de Vulnerability Response avec Veracode pour plus d'informations.
   - Intégration de Vulnerability Response avec NVD, nécessaire si vous souhaitez afficher les données améliorées pour les vulnérabilités associées aux composants chargés. Consultez Présentation des intégrations NVD pour plus d'informations.
   - Intégration complète de CWE 2000. Reportez-vous à la rubrique Configurer et exécuter la tâche planifiée pour la mise à jour des enregistrements CWE pour en savoir plus sur l'activation de cette tâche planifiée.

   Un message s'affiche après l'activation réussie d'une application.

6. Affectez les rôles suivants aux utilisateurs.
   - sn_sbom_dm.app_créer
   - sn_sbom_dm.app_lecture
   - sn_sbom_dm.app_écriture
   - sn_sbom_core.sbom_ingest
   - sn_sbom_core.admin
   - sn_sbom_resp.sbom_analyst
   - sn_sbom_resp.manage_avi_rule
   - sn_sbom_response.managelicense
   - sn_sbom_response.licenseresolver
7. **Facultatif :** Affectez des utilisateurs au groupe Gestionnaire de sécurité des applications si vous créez des éléments vulnérables d'applications pour les vulnérabilités de vos données importées SBOM .

   (Optional) Les utilisateurs affectés au groupe de gestionnaires App-Sec classent par ordre de priorité et gèrent les éléments vulnérables de l'application. Les utilisateurs de ce groupe héritent de la plupart des rôles requis pour lire et modifier les enregistrements et configurer les applications prises en charge par l'application Réponse aux vulnérabilités des applications et ses workflows de rattrapage.

8. **Facultatif :** Désactivez la propriété système Rouvrir les AVIT en cas de détection (`sn_sbom_resp.reopen_avits_if_detected`) si vous ne souhaitez pas que les AVIT **fermés** reviennent automatiquement à l'état **Ouvert** .

   (Optional) Un élément vulnérable d'application **fermé** (AVIT) pour un composant avec une vulnérabilité associée est rouvert (défini sur **Ouvert**) automatiquement et visible dans l'espace de travail SBOM si les conditions suivantes existent :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'AVIT avec la vulnérabilité associée est détecté à nouveau par les analyses de vulnérabilité d'une intégration tierce ou le composant avec la vulnérabilité fait partie d'un chargement SBOM ultérieur.
- Vous n'avez pas désactivé la propriété système Rouvrir les AVIT si détecté (*sn_sbom_resp.reopen_avits_if_detected*). Cette propriété système est activée par défaut.
- Le sous-état de l'AVIT **fermé** n'est pas l'un des suivants : **Contrôle d'atténuation en place**, **Non affecté** ou **Faux positif**. Les AVIT avec ces sous-états ne sont pas rouverts par la propriété système.

Que faire ensuite
Téléchargez vos SBOM fichiers. Voir Télécharger Nomenclature logicielle des fichiers manuellement et Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API pour plus d'informations.

Configuration des intégrations Deps.dev, OSV.dev et PaCE pour Nomenclature logicielle

Vous pouvez modifier certains des paramètres des intégrations Deps.dev et OSV.dev. Il existe également deux versions de déclencheur de code de ces intégrations qui sont utilisées uniquement pour les workflows internes, et vous ne devez pas initier ces intégrations à la demande. En outre, vous pouvez activer une tâche planifiée pour créer des politiques à l'aide de Policy as Code Engine (PaCE).

Intégrations de déclencheurs de code pour les workflows internes

À partir de la version 3.2 de SBOM Response, les améliorations des performances comprenaient l'ajout de deux intégrations OSV.dev et Deps.dev déclencheurs de code :

- Intégration OSV (déclencheur de code à la demande)
- Intégration Deps.dev (déclencheur de code à la demande)

Ces intégrations sont lancées automatiquement par des workflows internes et sont destinées à un usage interne uniquement. Bien que vous puissiez les localiser, vous ne devez pas initier ces intégrations sur demande avec le bouton **Exécuter maintenant** à partir de leurs enregistrements d'intégration.

Configuration du calendrier d'exécution pour l'intégration Deps.dev

L'intégration Deps.dev est installée avec SBOM Response. L'intégration est activée (case Actif cochée sur l'enregistrement d'intégration) par défaut et planifiée pour s'exécuter toutes les semaines. Notez qu'il ne s'agit pas de l'intégration de déclencheur de code de Deps.dev à la demande et que vous pouvez modifier le calendrier et lancer la tâche planifiée sur demande à partir de son enregistrement d'intégration. .

Pour modifier le calendrier, accédez à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations** > **Intégration Deps.dev**. Le rôle sn_vul.app_configure_integrations est requis pour modifier le calendrier de cette intégration.

Cette intégration Deps.dev est utilisée pour identifier les composants qui sont à **l'état périmé** et **abandonné** . La version d'un composant périmé a plus de deux versions majeures de retard sur la dernière version et deux ans de retard sur la dernière version. Un composant abandonné n'a pas été mis à jour depuis plus de deux ans. Les seuils de deux ans et de deux versions peuvent être modifiés avec les propriétés système. Pour modifier ces paramètres, accédez à **Tous** > **Propriétés système** > **Toutes les propriétés** et localisez les enregistrements suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_sbom_resp.pkg_abandoned_threshold
- sn_sbom_resp.pkg_stale_threshold
- sn_sbom_resp.pkg_stale_version_threshold

Les valeurs de seuil pour les éléments abandonnés et périmés sont exprimées en mois. La valeur de seuil de la version est numérique.

Vous pouvez afficher les données importées sur la page d'accueil de l'espace de travail et dans le module File d'attente BOM. Les données importées sont stockées dans la table Groupes de packages [sn_sbom_pkg_group].

Configuration et lancement de l'intégration OSV.dev : complète

L'intégration complète de OSV.dev est installée avec SBOM Response. L'intégration est activée par défaut (case Actif cochée sur l'enregistrement d'intégration). Notez qu'il ne s'agit pas de l'intégration de déclencheurs de code de OSV.dev à la demande et que vous devez initier cette intégration sur demande à partir de son enregistrement d'intégration.

Pour configurer et lancer cette intégration, accédez à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations** > **Intégration OSV.dev : complète**. Le rôle sn_vul.app_configure_integrations est requis.

Vous pouvez afficher les données importées sur la page d'accueil de l'espace de travail, sous l'onglet Vulnérabilité, sur les enregistrements de la liste des entités et dans le module Bibliothèques. Les données importées sont stockées dans les tables Entrées vulnérables de l'application [sn_vul_app_vul_entry] et Entrées de base de données de vulnérabilité nationale [sn_vul_nvd_entry].

Remarque : Vous pouvez configurer le paramètre d'intégration OSV.dev dans l'onglet Paramètres d'intégration *batchSize* de **l'instance Open Source Vulnerabilities située** à **Tous** > **Réponse aux vulnérabilités** > **Administration** > **Intégrations** > **Intégrations de vulnérabilité** > **Instance de vulnérabilités open source**. La valeur par défaut est de 75 PURLS par appel d'API.

Vous préférez peut-être conserver cette valeur dans son paramètre par défaut. La modification de la valeur peut avoir un impact sur les performances.

Activation de PaCE

À partir de la version 4.0 de SBOM Response, vous pouvez afficher les composants identifiés comme périmés ou abandonnés comme « non conformes » dans l'interface Policy as Code Engine (PaCE) disponible dans l'espace de SBOM travail.

- Déterminez si les composants sont périmés ou abandonnés avec la *Run PaCE policies for SBOM Response* tâche planifiée. Cette tâche planifiée est désactivée par défaut.
- Affichez les composants identifiés comme périmés ou abandonnés comme non conformes dans l'interface PaCE disponible et affichée dans l'espace de SBOM travail.

Consultez la section Intégrer PaCE avec d'autres applications pour plus d'informations sur PaCE et les politiques PaCE.

Chargement et affichage de vos SBOM fichiers dans l'espace de SBOM travail

Les SBOM applications vous permettent de charger des fichiers et d'afficher les détails des entités, les inventaires de composants, les informations de licence et d'autres détails dans l'espace de travail Nomenclature logicielle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble du chargement des SBOM fichiers

Vous pouvez charger vos fichiers de nomenclature logicielle via une API ou manuellement. Affichez les fichiers que vous importez en tant qu'entités, qui sont des inventaires des bibliothèques de composants tiers utilisées dans votre logiciel, y compris les dépendances transitives.

- Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API.

  L'API Upload est utilisée pour charger et ingérer un SBOM fichier (CycloneDX/SPDX) dans votre instance.

- Télécharger Nomenclature logicielle des fichiers manuellement.

  Chargez manuellement les fichiers de nomenclature logicielle. La méthode que vous utilisez pour télécharger vos fichiers varie selon que vous avez installé les SBOM applications Core ou SBOM Response.

- Chargement des Nomenclature logicielle fichiers DevOps SBOM.

  Générez et chargez des SBOM fichiers pour les logiciels tout au long de leurs cycles de développement d'intégration et de déploiement continus.

- Classez et résolvez les licences de composants dans le module Administration de licences.

  Examinez, classez et résolvez (attribuez) les informations de licence pour les composants que vous chargez dans vos SBOM fichiers conformément à vos politiques internes ou réglementaires. Vous pouvez faire correspondre vos composants aux licences et déterminer la conformité globale de votre licence pour voir votre exposition potentielle aux risques liés aux licences interdites, restreintes ou manquantes.

- Afficher des rapports et des tableaux de bord dans l'espace de Nomenclature logicielle travail

  Les analystes et les gestionnaires de vulnérabilité peuvent consulter les fichiers de nomenclature logicielle chargés et les données importantes dans les enregistrements et les visualisations de données, ainsi que des renseignements améliorés sur les vulnérabilités et des informations de licence dans l'espace de Nomenclature logicielle travail (SBOM).

  Remarque : Vous devez installer SBOM Réponse si vous souhaitez afficher les visualisations de données sur la page de destination (accueil) de l'espace de travail.

Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API

Vérifiez les informations suivantes avant de charger des Nomenclature logicielle fichiers à l'aide d'une API.

Utilisation de REST API

Pour charger un fichier SBOM avec une API, le rôle sn_sbom_core.sbom_ingest est requis.

API de chargement.

Cette API est utilisée pour charger et ingérer un fichier SBOM (CycloneDX/SPDX) dans votre instance.

La version 4.0 de SBOM Core prend en charge :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- XML et JSON dans CycloneDx (versions 1.0 - 1.6).
- JSON dans SPDX (versions 2.2-2.3)

- **Remarque :** Les fichiers de plus de 32 Mo peuvent ne pas se charger correctement.

Méthode HTTP : (POST)

URL d'API : `<host_name>/api/sbom/core/upload`

Remarque : `<host_name>` est le nom de votre ServiceNow instance.

Tous les paramètres de demande ci-dessous sont facultatifs ; le corps de la demande est le contenu du fichier SBOM. Si vous utilisez DevOps dans le cadre de votre processus de développement, la valeur de « requestedBy » doit être « devops ». Consultez la section Chargement des Nomenclature logicielle fichiers DevOps SBOM pour plus d'informations générales sur DevOps. Si la valeur de « requestedby » est « devops » (opérations de développement), ces paramètres sont obligatoires :

- ID de construction
- Étape du cycle de vie

De plus, si « requestedBy » est « devops », les données pour fetchVulenrabilityInfo et fetchPackageInfo sont incluses.

- buildId : chaîne que vous envoyez
- Étape du cycle de vie : deux valeurs, production ou pre_production
- fetchVulenrabilityInfo- t/f
- fetchPackageInfo-t/f

Paramètres de demande	Valeurs possibles	Description
productModelId	ID système	ID système du modèle de produit à mapper à l'application racine du SBOM.
businessApplicationId	ID système	ID système de l'application d'entreprise à mapper à l'application racine du SBOM.
businessApplicationName (déconseillé)	Nom de votre application d'entreprise	Nom de l'application d'entreprise à mapper à l'application racine du fichier .SBOM
Source sbom	Un produit tel que Veracode, par exemple	La source de votre SBOM fichier.
requestedBy	Un outil ou le nom d'une méthodologie, Jenkins. Si vous utilisez « devops », buildId et lifecycleStage sont obligatoires.	Chargement demandé par
ID de construction	Une chaîne que le demandeur envoie.	ID de build de la SBOM build.
Étape du cycle de vie	Production ou pre_production	Étape du cycle de vie de l'entité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de demande	Valeurs possibles	Description
fetchVulenrabilityInfo	T/F	Si vrai, déclenche l'intégration de Vulnerability Intelligence.
Informations sur fetchPackage	T/F	Si vrai, déclenche l'intégration de l'intelligence des packages.

Réponse de l'API de chargement : inclusion de la réussite/de l'échec « status », « message » (chaîne), « bomRecordId » (il s'agit de l'ID système de la nomenclature logicielle qui est renvoyé via l'API de chargement pour un chargement de nomenclature logicielle réussi).

```
{

"result": {

"status": "success",

"message": "Queued for processing.",

"bomRecordId": "f207059b4393c290629aa597cbb8f247"

}

}
```

API d'état

Cette API obtient l'état et le résumé d'une SBOM qui est en file d'attente pour l'ingestion.

- URL D'API : */API/SBOM/CORE/UPLOAD/STATUS*
- Méthode HTTP (GET)

Paramètres de demande	Valeurs possibles	Description
bomRecordId	ID système	ID d'enregistrement SBOM renvoyé via l'API de chargement pour un chargement SBOM réussi.

Exemple de réponse par défaut de l'API d'état.

```
{
  "result": {
    "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
    "uploadStatus": "processed",
    "additionalInfoStatus": "not_requested",
    "uploadSummary": {
      "components": {
        "added": 0,
        "removed": 0,
        "total": 70
      }
    }
  }
}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse d'API d'état avec exemple de paramètres supplémentaires. Si vous avez demandé fetchVulenrabilityInfo pour ce SBOM, vous obtenez la répartition des vulnérabilités dans le cadre de la réponse.


```
{
 "result": {
  "bomRecordId": "93af349b4393c290629aa597cbb8f258",
  "uploadStatus": "processed",
  "additionalInfoStatus": "complete",
  "uploadSummary": {
    "components": {
     "added": 0,
     "removed": 0,
     "total": 3
   },
   "vulnerabilityInfo": {
    "critical": 0,
    "high": 0,
    "medium": 0,
    "low": 0,
    "none": 0
   }
  },
  "buildId": "1"
 }
}
```


Si vous avez demandé fetchPackageInfo pour ce SBOM, vous obtenez des nombres périmés et abandonnés dans le cadre de la réponse.

Une fois qu'un SBOM est traité avec succès, l'endroit où vous affichez les enregistrements chargés dépend des applications que vous utilisez.

- Si vous utilisez SBOM Réponse, l'enregistrement d'entité BOM s'affiche dans la liste État d'ingestion SBOM du module File d'attente BOM de l'espace SBOM de travail.
- Si vous utilisez SBOM Core, accédez à **SBOM principal** > **État de l'ingestion BOM**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Améliorations des normes prises en charge SBOM et des informations générales d'utilisation

La version 4.0 de SBOM Core prend en charge :

- XML et JSON dans CycloneDx (versions 1.0 - 1.6).
- JSON dans SPDX (versions 2.2-2.3)

- **Remarque :** Les fichiers de plus de 32 Mo peuvent ne pas se charger correctement.

À partir de la version 4.0 de SBOM Core, les améliorations suivantes ont été apportées pour prendre en charge les normes CycloneDx pour les versions 1.0 à 1.6 :

- Importez des informations supplémentaires dans des fichiers SBOM CycloneDX avec la propriété (sn_sbom_core.collect_properties). Cette propriété est désactivée par défaut. Activez la propriété pour importer des informations qui ne sont généralement pas prises en charge. Toutes les informations importées à partir de ces propriétés sont téléchargées dans la table Propriété du composant SBOM [sn_sbom_comp_property] pour ce qui suit :
  - Fichiers SBOM chargés
  - Métadonnées
  - Vulnérabilités individuelles
  - Composants
- Affichez les données de composant importées pour les licences déclarées et conclues pour les fichiers SBOM dans les versions 1.4 et ultérieures de CycloneDX dans deux nouveaux champs de licence :
  - **Déclaré**
  - **Conclu**
- La prise en charge de l'analyse SBOM est étendue aux types de composants CycloneDX suivants :
  - Version 1.5 : plateforme, données, pilote d'appareil, modèle d'apprentissage machine
  - Version 1.6 : Cryptographique

La version 3.0 de SBOM Core prend en charge :

- XML et JSON dans CycloneDx (jusqu'à la version 1.4 incluse).
- JSON dans SPDX (jusqu'à la version 2.3 incluse).

Si l'utilisateur appelant est authentifié avec succès et qu'il dispose du rôle sn_sbom_core.sbom_ingest dans votre ServiceNow instance, vous pouvez accéder à l'API depuis l'extérieur de votre instance pour charger les SBOM données.

Une fois les données chargées, elles sont analysées. Avant d'analyser les données, les exigences suivantes sont vérifiées :

- La validité des données entrantes est vérifiée au format JSON ou XML.
- Le format BOM est pris en charge. À partir de la version 2.1 de SBOM Core, les formats CycloneDX (JSON et XML) et SPDX (XML) sont pris en charge.
- Les champs minimaux sont disponibles afin que les données puissent être analysées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois ces vérifications vérifiées, une entrée est effectuée dans la table Nomenclature [sn_sbom_doc] avec les données entrantes SBOM en pièce jointe.

La *`Process BOM file`* règle métier est déclenchée automatiquement suite à l'insertion de l'enregistrement et à l'analyse des données.

Remarque : Cette règle métier est activée lors de l'installation de SBOM Core par défaut.

Tous les composants répertoriés dans un SBOM ont un type défini.

- Les composants pour lesquels SBOM des fichiers ont été chargés sont considérés comme des entités BOM.
- Les composants répertoriés comme type=library sont considérés comme des composants tiers.

Information associée

Afficher l'état de chargement des Nomenclature logicielle fichiers

Afficher des rapports et des tableaux de bord dans l'espace de Nomenclature logicielle travail

Télécharger Nomenclature logicielle des fichiers manuellement

Chargez Nomenclature logicielle des fichiers (SBOM) manuellement.

Avant de commencer

À partir de la version 4.0, SBOM Core prend en charge :

- XML et JSON dans les versions 1.0 - 1.6 de CycloneDX.
- JSON dans les versions 2.2 et 2.3 de SPDX.

Rôle requis : sn_sbom_core.sbom_ingest

Procédure

1. Télécharger des fichiers manuellement.

La méthode que vous utilisez pour télécharger vos fichiers varie selon que vous avez installé les SBOM applications Core ou SBOM Response.

Option	Description
Si vous avez installé SBOM Core	**a.** Accédez à la **SBOM principal** > **État de l'in gestion BOM**. **b.** Dans la liste Nomenclature, sélectionnez **Nouveau**. **c.** Sélectionnez le lien **Cliquer pour ajouter** . Vous pouvez charger un fichier à la SBOM fois. **d.** Sélectionnez **Choisir un fichier** et locali–sez le fichier souhaité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Le nom du fichier s'affiche sur la page Choisir une pièce jointe. **e.** Sélectionnez **OK**.
Si vous avez installé SBOM Réponse commençant par la version v4.0	**a.** Accédez à la **Tous** > **Espaces de travail** > **Espace de travail SBOM** > **File d'attente BOM**. **b.** Sélectionnez **Charger BOM**. Le modal Charger un fichier SBOM s'affiche. **c.** Sélectionnez le lien **Joindre un fichier** . **d.** Localisez le fichier que vous voulez et sélectionnez **Ouvrir**. Une fois votre fichier chargé, un lien vers le fichier s'affiche avec trois icônes qui vous offrent les options suivantes : ▪ Télécharger le fichier. ▪ Modifiez le nom du fichier. ▪ Supprimez le fichier du chargement. **e.** Sélectionnez **Charger** pour continuer. Vous pouvez charger un fichier à la SBOM fois. **f.** (Facultatif) Sélectionnez une application d'entreprise et un modèle de produit dans les listes. Ces valeurs vous aident à associer ceci SBOM à une application d'entreprise ou à un modèle de produit dans votre organisation. Ces informations sont affichées dans l'enregistrement de l'entité BOM après le chargement. **g.** Sélectionnez **Charger**. La page de file d'attente BOM s'affiche et le fichier est répertorié dans la section d'ingestion SBOM avec l'état de chargement d'autres informations sur le fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. **Facultatif :** Chargez SBOM les fichiers importés par le Veracode Vulnerability Integration.

> **Remarque :** Vous pouvez télécharger Veracode des fichiers aux formats CycloneDX (JSON et XML) et SPDX (XML) uniquement si vous avez installé et activé l'intégration Veracode avec Réponse aux vulnérabilités des applications. Voir le pour plus d'informations Veracode Vulnerability Integration .

Résultats

Une fois qu'un SBOM est traité avec succès, l'endroit où vous affichez l'état du chargement dépend des applications que vous utilisez.

- Si vous utilisez SBOM Réponse, l'enregistrement de l'entité BOM s'affiche dans la liste État d'ingestion SBOM du module File d'attente BOM de l'espace SBOM de travail.
- Si vous utilisez SBOM Core, accédez à **SBOM principal** > **État de l'ingestion BOM**.

Information associée

Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API

Chargement des Nomenclature logicielle fichiers DevOps SBOM

Générez et chargez des Nomenclature logicielle SBOM fichiers pour les logiciels tout au long de leurs cycles de développement d'intégration et de déploiement continus.

DevOps et SBOM les fichiers

SBOM Les fichiers peuvent être générés à plusieurs étapes tout au long du cycle de vie du développement de l'intégration et du déploiement continus du logiciel (CI/CD). La plupart des opérations de développement logiciel (DevOps) dans les organisations utilisent un type de processus CI/CD pour les aider à identifier et à prévenir les bogues coûteux qui pourraient apparaître après la publication. Tout au long du pipeline CI/CD, DevOps peut générer des fichiers SBOM et rechercher de manière proactive les vulnérabilités et les composants à risque. Ces vérifications peuvent aider les organisations à améliorer la qualité des logiciels et à éviter une maintenance coûteuse par la suite. La génération de SBOM fichiers est essentielle pour implémenter et automatiser avec succès des évaluations de version précises pendant le développement du CI/CD.

Le chargement de fichiers SBOM à partir de pipelines de développement est pris en charge à partir des versions suivantes des SBOM applications.

Versions prises en charge

Application	Versions prises en charge
Modèle de données pour SBOM	v3.0, v2.0
SBOM Core	v5.0, v4.0, v3.0
SBOM Réponse	v5.0, v4.0, v3.2, 3.1

Cas d'utilisation

La génération SBOM de fichiers et leur envoi via l'API de chargement SBOM dans le cadre du pipeline de version DevOps peuvent fournir des nombres pour les éléments suivants afin de déterminer si le pipeline doit réussir ou échouer :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Composants ajoutés
- Composants supprimés
- Informations sur les vulnérabilités
- Informations sur le package (composants abandonnés/périmés)

Les politiques DevOps et les règles relatives à la réussite ou à l'échec d'un pipeline peuvent être définies par le nombre de vulnérabilités et les seuils de nombre de composants périmés et abandonnés reçus de l'API SBOM État.

Pour un pipeline défaillant, les utilisateurs DevOps peuvent accéder aux informations sur la version ayant échoué dans leur ServiceNow® instance afin de mieux comprendre la cause première et l'origine des vulnérabilités.

Pour Chargement de Nomenclature logicielle fichiers à l'aide d'une REST API plus d'informations sur les paramètres et les URL (POST) et (GET), reportez-vous aux API de chargement et d'état.

Séparation en domaines

Toutes les tables des applications SBOM sont séparées par domaine.

Classification des licences et résolution des licences de composants dans l'espace de Nomenclature logicielle travail

Classez les licences et résolvez-les (associez-les) à des composants, ou créez des licences dans le module Administration de licences de l'espace SBOM de travail. La classification et l'association des licences à vos composants vous permettent de déterminer la conformité de votre licence pour les composants logiciels propriétaires, open source et fournis par le fournisseur que vous chargez dans vos SBOM fichiers.

Données de licence et logiciels tiers

Au fur et à mesure que les organisations construisent davantage leurs propres applications logicielles, elles utilisent des composants open source et des logiciels fournis par des fournisseurs. L'utilisation de composants tiers et open source vous offre de nombreux avantages pour la création et la publication rapides de vos projets logiciels, cependant, l'utilisation de ces composants comporte des risques de licence :

- Les composants logiciels open source et fournis par les fournisseurs ont parfois des dépendances à d'autres composants, et chaque composant peut avoir ses propres exigences en matière de licence.
- Si vous ne respectez pas les termes de vos licences pour les composants et les logiciels de vos applications, vous risquez de diffuser par inadvertance du code qui enfreint vos politiques internes et vos exigences réglementaires en matière de gestion des licences.

Module Administration de licences

Le module Administration de licence de l'espace de travail SBOM vous permet d'effectuer les tâches suivantes.

- Classez les licences qui l'exigent pour les composants que vous chargez avec vos SBOM fichiers.
- Résolvez chaque licence que vous classifiez en un composant spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Voyez quel pourcentage des composants que vous utilisez ne sont pas conformes sur une visualisation de données sur la page d'accueil. Vous pouvez utiliser ces informations pour vous aider à déterminer votre posture de sécurité globale et l'exposition potentielle aux risques.

Si les SBOM fichiers que vous chargez incluent des informations de licence, la base de données de licences s'agrandit automatiquement au fur et à mesure que des licences uniques sont observées sur chaque chargement SBOM. Avec chaque chargement SBOM, vous pouvez créer une base de données de licences téléchargées, puis les classer si nécessaire avec le module Administration de licences de l'espace SBOM de travail. Vous créez un inventaire des licences afin de pouvoir les affecter à des composants après les avoir classés dans l'une des catégories suivantes :

- Autorisé
- Restreint
- Interdit
- Non classifié

Le personnel juridique, les gestionnaires de licences, les responsables de la conformité et les responsables de la réglementation effectuent des tâches dans le module Administration de licences.

Affichage des données de licence chargées

Vous disposez des options suivantes pour afficher toutes les informations de licence que vous avez téléchargées avec vos composants dans l'espace de travail SBOM.

- Accédez à la **Espaces de travail** > **Espace de travail SBOM** > **Composants**.

  Sur la page Composants, la carte Classification de licence des composants affiche une visualisation de la conformité globale de votre licence avec les catégories suivantes.

Catégorie	Description
Interdit	L'utilisation sous licence n'est pas autorisée.
Classification requise	La licence n'est pas encore classifiée et nécessite un examen.
Autorisé	L'utilisation sous licence est autorisée sans restriction.
Restreint	L'utilisation sous licence n'est pas autorisée dans des cas d'utilisation spécifiques.

  Cet instantané utilise les classifications et les informations de licence résolues que vous entrez dans le module Administration de licences pour calculer la conformité globale de votre licence.

  Si vous sélectionnez un enregistrement de composant dans cette liste, vous pouvez afficher les informations de licence du composant ainsi que d'autres informations dans le champ État.

- Vous pouvez également accéder à **Espaces de travail** > **Espace de travail SBOM** > **Administration de licences** > **Classification de licence**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette page suit le nombre total de licences uniques qui ont été détectées à partir des fichiers SBOM que vous avez chargés. Il les filtre également dans des cartes en haut de la page dans les catégories suivantes.

- Non classifié : la licence nécessite un examen et une classification.
- Interdit : l'utilisation de la licence n'est pas autorisée.
- Restreint : la licence n'est pas autorisée dans des cas d'utilisation spécifiques.
- Autorisé : l'utilisation de la licence est autorisée sans restriction.
- Toutes les licences : nombre total de licences.

Tous les composants de votre organisation utilisent l'une des licences répertoriées sur cette page. Lorsqu'une nouvelle licence est détectée à partir d'un chargement SBOM, un enregistrement est créé et stocké dans la table Licence SBOM [sn_sbom_license] et ajouté à cette liste. Sa classification par défaut est **Classification requise**. Les enregistrements de licence dans cet état doivent être examinés et classés avant de pouvoir les résoudre (les associer) aux composants afin que la conformité globale de votre licence soit calculée avec précision.

Pour plus d'informations sur la classification des licences, reportez-vous à la section Classer les licences importées dans l'espace de Nomenclature logicielle travail.

Rôles

Les nouvelles licences doivent être classées par un utilisateur disposant du rôle sn_sbom_response.managelicense. Cet utilisateur consulte les informations de licence téléchargées et détermine quelles licences sont autorisées et lesquelles sont interdites. Les utilisateurs disposant de ce rôle ne peuvent pas afficher le module de résolution de licence de composant à moins d'avoir le rôle sn_sbom_response.licenseresolver.

Après la classification, les licences doivent être résolues par un utilisateur disposant du rôle sn_sbom_response.licenseresolver afin que la conformité globale de votre licence puisse être déterminée. Cet utilisateur résout les licences en composants. Les utilisateurs disposant de ce rôle ne peuvent pas afficher le module de classification de licence à moins d'avoir le rôle sn_sbom_response.managelicense.

La classification des nouvelles informations de licence est un processus continu. Vous préférerez peut-être garder le nombre total affiché sur la carte Non classé bas. En tant que gestionnaire de licences, vous préférerez peut-être rechercher les licences qui doivent être classées tous les quelques jours et après avoir chargé des fichiers SBOM.

En tant que résolveur de licences, vous préférerez peut-être vérifier les licences classifiées mises à jour tous les quelques jours.

Classer les licences importées dans l'espace de Nomenclature logicielle travail

Classez les licences de composants que vous chargez avec vos fichiers avec la SBOM fonctionnalité Classification de licence.

Avant de commencer

La classification des nouvelles informations de licence est un processus continu. Vous préférerez peut-être garder le nombre total affiché sur la carte Non classé bas. En tant que gestionnaire de licences, vous préférerez peut-être rechercher les licences qui doivent être classées tous les quelques jours et après avoir chargé des fichiers SBOM.

Rôle requis : sn_sbom_response.managelicense

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail SBOM** > **Administration de licences** > **Classification de licence**.

   Remarque : À moins que vous ne disposiez également du rôle sn_sbom_response.licenseresolver, seul l'onglet Classification de licence est visible.

2. **Facultatif :** Sélectionnez une carte pour filtrer les licences en fonction de leurs classifications.
3. Pour classer les licences, choisissez-en une.

Option	Description
Modifier des enregistrements en bloc ou modifier plusieurs enregistrements dans la liste.	**a.** Sélectionnez plusieurs enregistrements. **b.** Double-cliquez sur l'en-tête de la colonne Classification (Classification). **c.** Mettez à jour la classification.
Modifier et mettre à jour la classification dans l'enregistrement.	**a.** Sélectionnez un enregistrement dans la liste pour l'ouvrir. **b.** Ajoutez des notes de travail et des pièces jointes, si nécessaire. **c.** Sélectionnez **Enregistrer**.

4. Une fois que vous avez classifié les licences, vous êtes prêt à résoudre les licences classifiées en composants.

Résoudre les licences en composants dans l'espace de Nomenclature logicielle travail

Résolvez (affectez) des licences classifiées à des composants spécifiques avec la fonctionnalité Résolution de licence de composant. Attribuez des licences aux composants dont les informations de licence sont manquantes ou incorrectes ou créez de nouvelles licences afin de pouvoir calculer la conformité globale de votre licence.

Avant de commencer

Rôle requis : sn_sbom_response.licenseresolver

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail SBOM** > **Administration de licences** > **Résolution de la licence du composant**.

   Remarque : À moins que vous ne disposiez également du rôle sn_sbom_response.managelicense, seul l'onglet Résolution de la licence du composant est visible.

   Cette page suit le nombre total de licences uniques et une vue d'un coup d'œil des totaux de licences qui ont été détectés à partir des fichiers SBOM que vous avez chargés. Les licences affichées sur cette page se répartissent en deux grandes catégories en ce qui concerne les composants.

   - Toutes les instances du composant conviennent d'une licence.
   - Il y a un désaccord sur une licence unique et il existe plusieurs licences pour un composant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le second cas, vous devez rapprocher ces licences afin qu'une seule licence soit résolue en un seul composant. La conformité des licences est calculée sur la base d'une licence résolue par composant.

Les licences sur cette page sont filtrées dans les catégories suivantes pour vous aider à les résoudre.

Valeur	Description
Composants avec des licences non résolues	Aucune licence n'est affectée au composant et cela nécessite une résolution. (vide) s'affiche dans la colonne Licence résolue pour ces composants. Les totaux de licences manquantes et multiples sont répertoriés dans cette catégorie.
Composants avec des licences manquantes.	Composants pour lesquels il manque des informations de licence qui nécessitent une résolution.
Composants avec plusieurs licences	Composants visibles dans plusieurs entités qui ont des licences différentes et nécessitent une résolution.
Tous les composants	Liste totale des composants suivis dans votre organisation. Vous pouvez changer les licences de cette liste filtrée.

2. Sélectionnez une carte.
3. Choisissez-en un pour résoudre une licence.

Option	Description
Affecter une licence existante à un composant.	**a.** Double-cliquez sur un champ de la colonne Licence résolue pour un composant. **b.** Sélectionnez une licence dans la liste des licences résolues. **c.** Votre modification est enregistrée et la carte associée en haut est mise à jour. **d.** Vous pouvez également sélectionner l'enregistrement dans la colonne Nom pour l'ouvrir. Il s'ouvre dans un nouvel onglet. **e.** Cliquez sur l'onglet **Entités BOM** pour voir où le composant est utilisé. **f.** Sélectionnez-en un dans la liste des licences résolues. **g.** Entrez une justification. **h.** Sélectionnez **Enregistrer**. **i.** Actualisez la page pour la mettre à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Modifiez une licence pour un composant qui en possède déjà une.	Vous pouvez choisir cette option si vous déterminez qu'une licence a été affectée de manière incorrecte à un composant ou doit être modifiée. **a.** Sélectionnez la carte **Tous les compo sants** . **b.** Localisez le composant que vous souhai–tez modifier. **c.** Sélectionnez l'enregistrement dans la liste pour l'ouvrir. **d.** Sélectionnez-en un dans la liste des li–cences résolues. **e.** Sélectionnez **Enregistrer**. **f.** Actualisez la page pour la mettre à jour.
Créez une licence.	Vous pouvez utiliser cette option si vous savez qu'une licence spécifique est utilisée dans votre or-ganisation, mais qu'aucun enregistrement n'a été dé-tecté lors d'un chargement précédent SBOM et qu'il n'existe aucun enregistrement répertorié dans le mo-dule Classification de licence. **a.** Sélectionnez **Nouveau** dans l'onglet Classification de licence et renseignez les champs. **b.** Nom : nom unique de cette licence. **Remarque :** Le nom d'affichage est basé sur le champ ID. Si le champ ID n'est pas défini, le nom d'affichage est basé sur le champ Nom. Si le champ Nom n'est pas défini, le nom d'affichage est basé sur le champ Expression. **c.** Classification. Sélectionnez l'une des op–tions : ▪ Non classifié : la licence nécessite un examen et une classification. ▪ Interdit : l'utilisation de la licence n'est pas autorisée. ▪ Restreint : la licence n'est pas auto–risée dans des cas d'utilisation spéci–fiques. ▪ Autorisé : l'utilisation de la licence est autorisée sans restriction. **d.** Type de licence. Ces informations ne sont pas utilisées par le système ou pour un workflow. Ces informations vous sont fournies pour vous aider à stocker des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	informations supplémentaires et à classer vos licences. **e.** URL : site web pour la source de la licence. Elle n'est pas utilisée par un workflow ou un système. **f.** Expression : Combiner arithmétiquement des licences. Par exemple, MIT ET Apache-2.0 WITH GPL-2.1-or-later sont combinés pour une expression. Les combinaisons ou expressions de licence sont traitées comme une seule licence dans le .ServiceNow AI Platform **g.** Pièces jointes. Ajouter une pièce jointe ou des notes de travail. **h.** Sélectionnez **Enregistrer**. Cette licence est ajoutée à votre base de données, est affichée sur la page Classification de licence et peut maintenant être détectée sur les composants lors SBOM des téléchargements.
Chargez plusieurs licences et classifications.	Vous pouvez choisir cette option si vous avez un fichier avec plusieurs licences et classifications pour lesquelles vous souhaitez créer des enregistrements. Vous pouvez charger des fichiers dans le format spécifié et les stocker dans la table de licence SBOM [sn_sbom_license]. **a.** Accédez à la table de SBOM licence [sn_sbom_license]. **b.** Sélectionnez le menu **Autres options** dans n'importe quelle colonne. **c.** Sélectionnez **Importer**. Sur la page qui s'affiche, chargez un modèle compatible existant ou téléchargez le modèle généré par la plateforme (**Créer un modèle Excel**). Vous chargez les données dans ce modèle qui est inséré dans la table. **d. Choisissez un fichier** et localisez-le. **e.** Sélectionnez **Charger**. Votre fichier est téléchargé et les enregistrements sont créés dans la table de licence SBOM [sn_sbom_license] et consultables dans l'espace de SBOM travail sur la page Classification de licence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Accédez à la page d'accueil dans l'espace de travail SBOM pour voir quel pourcentage des composants que vous utilisez ne sont pas conformes dans la visualisation de la classification de licence des composants. Les données de cette visualisation sont mises à jour quotidiennement par la tâche planifiée Répartition des licences des composants BOM. Cette tâche fait partie de la tâche planifiée du collecteur de données des rapports SBOM qui s'exécute quotidiennement.

Afficher des rapports et des tableaux de bord dans l'espace de Nomenclature logicielle travail

Les analystes de vulnérabilité consultent les fichiers de nomenclature logicielle chargés dans les enregistrements, les visualisations de données, ainsi que les renseignements améliorés sur les vulnérabilités dans l'espace Nomenclature logicielle de travail (SBOM).

SBOM Core

Vous pouvez afficher les entités BOM et la liste des composants que vous avez chargés sur la page d'accueil (de destination) et dans le module Composants de l'espace SBOM de travail.

SBOM Réponse

L'application SBOM Réponse vous fournit des visualisations de données avec des informations détaillées sur les entités BOM, les entités présentant des vulnérabilités et les éléments vulnérables de l'application actifs sur la page d'accueil (de destination) de l'espace SBOM de travail. L'espace de travail avec SBOM réponse comprend les modules suivants :

- Page d'accueil : visualisations de données et détails améliorés sur les vulnérabilités.
- Composants : informations sur la version et le correctif des composants et classification de licence des composants.
- Règles de création AVIT (élément vulnérable de l'application) : conditions de création des éléments vulnérables de l'application (AVIT).
- File d'attente BOM : statut et historique du chargement du fichier.
- Liste : enregistrements AVIT pour vos composants et bibliothèques vulnérables (vulnérabilités NVD, CWE et vulnérabilités d'application).

Les rubriques suivantes fournissent plus d'informations sur la façon de localiser les détails de vos composants dans l'espace de Nomenclature logicielle travail.

- Examiner la page d'accueil dans l'espace de Nomenclature logicielle travail
- Examen du module Composants dans l'espace de Nomenclature logicielle travail
- Afficher l'état de chargement des Nomenclature logicielle fichiers
- Vérification des vulnérabilités d'une Nomenclature logicielle entité
- Classification des licences et résolution des licences de composants dans l'espace de Nomenclature logicielle travail

Examiner la page d'accueil dans l'espace de Nomenclature logicielle travail

Les données chargées sont déployées sur les visualisations de la page de destination (accueil) dans l'espace Nomenclature logicielle de travail (SBOM). Les données sont modifiées après le chargement des fichiers afin que les analystes de vulnérabilité puissent voir les tendances et examiner les informations actuelles sur vos composants.

Avant de commencer
Rôles requis : sn_sbom_resp.sbom_analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail SBOM**.
   Par défaut, la page de destination (accueil) s'affiche.

   Ce que vous pouvez voir dans le module dépend des applications que vous avez installées.

   Les données importées ne sont pas calculées et renseignées par des requêtes en direct. Les scores des pages Accueil et Composants sont mis à jour une fois par jour avec des améliorations des performances pour le reporting. Cette amélioration peut vous fournir des temps de chargement plus rapides pour les tableaux de résultats sur les modules Accueil et Composants de l'espace SBOM de travail.

   Ces améliorations n'ont aucun impact sur la façon dont les données sont stockées ni sur l'endroit où elles sont stockées.

Application installée	Description
Si vous avez installé SBOM Core	Toutes les entités BOM. La liste comprend le nom, le classifieur (application, conteneur, bibliothèque, etc.) et le nombre de composants de chaque entité. Une entité BOM fait référence au composant de niveau racine d'un SBOM fichier pour lequel un SBOM document a été généré et téléchargé. Accédez à la page d'accueil dans l'espace de travail pour afficher la liste des entités BOM.
Si vous avez installé SBOM Réponse	Les visualisations de données suivantes s'affichent. ○ Toutes les entités BOM : répartition des entités BOM par type : application, conteneur, bibliothèque et autres. Une entité BOM fait référence au composant de niveau racine d'un SBOM fichier pour lequel un SBOM document a été généré et téléchargé. ○ Entités BOM avec vulnérabilités : entités dont une vulnérabilité est associée à un composant dont elles dépendent. Si une dépendance d'entité a une vulnérabilité **critique** , la gravité de l'entité est considérée comme critique. ○ AVI actifs : tendance du nombre d'éléments vulnérables de l'application (AVI) créés chaque jour. Les visualisations de données affichent les données des 30 derniers jours. La plage de 30 jours n'est pas modifiable. Ces données sont disponibles après avoir examiné et configuré les règles de création des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application installée	Description
	éléments vulnérables de l'application. Pour plus d'informations, consultez Création de règles pour les éléments vulnérables de l'application dans l'espace de Nomenclature logicielle travail.

2. Sélectionnez une carte de visualisation de données pour afficher sa liste d'enregistrements.
3. Sélectionnez l'onglet **Accueil** pour revenir à la page de destination.
4. Vous pouvez également sélectionner un enregistrement sous la liste **Entités BOM** .

   Le nom et la version de l'entité sont affichés en haut de l'enregistrement, par exemple, SNC-SECOPS-SIR2.0.

   Remarque : Avec le module Administration de licences, la relation entité-licence n'est pas affichée sur cette liste. Pour afficher les entités dans lesquelles un composant est utilisé, accédez au module Composants et ouvrez un enregistrement de composant. Sur l'enregistrement du composant, vous pouvez afficher l'état : non résolu ou non classifié.

5. Sélectionnez les onglets de l'enregistrement d'entité pour examiner les données.

   a. Si elle est décochée, sélectionnez l'onglet **Vue d'ensemble** .

   Examinez les données. Si un champ n'est pas renseigné sur cet enregistrement, les données n'ont pas été incluses dans les SBOM fichiers que vous avez chargés.

Nom	Description
Nom	Nom de l'entité.
Classifieur	Type d'entité, par exemple, une application, un composant ou une bibliothèque.
Version	Numéro de version de l'entité.
Fournisseur	Produit qui a fourni l'entité.
Modèle de produit	S'il n'existe aucun modèle de produit existant ou si vous n'en incluez pas un au moment de votre SBOM chargement via l'API, un modèle est créé. Le nom de l'entité est utilisé pour l'enregistrement du modèle de produit, par exemple SNC-SECOPS-SIR2.0.

   b. Sélectionnez l'onglet **Dépend de** .

   Toutes les dépendances de cette entité sont répertoriées, ainsi que les classificateurs, par exemple, Library. Le numéro de version, les licences et d'autres informations s'affichent.

   La sélection d'un lien dans cette liste ouvre un enregistrement. Son onglet s'affiche sous les onglets Accueil et Enregistrement d'entité. L'enregistrement que vous ouvrez peut inclure les listes connexes suivantes que vous pouvez passer en revue : vue d'ensemble, hachages, entités BOM, vulnérabilités et éléments vulnérables de l'application (AVIT).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La liste connexe Entités BOM affiche toutes les entités dans lesquelles cet élément affiché est utilisé.

c. Sélectionnez l'onglet **Vulnérabilités** pour voir les vulnérabilités associées à une dépendance de cette entité.

Pour plus d'informations sur les vulnérabilités affichées pour une entité, reportez-vous à la section Afficher l'état de chargement des Nomenclature logicielle fichiers.

d. Sélectionnez l'onglet **AVI** pour voir s'il existe des éléments vulnérables d'application pour cette entité.

6. Facultatif : Après avoir examiné les enregistrements, vous pouvez supprimer un ou plusieurs enregistrements d'entité BOM si vous déterminez que vous n'en avez plus besoin.

Remarque : La suppression des enregistrements d'entité BOM les supprime définitivement, ainsi que les relations qui les composent. Tous les éléments vulnérables de l'application (AVIT) associés aux entités BOM passent à **l'état Fermé**. Si vous décidez ultérieurement que vous souhaitez que les enregistrements et les relations de composant que vous supprimez figurent à nouveau dans la liste des entités BOM et soient disponibles dans l'espace de travail, vous devez charger à nouveau ces entités BOM.

a. Si vous n'êtes pas sur la page d'accueil, sélectionnez l'onglet **Accueil** pour y revenir.

b. Sélectionnez le ou les enregistrements de la liste **Entités BOM** que vous souhaitez supprimer.

c. Sélectionnez **Supprimer**.

Examen du module Composants dans l'espace de Nomenclature logicielle travail

Le module Composants de l'espace Nomenclature logicielle de travail (SBOM) affiche les informations actuelles sur les combinaisons vulnérables, périmées, abandonnées et à haut risque pour les composants que vous importez.

Affichage du module Composants

Rôle requis : sn_sbom_resp.sbom_analyst

Accédez à la **Espaces de travail** > **Espace de travail SBOM** > **Composants**.

Ce que vous pouvez voir dans le module dépend des applications que vous avez installées.

Les données importées ne sont pas calculées et renseignées par des requêtes en direct. Les scores des pages Accueil et Composants sont mis à jour une fois par jour avec des améliorations des performances pour le reporting. Cette amélioration peut vous fournir des temps de chargement plus rapides pour les tableaux de résultats sur les modules Accueil et Composants de l'espace SBOM de travail.

Ces améliorations n'ont aucun impact sur la façon dont les données sont stockées ni sur l'endroit où elles sont stockées.

Application installée	Description
Si vous avez installé SBOM Core	Un inventaire de tous les composants chargés qui comprend les informations suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application installée	Description
	• Nom • Description • Version • Nombre d'entités BOM
Si vous avez installé SBOM Réponse	Sélectionnez un graphique ou un nombre sur le graphique pour afficher une liste des enregistrements associés. **Tous les composants** La liste des composants **périmés** et **abandonnés** , ainsi que ceux ayant au moins une vulnérabilité dans votre nombre total de composants. Ces dénombrements peuvent vous aider à identifier les composants qui nécessitent votre attention. Ces sous-ensembles de composants peuvent ne pas correspondre à votre nombre total de composants, car tous vos composants peuvent ne pas correspondre à ces catégories. • La version d'un composant périmé a plus de deux versions majeures de retard sur la dernière version et deux ans de retard sur la dernière version. • Un composant abandonné n'a pas été mis à jour depuis plus de deux ans. • Les composants vulnérables sont des composants qui présentent des vulnérabilités avec une **gravité élevée ou** supérieure. **Combinaisons à haut risque** Les composants à haut risque peuvent nécessiter votre attention immédiate. L'intégration Deps.dev, qui est installée lorsque vous installez l'application SBOM Response, fournit l'intelligence des packages pour les composants ayant les états **périmé** et **abandonné** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application installée	Description
	Les combinaisons importées à haut risque sont composées de composants périmés et abandonnés présentant au moins une vulnérabilité grave (**critique** ou **élevée**) que vous pouvez corriger par des mises à jour, un remplacement ou un autre type de réparation. Le statut **Entièrement réparable** signifie qu'un composant dispose d'une version disponible qui peut le corriger. Le pourcentage du nombre total de composants à haut risque qui ont des versions réparables est noté. **Réparabilité des composants vulnérables** Totaux et répartitions des composants avec des vulnérabilités **critiques**, **élevées**, **moyennes** et **faibles** et si certaines ou toutes leurs vulnérabilités peuvent être corrigées. Si un composant a plusieurs vulnérabilités, la vulnérabilité la plus critique a priorité. L'état de la réparabilité : • Terminé : il existe des versions de correction pour toutes les vulnérabilités associées à la version actuelle du composant. • Partiel : il existe une version de correctif pour au moins une des vulnérabilités associées à la version actuelle du composant, mais pas toutes. **Classification de licence des composants** Totaux et répartitions des composants par classification de licence. La liste des composants sous les visualisations vous permet d'afficher le nom, la description, la version et le nombre d'entités. Dans le panneau de droite, vous pouvez afficher un historique de version. La version actuelle est mise en surbrillance dans l'historique des versions. Les colonnes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application installée	Description
	Common Vulnerabilities and Exposure (**CVE)** et **Fixability** sont également affichées.

Évaluer votre risque avec la connaissance des vulnérabilités

Consultez Vérification des vulnérabilités d'une Nomenclature logicielle entité pour plus d'informations sur la façon d'examiner les données de renseignement sur les vulnérabilités dans l'espace de travail.

Évaluation de votre risque avec la conformité de licence

Consultez Classification des licences et résolution des licences de composants dans l'espace de Nomenclature logicielle travail pour plus d'informations sur la gestion des licences pour les données que vous importez avec vos composants et pour afficher la conformité globale de votre licence dans l'espace de travail.

Création de règles pour les éléments vulnérables de l'application dans l'espace de Nomenclature logicielle travail

Avant de pouvoir voir les éléments vulnérables de l'application (AVIT) dans l'espace de travail NomenclatureSBOM logicielle, vous devez configurer les conditions de création des AVIT.

AVIT dans l'espace de SBOM travail

Si vous avez installé et activé l'application SBOM Response, les AVIT sont créés pour SBOM les fichiers si l'une des données importées correspond aux conditions de vos règles de création AVIT existantes.

La réponse et Réponse aux vulnérabilités les SBOM applications sont requises pour configurer des règles permettant de créer automatiquement des éléments vulnérables de l'application (AVIT) et de les corriger avec le Réponse aux vulnérabilités des applications workflow. Consultez Explorer Nomenclature logicielle pour plus d'informations.

En tant qu'utilisateur disposant du rôle sn_sbom_resp.manage_avi_rule, vous devez ajouter des règles de création AVIT dans l'espace de SBOM travail avant de pouvoir créer des AVIT pour les vulnérabilités trouvées dans vos données ingérées SBOM . Les AVIT vous permettent d'évaluer l'intégrité des composants tiers dans vos applications. Un AVIT est créé dans votre instance lorsqu'une application est mise en correspondance avec un composant associé à une vulnérabilité.

Dans l'espace SBOM de travail, vous ne pouvez afficher que les AVIT SBOM. Toutefois, vous pouvez afficher SBOM les AVIT ainsi que d'autres types d'éléments vulnérables dans l'espace de travail du gestionnaire de vulnérabilité dans Réponse aux vulnérabilités. Vous pouvez afficher tous les AVIT qui ont été créés dans l'espace de travail SBOM dans le module Liste. Le module de liste inclut également toutes les entrées NVD et CWE et les vulnérabilités d'application.

Vous pouvez également affecter des AVIT pour la correction en fonction des recommandations de listes de vulnérabilité connues telles que la Base de données de vulnérabilité nationale (NVD). Un travail planifié est déclenché, et si les conditions de vos règles de création correspondent aux données ingérées, des AVIT sont créés.

Vous pouvez suivre et corriger les AVIT en configurant des règles personnalisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consultez la rubrique Créer une règle d'élément vulnérable d'application dans l'espace de Nomenclature logicielle travail pour en savoir plus sur la création d'une règle.

SBOM AVIT dans Espace de travail du gestionnaire de vulnérabilités dans Réponse aux vulnérabilités

Vous pouvez afficher tous SBOM les AVIT créés dans l'espace SBOM de travail si Espace de travail du gestionnaire de vulnérabilités vous y avez accès.

Remarque : Pour afficher uniquement SBOM les AVIT de la liste des éléments vulnérables de l'application dans plutôt Espace de travail du gestionnaire de vulnérabilités que tous les AVIT, définissez la condition **[Source] [is] [SBOM] ET [Type d'analyse] [est] [SBOM-SCA]** sur la table Éléments vulnérables de l'application [sn_vul_app_vulnerable_item]. Pour afficher la table, accédez dans votre instance à **Tout** et saisissez **sn_vul_app_vulnerable_item.list** dans le navigateur de filtre.

Pour plus d'informations sur Vulnerability Manager Workspace, comment afficher les rubriques de visualisation, les efforts de rattrapage des applications et les règles de tâche de rattrapage des applications pour les AVIT configurés à partir de l'application Réponse aux vulnérabilités dans le , reportez-vous à la Espace de travail du gestionnaire de vulnérabilités section Utiliser des rubriques de visualisation dans le Espace de travail du gestionnaire de vulnérabilités.

Les tâches de rattrapage (AVUL) sont créées à partir d'AVIT et affectées automatiquement à des groupes pour rattrapage en fonction de vos règles d'affectation. Pour en savoir plus sur la création de ces règles, consultez les rubriques suivantes :

- Créer ou modifier Réponse aux vulnérabilités des règles d'affectation
- Créer ou modifier des Réponse aux vulnérabilités règles de tâche de rattrapage et Créer un effort de rattrapage dans le Espace de travail du gestionnaire de vulnérabilités.

Réouverture des éléments vulnérables de l'application dans la réponse SBOM

Un élément vulnérable de l'application (AVIT) **fermé** pour un composant avec une vulnérabilité associée est rouvert automatiquement et visible dans l'espace de SBOM travail si les conditions suivantes sont réunies :

- L'AVIT avec la vulnérabilité associée est détecté à nouveau par les analyses de vulnérabilité d'une intégration tierce ou le composant avec la vulnérabilité fait partie d'un chargement ultérieur SBOM .
- Vous n'avez pas désactivé la propriété système Rouvrir les AVIT si détecté (*sn_sbom_resp.reopen_avits_if_detected*). Cette propriété système est activée par défaut.
- Le sous-état de l'AVIT **fermé** n'est pas l'un des suivants : **Contrôle d'atténuation en place**, **Non affecté** ou **Faux positif**. Les AVIT avec ces sous-états ne sont pas rouverts par la propriété système.

Désactivez cette propriété système uniquement si vous ne souhaitez pas que les AVIT **fermés** se rouvrent automatiquement.

Afficher l'état de chargement des Nomenclature logicielle fichiers

Vérifiez l'état de chargement des fichiers de nomenclature logicielle (SBOM) que vous chargez dans le module File d'attente BOM de l'espace Nomenclature logicielle de travail (SBOM). Suivez les fichiers que vous chargez avec succès, votre historique de téléchargement et les erreurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_sbom_resp.sbom_analyst

Procédure

1. Consultez l'état de votre chargement.

La méthode que vous utilisez pour afficher votre état de chargement dépend des applications que vous avez installées.

Option	Description
SBOM Core	**a.** Accédez à la **Tous** > **SBOM principal** > **État de l'ingestion BOM**. **b.** Dans la liste Nomenclature, examinez les colonnes telles que **État**, **Délai de génération BOM** et **Colonnes Créé** pour plus d'informations.
SBOM Réponse	**a.** Accédez à la **Tous** > **Espace de travail SBOM** > **File d'attente BOM**. **b.** Sélectionnez une carte de visualisation pour examiner les détails suivants concernant les catégories de vos fichiers chargés : ▪ Mises à jour BOM au cours des 30 derniers jours : nombre total d'entités BOM téléchargées et analysées avec succès au cours des 30 derniers jours. ▪ Source du chargement : total des fichiers chargés SBOM avec succès et répartition des méthodes utilisées pour les ingérer (API ou manuel). ▪ Erreurs de chargement par catégorie : cinq principales catégories d'erreurs de chargement. Si aucune donnée n'apparaît sur cette visualisation, tous vos SBOM fichiers sont chargés avec succès.

Les informations d'état de la table Nomenclature [sn_sbom_doc_list] et du module File d'attente BOM incluent toutes deux les formats BOM, l'état d'ingestion et l'heure de génération BOM. La colonne État de l'ingestion BOM comprend les états suivants :

- Mis en file d'attente : les SBOM données ont été téléchargées.
- Traitement : les données du composant sont traitées dans le cadre de l'importation.
- Traité : l'ingestion de données a été effectuée avec succès.
- Erreur : une erreur s'est produite pendant le traitement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En plus de l'état de vos fichiers chargés, vous pouvez afficher les listes des composants que vous avez ingérés en sélectionnant un enregistrement d'entité BOM.

2. **Facultatif :** Accédez à plus d'informations sur les erreurs et l'état du chargement en sélectionnant l'icône ⚙ et en ajoutant des champs tels que **Catégorie d'erreur** et **Détails de l'erreur**.

Vérification des vulnérabilités d'une Nomenclature logicielle entité

Déterminez si des vulnérabilités sont associées aux composants dans un fichier chargé Nomenclature logicielle (SBOM).

Les applications suivantes doivent être installées et activées avant de pouvoir visualiser les vulnérabilités et les données de vulnérabilité améliorées :

- SBOM Réponse
- Vulnerability Response Integration avec les tâches NVD et CWE
- Réponse aux vulnérabilités

Consultez Explorer Nomenclature logicielle pour plus d'informations.

Rôle requis : sn_sbom_resp.sbom_analyst

1. Accédez à la **Tous** > **Espace de travail SBOM** > **Composants**.
2. Vous pouvez afficher les informations de vulnérabilité via une visualisation ou un enregistrement de composant.

Fonction de message REST	Actions
Entités BOM avec visualisation des vulnérabilités	Sélectionnez le graphique de visualisation **Entités BOM avec vulnérabilités** . ○ Si des vulnérabilités sont associées à ce composant, les totaux sont affichés dans les colonnes CVE et CWE de la liste. Un composant peut avoir plusieurs vulnérabilités. Si disponible, vous pouvez consulter la colonne Réparabilité de cette liste pour les entrées. ○ Si aucune vulnérabilité n'est associée à ce composant, ces colonnes affichent 0 ou aucune valeur pour le composant. Si les colonnes CVE, CWE et Fixibilty ne sont pas affichées, vous pouvez les ajouter à la page en sélectionnant ⚙ haut à droite de la page et **Modifier les colonnes**. Sélectionnez-les dans la liste des colonnes Disponibles, puis sélectionnez **OK**.
Enregistrement du composant	**a.** Sélectionnez un enregistrement dans la liste sous les visualisations. **b.** Sélectionnez l'onglet **Vulnérabilités** de l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonction de message REST	Actions
	i. Si aucune donnée n'est affichée, aucune vulnérabilité signalée n'est associée à l'enregistrement. ii. Si des données sont affichées, consultez Examen du module Composants dans l'espace de Nomenclature logicielle travail et suivez les étapes du workflow Réponse aux vulnérabilités des applications de rattrapage pour remédier à la vulnérabilité. Pour plus d'informations, consultez Rattrapage des Réponse aux vulnérabilités des applications vulnérabilités.

Évaluer votre risque avec la connaissance des vulnérabilités

Affichez des données de vulnérabilité améliorées plus nombreuses avec SBOM Réponse sur les enregistrements de composants. Les SBOM travaux planifiés de l'application Réponse, Réponse aux vulnérabilités, Intégration de la base de données de vulnérabilité nationale (NVD) et Énumération des faiblesses communes (CWE) décrits dans Applications prises en charge doivent être installés et activés.

1. Sélectionnez la visualisation **Tous les composants** pour afficher la liste des enregistrements associés.
2. Sélectionnez un lien **dans la colonne** Nom pour ouvrir un enregistrement.

   Les états **Périmé**, **Abandonné** et **Vulnérable** sont affichés sous le nom du composant. Un composant peut avoir n'importe quelle combinaison de ces états. Si aucun état n'est affiché, le composant n'est ni périmé, ni abandonné, ni vulnérable.

   Passez en revue la version actuelle et la dernière version publiée. Dans le panneau de droite, vous pouvez afficher un historique de version. La version actuelle est mise en surbrillance dans l'historique des versions et son emplacement dans la liste peut vous donner un aperçu des raisons pour lesquelles un composant est **périmé**, **abandonné** et **vulnérable**. Par exemple, vous pouvez utiliser une ancienne version d'un composant.

3. Sélectionnez les onglets connexes Vue **d'ensemble**, **Hachages**, **Entités BOM**, **Vulnérabilités** et **AVI** de l'enregistrement.
   - Vue d'ensemble : un résumé des détails du composant.
   - Entités BOM : liste des entités associées à ce composant.
   - Hachages : s'ils sont importés, les hachages sont affichés.
   - Vulnérabilités : informations sur les vulnérabilités connues associées à ce composant. Si cette liste est vide, il n'y a aucune vulnérabilité connue.

     Si la liste est remplie, sélectionnez l'onglet pour afficher les ID de vulnérabilité, les résumés et d'autres informations sur les vulnérabilités pour les données CVE (Common Vulnerabilities and Exposures) et Common Weakness Enumeration (CWE) associées à cet enregistrement. Les CVE sont ventilées par gravité, les CWE sont ventilées par la probabilité d'exploitation du composant. Vous pouvez afficher les enregistrements

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de vulnérabilité améliorés dans les Réponse aux vulnérabilités applications ou Réponse aux vulnérabilités des applications en sélectionnant le lien ID de vulnérabilité.

- AVI (AVIT) : éléments vulnérables de l'application associés à ce composant si vous avez créé des règles de création AVIT qui font correspondre le composant à une vulnérabilité connue. L'application Application Vulnerability Response (AVR) associe une vulnérabilité à une application pour créer un enregistrement AVI. Pour plus d'informations, consultez Création de règles pour les éléments vulnérables de l'application dans l'espace de Nomenclature logicielle travail.

Composants installés avec Nomenclature logicielle les applications

Plusieurs types de composants sont installés avec l'activation des applications, notamment les tables, les rôles d'utilisateur et les Nomenclature logicielle travaux planifiés.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
sn_sbom_response.managelicense	Ce rôle est installé avec l'application SBOM Response. Ce rôle vous permet de résoudre les licences de composants.	Aucun
sn_sbom_response.licenseresolver	Ce rôle est installé avec l'application SBOM Response. Ce rôle vous permet d'afficher les informations de licence téléchargées et détermine quelles licences sont autorisées et lesquelles sont interdites.	Aucun
SBOM Écrire [sn_sbom_dm.app_write], SBOM Créer [sn_sbom_dm.app_créer], SBOM Lire [sbom_dm.app_read]	Ces rôles sont installés avec le modèle de données de SBOM l'application. Ils vous permettent de lire, de créer et de modifier des enregistrements dans des SBOM tables.	Aucun
SBOM Principaux ingestions [sn_sbom_core.sbom_ingest] et SBOM administrateur principal [sn_sbom_core.admin]	Ces rôles sont installés avec l'application SBOM principale. Le rôle sn_sbom_core.sbom_ingest	• sn_sbom_dm.app_écriture • sn_sbom_dm.app_créer • sn_ sbom_dm.app_lecture

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	vous permet de charger des nomenclatures logicielles manuellement et via l'API REST. Le rôle sn_sbom_core.admin vous permet de créer, lire, modifier des données et charger des nomenclatures logicielles. Ce rôle vous donne également accès aux SBOM modules principaux de votre instance. Elle hérite des rôles du modèle de données pour SBOM l'application.	
Analyste SBOM [sn_sbom_resp.sbom_analyst]	Ce rôle est installé avec l'application SBOM Response. Il hérite du rôle sn_sbom_core.admin et vous permet d'accéder à l'espace de SBOM travail.	• sn_sbom_core.admin • sn_sbom_dm.app_écriture • sn_sbom_dm.app_créer • sn_ sbom_dm.app_lecture • sn_sbom_resp.manage_avi_rule • sn_sbom_config_rule table

Tables installées avec les SBOM applications

Les tables répertoriées dans le tableau suivant sont installées avec le modèle de données de SBOM l'application.

Modèle de données pour SBOM les tables

Table	Description
Document SBOM [sn_sbom_doc]	Contient les entités BOM que vous avez téléchargées.
SBOM composant [sn_sbom_component]	Contient les composants, classifieurs et versions importés SBOM qui sont inclus dans le composant parent.
SBOM Relation de composant [sn_sbom_comp_relationship]	Contient des composants et leurs dépendances.
SBOM Composant BOM M2M	Contient les mappages des composants BOM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modèle de données pour SBOM les tables (suite)

Table	Description
[sn_sbom_m2m_bom_comp]	
Licence SBOM [sn_sbom_license]	Contient les ID de licence open source utilisés pour les composants.
SBOM fournisseur [sn_sbom_supplier]	Contient l'organisation qui a fourni le composant, qui peut être un fabricant, un distributeur ou un reconditionneur.
SBOM ID de composant [sn_sbom_comp_id]	Contient les identificateurs de composants.
SBOM Propriétés des composants [sn_sbom_comp_property]	Contient les propriétés nom-valeur du composant.
SBOM hachis [sn_sbom_hash]	Contient des algorithmes de hachage de composants.
SBOM contact [sn_sbom_contact]	Contient les coordonnées du fournisseur.
SBOM Références externes [sn_sbom_comp_external_ref]	Contient des composants, des types de composants et des URL externes qui documentent les systèmes, les sites et les informations qui peuvent être pertinents mais qui ne sont pas inclus dans le SBOM.
SBOM Groupe de packages [sn_sbom_pkg_group]	Contient les informations sur le groupe de packages pour chaque composant. Plusieurs versions des bibliothèques peuvent être utilisées dans les applications. Les versions des mêmes composants sont regroupées et ajoutées à cette table pour éviter d'extraire les mêmes données plusieurs fois.

Les tables répertoriées dans la table suivante sont installées avec l'application SBOM Response

SBOM Tables de réponses

Table	Description
SBOM Configuration de la règle de création [sn_sbom_config_rule]	Contient les règles de création AVIT utilisées dans l'espace de SBOM travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

SBOM Tables de réponses (suite)

Table	Description
SBOM Vulnérabilités du composant M2M [sn_sbom_m2m_comp_vuln]	Contient les composants et les vulnérabilités associées.
Informations sur le correctif de vulnérabilité du composant [sn_sbom_comp_vuln_fix_info]	Contient les versions de correctifs pour chaque vulnérabilité tierce associée à une version du composant.
Aperçus du rapport sur les composants [sn_sbom_comp_report_insight]	Contient des aperçus des données périmées, abandonnées et réparables pour les composants.
Importations d'intégration Deps [sn_sbom_deps_integration_import]	Contient des informations sur la liste des versions importées pour un package ou une bibliothèque donné.
Importations d'intégration OSV [sn_sbom_osv_integration_import]	Contient des informations de veille sur les vulnérabilités pour une version donnée d'un package ou d'une bibliothèque.
Listes de versions de composants [sn_sbom_st_version_list]	Contient des informations sur la version et les dates de publication des composants.

Travaux planifiés

Tâche	Description
Calculer la réparabilité et la vulnérabilité du composant	Calcule des informations sur la façon de corriger les composants présentant des vulnérabilités et sur la probabilité que vous puissiez corriger les composants.
Nouveaux composants de l'intégration OSV	Récupère toutes les vulnérabilités connues du public associées aux packages (bibliothèques) qui ont été importés après la dernière exécution de l'intégration.
Intégration OSV complète	Récupère toutes les vulnérabilités connues du public associées à tous les packages qui ont été importés.
Intégration Deps.dev	Récupère toutes les versions connues du public pour les packages et utilisées pour identifier les composants dans **les états périmés** et **abandonnés** .
Mettre à jour les vuln_based_criticality sur les composants de nomenclature	Met à jour la criticité pour les composants présentant des vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une règle d'élément vulnérable d'application dans l'espace de Nomenclature logicielle travail

Configurez les conditions dans lesquelles les éléments vulnérables de l'application (AVIT) sont créés automatiquement dans le module Règles de création AVI de l'espace Nomenclature logicielle de travail (SBOM).

Avant de commencer

L'application SBOM Response est nécessaire si vous souhaitez créer des éléments vulnérables de l'application. Consultez Explorer Nomenclature logicielle pour plus d'informations.

Rôle requis : sn_sbom_resp.manage_avi_rule.

Procédure

1. Accédez à la **Espace de travail SBOM** > **Règles de création AVI**.
2. Sélectionnez **Nouveau**.
3. Remplissez les champs.

Champ	Description
Nom	Nom de la règle.
Actif	Indique si la règle de création est activée.
Ordre d'exécution	Ordre dans lequel les règles sont évaluées. La règle dotée de la valeur numérique la plus basse s'exécute en premier. Par exemple, vous pouvez créer des règles de priorité plus élevées pour les éléments qui nécessitent une gestion spéciale ou lorsque le risque est critique afin qu'elles soient exécutées en premier. Ensuite, créez des règles générales pour les articles qui ne nécessitent aucune manipulation spéciale. Enfin, créez une règle par défaut pour intercepter tous les composants qui présentent des vulnérabilités.
Description	Description de la règle pour vous aider à la distinguer des autres règles.
Conditions	Créez les conditions dans lesquelles les éléments vulnérables de l'application (AVI) sont créés. Par exemple, vous pouvez sélectionner **[Gravité > vulnérabilité][est][1-Critique]** pour créer des AVIT pour les composants qui présentent des vulnérabilités à haut risque et susceptibles d'avoir un impact grave sur vous. Notez que vous pouvez ajouter d'autres conditions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Enregistrer**.
   Votre règle de création s'exécute automatiquement après le chargement suivant et crée des AVI pour les composants qui correspondent à vos conditions. Vous pouvez également exécuter la règle sur demande à partir du module Règles de création AVI en sélectionnant **Exécuter maintenant**.

Résultats

Une fois qu'ils sont créés, vous pouvez vérifier qu'un AVIT a été créé spécifiquement pour SBOM les données en vérifiant les valeurs dans les champs **Source** et **Type d'analyse** d'un enregistrement AVI.

Champ	Valeur
Source	SBOM
Type d'analyse	SBOM-SCA

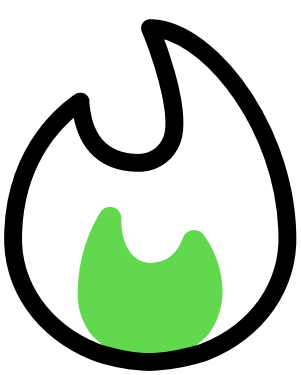
Applications de gestion des tickets de sécurité d'entreprise

Les applications de gestion des tickets de sécurité d'entreprise incluent Réponse aux incidents de sécurité, une solution d'orchestration et d'automatisation de la sécurité (SOAR) qui vous aide à répondre rapidement à l'évolution des menaces tout en optimisant et en orchestrant les opérations de sécurité de l'entreprise. Elle élimine les erreurs et les frictions inhérentes aux transferts manuels entre les systèmes, les équipes et les responsabilités.

Premiers pas

Les applications suivantes Réponse aux incidents de sécurité sont disponibles avec des abonnements distincts du ServiceNow® Store. Consultez la rubrique Opérations de sécurité et le ServiceNow Store pour plus d'informations sur la localisation, l'obtention d'une autorisation et le téléchargement d'applications sur votre instance.

Security Incident Response



En savoir plus sur l'application Security Incident Response

Gestion des incidents de sécurité majeurs



En savoir plus sur l'application Major Security Incident Management

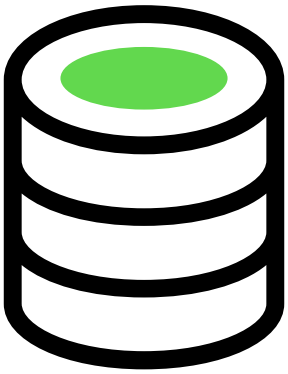
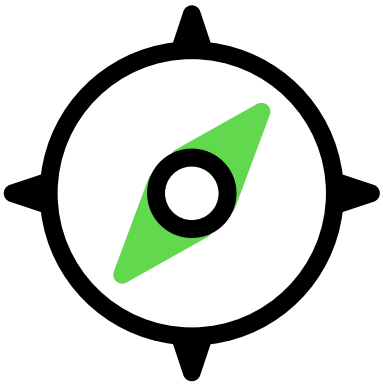
Renseignements sur les menaces



En savoir plus sur l'application Threat Intelligence

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Centre de sécurité des renseignements sur les menaces	Data Loss Prevention Incident Response	Fonctionnalités partagées des applications Security Incident Response
		
En savoir plus sur l’application Centre de sécurité des renseignements sur les menaces	En savoir plus sur l’application de prévention des pertes de données	Découvrez les fonctionnalités partagées entre les applications Security Incident Response

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Réponse aux incidents de sécurité

L’application ServiceNow® Réponse aux incidents de sécurité suit la progression des incidents de sécurité, de la découverte et de l’analyse initiale au confinement, en passant par l’éradication et la récupération, jusqu’à la revue post-incident finale, la création d’articles de la base de connaissances et la fermeture.

Demander des applications dans l'App Store

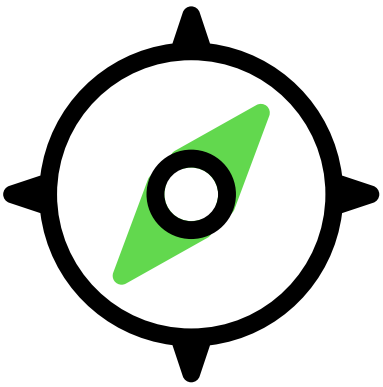
Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

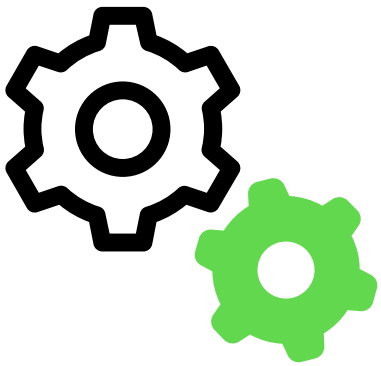
Réponse aux incidents de sécurité

Explorer



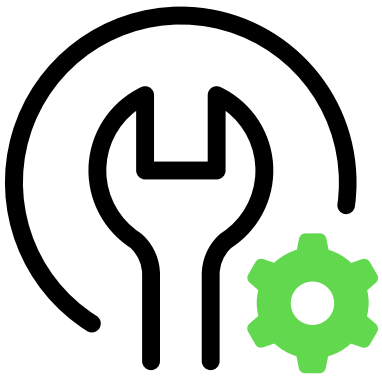
En savoir plus sur les fonctionnalités de Security Incident Response

Mettre en place et configurer



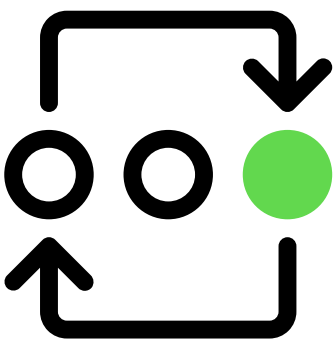
Installez et configurez votre application Security Incident Response

Administrer



Gérez et personnalisez vos incidents de sécurité

Intégrer



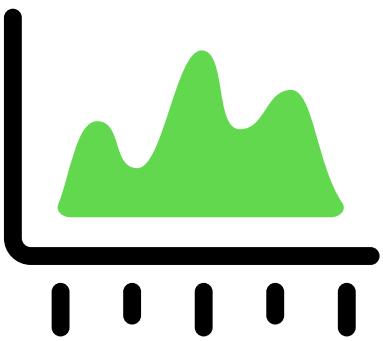
Étendre Security Incident Response en l'intégrant à d'autres applications

Utiliser l'espace de travail Réponse aux incidents de sécurité



Découvrir comment utiliser les espaces de travail Réponse aux incidents de sécurité et Rattrapage informatique

Analyses et reporting



Surveiller la progression du rattrapage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Obtenir des informations supplémentaires sur Réponse aux incidents de sécurité

Demander une application Opérations de sécurité dans l'App Store

Si vous êtes un nouveau Opérations de sécurité client du London correctif 6 ou d'une version ultérieure, consultez le ServiceNow Store pour afficher toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique.

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Présentation de Réponse aux incidents de sécurité

Avec Réponse aux incidents de sécurité (SIR), gérez le cycle de vie de vos incidents de sécurité, de l'analyse initiale au confinement, en passant par l'éradication et la reprise. Security Incident Response vous permet d'obtenir une compréhension complète des procédures de réponse aux incidents exécutées par vos analystes, ainsi que de comprendre les tendances et les goulots d'étranglement de ces procédures grâce à des tableaux de bord et des rapports basés sur des analyses.

Une introduction à Security Incident Response, montrant comment commencer à utiliser l'application.

Regardez cette vidéo de neuf minutes pour en savoir plus sur le processus SIR, son utilisation Réponse aux incidents de sécurité pour déjouer les attaques et visualiser l'activité de sécurité dans l'Explorateur Réponse aux incidents de sécurité .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les intégrations intégrées avec des solutions de cybersécurité tierces et les intégrations développées par des partenaires à partir de la boutique permettent l'automatisation et l'orchestration de la ServiceNow sécurité pour une réponse efficace et précise aux incidents.

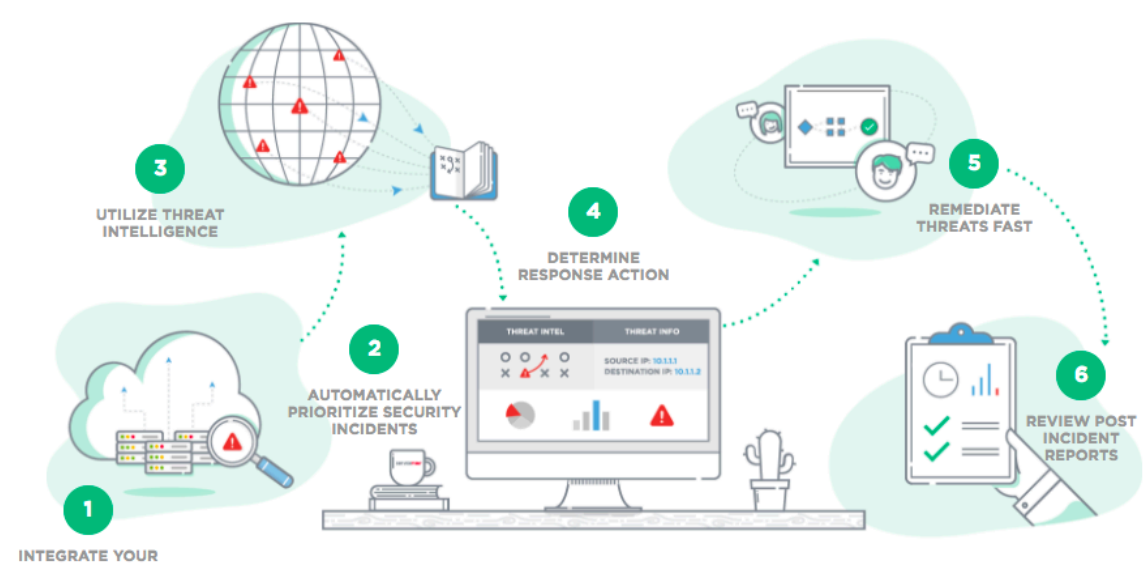
Pour protéger vos enquêtes et préserver la confidentialité des incidents de sécurité, Réponse aux incidents de sécurité fournit des moyens de restreindre l'accès au système à des rôles et ACL spécifiques liés à la sécurité. L'accès peut être restreint aux administrateurs non liés à la sécurité, sauf si vous leur autorisez expressément l'entrée.

Remarque : Les administrateurs de système informatique [admin] peuvent emprunter l'identité d'utilisateurs ServiceNow. Toutefois, lorsqu'il emprunte l'identité d'un utilisateur avec un rôle d'administrateur d'application pour Réponse aux incidents de sécurité, un administrateur ne peut pas accéder aux fonctionnalités accordées par ce rôle, y compris les incidents de sécurité et les informations de profil. L'accès aux modules et aux applications dans la barre de navigation est également limité. En outre, l'administrateur ne peut pas modifier le mot de passe d'un utilisateur disposant d'un rôle d'administrateur d'application pour Réponse aux incidents de sécurité.

Flux d'informations sur Réponse aux incidents de sécurité

Security Incident Response utilise le flux d'informations suivant, de l'intégration à l'enquête, puis à la résolution et à l'examen.

Remarque : Il s'agit d'une infographie interactive, vous pouvez donc essayer de cliquer sur l'une des icônes ou étapes de l'image pour en savoir plus sur ce processus ou cette tâche.



1. Cliquez sur cette image pour en savoir plus sur les intégrations SIR
2. Cliquez sur cette image pour en savoir plus sur la création d'incidents de sécurité
3. Cliquez sur cette image pour en savoir plus sur Threat Intelligence
4. Cliquez sur cette image pour en savoir plus sur l'espace de travail SIR
5. Cliquez sur cette image pour en savoir plus sur les fonctionnalités d'attaque MITRE
6. Cliquez sur cette image pour en savoir plus sur les activités de revue post-incident

Découverte

Les incidents de sécurité peuvent être journalisés ou créés de la manière suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- À partir du formulaire d'incident de sécurité
- À partir d'événements qui sont engendrés en interne, ou créés par des systèmes externes de surveillance ou de suivi des vulnérabilités via des règles d'alerte, ou manuellement
- À partir de systèmes de surveillance ou de suivi externes
- À partir du catalogue de services

Analyse

Selon la vue sélectionnée que vous utilisez (par défaut, Sécurité non informatique, Sécurité ITIL, etc.), le formulaire d'incident de sécurité peut afficher n'importe quelle combinaison de vulnérabilités, d'incidents, de changements, de problèmes et de tâches sur le CI affecté et les groupes de CI affectés. Le système peut identifier les logiciels malveillants, les virus et d'autres zones de vulnérabilité en recoupant la base de données du National Institute of Standards and Technology (NIST) ou d'autres logiciels de détection tiers. Au fur et à mesure que les incidents de sécurité sont résolus, vous pouvez utiliser n'importe quel incident pour créer un article de la base de connaissances de sécurité pour référence ultérieure.

Effectuez une analyse plus approfondie à l'aide d'une carte des services d'entreprise pour localiser d'autres systèmes ou services d'entreprise affectés qui peuvent être infectés.

Confinement, éradication et reprise

Lorsque vous surveillez et analysez les vulnérabilités, vous pouvez créer et affecter des tâches à d'autres départements. Vous pouvez utiliser une carte de service d'entreprise pour créer des tâches, des problèmes ou des changements pour tous les systèmes, documents, activités, messages SMS, appels de pont, etc.

Revue

Une fois l'incident résolu, d'autres étapes peuvent avoir lieu avant la fermeture. Vous pouvez effectuer une revue post-incident. La création d'articles de la base de connaissances peut aider lors de futurs incidents similaires. Les incidents importants peuvent nécessiter un examen de résolution post-incident. Cet examen peut prendre plusieurs formes. Par exemple :

- Organisez une réunion pour discuter de l'incident et recueillir des réponses.
- Rédigez et distribuez aux équipes qui ont travaillé sur un incident une liste de questions d'examen de résolution conçues pour chaque catégorie ou priorité d'incident.
- Les gestionnaires d'incidents peuvent rédiger le rapport et recueillir les informations par eux-mêmes.

Un rapport d'examen de résolution d'incident comprenant :

1. Un résumé de ce qui a été fait
2. la chronologie
3. Type d'incident de sécurité rencontré
4. tous les incidents, changements, problèmes, tâches, groupes de CI associés
5. Les détails de la résolution

En outre, un système d'enquête automatisé d'examen de la résolution des incidents de sécurité est disponible. Il rassemble les noms de tous les utilisateurs affectés à un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

incident de sécurité et envoie une enquête personnalisée pour recueillir des données sur la gestion de l'incident. Ces données peuvent ensuite être mises à disposition dans un rapport d'examen des incidents de sécurité généré, que vous pouvez modifier dans une version finale. Des données similaires peuvent être ajoutées à un article de la base de connaissances pour contenir les enseignements tirés et les mesures à prendre pour résoudre des problèmes similaires à l'avenir.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Terminologie de Security Incident Response

Les termes suivants sont utilisés dans .Réponse aux incidents de sécurité

Terme	Définition
Actif	Tout incident de sécurité dont l'état n'est pas fermé ou annulé.
Verrouillage de l'administrateur	La possibilité de restreindre Réponse aux incidents de sécurité l'accès au personnel ayant des rôles et des ACL liés à la sécurité.
Demandes de sécurité entrantes	Demandes soumises pour des demandes de sécurité à faible impact, telles que la demande d'un nouveau badge électronique.
Gérer les activités post-incident	Un examen des origines et de la gestion d'un incident de sécurité Le produit final est un rapport post-incident, qui documente toutes les actions effectuées et les raisons pour lesquelles elles ont été effectuées.
Tâches de réponse	Tâches affectées à un incident de sécurité pour le suivi des actions en réponse à la menace.
Comprendre les calculateurs d'incidents de sécurité	Calculateurs utilisés pour mettre à jour les valeurs d'enregistrement lorsque les conditions préconfigurées sont remplies.
Arborescences d'incidents de sécurité	Type de graphique qui affiche hiérarchiquement les données d'incident de sécurité sous la forme de rectangles imbriqués.
Recherche de menace	Demande soumise à partir du catalogue des incidents de sécurité pour l'analyse des fichiers, des URL et des adresses IP à la recherche de programmes malveillants.
Analyse des vulnérabilités	Une demande initiée à partir du formulaire d'incident de sécurité pour analyser les ressources affectées (serveurs, ordinateurs et autres éléments de configuration) pour détecter les vulnérabilités.

Séparation de domaine et Réponse aux incidents de sécurité

L'application Séparation de domaine est prise en charge dans Réponse aux incidents de sécurité. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau de prise en charge : Standard

- Inclut tous les aspects du support de niveau **basique** .
- Les propriétés d'application sont sensibles au domaine selon les besoins.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Vue d'ensemble

Dans l'application, Séparation Réponse aux incidents de sécurité de domaine permet aux fournisseurs de services (SP) de standardiser les procédures SOC (Security Operations Center) et Security Incident Response (SIR) sur l'ensemble de la base de clients qu'ils servent, avec des coûts opérationnels réduits et une meilleure qualité de service. Séparer les espaces de travail des clients pour les workflows, les tableaux de bord, les rapports, etc., garantit que les données client sont séparées et ne sont jamais exposées à d'autres clients.

Prise en charge de Domain Separation dans Security Incident Response par version et versions

Mise en production	Niveau de prise en charge	Notes
Genève, Helsinki	Aucune prise en charge	Lancement de la séparation de domaine au niveau des données
Istanbul	Les données uniquement	
Jakarta	Niveau 2 (données, demandeur, prestataire)	**Nouvelles fonctionnalités** : prise en charge des intégrations tierces avec séparation de domaine de niveau 2 dans une instance unique d'intégration, y compris les intégrations Threat Intelligence
Kingston	Niveau 2 (données, demandeur, prestataire)	**Nouvelles fonctionnalités** : l'intégration de la recherche de perceptions pour SIR est activée avec plusieurs instances, mais toutes les instances sont toujours hébergées sous un seul domaine. Exemple : si deux instances d'une intégration Splunk sont configurées (SplunkCLOUD et SplunkCORP), les deux sont toujours exploitées pour les activités de réponse aux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prise en charge de Domain Separation dans Security Incident Response par version et versions (suite)

Mise en production	Niveau de prise en charge	Notes
		incidents dans un seul domaine, où l'implémentation a été configurée à l'origine.
Londres	Niveau 2 (données, demandeur, prestataire)	**Nouvelles fonctionnalités** : toutes les intégrations résident dans plusieurs domaines
Madrid	Niveau 2 (données, demandeur, prestataire)	Toutes les intégrations peuvent désormais résider dans plusieurs domaines. Dans l'exemple ci-dessus, SplunkCloud peut être domaine1 et SplunkCORP domaine2.
New York	Niveau 2 (données, demandeur, prestataire)	Toutes les intégrations résident dans plusieurs domaines.
Orlando	Standard	Toutes les intégrations résident dans plusieurs domaines.
Paris	Standard	Toutes les intégrations résident dans plusieurs domaines.

Séparation de domaine pour l'application Réponse aux incidents de sécurité couvre les fonctionnalités de produit suivantes :

- Les alertes de sécurité sont dirigées vers le domaine approprié de l'utilisateur dont l'ID/les informations d'identification ou le champ d'application génère l'incident et qui est enregistré comme incident de sécurité.
- Les alertes génèrent des « observables », qui représentent des propriétés avec état ou des événements mesurables : les workflows de sécurité dans le domaine de l'incident de sécurité sont utilisés pour orchestrer la réponse.
- Les intégrations sont configurées dans le domaine de l'incident de sécurité pour l'automatisation des réponses.
- Les options sont configurées dans le domaine de l'incident de sécurité pour l'automatisation des réponses. Ces fonctionnalités (à partir de la version Kingston) comprennent :
  - Recherche de menace
  - Enrichir l'observable
  - Enrichir l'élément de configuration
  - Obtenir les processus d'exécution
  - Obtenir les statistiques réseau
  - Bloquer la demande
  - Isoler l'hôte
  - Recherche de perception

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

  - Recherche et suppression d'e-mails
  - Publier dans la liste de surveillance
- Les résultats de l'automatisation des réponses (telles que la recherche de menaces ou la recherche de perception) sont stockés dans le domaine de l'incident de sécurité.
- D'autres incidents de sécurité sont recoupés dans le même domaine de l'incident de sécurité en fonction d'un ensemble partagé d'observables.
- Les autres utilisateurs sont référencés dans le domaine de l'incident de sécurité.
- Les éléments de configuration sont référencés dans le même domaine que l'incident de sécurité.
- Des tâches de réponse manuelle sont ajoutées au domaine de l'incident de sécurité.
- Les articles de la base de connaissances et les guides d'exploitation sont référencés dans le domaine de l'incident de sécurité.
- Les mesures de Réponse aux incidents de sécurité pertinentes pour les incidents dans le domaine sont affichées sur les tableaux de bord ainsi que dans les rapports.

Remarque : Dans les cas précédents, les principes généraux de la visibilité dans des domaines séparés dans la NOW Platform s'appliquent. Comme toujours, un incident dans le domaine parent peut faire référence à des artefacts dans le domaine enfant, mais pas l'inverse.

Fonctionnement de Séparation de domaine dans Security Incident Response

L'application Réponse aux incidents de sécurité gère le cycle de vie d'un incident de sécurité de bout en bout. Les cas d'utilisation suivants sont sensibles à la séparation de domaine :

- **Ingestion d'événements et d'alertes** pour créer des incidents de sécurité auxquels l'analyste du SOC client ou le MSP doit répondre :
  - Analyseurs d'e-mails (basés sur la plateforme, hameçonnage signalé par un utilisateur, personnalisés)
  - Événements/alertes de déduplication avant la création de l'incident
  - Extraction automatique des observables
  - Applications dans le magasin SIEM tiers
- **Enrichissement** des artefacts impliqués dans les incidents (IP, URL, domaines, hachages de fichiers) :
  - Enrichissement des actifs (CMDB)
  - Utilisateurs (plateforme)
  - Automatisation : enrichissement des observables (p. ex. : Whols)
- **Enquêter sur** les incidents à l'aide des artefacts et sur leur réputation ou leur association avec des menaces connues
  - Orchestrer : Playbooks et articles de la base de connaissances
  - Automatisation : recherche de menaces (ex : VirusTotal), recherche de perception (ex : Splunk), obtenir les processus en cours d'exécution (ex : Carbon Black)
- **Éradiquez** les artefacts liés aux menaces impliqués dans l'incident sur la base de l'enquête effectuée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Orchestrer : Playbooks et articles de la base de connaissances
- Automatisation : recherche et suppression d'e-mails (ex : Microsoft Exchange), bloquer IP (ex : pare-feu Palo Alto)

- **Mesurer** l'efficacité des opérations de réponse aux incidents
  - Tableaux de bord Performance Analytics : productivité et tendances des incidents
  - Reconstitution des étapes d'enquête sur les incidents à partir des notes de travail
  - Examen post-incident

Configuration de Domain Separation

La configuration de Séparation de domaine pour Réponse aux incidents de sécurité ne nécessite aucune étape supplémentaire. Toutes les Réponse aux incidents de sécurité tables acquièrent la colonne Domaine une fois que l'instance est séparée par domaine.

Données séparées par domaine

Les données peuvent être séparées par domaine, ce qui signifie :

- Les incidents de sécurité dans un domaine ne peuvent pas être visualisés à partir d'autres domaines.
- Les observables extraits de l'incident de sécurité sont placés dans le même domaine et ne peuvent pas être visualisés à partir d'autres domaines.
- Jusqu'à la version Kingston, des intégrations tierces configurées existent dans le domaine global et sont accessibles à tous les autres domaines de l'instance.
- Dans la version Madrid, les intégrations tierces peuvent être configurées et activées pour chaque domaine. Cela signifie que l'intégration activée et configurée dans un domaine ne peut pas être exploitée dans un autre domaine.
- Les automatisations qui s'exécutent sur les observables à l'aide d'intégrations tierces (pour l'examen, l'action de maîtrise ou l'éradication des menaces), placent leurs résultats dans le domaine de l'incident de sécurité et les résultats ne peuvent pas être consultés à partir d'un autre domaine.
- Les workflows Orchestration créés dans un domaine ne sont pas visibles dans un autre domaine.
- Les options (telles que délimitées dans la liste des fonctions d'options de préparation) qui sont invoquées restent génériques dans tous les domaines avec une implémentation spécifique au domaine de l'option appelée. Par exemple, une recherche de perception sur une adresse IP peut invoquer une implémentation Splunk dans un domaine et une implémentation QRadar dans un autre.

Configuration

Tous les aspects de la configuration du produit sont autonomes dans un environnement séparé par domaine. La configuration peut être adaptée à chaque domaine.

Remarque : La logique métier et les processus dans #2-5 ci-dessous peuvent être administrés dans le domaine du locataire.

Les tâches suivantes doivent être configurées :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Administration système
   - Affectez des rôles à des utilisateurs et à des groupes d'utilisateurs : Rôles d'utilisateur installés avec Réponse aux incidents de sécurité
   - Installez un ou plusieurs modules d'extension d'intégration tiers à utiliser Réponse aux incidents de sécurité: Intégrations de Réponse aux incidents de sécurité
2. Administration du Réponse aux incidents de sécurité
   - Ajoutez ou passez en revue les rôles : Composants installés avec Réponse aux incidents de sécurité
   - Configurez les groupes et les utilisateurs : Créer un groupe d'incidents de sécurité
   - Configurez les escalades d'incidents : Escalader un incident de sécurité
   - Configurez les calculateurs de score de risque d'incidents de sécurité : Comprendre les calculateurs d'incidents de sécurité
   - Configurer des accords sur les niveaux de service : Créer un Réponse aux incidents de sécurité SLA
   - Configurez les définitions du processus d'incident de sécurité : Comprendre la définition du processus de Security Incident Response
   - Configurez des processus d'examen post-incident : Gérer les activités post-incident
3. Paramètres d'e-mail de l'incident de sécurité
   - Définissez la boîte de réception de l'analyse des e-mails : Opérations de sécurité Analyse des e-mails
   - Configurez les analyseurs d'e-mails pour l'ingestion d'alertes : Créer des analyseurs d'e-mails dans Security Operations
   - Configurez des règles de correspondance d'e-mails pour le hameçonnage signalé par les utilisateurs : Créer des règles pour valider les attaques par hameçonnage signalées par un utilisateur
   - Configurer les actions entrantes d'e-mail :Actions d'e-mail entrant
4. Paramètres du Playbook pour les incidents de sécurité
   - Examiner et configurer les documents du Runbook : Créer un Runbook de réponse aux incidents de sécurité
   - Configurez les workflows d'incidents de sécurité : Opérations de sécurité Fonctionnalité commune
5. Configurations d'aptitudes
   - Demande de bloc : Security Operations Integration : option Demande de bloc
   - Recherche et suppression d'e-mails : Security Operations Integration : option de recherche et de suppression d'e-mails
   - Enrichir l'élément de configuration : Security Operations Integration : enrichir l'aptitude CI
   - Enrichir l'observable : Security Operations Integration : enrichir l'aptitude des observables
   - Obtenir les statistiques réseau : Security Operations Integration : obtenir l'aptitude de statistiques réseau
   - Obtenir les processus en cours d'exécution : Security Operations Integration : obtenir l'aptitude d'exécution des processus
   - Isoler l'hôte : Security Operations Integration : capacité d'isolement de l'hôte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Publier dans la liste de surveillance : Security Operations Integration : aptitude de publication dans la liste de surveillance
- Recherche de perception : Security Operations Integration - Option de recherche de perceptions
- Recherche de menaces : Security Operations Integration - Aptitude de recherche de menace

Comment les domaines des locataires gèrent leurs propres données d'application

- Les propriétaires de domaines du locataire créent leurs propres règles d'analyse des e-mails pour l'ingestion des incidents de sécurité.
- Les propriétaires de domaines locataires peuvent configurer des intégrations spécifiques exclusivement destinées à être utilisées dans le domaine.
- Les propriétaires de domaines du locataire peuvent créer leurs propres workflows de réponse aux incidents.
- Les propriétaires de domaines du locataire peuvent créer leurs propres catégories d'incidents, articles de la base de connaissances de réponse aux incidents et runbooks à associer aux workflows de réponse aux incidents.
- Les utilisateurs du domaine locataire créent et ferment leurs propres incidents de sécurité.

Logique métier et processus pouvant être séparés par domaine par le propriétaire de l'instance

- Réponse aux incidents de sécurité Utilisateurs et groupes
- Réponse aux incidents de sécurité intégrations (à partir de la version Madrid)
- Règles d'analyse des e-mails pour la création d'incidents
- Règles métier pour consolider plusieurs événements ou alertes dans un incident de sécurité
- Workflows pour l'orchestration de la réponse aux incidents
- Calculateurs de score de risque d'incidents de sécurité
- Chemin d'escalade des incidents de sécurité
- SLA d'incidents de sécurité
- Définitions de processus d'incidents de sécurité
- Processus de revue post-incident de l'incident de sécurité

Information associée

Séparation de domaine pour les fournisseurs de services

Configurer Réponse aux incidents de sécurité

La configuration de Réponse aux incidents de sécurité implique des étapes obligatoires et plusieurs étapes facultatives, en fonction de vos besoins spécifiques. Une fois que vous l'avez téléchargé Réponse aux incidents de sécurité à partir de et ServiceNow Store que vous l'avez installé, vous êtes prêt à exécuter l'assistant de configuration pour effectuer la configuration de base et Réponse aux incidents de sécurité les intégrations tierces.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

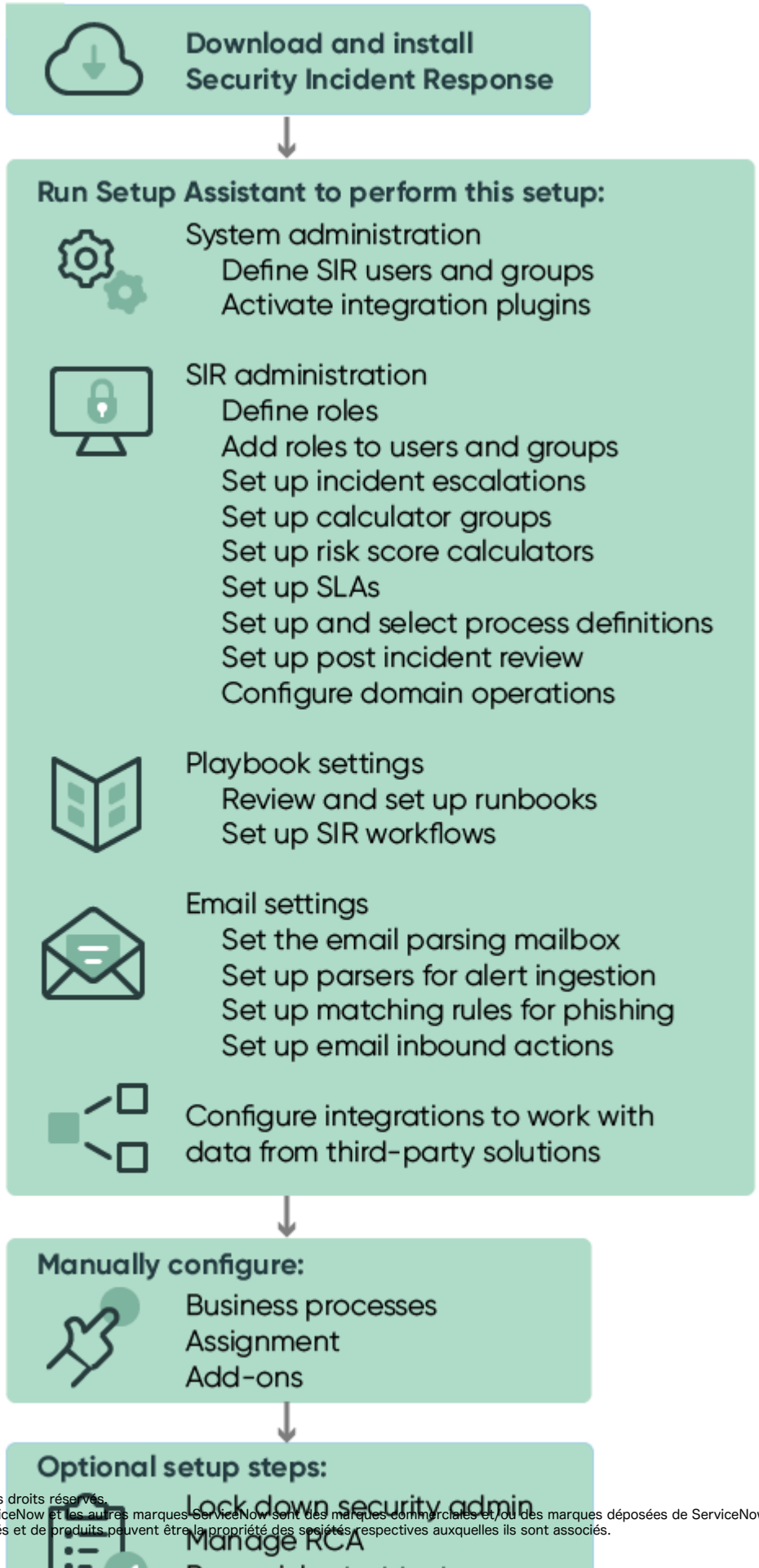
Processus Réponse aux incidents de sécurité de configuration

Le diagramme suivant illustre le processus de configuration. Il est séparé en deux sous-processus : le téléchargement et la configuration de l’application Réponse aux incidents de sécurité .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La première étape de configuration consiste à Télécharger le Réponse aux incidents de sécurité application à partir de ServiceNow Store. Une fois le téléchargement terminé, plusieurs applications dépendantes, y compris l'assistant de configuration, sont chargées et prêtes à être configurées Réponse aux incidents de sécurité.

Assistant de configuration

L'assistant Réponse aux incidents de sécurité de configuration est une application de type assistant qui vous guide, étape par étape, tout au long de la configuration de votre instance de base Réponse aux incidents de sécurité .



Les étapes de configuration sont assez explicites ; toutefois, si vous avez besoin d'explications supplémentaires, vous trouverez de l'aide supplémentaire dans la référence de l'assistant de configuration. Une fois que vous avez terminé la configuration à l'aide de l'assistant de configuration, vous pouvez effectuer d'autres procédures de configuration facultatives, si nécessaire. Ces procédures comprennent des options pour :

- Configurer le cycle de vie de la demande
- Création de catalogues et de demandes
- Configuration des notifications
- Configurer l'affectation manuelle et automatique
- Activation de la base de connaissances, des documents gérés et des activités de tâche

Un nouvel espace de travail amélioré pour la Réponse aux incidents de sécurité est disponible. Pour plus d'informations, consultez Espace de travail de la Réponse aux incidents de sécurité.

Installer et configurer Réponse aux incidents de sécurité

Avant de l'exécuter Réponse aux incidents de sécurité dans votre instance, vous devez la télécharger à partir de et terminer les ServiceNow Store étapes de configuration.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

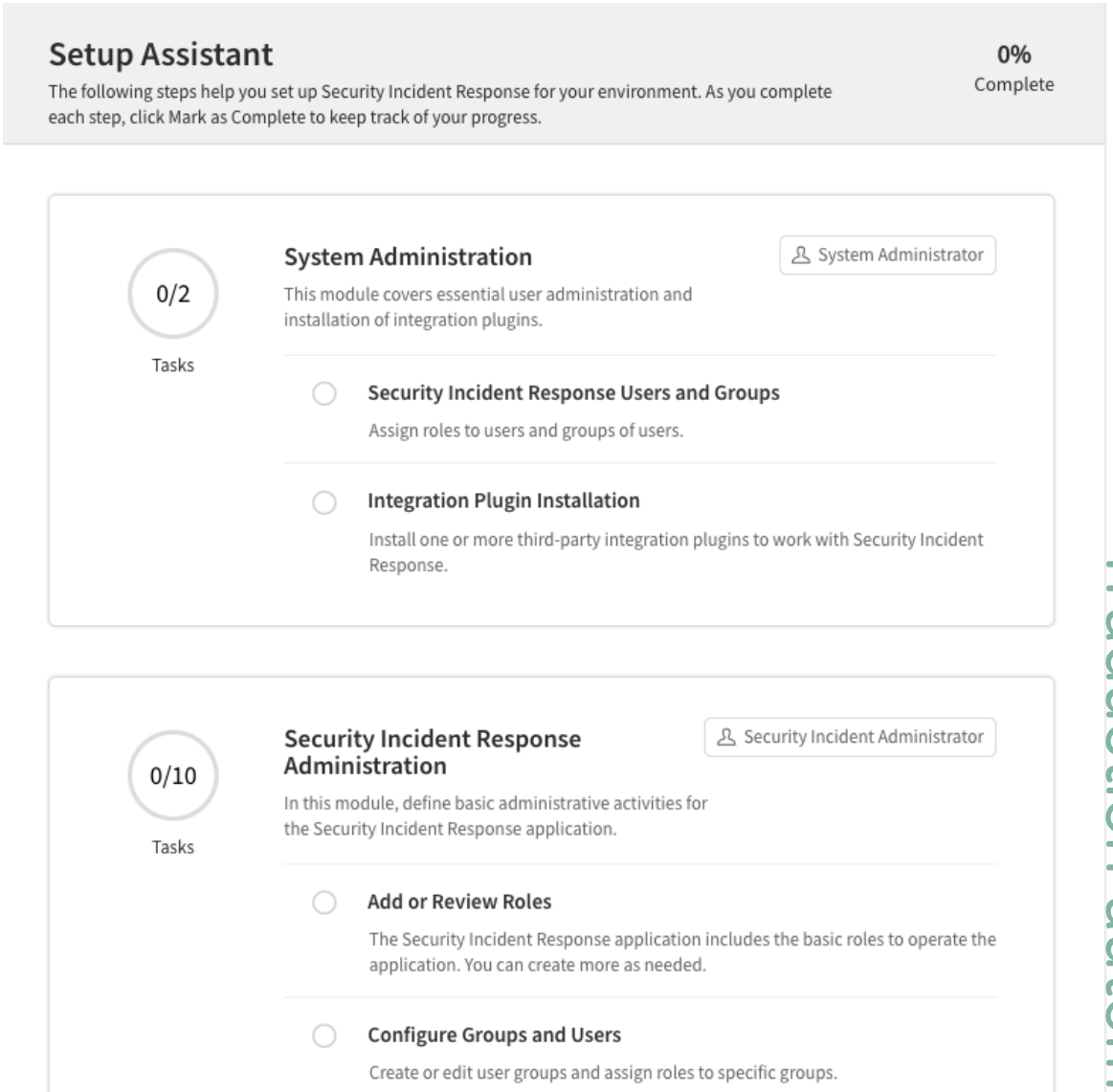
- L'installation de la Réponse aux incidents de sécurité version 13.4.5 ou ultérieure à partir de la ServiceNow StoreEspace de travail de la Réponse aux incidents de sécurité version sn_si_aw 1.5.1 ou ultérieure sera automatiquement installée par défaut. Pour plus d'informations sur les applications dépendantes, reportez-vous à la Espace de travail SIR Modules d'extension et rôles section.
- Veuillez noter que les versions 1.5.1 et supérieures de l'espace de travail Réponse aux incidents de sécurité ne peuvent être installés/mis à niveau que par le biais d'une installation/mise à niveau de Réponse aux incidents de sécurité et ne peuvent pas être installés indépendamment.
- Les dernières fonctionnalités de sont Réponse aux incidents de sécurité exclusivement disponibles dans le Espace de travail de la Réponse aux incidents de sécurité. Veuillez installer ou mettre à niveau vers la dernière Réponse aux incidents de sécurité version pour Espace de travail de la Réponse aux incidents de sécurité accéder aux fonctionnalités telles que le transfert d'équipe, le calculateur de score de risque, entre autres.

Procédure

1. Suivez les instructions pour Télécharger une application à partir de ServiceNow Store.
2. Une fois que vous avez téléchargé l'application Réponse aux incidents de sécurité et toutes ses applications dépendantes, accédez à **Incident de sécurité** > **Configuration d'Analyst Workspace** > **Assistant de configuration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Suivez les instructions figurant sur les formulaires pour configurer le système de Réponse aux incidents de sécurité base.
   Pour en savoir plus sur certaines des tâches de configuration les plus complexes, reportez-vous à la section Référence de l'assistant de configuration, selon les besoins.

Télécharger et installer Security Analyst Workspace

Avant d'exécuter la Réponse aux incidents de sécurité nouvelle interface utilisateur dans votre instance, vous devez la télécharger à partir de et l'installer ServiceNow® Store .

Avant de commencer

Pour garantir une installation fluide, vérifiez que vous disposez des rôles requis ServiceNow pour votre instance. Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus :

- S'il n'est pas déjà affecté, l'administrateur système [admin] installe l'application et lui attribue le rôle d'administrateur de Réponse aux incidents de sécurité [sn_si.admin].
- L'administrateur de Security Incident Response [sn_si.admin] supervise la configuration et vérifie les résultats attendus.

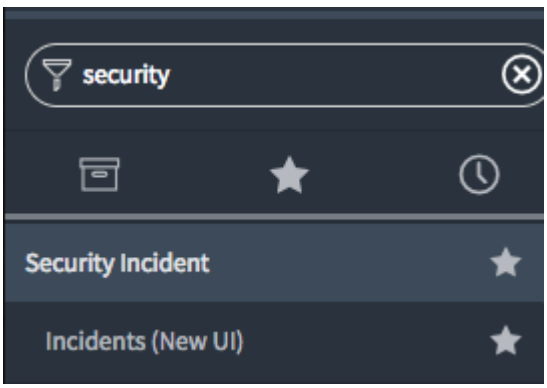
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : admin

Procédure

1. Suivez les instructions pour Télécharger une application à partir de ServiceNow Store et installer l'application **d'interface utilisateur Réponse aux incidents de sécurité** .
2. Une fois l'installation terminée, vous pouvez ouvrir Security Analyst Workspace en accédant à **Incident de sécurité** > **Incidents (nouvelle interface utilisateur)**



Composants installés avec Réponse aux incidents de sécurité

Plusieurs types de composants sont installés lorsque vous téléchargez et activez l'application, notamment les rôles d'utilisateur, les tables, les propriétés et les Réponse aux incidents de sécurité travaux planifiés.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Propriétés installées

Les utilisateurs disposant du rôle d'administrateur système [admin] peuvent afficher les propriétés. Les utilisateurs disposant du rôle d'administrateur de sécurité [sn_si.admin] peuvent les modifier.

Propriété	Utilisation
Les nœuds de catégorie par défaut affichés dans l'onglet Graphe des relations de l'espace de travail. Les valeurs par défaut représentent les noms de tables correspondant aux enregistrements connexes. sn_si_aw.defaultCategories	• **Type** : chaîne • **Valeur par défaut** : sn_ti_m2m_task_observables,sn_si_m2m_task_affected_user,s
L'heure de début par défaut pour tous les agents quand aucune planification n'est définie, au format suivant : 08:00 sn_si.default.start.time	• **Type** : chaîne • **Valeur par défaut** : 08:00 • **Emplacement** : **Incident de sécurité** > **Administration** > **Propri**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
Heure de fin par défaut pour tous les agents quand aucune planification n'est définie, au format suivant : 17:00 sn_si.default.end.time	• **Type** : chaîne • **Valeur par défaut** : 17:00 • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Inclure les observables de type Destination ainsi que d'autres observables de type contexte dans les relations entre l'utilisateur de l'incident de sécurité et le CI sn_si.link_dest_ip	Détermine si un observable d'incident de sécurité avec un type de contexte D affiché sous les onglets **Éléments de configuration** ou **Utilisateurs affe** défaut, les observables ayant un type de contexte Destination sont exclus. Pou observables, choisissez Oui.
Autoriser la personnalisation lors de la création d'un problème ou d'une demande de changement à partir d'un incident de sécurité sn_si.popup	Lorsqu'un problème ou un changement est créé, cette propriété fenêtre contextuelle pour modifier la demande. Si ces propriétés sont définies sur **faux**, le problème ou la demande changement a la même priorité, la même description brève et la description que l'incident de sécurité, sans possibilité d'ajouter modifier ces champs. • **Type** : vrai | faux • **Valeur par défaut** : true • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Associez les résultats de la recherche de perception aux CI dans la CMDB. sn_si.associate_ci_with_sighting_search	Lorsqu'ils sont définis sur vrai, les résultats de la recherche de perceptions inc éléments de configuration associés qui se trouvent dans votre CMDB. • **Type** : vrai | faux • **Valeur par défaut** : true • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Le score de risque dans la plage est en surbrillance verte, au format 0-49 sn_si.risk.score.green	Dans la liste des incidents de sécurité, les incidents de sécurité dont le score d compris entre 0 et 49 sont marqués d'un point vert.
Le score de risque dans la plage est en surbrillance orange, au format 50-79 sn_si.risk.score.orange	Dans la liste des incidents de sécurité, les incidents de sécurité dont le score d compris entre 50 et 79 sont marqués d'un point orange.
Le score de risque dans la plage est en surbrillance rouge, au format 80-100 sn_si.risk.score.red	Dans la liste des incidents de sécurité, les incidents de sécurité dont le score d compris entre 80 et 100 sont marqués d'un point rouge.
Ce paramètre active ou désactive les configurations de recherche de perceptions qui ont implémenté cette fonctionnalité.	Lorsque la valeur est définie sur vrai, les recherches de perceptions peuvent ê sur les intégrations activées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
sn_si.enable_sighting_search	• **Type** : vrai | faux • **Valeur par défaut** : true • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Nombre de lignes de données brutes qui sont enregistrées lorsqu'une recherche d'observation est effectuée. Plage 0-100 sn_si.sighting_search_raw_data_rows	Cette propriété utilise par défaut 50 lignes de données brutes. La moitié des li résultats sont signalées à partir du début de la période de recherche et l'autre m de la fin de la période de recherche. Ainsi, si vous sélectionnez 50 lignes, 25 p début du délai de recherche et 25 de la fin du délai de recherche.
Faire passer automatiquement l'état de l'incident à Maîtriser lorsqu'une tâche de réponse passe à Travail en cours sn_si.rollup_task_state	Lors de l'utilisation de flux ou de workflows, pensez à définir cette propriété vous permet de contrôler l'état de l'incident à partir des flux ou des workflow également d'éviter tout conflit potentiel lors de la transition d'un état d'incide • **Type** : vrai | faux • **Valeur par défaut** : true • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Propriétés d'affectation pour Réponse aux incidents de sécurité	
Poids de l'emplacement sn_si.location.weight	Une évaluation utilisée lors du calcul des critères à utiliser pour l'affectation a d'un analyste de sécurité. Si, par exemple, l'emplacement est pris en compte p la valeur Poids de l'emplacement est ajoutée à l'évaluation de l'analyste de sé • **Type** : nombre entier • **Valeur par défaut** : 10 • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Poids des compétences sn_si.skills.weight	Une évaluation utilisée lors du calcul des critères à utiliser pour l'affectation a d'un analyste de sécurité. Si, par exemple, les compétences sont prises en con tâche, la valeur Poids des compétences est ajoutée à l'évaluation de l'analyste • **Type** : nombre entier • **Valeur par défaut** : 10 • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Définir le nombre maximal d'analystes de sécurité à traiter par affectation automatique à un moment donné sn_si.max.agents.processed	Le système a une limite absolue de 300 analystes de sécurité. Si vous spécifie 300, la valeur est définie à ce niveau. Le système ne peut pas répartir automat tâche pour un groupe de distribution qui contient plus d'analystes de sécurité configurée. • **Type** : nombre entier • **Valeur par défaut** : 100 • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Poids du fuseau horaire sn_si.timezone.weight	Une évaluation utilisée lors du calcul des critères à utiliser pour l'affectation a d'un analyste de sécurité. Si, par exemple, le fuseau horaire de l'analyste de s pris en compte pour une tâche, la valeur de pondération du fuseau horaire est l'évaluation de l'analyste de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
	• **Type** : nombre entier • **Valeur par défaut** : 10 • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Durée (en minutes) à ajouter entre la fin d'une tâche et le début du déplacement pour la suivante. sn_si.espacement.travail	Un exemple d'une valeur de temps valide est 10. • **Type** : nombre entier • **Valeur par défaut** : 0 • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Champs de journal spécifiés contenant des balises de code qui restituent le contenu au format HTML. sn_si.journal_field.html_enabled	• **Type** : chaîne • **Valeur par défaut** : work_notes, commentaires • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Calculez les services impactés en arrière-plan. sn_si.refresh_impacted.event	La liste connexe des services affectés et des CI impactés est générée par le bia d'événements. Lorsqu'elle est activée, l'actualisation est exécutée en arrière-p balises de sécurité sont ajoutées à l'incident. Définissez la valeur sur **vrai** pour effectuer l'opération en arrière • **Type** : vrai | faux • **Valeur par défaut** : faux • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**
Récupérez le service critique à partir de données précalculées. sn_si.critical_service.calculator.use_cache	Permet au calculateur de services critiques d'utiliser les donnée précalculées des éléments de configuration. Définir la valeur sur **vrai** pour effectuer une recherche à partir d précalculées • **Type** : vrai | faux • **Valeur par défaut** : faux • **Emplacement** : **Incident de sécurité** > **Administration** > **Propriété**

Traduction automatique

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
Administrateur des incidents de sécurité [sn_si.admin]	Contrôle total sur toutes les Réponse aux incidents de sécurité données. Administre également les territoires et les compétences, selon les besoins.	• assessment_admin • catalog_admin • decision_table_admin • decision_table_reader

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	Remarque : Dans le système de base, l'administrateur a également accès à sn_si.admin. Réponse aux incidents de sécurité peut être restreint par l'administrateur tant qu'au moins un autre utilisateur est affecté au rôle d'administrateur de sécurité.	• filter_admin • flow_designer • pd_author • pd_content_author • pd_operator • skill_admin • skill_model_admin • sn_si.analyst • sn_si.ingestion_profile_admin • sn_si.knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_access_manager • sn_si.special_access_read_manager • sn_si.special_access_write_manager • sn_ti.malicious_attachment_access • sn_ti.observable.admin • tags_admin • template_admin • territory_admin • treemap_admin • user_admin
Administrateur de profil [sn_si.ingestion_profile_admin]	Configurez les modules d'extension, créez, modifiez, supprimez et gérez les profils pour Splunk, Splunk ES et l'application Azure Sentinel Integration pour Security Operations. **Remarque :** Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut. Le rôle sn_si.ingestion_profile_admin peut être affecté aux utilisateurs par le sn_si.admin.	N/A

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
Analyste des incidents de sécurité [sn_si.analyste]	Gérer les incidents de sécurité Rôle sous-jacent de l'accès de sécurité de base. Les utilisateurs disposant de ce rôle peuvent créer et mettre à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes, des changements et des pannes liés à leurs incidents.	• pd_operator • snc_platform_rest_api_access • sn_msi.promoteur • sn_msi.proposer • sn_si.basic • sn_ti.malicious_attachment_access
Incident de sécurité de base [sn_si.basic]	Rôle sous-jacent de l'accès de sécurité de base. Les utilisateurs disposant de ce rôle peuvent créer et mettre à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes, des changements et des pannes liés à leurs incidents.	• canvas_user • document_management_user • email_composer • flow_operator • inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write • sn_si.read • sn_ti.observable.read • sn_ti.observable.write • sn_ti.lire • task_activity_writer • task_editor • treemap_user
Directeur de la sécurité de l'information (CISO) [sn_si.ciso]	Affichez et manipulez le tableau de bord du CISO. En outre, si le module d'extension est activé, les Réponse aux vulnérabilités utilisateurs disposant de ce rôle peuvent ajouter des arborescences de définition de l'importance de la vulnérabilité au tableau de bord. Vous pouvez également faire de même avec Réponse aux incidents de sécurité le plugin.	• pa_viewer • sn_si.basic • sn_si.read
Incident de sécurité externe [sn_si.externe]	Afficher tous les incidents de sécurité qui appartiennent à son groupe particulier.	service_fulfiller

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
	Remarque : Les deux règles suivantes s'appliquent partout ServiceNow , indépendamment de l'administrateur ou de l'application du champ d'application. • Lorsque vous ajoutez un utilisateur à un groupe, vous affectez également des rôles à ce groupe. De même, lorsque vous supprimez un utilisateur d'un groupe, les rôles hérités sont également supprimés. • Chaque rôle peut être affecté par un rôle de priorité supérieure.	
Utilisateur d'intégration des incidents de sécurité [sn_si.integration_user]	Les outils externes peuvent fournir de nouveaux enregistrements d'incidents de sécurité et mettre à jour les enregistrements d'incidents de sécurité.	import_transformer
Administrateur des connaissances sur les incidents de sécurité [sn_si.knowledge_admin]	Gérez, mettez à jour et supprimez les informations contenues dans la base de connaissances des incidents de sécurité.	• knowledge_admin • sn_si.read
Gestion des incidents de sécurité [sn_si.responsable]	Même accès que les analystes de sécurité.	• pd_author • pd_operator • sn_si.basic
Lecture de l'incident de sécurité [sn_si.lire]	Lire les incidents de sécurité.	• canvas_user • sn_sec_cmn.lire • sn_templated_snip.template_snippet • sn_ti.observable.read • workspace_user
Gestionnaire d'accès aux restrictions de sécurité [sn_si.restriction_access_manager]	Permet aux utilisateurs ou aux groupes d'appliquer des restrictions sur les incidents de sécurité. Cela ne s'applique qu'au changement de champ.	N/A
Accès spécial aux incidents de sécurité sn_si.accès_spécial_	Fournit l'accès à des incidents de sécurité spécifiques à des utilisateurs extérieurs à l'organisation Security Operations.	N/A

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre du rôle [name]	Description	Contient des rôles
Activateur d'accès spécial de sécurité [sn_si.special_access_enabler]	Fournit un rôle d'accès spécial à un utilisateur extérieur à l'organisation Security Operations pour des incidents de sécurité spécifiques.	N/A
Gestionnaire de lecture d'accès spécial aux incidents de sécurité [sn_si.special_access_read_manager]	Gérez le rôle Accès spécial aux incidents de sécurité [sn_si.special_access]. Utilisez ce rôle pour modifier le champ **Accès en lecture** du formulaire d'incident de sécurité. Ce rôle peut être affecté par sn_si.admin.	sn_si.special_access_enabler
Gestionnaire de rédacteur d'accès spécial aux incidents de sécurité [sn_si.special_access_write_manager]	Gérez le rôle Accès spécial aux incidents de sécurité [sn_si.special_access]. Utilisez ce rôle pour modifier le champ **Accès privilégié** dans le formulaire d'incident de sécurité. Ce rôle peut être affecté par sn_si.admin.	sn_si.special_access_enabler

Travaux planifiés installés

Tâche planifiée	Description
Rechercher les observables d'incident de sécurité	Effectue une recherche d'observables selon un calendrier défini par l'utilisateur.

Tables installées

Table	Description
Configuration du flux d'actualités [sn_si_feed_configuration]	Enregistrements de configuration utilisés pour définir le contenu affiché dans le flux d'actualités des incidents de sécurité.
Règle d'affectation de revue post-incident [sn_si_pir_condition]	Automatise la sélection des participants à une enquête d'examen post-incident lorsqu'un incident de sécurité est fermé.
Incident de sécurité [sn_si_incident]	Stocke un incident de sécurité, les réponses à l'incident, toutes les tâches connexes, les changements, les problèmes et les incidents liés à cet incident de sécurité.
Vecteurs d'attaque des incidents de sécurité [sn_si_attack_vector]	Options de vecteur d'attaque.
Journal d'audit des incidents de sécurité [sn_si_audit_log]	Stocke les journaux d'audit d'enrichissement des incidents de sécurité.
Calculateur d'incidents de sécurité [sn_si_calculator]	Calculateur permettant de définir certains champs d'incident de sécurité lorsque certaines conditions sont remplies.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Groupe de calculateurs d'incidents de sécurité [sn_si_calculator_group]	Un regroupement de calculateurs d'incidents de sécurité. L'ordre du groupe de calculateurs détermine quel groupe est évalué en premier, et dans chaque groupe, un calculateur au maximum est utilisé.
Pare-feu d'enrichissement des incidents de sécurité [sn_si_enrichment_firewall]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques à Palo Alto Networks Firewall.
Enrichissement des incidents de sécurité Résultats des programmes malveillants [sn_si_enrichment_malware]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques aux programmes malveillants.
Enrichissement des incidents de sécurité Statistiques réseau [sn_si_enrichment_network_statistics]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques aux statistiques de réseau.
Enrichissement des incidents de sécurité Processus en cours [sn_si_enrichment_running _processes]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques aux processus en cours d'exécution.
Enrichissement des incidents de sécurité Services d'exécution [sn_si_enrichment_running_service]	S'étend à partir de la table de base (sn_sec_cmn_enrichment_data_base) et inclut tous les enregistrements d'enrichissement spécifiques aux services en cours d'exécution.
Recherche d'e-mails d'incidents de sécurité [sn_si_m2m_incident_email_search]	Mappe les enregistrements de recherche d'e-mails aux incidents de sécurité.
Importation des incidents de sécurité [sn_si_incident_import]	Table à importer pour les incidents de sécurité. Utilisée pour créer des incidents de sécurité à partir de systèmes externes.
Définition de processus d'incident de sécurité [sn_si_process_definition]	Stocke la configuration des flux de processus des incidents de sécurité.
Sélecteur de définitions de processus d'incidents de sécurité [sn_si_process_definition_selector]	Stocke la définition du processus d'incident de sécurité à utiliser pour les incidents de sécurité.
Incident de sécurité associé au ticket du service clientèle [sn_si_m2m_incident_customerservice_case]	Mappe les tickets du service clientèle et les incidents de sécurité
Données d'enrichissement associées aux incidents de sécurité [sn_si_m2m_incident_enrichment]	Mappe les incidents de sécurité et les enregistrements de données d'enrichissement connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Tâche Réponse aux incidents de sécurité [sn_si_task]	Gère les sous-tâches liées à la gestion d'un incident de sécurité. Ces tâches peuvent être affectées au personnel de sécurité ou à des personnes d'autres départements pour gérer la communication interdépartementale et le suivi des tâches.
Modèle de tâche Réponse aux incidents de sécurité [sn_si_task_template]	Utilisé pour créer une Réponse aux incidents de sécurité tâche. Ces modèles sont souvent utilisés dans les entrées de catalogue, afin de créer automatiquement un ensemble de sous-tâches appropriées pour un type particulier d'incident de sécurité.
Document Runbook des incidents de sécurité [sn_si_runbook_document]	Associe les conditions ou les filtres d'incident de sécurité à un article de la base de connaissances. Utilisée pour spécifier les procédures de Runbook pour la correction des incidents de sécurité.
Modèle d'incident de sécurité [sn_si_incident_template]	Utilisée pour créer un incident de sécurité. Ces modèles sont souvent utilisés dans les entrées de catalogue pour créer un incident de sécurité prédéfini.
Demande de sécurité [sn_si_request]	Une demande liée à la sécurité adressée à l'équipe de sécurité.
Demande d'analyse de sécurité [sn_si_scan_request]	Une demande de recherche de menace.
Calculateur de gravité sn_si_severity_calculator	Définit les valeurs de gravité, d'impact, de risque et de criticité d'un incident de sécurité.
Tâche Utilisateur concerné [sn_si_m2m_task_affected_user]	Une table de plusieurs à plusieurs associant les incidents de sécurité aux utilisateurs affectés.
Évaluateur de résultats de l'activité du workflow de modèle [sn_si_wf_activity_outcome_evaluator]	Mappe une option avec un script d'évaluation. Un nouveau flux secondaire peut être ajouté à un workflow de modèle pour définir un résultat de tâche de réponse plutôt que de le laisser un analyste le définir manuellement.

Autres tâches de configuration supplémentaires Réponse aux incidents de sécurité

Si vous êtes administrateur dans le domaine global, vous configurez la manière dont Réponse aux incidents de sécurité vous gérez les opérations quotidiennes.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Ces options sont standard dans de nombreuses applications de gestion des services et, en tant que telles, elles utilisent la terminologie de gestion des services. Par exemple, Demande est utilisé pour la tâche principale (c'est-à-dire l'incident de sécurité) et Tâche est utilisé pour les sous-tâches ou les tâches de réponse.

Si vous êtes administrateur dans un domaine inférieur au domaine global, vous pouvez afficher l'écran Configurations, mais vous ne pouvez pas modifier les paramètres.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Administration** > **Configuration**.
   Les options de configuration des applications sont organisées sous les onglets suivants :
   - L'onglet **Processus de gestion** contient des options pour configurer le cycle de vie de la demande, créer des catalogues et des demandes et configurer des notifications.
   - L'onglet **Affectation** contient des options pour configurer l'affectation manuelle et automatique.
   - L'onglet **Compléments** contient des options pour l'activation de la base de connaissances, des documents gérés et des activités de tâches.
2. Renseignez les champs de l'onglet **Processus de gestion** .

Écran de configuration : onglet Processus business

Champ	Description
Cycle de vie.	
Des notes de travail sont requises pour fermer ou annuler une demande ou une tâche	Activez cette option pour exiger de l'utilisateur qu'il saisisse des notes de travail avant qu'un incident de sécurité ou une tâche de réponse puisse être fermé ou annulé.
Copier les notes de travail de la tâche dans la demande	Activez cette option pour synchroniser les notes de travail de la tâche de réponse avec les notes de travail sur l'incident de sécurité. Ainsi, lorsque des notes de travail sont ajoutées à la tâche, les mêmes notes de travail apparaissent dans l'incident de sécurité parent.
Catalogue et création de demande	
Créer ou mettre à jour les demandes par e-mail entrant	Activez cette option pour créer ou mettre à jour des incidents de sécurité à partir d'e-mails entrants.
Les demandes sont créées avec	Sélectionnez le **catalogue ou le formulaire standard** pour activer le catalogue et permettre la publication automatique des modèles d'incidents de sécurité dans le catalogue. Sélectionnez le **formulaire standard uniquement** pour désactiver le catalogue et désactiver la publication automatique des modèles d'incidents de sécurité dans le catalogue.
Les modèles créent un élément de catalogue dédié	Activez cette option pour activer la publication automatique des éléments de catalogue pour l'application.
Notifications	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Pour une demande ou une tâche, lorsque le champ sélectionné change, envoyer une notification aux destinataires	Vous pouvez configurer l'envoi de notifications à des destinataires spécifiques lorsque les champs sélectionnés dans les incidents de sécurité et les tâches de réponse changent. **a.** Dans **Table**, sélectionnez **Demande (incident de sécurité)** ou **Tâche (tâche de réponse).** **b.** Dans **Champ**, sélectionnez le champ à utiliser pour générer des notifications. Lorsqu'un changement est apporté au champ sélectionné, une notification est envoyée aux destinataires identifiés. **c.** Dans **Destinataires**, sélectionnez un ou plusieurs destinataires. **d.** Si vous sélectionnez **un utilisateur spécifique** ou **un groupe spécifique**, vous êtes invité à sélectionner un utilisateur ou un groupe. **e.** Pour définir d'autres notifications à l'aide d'autres champs ou destinataires, répétez les étapes précédentes pour le prochain ensemble de paramètres de notification. **f.** Pour supprimer une notification, cliquez sur l'icône du ⊖ située à droite de la notification.

3. Cliquez sur l'onglet **Affectation** et remplissez les champs.

Écran de configuration : onglet d'affectation

Champ	Description
Méthode d'affectation des demandes	Sélectionnez la méthode d'affectation des incidents de sécurité : ○ **à l'aide de l'affectation automatique** : les incidents de sécurité sont automatiquement affectés. ○ **à l'aide d'un workflow** : les incidents de sécurité sont affectés par le workflow sélectionné. ○ **manuellement** : les incidents de sécurité sont affectés manuellement.
Utilisez ce workflow pour affecter des demandes	Sélectionnez le workflow pour la répartition des incidents de sécurité. Ce champ **s'affiche lorsque l'utilisation d'un workflow** est sélectionnée dans la liste **Méthode d'affectation des demandes** .
Méthode d'affectation des tâches	Sélectionnez la méthode d'affectation des tâches de réponse : ○ **à l'aide de l'affectation automatique** : les tâches de réponse sont automatiquement affectées. ○ **à l'aide d'un workflow** : les tâches de réponse sont affectées par le workflow sélectionné. ○ **manuellement** : les tâches de réponse sont affectées manuellement.
Utilisez ce workflow pour affecter des tâches	Sélectionnez le workflow pour l'affectation des tâches de réponse. Ce champ **s'affiche lorsque l'utilisation d'un workflow** est sélectionnée dans la liste **Méthode d'affectation des tâches** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Affecter les demandes ou les tâches en fonction des zones de couverture des zones d'affectation	Activez cette option pour limiter l'affectation des incidents de sécurité et des tâches de réponse aux groupes qui couvrent l'emplacement de la tâche.
Ordonnancement	
La sélection automatique d'agents tient compte du fuseau horaire pour les tâches	Activez cette option pour tenir compte du fuseau horaire de l'agent lors de l'affectation d'une tâche. Ce champ s'affiche lorsque l'affectation automatique est sélectionnée pour les incidents de sécurité ou les tâches de réponse.
Facteurs supplémentaires	
La sélection automatique d'agents tient compte de leur localisation	Activez cette option pour donner la préférence aux agents plus proches de l'emplacement de la tâche lors de l'affectation de tâches. Ce champ s'affiche lorsque l'affectation automatique est sélectionnée pour les incidents de sécurité ou les tâches de réponse.
La sélection automatique d'agents pour des tâches requiert qu'ils aient des compétences	Sélectionnez le degré de correspondance des compétences de l'agent avec une tâche lors de la détermination de l'affectation automatique. ○ Sélectionnez **tout** pour exiger qu'un agent affecté possède toutes les compétences nécessaires pour effectuer la tâche. Un agent qui n'a qu'une seule compétence est éliminé. ○ **Sélectionnez-en quelques-unes** si vous voulez des agents qui possèdent la plupart des compétences requises pour effectuer la tâche. ○ Sélectionnez **Aucun** si vous souhaitez affecter automatiquement des agents sans tenir compte des compétences. Ce champ s'affiche lorsque l'affectation automatique est sélectionnée pour les incidents de sécurité ou les tâches de réponse.
Tentative de sélection automatique d'affecter le même agent à toutes les tâches d'une demande	Activez cette option pour affecter automatiquement toutes les tâches de réponse pour un incident de sécurité au même agent.

4. Cliquez sur l'onglet **Compléments** et remplissez les champs.

Écran de configuration — Onglet Compléments

Champ	Description
Documentation	
Activer une base de connaissances dédiée	Activez cette option pour activer la base de connaissances pour Réponse aux incidents de sécurité.
Activer les documents gérés	Activez cette option pour ajouter une liste connexe aux documents gérés.
Activer les activités de la tâche	Activez cette option pour consigner les interactions et les communications liées aux tâches, telles que les appels téléphoniques et les e-mails.

5. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Verrouiller l'administration de la sécurité

Pour protéger les enquêtes et préserver la confidentialité des incidents de sécurité, vous pouvez restreindre Réponse aux incidents de sécurité l'accès aux rôles et ACL spécifiques à la sécurité. L'accès peut être restreint aux administrateurs non liés à la sécurité, sauf si vous leur autorisez expressément l'entrée.

Avant de commencer

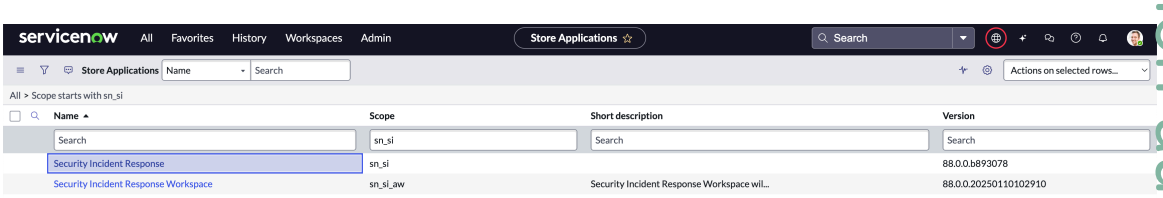
Lorsque l'application Réponse aux incidents de sécurité est activée, le rôle sn_si.admin est attribué par défaut à l'utilisateur Administrateur système. L'administrateur système est le seul administrateur qui peut configurer des groupes et des utilisateurs de sécurité.

Un rôle de sécurité est requis pour avoir accès aux fonctionnalités et aux Réponse aux incidents de sécurité enregistrements.

Rôle requis : sn_si.admin

Procédure

1. Une fois le Réponse aux incidents de sécurité module d'extension activé, un utilisateur disposant du rôle admin affecte le rôle Administrateur inclus dans le périmètre (sn_si.admin) à au moins un utilisateur.
2. L'utilisateur disposant du rôle administrateur passe au périmètre de l'incident de sécurité.
3. Accédez à la **Tous** > **sys_store_app.liste**.
4. Saisissez **sn_si** dans le champ **Champ d'application** .



5. Cliquez sur **Réponse aux incidents de sécurité**.
6. Faites défiler la page vers le bas jusqu'aux **liens connexes** et cliquez sur **Supprimer du rôle contenu par administrateur**.
7. Déconnectez-vous puis reconnectez-vous.
   L'utilisateur administrateur ne peut pas accéder à l'application Réponse aux incidents de sécurité .

Information associée

Administration d'application

Gérer l'accès restreint pour l'appelant

La fonctionnalité Accès restreint pour l'appelant (RCA) permet à un administrateur de définir l'accès entre périmètres d'une application ou d'une ressource d'application et d'autoriser ou de refuser les demandes d'accès. Cette fonctionnalité est activée Réponse aux incidents de sécurité par défaut afin que les analystes de sécurité puissent protéger les informations sensibles liées à la sécurité.

Un champ appelé **Accès pour l'appelant** a été ajouté à toutes les tables et inclut le script dans Réponse aux incidents de sécurité, et le champ est attribué par défaut au **suivi de l'appelant**. Ce paramètre signifie que les périmètres de l'application sont autorisés à accéder aux tables et aux includes de Réponse aux incidents de sécurité script. Toutefois, un enregistrement de suivi est créé pour chaque enregistrement et stocké dans la table Privilège d'accès restreint pour l'appelant [sys_restricted_caller_access].

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Soyez prudent lorsque vous passez des enregistrements de **Suivi de l'appelant** à **Appelant restreint.** Les enregistrements avec cet état ne sont pas accessibles tant qu'un administrateur n'autorise pas manuellement l'accès. L'administrateur doit accéder à **Applications système** > **Accès restreint à l'application pour l'appelant**, localisez la table ou l'include de script pour lequel l'accès a été demandé et modifiez le champ **État** de **Demandé** à **Autorisé**.

Information associée

Paramètres des privilèges d'accès restreint pour l'appelant

Définir le périmètre de l'application, la ressource d'application et l'accès aux événements

Exécuter des tests de démarrage rapide pour Réponse aux incidents de sécurité

Validez que cela Réponse aux incidents de sécurité fonctionne toujours après avoir apporté des modifications de configuration, telles que l'application d'une mise à niveau ou le développement d'une application. Copiez et personnalisez ces tests de démarrage rapide à effectuer lorsque vous utilisez des données spécifiques à votre instance.

Les tests de démarrage rapide pour Réponse aux incidents de sécurité nécessitent l'activation du module d'extension Réponse aux incidents de sécurité (com.snc.security_incident) et le chargement des données de démonstration.

Tests Réponse aux incidents de sécurité

Test	Description	Version
SIR : créer un incident de sécurité	Déterminez si un utilisateur peut créer un incident de sécurité depuis le formulaire d'incident de sécurité.	Madrid
SIR : créer un incident de sécurité via le catalogue d'incidents de sécurité	Déterminez si un utilisateur peut créer un incident de sécurité depuis le catalogue.	Madrid
SIR : cycle de vie des incidents de sécurité	Validez les tâches de réponse du workflow de violation de la politique.	Madrid
SIR : test de configuration prêt à l'emploi des évaluations PIR	Utilisez ce test pour valider les évaluations PIR et les configurations du système de base.	Tokyo
SIR : tests de configuration conditionnels des évaluations PIR	Vérifiez que les incidents de sécurité correspondant à la règle conditionnelle obligatoire ne sont pas fermés avant que l'évaluation post-incident ne soit terminée. Vérifiez que les incidents de sécurité correspondant à la règle conditionnelle facultative peuvent être fermés avant que l'évaluation post-incident ne soit terminée.	Tokyo

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux incidents de sécurité (suite)

Test	Description	Version
	Vérifiez que les évaluations ne sont pas générées pour les incidents de sécurité qui ne correspondent à aucune règle.	
SIR : expérience de temps d'exécution PIR	Vérifiez que les rapports PIR sont configurés et joints aux incidents de sécurité selon la nouvelle conception.	Tokyo
SIR : expérience de conception PIR	Vérifiez que l'incident de sécurité est mappé au modèle de rapport en fonction de la configuration de l'administrateur.	Tokyo
SIR : lier l'incident de sécurité à un incident de sécurité majeur	Liez un incident de sécurité à un incident de sécurité majeur existant et validez les données de l'incident de sécurité repris sur l'incident de sécurité majeur.	Tokyo
SIR : promouvoir l'incident de sécurité comme incident de sécurité majeur	Promouvoir un incident de sécurité en tant qu'incident de sécurité majeur et valider les données de l'incident de sécurité déployé jusqu'à l'incident de sécurité majeur.	Tokyo
SIR : proposer un incident de sécurité comme incident de sécurité majeur	Proposez un incident de sécurité en tant qu'incident de sécurité majeur et validez les données de l'incident de sécurité déployé jusqu'à l'incident de sécurité majeur.	Tokyo
SIR : cycle de vie des incidents de sécurité	Validez le cycle de vie d'un incident de sécurité avec le workflow de tâches de réponse en cas de violation de politique.	Yokohama
SIR : créer un ticket de sécurité	Créez un ticket de sécurité à partir du formulaire Incident de sécurité.	Yokohama
Vérifier que seuls les membres autorisés peuvent accéder à l'incident de sécurité une fois que l'option Appliquer la restriction est activée	Vérifiez que seuls les membres autorisés peuvent accéder à l'incident de sécurité une fois que l'option Appliquer la restriction est activée.	Yokohama
Vérifiez que l'incident de sécurité activé avec « Appliquer la restriction » n'est visible pour aucun utilisateur	Vérifiez que l'incident de sécurité activé avec « Appliquer la restriction » n'est visible par aucun utilisateur.	Yokohama
Valider l'accès en lecture	Validez l'accès à l'affichage.	Yokohama

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests Réponse aux incidents de sécurité (suite)

Test	Description	Version
Valider l'accès en écriture	Validez l'accès en modification.	Yokohama
Espace de travail SIR : accès en lecture	Vérifiez que l'utilisateur avec accès en lecture peut voir l'incident de sécurité sans disposer des rôles de sécurité, même dans l'espace de travail.	Yokohama
Espace de travail SIR : accès en écriture	Vérifiez que l'utilisateur disposant d'un accès en écriture peut mettre à jour l'incident de sécurité sans disposer de rôles de sécurité.	Yokohama
Espace de travail SIR : créer un incident de sécurité	Créer un incident de sécurité à partir de l'espace de travail.	Yokohama
Espace de travail SIR : créer une tâche de réponse	Créez une nouvelle tâche de réponse à partir d'un incident de sécurité existant.	Yokohama
Now Assist pour Sécurité : synthèse des incidents de sécurité actifs	Résumez un incident de sécurité actif et validez les sections affichées.	Zurich
Now Assist pour Sécurité : incident de sécurité Summarization_Share aux notes de travail	Partagez le résumé généré dans les notes de travail.	Zurich
Now Assist pour Sécurité : synthèse des incidents de sécurité fermés	Résumez un incident de sécurité clôturé et validez les sections affichées.	Zurich

Information associée

Tests de démarrage rapide

Référence de l'assistant de configuration

L'assistant de configuration vous guide tout au long des étapes à suivre pour configurer le système de Réponse aux incidents de sécurité base. Cette section fournit des informations supplémentaires sur les étapes compliquées pour lesquelles vous pourriez avoir besoin de plus d'explications.

Créer une définition de Réponse aux incidents de sécurité processus

Vous pouvez créer une définition de processus pour définir la façon dont les incidents de sécurité passent d'un état à l'autre. Les définitions de processus permettent aux centres de services et aux utilisateurs finaux de suivre le problème tout au long de son cycle de vie.

Avant de commencer
Rôle requis : sn.si_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Administration** > **Définition de processus**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient.

Création de définitions de processus

Champ	Description
Nom	Nom de l'enregistrement qui décrit le processus codé dans le fichier d'include de script. Le nom s'affiche sous forme de choix dans la liste **sélecteur de définition de processus** .
Include de script	Nom (y compris le préfixe `sn_si`.) de l'include de script contenant la définition du processus. Le script doit se trouver dans le périmètre de l'application Incident de sécurité (`sn_si`). Consultez Créer un script include de définition de processus personnalisé Réponse aux incidents de sécurité pour plus d'informations. Si ce champ ne contient pas de nom d'include de script valide, la définition de ProcessDefinition_NIST_Stateful par défaut est utilisée.
Description	Informations utiles sur l'include de script.
Ordre	Détermine la position dans la liste de définition du processus.
Actif	Lorsque cette option est cochée, cette définition de processus peut être sélectionnée à partir de la page **Sélecteur de définition de processus** .

4. Cliquez sur **Envoyer**.

Information associée

Sélection du processus de Security Incident Response

Comprendre la définition du processus de Security Incident Response

Comprendre la définition du processus de Security Incident Response

Réponse aux incidents de sécurité Définition du processus Remplace les flux d'états et fournit aux utilisateurs finaux et aux centres de services l'état d'un problème. Une définition de processus permet de suivre le problème tout au long de son cycle de vie. Réponse aux incidents de sécurité est une application de Gestion des services (SM) qui possède son propre ensemble d'états. Les états non valides sont signalés comme faisant partie de Sélection du processus.

Définition du processus de Réponse aux incidents de sécurité

La définition de processus par défaut (état NIST) définit les états d'incident suivants :

Remarque : Les états disponibles varient en fonction de l'état actuel de l'incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

États de définitions des processus d'incidents de sécurité

État	Description
Brouillon	L'initiateur de la demande ajoute des informations sur l'incident de sécurité, mais celles-ci ne sont pas encore prêtes à être traitées.
Analyse	L'incident a été affecté et le problème est en cours d'analyse.
Contenir	Le problème a été identifié et le personnel de sécurité s'efforce de le contenir et de limiter les dégâts. Ces actions peuvent inclure la mise hors ligne des serveurs, la déconnexion de l'équipement d'Internet et la vérification de l'existence de sauvegardes.
Éradiquer	Le problème a été maîtrisé et le personnel de sécurité prend des mesures pour le résoudre.
Récupérer	Le problème est résolu et l'état de préparation opérationnelle des systèmes affectés est en cours de vérification.
Revue	L'incident de sécurité est terminé et tous les systèmes ont repris leur fonctionnement normal, mais un examen post-incident reste nécessaire.
Fermé	L'incident est terminé, mais avant qu'un incident de sécurité puisse être fermé, vous devez renseigner les informations dans l'onglet **Informations sur la fermeture** .

Définitions des processus de tâche d'incident de sécurité

Les définitions de processus suivantes sont utilisées pour les tâches d'incident de sécurité.

États de définitions des processus de tâches

État	Description
Prêt	La tâche est prête à être traitée une fois affectée à un agent.
Affecté	La tâche est affectée à un agent.
Travail en cours	L'agent affecté travaille sur la tâche.
Terminé	La tâche est terminée.
Annulé	La tâche a été annulée.

Le NIST prend en charge les deux modèles suivants :

- **NIST Stateful**

  Cette définition de processus permet aux analystes de passer d'un état à un autre dans un ordre séquentiel sans ignorer aucune étape. Par exemple, si l'analyste commence par l'état **Brouillon** , l'ordre séquentiel de cette définition de processus est **Brouillon**>**Analyse**>**Contenir**>**Éradiquer**>**Récupérer**. Ainsi, la définition du processus avec

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

état NIST est unidirectionnelle et permet aux analystes de progresser uniquement vers les états directs.

Voici un autre exemple : si l'analyste commence par l'état Analyse, l'ordre séquentiel de cette définition de processus est **Analyse**>**Contenir**>**Éradiquer**>**Récupérer**.

- **NIST Open**

  Cette définition de processus permet aux analystes de passer d'un état à un autre, en avant ou en arrière. Par exemple, si l'analyste commence par l'état **Analyse** , l'ordre de la définition du processus peut être **Analyse**>**Contenir**>**Éradiquer**>**Récupérer** ou **Analyse**>**Brouillon**. Ainsi, la définition du processus NIST Open est bidirectionnelle et permet aux analystes de passer à des états en avant ou en arrière en fonction de leurs besoins.

Sélection du processus de Security Incident Response

Réponse aux incidents de sécurité La sélection de processus répertorie les processus présentant des états non valides pour les incidents de sécurité et les tâches de réponse.

Un administrateur peut corriger l'incident ou la tâche pour rétablir des états valides manuellement ou à l'aide d'un script. Une liste connexe vide (aucun incident ; aucune tâche) indique que chaque tâche active est dans un état valide. Les états disponibles varient en fonction de l'état actuel de l'incident. Pour plus d'informations, consultez Corriger un état d'incident ou de tâche de sécurité non valide avec la définition du processus.

Sélectionner une définition de Réponse aux incidents de sécurité processus

Vous pouvez sélectionner la définition de processus à utiliser pour les états appropriés pour les incidents de sécurité et les tâches de réponse de votre entreprise.

Avant de commencer

Rôle requis : admin et sn_si.admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tous** > **Security Incident Response** > **Administration** > **Sélection du processus**.
2. Cliquez sur l'icône de recherche pour répertorier les définitions de processus disponibles.



3. Sélectionnez une définition de processus.
4. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un script include de définition de processus personnalisé Réponse aux incidents de sécurité

Créez un script de définition de processus personnalisé pour les états appropriés des incidents de sécurité et des tâches de réponse de votre entreprise.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Le sn_si. Le script principal de ProcessDefinition comprend des contrôles, des définitions de processus. **La définition de processus** détermine quelle définition est utilisée (à l'aide de la **sélection de processus**). Il appelle le fichier d'include de script approprié pour déterminer les états initiaux et les transitions pour les incidents de sécurité et les tâches de réponse.

Procédure

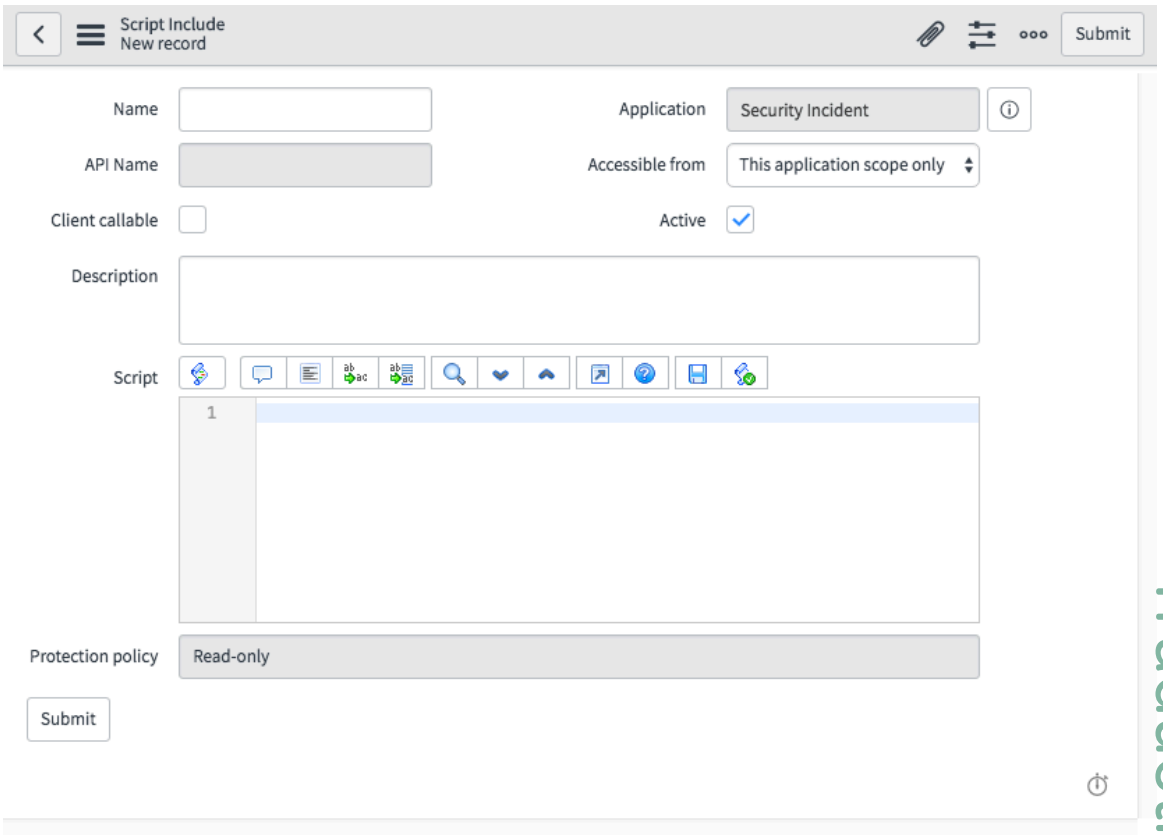
1. Accédez à la **Tous** > **Définition du système** > **Includes de script**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient.

Création de définitions de processus

Champ	Description
Nom	Nom de l'include de script.
Nom de l'API	Créé en fonction du nom de l'include de script.
Client joignable	Met l'include de script à la disposition des scripts clients, des filtres de liste et de rapport, des qualificatifs de référence ou, s'il est spécifié, dans le cadre de l'URL.
Application	Incident de sécurité
Accessible depuis	Choisissez **Ce périmètre de l'application uniquement** .
Actif	Lorsque cette option est cochée, cet include de script peut être sélectionné à partir de la page **Définition du processus** .
Description	Informations utiles sur l'include de script.
Script	Définit le script côté serveur à exécuter lorsqu'il est appelé à partir d'autres scripts. Le script doit définir une seule classe JavaScript ou une fonction globale. Le nom de classe ou de fonction doit correspondre au champ Nom. Pour plus d'informations sur le contenu des scripts, reportez-vous à la section Script include de définition de processus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Envoyer**.

Information associée

Script include de définition de processus

Script include de définition de processus

L'include de script de définition de processus fournit des méthodes pour définir une définition de processus.

Implémentez les constantes, les attributs, les tableaux et les appels de méthode décrits ici pour personnaliser un script include de définition de processus.

Où l'utiliser

Utilisez cet include de script pour créer une définition de processus.

Corps du script include

Le corps du script include est composé de trois sections :

- Constantes : définitions de l'état initial
- Tâche Security Incident and Response : tableaux de définition de processus
- Appels de méthode : récupération d'informations

Constantes

Les constantes sont utilisées pour définir les états initiaux des incidents de sécurité et des tâches de réponse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'utilisation de constantes est facultative mais encouragée pour la lisibilité. Par exemple :

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Qui sont utilisées ultérieurement par les méthodes suivantes :

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

L'ensemble suivant de constantes définit les états des incidents de sécurité et des tâches de réponse.

Chaque tableau contient également la définition des états disponibles lorsque l'incident ou la tâche est dans un état spécifique.

Par exemple :

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

L'exemple est un tableau d'objets. Chaque objet définit un état et des états de transition possibles.

L'ordre de l'objet de l'état détermine l'ordre souhaité pour le flux.

Lorsque la tâche est à l'état « Brouillon » (valeur 1), les états possibles sont : 1 (Brouillon, ce qui n'a pas changé) et 10 (Prêt, la prochaine étape du processus).

Il n'y a pas de limite au nombre de transitions hors d'un état. Les états « Fermé terminé » et « Annulé » sont des états finaux et n'ont donc pas de transitions d'état possibles.

L'ordre des attributs dans l'objet n'a pas d'importance. Si cela rend la définition plus claire, mettez l'étiquette en premier.

Attributs

Les attributs requis dans un objet de définition d'état sont les suivants :

- État : valeur numérique de l'état
- Étiquette : texte lisible par l'homme associé à l'état
- Choix : un tableau de valeurs d'état vers lesquelles l'état peut effectuer la transition (détermine le contenu de la liste déroulante d'état)

Les attributs facultatifs sont les suivants :

- obligatoire : liste des ID de champs qui deviennent obligatoires dans cet état
- readonly : liste des ID de champs qui passent en lecture seule dans cet état

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- visible : liste des ID de champs qui deviennent visibles dans cet état
- notmandatory : liste des ID de champs qui deviennent non obligatoires dans cet état
- notvisible : liste des ID de champs qui ne seraient plus visibles dans cet état

Remarque :

Si des attributs facultatifs sont utilisés, il est de la responsabilité de l'auteur de s'assurer que les champs sont rendus visibles/invisibles, obligatoires/non obligatoires, visibles/masqués ou en lecture seule de manière appropriée entre les états.

Par exemple, masquer un champ dans un état ne le rend pas visible dans un autre état ultérieurement, sauf si l'attribut « visible » est utilisé.

Tableaux de définition de flux de processus

Pour définir les informations affichées dans le formateur de flux de processus (barre en haut des formulaires de tâche Security Incident et Response), le système a besoin d'informations sur ce qu'il faut afficher pour chaque état.

Par exemple :

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ", description:"<p>Security Incident Response Task is in draft</p>"},
{label:"Ready", condition:"state=10^EQ", description:"<p>Security Incident Response Task is ready to be assigned</p>"},
{label:"Assigned", condition:"state=16^EQ", description:"<p>Security Incident Response Task is assigned</p>"},
{label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work has started on this Security Incident Response Task</p>"},
{label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ", description:"<p>Security Incident Response Task is complete</p>"},
],
```

Le tableau TASK_PF est une collection d'étiquettes, de conditions et de descriptions utilisées pour déterminer le texte affiché dans la barre du formateur de processus (y compris l'ordre et l'activité).

Dans l'exemple, le texte « Prêt » est le deuxième élément affiché. Elle est mise en surbrillance lorsque la tâche satisfait à la condition « state=10^EQ ».

Lorsque le pointeur survole le texte, la description « La tâche Réponse aux incidents de sécurité est prête à être affectée » s'affiche.

Remarque :

Les états peuvent être combinés en un seul état de formateur.

Dans l'exemple, les états « Fermé terminé » et « Annulé » s'affichent comme « Fermé » dans la barre supérieure.

Appels de méthodes

Les méthodes suivantes doivent être présentes dans l'include de script car elles sont utilisées par sn_si. Définition du processus :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de retour	Résumé de la méthode	Description
Chaîne	getInitialIncidentState : fonction()	Renvoyer la valeur numérique de l'état de l'incident initial
Chaîne	getInitialTaskState : fonction() :	Renvoyer la valeur numérique de l'état de la tâche initiale
Tableau de chaîne	getIncidentStates : fonction() :	Renvoyer le tableau de l'état de l'incident
Tableau de chaîne	getTaskStates : fonction() :	Renvoyer le tableau de l'état de la tâche
Tableau d'objets	getIncidentProcessFlows : fonction() :	Renvoyer le tableau de définition du flux de processus de l'incident
Tableau d'objets	getTaskProcessFlows : fonction() :	Renvoyer le tableau de définition du flux de processus de tâche

L'ensemble de méthodes suivant est appelé chaque fois qu'un incident ou une tâche est mis à jour et permet de prendre des mesures sur des transitions de changement spécifiques.

Type de retour	Résumé de la méthode	Description
nul	performIncidentStateChange : fonction(current, précédent)	Dans les exemples, cette méthode est utilisée pour définir les valeurs liées à SM et s'assurer qu'un incident passe de l'état « Brouillon » une fois qu'une personne lui est affectée.
nul	performTaskStateChange : fonction (current, previous)	Dans l'exemple, cette méthode est utilisée pour mettre à jour les horodatages (lors de l'affectation et de la fermeture) et faire passer la tâche de « Prêt » à « Affecté » une fois le champ assigned_to renseigné.

Les mêmes actions effectuées par ces deux méthodes peuvent être accomplies à l'aide d'une règle métier. En les définissant dans l'include de script, le changement de définition de processus est facilité.

Corriger un état d'incident ou de tâche de sécurité non valide avec la définition du processus

Un administrateur peut corriger l'incident ou la tâche de sécurité sur des états valides, manuellement ou à l'aide d'un script. Les états disponibles varient en fonction de l'état actuel de l'incident.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Une fois que vous avez changé de définition de processus, la nouvelle définition peut ne pas prendre en charge certains des anciens états. Pour corriger les états d'incident ou de tâche orphelins, vous pouvez modifier votre définition de processus, modifier votre script include ou ouvrir manuellement chaque incident ou tâche pour mettre à jour l'état. En général, la mise à jour de l'état (qui peut être effectuée en masse) est la solution la plus simple.

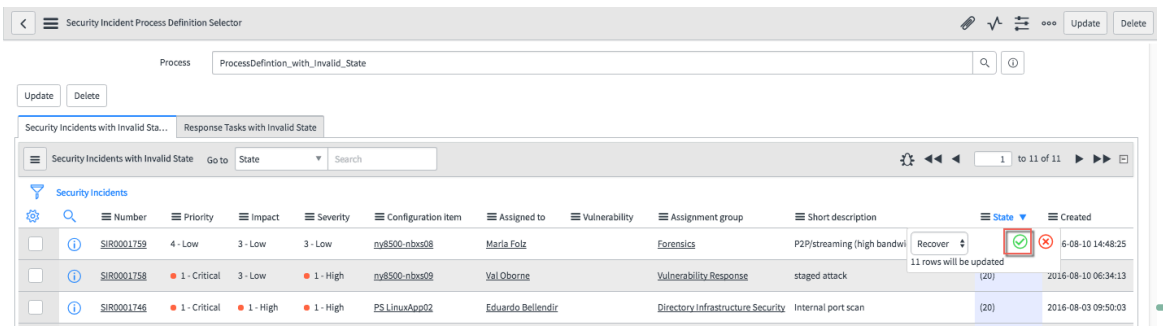
Pour changer les états en bloc, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Sélection du processus**.
2. Mettez en surbrillance le champ **État** pour les incidents ou les tâches que vous souhaitez modifier.
3. Double-cliquez sur le champ **État** du premier enregistrement, sélectionnez le nouvel **état,** puis cliquez sur la coche verte (coche) pour terminer la modification.



4. Cliquez sur **Mettre à jour**.

Créer un groupe d'incidents de sécurité

Configurez un groupe d'incidents de sécurité et affectez-lui les rôles et les utilisateurs appropriés.

Avant de commencer

Rôles requis :

- Si vous disposez du rôle user_admin, vous pouvez créer des groupes d'affectation d'incidents de sécurité.
- Si vous disposez du rôle sn_si.admin, vous pouvez créer et modifier des groupes d'affectation d'incidents de sécurité.

Pourquoi et quand exécuter cette tâche

Les utilisateurs d'un groupe héritent les rôles du groupe. Il est donc inutile d'affecter des rôles à chaque utilisateur séparément.
Il est recommandé de créer autant de groupes que nécessaire dans votre organisation. Il est également recommandé de créer un groupe pour les administrateurs et de n'affecter le rôle administrateur qu'à ce groupe.

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Groupes** ou **Incident de sécurité** > **Configuration** > **Groupes**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Remarque :

Pour plus d'informations, consultez Créer un groupe d'utilisateurs .

4. Veillez à sélectionner le type **d'incident de sécurité** pour ce groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Si le champ **Type** n'est pas visible, configurez le formulaire pour l'ajouter.

b. Cliquez sur l'icône de verrouillage à côté du champ **Type**.

c. Cliquez sur  de recherche de référence (icône de recherche).

d. Recherchez et sélectionnez le type **d'incident de sécurité** .

5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
6. Dans la liste connexe **Rôles** , ajoutez les rôles que chaque membre de ce groupe reçoit.
   Par exemple, si vous créez un groupe pour Réponse aux incidents de sécurité les membres de l'équipe, ajoutez sn_si.analyst. Si vous créez un groupe pour Réponse aux incidents de sécurité les administrateurs, ajoutez sn_si.admin.
7. Dans la liste connexe **Membres du groupe** , ajoutez des utilisateurs à ce groupe.
8. Cliquez sur **Mettre à jour**.

Créer un groupe de calculateurs d'incidents de sécurité

Les groupes de calculateurs d'incidents de sécurité sont utilisés pour regrouper les calculateurs.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Configuration** > **Groupes de calculateurs d'incidents de sécurité**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Le nom du calculateur d'incident de sécurité.
Application	L'application qui contient l'enregistrement.
Ordre	Ordre dans lequel le calculateur d'incident de sécurité est exécuté. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Description	Description de ce groupe de calculateurs.
Créé par	Entrez le nom de l'utilisateur qui a créé

4. Cliquez sur **Envoyer**.

Créer un calculateur d'incident de sécurité

Les calculateurs d'incidents de sécurité vous permettent de calculer la gravité d'un incident de sécurité en fonction de formules prédéfinies. Vous pouvez définir vos propres calculateurs d'incident de sécurité, selon vos besoins.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Configuration** > **Groupes de calculateurs d'incidents de sécurité**.
2. Cliquez sur le nom du groupe pour lequel vous souhaitez créer un calculateur, ou vous pouvez créer un groupe de calculateurs.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Le nom du calculateur d'incident de sécurité.
Groupe de calculateurs	Nom du groupe auquel ce calculateur appartient. **Remarque :** La création ou la modification du groupe de calculateurs devient disponible une fois que vous avez entré un **nom** et une **table**.
Table	Sélectionnez la table à utiliser pour ce calculateur. Lorsque vous ajoutez des calculateurs à des tables autres que Vulnérabilité [sn_vul_vulnerability] et Élément vulnérable [sn_vul_vulnerable_item], vous devez ajouter des règles métier et des actions d'interface utilisateur à ces tables. Pour afficher des exemples : ○ Accédez à la **Définition du système** > **Règles métier**et localisez la règle métier **Calculer la gravité** dans la table Élément vulnérable [sn_vul_vulnerable_item]. ○ Accédez à la **Interface utilisateur du système** > **Actions d'interface utilisateur**et localisez l'action d'interface utilisateur **Calculer la gravité** sur la table Élément vulnérable [sn_vul_vulnerable_item]. En outre, le rôle d'administrateur de vulnérabilité doit disposer d'options complètes de lecture, d'écriture (ou de save_as_template) sur n'importe quelle table utilisée par un calculateur pour voir correctement les valeurs à appliquer au modèle.
Application	L'application incluse dans le périmètre à laquelle le calculateur appartient.
Ordre	Ordre dans lequel le calculateur d'incident de sécurité s'exécute. Un calculateur avec une entrée d'ordre de 100 s'exécute avant un calculateur avec une entrée d'ordre de 200.
Actif	Allumez ou désactivez la calculatrice.
Description	Description de ce calculateur.

5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
   Les onglets **Conditions** et **Valeurs à appliquer s'affichent** .
6. Renseignez les champs de l'onglet **Conditions** comme il convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utiliser un groupe de filtres	Cochez cette case pour utiliser un groupe de filtres prédéfini ou créer un nouveau groupe de filtres pour définir les critères du calculateur.
Groupe de filtres	Sélectionnez le groupe de filtres à utiliser pour définir un calculateur. Ce champ s'affiche uniquement si vous avez coché la case **Utiliser les groupes de filtres** .
Utiliser une condition avancée	Cochez cette case pour indiquer qu'une condition de script est utilisée pour déterminer quand ce calculateur est appliqué. Lorsque vous cochez la case, un champ de scripting **de condition avancée** s'affiche. Si vous avez coché la case **Utiliser un groupe de filtres** , ce champ est masqué. **Remarque :** Avant de définir des conditions avancées et d'écrire des scripts pour déterminer quand les calculateurs d'incident de sécurité sont appliqués, revenez à la liste des calculateurs d'incident de sécurité. Explorez les enregistrements de calculateur fournis avec le système de base.
Condition	Définit les conditions de filtre de base pour déterminer si le calculateur est utilisé. Si vous avez coché l'une des cases **Utiliser le groupe de filtres** ou Utiliser des **conditions avancées** , ce champ est masqué.

7. Cliquez sur **l'onglet Valeurs à appliquer** et renseignez les champs du formulaire comme il convient. Vous avez le choix de créer un script pour définir les valeurs à appliquer au calcul ou de définir un modèle basé sur les champs de la table sélectionnée.

Champ	Description
Utiliser des valeurs de script	Cochez cette case pour définir des valeurs de champ avec un script.
Valeurs de script	Définit les valeurs auxquelles appliquer les calculs. Ce champ s'affiche uniquement si vous avez coché la case **Utiliser des valeurs de script** .
Modèle	Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**. Sélectionnez les champs et les valeurs que vous souhaitez utiliser pour le calculateur.

8. Lorsque vous avez terminé toutes les entrées, cliquez sur **Soumettre**.

Comprendre les calculateurs d'incidents de sécurité

Les calculateurs d'incidents de sécurité sont utilisés pour mettre à jour les valeurs d'enregistrement lorsque des conditions prédéfinies sont remplies. Les calculateurs sont regroupés en fonction des critères utilisés pour déterminer le mode de mise à jour des enregistrements.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le Réponse aux incidents de sécurité système de base comprend les groupes de calculateurs et les calculateurs d'incidents de sécurité suivants. Au sein de chaque groupe, c'est le premier calculateur qui correspond aux conditions qui est exécuté.

Calculateurs d'incidents de sécurité dans le système de base

Nom du groupe du calculateur d'incidents de sécurité	Calculateurs inclus dans le groupe	Description
Impact sur l'entreprise	Regrouper à partir des calculateurs de gravité	Ce calculateur délègue au calculateur de criticité de sécurité qui détermine la criticité en pondérant les valeurs d'autres champs.
Gravité	Impact sur l'entreprise	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions simple.
	Service critique affecté	Ce calculateur de gravité définit ses critères de sélection à l'aide d'une condition avancée. Si l'élément de configuration dans l'incident de sécurité est associé à un service d'entreprise hautement critique, les champs **Score de risque**, **Impact sur l'entreprise** et **Priorité** sont élevés comme défini par le calculateur.
	Changements de services critiques	Ce calculateur de gravité définit ses critères de sélection à l'aide d'une condition avancée. Si l'incident de sécurité remplit les conditions, un script s'exécute pour définir les niveaux auxquels les champs sont élevés. Si l'élément de configuration dans l'incident de sécurité est associé à un service d'entreprise très critique ou quelque peu critique, les champs **Score de risque**, **Impact sur l'entreprise** et **Priorité** sont élevés comme défini par le calculateur.
	Vecteurs d'attaques multiples	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions simple. Si l'élément de configuration de l'incident de sécurité est associé à des vecteurs d'attaque Web, par e-mail et par emprunt d'identité, le **score de risque**, l'impact **sur**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculateurs d'incidents de sécurité dans le système de base (suite)

Nom du groupe du calculateur d'incidents de sécurité	Calculateurs inclus dans le groupe	Description
		l'entreprise et les champs **Priorité** sont élevés comme défini par le calculateur.
	Définir la priorité avec la catégorie et les services	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions avancé. La priorité de l'incident de sécurité est définie sur **1 - Critique** lorsque les conditions suivantes sont remplies : • L'incident de sécurité a des services affectés associés et l'un d'eux est critique. • La catégorie d'incident de sécurité est l'une des suivantes : ◦ Déni de service ◦ Harponnage ◦ Activité du code malveillant **Remarque :** Ce calculateur est disponible dans le système de base lorsque vous disposez du niveau tarifaire Opération de sécurité de démarrage.
	Définir la priorité avec les observables	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions avancé. La priorité de l'incident de sécurité est définie sur**1 - Critique** lorsque les conditions suivantes sont remplies : • L'incident de sécurité a des services affectés associés et l'un d'eux est critique. • La catégorie d'incident de sécurité est l'une des suivantes : ◦ Déni de service ◦ Harponnage ◦ Activité du code malveillant • L'un des observables ou indicateurs associés a un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculateurs d'incidents de sécurité dans le système de base (suite)

Nom du groupe du calculateur d'incidents de sécurité	Calculateurs inclus dans le groupe	Description
		nombre d'observations qui dépasse deux observations avec des indicateurs actifs (c'est-à-dire que les observables ou les indicateurs sont confirmés comme étant mauvais à partir de plusieurs sources). **Remarque :** Ce calculateur est disponible dans le système de base lorsque vous disposez du niveau tarifaire Opération de sécurité avancée et que vous activez le module d'extension Flux de menaces.
Criticité de l'utilisateur	Obtenir la criticité de l'utilisateur	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions simple. Ce calculateur de gravité fait passer la criticité opérationnelle de l'utilisateur à **1 - Critique** lorsque le champ **Département** est changé en **Finances**.
	Obtenir la criticité du groupe d'utilisateurs	Ce calculateur de gravité définit ses critères de sélection à l'aide d'un générateur de conditions avancé. Ce calculateur de gravité fournit un exemple de calculateur qui s'exécute sur les données d'une liste connexe.

Traduction automatique

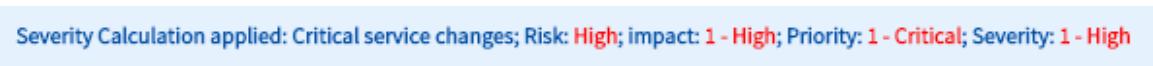
Calculateurs de gravité

Lorsque vous créez un incident de sécurité, les champs **Score de risque**, **Impact sur l'entreprise** et **Priorité** contiennent des valeurs par défaut. Lorsque vous enregistrez l'incident, une règle métier valide automatiquement les informations contenues dans l'incident de sécurité par rapport aux conditions définies dans chacun de vos calculateurs de gravité actifs. Ils sont validés un calculateur de sécurité à la fois, dans l'ordre défini par le champ **Ordre** de chaque calculateur. Si les informations contenues dans l'incident de sécurité correspondent aux conditions définies dans l'un des calculateurs, les valeurs des champs de gravité sont mises à jour en fonction des règles définies dans le calculateur.

Supposons, par exemple, que vous créez un incident de sécurité pour un CI affecté et que le CI est très critique. Lorsque l'incident de sécurité est enregistré, les informations de CI sont comparées aux conditions définies dans les calculateurs de gravité. Lorsque l'incident

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de sécurité est validé par rapport au calculateur de gravité affecté par le **service critique** , les champs de gravité sont automatiquement mis à jour et un message similaire au suivant s'affiche en haut de l'incident de sécurité.



Vous pouvez utiliser ces calculateurs de gravité tels quels ou vous pouvez les modifier pour mieux répondre aux besoins de votre entreprise. Par exemple, si vous souhaitez identifier les menaces Web et de messagerie spécifiques à l'unité business Finance, vous pouvez modifier les conditions du calculateur de **Vecteurs d'attaques multiples** :

- [Vecteur d'attaque] [contient] [Web]
- [Vecteur d'attaque] [contient] [Courriel]
- [Unité business] [contient] [Finances]

Vous pouvez également mettre à jour les valeurs de gravité d'un incident de sécurité existant à tout moment en ouvrant l'enregistrement et en cliquant sur le lien connexe **Calculer la gravité** .

Calculateurs de score de risque d'incidents de sécurité

Les calculateurs **Définir la priorité avec la catégorie et les services** et **Définir la priorité avec les observables** sont utilisés pour calculer un score de risque pour un incident de sécurité.

Calculateurs de criticité utilisateur

Les deux calculateurs du groupe de **criticité de l'utilisateur** (**Obtenir la criticité de l'utilisateur** et **Obtenir la criticité du groupe d'utilisateurs**) fournissent des exemples de la façon dont vous pouvez gérer la criticité en fonction de critères définis dans un enregistrement utilisateur ou en fonction du groupe auquel un utilisateur appartient.

Elles peuvent être modifiées si nécessaire ou de nouveaux calculateurs de criticité utilisateur peuvent être créés.

Le calculateur **Obtenir la criticité de l'utilisateur** fait passer la criticité opérationnelle de l'utilisateur à **1 - Critique** lorsque le champ **Département** est changé en **Finances**.

Le calculateur **Obtenir la criticité du groupe d'utilisateurs** fait passer la criticité opérationnelle de l'utilisateur à **1 - Critique** lorsque l'utilisateur est ajouté au groupe **de base de données** .

> **Remarque : Obtenir la criticité du groupe d'utilisateurs** est un exemple de calculateur qui s'exécute sur les données d'une liste connexe. Si vous souhaitez ajouter d'autres groupes pour initier un changement de criticité, ajoutez une liste de groupes séparés par des virgules sys_ids à la première ligne du script. Exemple : `var CRITICAL_GROUPS = [group1_sys_id, group2_sys_id, group3_sys_id];`.

Calculs du score de risque d'incidents de sécurité

Le score de risque est calculé comme une moyenne arithmétique qui représente le risque en fonction de la priorité d'un incident de sécurité, du type d'incident de sécurité (déni de service, harponnage ou activité de code malveillant) et du nombre de sources qui ont déclenché un score de réputation échoué sur un indicateur.

Le score de risque aide à hiérarchiser le travail d'incident de sécurité pour les analystes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Si vous souhaitez utiliser le nouveau calculateur de score de risque, reportez-vous à .Définir les nouvelles règles du calculateur de score de risque

Les calculateurs d'incidents de sécurité**Définir la priorité avec la catégorie et les services** et **Définir la priorité avec les observables** sont utilisés pour calculer un score de risque pour un incident de sécurité. En outre, les règles métier suivantes déclenchent le calcul automatique des scores de risque :

- Calculer la gravité
- Mettre à jour le score de risque
- Mettre à jour le score de risque SI

Remarque : Le calculateur de risque disponible dans le système de base dépend de votre niveau tarifaire Security Operations.

Lorsque vous consultez une liste d'incidents de sécurité dans le système de base, notez la colonne **Score de risque** .

Incidents de sécurité

Security Incidents | New | Go to | Risk score | Search

All > Active = true

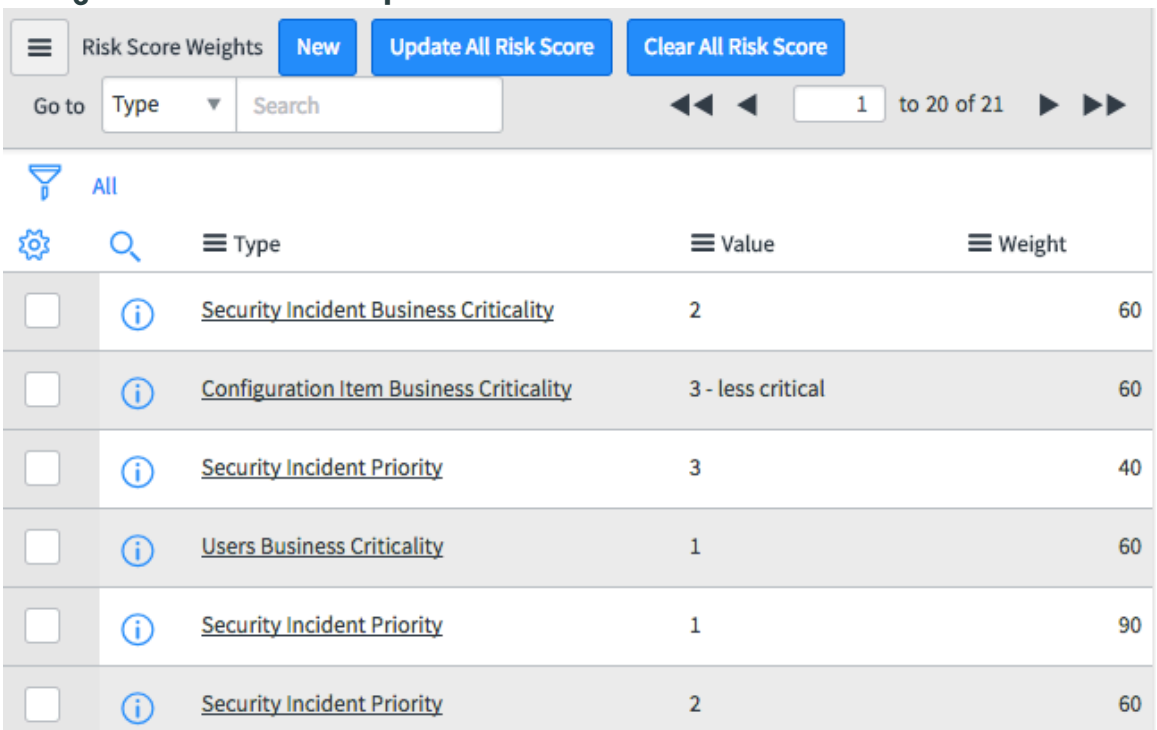
Number	Risk score	Priority	Configuration item	Assigned to	Assigr
SIR0001764	92	1 - Critical	SAP Plant Maintenance	Raphael Bickel	Applicati
SIR0001733	92	1 - Critical	SAP LoadBal01	Malissa Ziesemer	SecOps E
SIR0001734	92	1 - Critical	SAP AppSRV02	Saundra Mcaulay	Unix Sec
SIR0001759	92	1 - Critical	ny8500-nbxs08	Marla Folz	Forensics
SIR0001738	92	1 - Critical	VMWARE-SD-07	Raphael Bickel	Applicati
SIR0001747	92	1 - Critical	VMWARE-SD-04	Helga Windle	Windows
SIR0001741	92	1 - Critical	bond_trade_ny	Corinne Cowan	Network
SIR0001762	92	1 - Critical	PeopleSoft Financials	Deepa Shah	SecOps A
SIR0001749	92	1 - Critical	ny8500-nbxs08	Simone Lundie	Directory Security

Le score de risque est calculé à l'aide des poids définis dans la **configuration du score de risque**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de score du risque



Par exemple, si un incident de sécurité a un **impact sur l'entreprise** défini sur **2-Élevé** et une **priorité** définie sur **3-Modéré**, les poids respectifs dans la table des pondérations du score de risque sont recherchés et calculés comme suit :

Impact opérationnel de **l'incident de sécurité** avec une valeur de 2 = un poids de 60.

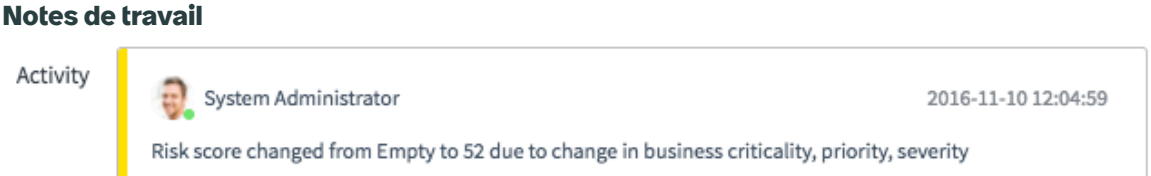
Priorité de l'incident de sécurité avec une valeur de 3 = un poids de 40.

(60 + 40)/2 = un score de risque de 50.

La position de l'incident de sécurité dans la liste des incidents de sécurité est ensuite réorganisée en fonction de son score de risque mis à jour.

Si, dans l'exemple ci-dessus, **l'impact sur l'entreprise** ou la **priorité** de l'incident de sécurité est modifié, le score de risque est recalculé et les changements sont reflétés dans les notes de travail.

Notes de travail



Les notes de travail sont mises à jour lorsque les champs suivants sont modifiés (entraînant la mise à jour du score de risque) :

- **Impact sur l'activité** du formulaire d'incident de sécurité
- **Priorité** sur le formulaire d'incident de sécurité
- **Gravité** sur le formulaire d'incident de sécurité (masqué par défaut)
- **Impact sur l'activité** sur la liste connexe **Utilisateurs affectés**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Impact sur l'activité** sur la liste connexe **Services affectés**
- **Impact sur l'activité des** vulnérabilités sur la liste connexe **des éléments vulnérables**

En outre, les notes de travail sont mises à jour dans les situations suivantes :

- Lorsqu'une association entre les utilisateurs affectés et un incident de sécurité est créée ou modifiée
- Lorsqu'une association entre les services affectés et un incident de sécurité est créée ou modifiée
- Lorsqu'une association entre des éléments vulnérables et un incident de sécurité est créée ou modifiée

Les notes de travail sont également mises à jour chaque fois que l'utilisateur clique **sur Mettre à jour tous les scores de risque** et **Effacer tous les scores de risque** sur le formulaire Poids des scores de risque .

Gérer les pondérations des scores de risque

Les pondérations des scores de risque utilisées pour calculer les scores de risque dans les incidents de sécurité peuvent être supprimées ou mises à jour individuellement. Ils peuvent également être supprimés ou mis à jour pour tous les incidents de sécurité. La possibilité de les supprimer des incidents de sécurité est utile lors du changement des valeurs de poids.

Avant de commencer

Rôle requis : sn_sec_cmn.admin

Remarque : Les utilisateurs disposant du rôle sn_si.read peuvent afficher la configuration du score de risque dans Réponse aux incidents de sécurité.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Configuration** > **Configuration du score de risque**.

   Remarque : Les utilisateurs disposant du rôle sn_si.read peuvent afficher la configuration du score de risque en accédant à **Incident de sécurité** > **Alertes et événements** > **Configuration du score des risques**.

2. Pour ajouter un nouveau poids de score de risque, cliquez sur **Nouveau** et saisissez les informations dans les champs.

Champ	Description
Type	Sélectionnez le type de score de risque que vous définissez.
Valeur	Spécifiez la valeur associée au type sélectionné. Si plusieurs valeurs sont disponibles pour le type, vous pouvez définir plusieurs enregistrements de poids de score de risque. Exemple : priorité d'incident de sécurité avec une valeur de 1, priorité d'incident de sécurité avec une valeur de 2, et ainsi de suite.
Pondération	Poids associé à la paire type/valeur sélectionnée. Les entrées valides sont comprises entre 0 et 100, 0 étant le poids le plus bas et 100 le poids le plus élevé.

3. Cliquez sur **Envoyer**.
4. Effectuez l'une de ces étapes, selon les besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour effacer un enregistrement de poids de score de risque, **ouvrez-le** à partir de la liste et cliquez sur Supprimer.
- Pour effacer tous les enregistrements de poids de score de risque, cliquez sur **Effacer tous les scores de risque**.
- Pour mettre à jour tous les enregistrements de poids de score de risque, cliquez sur **Mettre à jour tous les scores de risque**.

Créer un Réponse aux incidents de sécurité SLA

Vous pouvez définir un accord sur les niveaux de service (SLA) pour Réponse aux incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Configuration** > **SLA**.
2. Cliquez sur **Nouveau**.
   Pour obtenir une description des champs et des instructions détaillées, reportez-vous à la section Créer une définition de SLA .

Réparer les SLA d'incidents de sécurité

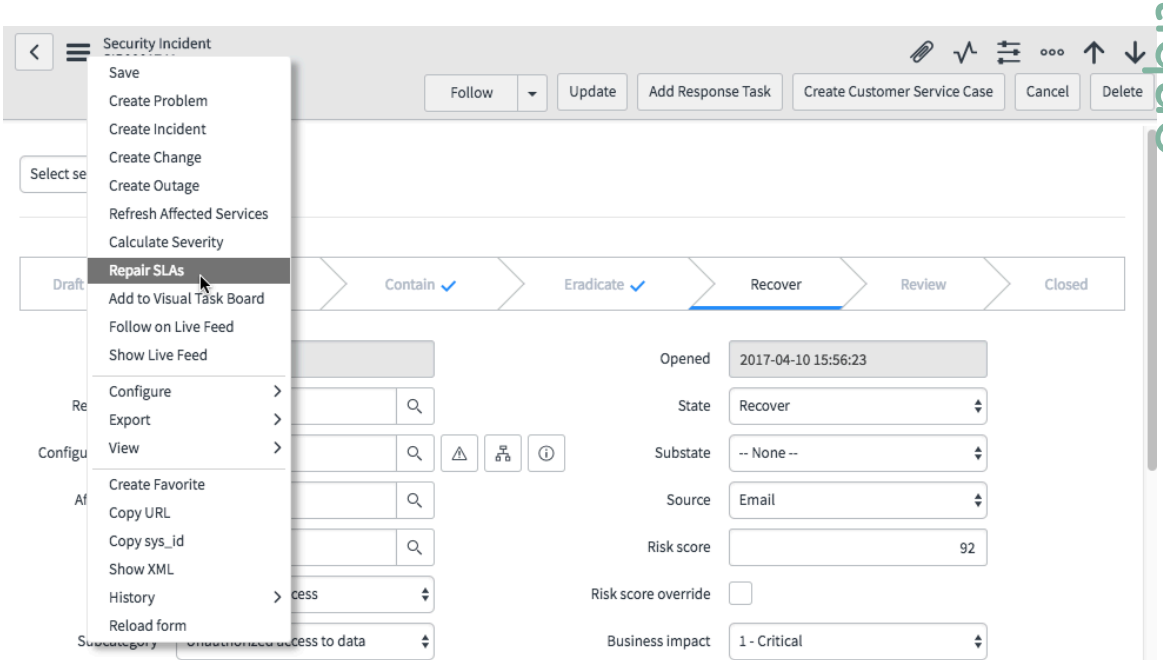
Vous pouvez réparer les enregistrements SLA pour vous assurer que les informations de calendrier et de durée des SLA sont exactes.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez réparer des SLA.
2. Cliquez sur le menu contextuel de l'en-tête du formulaire et sélectionnez **Réparer les SLA** :



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **OK** dans la zone de confirmation Avertissement.
   Pour plus d'informations, consultez Réparation des SLA .

Créer un Runbook de réponse aux incidents de sécurité

Un Runbook est une association entre un article de la base de connaissances publié et une tâche spécifique. Pendant que vous effectuez la tâche, un article de la base de connaissances dans le Runbook s'ouvre automatiquement et fournit des informations pertinentes pour la tâche.

Avant de commencer

Il doit y avoir des articles de la base de connaissances existants dans la base de Réponse aux incidents de sécurité connaissances Runbook. Lorsque vous créez un article de la base de connaissances sur les incidents de sécurité, veillez à sélectionner **Runbook Security Incident Response** dans le champ Base de **connaissances** . Après avoir publié l'article, vous pouvez cliquer sur le bouton **Créer un runbook** .

Rôle requis : sn.si.knowledge_admin

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser des runbooks pendant les processus de création d'incidents de sécurité ou de tâches de réponse, ou vous pouvez associer les articles de la base de connaissances d'un runbook aux tâches du playbook.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Runbook manuel** > **Créer un nouveau Runbook**.
2. Renseignez les champs comme il convient.

Champ	Description
Article de la base de connaissances	Sélectionnez un article de la base de connaissances à inclure dans le runbook.
Actif	Cochez la case pour rendre le runbook disponible à partir du **navigateur de filtre**.
Utiliser un groupe de filtres	Cochez cette case pour utiliser un groupe de filtres prédéfini ou créer un nouveau groupe de filtres pour définir les critères du runbook.
Groupe de filtres	Sélectionnez le groupe de filtres à utiliser pour définir un runbook. Ce champ s'affiche uniquement si la case **Utiliser des groupes de filtres** est cochée.
Table	Sélectionnez Incident de sécurité [sn_si_incident] ou Réponse aux incidents de sécurité Tâche [sn_si_task]. Si vous avez coché la case **Utiliser un groupe de filtres** et sélectionné un groupe de filtres, ce champ est défini par défaut sur la table associée au groupe de filtres sélectionné.
Condition	Définissez les conditions qui relient ce Runbook à l'incident ou à la tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si vous avez coché la case **Utiliser un groupe de filtres** et sélectionné un groupe de filtres, les champs **Condition** ne s'affichent pas.

3. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
   L'onglet Détails de l'article de la base de connaissances et une série de boutons s'affichent.
4. Pour afficher les détails du runbook, cliquez sur l'onglet Détails de la **base de connaissances** .
5. Pour afficher l'article de la base de connaissances tel qu'il apparaît à l'utilisateur, cliquez sur **Afficher l'article**.
6. À Modifiez les détails de l'article de la base de connaissances , cliquez sur **Modifier l'article**.

Créer des règles pour valider les attaques par hameçonnage signalées par un utilisateur

Lorsque vos employés reçoivent des e-mails qui semblent être des attaques de phishing, ils peuvent vous les signaler à l'aide d'une adresse e-mail de phishing. L'e-mail suspect est validé à l'aide de règles définies par votre organisation.

Avant de commencer

Avant que les règles de correspondance d'e-mail ne puissent être utilisées pour identifier les attaques de phishing potentielles, définissez une adresse e-mail vers laquelle les e-mails transférés par vos employés seront envoyés pour traitement. Vous disposez des options suivantes pour définir cette adresse e-mail (en supposant que le domaine de messagerie de votre entreprise est acme.com) :

- Définissez une adresse e-mail telle que **acme+phishing@service-now.com**. La balise **+phishing** est prise en charge par SMTP pour activer le filtrage et votre instance peut recevoir les e-mails qui lui sont envoyés.
- Définissez une adresse e-mail, telle que **phishing@acme.com** (votre boîte aux lettres Exchange), qui la transmet à **son tour à acme+phishing@service-now.com** (votre boîte aux lettres d'instance définie par une règle de transfert de courrier).

Rôle requis : sn_sec_cmn.write

Pourquoi et quand exécuter cette tâche

Lorsqu'un employé rencontre un e-mail suspect, il doit le transférer en pièce jointe à votre adresse e-mail d'hameçonnage. Si l'e-mail en pièce jointe correspond à une règle définissant une menace, un incident de sécurité est créé.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Traitement des e-mails** > **Hameçonnage signalé par un utilisateur**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs nécessaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

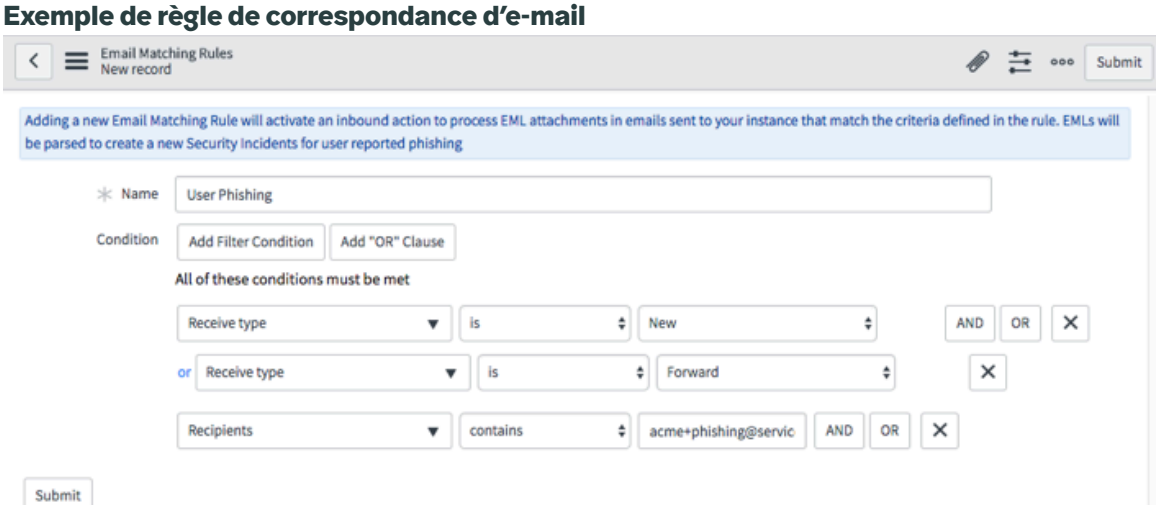
Formulaire Règles de correspondance d'e-mails

Champ	Description
Nom	Nom de cette règle de correspondance d'e-mail. Par exemple, Hameçonnage signalé par un utilisateur.
Conditions	Utiliser le Créateur de conditions permettant de valider si un e-mail envoyé à l'adresse e-mail d'hameçonnage de votre entreprise est une attaque d'hameçonnage. Consultez l'exemple suivant.

4. Cliquez sur **Envoyer**.

Example:
Cet exemple montre une règle de correspondance pour le traitement du hameçonnage signalé par un utilisateur.

Exemple de règle de correspondance d'e-mail



Configurez la Security Analyst Workspace.

Configurez l'interface utilisateur de l'enregistrement d'incident dans Security Analyst Workspace le pour spécifier les champs que vous souhaitez afficher.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Spécifiez les champs à afficher dans votre enregistrement d'incident et l'ordre dans lequel ils doivent apparaître sur le formulaire d'incident de sécurité et le formulaire de tâche de réponse. Vous pouvez également définir une limite sur le nombre de champs que vous souhaitez afficher.

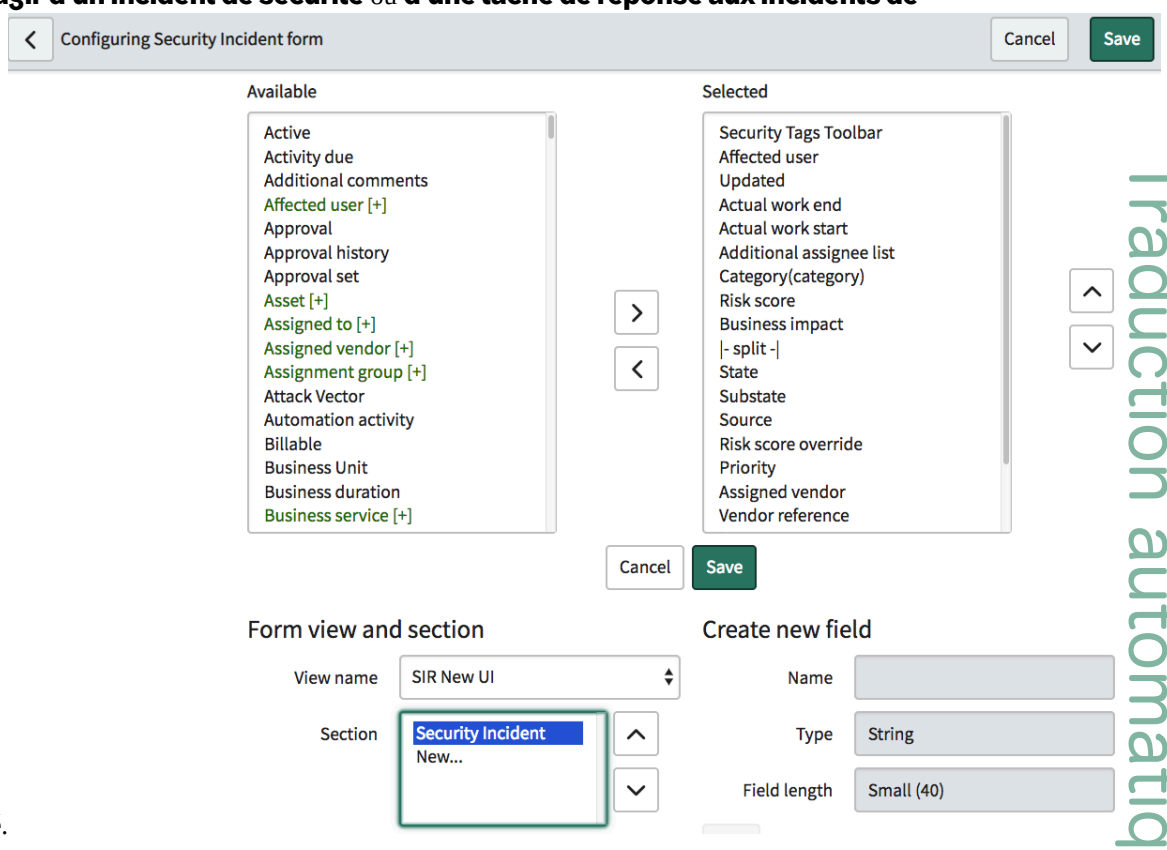
Remarque : Vous pouvez créer des règles pour déterminer quelle vue doit être utilisée pour un formulaire spécifique. Plusieurs vues sont incluses dans le système de base, notamment les vues Par défaut et Nouvelle interface utilisateur SIR. Plusieurs règles de vue sont également fournies avec le système de base, y compris la règle de tâche de réponse Toutes les autres. Cette règle applique la vue par défaut sur le formulaire de tâche de réponse lorsque la condition spécifiée dans la règle de vue est remplie. Le Security Analyst Workspace utilise la nouvelle vue d'interface utilisateur SIR. Si les champs de formulaire affichés ne Security Analyst Workspace correspondent pas aux champs de formulaire de l'environnement classique, une règle de vue est très probablement appliquée. Pour utiliser la **nouvelle vue d'interface utilisateur SIR** pour le formulaire, vous devez désactiver la règle de vue. Pour plus d'informations, voir Contrôler quand le système affiche une vue .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à une liste d'incidents de sécurité (par exemple, **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**).
2. Pour ouvrir l'enregistrement d'incident de sécurité, cliquez sur un lien d'incident de sécurité.
3. Pour accéder à la page du formulaire de configuration des incidents de sécurité, cliquez sur l'icône du ☰ et sélectionnez **Configurer** > **Mise en page**.
4. Dans la liste Nom de la **vue** , sélectionnez **Nouvelle interface utilisateur SIR**.
5. Dans le champ **Section** , sélectionnez la section appropriée.
   Il peut **s'agir d'un incident de sécurité** ou **d'une tâche de réponse aux incidents de sécurité**.



6. Sélectionnez les champs et l'ordre dans lequel vous souhaitez qu'ils apparaissent dans la bannière d'incident de la nouvelle interface utilisateur.
7. Cliquez sur **Enregistrer**.

Traduction automatique

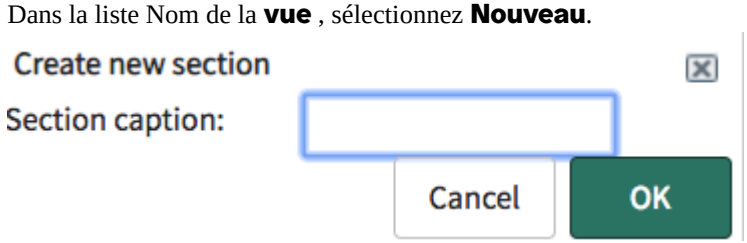
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Certains champs sont masqués par défaut dans les bannières Incident et Tâche de réponse. Modifiez les champs masqués ou affichés en modifiant les propriétés `sn_app_secops_ui.form.excluded_fields.incident` et `sn_app_secops_ui.form.excluded_fields.response_task` comme décrit dans Propriétés de Security Analyst Workspace.
- Spécifiez le nombre de champs qui peuvent être affichés dans les bannières Incident et Tâche de réponse et sur la première ligne de la bannière d'incident en définissant ces propriétés :
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_app_secops_ui.task_summary.single_summary.limit.response_task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

8. Pour configurer les styles des cercles en pointillés qui apparaissent à côté d'une valeur de champ dans l'enregistrement d'incident, par exemple, , accédez à **Interface utilisateur du système** > **Styles de champ** et modifiez ou créez un enregistrement de style pour la table et le nom de champ spécifiques. La propriété background-color dans le champ Style de l'enregistrement de style détermine la couleur du cercle en pointillés.
9. Pour afficher la bannière d'incident mise à jour, cliquez sur **Incidents de sécurité** > **Incidents (nouvelle interface utilisateur)** pour accéder à l'enregistrement d'incident dans le Security Analyst Workspace et actualiser la page pour afficher la bannière d'incident mise à jour.
10. Pour configurer la bannière de tâche de réponse dans l'enregistrement d'incident, accédez à **Incidents de sécurité** > **Tâches de réponse** > **Afficher toutes les tâches** et répétez les étapes.
11. Si vous créez une table de tâches à partir de la table de tâche de Security Incident Response de base, vous devez également ajouter la vue Nouvelle interface utilisateur SIR à la table.

    a. Dans la liste Nom de la **vue** , sélectionnez **Nouveau**.



    b. Entrez **SIR Nouvelle interface utilisateur** (sensible à la casse) dans la fenêtre Créer une nouvelle vue et cliquez sur **OK**.

Résultats

Les bannières des incidents de sécurité et des tâches de réponse sont mises à jour dans le Security Analyst Workspace (Gérer les menaces de sécurité à l'aide de l' Security Analyst Workspace).

Configurer des filtres primaires et secondaires pour Security Analyst Workspace

Le Security Analyst Workspace système de base comprend un ensemble de filtres primaires pour réduire la liste des incidents de sécurité à analyser (pour les incidents de sécurité qui vous sont affectés, tous les incidents ouverts, et ainsi de suite) et un ensemble de filtres rapides (ou secondaires) pour affiner encore plus la liste (par nouveaux incidents, incidents ouverts, incidents critiques uniquement, et ainsi de suite).

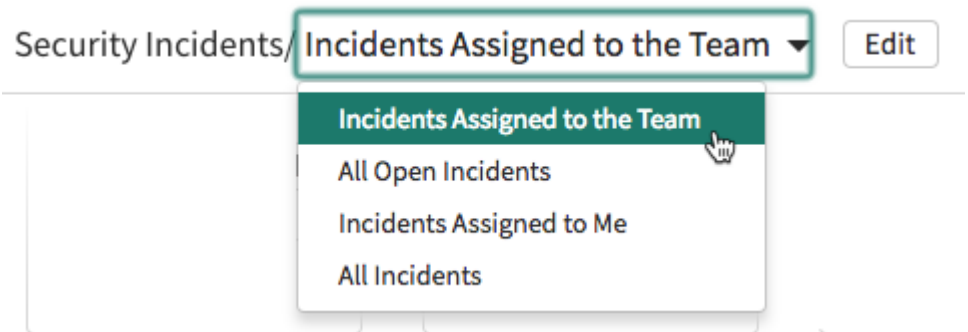
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

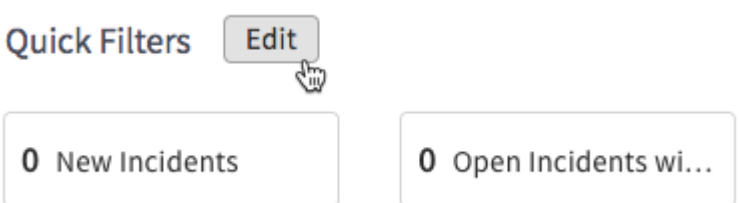
Avant de commencer

Vous pouvez utiliser l'environnement classique pour définir des filtres primaires et secondaires supplémentaires.

Lorsque vous définissez les filtres à utiliser dans le Security Analyst Workspace, vous pouvez affecter des balises pour indiquer s'ils peuvent être utilisés comme filtres primaires ou secondaires. Les filtres primaires sont affichés en haut de la liste des incidents de sécurité.



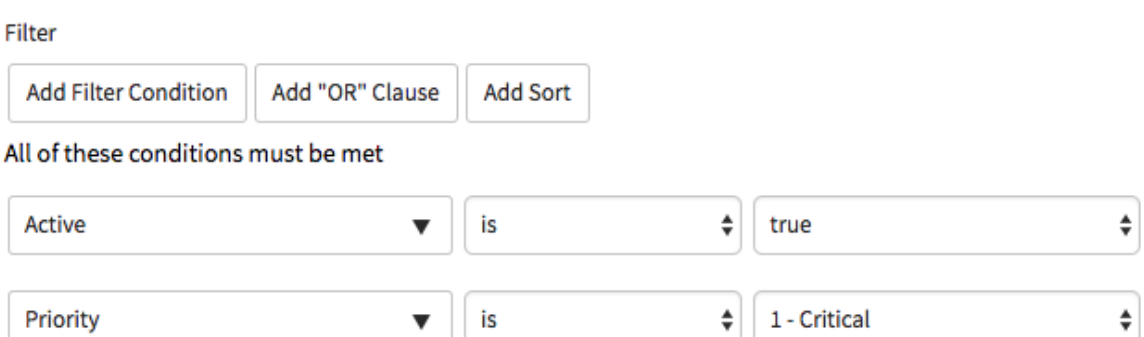
Cliquez sur **Modifier** à côté de l'option Filtres rapides pour sélectionner des filtres secondaires (ou rapides).



Rôle requis : admin ou sn_sec_cmn.write

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Filtres**.
2. Cliquez sur **Nouveau** et procédez comme suit.
   a. Saisissez un **titre**.
   b. Sélectionnez **Incident de sécurité [sn_si_incident]** dans la liste de choix de **table** .
   c. Ajoutez vos conditions de filtre.
   Par exemple, le filtre **Incidents ouverts avec priorité = critique** utilise ces conditions.



   d. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Si la colonne **Balises** n'est pas visible sur la liste de filtres, cliquez sur l'icône d'engrenage et personnalisez la vue pour l'ajouter.
4. Localisez le filtre que vous avez créé et ajoutez l'une des balises suivantes pour indiquer comment le filtre doit apparaître dans le Security Analyst Workspace.
   - **SN_SI_Primary** : si cette balise est sélectionnée, le filtre peut être sélectionné à partir de la zone de sélection de filtre primaire dans le Security Analyst Workspace.
   - **SN_SI_Primary_OOB** : si cette balise est sélectionnée, le filtre apparaît par défaut dans le côté **sélectionné** de la zone de sélection du filtre primaire.
   - **SN_SI_Secondary** : si cette balise est sélectionnée, le filtre peut être sélectionné à partir de la zone de sélection de filtre secondaire (rapide).
   - **SN_SI_Secondary_OOB** : si cette balise est sélectionnée, le filtre apparaît par défaut dans le côté **sélectionné** de la zone de sélection du filtre primaire.

Information associée

Créer et modifier des filtres

Propriétés de Security Analyst Workspace

Ces propriétés système sont utilisées pour configurer Security Analyst Workspace.

Il existe deux types de propriétés :

- Propriétés qui ne sont généralement pas modifiées, telles que les clés sys_ids et les clés de produit.
- Propriétés qui sont modifiées selon les besoins, comme les intervalles d'interrogation longs et les configurations de l'interface utilisateur.

Remarque : Les propriétés de Security Analyst Workspace se trouvent à cet emplacement : **Incident de sécurité** > **Configuration d'Analyst Workspace** > **Propriétés d'Analyst Workspace**.

Propriétés de Security Analyst Workspace

Nom de la propriété	Description
Champs masqués par défaut dans la bannière de tâche de réponse. sn_app_secops_ui.formulaire.champs_exclus.réponse_tâche	• **Type** : chaîne • **Valeur par défaut** : ◦ Numéro ◦ Description brève ◦ commentaires ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity
Champs masqués par défaut dans la bannière d'incident.	• **Type** : chaîne • **Valeur par défaut** :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
sn_app_secops_ui.formulaire.champs_exclus.incident	◦ Numéro ◦ Description brève ◦ commentaires ◦ work_notes ◦ comments_and_work_notes ◦ work_notes_list ◦ automation_activity ◦ security_tags
Le style de couleur d'arrière-plan est appliqué aux champs répertoriés ici. sn_app_secops_ui.formulaire.couleurs_coded_champs	• **Type** : chaîne • **Valeur par défaut** : ◦ Criticité opérationnelle ◦ impact ◦ Priorité ◦ risk_score ◦ severity
Si vrai, les tables étendues à partir de la table de tâches de réponse de base sn_si_task auront également accès aux modèles d'e-mail créés pour la table de tâche de réponse de base. sn_app_secops_ui.extend.base.response_task.email_templates	• **Type** : vrai | faux • **Valeur par défaut** : true
Définit la largeur de chaque champ de résumé dans chaque bannière de tâche de réponse. sn_app_secops_ui.task_summary.single_summary.width.response_task	• **Type** : nombre entier • **Valeur par défaut** : 10
Définit la largeur de chaque champ de résumé dans chaque bannière d'incident. sn_app_secops_ui.task_summary.single_summary.width.incident	• **Type** : nombre entier • **Valeur par défaut** : 15
Définit une limite sur le nombre de champs de résumé autorisés dans la bannière d'incident. sn_app_secops_ui.task_summary.single_summary.limit.incident	• **Type** : nombre entier • **Valeur par défaut** : 12

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
Définit une limite de champs de résumé autorisés dans la bannière de tâche de réponse. sn_app_secops_ui.task_summary.single_summary.limit.response_task	• **Type** : nombre entier • **Valeur par défaut** : 12
Définit une limite de champs de résumé autorisés dans la première ligne de la bannière d'incident. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• **Type** : nombre entier • **Valeur par défaut** : 3
Liste de champs séparés par des virgules qui peuvent contenir des photos d'utilisateurs. sn_app_secops_ui.form.user_fields	• **Type** : chaîne • **Valeur par défaut** : ◦ affected_user ◦ appelant ◦ sys_updated_by ◦ sys_created_by ◦ opened_by ◦ closed_by ◦ submitted_by
Définit la largeur de chaque champ de résumé dans chaque vue d'aperçu d'incident. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• **Type** : nombre entier • **Valeur par défaut** : 13,5
Liste de champs qui affichent l'heure séparés par des virgules. sn_app_secops_ui.formulaire.champs_temps	• **Type** : chaîne • **Valeur par défaut** : ◦ opened_at ◦ sys_created_on ◦ sys_updated_on
Contrôle la fréquence (en millisecondes) à laquelle les résultats de la recherche de perception sont actualisés. sn_app_secops_ui.poller_interval.search_action	• **Type** : nombre entier • **Valeur par défaut** : 30000 **Minimum** : 15000

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
Contrôle la fréquence (en millisecondes) à laquelle le nombre ou les données de requête sont actualisés. sn_app_secops_ui.poller_interval.related_list	• **Type** : nombre entier • **Valeur par défaut** : 30000 **Minimum** : 15000
Contrôle la fréquence (en millisecondes) à laquelle les données de résultat sont actualisées (pour le playbook). sn_app_secops_ui.poller_interval.playbook_tasks	• **Type** : nombre entier • **Valeur par défaut** : 30000 **Minimum** : 15000
ID du workflow Intégration de Security Operations - Isoler l'hôte. sn_app_secops_ui.workflow.id.isolate_host	• **Type** : chaîne • **Valeur par défaut** : d72041f1ff203200c68c84648e94fa5e
ID du workflow Intégration de Security Operations - Liste de surveillance. sn_app_secops_ui.workflow.id.publish_to_watchlist	• **Type** : chaîne • **Valeur par défaut** : 35800c0eff343200c68c84648e94fa85
ID du workflow Security Operations *Integration* - Block Request. sn_app_secops_ui.workflow.id.block_request	• **Type** : chaîne • **Valeur par défaut** : 11a6a5270b9032008f9108e3c5673a24
ID du rôle d'utilisateur sn_si_analyst. sn_app_secops_ui.roles.id.sn_si.write	• **Type** : chaîne • **Valeur par défaut** : 66878663ff123100158bfffffffff8d
ID du rôle d'utilisateur sn_si_read. sn_app_secops_ui.roles.id.sn_si.read	• **Type** : chaîne • **Valeur par défaut** : ae878663ff123100158bfffffffff8e
ID du rôle d'utilisateur sn_si_admin. sn_app_secops_ui.roles.id.sn_si.admin	• **Type** : chaîne • **Valeur par défaut** : 22878663ff123100158bfffffffff8d
ID du workflow Microsoft Exchange : effectuer une recherche et supprimer des e-mails.	• **Type** : chaîne • **Valeur par défaut** : ed9f289cc310220031fbdccdf3d3aeb4

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
sn_app_secops_ui.email.phishing.manual.workflow	
ID de l'action personnalisée Ajouter à la liste de refus sous l'onglet Explorer dans le Security Analyst Workspace. sn_app_secops_ui.explore.action.direct.id.deny_list	• **Type** : chaîne • **Valeur par défaut** : DENY_e9bd0ac50b632200263a089b37673a0b
ID de l'action personnalisée Ajouter à la liste d'autorisation sous l'onglet Explorer dans le Security Analyst Workspace sn_app_secops_ui.explore.action.direct.id.allow_list	• **Type** : chaîne • **Valeur par défaut** : ALLOWLIST_e9bd0ac50b632200263a089b37673a0b
ID de l'action d'interface utilisateur Exécuter la recherche de menace. sn_app_secops_ui.explore.action.id.run_threat_lookup	• **Type** : chaîne • **Valeur par défaut** : da5ff4420b540300263a089b37673ae7
ID de l'option d'intégration Recherche de menace. sn_app_secops_ui.explore.capability.id.threat_lookup	• **Type** : chaîne • **Valeur par défaut** : 39344d4f0b273200263a089b37673ab1
ID de l'action personnalisée Enrichissement des observables sous l'onglet Explorer dans le Security Analyst Workspace. sn_app_secops_ui.explore.action.id.observable_enrichment	• **Type** : chaîne • **Valeur par défaut** : OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673
ID de l'option d'intégration Enrichir les observables. sn_app_secops_ui.explore.capability.id.observable_enrichment	• **Type** : chaîne • **Valeur par défaut** : 9ad183640b1003009f66e94685673af4
ID de l'action d'interface utilisateur Publier dans la liste de surveillance. sn_app_secops_ui.explore.action.id.publish_to_watchlist	• **Type** : chaîne • **Valeur par défaut** : 8ee94002ff743200c68c84648e94faf9
ID de l'action d'interface utilisateur Demande de bloc. sn_app_secops_ui.explore.action.id.block_request	• **Type** : chaîne • **Valeur par défaut** : 7158f6e40b2032008f9108e3c5673adf

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de Security Analyst Workspace (suite)

Nom de la propriété	Description
ID de l'action d'interface utilisateur Exécuter la recherche de perceptions. sn_app_secops_ui.explore.action.id.sightings_search	• **Type** : chaîne • **Valeur par défaut** : 43f91a6f0b032200b97c67d985673a2c
ID de l'action d'interface utilisateur Créer un incident de sécurité enfant. sn_app_secops_ui.explore.action.id.create_child_incident	• **Type** : chaîne • **Valeur par défaut** : 5a6882645363530099d5ddeeff7b1272
ID de l'action d'interface utilisateur Ajouter une annotation de sécurité. sn_app_secops_ui.explore.action.id.add_security_annotation	• **Type** : chaîne • **Valeur par défaut** : 1e3a3e723b5332005a9149a4d2efc4eb
ID de l'action personnalisée d'enrichissement de CI sous l'onglet Explorer dans le Security Analyst Workspace. sn_app_secops_ui.explore.action.id.ci_enrichment	• **Type** : chaîne • **Valeur par défaut** : CI_ENRICHMENT_54e2f5d60b5003009f66e94885673a1
ID de l'action d'interface utilisateur Isoler l'hôte. sn_app_secops_ui.explore.action.id.isolate_host	• **Type** : chaîne • **Valeur par défaut** : d6244e0aff203200c68c84648e94fad3
ID de l'action d'interface utilisateur Ajouter plusieurs observables. sn_app_secops_ui.explore.action.id.multiple_observable	• **Type** : chaîne • **Valeur par défaut** : 138de478d78322007a6de294de6103aa
Clé de produit pour ag-Grid-Enterprise. sn_app_secops_ui.ag-grid-license	• **Type** : chaîne • **Valeur par défaut** :ServiceNow_ServiceNow_5Devs2_August_2018__N

Configuration supplémentaire de Security Analyst Workspace

Configurer et définir des filtres, des actions d'interface Security Analyst Workspace utilisateur et des listes connexes.

- Configuration du filtre de la page de destination
- Activer les actions d'interface utilisateur
- Actions d'interface utilisateur du formulaire
- Configuration de la liste connexe
- Actions d'interface utilisateur de la liste connexe

Traduction automatique

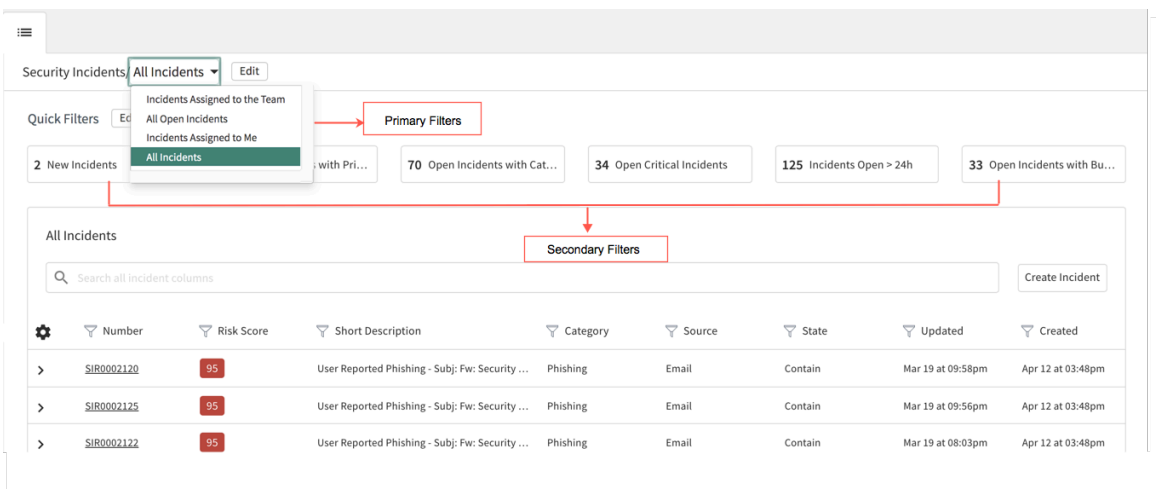
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Propriétés système de configuration du formulaire
- Activer les playbooks pour la sélection des analystes

Configuration du filtre de la page de destination

Vous pouvez ajouter de nouveaux filtres ou modifier les filtres existants qui apparaissent dans le Security Analyst Workspace.

L'dispose Security Analyst Workspace de filtres primaires et secondaires qui vous permettent de filtrer la liste des incidents de sécurité afin de trouver rapidement les incidents de sécurité que vous souhaitez analyser. Pour plus d'informations, voir Gérer les menaces de sécurité à l'aide de l' Security Analyst Workspace.



Créer un nouveau filtre

1. Accédez à la **Incidents de sécurité** > **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Configuration du filtre de la page de destination**.
2. Cliquez sur **Nouveau**.
3. Donnez un titre au filtre, spécifiez la condition de filtre et cliquez sur **Envoyer** pour revenir à la page précédente.

   Vous verrez le filtre nouvellement ajouté répertorié sur la page.
4. Ajoutez une balise pour ce filtre afin d'indiquer s'il s'agit d'un filtre primaire ou secondaire. Les balises suivantes sont disponibles :
   - SN_SI_Primary
   - SN_SI_Secondary

Modifier les filtres existants

Vous pouvez également effectuer les opérations suivantes :

- Modifier les filtres existants : cliquez sur le titre d'un filtre existant. Modifiez le titre et la condition de filtre, puis cliquez sur **Mettre à jour**.
- Modifier les balises : sélectionnez un filtre et cliquez sur la colonne Balise dans la configuration du filtre de la page de destination. Vous pouvez supprimer la balise existante ou ajouter une nouvelle balise pour le filtre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer les actions d'interface utilisateur

Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles soient disponibles pour la configuration dans le Security Analyst Workspace.

Remarque : Pour modifier les actions d'interface utilisateur, connectez-vous en tant qu'utilisateur avec les rôles suivants :

- ui_action_admin
- ui_page_admin
- web_service_admin

Il existe deux types d'actions d'interface utilisateur qui peuvent être configurées pour :Security Analyst Workspace

- Action d'interface utilisateur basée sur une boîte de dialogue
- Action d'interface utilisateur côté serveur

Action d'interface utilisateur basée sur une boîte de dialogue

Pour activer les actions d'interface utilisateur basées sur la boîte de dialogue dans , Security Analyst Workspace apportez les modifications suivantes aux pages de l'interface utilisateur associées aux actions d'interface utilisateur standard respectives.

1. **Section HTML** : modifiez la section HTML pour inclure la balise d'entrée *`react`* . La valeur de la balise d'entrée *`react`* est utilisée dans la section du script client pour identifier si la page de l'interface utilisateur a été lancée à partir du Security Analyst Workspace. Un exemple est présenté ci-dessous :

   ```
   <input id="react" name="react" type="hidden"
   value="${JS,HTML:sysparm_react}" />
   ```

2. **Script client** : une logique supplémentaire doit être écrite dans le script client lorsque le marqueur *`React`* est vrai. Ceci est nécessaire pour gérer les événements des boutons **Soumettre** et **Annuler** affichés dans le cadre de la fenêtre de dialogue.
   a. Le gestionnaire d'événements onCancel () doit répartir l'événement « SIR_WORKBENCH_POPUP_CANCEL » à partir de Security Analyst Workspace
   b. Le gestionnaire d'événements onSubmit () doit répartir l'événement « SIR_WORKBENCH_POPUP_SUBMIT » à partir de Security Analyst Workspace
3. L'exécution du script de traitement est ignorée depuis le Security Analyst Workspace contexte, car l'action « onSend » a été modifiée pour renvoyer la valeur faux lorsque la valeur de la balise d'entrée *`de réaction`* est vrai. La logique du script de traitement doit être gérée soit via un script appelable par le client (appelé via l'API GlideAjax), soit via un point de terminaison de ressource REST.

Consultez les exemples de pages d'interface utilisateur suivants pour en savoir plus :

- Exemple d'action d'interface utilisateur de liste connexe : Publier dans la liste de surveillance (nom de la page de l'interface utilisateur : publish_to_watchlist)
- Exemple d'action d'interface utilisateur de formulaire : Créer un problème (nom de page d'interface utilisateur : create_prb_change_inc)

Action d'interface utilisateur côté serveur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour activer les actions d'interface utilisateur côté serveur, vous devez effectuer les opérations suivantes :

La logique du script d'action d'interface utilisateur standard doit être traitée dans le cadre d'une ressource REST scriptée.

Consultez les exemples d'actions d'interface utilisateur de formulaire suivants pour en savoir plus :

- Créer une panne
- Annuler

Actions d'interface utilisateur du formulaire

Vous pouvez configurer les actions d'interface utilisateur affichées dans le Security Analyst Workspace fichier .

Conditions préalables:

Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles soient disponibles pour la configuration dans le Security Analyst Workspace. Consultez Activer les actions d'interface utilisateur pour en savoir plus.

Pour configurer une action d'interface utilisateur de formulaire pour , Security Analyst Workspace procédez comme suit :

1. Accédez à la **Incidents de sécurité** > **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Actions d'interface utilisateur de formulaire**.
2. Entrez les détails suivants :

Nom de champ	Description
Action	Sélectionnez une action d'interface utilisateur dans la liste de choix.
Type	Sélectionnez le type d'action. Cela peut être : ○ Action basée sur la boîte de dialogue : ce type d'action est utilisé lorsqu'une interaction ou des entrées de l'utilisateur sont nécessaires pour exécuter une logique métier spécifique. ○ Action côté serveur : cette action exécute la logique métier requise sans aucune entrée supplémentaire de l'utilisateur. **Remarque :** Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles soient disponibles pour la configuration dans le Security Analyst Workspace. Consultez Activer les actions d'interface utilisateur pour en savoir plus.
Application	Le nom du périmètre de l'application (Security Incident Response UI) dans lequel l'action d'interface utilisateur est ajoutée est affiché ici.
Action basée sur la boîte de dialogue Si vous sélectionnez Action basée sur la boîte de dialogue dans le champ Type, entrez les détails suivants :	
Page de l'IU	Sélectionnez la page de l'interface utilisateur associée à l'action.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

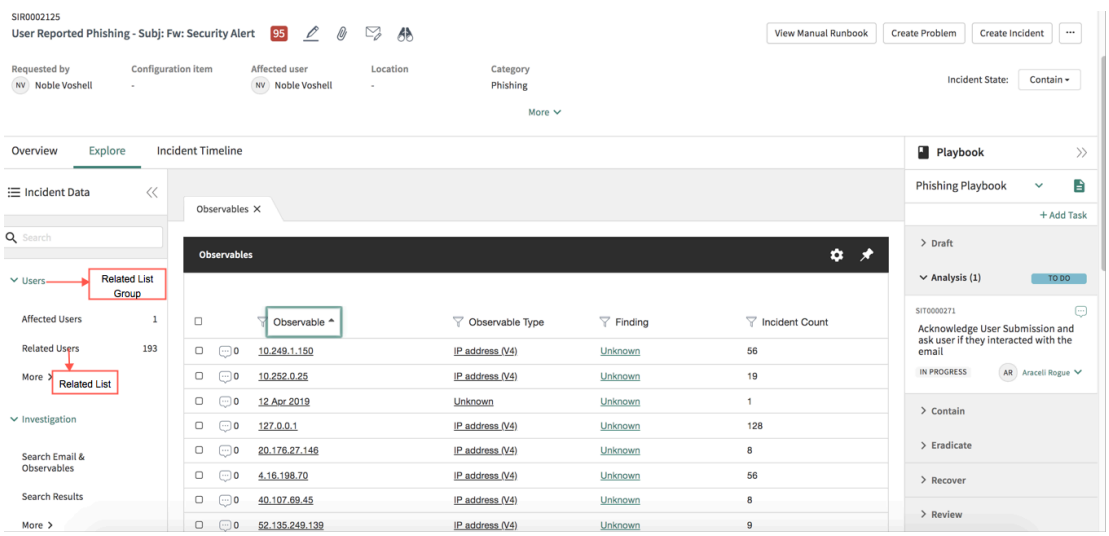
Nom de champ	Description
Titre de la boîte de dialogue	Entrez un titre pour l'action de boîte de dialogue.
Largeur et hauteur de la boîte de dialogue	Entrez la hauteur et la largeur de la boîte de dialogue en pixels.
Script	Pour la page d'interface utilisateur sélectionnée, vous pouvez spécifier des paramètres de requête supplémentaires ici. Le modèle fourni avec le système de base construit et renvoie `sysparm_sys_id` paramètre uniquement. Vous pouvez remplacer cela en spécifiant différents paramètres ici.
Action côté serveur Si vous sélectionnez Action côté serveur dans le champ Type, entrez les détails suivants :	
Ressource REST scriptée	Sélectionnez la ressource REST scriptée qui définit l'action. **Remarque :** L'ACL **d'analyste d'interface utilisateur SIR** doit être ajoutée à la ressource REST.

3. Cliquez sur **Envoyer**.
4. Accédez à la **Incidents de sécurité** > **Incidents (nouvelle interface utilisateur)** la page.
5. Cliquez sur le numéro d'un incident de sécurité pour afficher l'enregistrement de l'incident de sécurité. La nouvelle action d'interface utilisateur s'affiche en haut de la page.

Pour modifier une action d'interface utilisateur de formulaire existante, cliquez sur le nom de l'action pour accéder à la page Actions d'interface utilisateur du formulaire. Vous pouvez modifier le nom de l'action, le type et les autres champs en fonction du type sélectionné.

Configuration de la liste connexe

Vous pouvez ajouter de nouvelles listes connexes ou de nouveaux groupes de listes connexes, et modifier les groupes existants ou les listes connexes qui s'affichent dans l'.Security Analyst Workspace



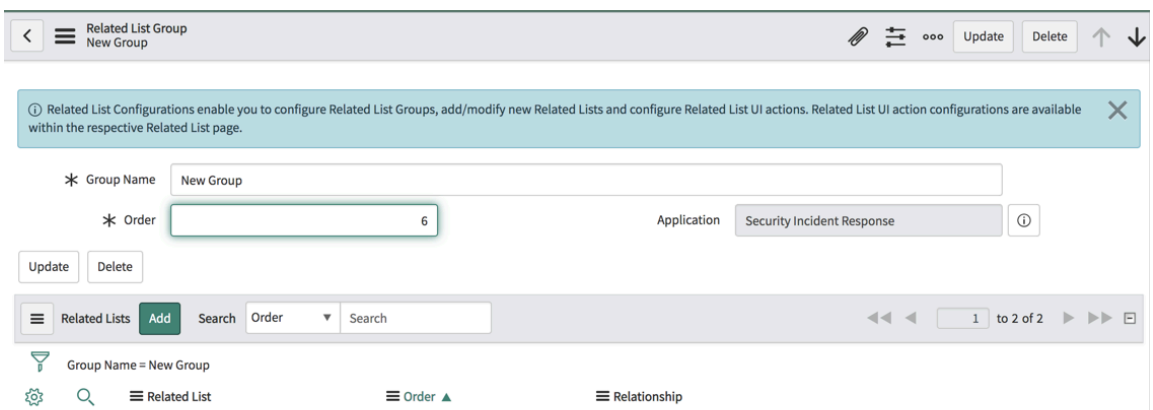
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter un groupe de listes connexes

Pour ajouter un groupe de liste connexe, procédez comme suit :

1. Accédez à la **Incidents de sécurité** > **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Configurations de la liste connexe**.
2. Cliquez sur **Nouveau** pour ajouter un nouveau groupe de Liste connexe. Entrez le nom du groupe et l'ordre dans lequel il doit apparaître sur la page Incidents (nouvelle interface utilisateur).
3. Cliquez sur **Envoyer**. Le groupe nouvellement ajouté apparaît dans la page Groupes de liste connexe.



Ajouter une liste connexe

Pour ajouter une nouvelle liste connexe, procédez comme suit :

1. Cliquez sur un lien de groupe de liste connexe.
2. Dans la section Listes connexes, cliquez sur **Ajouter** pour ajouter une nouvelle liste connexe.

   Si le bouton **Ajouter** n'est pas disponible, vérifiez si vous êtes dans le même périmètre de l'application que le groupe de liste connexe.
3. Sélectionnez la liste connexe à inclure dans le groupe.

   Remarque : Si vous ne voyez pas de liste connexe spécifique, procédez comme suit :

   a. Accédez à la **Interface utilisateur du système** > **Listes connexes** et recherchez les listes connexes présentes dans la table `sn_si_incident` .

   b. Cliquez sur la table `sn_si_incident` associée à la **nouvelle vue d'interface utilisateur SIR**.

   c. Dans la section Entrées de la liste connexe, cliquez sur **Nouveau** pour ajouter la liste connexe à la vue **Nouvelle interface utilisateur SIR** .
4. Indiquez l'ordre dans lequel il doit apparaître et cliquez sur **Soumettre**.

   La liste connexe que vous avez ajoutée apparaîtra dans le .Security Analyst Workspace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour modifier un groupe de liste connexe existant, cliquez sur son nom pour accéder à la page Groupe de liste connexe. Vous pouvez modifier le nom et l'ordre du groupe et ajouter ou supprimer des listes connexes du groupe.

Actions d'interface utilisateur de la liste connexe

Vous pouvez ajouter de nouvelles actions d'interface utilisateur aux listes connexes qui apparaissent dans le Security Analyst Workspace.

Conditions préalables:

Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles soient disponibles pour la configuration dans le Security Analyst Workspace. Consultez Activer les actions d'interface utilisateur pour en savoir plus.

Pour ajouter une nouvelle action d'interface utilisateur de la liste connexe, procédez comme suit :

1. Accédez à la **Incidents de sécurité** > **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Configurations de la liste connexe**.
2. Cliquez sur le nom du groupe. La page de configuration du groupe de listes connexes s'affiche.
3. Cliquez sur la liste connexe pour laquelle vous souhaitez ajouter une action d'interface utilisateur.
4. Cliquez sur **Ajouter** dans la section Actions d'interface utilisateur de la liste connexe.
5. Entrez les détails suivants :

Nom de champ	Description
Action	Sélectionnez une action d'interface utilisateur dans la liste de choix.
Type	Sélectionnez le type d'action. Cela peut être : ○ Action basée sur la boîte de dialogue : ce type d'action est utilisé lorsqu'une interaction ou des entrées de l'utilisateur sont nécessaires pour exécuter une logique métier spécifique. ○ Action côté serveur : cette action exécute la logique métier requise sans aucune entrée supplémentaire de l'utilisateur. **Remarque :** Avant de configurer des actions d'interface utilisateur, vous devez effectuer certaines étapes pour les activer afin qu'elles soient disponibles pour la configuration dans le Security Analyst Workspace. Consultez Activer les actions d'interface utilisateur pour en savoir plus.
Application	Le nom du périmètre de l'application (Security Incident Response UI) dans lequel l'action d'interface utilisateur est ajoutée est affiché ici.
Action basée sur la boîte de dialogue Si vous sélectionnez Action basée sur la boîte de dialogue dans le champ Type, entrez les détails suivants :	
Page de l'IU	Sélectionnez la page de l'interface utilisateur associée à l'action.
Titre de la boîte de dialogue	Entrez un titre pour l'action de boîte de dialogue.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description
Largeur et hauteur de la boîte de dialogue	Entrez la hauteur et la largeur de la boîte de dialogue en pixels.
Script	Pour la page d'interface utilisateur sélectionnée, vous pouvez spécifier des paramètres de requête supplémentaires ici. Le modèle fourni avec le système de base construit et renvoie uniquement les paramètres sysparm_incident_id, sysparm_record_table et sysparm_related_sys_ids . Vous pouvez les remplacer en spécifiant différents paramètres ici.
Action côté serveur Si vous sélectionnez Action côté serveur dans le champ Type, spécifiez les éléments suivants :	
Ressource REST scriptée	Sélectionnez la ressource REST scriptée qui définit l'action. **Remarque :** L'ACL **d'analyste d'interface utilisateur SIR** doit être ajoutée à la ressource REST.

6. Cliquez sur **Envoyer**.
7. Accédez à la **Incidents de sécurité** > **Incidents (nouvelle interface utilisateur)** la page.
8. Cliquez sur le numéro d'un incident de sécurité pour afficher l'enregistrement de l'incident de sécurité. Lancez la liste connexe respective pour afficher la nouvelle action d'interface utilisateur.

Propriétés système de configuration du formulaire

Ces propriétés système définissent les intervalles d'actualisation du formulaire pour les tâches du playbook.

Pour configurer ces propriétés, accédez à **Configuration d'Analyst Workspace (nouvelle interface utilisateur)** > **Propriétés d'Analyst Workspace**.

Propriété	Valeur par défaut	Description
sn_app_secops_ui.poller_interval.playbook_tasks	10000 ms	Intervalle de temps utilisé par le composant de playbook pour actualiser ses tâches de réponse pour chaque intervalle de temps configuré.
sn_app_secops_ui.poller_interval_count.playbook_tasks	9 fois	Nombre d'interrogations du composant Playbook pour les tâches de réponse.
sn_app_secops_ui.poller_interval.related_lists	30000 ms	Cet intervalle est utilisé par le composant Explore pour actualiser ses nombres de listes connexes pour chaque intervalle de temps configuré.

Activer les playbooks pour la sélection des analystes

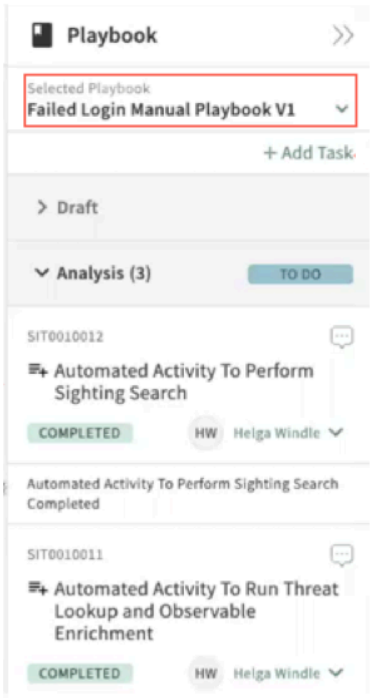
Ajouter de nouveaux playbooks à la liste de sélection de playbooks.

Vous pouvez sélectionner un playbook approprié pour enquêter sur les incidents de sécurité dans le Security Analyst Workspace (Gérer les menaces de sécurité à l'aide de l' Security Analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workspace). L'option de sélection de playbook ne prend en charge que les playbooks conçus à l'aide de Concepteur de flux.



Une fois que vous avez créé un playbook à l'aide de Concepteur de flux, procédez comme suit pour l'inclure dans la liste de choix de Playbooks sélectionnés :

1. Accédez à *sys_hub_flow* table.
2. Recherchez le nouveau playbook que vous avez créé à l'aide de Concepteur de flux.
3. Ajoutez la balise **sir_playbook** aux Playbooks que vous souhaitez inclure dans la liste de choix de Playbooks sélectionnés.

Remarque : Si vous avez d'anciens playbooks qui n'ont pas été migrés des workflows vers Flow Designer, ils n'apparaîtront pas dans la liste. Toutefois, si un playbook créé à l'aide de workflows est affecté à un incident de sécurité soit par une condition de déclenchement, soit par sélection manuelle (à l'aide de l'option **Exécuter l'orchestration** dans l'environnement classique), ce playbook est lancé lorsque vous ouvrez l'incident de sécurité dans le Security Analyst Workspace.

Dépannage de Security Incident Response

Cette section présente des conseils de dépannage importants et les questions fréquemment posées relatives à Réponse aux incidents de sécurité.

Problèmes de règles de contrôle d'accès

Les règles de contrôle d'accès autorisent l'accès à la ressource spécifiée si les trois conditions suivantes sont remplies :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'utilisateur a l'un des rôles spécifiés dans la liste **de rôles** , ou la liste est vide.
- Les conditions du champ **Condition** sont vraies, ou les conditions sont vides.
- Le script dans le champ **Script** (avancé) est vrai, ou définit la **réponse** variable sur vrai, ou est vide.

Pour en savoir plus sur les règles de contrôle d'accès, consultez Explorer les listes de contrôle d'accès

Important : Si l'option **Remplacement** administrateur est désactivée pour une table d'incidents de sécurité et si l'administrateur est en mesure d'accéder à la table d'incidents de sécurité, consultez KB1444673

Réponse aux incidents de sécurité Platform Analytics et Reporting

Platform Analytics et Reporting contiennent des tableaux de bord préconfigurés. Les tableaux de bord présentent des mesures importantes pour analyser votre Réponse aux incidents de sécurité processus, telles que les nouveaux incidents de sécurité ou l'ancienneté moyenne des incidents de sécurité ouverts.

Platform Analytics Les visualisations de données utilisent des données Analyse des performances *d'indicateur* pour vous montrer des données au fil du temps, ce qui vous aide à analyser vos processus business et à identifier des domaines d'amélioration. Avec Platform Analytics et Reporting, vous pouvez optimiser votre application avec Analyse des performances sans configuration minimale. Vous pouvez aussi toujours créer vos propres objets.

La Réponse aux incidents de sécurité Analyse des performances solution est disponible auprès du ServiceNow Store. Pour en savoir plus sur le téléchargement et l'installation de cette application, consultez Opérations de sécurité et ServiceNow Store.

Remarque : Pour évaluer les fonctionnalités, vous pouvez activer les solutions Analyse des performances et les analyses en formulaire sur des instances qui n'ont pas de licence Analyse des performances. Cependant, vous serez sujet aux limitations suivantes :

- Vous ne pouvez pas créer de nouveaux indicateurs.
- Vous ne pouvez pas collecter de données datant de plus de 180 jours.

Pour une fonctionnalité complète, achetez une licence Analyse des performances. Pour plus d'informations, consultez Activer votre abonnement Analyse des performances .

Important : Par défaut, la limite de collecte de données pour la propriété `(com.snc.pa.dc.max_records)` dans Analyse des performances est fixée à 5 000 enregistrements. Mais vous pouvez augmenter cette limite selon vos besoins, par exemple 50 000 enregistrements. Toutefois, l'augmentation de cette limite peut avoir un impact sur les performances lors de la collecte de données ou lors de l'exécution d'opérations sur la table Instantané. Pour en savoir plus sur les propriétés d'Analyse des performances, reportez-vous à la section Propriétés du Analyse des performances .

Information associée

Activer votre abonnement Analyse des performances

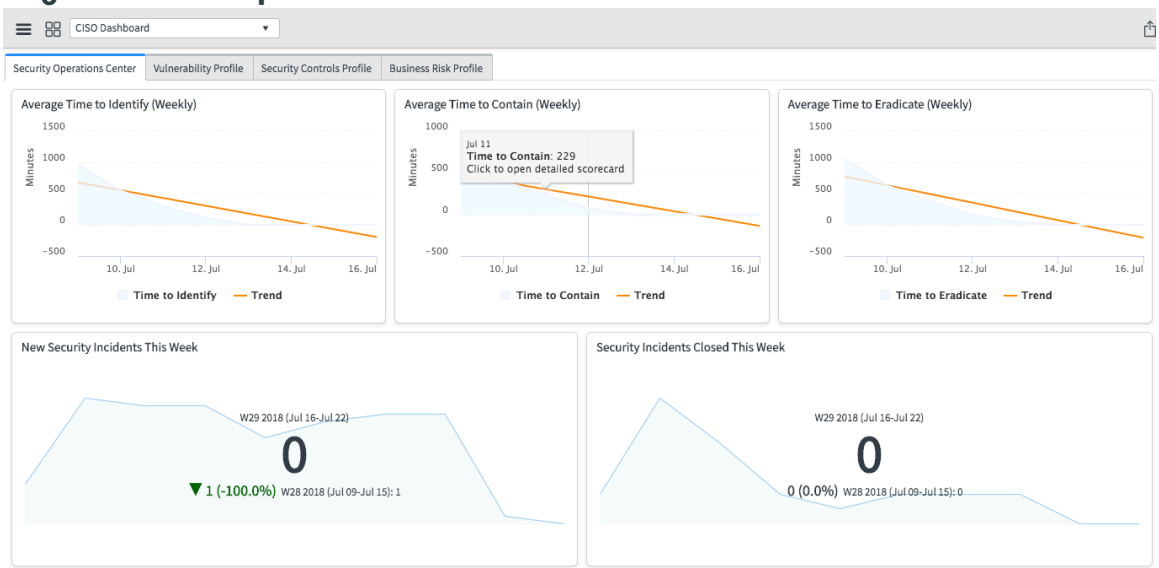
Tableau de bord des CISO

Ce tableau de bord révèle la posture de sécurité globale de votre organisation, y compris les vulnérabilités et les incidents de sécurité.

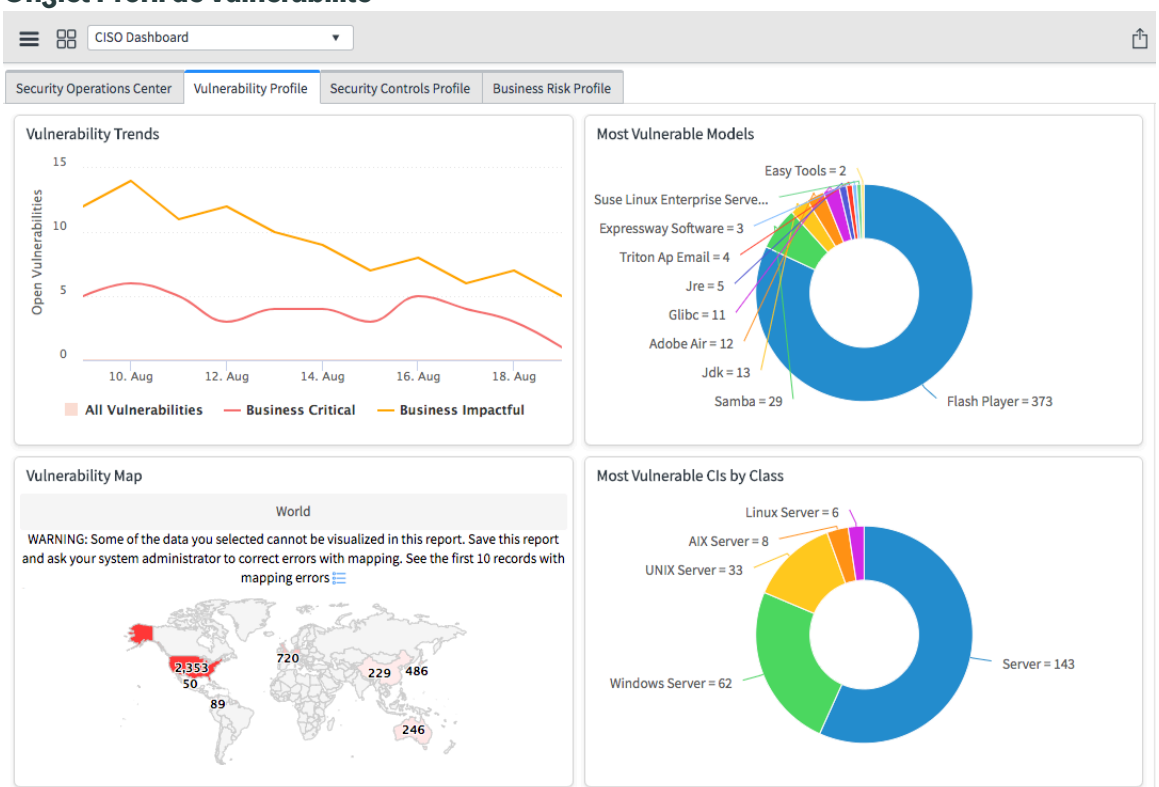
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Centre des opérations de sécurité



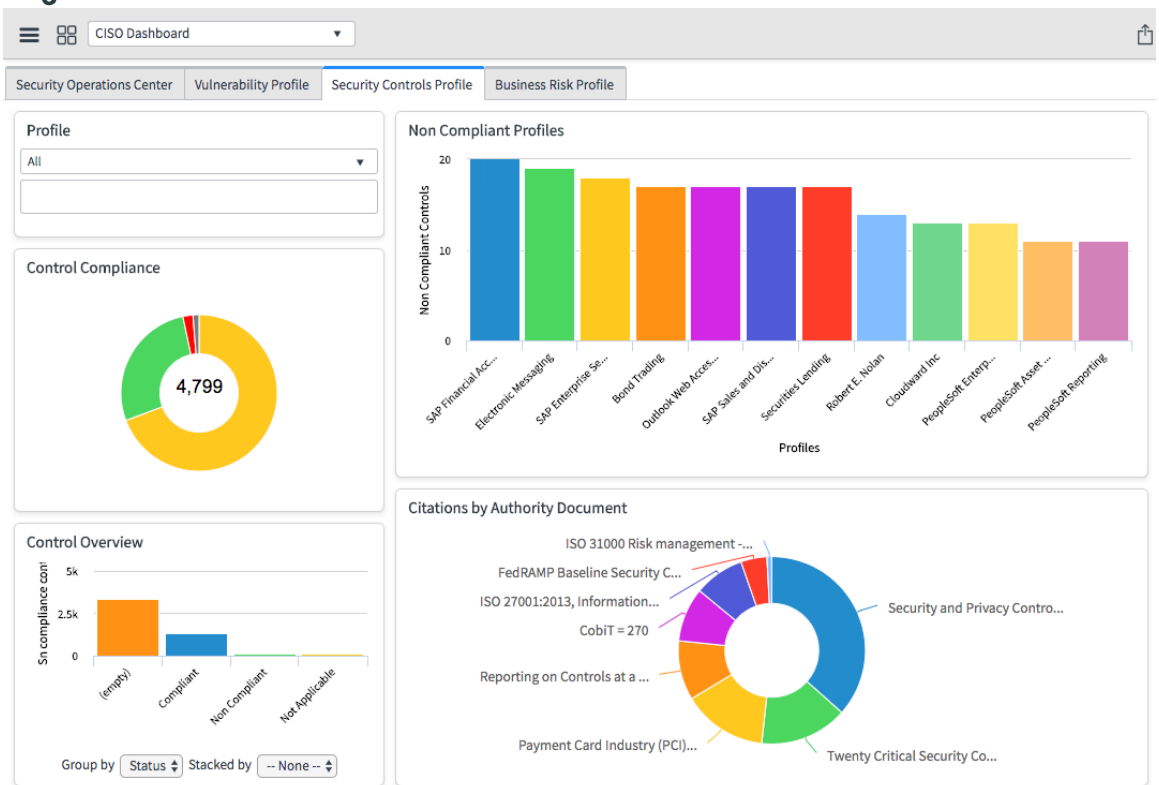
Onglet Profil de vulnérabilité



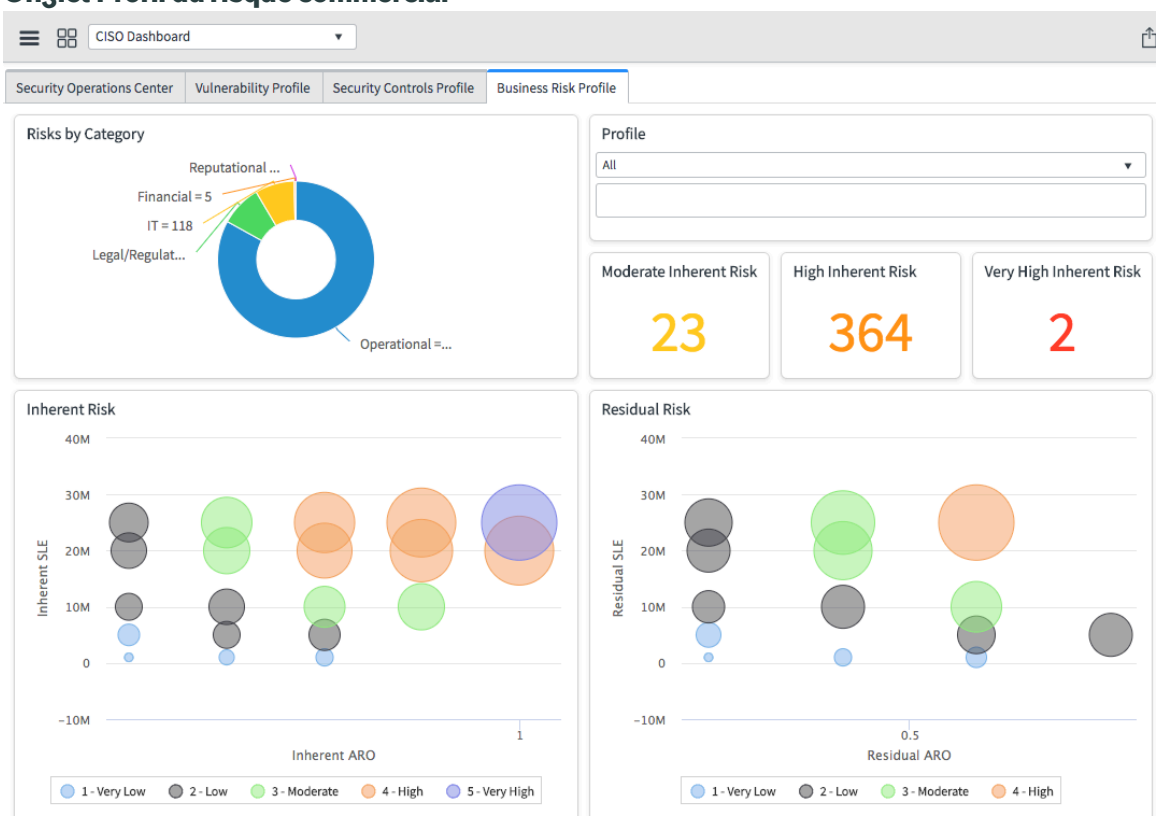
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Profil des contrôles de sécurité



Onglet Profil du risque commercial



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs finaux et rôles

Utilisateur final et objectif	Rôle requis
CISO : besoin d'une visibilité claire sur la posture de sécurité actuelle de l'organisation globale	sn_si.ciso

Indicateurs du tableau de bord des CISO

Le tableau de bord CISO présente les indicateurs clés de performance suivants :

SI : durée moyenne d'identification

Moyenne sur 7 jours du temps en minutes nécessaire à l'identification d'un incident de sécurité, calculée quotidiennement.

Délai moyen pour contenir

Moyenne sur 7 jours du temps en minutes nécessaire pour contenir un incident de sécurité, calculée quotidiennement.

Délai moyen pour éradiquer

Moyenne sur 7 jours du temps en minutes nécessaire pour éradiquer un incident de sécurité, calculée quotidiennement. Le délai moyen pour contenir et le délai moyen pour éradiquer sont tous deux basés sur l'indicateur SI : durée moyenne répartie par état d'incident de sécurité.

Nouveaux incidents de sécurité de cette semaine

Somme hebdomadaire du score de l'indicateur Nombre de nouveaux incidents de sécurité quotidien.

Incidents de sécurité clôturés (hebdomadaire)

Somme cumulée sur 7 jours de l'indicateur quotidien du nombre d'incidents de sécurité fermés.

Nouveaux incidents de sécurité, par priorité

Répartition quotidienne de l'indicateur Nombre de nouveaux incidents de sécurité par priorité.

Volume d'incidents de sécurité nouveaux par rapport à fermés (hebdomadaire)

Série chronologique de la somme cumulée sur 7 jours de l'indicateur Nombre de nouveaux incidents représentée graphiquement par rapport à la série chronologique de la somme cumulée sur 7 jours de l'indicateur Nombre d'incidents fermés.

Carte thermique des incidents de sécurité

Carte globale montrant le nombre d'incidents de sécurité ouverts dans chaque pays.

Arborescence des incidents de sécurité

Une arborescence interactive dans laquelle vous pouvez choisir de voir :

- Incidents de sécurité par service d'entreprise, répartis par criticité opérationnelle
- Incidents de sécurité répartis par catégorie ou sous-catégorie d'incident
- Incidents de sécurité par groupe d'affectation ou par délégataire
- « Statistiques sur les victimes » d'incident de sécurité par ressource affectée ou par utilisateur affecté

Répartitions

Les répartitions suivantes s'appliquent aux indicateurs du tableau de bord :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Criticité opérationnelle
- Groupe de sécurité
- Âge de l'incident de sécurité
- Catégorie d'incident de sécurité
- Code de fermeture de l'incident de sécurité
- Priorité de l'incident de sécurité
- État de l'incident de sécurité
- IS : service d'entreprise
- Vulnérabilité

Visualisations des données

Le tableau de bord comprend les visualisations suivantes :

Titre	Type	Description
Incidents de sécurité ouverts depuis plus de 30 jours par groupe d'affectation et par état	Carte thermique 	Affiche les modèles avec les éléments les plus vulnérables.
Risques par catégorie	Anneau 	Répertorie l'âge des éléments vulnérables rouverts.
Contenus des documents de référence par document de référence	Anneau 	Nombre de vulnérabilités actives
Incidents de sécurité avec un délégataire qui n'est pas actif	Carte thermique 	Affiche le nombre d'éléments vulnérables ouverts associés à des vulnérabilités (enregistrements CVE [Common Vulnerability Enumeration])), du plus important au moins élevé.
Incidents de sécurité non mis à jour pendant plus de 30 jours par groupe d'affectation et par état	Carte thermique 	Affiche les éditeurs avec les éléments les plus vulnérables.
Carte de vulnérabilité		Carte du monde montrant les vulnérabilités par emplacement
Modèles les plus vulnérables	Anneau 	Applications qui contiennent le plus de vulnérabilités
CI les plus vulnérables par classe	Anneau 	CI par type de serveur
Services avec des vulnérabilités d'importance critique	Liste 	
Profils non conformes	Barre 	Contrôles non conformes par profil
Vue d'ensemble des contrôles	Barre 	Nombre de contrôles conformes et non conformes
Exceptions de politique	Liste 	Exceptions de politique avec priorité, propriétaire et brève description

Traduction automatique

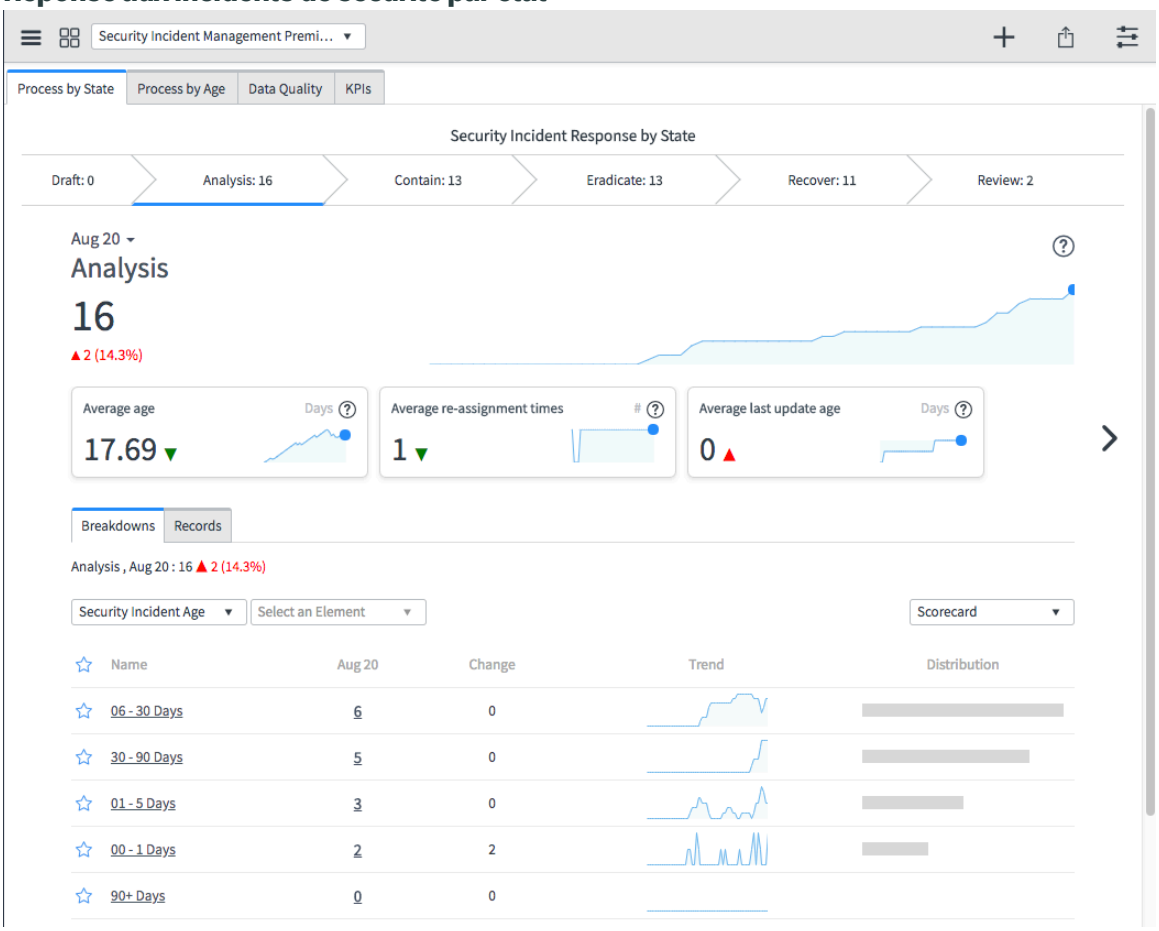
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre	Type	Description
Risques par catégorie	Anneau	Nombre de risques dans chaque catégorie de risque
Risque inhérent	Bulle	SLE inhérent vs ARO inhérent
Risque résiduel	Bulle	SLE résiduelle par rapport au ARO résiduel
Risques modérés, élevés et très élevés		Nombres de risques modérés, élevés et très élevés, respectivement
Risque par profil	Barre	Décompte des risques où vous pouvez sélectionner les éléments à regrouper et les éléments à empiler

Tableau de bord de premier plan de Gestion des incidents de sécurité

Ce tableau de bord utilise des visualisations avancées Platform Analytics pour aider les responsables de la sécurité à suivre le volume, les performances et la progression des incidents de sécurité, de l'analyse initiale/détection au confinement, à l'éradication et à la récupération. La version sous licence de Analyse des performances est donc requise.

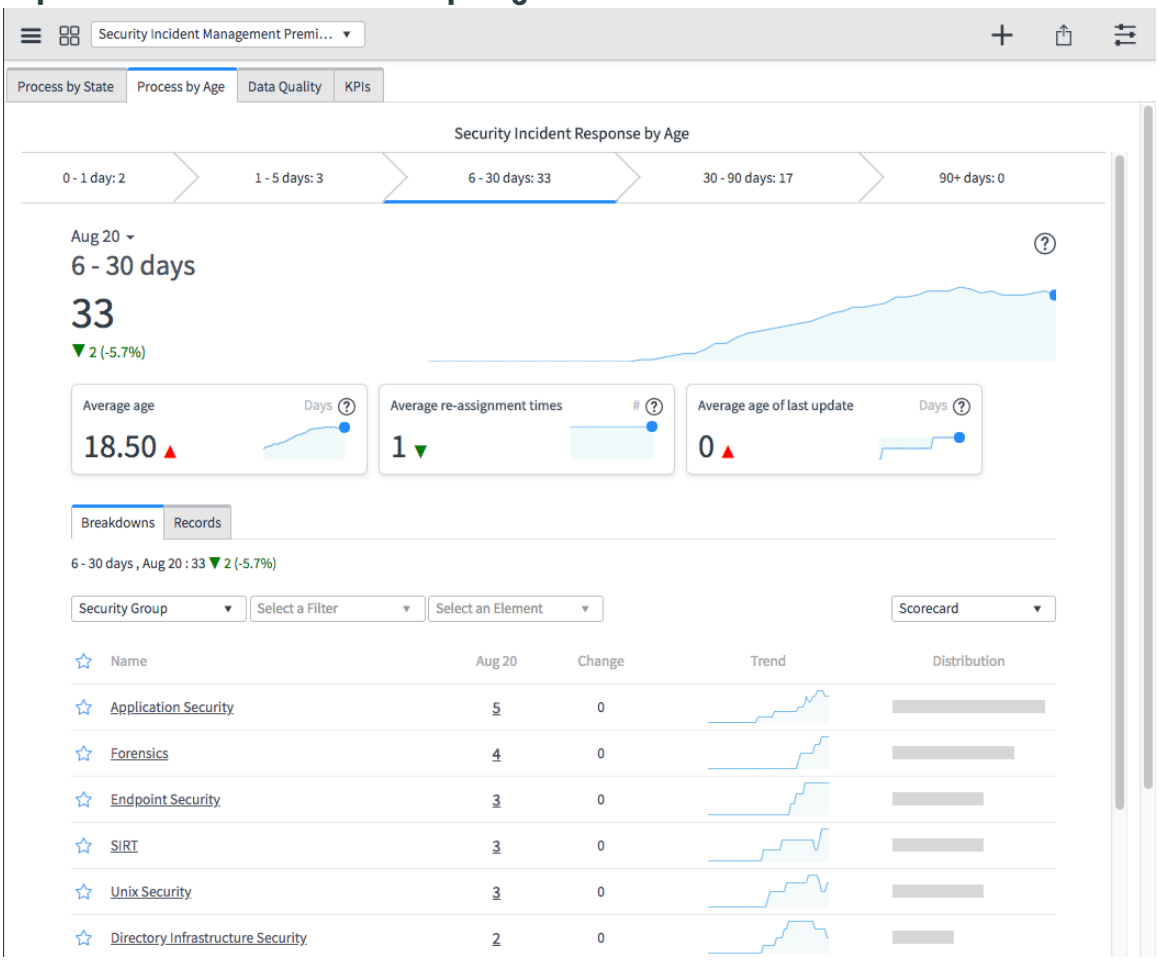
Réponse aux incidents de sécurité par état



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux incidents de sécurité par âge



Utilisateurs finaux et rôles

Utilisateur final et objectif	Rôle requis	Avantages
Gestionnaire de Security Response : nécessite une visibilité claire de l'état global et du volume des incidents de sécurité associés aux applications et aux services.	sn_si.manager	Peut examiner la posture de sécurité globale avec la possibilité d'ajuster les membres des groupes d'affectation.
Administrateur Security Response : doit identifier rapidement les zones de préoccupation et avoir un contrôle total sur toutes les données de Security Incident Response tout en administrant les territoires et les compétences, selon les besoins.	sn_si.admin	Peut ajuster les paramètres de calcul du risque pour s'assurer que les éléments vulnérables les plus pertinents pour l'organisation sont traités en premier.
Analystes des réponses de sécurité : besoin de hiérarchiser rapidement les vulnérabilités sur lesquelles se concentrer en fonction de leur criticité pour l'organisation.	sn_si.analyst	Les analystes de sécurité de niveau 1 et 2 travaillent sur les incidents de sécurité. Ils peuvent créer et mettre à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur final et objectif	Rôle requis	Avantages
		des changements et des pannes liés à leurs incidents.

Indicateurs de premier plan pour la gestion des incidents de sécurité

Les onglets Processus par état et Processus par âge contiennent des widgets de console avec les indicateurs suivants :

Âge moyen

L'indicateur Âge moyen des incidents de sécurité ouverts utilise la formule [[Âge cumulé des incidents de sécurité ouverts]] / [[Nombre d'incidents de sécurité ouverts]] / 24 pour donner un résultat en jours.

Délais moyens de réaffectation

L'indicateur Réaffectation moyenne des incidents de sécurité ouverts utilise la formule Réaffectation cumulée des incidents de sécurité ouverts/Nombre d'incidents de sécurité ouverts.

Âge moyen de la dernière mise à jour

L'indicateur Âge moyen de la dernière mise à jour des incidents de sécurité ouverts utilise la formule suivante : Âge cumulé de la dernière mise à jour des incidents de sécurité ouverts/Nombre d'incidents de sécurité ouverts/24 pour donner un résultat en jours.

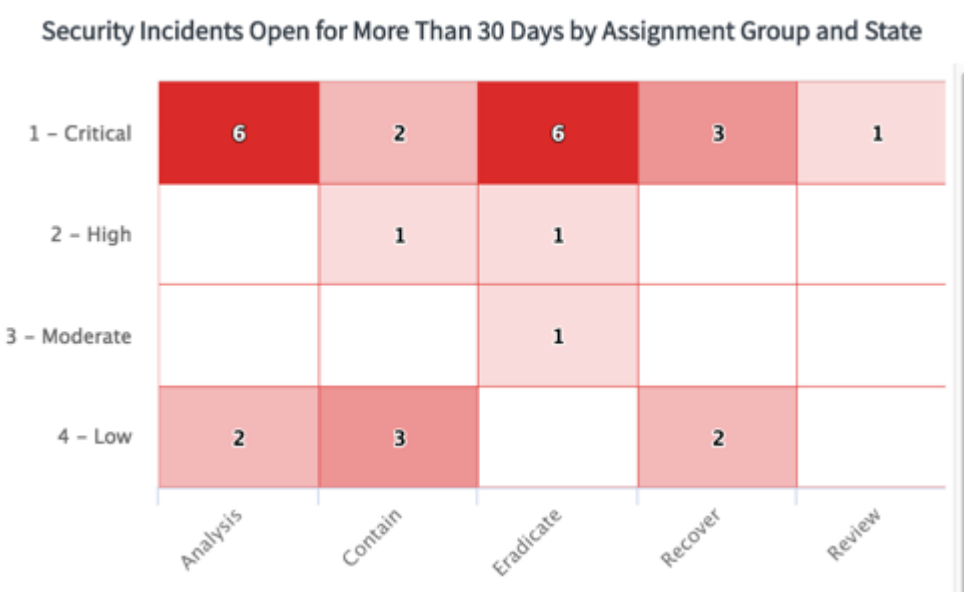
% non mis à jour en 5 jours

L'indicateur % d'incidents de sécurité ouverts non mis à jour au cours des 5 derniers jours utilise la formule ([[Nombre d'incidents de sécurité ouverts non mis à jour au cours des 5 derniers jours]] / [[Nombre d'incidents de sécurité ouverts]]) * 100.

L'onglet Qualité des données comporte des filtres interactifs pour la catégorie de l'incident de sécurité et les niveaux de risque, de priorité et de gravité. Ces filtres sont appliqués simultanément aux indicateurs suivants :

Incidents de sécurité ouverts depuis plus de 30 jours par groupe d'affectation et par état

Nombre d'incidents de sécurité ouverts filtrés pour une période de 30 jours et répartis par groupe d'affectation et état.



Incidents de sécurité avec un délégataire qui n'est pas actif

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nombre d’incidents de sécurité ouverts sans délégataire ou avec délégataire inactif.

Incidents de sécurité ouverts depuis plus de 30 jours par groupe d’affectation et par état

Indicateur Nombre d’incidents de sécurité ouverts non mis à jour au cours des 30 derniers jours, répartis par groupe d’affectation et par état.

L’onglet KPI comporte les indicateurs supplémentaires suivants :

- % de nouveaux incidents de sécurité critiques
- Âge moyen des incidents de sécurité ouverts
- Délai moyen de clôture des incidents de sécurité
- % d’incidents de sécurité qui ont été réaffectés
- % d’incidents de sécurité clôturés lors de leur première affectation
- % d’incidents de sécurité fermés par libre-service
- % d’incidents de sécurité non résolus
- Délai moyen de clôture des tâches d’incident de sécurité

Répartitions

Les répartitions suivantes s'appliquent aux indicateurs du tableau de bord :

- Groupe de sécurité
- Âge de l'incident de sécurité
- Catégorie d'incident de sécurité
- Priorité de l'incident de sécurité
- État de l'incident de sécurité

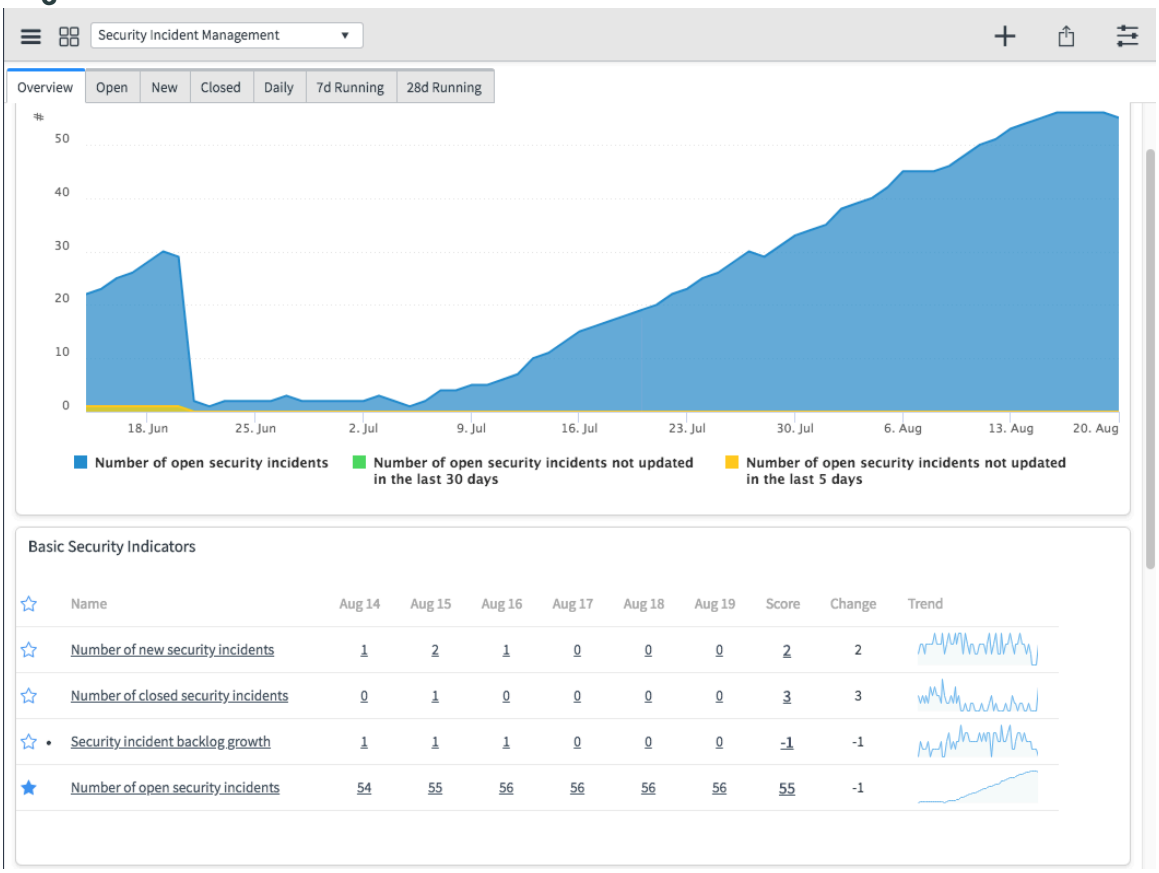
Tableau de bord de la gestion des incidents de sécurité

Grâce à ce tableau de bord, les responsables de la sécurité peuvent facilement suivre le volume, les performances et la progression des incidents de sécurité, de l’analyse et de la détection initiales au confinement, à l’éradication et à la récupération.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

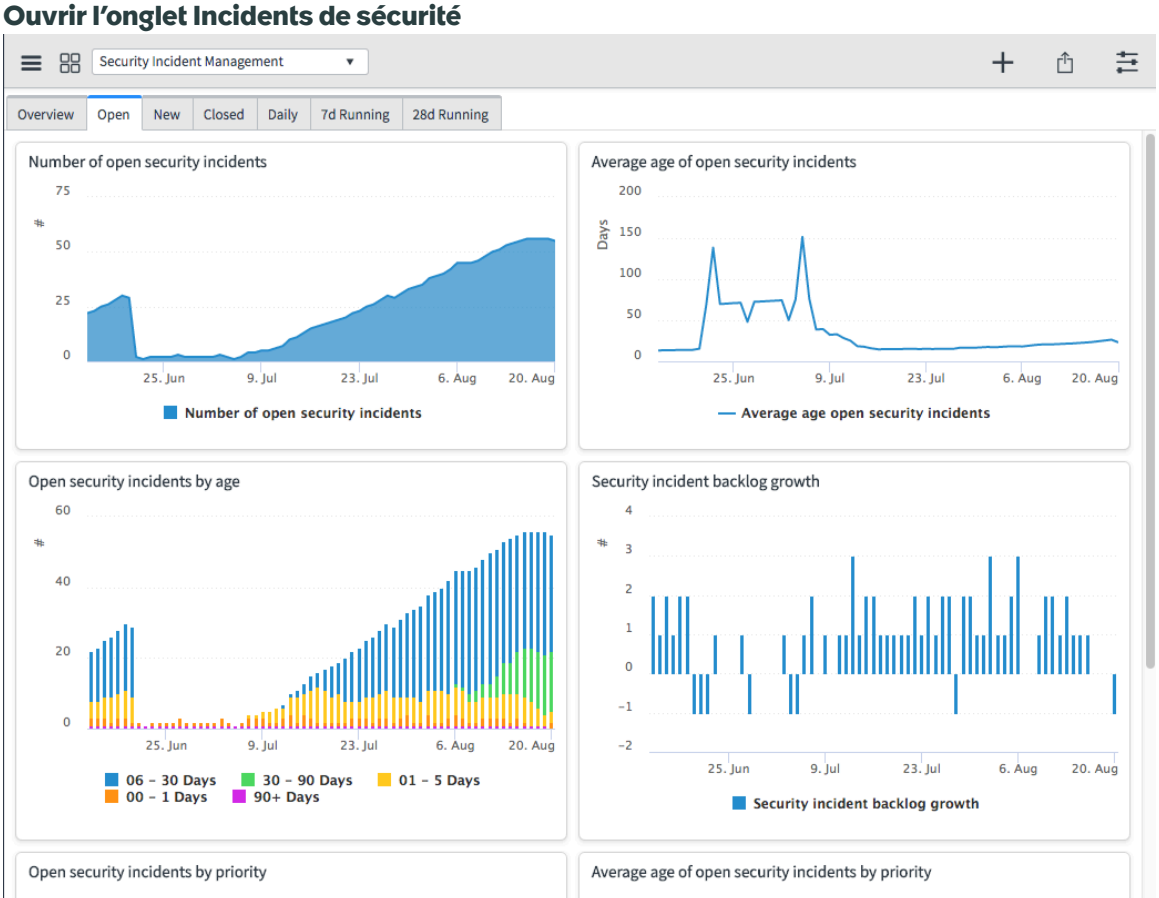
Onglet Vue d'ensemble



Basic Security Indicators

Name	Aug 14	Aug 15	Aug 16	Aug 17	Aug 18	Aug 19	Score	Change	Trend
Number of new security incidents	1	2	1	0	0	0	2	2	
Number of closed security incidents	0	1	0	0	0	0	3	3	
Security incident backlog growth	1	1	1	0	0	0	-1	-1	
Number of open security incidents	54	55	56	56	56	56	55	-1	

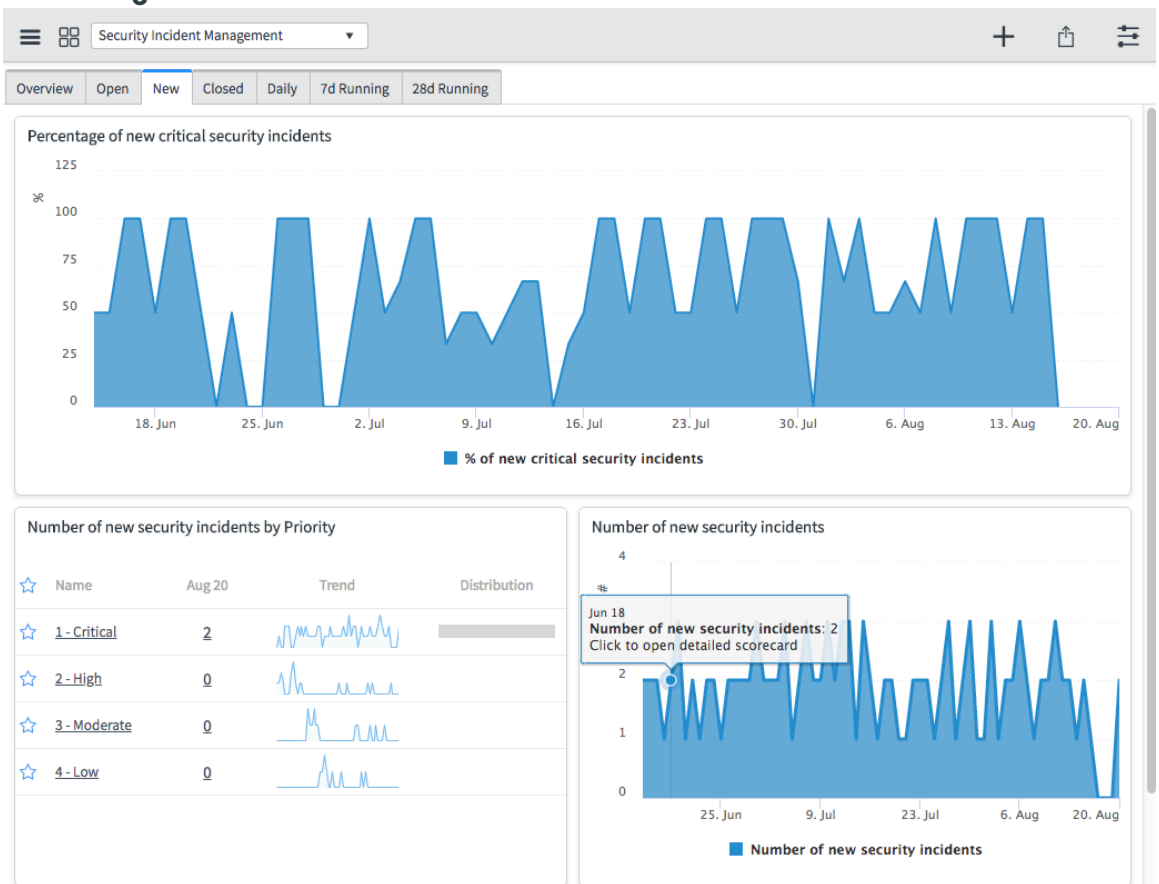
Ouvrir l'onglet Incidents de sécurité



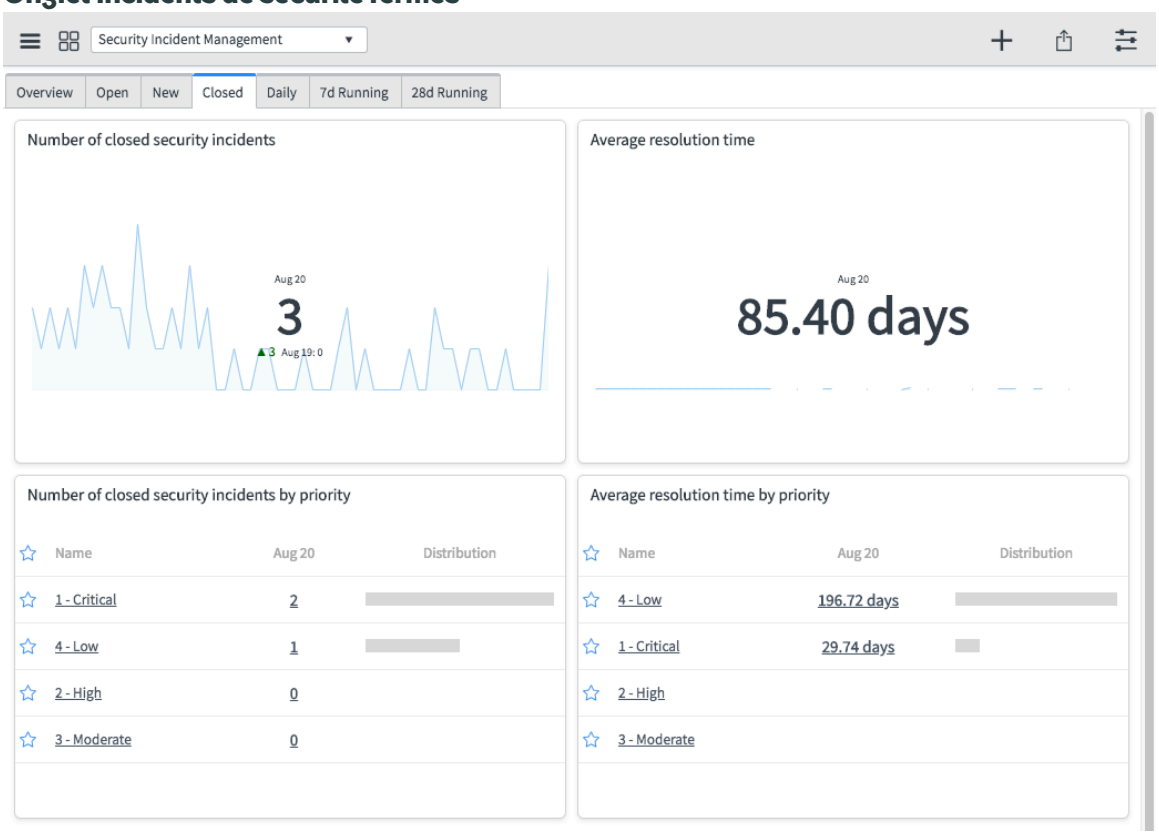
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nouvel onglet Incident de sécurité



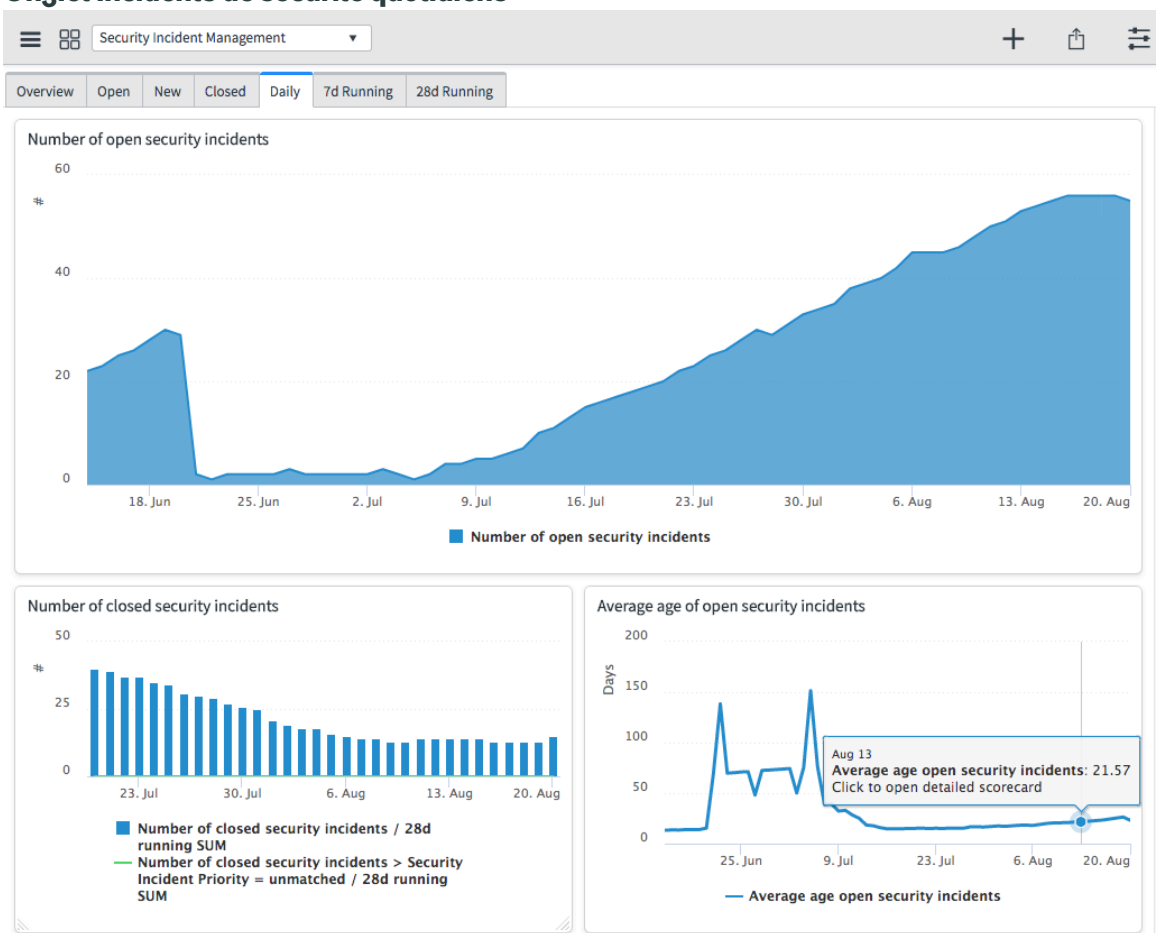
Onglet Incidents de sécurité fermés



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Incidents de sécurité quotidiens



Les onglets **7 jours consécutifs** et **28 jours consécutifs** suivent le format de l'onglet **quotidien** .

Utilisateurs finaux et rôles

Utilisateur final et objectif	Rôle requis	Avantages
Gestionnaire de Security Response : nécessite une visibilité claire de l'état global et du volume des incidents de sécurité associés aux applications et aux services.	sn_si.manager	Peut examiner la posture de sécurité globale avec la possibilité d'ajuster les membres des groupes d'affectation.
Administrateur Security Response : doit identifier rapidement les zones de préoccupation et avoir un contrôle total sur toutes les données de Security Incident Response tout en administrant les territoires et les compétences, selon les besoins.	sn_si.admin	Peut ajuster les paramètres de calcul du risque pour s'assurer que les éléments vulnérables les plus pertinents pour l'organisation sont traités en premier.
Analystes des réponses de sécurité : besoin de hiérarchiser rapidement les vulnérabilités sur lesquelles se concentrer en fonction de leur criticité pour l'organisation.	sn_si.analyst	Les analystes de sécurité de niveau 1 et 2 travaillent sur les incidents de sécurité. Ils peuvent créer et mettre à jour des incidents de sécurité, des demandes et des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur final et objectif	Rôle requis	Avantages
		tâches, ainsi que des problèmes, des changements et des pannes liés à leurs incidents.

Indicateurs de Gestion des incidents de sécurité

Le tableau de bord Gestion des incidents de sécurité présente les indicateurs clés de performance suivants :

Nouveaux incidents de sécurité

Graphique du nombre de nouveaux incidents de sécurité.

Incidents de sécurité ouverts

Graphique dans lequel vous pouvez comparer le nombre d'incidents de sécurité ouverts, le nombre d'incidents de sécurité ouverts non mis à jour au cours des 30 derniers jours et le nombre d'incidents de sécurité ouverts non mis à jour au cours des 5 derniers jours.

Indicateurs de sécurité de base

Les 6 derniers jours des scores du nombre de nouveaux incidents de sécurité, du nombre d'incidents de sécurité fermés, de la croissance du backlog des incidents de sécurité et du nombre d'indicateurs d'incidents de sécurité ouverts.

Nouveaux incidents de sécurité, par priorité

Nombre de nouveaux incidents de sécurité répartis par priorité.

Répartitions

Les répartitions suivantes s'appliquent aux indicateurs du tableau de bord :

- Groupe de sécurité
- Âge de l'incident de sécurité
- Catégorie d'incident de sécurité
- Priorité de l'incident de sécurité
- État de l'incident de sécurité

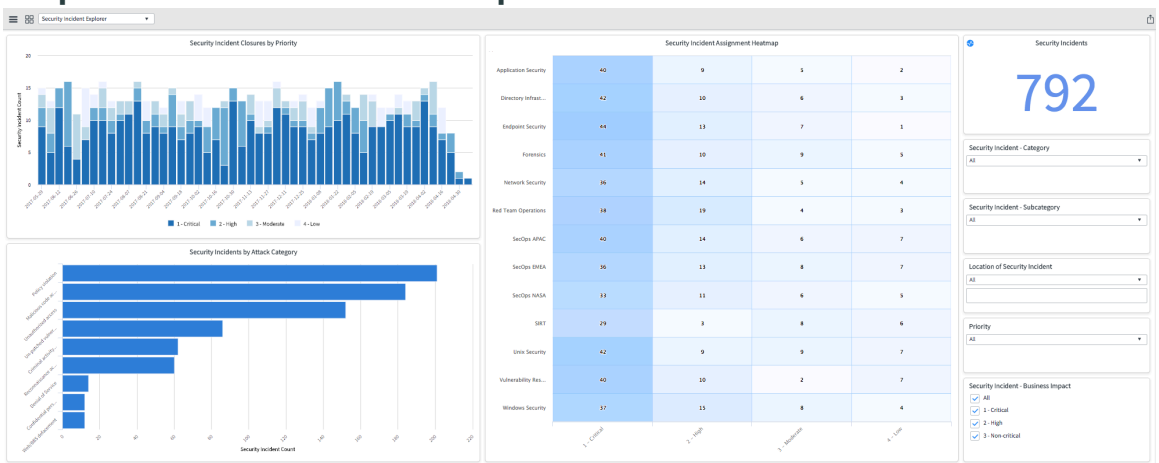
Tableau de bord de l'explorateur des incidents de sécurité

Grâce à ce tableau de bord, les responsables de la sécurité peuvent visualiser les incidents de sécurité résumés et regroupés par catégorie, sous-catégorie, emplacement, priorité et impact sur l'entreprise. Ces vues permettent aux responsables d'avoir rapidement un aperçu de la fréquence des attaques et des services aux entreprises touchés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue partielle du tableau de bord de l’explorateur d’incidents de sécurité



Utilisateurs finaux et rôles

Utilisateur final et objectif	Rôle requis	Avantages
Gestionnaire de Security Response : nécessite une visibilité claire de l’état global et du volume des incidents de sécurité associés aux applications et aux services.	sn_si.manager	Peut examiner la posture de sécurité globale avec la possibilité d’ajuster les membres des groupes d’affectation.
Administrateur Security Response : doit identifier rapidement les zones de préoccupation et avoir un contrôle total sur toutes les données de Security Incident Response tout en administrant les territoires et les compétences, selon les besoins.	sn_si.admin	Peut ajuster les paramètres de calcul du risque pour s’assurer que les éléments vulnérables les plus pertinents pour l’organisation sont traités en premier.
Analystes de Security Response : Besoin de hiérarchiser rapidement les vulnérabilités sur lesquelles se concentrer en fonction de leur criticité pour l’organisation.	sn_si.analyst	Les analystes de sécurité de niveau 1 et 2 travaillent sur les incidents de sécurité. Ils peuvent créer et mettre à jour des incidents de sécurité, des demandes et des tâches, ainsi que des problèmes, des changements et des pannes liés à leurs incidents.

Indicateurs de l’explorateur des incidents de sécurité

Le tableau de bord de l’explorateur d’incidents de sécurité présente les indicateurs clés de performance suivants :

Incidents de sécurité

Volume total d’incidents de sécurité ouverts et en attente.

Fermetures d'incidents de sécurité par priorité

Nombre d’incidents de sécurité fermés répartis par priorité.

Incidents de sécurité par catégorie d'attaque

Nombre d’incidents de sécurité ouverts, répartis par catégorie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Carte thermique d’affectation des incidents de sécurité

Répartition à deux niveaux du nombre d’incidents de sécurité ouverts, par groupe d’affectation et par priorité.

Carte thermique des incidents de sécurité

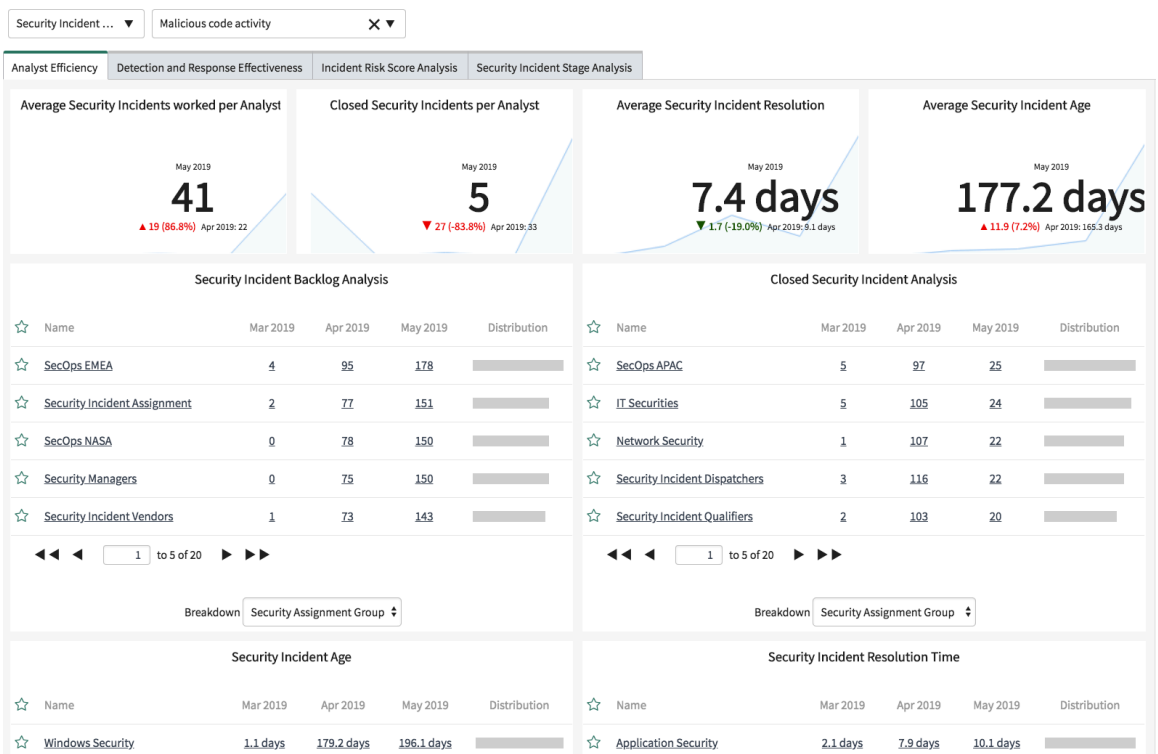
Carte globale montrant le nombre d’incidents de sécurité ouverts dans chaque pays.

Tableau de bord Efficience de Security Operations

Les gestionnaires du centre des opérations de sécurité (SOC) peuvent afficher les mesures d’efficacité globales et mesurer les performances individuelles des membres de l’équipe SOC au sein de l’organisation.

Le gestionnaire SOC peut utiliser le tableau de bord Analyse des performances pour améliorer l’efficacité et se faire une idée des performances du SOC dans des domaines généraux et spécifiques au fil du temps.

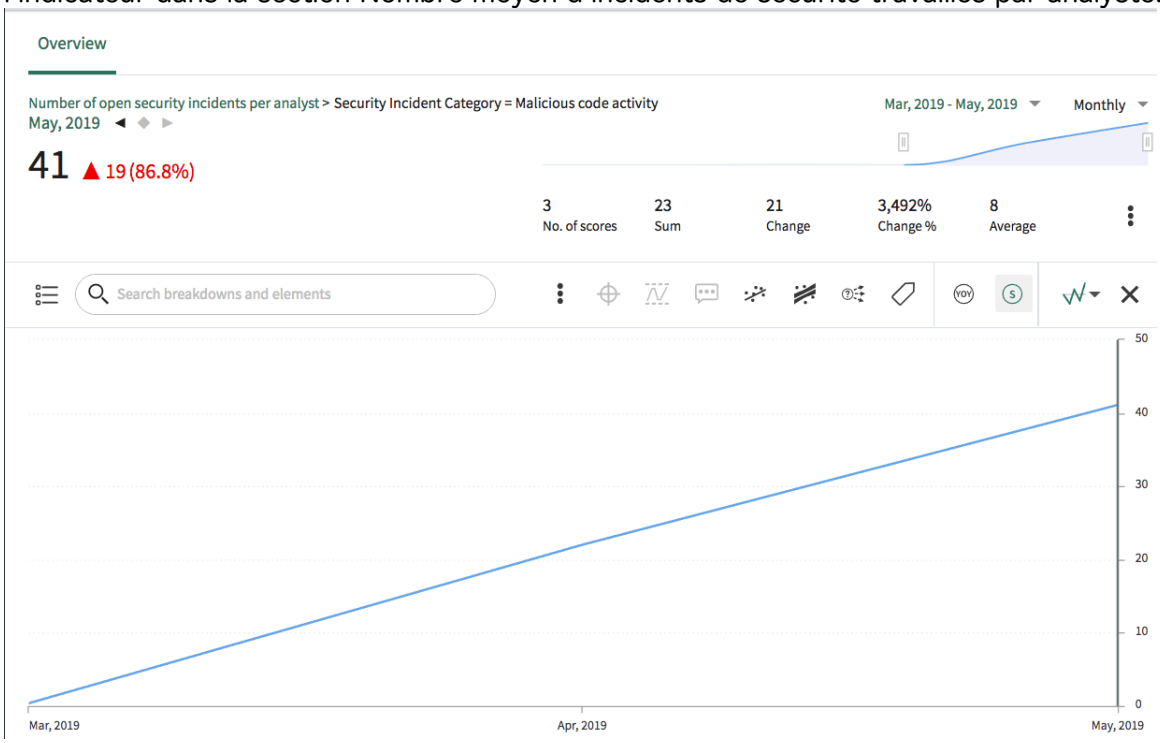
Onglet Efficacité de l’analyste



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cliquez sur l'un des indicateurs pour l'explorer plus en détail. Par exemple, cliquez sur l'indicateur dans la section Nombre moyen d'incidents de sécurité travaillés par analyste.



Le graphique montre que le nombre d'incidents de sécurité ouverts est passé de 0 en mars à plus de 40 en mai. Notez les données affichées dans l'en-tête :

- Indicateur de tendance : affiche la variation du nombre d'incidents ouverts au cours de la dernière période pour laquelle les données ont été collectées. Ce graphique montre les données pour la période de mars 2019 à mai 2019 et le nombre d'incidents ouverts a augmenté de 19 au mois de mai. L'efficacité des analystes est meilleure si le nombre d'incidents ouverts a diminué au fil du temps.
- Non. des scores : La période pour laquelle les données ont été collectées (mars à mai 2019).
- Somme : nombre de nouveaux incidents ouverts pour la période entre mars et mai.
- Changement : nombre de nouveaux incidents ouverts entre mars et avril.
- Moyenne : nombre moyen d'incidents ouverts par analyste pour la période sélectionnée.

Onglet Efficacité de l'analyste

Indicateur	Description
Nombre moyen d'incidents de sécurité travaillés par analyste	Nombre moyen d'incidents de sécurité ouverts par analyste pour la période spécifiée. La formule utilisée est la suivante : [[Nombre d'incidents de sécurité ouverts / MOY par mois +]] / [[Nombre d'agents de sécurité]]
Incidents de sécurité fermés par analyste	Nombre total d'incidents fermés par chaque analyste dans la catégorie sélectionnée au cours de la période spécifiée. La formule utilisée est la suivante : [Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = <category_name> / SOMME par mois +]] / [[Nombre d'agents de sécurité / MOY par mois +]]
Résolution moyenne des incidents de sécurité	Délai moyen nécessaire à chaque analyste pour fermer les incidents de sécurité au cours de la période spécifiée. La formule utilisée pour afficher le résultat en jours

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

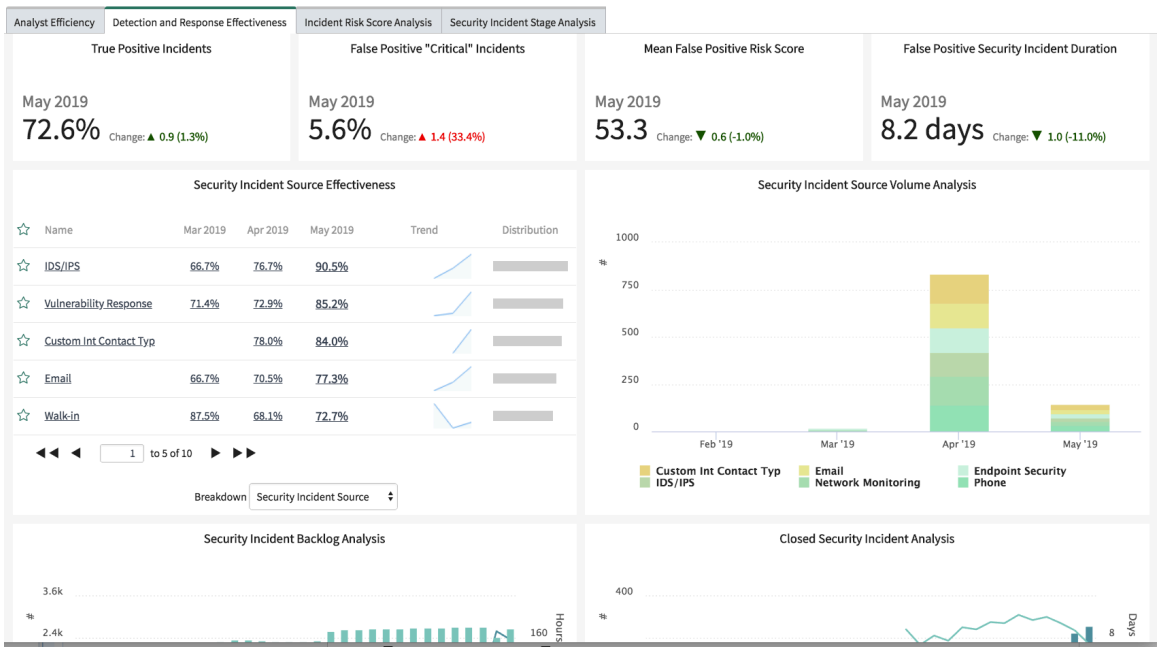
Onglet Efficacité de l'analyste (suite)

Indicateur	Description
	est la suivante : ([[Durée cumulée des incidents de sécurité fermés > catégorie d'incident de sécurité = <category_name> / MOY par mois +]] / [[Nombre d'incidents de sécurité fermés > catégorie d'incident de sécurité = <category_name> / MOY par mois +]]) / 24
Âge moyen de l'incident de sécurité	Nombre moyen de jours pendant lesquels les incidents de sécurité restent ouverts pour chaque analyste. La formule utilisée pour afficher le résultat en jours est la suivante : ([[Âge cumulé des incidents de sécurité ouverts > la catégorie d'incident de sécurité = <category_name> / MOY par mois +]] / [[Nombre d'incidents de sécurité ouverts > la catégorie d'incident de sécurité = <category_name> / MOY par mois +]]) / 24
Analyse en backlog d'incidents de sécurité	Nombre total d'incidents de sécurité ouverts au cours de la période spécifiée. Sélectionnez une option dans la liste Répartition pour afficher le backlog de chaque analyste, groupe de sécurité, priorité, etc. Vous pouvez également comparer le nombre d'incidents de sécurité ouverts entre deux mois sélectionnés.
Analyse des incidents de sécurité fermés	Nombre total d'incidents de sécurité qui sont fermés au cours de la période spécifiée. Sélectionnez une option dans la liste Répartition pour afficher le nombre de chaque analyste, groupe de sécurité, priorité, etc. Vous pouvez également comparer le nombre d'incidents de sécurité qui ont été fermés entre deux mois sélectionnés.
Âge de l'incident de sécurité	Le nombre moyen de jours pendant lesquels les incidents de sécurité restent ouverts au cours de la période spécifiée. Sélectionnez une option dans la liste Répartition pour afficher l'âge de l'incident de sécurité pour chaque analyste, groupe de sécurité, priorité, etc. La formule utilisée pour afficher le résultat en jours est la suivante : ([[Âge cumulé des incidents de sécurité ouverts > la catégorie d'incident de sécurité = <category_name> > Groupe d'affectation de sécurité = <group_name> / MOY par mois +]] / [[Nombre d'incidents de sécurité ouverts > la catégorie d'incident de sécurité = <category_name> > Groupe d'affectation de sécurité = <group_name> / MOY par mois +]]) / 24
Délai de résolution des incidents de sécurité	Nombre moyen de jours nécessaires pour résoudre les incidents de sécurité au cours de la période spécifiée. Sélectionnez une option dans la liste Répartition pour afficher le délai de résolution des incidents de sécurité pour chaque analyste, groupe de sécurité, priorité, etc. La formule utilisée pour afficher le résultat en jours est la suivante : ([[Durée cumulée des incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité de code malveillant > Sécurité affectée à = John Ashby / MOY par mois +]] / [[Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = John Ashby / MOY par mois +]]) / 24

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Efficacité de la détection et de la réponse



Onglet Efficacité de la détection et de la réponse

Indicateur	Description
Incidents avec de vrais positifs	Pourcentage d'incidents de sécurité vrais positifs dans la catégorie sélectionnée pour la période spécifiée. La formule utilisée est la suivante : (1-([[Nombre d'incidents de sécurité signalés comme faux positifs > Catégorie d'incident de sécurité = Activité du code malveillant / SOMME par mois +]] / [[Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant / SOMME par mois +]])) * 100
Incidents critiques signalés comme faux positifs	Pourcentage d'incidents de sécurité critiques signalés comme faux positifs dans la catégorie sélectionnée pour la période spécifiée. La formule utilisée est la suivante : ([[Nombre d'incidents de sécurité signalés comme faux positifs > score de risque d'incident de sécurité = risque critique > catégorie d'incident de sécurité = activité du code malveillant / SOMME par mois +]] / [[nombre d'incidents de sécurité fermés > catégorie d'incident de sécurité = activité de code malveillant / SOMME par mois +]]) * 100 **Remarque :** Tout incident de sécurité dans lequel le code Fermé = Vulnérabilité non valide ou Faux positif est traité comme un incident de faux positif

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Efficacité de la détection et de la réponse (suite)

Indicateur	Description
Score moyen de risque de faux positif	Score de risque mensuel moyen des incidents de sécurité fermés qui ont été identifiés comme des incidents de faux positif. Un score de risque plus faible indique que les analystes de sécurité ont passé moins de temps à analyser les incidents signalés comme faux positifs. La formule utilisée est la suivante : ([[Nombre d'incidents de sécurité signalés comme faux positifs > score de risque d'incident de sécurité = risque critique > catégorie d'incident de sécurité = activité du code malveillant / SOMME par mois +]] / [[nombre d'incidents de sécurité fermés > catégorie d'incident de sécurité = activité de code malveillant / SOMME par mois +]]) * 100
Durée de l'incident de sécurité signalé comme faux positif	Nombre moyen de jours que les analystes de sécurité ont consacrés à enquêter sur les incidents signalés comme faux positifs. La formule utilisée est ([[Durée cumulée des incidents de sécurité signalés comme faux positifs]] / [[Nombre d'incidents de sécurité signalés comme faux positifs]]) / 24
Efficacité des sources d'incidents de sécurité	Pourcentage d'incidents de sécurité vrais positifs identifiés par une source spécifique pour la période spécifiée. La source peut être un e-mail, une activité réseau, le support client, etc. Ces données permettent de mesurer l'efficacité de la source d'incident de sécurité. La formule utilisée est la suivante : (1-([[Nombre d'incidents de sécurité signalés comme faux positifs > Catégorie d'incident de sécurité = Activité du code malveillant > Source d'incident de sécurité = IDS/IPS / SOMME par mois +]] / [[Nombre d'incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant > Source d'incident de sécurité = IDS/IPS / SOMME par mois +]])) * 100
Analyse du volume source des incidents de sécurité	Nombre d'incidents de sécurité fermés pour le mois en cours pour chaque source d'incident de sécurité. Vous pouvez également comparer le nombre d'incidents de sécurité pour chaque type de source entre deux mois sélectionnés.
Analyse en backlog d'incidents de sécurité	Nombre total d'incidents de sécurité ouverts au cours de la période spécifiée et nombre moyen de jours pendant lesquels les incidents restent ouverts. Vous pouvez également comparer le nombre d'incidents de sécurité ouverts entre deux mois sélectionnés. La formule utilisée pour calculer la période de backlog moyenne est la suivante : ([[Âge cumulé des

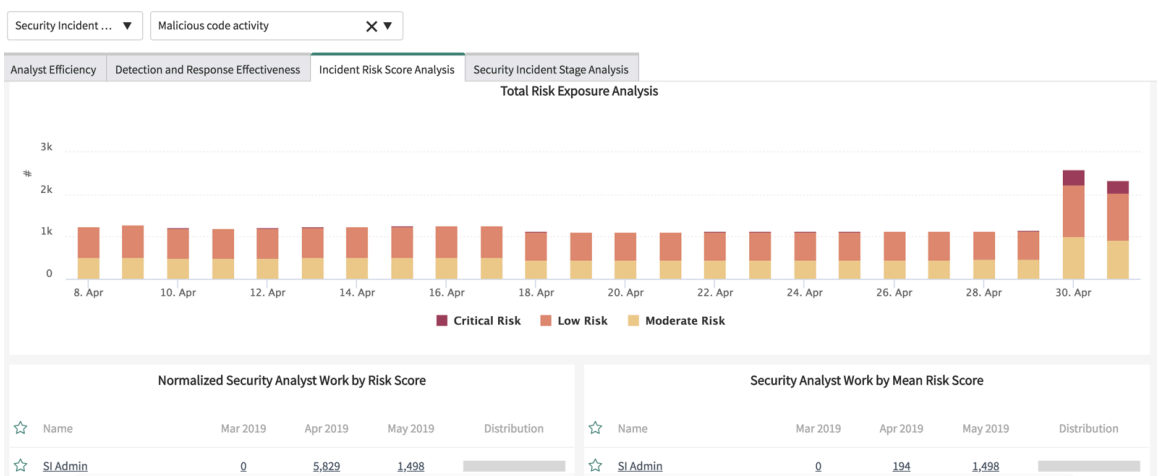
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Efficacité de la détection et de la réponse (suite)

Indicateur	Description
	incidents de sécurité ouverts > Catégorie d'incident de sécurité = Activité du code malveillant]] / [[Nombre d'incidents de sécurité ouverts > Catégorie d'incident de sécurité = Activité du code malveillant]]) / 24
Analyse des incidents de sécurité fermés	Nombre total d'incidents de sécurité fermés au cours de la période spécifiée et délai de résolution moyen de ces incidents. La formule utilisée pour calculer le délai de résolution moyen est la suivante : ([[durée cumulée des incidents de sécurité fermés > catégorie d'incident de sécurité = activité de code malveillant]] / [[nombre d'incidents de sécurité fermés > catégorie d'incident de sécurité = activité de code malveillant]]) / 24

Onglet Analyse du score de risque d'incident



Onglet Analyse du score de risque d'incident

Indicateur	Description
Analyse totale de l'exposition au risque	Nombre total d'incidents ouverts dans chaque catégorie de risque (faible, modéré et critique) au cours de la période spécifiée. Vous pouvez également comparer le nombre d'incidents dans les différentes catégories de risque entre deux mois.
Travail d'analyste de sécurité normalisé par score de risque	Score de risque total de chaque analyste de sécurité pour la période spécifiée. Cette valeur est calculée sur la base du nombre d'incidents de sécurité vrais positifs que l'analyste de sécurité a fermés. La formule utilisée est la suivante : [[Cumul des scores de risque des incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité

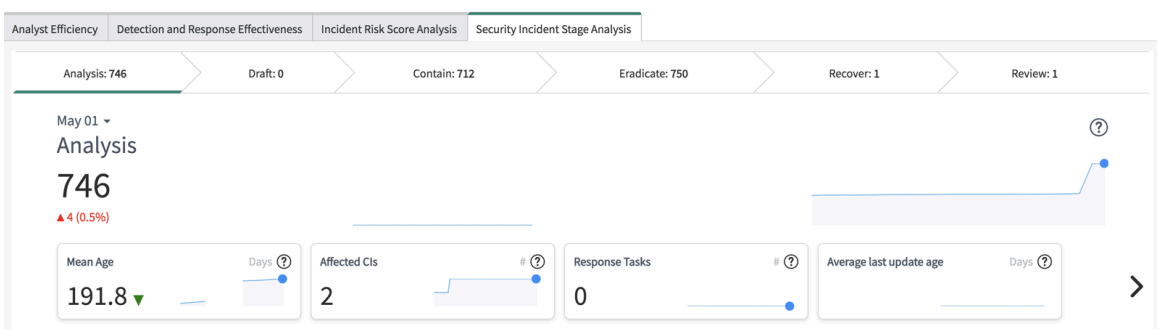
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Analyse du score de risque d'incident (suite)

Indicateur	Description
	affectée à = Administrateur SI / SOMME par mois +]] - [[Score de risque cumulé des incidents de sécurité signalés comme faux positifs > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = Administrateur SI / SOMME par mois +]]
Travail d'analyste de sécurité par score de risque moyen	Score de risque moyen de chaque analyste de sécurité pour la période spécifiée. La formule utilisée est la suivante : [[Cumul des scores de risque des incidents de sécurité fermés > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = Administrateur SI / MOY par mois +]] - [[Score de risque cumulé d'incidents de sécurité signalés comme faux positifs > Catégorie d'incident de sécurité = Activité du code malveillant > Sécurité affectée à = Administrateur SI / MOY par mois +]]

Onglet Analyse de l'étape de l'incident de sécurité



Vous pouvez afficher le nombre d'incidents ouverts sur un jour spécifique et leur état (analyse, brouillon, contenir, éradiquer, récupérer ou examiner) de ces incidents. À chaque étape, vous pouvez afficher l'âge moyen, les CI affectés, les tâches de réponse, etc. Cliquez sur un lien pour afficher des détails supplémentaires ou la répartition de ces incidents.

Espace de travail de la Réponse aux incidents de sécurité

Il s'agit ServiceNow® Espace de travail de la Réponse aux incidents de sécurité d'une interface réinventée qui offre une expérience utilisateur de nouvelle génération aux analystes de la sécurité et aux gestionnaires SOC. Les analystes de sécurité peuvent l'utiliser pour gérer le cycle de vie des incidents de sécurité, de l'analyse initiale au confinement, en passant par l'éradication et la récupération.

Introduction à Espace de travail SIR

Sélectionnez une tuile pour commencer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer l’espace de travail



En savoir plus sur les concepts et les fonctionnalités de l’espace de travail SIR

Administrateurs à l’aide de l’espace de travail



Configurer l’espace de travail et les fonctionnalités SIR

Analystes à l’aide de l’espace de travail



Découvrez comment les analystes utilisent l’espace de travail SIR

Afficher les tableaux de bord SIR



Afficher les tableaux de bord de l’espace de travail SIR

Traduction automatique

Demander des applications dans l’App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Important :

- L'installation de la Réponse aux incidents de sécurité version 13.4.5 ou ultérieure à partir de la ServiceNow StoreEspace de travail de la Réponse aux incidents de sécurité version sn_si_aw 1.5.1 ou ultérieure sera automatiquement installée par défaut. Pour plus d'informations sur les applications dépendantes, reportez-vous à la Espace de travail SIR Modules d'extension et rôles section.
- Veuillez noter que les versions 1.5.1 et supérieures de l'espace de travail Réponse aux incidents de sécurité ne peuvent être installés/mis à niveau que par le biais d'une installation/mise à niveau de Réponse aux incidents de sécurité et ne peuvent pas être installés indépendamment.

Plus de ressources

Visitez le Réponse aux incidents de sécurité forum sur le ServiceNow Community.

Explorer Espace de travail SIR

Explorez Espace de travail de la Réponse aux incidents de sécurité pour comprendre comment les analystes et les gestionnaires de sécurité effectuent leurs opérations quotidiennes avec une expérience utilisateur améliorée, effectuer une enquête complète sur les incidents et obtenir une vue d'ensemble des incidents de sécurité, des tâches de réponse et des SLA affectés à l'analyste et à l'équipe de sécurité.

Cette section décrit les éléments suivants :

- Espace de travail SIR modules d'extension et rôles requis.
- Fonctionnalités principales Espace de travail SIR .

Espace de travail SIR Modules d'extension et rôles

Voici les applications requises pour travailler avec Espace de travail de la Réponse aux incidents de sécurité le module d'extension (sn_si_aw).

Applications

L'installation de la version 13.4.5 ou ultérieure de l'application Réponse aux incidents de sécurité installe automatiquement le Espace de travail de la Réponse aux incidents de sécurité et les applications suivantes.

- Gestion des tickets de sécurité d'entreprise PAD Commons [sn_escm_pad_cmn]
- Espace de travail commun Security Operations [sn_escm_ws_cmn]
- Composant de carte d'interface utilisateur d'incident de sécurité [sn_sirw_evam]
- Spoke Security Operations [sn_sec_spoke]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

- L'installation de la Réponse aux incidents de sécurité version 13.4.5 ou ultérieure à partir de la ServiceNow StoreEspace de travail de la Réponse aux incidents de sécurité version sn_si_aw 1.5.1 ou ultérieure sera automatiquement installée par défaut. Pour plus d'informations sur les applications dépendantes, reportez-vous à la Espace de travail SIR Modules d'extension et rôles section.
- Veuillez noter que les versions 1.5.1 et supérieures de l'espace de travail Réponse aux incidents de sécurité ne peuvent être installés/mis à niveau que par le biais d'une installation/mise à niveau de Réponse aux incidents de sécurité et ne peuvent pas être installés indépendamment.

Gestion des tickets de sécurité d'entreprise PAD Commons nécessite le module d'extension Expérience de playbook [playbook_experience].

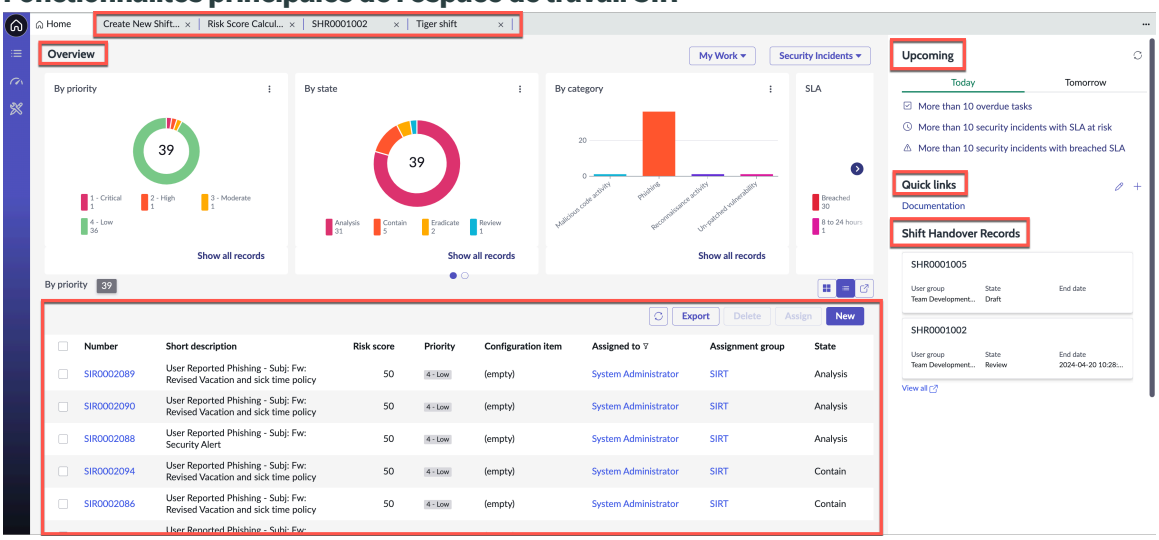
Pour en savoir plus sur les rôles, les tables, les propriétés et les Réponse aux incidents de sécurité travaux planifiés, consultez Composants installés avec Réponse aux incidents de sécurité

Fonctionnalités de l'espace de travail SIR

Le Espace de travail de la Réponse aux incidents de sécurité se compose des fonctionnalités clés suivantes.

- Section Vue d'ensemble
- Section À venir
- Section Liens rapides
- Section des enregistrements de transfert d'équipe
- Vue liste
- Interface multionglet prenant en charge l'ouverture de plusieurs incidents de sécurité

Fonctionnalités principales de l'espace de travail SIR



Espace de travail SIR Vue d'ensemble de l'interface

La Espace de travail SIR page Vue d'ensemble contient les détails Incidents de sécurité et Tâches de réponse qui se trouvent sous les analystes de sécurité et leur équipe.

Sous chaque filtre, différents widgets sont présents, regroupés par priorité, catégorie, état et SLA, qui se trouvent dans les files d'attente des analystes de sécurité et de l'équipe d'analystes de sécurité.

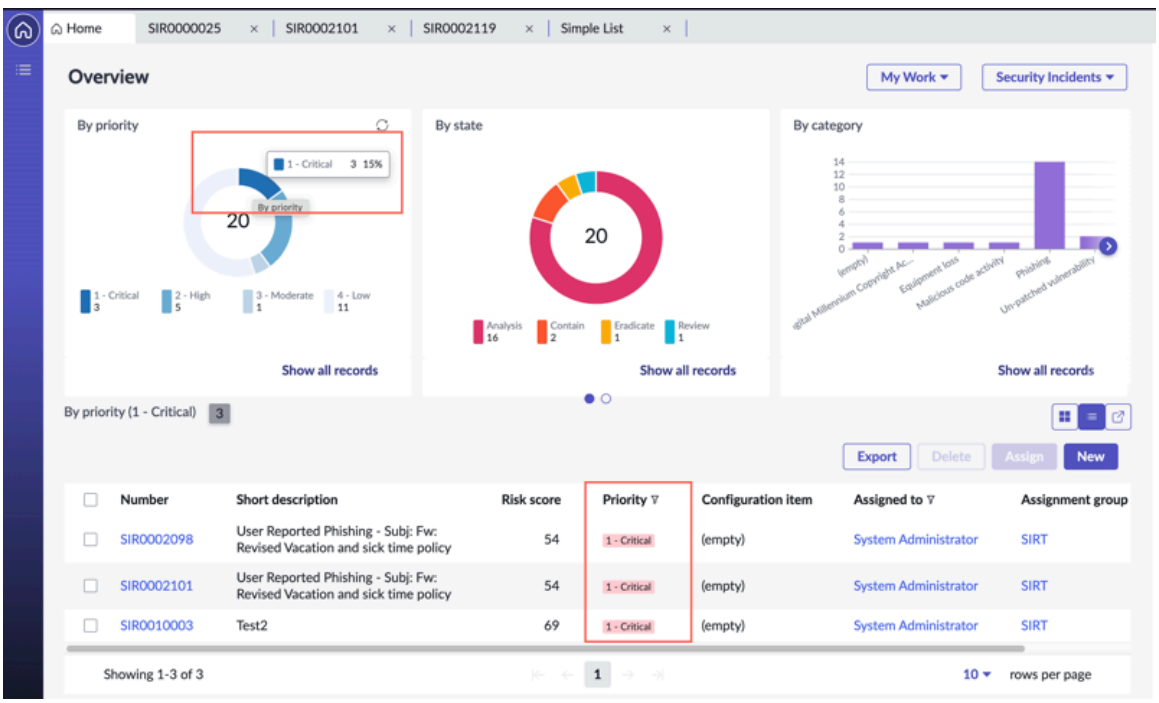
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque des filtres sont appliqués aux widgets, la moitié inférieure de la page de vue d'ensemble est remplie avec les incidents de sécurité ou les tâches de réponse correspondants présentés sous forme de cartes ou d'éléments de liste. L'analyste peut basculer entre la vue de carte ou la vue de liste comme il le souhaite.

Par exemple, dans le widget **Priorité** , si vous souhaitez sélectionner tous les incidents critiques ou les tâches de réponse, cliquez sur le segment **critique** (exemple de capture d'écran ci-dessous) du widget et les incidents ou la tâche de réponse qui sont critiques s'affichent dans la vue de liste ou de carte.

Section Vue d'ensemble

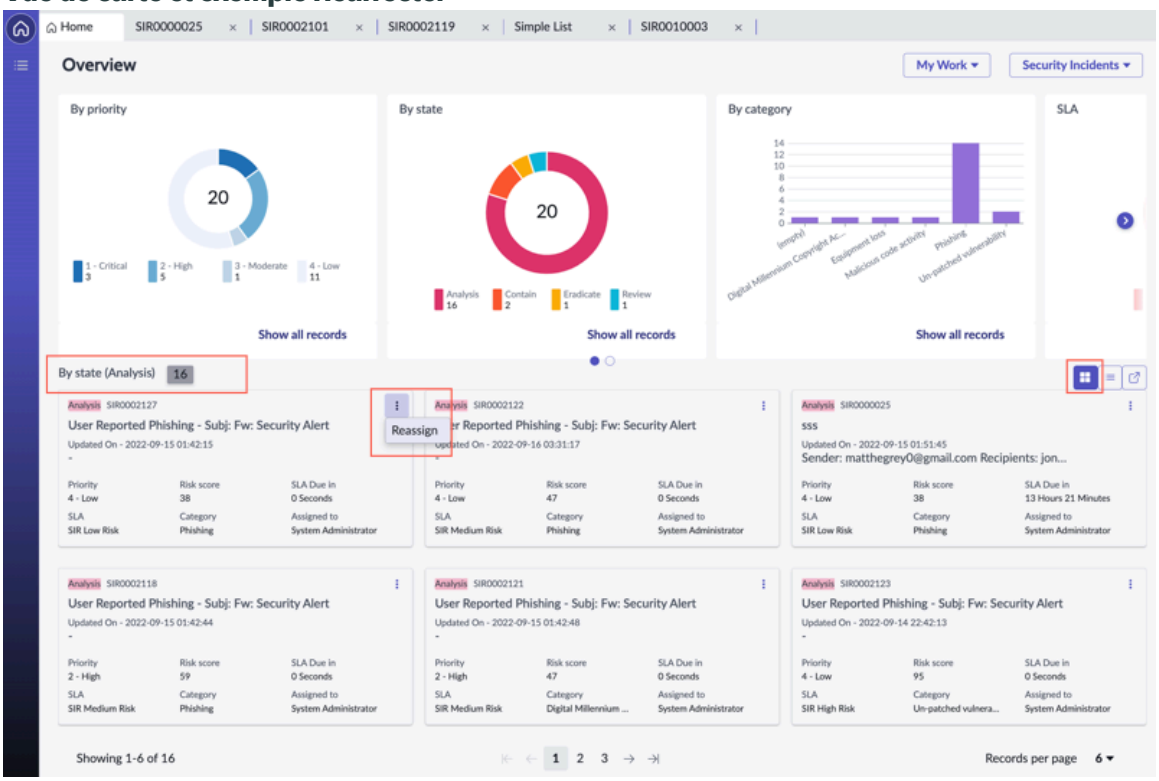


Vous pouvez affecter ou réaffecter les incidents de sécurité ou les tâches de réponse directement à partir de cette vue en cliquant sur l'icône en forme d'ellipse et en sélectionnant **Affecter** (option dans la vue de carte) ou directement le bouton **Affecter** (option dans la vue de liste) en conséquence pour affecter un incident.

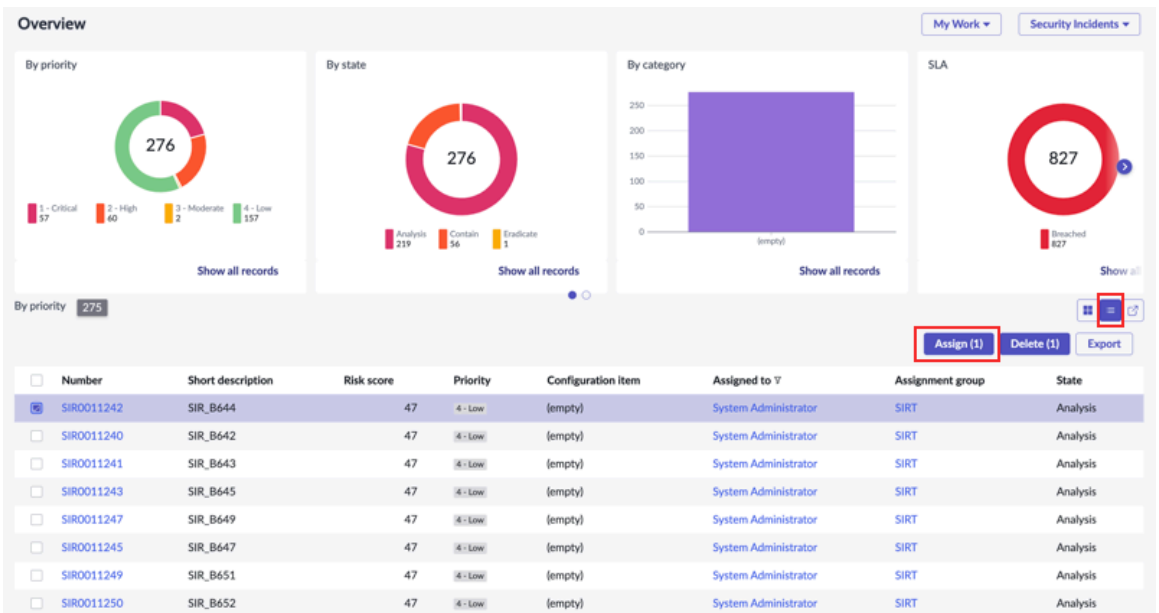
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue de carte et exemple Réaffecter



Affecter l'incident

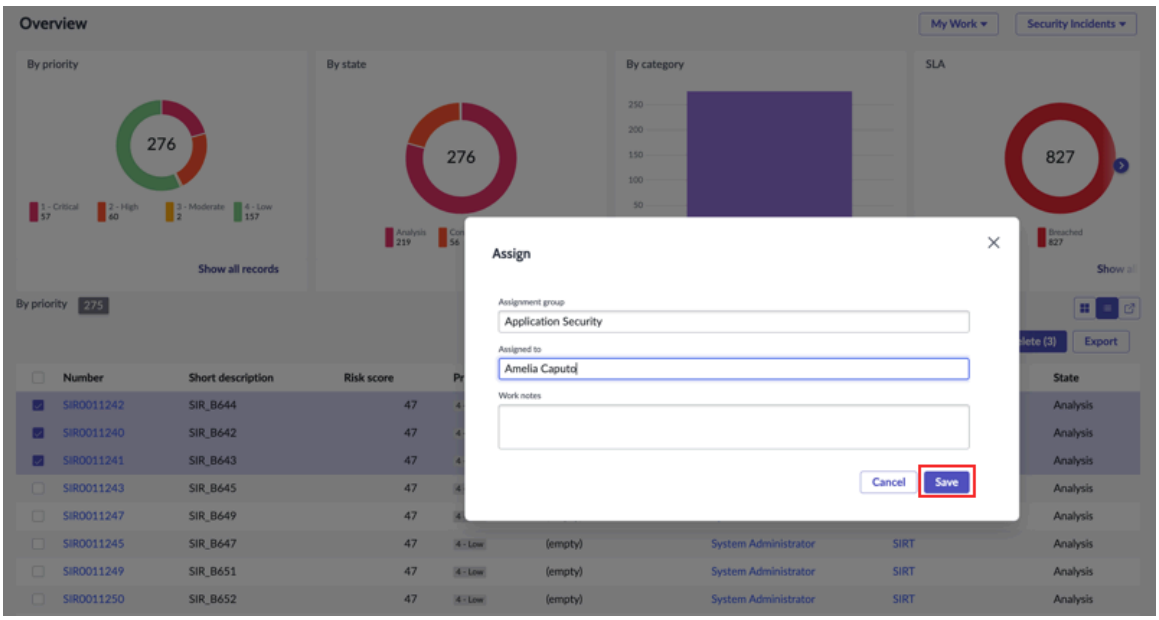


Voici un exemple de vue de liste. L'utilisateur peut également affecter des incidents à partir de la vue de liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affecter l'incident



Ajoutez ou modifiez les détails du délégataire tels que Groupe d'affectation et Affecté à, ajoutez des notes de travail, si nécessaire.

Remarque : Vous pouvez affecter un ou plusieurs incidents de sécurité ou tâches de réponse aux groupes d'affectation. Le numéro sélectionné s'affiche sur le bouton **Affecter** .

L'utilisateur peut supprimer des incidents de sécurité à partir de cette vue. Cliquez sur le bouton **Supprimer** pour supprimer l'incident de sécurité, l'enregistrement sera supprimé de la vue de liste.

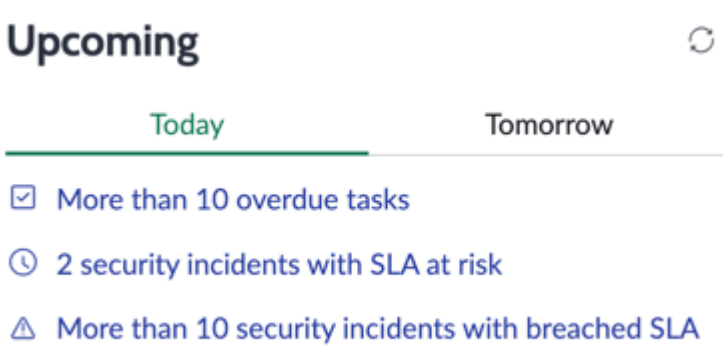
L'utilisateur peut également exporter le contenu de la liste. Cliquez sur le bouton **Exporter** pour exporter la liste au format souhaité.

Section À venir

Cette section affiche les tâches à venir telles que les incidents de sécurité et les tâches de réponse qui arrivent à échéance le jour même et le jour suivant.

La liste des incidents de sécurité et des tâches de réponse qui s'affiche est basée sur le champ de date d'échéance et la définition de SLA définis pour ces enregistrements.

Si cette section contient plusieurs tâches de réponse ou d'incident de sécurité, l'incident ou les enregistrements ouvrent tous ces enregistrements dans un nouvel onglet.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

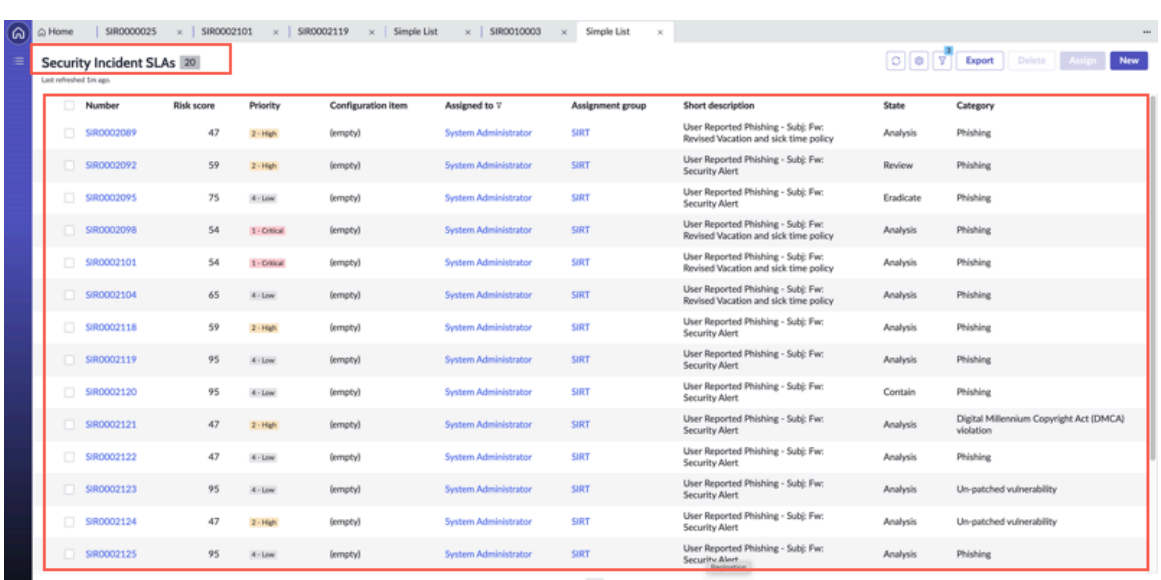
Afficher les tâches à venir

L'analyste de la sécurité peut afficher les tâches à venir liées aux incidents de sécurité et aux tâches de réponse qui sont dues, en retard ou qui ne respectent pas le SLA défini.

Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **À venir**.
2. Cliquez sur l'onglet **Aujourd'hui** pour afficher les tâches qui arrivent à échéance le même jour.
3. Sélectionnez l'onglet **Demain** pour afficher les tâches en retard au lendemain.
   La section À venir répertorie les incidents de sécurité ou les tâches de réponse qui sont en retard en fonction de la date d'échéance et qui n'ont pas respecté la définition de SLA.
4. Cliquez sur l'icône **Actualiser** pour actualiser la liste des sections à venir.
   Par exemple, si vous cliquez sur le lien **Plus de 10 incidents de sécurité avec SLA violé** , la liste des incidents SLA violés s'affiche dans un nouvel onglet dans l'espace de travail.



Remarque : Vous pouvez effectuer les opérations Nouveau, Affecter, Exporter et Supprimer à partir de n'importe quelle vue de liste.

Section Liens rapides

Les liens rapides fonctionnent comme des liens de signet. Vous pouvez ajouter des URL externes et y accéder rapidement à partir de l'espace de travail.

Utiliser des liens rapides

Ajoutez des liens rapides pour faciliter la consultation.

Avant de commencer
Rôle requis : sn_si.analyst

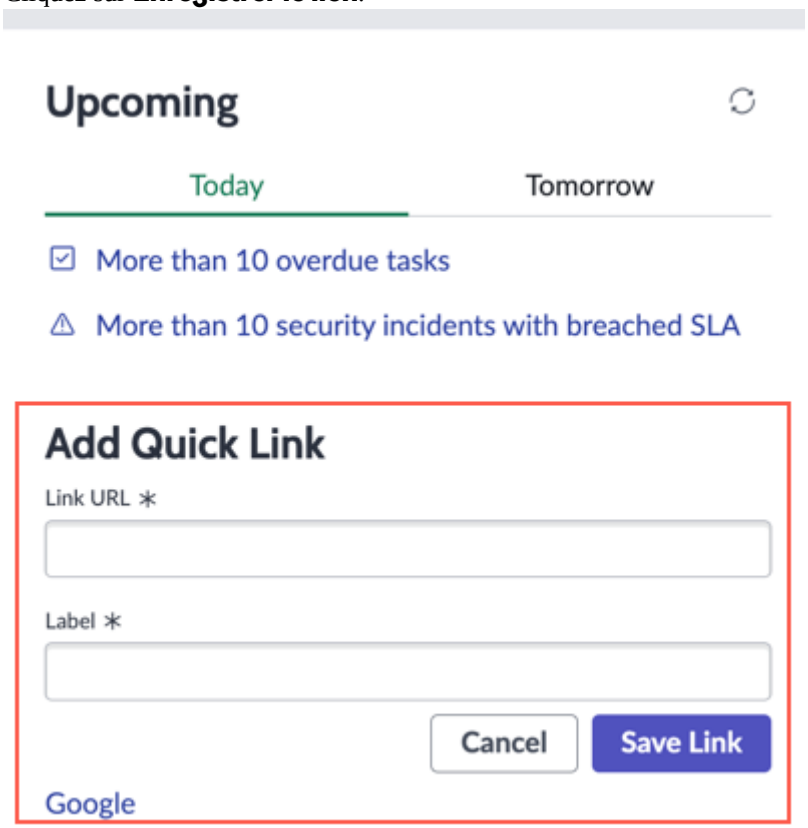
Pourquoi et quand exécuter cette tâche
Vous pouvez ajouter et modifier tous les liens rapides utiles et placer ces liens en signet pour faciliter la résolution des incidents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Liens rapides**.
2. Cliquez sur l'icône **Ajouter un lien rapide** pour ajouter les liens.
3. Entrez le lien vers l'URL et l'étiquette.
4. Cliquez sur **Enregistrer le lien**.



Le nouveau lien est ajouté sous la section des liens rapides.

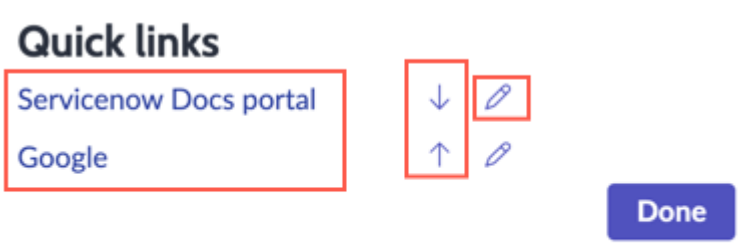
5. **Pour modifier ou supprimer les liens :**

   a. Cliquez sur **l'icône Modifier le lien** .

   b. Modifiez le lien ou le texte d'affichage souhaité qui est l'étiquette de l'URL.

   c. Cliquez sur **Enregistrer**.

   d. Cliquez sur **Terminé**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Utilisez les flèches vers le haut et vers le bas pour déplacer la position des liens.

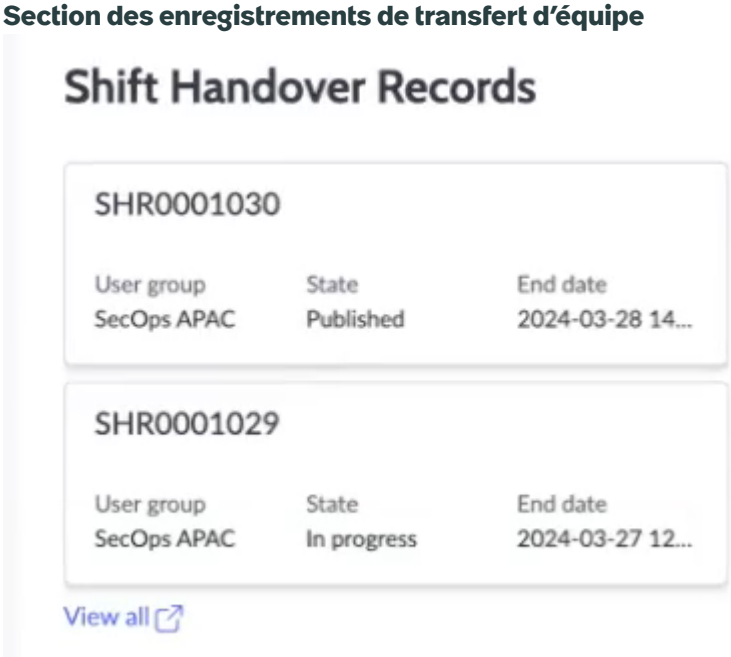
f. Cliquez sur **Supprimer** pour supprimer les liens lors de la modification qui ont été marqués d'un signet.

Section des enregistrements de transfert d'équipe

La section affiche la liste des enregistrements de transfert d'équipe dans l'espace de travail Réponse aux incidents de sécurité.

La section Enregistrements de transfert d'équipe de l'espace de travail Réponse aux incidents de sécurité affiche les deux derniers enregistrements de transfert d'équipe en fonction des champs Date de fin, État et Groupe d'utilisateurs définis pour ces enregistrements. Pour afficher tous les enregistrements de transfert d'équipe, sélectionnez **Afficher tout**.

Section des enregistrements de transfert d'équipe



Vue de liste dans Espace de travail SIR

La vue de liste comprend les incidents de sécurité, les tâches de réponse, les e-mails d'hameçonnage et les évaluations.

La vue de liste comporte des filtres pré-appliqués tels que Affecté à moi-même, Affecté à une équipe, Non affecté, Tous ouverts, Tous, etc.

À l'aide de ces catégories de liste et de ces listes filtrées, les analystes peuvent trouver rapidement les enregistrements d'incidents de sécurité et de tâches de réponse sur lesquels ils doivent travailler.

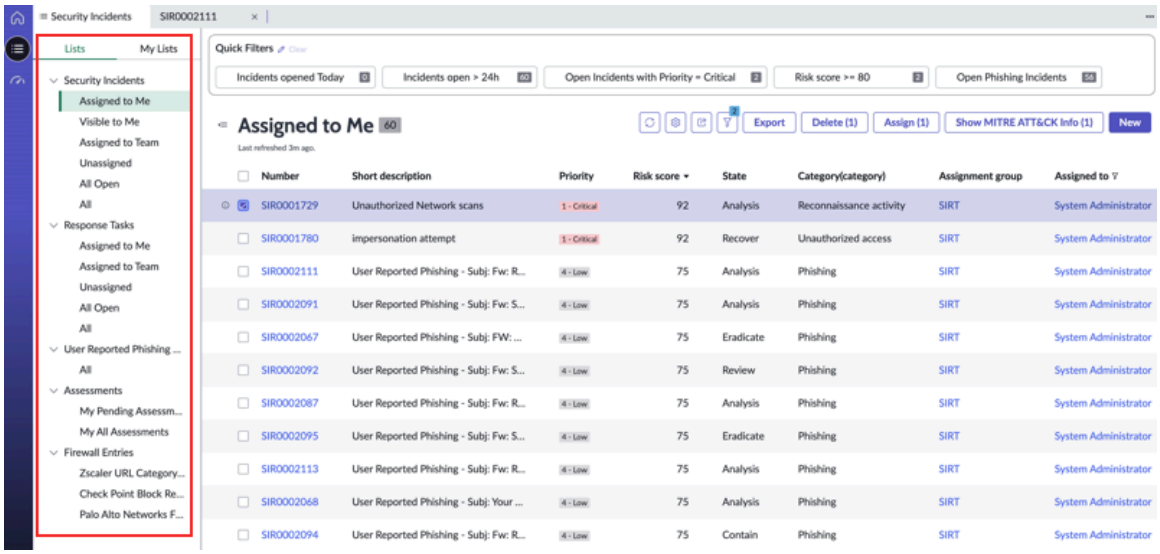
Pour accéder à la vue de liste, vous devez cliquer sur l'icône de liste (icône de). Lorsque vous cliquez sur un enregistrement dans une vue de liste, l'enregistrement s'ouvre dans un nouvel onglet.

Types de listes

Vous trouverez ci-dessous un exemple de vue des listes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le volet de liste contient les sections suivantes :

Listes

Élément de liste	Description	Option
Incidents de sécurité	Affichez la liste des incidents de sécurité et accédez à l'incident souhaité pour commencer à travailler dessus. Les listes suivantes sont disponibles : • **Visibles par moi** : incidents de sécurité visibles par l'utilisateur connecté. • **Affectés à moi** : incidents de sécurité qui sont affectés à l'analyste. • **Affectés à l'équipe** : incidents de sécurité affectés à toutes les équipes auxquelles appartiennent les analystes. • **Non affecté :** liste des incidents de sécurité non affectés. • **Tous ouverts** : liste de tous les incidents de sécurité ouverts. • **Tous** : liste de tous les incidents de sécurité.	• Dans la vue de liste, l'analyste peut configurer la liste des colonnes en cliquant sur l'icône d'engrenage disponible au-dessus des colonnes d'incident. • L'analyste peut sélectionner un ou plusieurs incidents de sécurité et affecter ces incidents aux autres utilisateurs. • L'analyste peut supprimer les incidents de sécurité. • L'analyste peut créer un nouvel incident de sécurité. • L'analyste peut appliquer les filtres rapides. Appliquez les filtres en cliquant sur l'option **Filtres rapides** au lieu d'utiliser l'option **Filtre** avancé. À l'aide des filtres rapides, vous pouvez filtrer rapidement la liste des incidents de sécurité qui nécessitent une attention immédiate. Pour plus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Option
		d'informations, consultez Utilisation de filtres rapides. • Les analystes peuvent actualiser la liste des incidents. • L'analyste peut exporter la vue de liste aux formats Excel, CSV, JSON et PDF.
Enregistrements de transfert d'équipe	Affichez la liste des enregistrements de transfert d'équipe. Les listes suivantes sont disponibles : • **Affecté à l'équipe** : enregistrements de transfert d'équipe qui sont affectés à toutes les équipes/groupes d'utilisateurs auxquels appartient l'analyste. • **Tous** : liste de tous les incidents de sécurité.	Le transfert d'équipe prend en charge les trois rôles suivants : • Administrateur : rôle du propriétaire du quart • Analyste de la sécurité : Rôle d'analyste d'équipe • Gestionnaire de sécurité : rôle de propriétaire du quart, mais n'a pas accès au groupe d'utilisateurs auquel l'enregistrement de transfert d'équipe est affecté. • Les utilisateurs disposant du rôle d'équipe/analyste qui font partie du groupe d'utilisateurs dans l'équipe active peuvent ajouter ou modifier du contenu dans les enregistrements de transfert d'équipe à l'état brouillon. • Les utilisateurs qui n'ont pas le rôle de propriétaire d'équipe/ analyste ou qui ne font pas partie du groupe d'utilisateurs de l'équipe active peuvent uniquement afficher le contenu des enregistrements de transfert d'équipe.
Tâches de réponse	Affichez la liste des tâches de réponse et accédez à la tâche de réponse souhaitée pour commencer à travailler dessus. La vue de liste contient :	• Dans la vue de liste, l'analyste peut configurer la liste des colonnes en cliquant sur l'icône d'engrenage disponible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Option
	• **Affecté à moi** : tâches de réponse affectées à l'analyste. • **Affecté à l'équipe** : les tâches de réponse qui sont affectées aux équipes des analystes appartiennent à. • **Non affecté :** liste des tâches de réponse non affectées. • **Tous ouverts** : liste de toutes les tâches de réponse ouvertes. • **Toutes** : liste de toutes les tâches de réponse.	au-dessus des colonnes d'incident. • L'analyste peut sélectionner une ou plusieurs tâches de réponse et affecter ces tâches à d'autres utilisateurs. • L'analyste peut créer une nouvelle tâche de réponse. • L'analyste peut appliquer les filtres rapides. Appliquez les filtres en cliquant sur l'option **Filtres rapides** au lieu d'utiliser l'option **Filtre** avancé. À l'aide des filtres rapides, vous pouvez filtrer rapidement la liste des tâches de réponse qui nécessitent une attention immédiate. • Les analystes peuvent actualiser la liste des tâches de réponse. • L'analyste peut exporter la vue de liste aux formats Excel, CSV, JSON et PDF. Pour plus d'informations, consultez Exporter des incidents de sécurité ou des tâches de réponse.
E-mails d'hameçonnage	Affichez la liste de tous les e-mails d'hameçonnage. La vue de liste est triée en fonction de la dernière mise à jour.	• Signaler un e-mail d'hameçonnage. Pour plus d'informations, consultez la section Signaler un e-mail d'hameçonnage Comment signaler un e-mail d'hameçonnage. • Supprimer les e-mails d'hameçonnage. • Exportez la vue de liste des e-mails d'hameçonnage aux formats Excel, CSV, JSON et PDF.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes (suite)

Élément de liste	Description	Option
Évaluations	Affichez la liste des évaluations nécessaires pour effectuer une revue post-incident. • **Mes évaluations en attente** : liste des évaluations en attente. • **Toutes mes évaluations** : liste de toutes les évaluations.	Faites des évaluations.

Personnaliser une liste

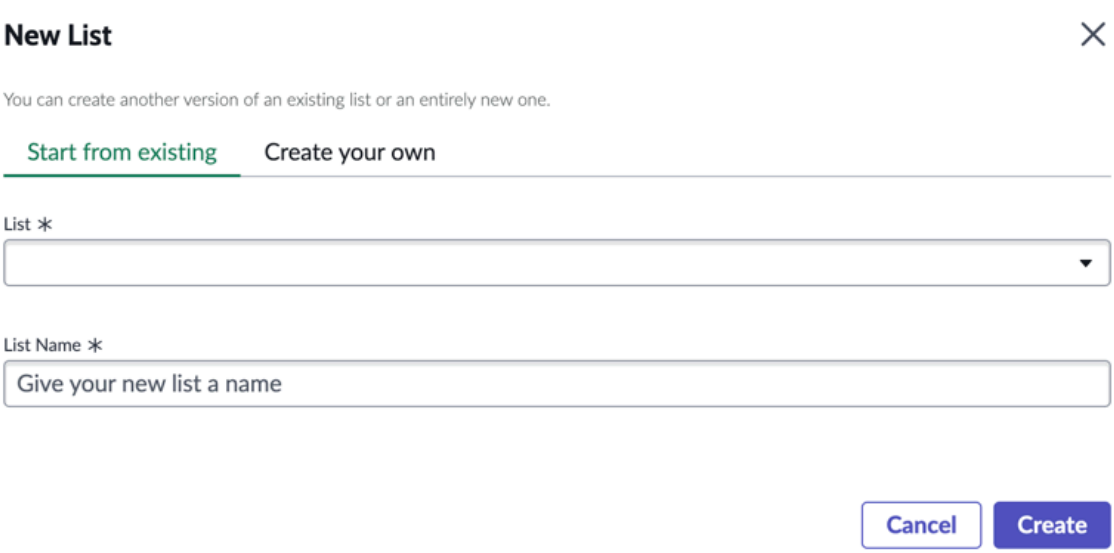
Les analystes ou les gestionnaires de sécurité peuvent personnaliser la vue de liste personnalisée des incidents de sécurité ou des tâches de réponse ou des e-mails d'hameçonnage en fonction de leurs préférences individuelles.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur **Vue de liste**.
3. Cliquer sur **Mes listes**.
4. Cliquez sur **Ajouter une nouvelle liste**, disponible en bas de la vue **Mes listes** .



Les analystes de sécurité peuvent créer une autre version d'une liste existante ou une liste personnalisée entièrement nouvelle.

5. **Pour créer à partir d'une vue de liste existante :**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Cliquez sur **Démarrer à partir du lien existant** .

b. Sélectionnez la **liste** dans la liste déroulante.

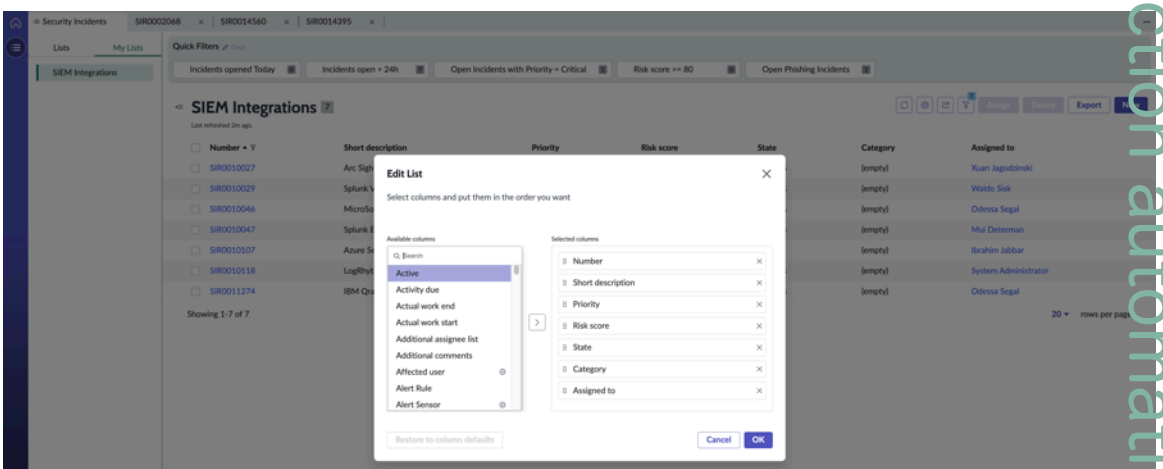
> **Remarque :** Quelle que soit la liste que vous sélectionnez dans la liste déroulante, le nom de la liste sera la copie de votre liste principale. Par exemple, si vous sélectionnez **Affecté à moi** dans la section Incidents de sécurité, le nom de la liste sera **Me l'affecter Copie** de la section Incidents de sécurité.

c. Sélectionnez les colonnes à personnaliser et ajoutez des filtres.
Créez un filtre en ajoutant des conditions qui contiennent un champ, un opérateur et une ou des valeurs.

d. Cliquez sur **Créer**.

> **Remarque :** Pour personnaliser votre propre vue de liste, vous pouvez ajouter des colonnes personnalisées, des filtres, définir des conditions, trier par ordre selon vos besoins.

e. Une fois qu'une vue de liste personnalisée est créée, cliquez sur l'icône en forme d'engrenage et personnalisez les colonnes de liste en choisissant l'option **Modifier les colonnes** pour modifier les colonnes et les classer dans l'ordre que vous préférez.



Vous pouvez également :

- **Renommez** la vue de liste personnalisée.
- **Supprimez** la vue de liste personnalisée.
- Enregistrez la vue de liste personnalisée comme vous le souhaitez à l'aide de l'option **Enregistrer sous** .
- **Réinitialiser la largeur** de la vue de liste.

> **Remarque :** Vous pouvez également effectuer directement ces opérations à l'aide des autres boutons Actions de liste tels que l'affectation, la suppression et l'exportation de la vue de liste qui sont fournis.

6. Pour créer votre propre liste :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

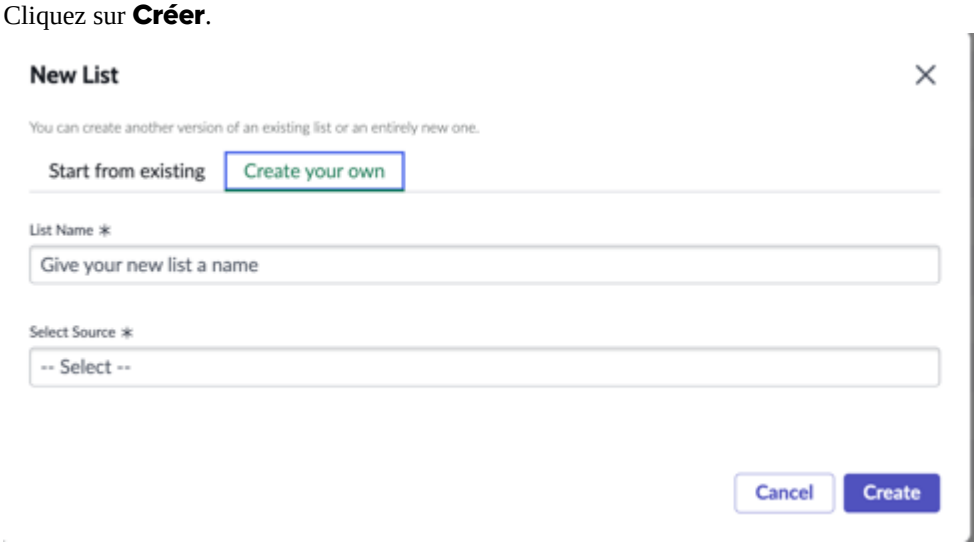
a. Cliquez sur **Créer votre propre** lien.

b. Fournissez un **nom de liste**.

c. Sélectionnez la **source** et les **colonnes**.

d. Ajoutez des filtres.
Créez un filtre en ajoutant des conditions et indiquez l'ordre dans lequel la liste doit être affichée.

e. Cliquez sur **Créer**.



Une nouvelle liste est créée telle que définie et personnalisée par vous sous la section **Mes listes** .

Remarque : vous pouvez **réorganiser** votre vue personnalisée en déplaçant leurs positions.

Affecter les incidents de sécurité

Affecter les incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

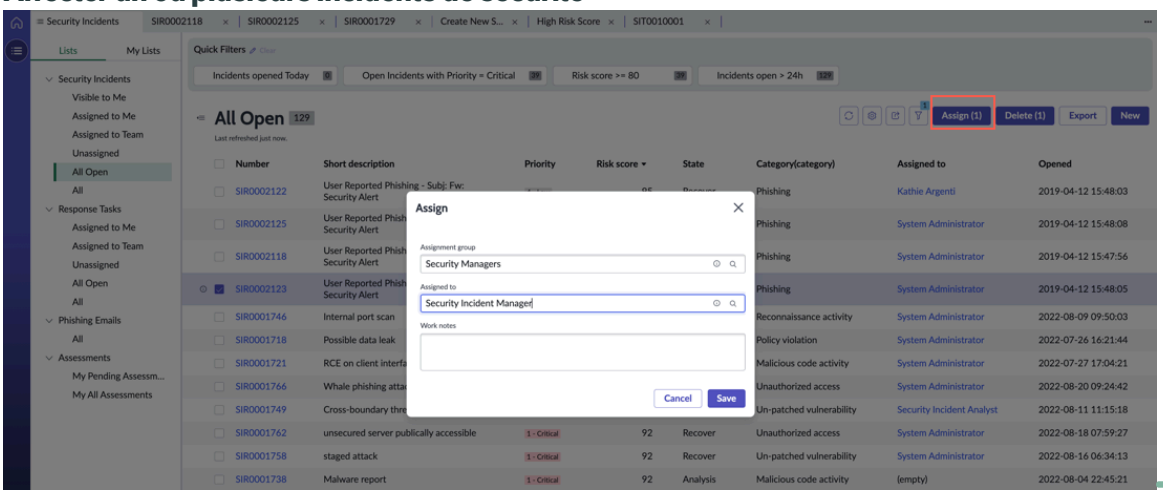
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône Liste (icône de).
3. Cliquez sur **Listes**.
4. Par exemple, accédez à **Incidents de sécurité** > **Tous les éléments ouverts**.
5. Sélectionnez un ou plusieurs incidents de sécurité.
6. Cliquez sur **Affecter**.
7. Renseignez les détails tels que Groupe d'affectation, Affecté à, et ajoutez des notes de travail si nécessaire.
L'incident sera ensuite affecté à l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Cliquez sur **Enregistrer**.

Affecter un ou plusieurs incidents de sécurité



Fermer plusieurs incidents de sécurité

Fermez plusieurs incidents de sécurité en même temps pour éviter d'avoir à fermer les incidents associés individuellement, tels que les incidents créés avec une cause première commune ou les incidents de faux positif .

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez l'icône List ( ).
3. **Sélectionnez Listes**.
4. Sélectionner **Incidents de sécurité** > **Tous les éléments ouverts**.
5. Sélectionnez un ou plusieurs incidents de sécurité à fermer, puis sélectionnez **Fermer**.
   La fenêtre Fermer en bloc les incidents de sécurité affiche des liens vers les listes d'accès aux incidents de sécurité sélectionnés pour être fermés.
   - Si au moins un incident de sécurité sélectionné a des activités en attente telles que des tâches actives, des playbooks, des SI enfants, des évaluations ou des flux actifs, les **incidents de sécurité avec des tâches actives, des playbooks, des SI enfants, des évaluations et des flux actifs** s'affichent.
   - Si au moins un incident de sécurité sélectionné pour la fermeture n'a aucune activité de fermeture en attente, les **incidents de sécurité prêts à être fermés** sont diffusés.
6. **Facultatif :** Examinez les incidents de sécurité avec des activités en attente.

   Remarque : Si vous ne fermez pas manuellement les activités en attente, elles sont fermées automatiquement si vous procédez à la fermeture en bloc.

   a. Fermez toutes les tâches actives, les playbooks, les SI enfants, les évaluations et les flux actifs.

   b. Sélectionner **Me ramener** pour revenir au bloc Fermer la fenêtre Incidents de sécurité.
7. Sélectionnez **Suivant**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Sélectionnez le **code de fermeture** applicable.
9. **Saisissez des notes de fermeture**.
10. Sélectionnez **Fermer en bloc**.
    L'activité de fermeture de l'incident s'exécute en arrière-plan.

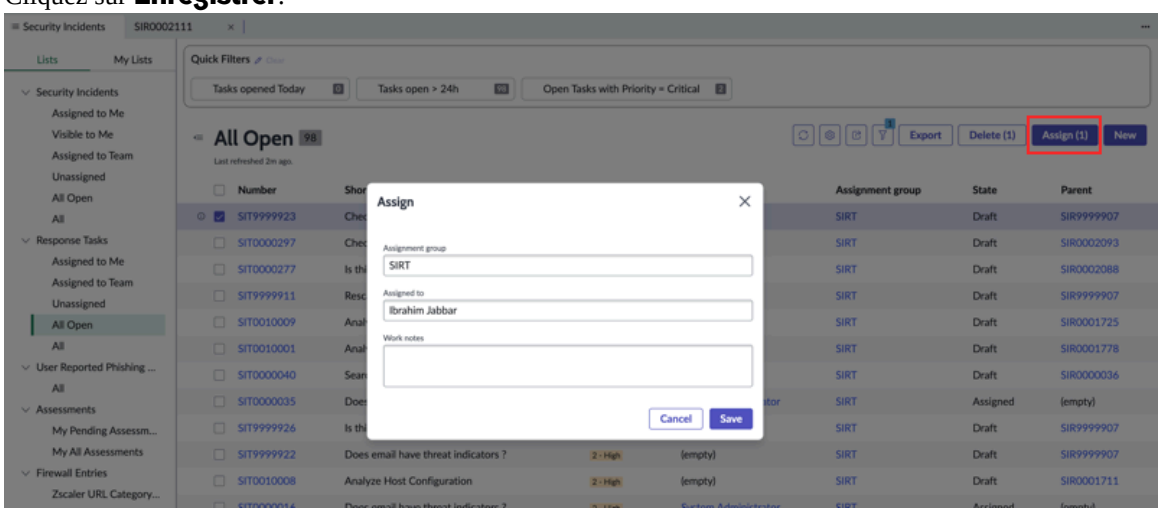
Affecter des tâches de réponse

Affectez des tâches de réponse pour un problème de sécurité.

Avant de commencer
Rôle requis : sn_si.basic

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône Liste (icône de).
3. Cliquez sur **Listes**.
   Par exemple, accédez à **Tâches de réponse** > **Tous les éléments ouverts**.
4. Sélectionnez une ou plusieurs tâches de réponse.
5. Cliquez sur **Affecter**.
6. Renseignez les détails tels que Groupe d'affectation, Affecté à, et ajoutez des notes de travail si nécessaire.
   L'incident sera ensuite affecté à l'utilisateur.
7. Cliquez sur **Enregistrer**.



Signaler un e-mail d'hameçonnage

Signalez des e-mails d'hameçonnage à partir de la vue de listes.

Avant de commencer
Rôle requis : sn_si.analyst

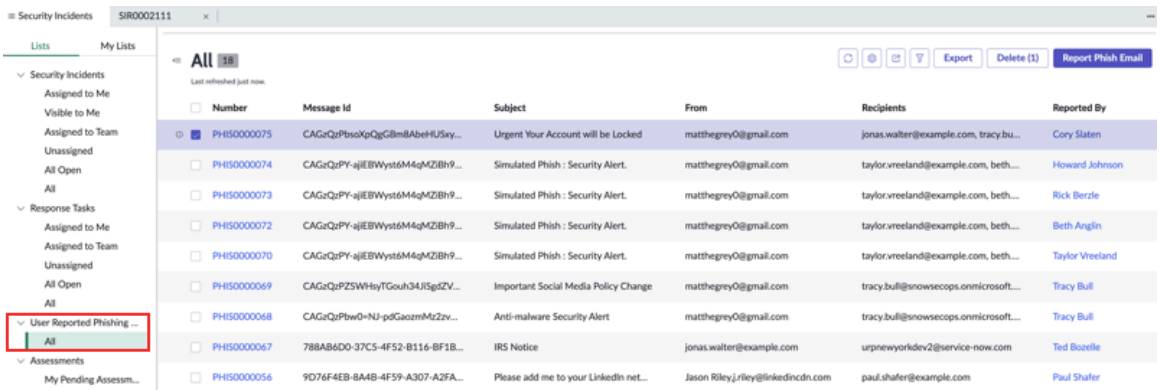
Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône Liste (icône de).
3. Accéder à **E-mails d'hameçonnage signalés par un utilisateur** > **Tous**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La liste des e-mails d’hameçonnage signalés par un utilisateur s’affiche.



4. Cliquez sur le bouton **Signaler un e-mail d’hameçonnage** .
   Signalez un e-mail d’hameçonnage en le téléchargeant.
5. Cliquez sur **Ajouter un fichier** pour ajouter des pièces jointes.
6. Cliquez sur **Charger**.

> **Remarque :** Signalez un e-mail d’hameçonnage en téléchargeant les pièces jointes. Vous ne pouvez charger qu’un seul e-mail d’hameçonnage à la fois et doit être au format .eml.

7. Cliquez sur **Envoyer**.
   L’e-mail d’hameçonnage pour enregistrer un incident de sécurité est créé.

Utilisation de filtres rapides

Les filtres rapides sont des filtres facilement accessibles disponibles sur les listes d’incidents de sécurité et de tâches de réponse.

Avant de commencer
Rôle requis : sn_si.admin

La Espace de travail SIR fournit une fonctionnalité de filtres rapides qui vous permet de filtrer facilement la liste des incidents de sécurité ou des tâches de réponse.

Vous pouvez utiliser des filtres rapides pour configurer de nouveaux filtres ou modifier les filtres existants qui apparaissent par rapport à ces listes. Le système de base fournit les filtres rapides suivants pour chaque incident de sécurité :

- **Incidents ouverts aujourd'hui**
- **Incidents ouverts > 24 heures**
- **Incidents ouverts avec priorité = critique**
- **> de risque = 80**
- **Incidents d’hameçonnage ouverts**

Le système de base fournit les filtres rapides suivants pour chaque tâche de réponse :

- **Tâches ouvertes > 24h**
- **Tâches ouvertes avec priorité = critique**

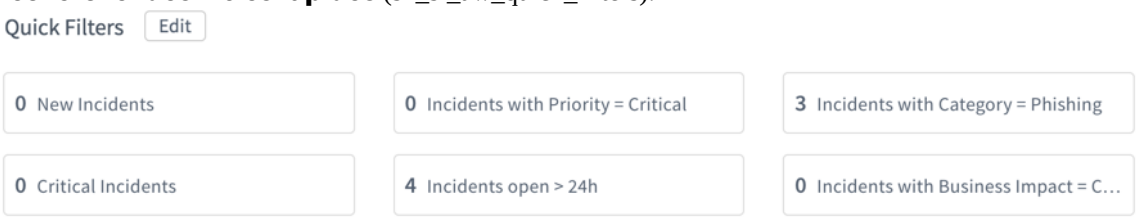
> **Remarque :** Un administrateur peut configurer la liste requise de filtres rapides en fonction des besoins de l’organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Définition du système** > **Tables**.
2. **Rechercher des filtres rapides** (sn_si_aw_quick_filters).

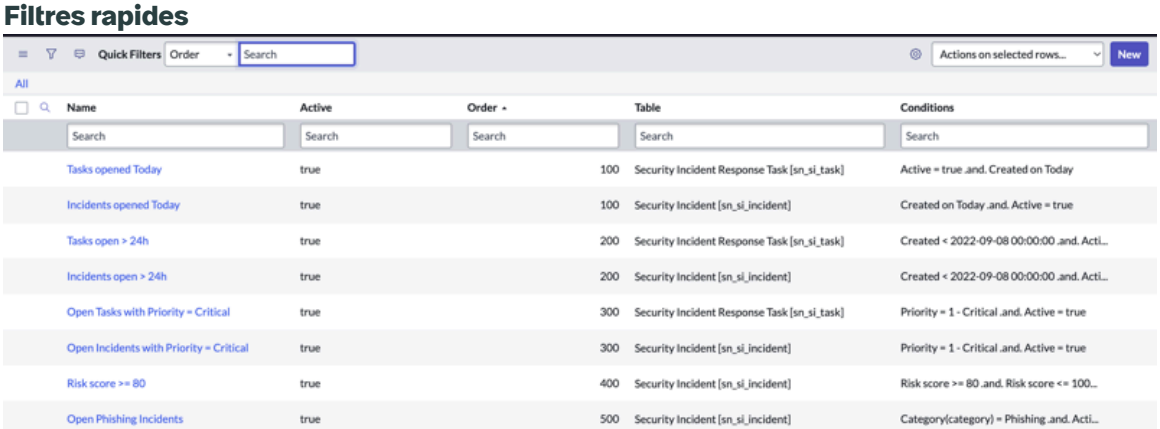


3. Accéder à **Liens connexes** > **Afficher la liste** section.
   La page de liste **Filtres rapides** s'affiche. Prêt à l'emploi, voici la liste des filtres rapides fournis avec l'application.

Nom	Table	Valeur
Tâches ouvertes aujourd'hui	Tâche d'incident de sécurité [sn_si_task]	Vrai
Incidents ouverts aujourd'hui	Incident de sécurité [sn_si_incident]	Vrai
Tâches ouvertes > 24h	Tâche Réponse aux incidents de sécurité [sn_si_task]	Vrai
Incidents ouverts > 24h	Incident de sécurité [sn_si_incident]	Vrai
Tâches ouvertes avec priorité = critique	Tâche Réponse aux incidents de sécurité [sn_si_incident]	Vrai
Incidents ouverts avec Priorité = Critique	Incident de sécurité [sn_si_incident]	Vrai
Score de risque >= 80	Incident de sécurité [sn_si_incident]	Vrai
Incidents d'hameçonnage ouverts	Incident de sécurité [sn_si_incident]	Vrai

Remarque : L'administrateur de sécurité peut poursuivre et configurer ces filtres rapides. Selon les besoins de l'entreprise, l'administrateur peut modifier la valeur existante sur faux et créer un nouveau filtre rapide.

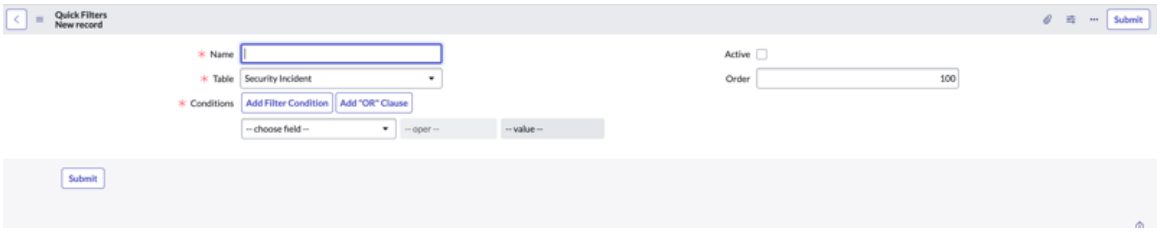
Filtres rapides



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

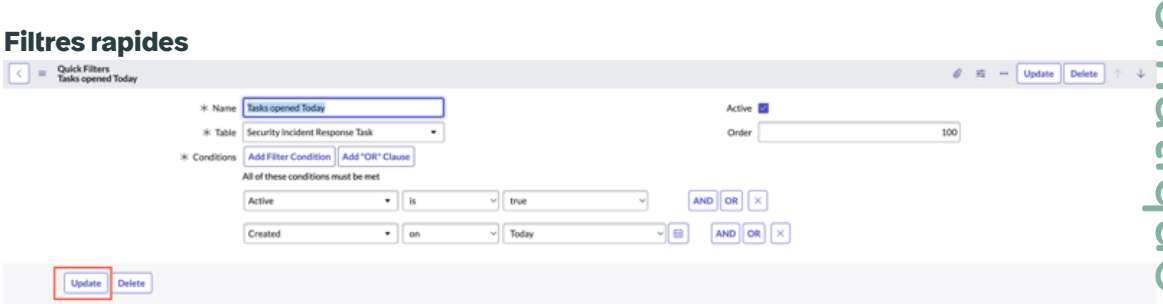
4. Cliquez sur **Nouveau** pour créer un nouveau filtre.
5. Donnez un nom au filtre, sélectionnez la table, spécifiez la condition de filtre.
6. Cliquez sur **Soumettre** pour revenir à la page de liste précédente.
   Vous verrez le filtre nouvellement ajouté répertorié sur la page.



Remarque :

- Le filtre rapide n'est applicable que si la case **Actif** est cochée.
- Dans l'espace de travail, tout utilisateur connecté peut personnaliser les filtres rapides actifs disponibles dans l'application. Les utilisateurs peuvent masquer ou afficher les filtres rapides nouvellement créés. Cette fonctionnalité est basée sur leurs préférences utilisateur.
- Si un utilisateur a modifié les préférences pour les filtres rapides et qu'un nouveau filtre rapide est créé après cela, si le filtre rapide est défini sur actif, il ne s'appliquera pas à la préférence de l'utilisateur. L'utilisateur doit modifier manuellement les préférences dans la vue personnalisée.

7. Sélectionnez un enregistrement de filtre existant pour modifier les filtres rapides existants.
8. Modifiez le nom et la condition de filtre.
9. Cliquez sur **Mettre à jour**.



Ajouter ou modifier des filtres rapides

Ajoutez ou modifiez des filtres rapides pour les incidents de sécurité ou les tâches de réponse dans la vue de liste.

Avant de commencer

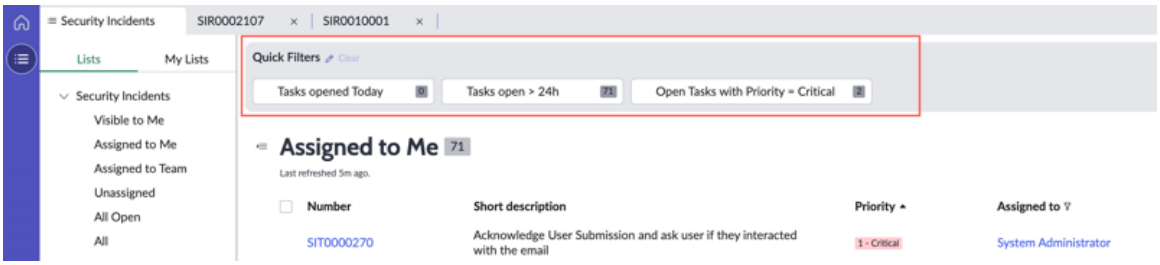
Rôle requis : sn_si.basic

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône Liste (icône de).
3. Par exemple, accédez à **Listes** > **Incidents de sécurité** > **Filtres rapides** section.

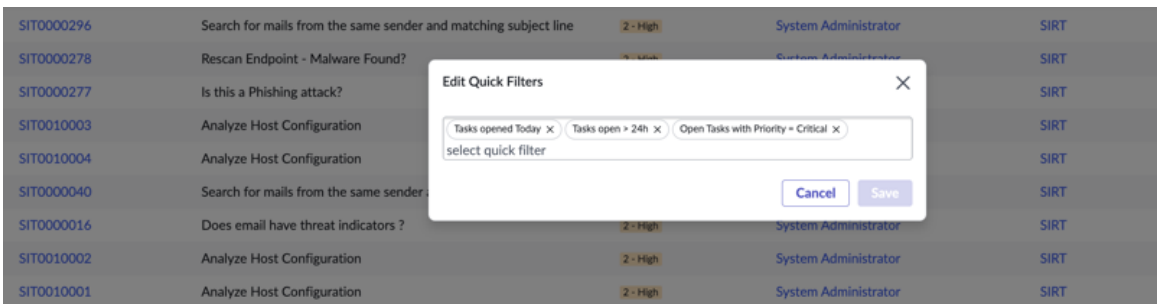
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur l'icône **Modifier** pour apporter les modifications.

> **Remarque :** La modification que vous apportez est conservée et, lorsque l'utilisateur revient sur cette page la prochaine fois, la préférence persistante s'affiche.



5. Cliquez sur **Enregistrer**.

Exporter des incidents de sécurité ou des tâches de réponse

Exportez les incidents de sécurité ou les tâches de réponse à partir de la vue de liste.

Avant de commencer

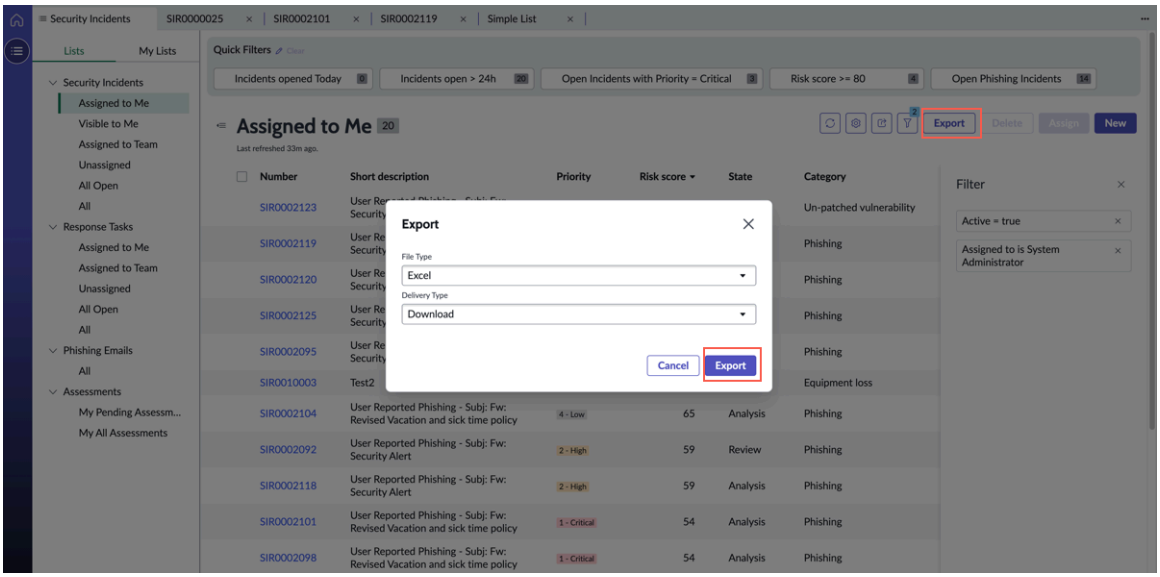
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur l'icône Liste .
3. Cliquez sur **Listes**.
4. Accéder à **Incidents de sécurité ou tâches de réponse** > **Tous les éléments ouverts**.
5. Affichez la liste et cliquez sur **Exporter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Sélectionnez le **type de fichier** et le **type de livraison**.
   Par exemple, **Excel** et **téléchargez** ou envoyez la liste **par e-mail** .
7. Cliquez sur **Exporter**.
   Le fichier sera téléchargé ou envoyé par e-mail selon l'option choisie.

Gérer les enregistrements de transfert d'équipe

Utilisez la vue de liste des enregistrements de transfert d'équipe pour créer, modifier, copier ou supprimer des enregistrements de transfert d'équipe. Chaque enregistrement de transfert d'équipe est associé à un modèle de rapport de transfert d'équipe.

Avant de commencer

Rôle requis :

- sn_escm_sh.shift_analyst : configuration minimale requise pour accéder aux enregistrements de transfert d'équipe.
- sn_escm_sh.shift_owner : créer, modifier et supprimer des enregistrements du journal de relais dans les groupes d'utilisateurs dont le propriétaire du quart fait partie. Ce rôle hérite du rôle sn_escm_sh.shift_analyst.
- sn_escm_sh.shift_analyst : afficher tous les enregistrements du journal de transfert d'équipe, mais ne peut contribuer qu'aux enregistrements de transfert d'équipe en cours affectés au groupe de l'analyste d'équipe.
- sn_si.analyst : hérite du rôle sn_escm_sh.shift_analyst.
- sn_si.admin : hérite du rôle sn_escm_sh.shift_admin.
- sn_escm_sh.shift_admin : hérite du rôle sn_escm_sh.shift_owner

Important : Pour savoir comment configurer le modèle de transfert d'équipe en tant qu'administrateur, reportez-vous à la section Configurer les modèles de transfert d'équipe.

Pourquoi et quand exécuter cette tâche

Le propriétaire de l'équipe et l'équipe ou le groupe d'utilisateurs respectif créent les enregistrements du journal de transfert d'équipe. Le propriétaire du quart doit choisir le modèle de transfert d'équipe et le groupe d'utilisateurs qui travaillera sur le rapport de transfert d'équipe. Une fois le rapport de transfert d'équipe terminé, il est partagé avec le prochain propriétaire d'équipe actif et l'équipe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Points clés du modèle de transfert d'équipe :

- Si un autre analyste de l'équipe active a déjà mis à jour le rapport avant vous et si des changements sont en cours de traitement, vous pouvez voir un message d'erreur indiquant que des mises à jour de contenu sont en attente. Vous devez patienter 30 secondes, puis sélectionner à nouveau **Passer à l'état « Revue ».** Vous pouvez voir le rapport consolidé sur le volet droit être mis à jour avec le contenu mis à jour d'autres analystes.
- Si le propriétaire du quart a modifié le contenu d'une section à l'état Révision, le même contenu est reflété pour l'analyste lorsque l'enregistrement revient à l'état En cours.
- Le propriétaire d'équipe doit être attentif lorsqu'il modifie le contenu à l'état Révision et qu'il effectue des actions telles que la fusion de deux lignes, la fusion de deux sections, la suppression d'une section, car cela affectera le rapport de transfert d'équipe des autres analystes.
- Après avoir publié le rapport de transfert d'équipe, le propriétaire de l'équipe peut modifier le contenu, mais il ne peut pas changer l'état de l'enregistrement.
- Lorsque quelqu'un modifie le contenu et pendant ce temps, si l'état de l'enregistrement passe de En cours à Révision, les changements de contenu non enregistrés sont alors ignorés.
- L'administrateur d'équipe aura un accès en écriture à tous les enregistrements du journal de transfert d'équipe, quel que soit le groupe d'utilisateurs.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez Liste des incidents de sécurité.
3. Sous l'onglet **Listes** , sélectionnez **Enregistrements de transfert d'équipe**.
4. Sélectionnez **Tous les enregistrements** pour afficher la liste de tous les enregistrements de transfert d'équipe.
5. Sélectionnez **Affecté à une équipe** pour afficher la liste des enregistrements de transfert d'équipe affectés à toutes les équipes/groupes d'utilisateurs auxquels appartiennent les analystes.
6. Pour créer un enregistrement de transfert d'équipe, sélectionnez **Nouveau**.
7. Renseignez les champs du formulaire.

Enregistrements de transfert d'équipe

Champ	Description
Numéro	Numéro unique automatiquement généré pour un enregistrement de transfert d'équipe.
Modèle	Le modèle de transfert d'équipe à utiliser. Par exemple, Exemple de modèle d'équipe.
Description	Description de l'enregistrement du transfert d'équipe.
Groupe d'utilisateurs	Le groupe/l'équipe d'utilisateurs auxquels l'enregistrement de transfert d'équipe doit être affecté. Par exemple, Réviseurs de code de Développement de l'équipe.

Traduction automatique

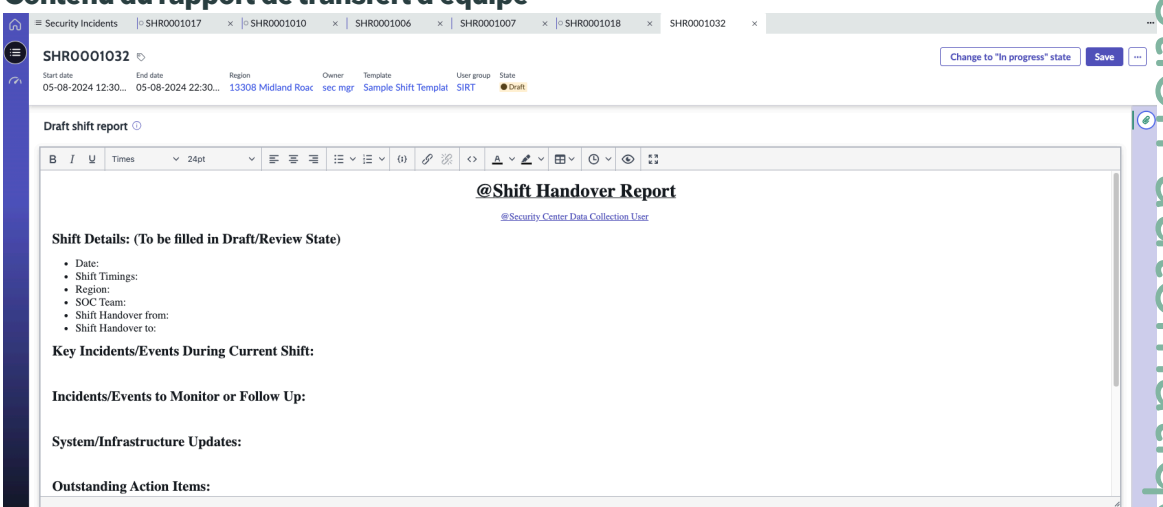
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
État	État actuel de l’enregistrement de transfert d’équipe. Par défaut, l’état initial est Brouillon **Remarque :** L’état ne peut pas être modifié pendant la création d’un enregistrement.
Nom de l'équipe	Nom de l’équipe contenant les détails de début et de fin de l’équipe. Par exemple, US Day Shift.

8. Sélectionnez **Créer**.
   Un nouvel enregistrement de transfert d’équipe est créé en fonction du modèle que vous avez sélectionné et ajouté à la vue de liste.
9. Ouvrez le nouvel enregistrement de transfert d’équipe pour mettre à jour l’état et les détails des incidents de sécurité dans le rapport de transfert d’équipe.
   Par défaut, l’enregistrement de transfert d’équipe est à l’état **Brouillon** .

   Remarque : Seul le propriétaire du quart peut modifier le contenu.

   Contenu du rapport de transfert d’équipe

10. Dans l’éditeur de brouillon de rapport d’équipe, utilisez les sections du modèle de rapport de transfert d’équipe pour mettre à jour les détails des incidents de sécurité et des utilisateurs.

    Vous pouvez mettre en forme votre rapport avec toutes les options de l’éditeur, telles que les polices, les couleurs, les puces, les liens et les pièces jointes.

    Remarque : Le chef d’équipe et l’analyste d’équipe peuvent tous deux modifier le contenu.

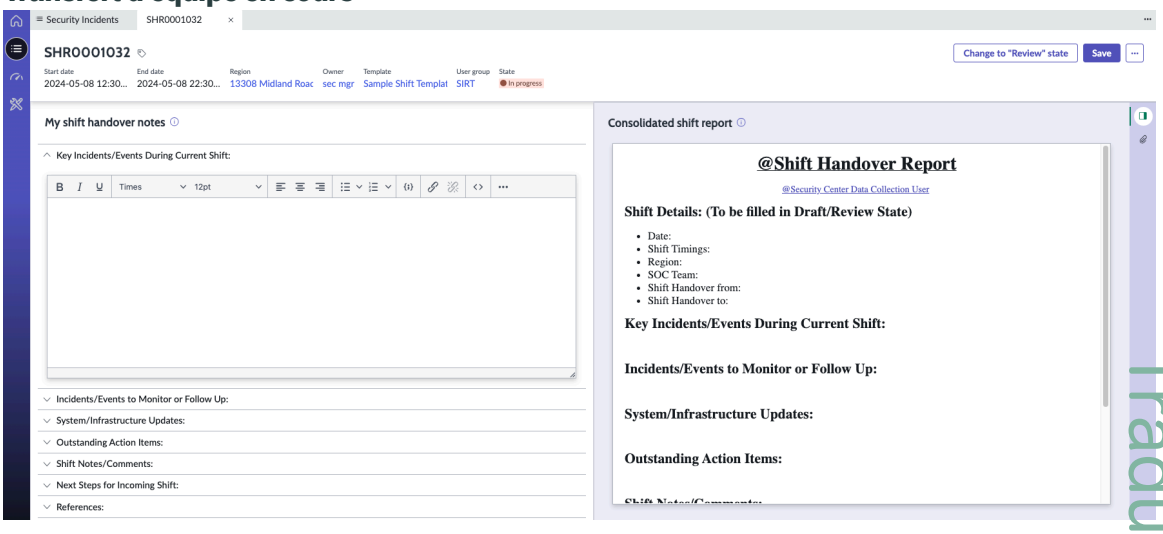
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Après avoir apporté les modifications requises au rapport de transfert d'équipe, sélectionnez **Enregistrer**.

b. Sélectionnez l'action **Changer l'état « En cours »** pour déplacer l'enregistrement du transfert d'équipe vers l'état En cours.

Transfert d'équipe en cours

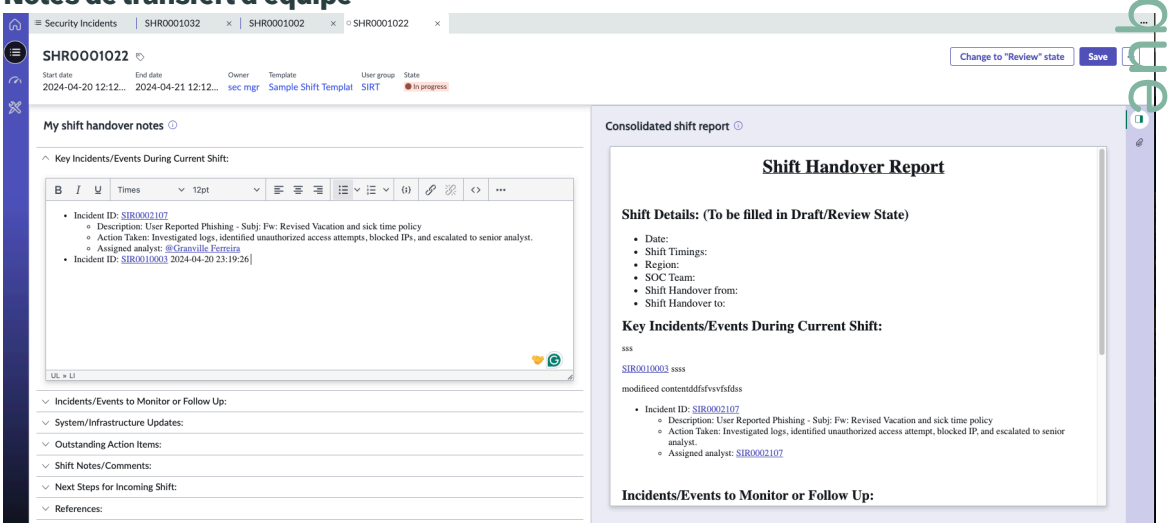


11. Dans l'éditeur de notes de transfert d'équipe, mettez à jour les détails requis pour toutes les sections telles que l'incident de sécurité et les détails de l'utilisateur.

Remarque : Le chef d'équipe et l'analyste d'équipe peuvent tous deux modifier le contenu.

a. Pour mentionner un enregistrement particulier dans l'éditeur, utilisez **/** et choisissez **Sélectionner un enregistrement**, puis sélectionnez un enregistrement dans la liste des tables qui s'affiche.
Par exemple, si vous sélectionnez **un enregistrement d'incidents de sécurité** , une liste d'incidents de sécurité apparaît. Sélectionnez un incident de sécurité (**SIR0010025**) dans la liste et mettez à jour les détails de transfert d'équipe requis. Vous pouvez également mentionner les champs associés à l'incident de sécurité comme description courte, regarder list en utilisant **/** après le numéro d'incident de sécurité.

Notes de transfert d'équipe



b. Pour mentionner un utilisateur particulier dans l'éditeur, utilisez **/** et choisissez **Sélectionner un utilisateur**, puis sélectionnez un utilisateur dans la liste qui s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

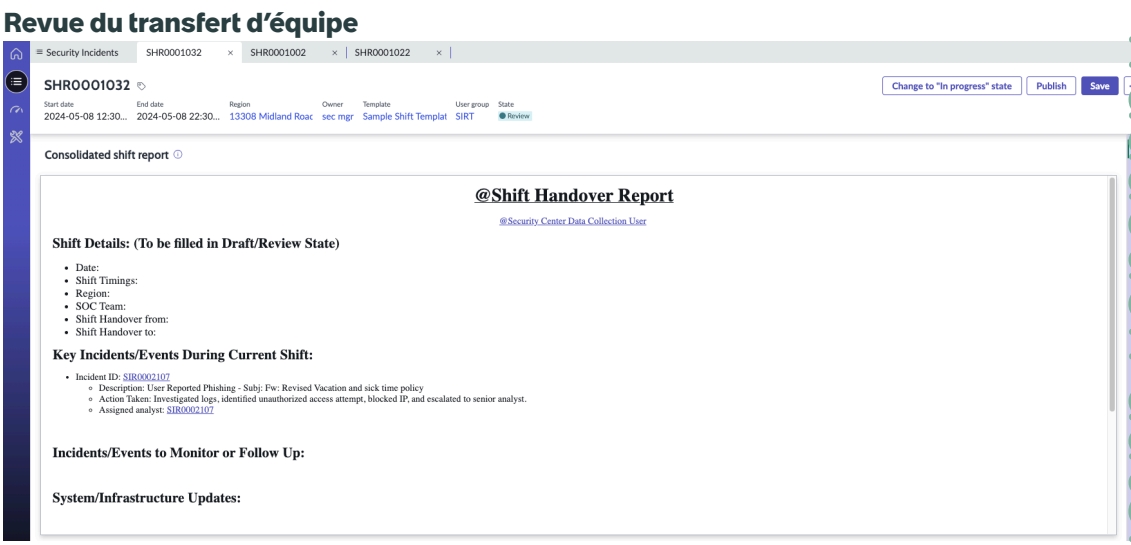
c. Pour mentionner le nombre d'enregistrements dans l'éditeur, utilisez **/** et choisissez **Nombre de mentions**, puis sélectionnez l'enregistrement dans la liste qui s'affiche.

d. Vous pouvez mettre en forme votre rapport avec toutes les options de l'éditeur, telles que les polices, les couleurs, les puces, les liens et les pièces jointes.

e. Après avoir apporté les modifications requises aux notes de transfert d'équipe, sélectionnez **Enregistrer**.

f. Sélectionnez l'action **Changer en état « Revue »** pour déplacer l'enregistrement de transfert d'équipe en état Révision.

Remarque : Si un autre analyste de l'équipe active a déjà mis à jour le rapport avant vous et si des changements sont en cours de traitement, un message d'erreur peut s'afficher. Vous devez patienter quelques secondes, puis sélectionner à nouveau **Passer à l'état « Revue ».**



12. Dans le rapport d'équipe consolidé, examinez le rapport de transfert d'équipe et apportez les modifications nécessaires.

Remarque : Seul le propriétaire du quart peut modifier le contenu.

a. Après avoir apporté les modifications requises aux notes de transfert d'équipe, sélectionnez **Enregistrer**.

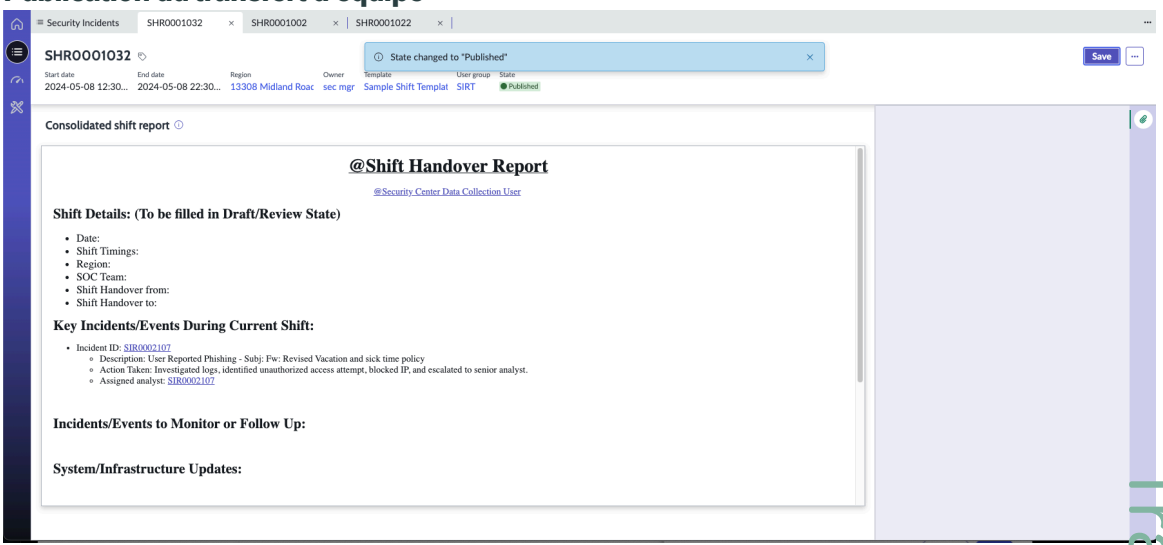
b. Si le rapport de transfert d'équipe nécessite d'autres mises à jour de la part des analystes, vous pouvez sélectionner **Passer à l'état « En cours ».**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Sélectionnez **l'action Publier** pour publier le rapport de transfert d'équipe.

Publication du transfert d'équipe



13. Sélectionnez **Enregistrer** pour enregistrer le rapport de transfert d'équipe.
Une fois que vous avez enregistré, vous pouvez afficher un aperçu du rapport de transfert d'équipe avec vos dernières mises à jour dans le volet Aperçu.

Remarque : Bien que vous puissiez prévisualiser immédiatement les mises à jour que vous avez apportées au rapport de transfert d'équipe, les autres analystes peuvent prendre quelques secondes pour voir les changements.

14. En tant que propriétaire d'équipe, vous pouvez également effectuer les actions suivantes dans la vue de liste Transfert d'équipe.

a. Pour modifier un enregistrement de transfert d'équipe existant, sélectionnez l'enregistrement et sélectionnez l'action **Modifier** .
Vous pouvez modifier uniquement l'heure de début, l'heure de fin, la description et la région.

b. Pour créer une copie d'un enregistrement de transfert d'équipe, sélectionnez l'enregistrement et sélectionnez **Créer une action de copie** .

c. Pour supprimer un enregistrement de transfert d'équipe existant, sélectionnez l'enregistrement et sélectionnez l'action **Supprimer** .

Configurer Espace de travail SIR

Cette section décrit les configurations nécessaires pour utiliser le Espace de travail de la Réponse aux incidents de sécurité.

Configurer la vue des enregistrements SIR

Cette section décrit comment les listes connexes sont regroupées et présentées dans l'onglet Enregistrements connexes SIR pour faciliter la navigation.

Les utilisateurs de l'espace de travail peuvent également effectuer une recherche par nom dans la liste connexe. Pour plus d'informations sur la configuration des listes connexes, reportez-vous à la section Espace de travail SIR Enregistrements connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'examen du temps de conception SI

Utilisez cette section pour configurer la page d'examen du temps de conception des incidents de sécurité afin d'ajouter plusieurs points d'entrée et ses enregistrements associés dans la Espace de travail de la Réponse aux incidents de sécurité.

Rôle requis : sn_si.admin.

La section suivante détaille les étapes de configuration de la page d'enquête sur le .Espace de travail de la Réponse aux incidents de sécurité

- Création d'une vue pour les tables d'informations associées
- Ajout d'une liste de points d'entrée
- Vue de mappage des informations associées à la liste de points d'entrée
- Configurer chaque liste associée à partir de la vue pour gérer le rendu des données au moment de l'exécution

Information associée

Explorer le canevas d'examen

Création d'une vue pour les tables d'informations associées

L'écran d'examen exploite les vues de listes connexes créées sur l'incident de sécurité pour configurer les listes associées.

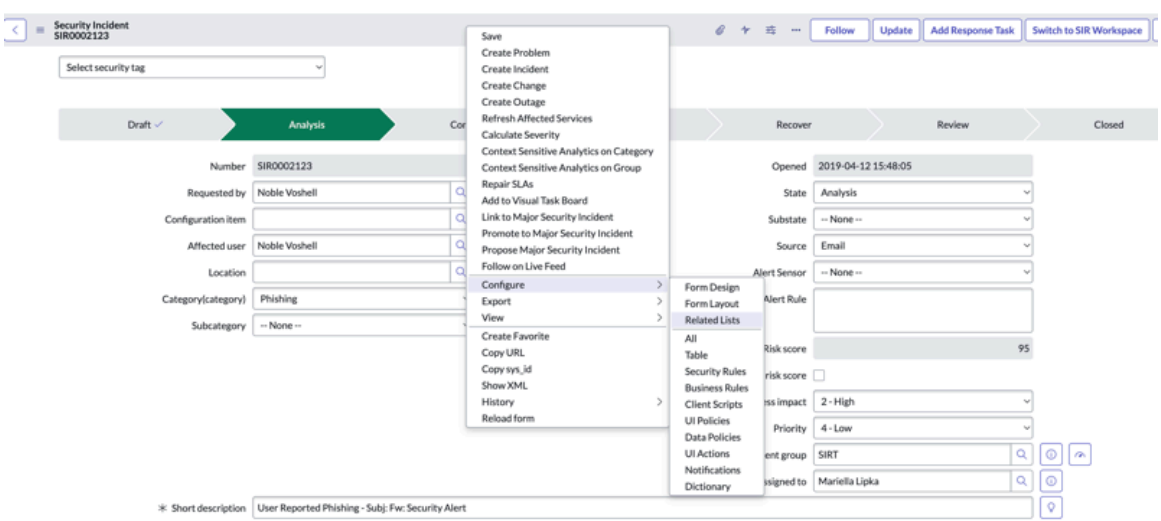
Avant de commencer

Rôle requis : sn_si.admin

Voici la procédure à suivre pour créer une vue et y ajouter des listes connexes.

Procédure

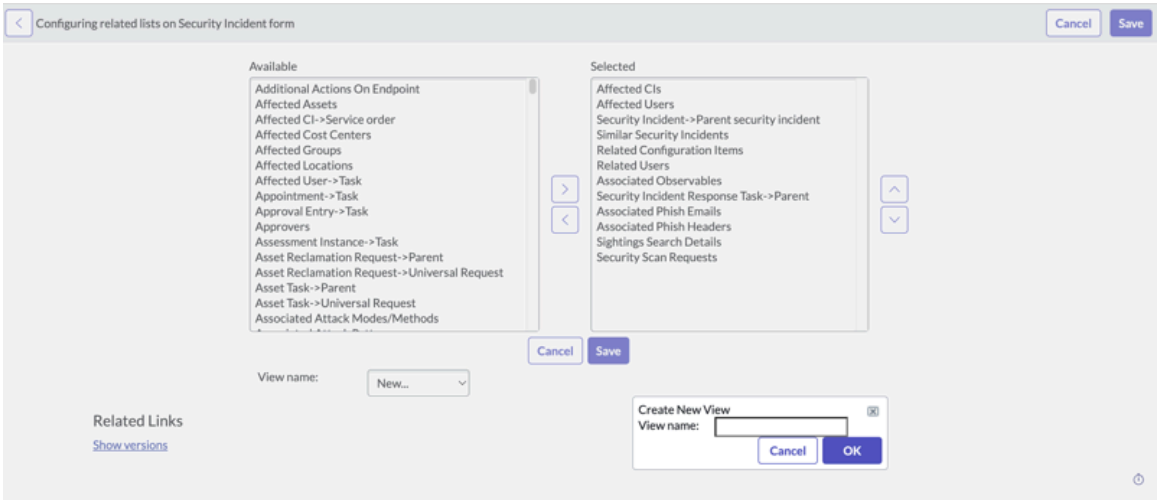
1. Accédez à la liste **des incidents de sécurité** .
2. Ouvrez n'importe quel incident de sécurité dans l'interface utilisateur classique.
3. Dans le menu contextuel du formulaire, accédez à **Configurer** > **Listes connexes**.
   La fenêtre de la zone de sélection s'affiche.



4. Accédez à la liste déroulante **Nom de la vue** et cliquez sur **Nouveau** pour créer une nouvelle vue.
   Vous devez ajouter un nom à la vue.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Ajoutez les listes connexes souhaitées au compartiment droit sous la vue nouvellement créée et enregistrez la vue.
   Cette vue sera utilisée pour afficher les informations associées dans l'onglet Examen.

Ajout d'une liste de points d'entrée

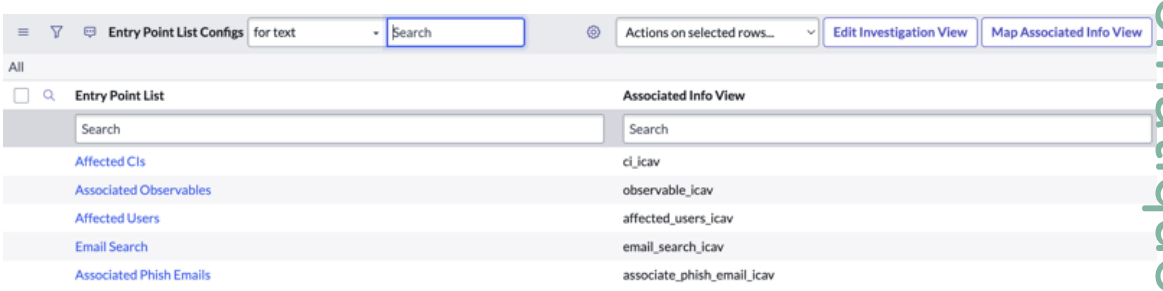
Configurez la nouvelle liste de points d'entrée pour l'ajouter à la page d'examen.

Avant de commencer

Rôle requis : admin

Procédure

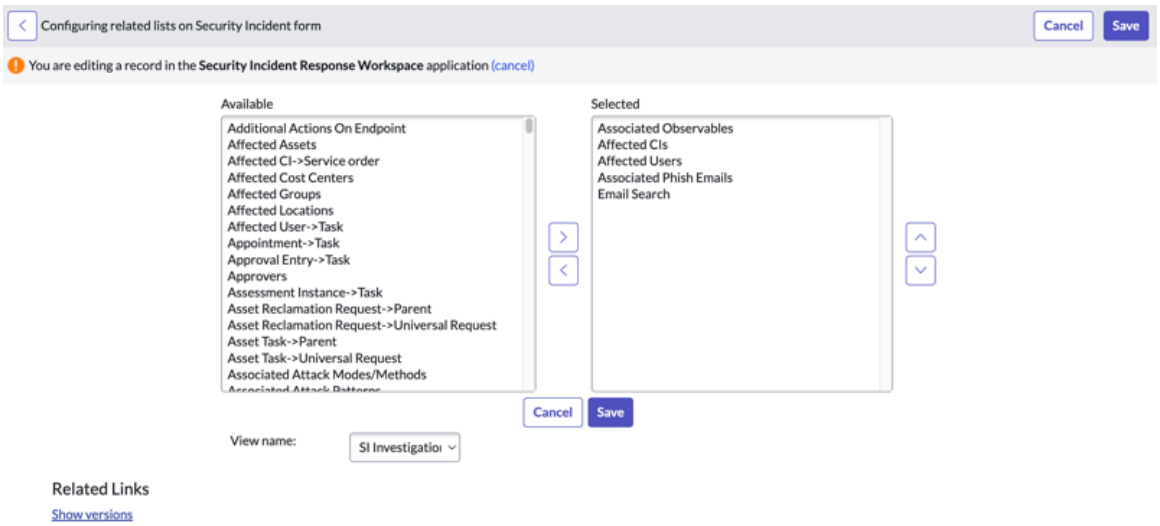
1. Accédez à la **sn_si_aw_entry_point_config.liste**.
   La page **Configurations des listes de points d'entrée** s'affiche.



2. Cliquez sur le bouton **Modifier la vue d'enquête** pour ajouter une liste de points d'entrée à l'écran d'enquête.
   Le **formulaire Configuration des listes connexes sur le formulaire Incident de sécurité** s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Ajoutez ou supprimez la liste de points d'entrée de la vue de la zone de liste double.
4. Cliquez sur **Enregistrer**.

> **Remarque :** La vue correspondant à l'écran Examen contenant les listes de points d'entrée est appelée **Vue Examen SI** et elle est sélectionnée par défaut lorsque vous accédez à la page **Modifier la vue d'examen** .
>
> L'ordre dans lequel les listes de points d'entrée sont affichées sur le canevas d'examen est déterminé par l'ordre dans la vue sélectionnée de la zone de sélection.

Vue de mappage des informations associées à la liste de points d'entrée

Mappez la vue d'informations associée à la liste de points d'entrée nouvellement ajoutée à l'aide de l'action Mapper la vue d'informations associée.

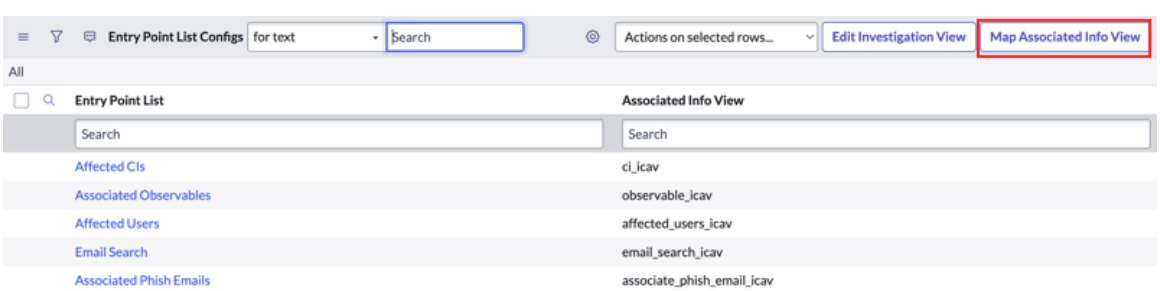
Avant de commencer

> **Remarque :** Cette étape est nécessaire pour que la liste des points d'entrée soit visible sur la page Examen. Même si vous ne souhaitez pas que des listes d'informations associées s'affichent sous un point d'entrée, vous devez toujours créer une vue factice et la mapper.

Rôle requis : admin

Procédure

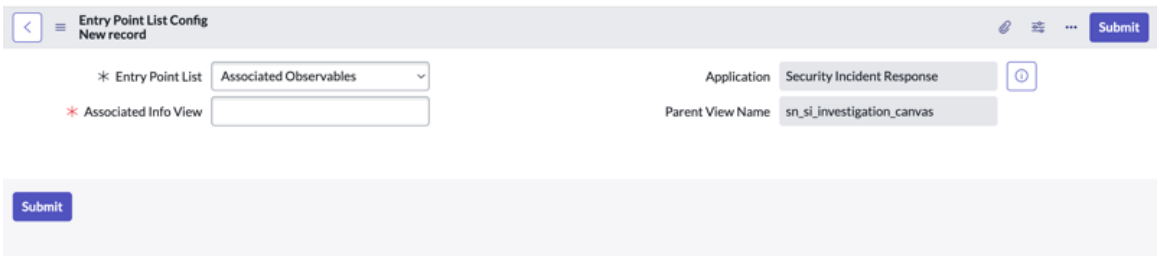
1. Cliquez sur le bouton **Vue des informations associées** à la carte sur la page **Configurations des points d'entrée** .



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Sélectionnez la liste de points d'entrée nouvellement ajoutée dans la liste déroulante **Liste de points d'entrée** .
3. Entrez le nom de la vue contenant les listes connexes d'informations associées dans le champ **Vue d'informations associée** .
   Pour en savoir plus sur la création d'une vue pour les listes connexes d'informations associées, reportez-vous à la section Création d'une vue pour les tables d'informations associées.



4. **Enregistrez** le formulaire.
5. En outre, si nécessaire, vous pouvez ajouter ou supprimer d'autres listes associées à l'aide de la **vue Modifier les informations associées**.
   Vous pouvez également configurer la mise en page de la liste de points d'entrée à l'aide de l'action **Modifier la mise en page de la liste de points d'entrée** . Ajoutez ou supprimez des colonnes de la zone de sélection comme vous le souhaitez, puis enregistrez le formulaire.

Configurer chaque liste associée à partir de la vue pour gérer le rendu des données au moment de l'exécution

Configurez chaque liste associée à partir de la vue pour gérer le rendu des données d'exécution.

Avant de commencer

Remarque : Cette étape est obligatoire pour chaque liste associée configurée dans la vue d'informations associée. Sinon, la liste associée ne sera pas disponible sur la page d'examen.

Chacune des listes associées ajoutées (lors du mappage d'une vue d'informations associée à une liste de points d'entrée) Vue de mappage des informations associées à la liste de points d'entrée (ou directement à partir de la vue) nécessite une configuration supplémentaire pour filtrer les données en ce qui concerne la sélection d'enregistrement d'exécution et la sélection de filtres.

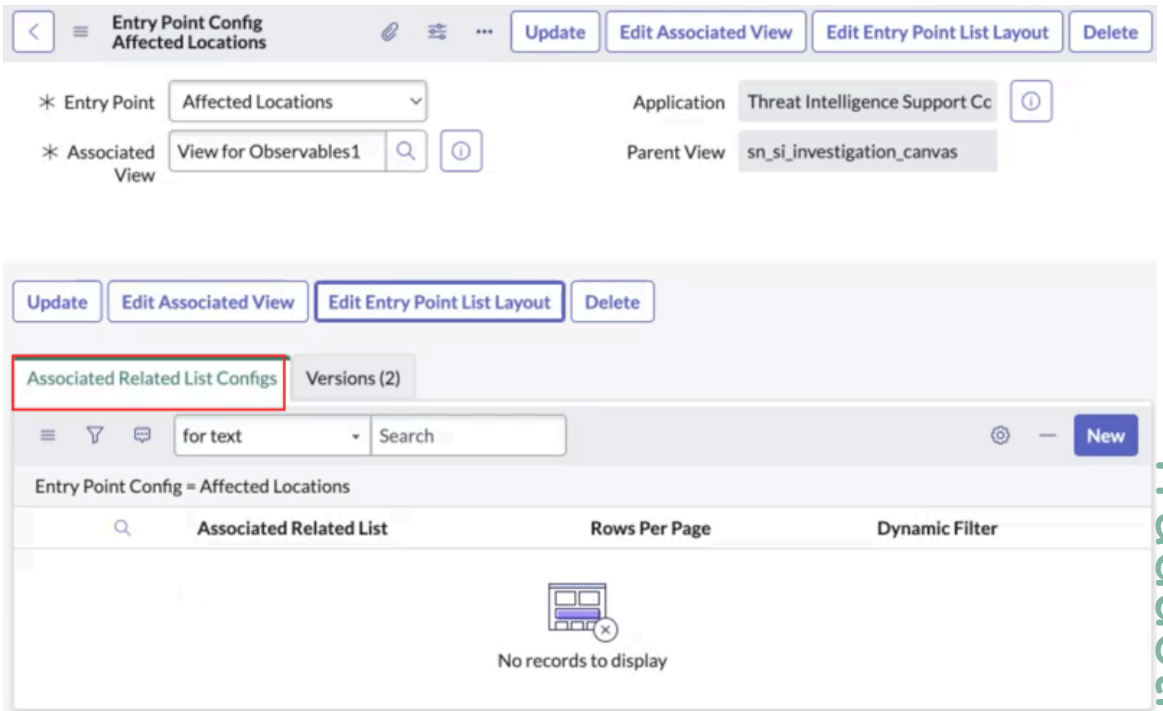
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

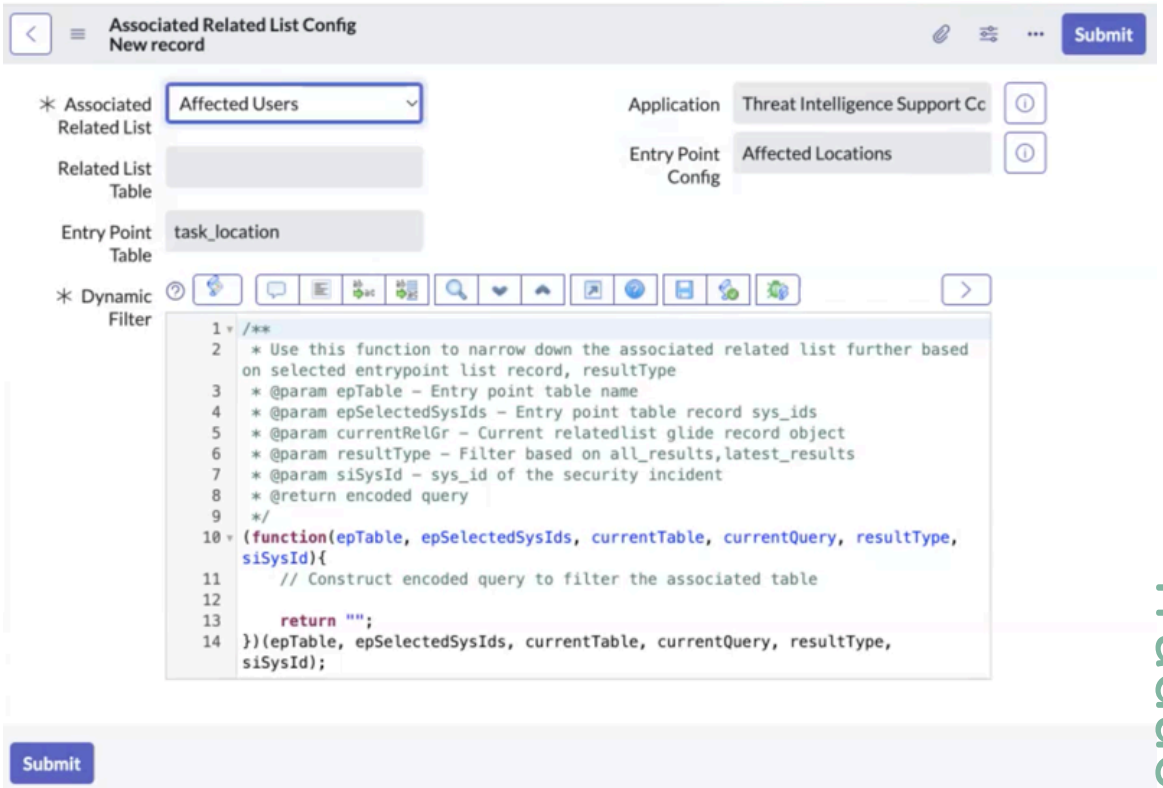
1. Cliquez sur **Nouveau** dans les **configurations de liste associées**.



2. Sélectionnez la valeur du champ **Liste associée** .
3. Utilisez la colonne **Filtre dynamique** pour filtrer davantage la liste associée en fonction des enregistrements de liste de points d'entrée sélectionnés et du type de résultat (derniers résultats de chaque implémentation de fournisseur, tous les résultats).
   Reportez-vous aux exemples existants qui sont expédiés dans le produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Vous pouvez également configurer la mise en page de liste associée à l'aide de l'action **Modifier la mise en page de la liste associée** .
   Dans la fenêtre de la zone de sélection, ajoutez ou supprimez des colonnes selon vos besoins.

Espace de travail SIR Enregistrements connexes

Cette section contient les éléments de listes connexes regroupés en sections, tels que les observables associés et les éléments de configuration.

La liste connexe suivante répertorie les groupes qui sont disponibles dans le cadre du système de base. Vous pouvez modifier ces groupes ou créer des groupes au sein de l'application et de leurs actions respectives.

Vous pouvez modifier ces groupes ou en créer de nouveaux. Pour plus d'informations, consultez la rubrique Configurer la liste connexe des incidents de sécurité Comment configurer et regrouper la liste connexe pour les incidents de sécurité et les tâches de réponse. Chaque liste connexe est entièrement fonctionnelle dans le Espace de travail SIR.

Liste connexe	Élément groupé
Impact sur l'entreprise	• Éléments de configuration • Utilisateurs affectés • Éléments de configuration associés • Utilisateurs associés • Services affectés

Traduction automatique

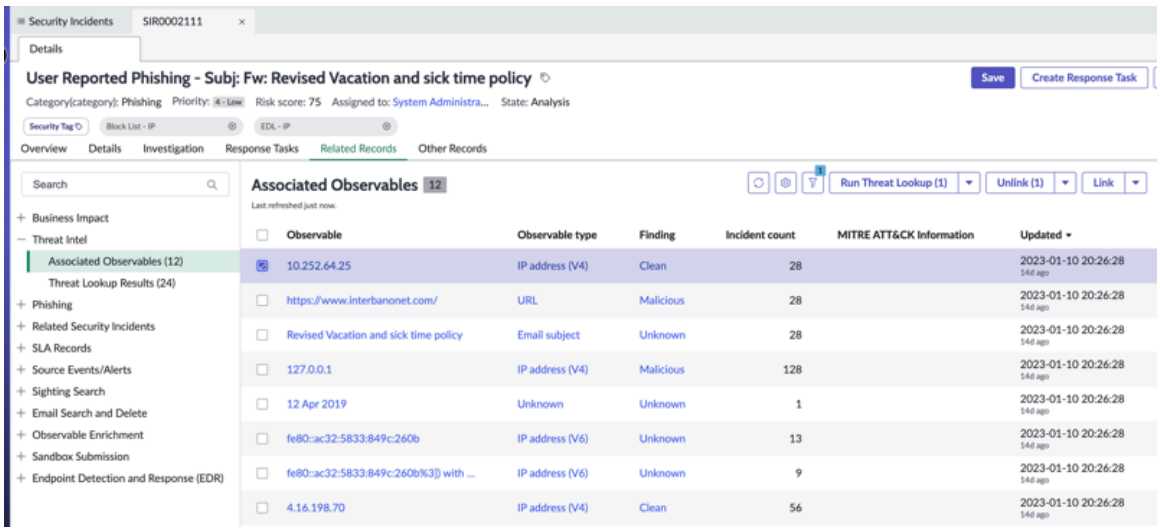
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Élément groupé
Connaissance de la menace	• Observables associés • Résultats de la recherche de menace
Hameçonnage	• E-mails associés Phish • En-têtes d'hameçonnage associés
Incidents de sécurité associés	• Incident de sécurité parent • Incident de sécurité enfant • Incident de sécurité similaire
Enregistrements SLA	SLA de tâche
Événements/alertes sources	Les événements ou alertes sources correspondent à la liste connexe activée de l'intégration SIEM, telle que l'e-mail source, les journaux d'exploration LogRhythm, les événements LogRhythm, l'attaque IBM QRadar agrégée, et ainsi de suite. **Remarque :** Cette liste dépend entièrement de l'intégration que vous avez dans votre instance. Pour afficher la liste connexe d'intégration SIEM pertinente, vous devez installer la dernière version.
Recherche de perception	• Résultats de recherche de perceptions • Détails de la recherche de perception • Perception
Enrichissement des éléments observables	• Résultats de l'enrichissement de l'observable • Événements MISP associés • Résultats de l'enrichissement MISP
Protection évolutive des points de terminaison (PEPT)	• Détails de l'hôte • Processus en cours • Services d'exécution • Utilisateurs connectés • Statistiques réseau • Obtenir un fichier • Isoler les entrées de l'hôte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Élément groupé
	• Actions supplémentaires sur le point de terminaison • Détails des ordinateurs liés à Microsoft Defender pour point de terminaison



Remarque : En général, vous pouvez créer de nouveaux enregistrements, lier ou dissocier des enregistrements existants ou de nouveaux enregistrements par rapport au groupe de listes connexes, le cas échéant.

Information associée

Configurer la liste connexe des incidents de sécurité

Configurer la liste connexe des incidents de sécurité

Vous pouvez ajouter de nouvelles listes connexes ou de nouveaux groupes de listes connexes, et modifier les groupes existants ou les listes connexes qui s'affichent dans l'.Espace de travail SIR

Avant de commencer

Les listes connexes des incidents de sécurité sont regroupées et affichées sous forme d'éléments de liste connexe de groupe dans l'onglet **Enregistrements connexes** de l'espace de travail.

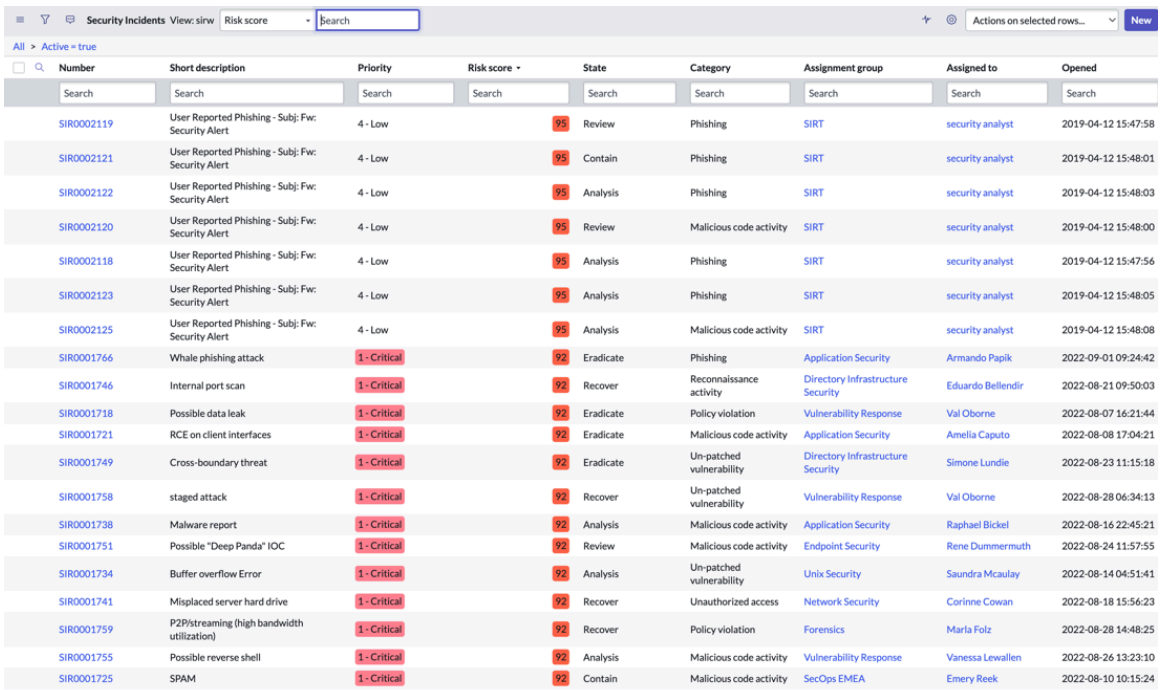
Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans l'interface utilisateur classique, accédez à **Tous** > **Incident de sécurité** > **Afficher les incidents ouverts**.

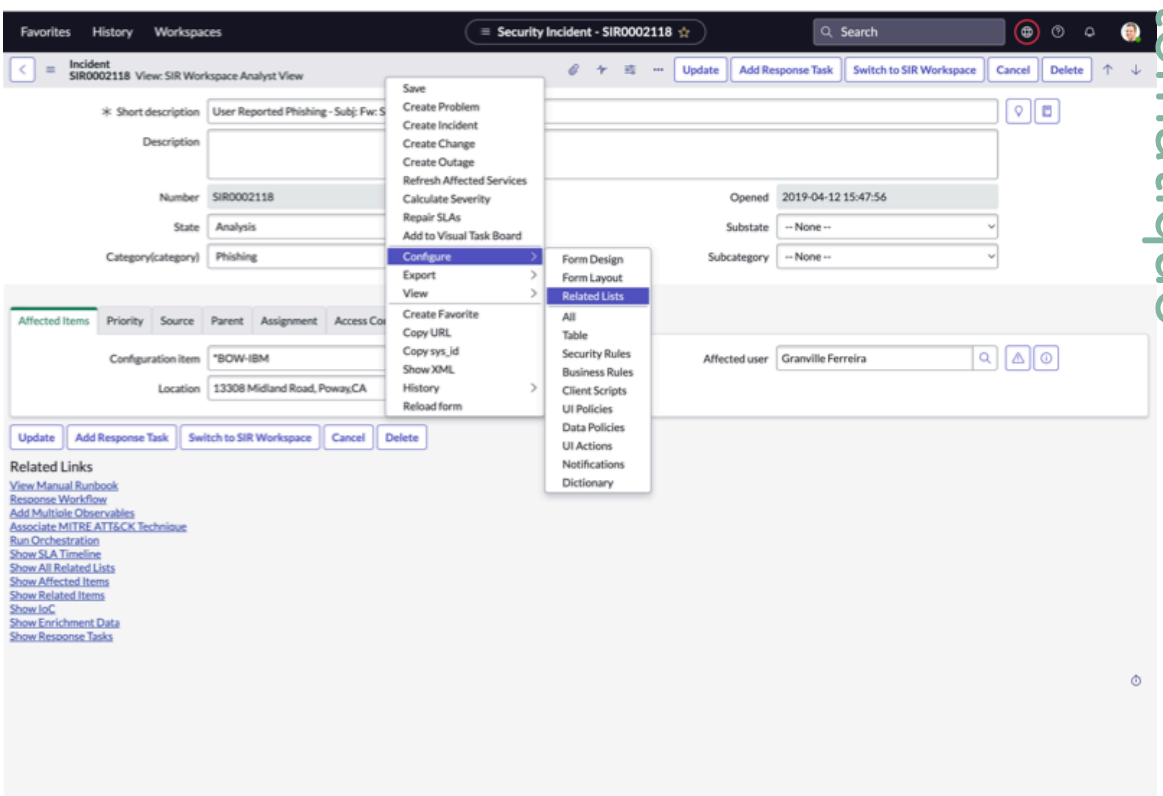


Security Incidents View: sirw | Risk score | Search | Actions on selected rows... | New

All > Active = true

Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. Sélectionnez n'importe quel enregistrement d'incident.
3. Cliquez avec le bouton droit sur le menu contextuel de l'incident.
4. Accéder à **Configurer** > **Liste connexe**.

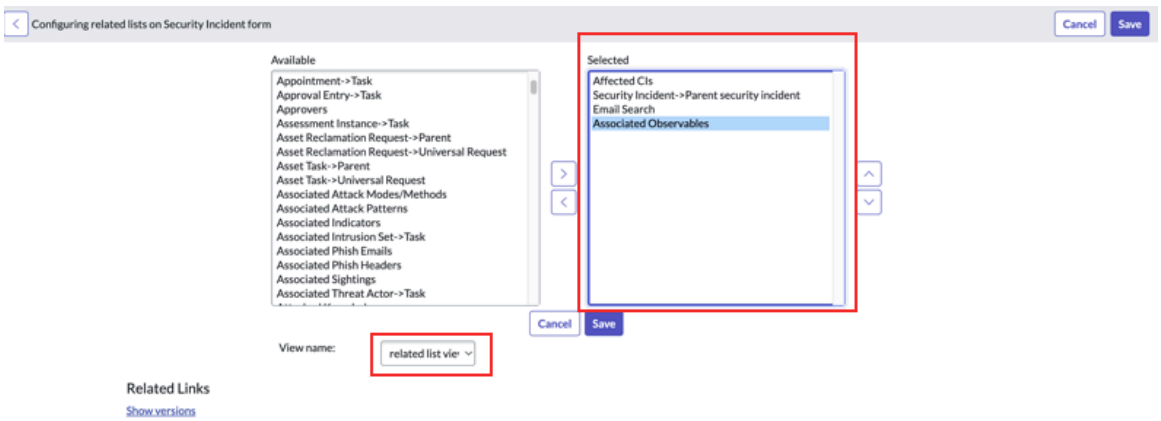


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

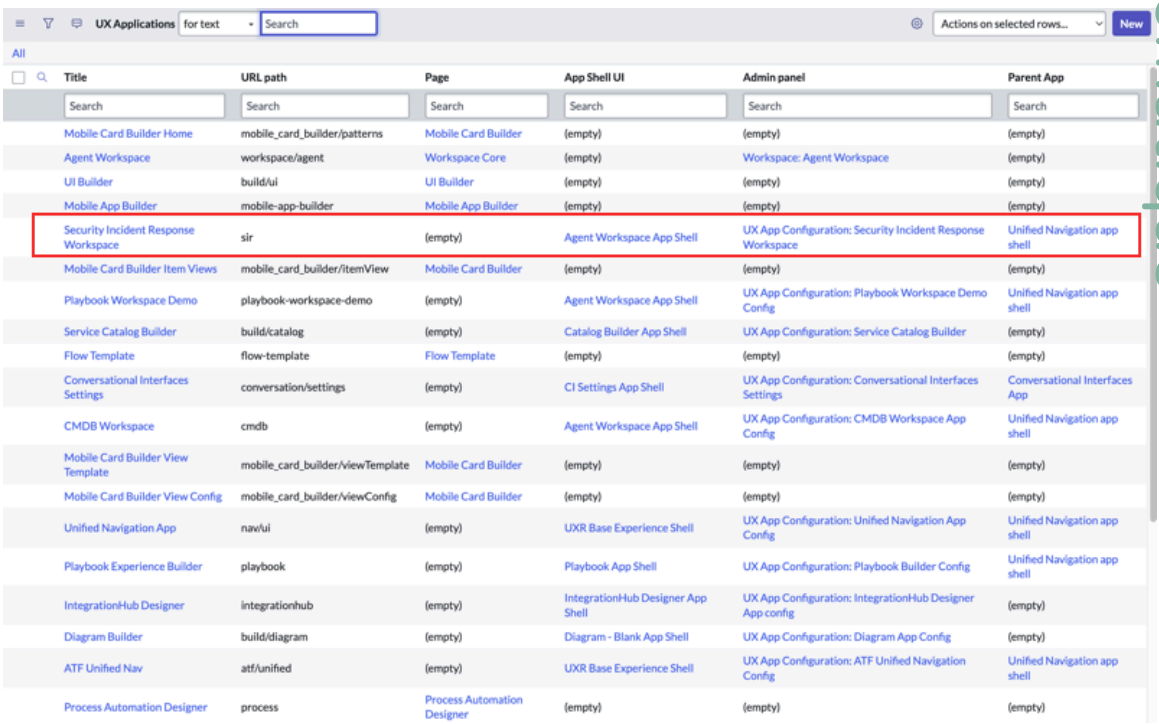
Le **formulaire Configuration des listes connexes sur le formulaire Incident de sécurité** s'affiche.

5. Accédez à **Afficher le nom** et sélectionnez **Nouveau**.
6. Donnez un nom à la vue.
7. Sélectionnez la vue nouvellement créée.
   Après avoir sélectionné la vue, choisissez les champs de liste connexe requis dans la zone de sélection.



Remarque : Si vous souhaitez modifier quoi que ce soit, sélectionnez la vue et supprimez ou ajoutez les éléments.

8. Cliquez sur **Enregistrer**.
9. Dans le volet de navigation de gauche, accédez à **Tous** > **Cadre de travail Now Experience** > **Expériences**.
10. Sélectionnez **Espace de travail de Réponse aux incidents de sécurité**.

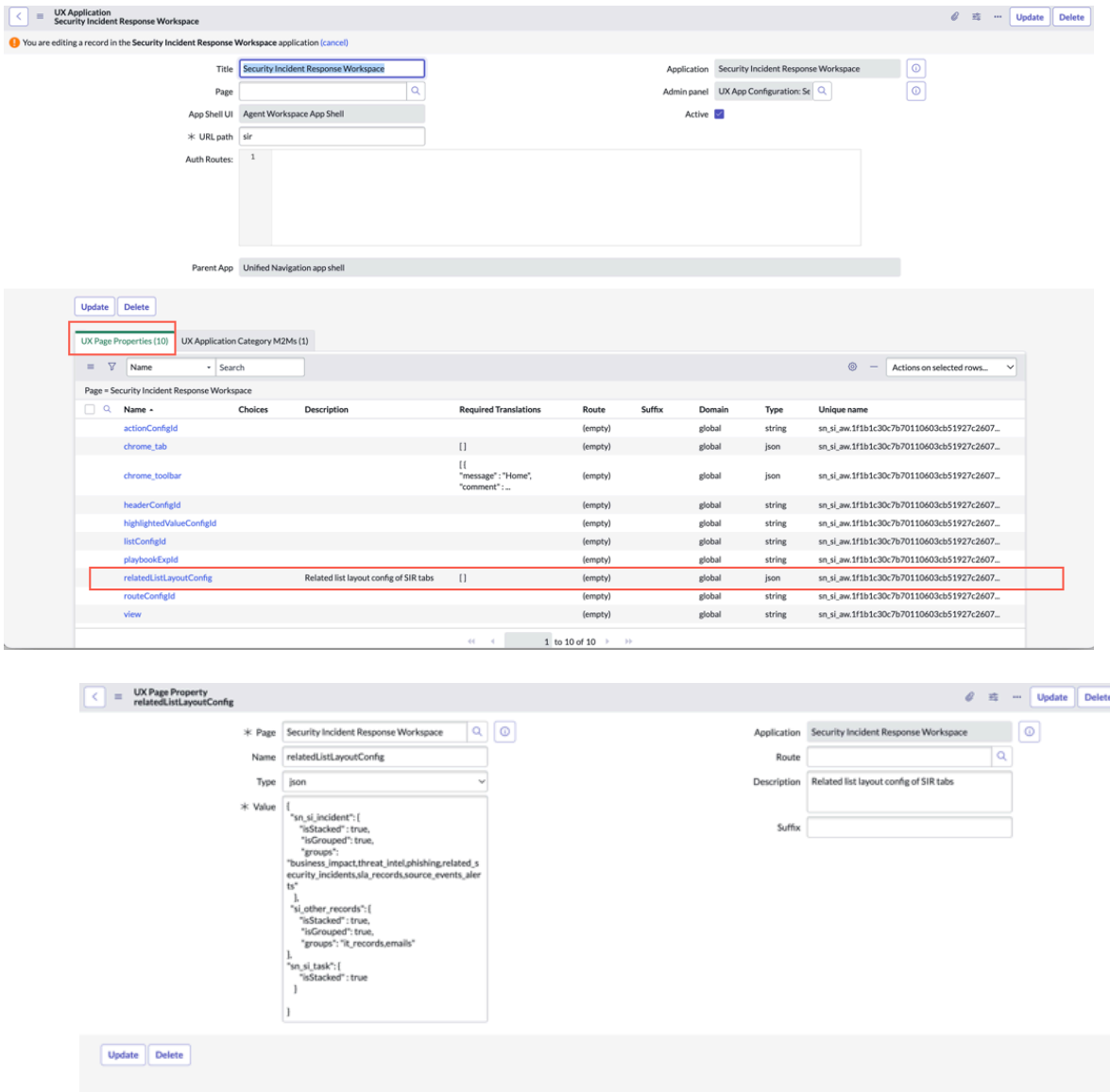


La page **Espace de travail de Réponse aux incidents de sécurité des applications UX** s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

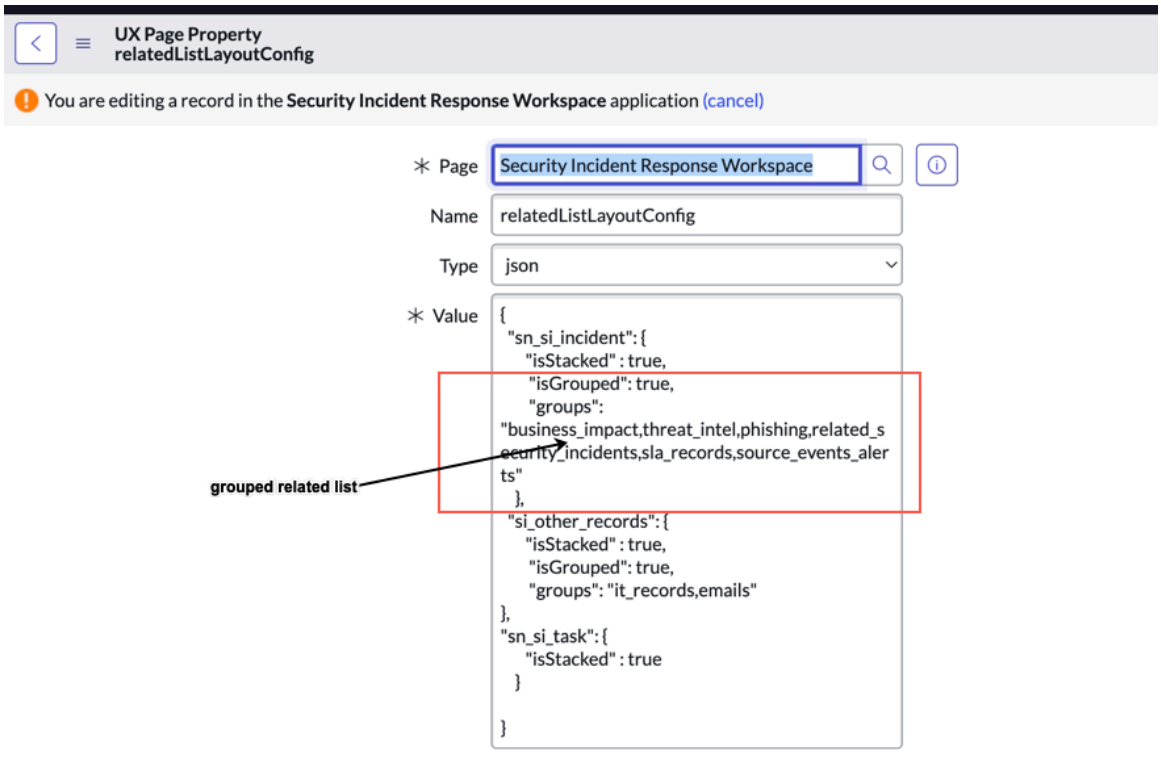
11. Accédez à l'onglet Propriétés de la **page UX** et sélectionnez l'option **relatedListLayoutConfig** dans la vue de liste.



12. Ajoutez le nom de la vue nouvellement créée, séparé par une virgule, à une liste de valeurs déjà existante dans la zone de texte **Valeur** sous le champ **sn_si_incident.viewsUsedForGrouping** .
Par exemple, si vous avez créé un nouveau nom d'affichage en tant que **Business Impact**, vous devez le **business_impact** spécifier dans la zone de texte **Valeur** (qui est séparé par un trait de soulignement dans le nom de la vue et séparé par une virgule après une valeur existante) sous le champ sn_si_incident :groups.

Traduction automatique

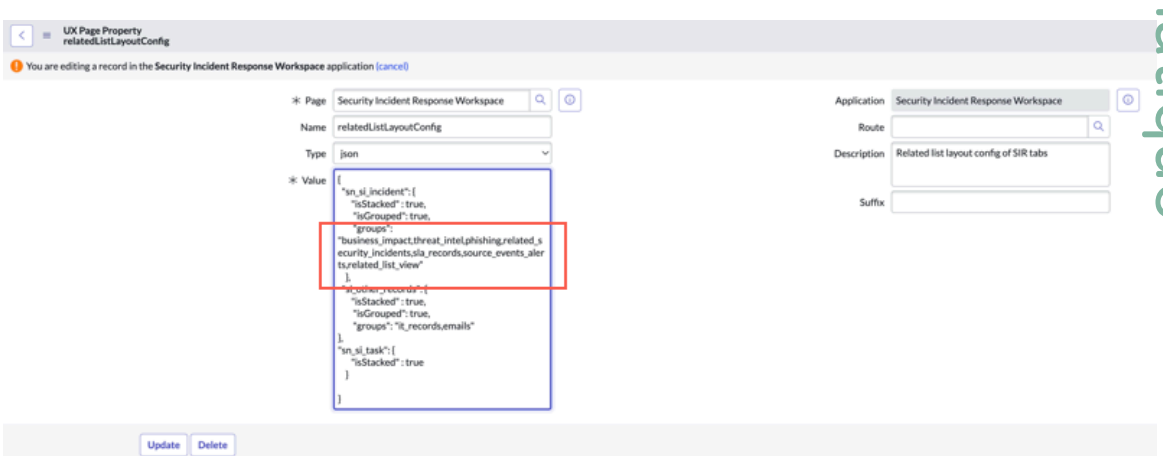
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Si vous ajoutez le nouveau nom de la vue sous **le champ sn_si_incident.viewsUsedForGrouping** , l'entrée est créée dans l'onglet **Enregistrements connexes** de l'espace de travail.

Si vous mettez à jour l'entrée du nom de la vue dans **si_other_records.viewsUsedForGrouping** , le groupe de listes connexe est ajouté dans l'onglet **Autres enregistrements** de l'espace de travail.

Vous trouverez ci-dessous un exemple de vue qui montre les vues ajoutées nouvellement créées.



Remarque : **requiredRolesForGrouping contient des noms d'enregistrements** de sys_user_role séparés par des virgules. L'utilisateur de l'espace de travail SIR doit avoir au moins un de ces rôles pour utiliser les listes connexes groupées. Lorsqu'un utilisateur ne possède aucun de ces rôles, la vue de listes connexes configurée pour le rôle d'utilisateur actuel à l'aide de la configuration de la règle de vue est représentée verticalement sans regroupement. Cette propriété est **ignorée lorsque la propriété isGrouped** est définie sur false. Si cette propriété est vide, tout utilisateur peut accéder aux listes connexes groupées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

13. Cliquez sur **Enregistrer**.
14. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
15. Sélectionnez un incident de sécurité spécifique.
16. Accédez à l'onglet **Enregistrements connexes** de l'espace de travail.
    Les listes connexes groupées s'affichent.

Configurer la liste connexe des tâches de réponse

Utilisez cette section pour configurer les tâches de réponse nouvelles listes connexes qui apparaissent sur l'application Réponse aux incidents de sécurité.

Avant de commencer

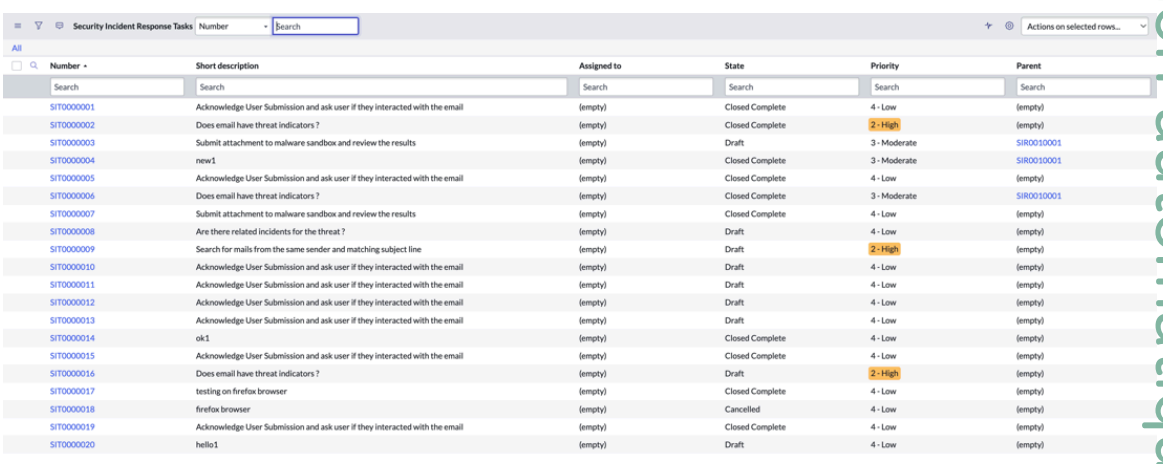
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

La liste connexe des tâches de réponse n'est pas regroupée, mais s'affiche sous forme d'éléments de liste connexes individuels, car il existe peu de listes par défaut. Affichez les éléments connexes des tâches de réponse dans l'onglet **Tâches de réponse** de l'enregistrement d'incident de sécurité de l'espace de travail.

Procédure

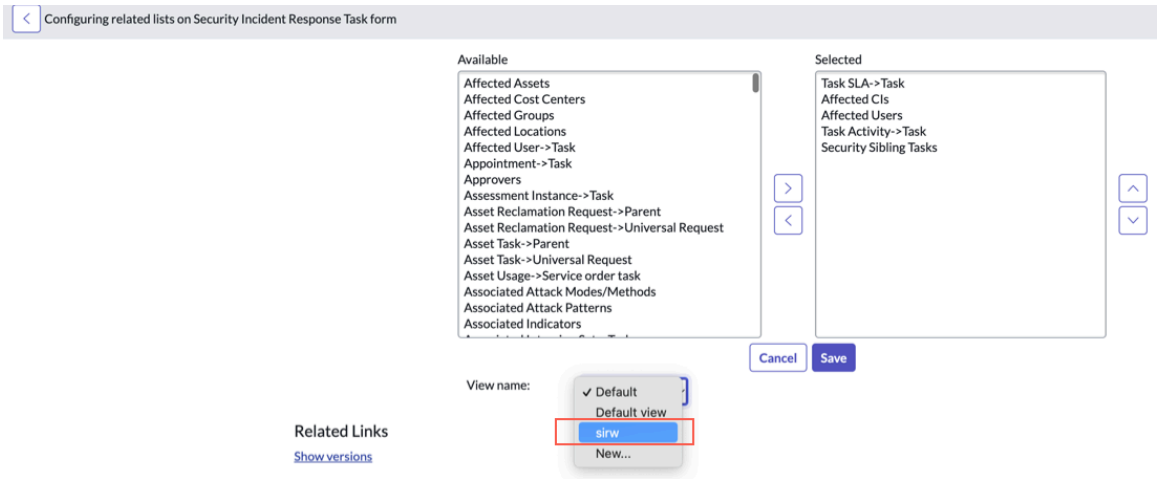
1. Accédez à la **Tous** > **Incident de sécurité** > **Tâches de réponse** > **Afficher toutes les tâches**.



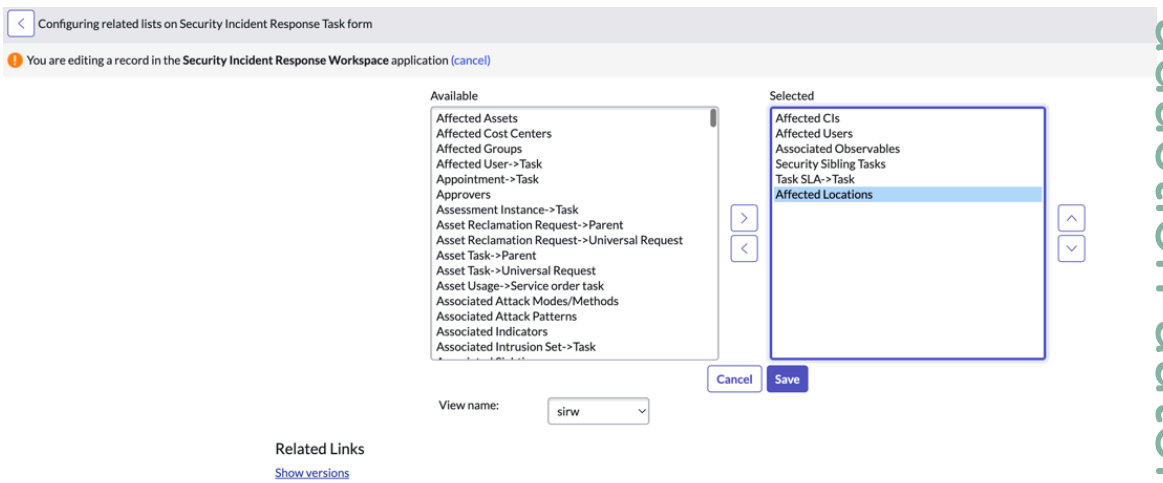
2. Sélectionnez n'importe quel enregistrement de tâche de réponse.
3. Cliquez avec le bouton droit sur le menu contextuel de la tâche Réponse aux incidents de sécurité.
4. Accédez à la **Configurer** > **Liste connexe**.
   La **configuration des listes connexes du formulaire Tâche de réponse de sécurité** s'affiche.
5. Allez dans **Afficher le nom** et sélectionnez la vue **sirw** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Sélectionnez les champs de liste connexe souhaités dans la zone de sélection.
   Par exemple, Emplacements affectés.

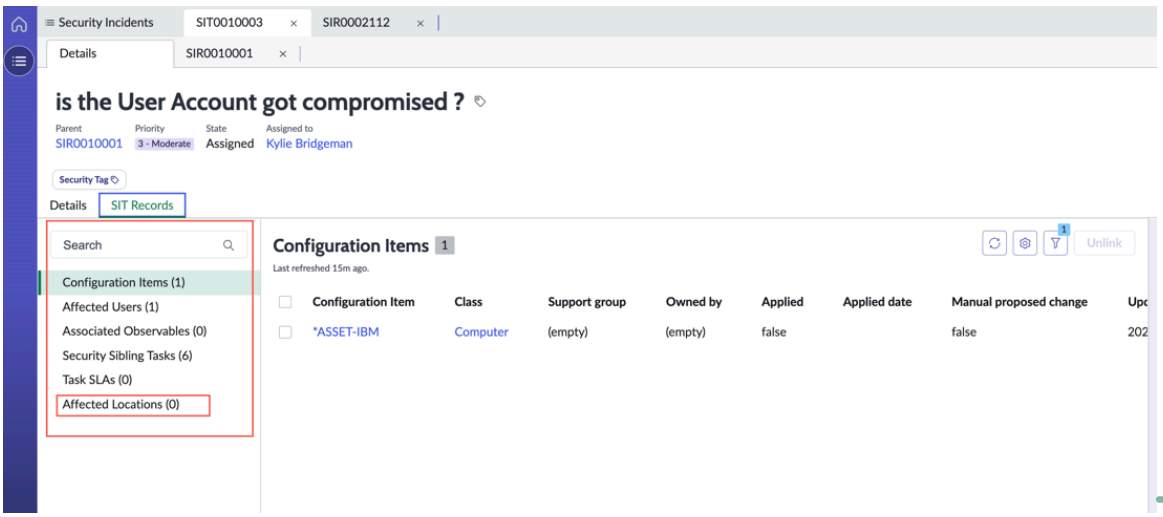


7. Cliquez sur **Enregistrer**.
8. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Tâches de réponse** > **Enregistrements SIT**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les listes connexes configurées (par exemple, emplacements affectés selon la sélection) sont répertoriées dans la liste des enregistrements SIT.



Définir les nouvelles règles du calculateur de score de risque

Utilisez le nouveau calculateur de score de risque pour définir et calculer le score de risque des incidents de sécurité en fonction des critères définis par l'utilisateur, qui fournissent un score d'intelligence transparent des incidents de sécurité. Le score de risque est calculé automatiquement pour les enregistrements d'incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.admin.

Activez le nouveau calculateur de score de risque en définissant la propriété système sn_si_aw.activate_new_risk_score_calculator sur vrai.

Pourquoi et quand exécuter cette tâche

Définissez un score de risque pour les enregistrements d'incidents de sécurité qui sont générés en fonction des paramètres définis par l'utilisateur. Le système de base est approvisionné avec une règle de notation des risques, qui peut être personnalisée et activée en conséquence.

Remarque :

- Par défaut, la nouvelle règle du calculateur de score de risque est inactive et vous devez activer la règle pour consulter le score de risque des incidents de sécurité.
- Pour calculer le score de risque pour d'autres tables connexes que celles disponibles dans le système de base, reportez-vous à .Calculateur de score de risque pour les tables connexes supplémentaires

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Administration**.
2. Accédez à la **Moteur de règles** > **Règle du calculateur de score de risque**.
   La page Règle du calculateur de score de risque s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Dans le cadre du système de base, vous disposez d'un modèle de règle de notation du risque prédéfini pour afficher, modifier ou modifier le score du risque. Toutefois, vous ne pouvez pas créer ou supprimer le modèle de règle de score de risque prédéfini.
- Les modifications que vous apportez s'appliqueront à tous les nouveaux incidents de sécurité ou aux mises à jour des incidents existants. Pour reformuler les scores historiques, utilisez l'action **Recalculer le score** .

3. Sélectionnez la règle du **calculateur de score de risque** .

4. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom de la valeur du score de risque. Par exemple, Calculateur de score de risque.
Pondération globale (applicable au générateur de critères)	Pondération de ce champ dans la règle de risque. Ce champ n'est pas modifiable et affiche la pondération globale calculée par le système en fonction du poids correspondant aux critères activés. La pondération globale doit toujours être de 100 %.
Description	Description de l'enregistrement du score de risque. Par exemple, calcule le score de risque en fonction de la somme pondérée des scores de critères prédéfinis.
Critères de notation	Indique les critères de notation d'un incident de sécurité. Vous pouvez définir les **critères de score** du risque à l'aide des options suivantes : ○ **Générateur de critères** : Utilisez cette option pour ajouter, modifier ou supprimer, activer et désactiver les critères qui contribuent au calcul du score de risque et vérifier que la pondération agrégée totale est de 100 %. ○ **Utiliser un script (avancé)** : la fonctionnalité de scripting est une fonctionnalité avancée permettant de créer un script personnalisé qui doit renvoyer le score de risque, qui est une valeur entière comprise entre 0 et 100.

5. Pour définir les **critères de notation** à l'aide du **générateur de critères**, procédez comme suit :

Remarque : Vous pouvez modifier les critères existants ou en ajouter un nouveau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Pour ajouter un nouveau critère, sélectionnez l'action **+Nouveau critère** .

b. Sélectionnez la **table** pour laquelle vous souhaitez définir les critères.

Remarque :

- Si la table sélectionnée est un incident de sécurité, la condition est appliquée à l'enregistrement d'incident de sécurité pour lequel le score de risque est calculé. Si la table sélectionnée n'est pas un incident de sécurité, la condition est appliquée uniquement si les enregistrements sont liés à l'incident de sécurité pour lequel le score de risque est calculé.
- Un type d'agrégat supplémentaire est ajouté pour définir les scores en fonction du nombre de relations associées aux incidents de sécurité.

c. Sélectionnez le critère **Type** pour la table sélectionnée.
La valeur Type peut être **Champ** ou **Agrégat** en fonction de la table que vous choisissez.

d. Sélectionnez les critères de **champ** de la table sélectionnée.
Si vous avez sélectionné la valeur Type **Champ**, les critères Champ affichent les valeurs de champ associées à la table. Si vous avez sélectionné la valeur Type **Agrégat,** les critères Champ affichent les valeurs agrégées associées à la table.

Remarque : Le type d'agrégat prend uniquement en charge la valeur Nombre.

Par exemple, si vous sélectionnez les critères de table comme **incident de sécurité**, les critères de type affichent uniquement l'option **Champ** . Les critères Champ affichent toutes les valeurs de champ associées à la table, qui peuvent être Gravité, Actif, etc. De même, si vous sélectionnez les critères Table en tant **qu'Utilisateurs affectés**, les critères Type affichent les options **Champ** et **Agrégat.** Si vous sélectionnez le type Agrégat, les critères de champ affichent les valeurs agrégées associées à la table, à savoir **Nombre**.

e. Entrez la **pondération** des critères entre 0 et 100.
La pondération globale de tous les critères doit être de 100 %.

f. Entrez le nom et une brève description des critères.

g. Cochez la case **Activer les critères de notation** pour activer les critères de notation.

h. Définissez les **conditions** et définissez le score pour les conditions.

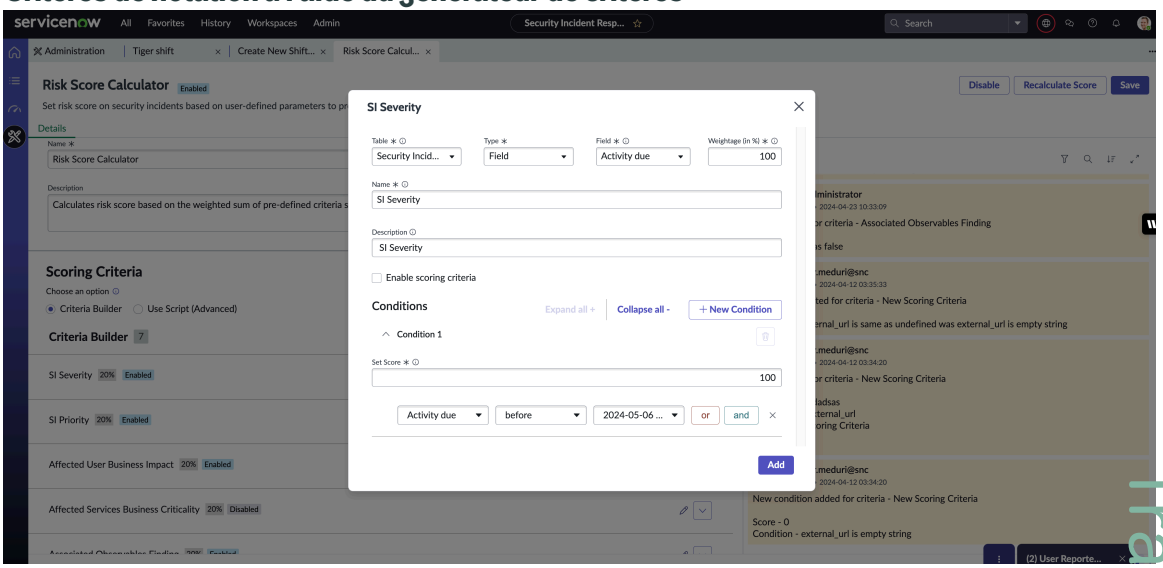
i. Vous pouvez également ajouter de nouvelles conditions à l'aide de l'option **Nouvelle condition** et supprimer des conditions existantes à l'aide de l'icône **Supprimer les critères** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

j. Sélectionnez **Ajouter** pour ajouter les critères configurés.

Critères de notation à l'aide du générateur de critères



6. Sélectionnez l'option **Recalculer le score** pour recalculer le score de risque.

   Par exemple, si des changements sont apportés à la règle du score de risque. Dans ce cas, vous devez réappliquer la règle de notation aux incidents de sécurité dont le score de risque a déjà été calculé dans le passé. Utilisez l'action **Recalculer le score** pour déclencher la tâche de recalcul.

7. Sélectionnez **Confirmer**.

   Remarque : Une fois que vous avez déclenché cette action, le processus s'exécute en arrière-plan et prend quelques minutes. Vous ne serez pas en mesure d'apporter des changements tant qu'elle n'est pas terminée.

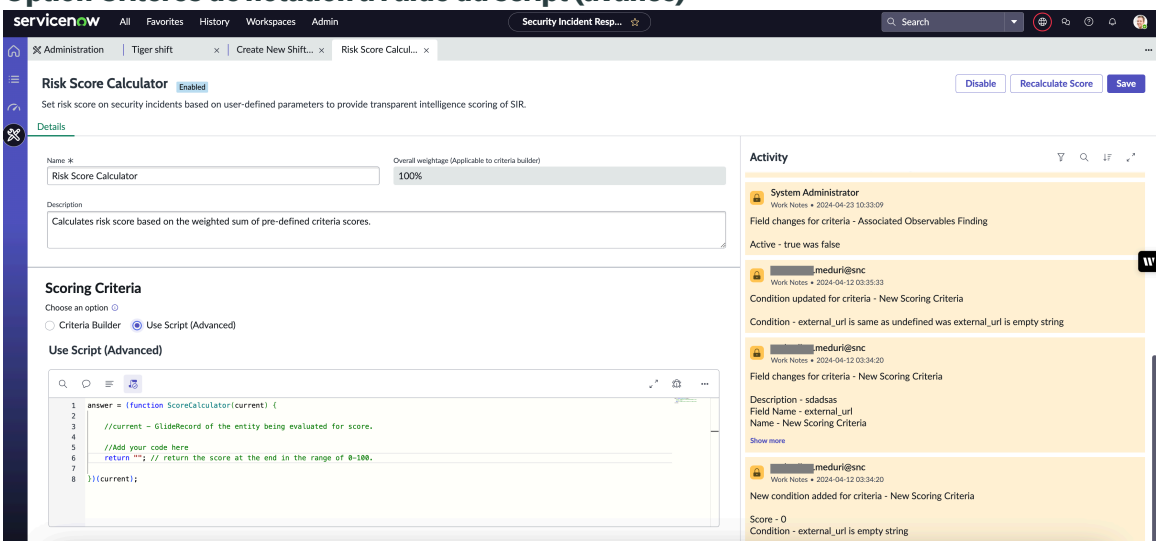
8. Pour définir les **critères de notation** à l'aide de l'option **Utiliser le script (avancé),** procédez comme suit :

   a. Utilisez ce script prédéfini pour créer un script personnalisé qui doit renvoyer le score de risque, qui est une valeur entière comprise entre 0 et 100.
   Le champ de script avancé est rempli automatiquement avec une fonction, qui prend les paramètres **actuels** et cette fonction doit renvoyer le score de risque, qui est une valeur entière comprise entre 0 et 100.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option Critères de notation à l'aide du script (avancé)



Ici, le paramètre actuel est l'objet GlideRecord de l'entité (incident de sécurité) pour laquelle le score de risque est calculé. Pour les incidents de sécurité, cela correspond au GlideRecord pour la table sn_si_incident.

9. Pour désactiver le calculateur de score de risque, sélectionnez **Désactiver**.
10. Sélectionnez **Enregistrer**.

Calculateur de score de risque pour les tables connexes supplémentaires

Le calculateur de score de risque est doté d'une règle de notation du risque dans le cadre du système de base pour calculer le score de risque des incidents de sécurité en fonction des critères définis par l'utilisateur. Toutefois, vous pouvez personnaliser et inclure des tables connexes supplémentaires pour calculer le score de risque.

Avant de commencer

Rôle requis : sn_si.admin.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez n'importe quel enregistrement d'incident de sécurité.
3. Sélectionnez l'option **Actions supplémentaires** en regard du numéro d'incident de sécurité.
4. Accéder à **Configurer** > **Listes connexes**.
5. Accédez au nom de la vue, puis sélectionnez **Calculateur de score de risque**.
   Après avoir sélectionné la vue, choisissez la liste connexe requise que vous souhaitez ajouter à partir de la zone de sélection. Par exemple, Perceptions associées.
6. Sélectionnez **Enregistrer**.
   Vous avez ajouté avec succès les nouvelles listes connexes ou tables pour lesquelles vous souhaitez calculer le score de risque.

> **Important :** Pour calculer le score de risque des incidents de sécurité qui présentent de nouveaux critères avec les listes connexes nouvellement créées, vous devez définir des règles métier sur la table de base de la liste connexe.

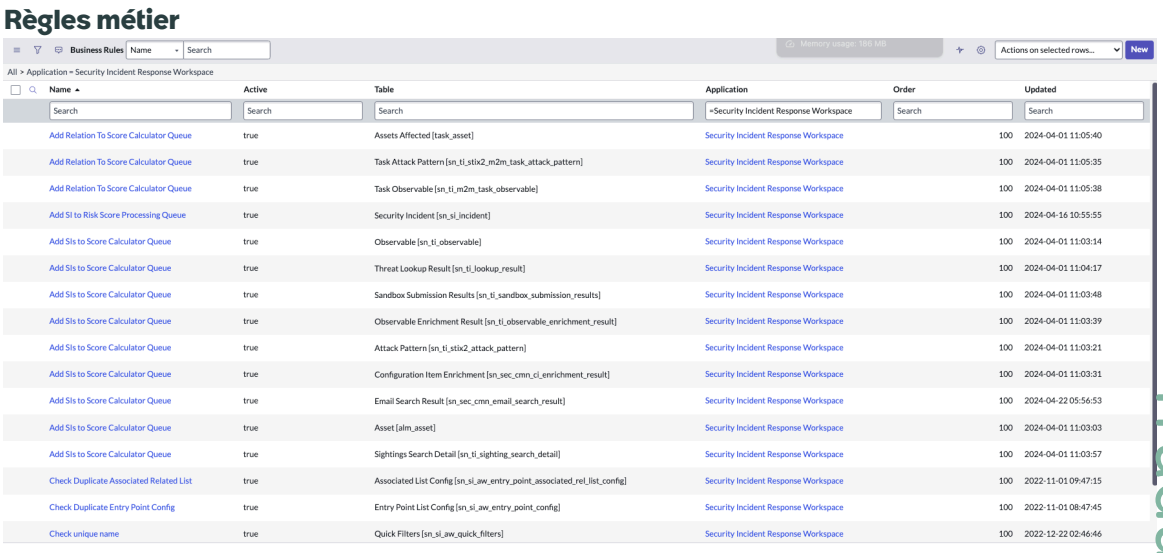
7. Accédez à la **Tous** > **Définition du système** > **Règles métier**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez utiliser les deux règles métier suivantes comme référence pour créer vos propres règles métier :

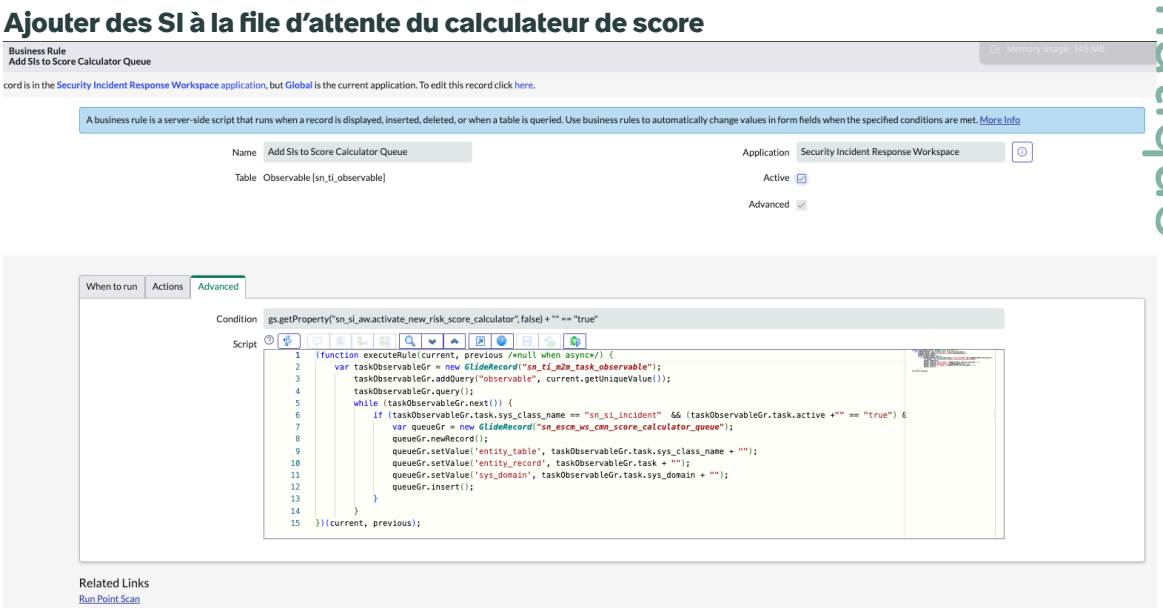
- Ajouter des incidents de sécurité (SI) à la file d'attente du calculateur de score
- Ajouter une relation à la file d'attente du calculateur de score (cela s'applique aux tables m2m)



8. Par exemple, pour que les critères observables associés fonctionnent, nous avons défini deux règles métier.

   La première est la règle métier **Ajouter des SI à la file d'attente du calculateur de score** .

   Par exemple, un nouvel incident de sécurité est créé et associé à une table d'observables (Observables[sn_ti_observable]). Après la recherche de menace, l'observable s'avère malveillant. Vous devez ensuite ajouter tous les incidents de sécurité associés à cet observable malveillant à la file d'attente pour recalculer le score de risque des incidents de sécurité.



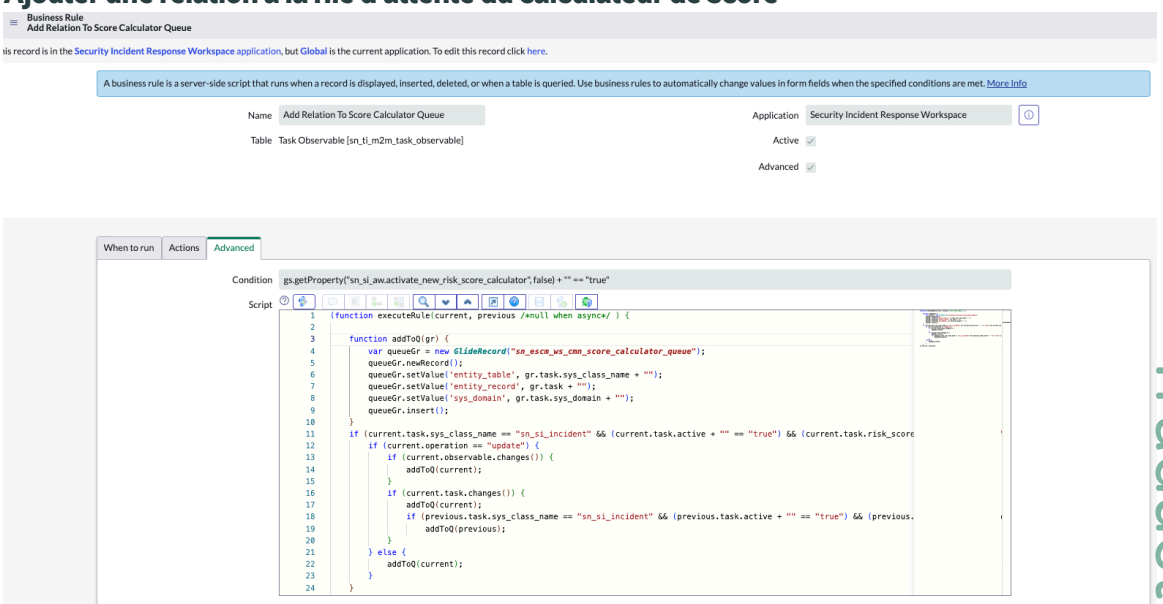
   La seconde est la règle métier **Ajouter une relation à la file d'attente du calculateur de score** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, un nouvel incident de sécurité est créé ou supprimé et associé à une table d'observables (Observables de tâche[sn_ti_m2m_task_observable]). Il y a donc un changement dans l'association de l'incident de sécurité. Vous devez ensuite ajouter cet incident de sécurité à la file d'attente pour recalculer le score de risque de l'incident de sécurité.

Ajouter une relation à la file d'attente du calculateur de score



Configurer le transfert d'équipe

Configurez les paramètres de transfert d'équipe pour fournir des informations complètes sur l'équipe aux analystes d'équipe suivants.

Configurer les modèles de transfert d'équipe

L'administrateur peut définir et configurer différents modèles de transfert d'équipe pour que le propriétaire d'équipe crée des enregistrements de transfert d'équipe et les remette à l'équipe d'équipe suivante.

Avant de commencer

Rôle requis :

- sn_escm_sh.shift_admin
- sn_si.admin hérite du rôle sn_escm_sh.shift_admin

Pourquoi et quand exécuter cette tâche

Pour configurer un modèle de transfert d'équipe, l'administrateur crée un nouveau modèle de transfert d'équipe ou ouvre un modèle existant dans le système de base avec le nom **Exemple de modèle d'équipe** et modifie les détails et les sections en fonction de vos besoins.

Le propriétaire du quart peut utiliser le modèle configuré pour créer des enregistrements du journal de transfert d'équipe, puis le rapport de transfert d'équipe est partagé avec le propriétaire du quart actif suivant et l'équipe.

Remarque : Seuls les modèles de transfert d'équipe actifs sont visibles pour que le propriétaire du quart crée des enregistrements de journal de relais.

Traduction automatique

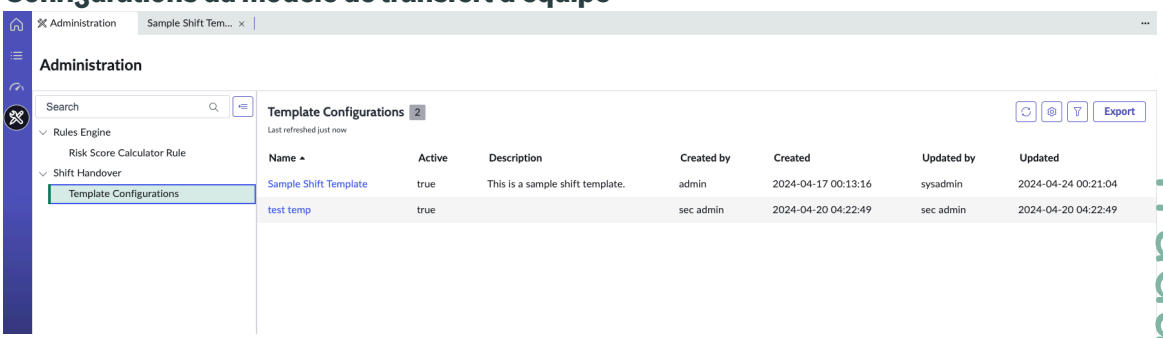
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Administration**.
2. Accédez à la **Transfert d'équipe** > **Configurations de modèles**.
   La page Modèles de configuration s'affiche.

> **Remarque :** Dans le cadre du système de base, vous disposez d'un modèle de transfert d'équipe prédéfini pour afficher, modifier ou modifier le modèle de transfert d'équipe. Toutefois, vous ne pouvez pas créer ni supprimer la configuration prédéfinie du modèle de transfert d'équipe.

Configurations du modèle de transfert d'équipe



3. Pour créer un nouveau modèle de transfert d'équipe, sélectionnez **Nouveau**.
4. Renseignez les champs du formulaire Détails.

Créer un nouveau modèle de transfert d'équipe

Champ	Description
Nom	Nom du modèle de transfert d'équipe. Par exemple, Modèle SIR.
Application	Nom de l'application pour laquelle vous créez le modèle de transfert d'équipe. Par exemple, Espace de travail Réponse aux incidents de sécurité.
Actif	Option permettant d'indiquer si le modèle de transfert d'équipe est actif. Activez cette option pour activer le modèle de transfert d'équipe.
Description	Description du modèle de transfert d'équipe.
Enregistrer la configuration de la mention	Utilisez ce champ pour configurer les détails de la mention de l'enregistrement de l'éditeur de texte enrichi (RTE). L'entrée est un tableau d'objets JSON contenant les champs suivants : ○ `sourceTable` : nom de la table source. ○ `label` : nom de l'étiquette à afficher. ○ `filterCondition` : requête codée pour le filtrage. Vous pouvez ajouter plusieurs requêtes pour la même table afin de récupérer les valeurs de manière dynamique. Ces valeurs sont mises à jour lorsque l'enregistrement de transfert d'équipe est publié ou en fonction de la date de début et/ou de fin de l'équipe. Par exemple, nombre d'enregistrements d'incidents

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	de sécurité par priorité, nombre d'enregistrements d'incidents de sécurité par état. Vous pouvez utiliser les arguments {start_date} et {end_date} dans la requête pour spécifier une plage de dates. Par exemple, « filterCondition » : « active=true^sys_created_on>=${start_date}^sys_created_on<=${end_date} » ○ *`fields`* : sélectionnez les champs pour interroger le modèle. Exemple de configuration que vous pouvez copier et coller dans le champ de configuration de la mention de l'enregistrement. `[ { "sourceTable": "incident", "label": "Incidents active", "filterCondition": "active=true", "fields": [ "number" ] } { "sourceTable": "incident", "label": "Active incidents created after selected date", "filterCondition": "active=true^sys_created_on>=${start_date}", "fields": [ "number" ] } ]` Pour copier l'exemple de configuration, utilisez l'action **Copier dans le presse-papiers** du volet Assistance contextuelle. Ensuite, vous pouvez apporter des modifications supplémentaires en fonction de vos besoins.
Modèle	Créez un modèle de transfert d'équipe à l'aide de sections. Assurez-vous qu'il existe au moins une section pour que les analystes puissent contribuer aux enregistrements du journal de transfert d'équipe basés sur le modèle. Le modèle peut contenir du texte statique, des images, etc., dans les sections appropriées. Vous pouvez copier et coller des images directement dans le champ Modèle. Vous pouvez créer des sections dans le modèle à l'aide du code suivant : `${section:Section Label}` Exemple :

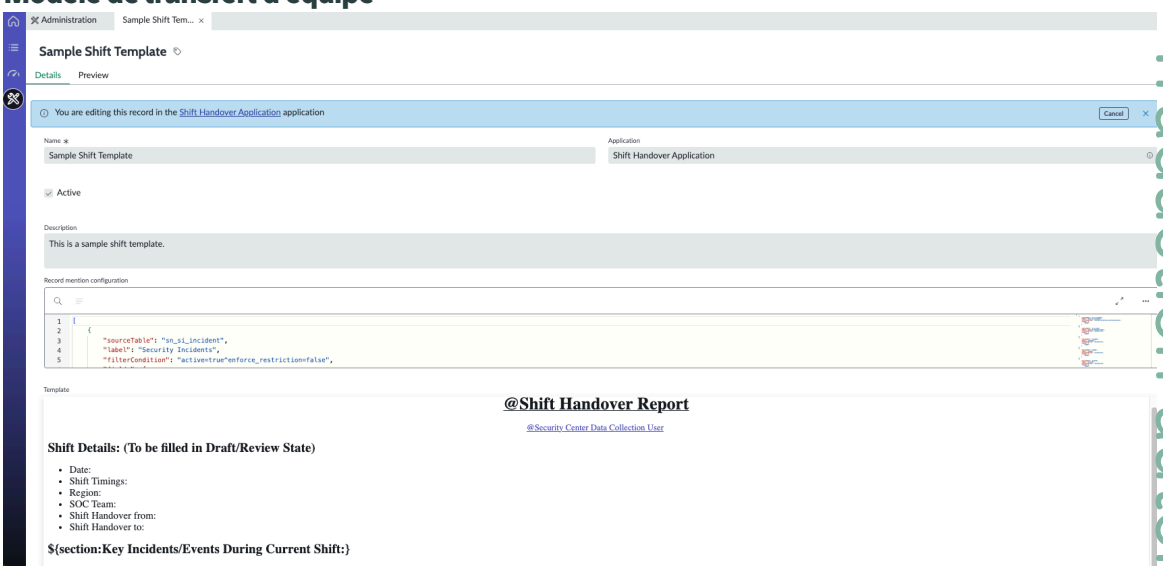
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	${section:Key Incidents/Events During Current Shift} ${section:Incidents/Events to Monitor or Follow Up} ${section:System/Infrastructure Updates} ${section:Next Steps for Incoming Shift} ${section:References} **Remarque :** Pour plus d'informations, reportez-vous à **l'assistance contextuelle** dans le volet droit.

5. Pour utiliser et modifier un modèle de transfert d'équipe existant, sélectionnez **Exemple de modèle d'équipe**.

Modèle de transfert d'équipe



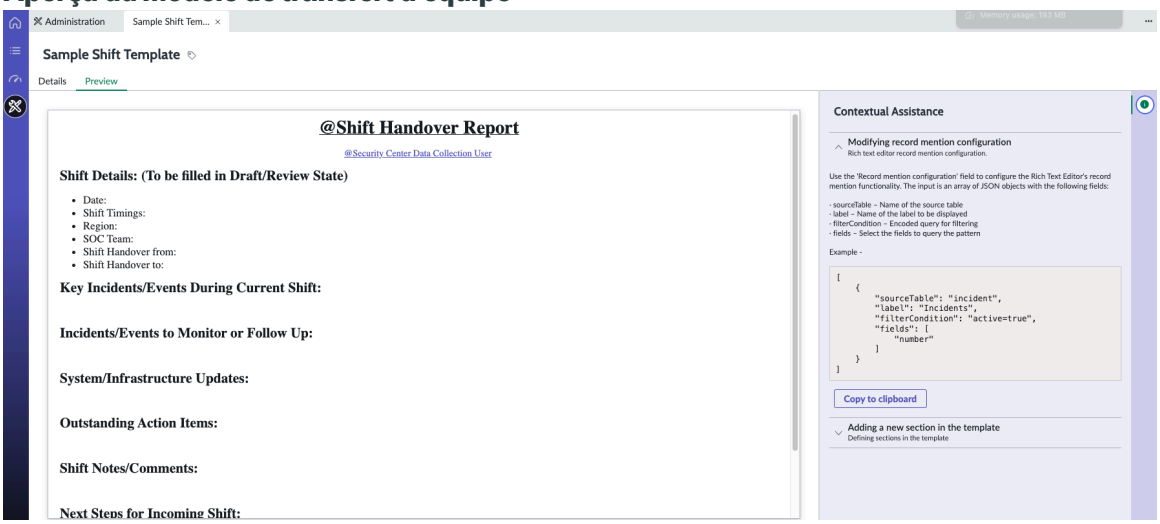
6. Mettez à jour le modèle de transfert d'équipe en fonction de vos besoins.
7. Sélectionnez **Aperçu** pour afficher l'aperçu d'exécution du modèle de transfert d'équipe.

   Le rapport génère un aperçu en fonction de la configuration du modèle de transfert d'équipe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçu du modèle de transfert d’équipe



8. Sélectionnez **Enregistrer** pour enregistrer le modèle de transfert d’équipe.

Que faire ensuite

Pour apprendre à gérer les enregistrements de transfert d’équipe dans la vue de liste et à effectuer des actions telles que créer, modifier, copier ou supprimer des enregistrements de transfert d’équipe, reportez-vous à la section Gérer les enregistrements de transfert d’équipe.

Créer des accèsEspace de travail de la Réponse aux incidents de sécurité

Créez des équipes via le à utiliser lors de la Espace de travail de la Réponse aux incidents de sécurité configuration desrapports hiérarchiques.

Avant de commencer

Rôle requis :

- sn_escm_sh.shift_admin
- sn_si.admin hérite du rôle sn_escm_sh.shift_admin

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Administration**.
2. Accédez à la **Transfert d'équipe** > **Configurations des planifications d'équipe**.
   La page Configuration du temps d’équipe affiche toutes les équipes existantes.
3. Sélectionnez **Nouveau**.
4. Entrez un nom dans le champ**Équipe**.
5. Indiquez les heures de début et de fin de l’équipe dans les champs**Heure de début** et **Heure de fin** .

   Remarque : L’heure de début et l’heure de fin se trouvent dans le fuseau horaire configuré de l’utilisateur actuel.

6. Sélectionnez **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux incidents de sécurité COnference CToute l'intégration

L'intégration Réponse aux incidents de sécurité de la téléconférence vous permet de gérer et de lancer une téléconférence ainsi qu'un chat pour les analystes, les responsables et les utilisateurs concernés.

La Réponse aux incidents de sécurité fonctionnalité de téléconférence vous permet de collaborer avec des clients et des agents pairs pour résoudre des incidents de sécurité au cours d'un appel. Vous pouvez également collaborer à l'aide d'une discussion de groupe.

Vous pouvez lancer des téléconférences à l'aide de canaux de communication tiers tels que Microsoft Teams, Cisco Webex ou les réunions Zoom. Pour collaborer à l'aide de la messagerie instantanée, utilisez la messagerie instantanée Barre latérale de l'application SIR.

Fonctionnalités principales

La Réponse aux incidents de sécurité collaboration d'appel offre les fonctionnalités clés suivantes :

- Les gestionnaires/analystes SIR peuvent lancer une téléconférence Microsoft Teams, Cisco Webex ou Zoom directement à partir de l'incident de sécurité.
- Les gestionnaires/analystes SIR peuvent lancer une conversation de messagerie instantanée directement à partir de l'application SIR.
- Invitez d'autres participants à l'appel ou à la messagerie instantanée.
- Afficher les enregistrements d'appels et les détails de la messagerie instantanée.
- Envoyez des invitations aux participants par e-mail et via la messagerie instantanée Microsoft Teams.

Gérer les utilisateurs et les groupes de téléconférence

L'administrateur peut configurer les paramètres de la téléconférence pour afficher une liste prédéfinie d'utilisateurs et de groupes à ajouter à un appel.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Espaces de travail** > **Espaces de travail de Réponse aux incidents de sécurité** > **Administration**.
2. Sélectionnez **Téléconférence**, puis **Configuration de l'appel**.
3. Sur la page Configuration de l'appel, sélectionnez **Configuration de téléconférence**.
   La page de configuration s'affiche pour configurer une liste prédéfinie d'utilisateurs et de groupes.
4. Renseignez les champs du formulaire Détails.

Champ	Description
Nom	Nom de la configuration de la téléconférence.
Remplir automatiquement les utilisateurs	Option permettant de renseigner automatiquement les utilisateurs configurés pour une téléconférence. La sélection de cette option ajoute les utilisateurs et les groupes configurés à une téléconférence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Vous pouvez également ajouter ou supprimer des utilisateurs/groupes lors du lancement d'un appel.
Afficher les utilisateurs affectés	Option permettant d'afficher les utilisateurs affectés pour les ajouter à un appel.
Afficher les utilisateurs du groupe d'affectation	Option permettant d'afficher les utilisateurs du groupe d'affectation à ajouter à un appel.
Groupes par défaut	Option permettant d'ajouter des groupes par défaut à un appel.
Utilisateurs par défaut	Option permettant d'ajouter des utilisateurs par défaut à un appel.

5. Sélectionnez **Enregistrer** pour enregistrer la configuration de la téléconférence.

Intégrer SIR à des canaux de communication tiers

L'intégration de la conférence téléphonique SIR à des canaux de communication tiers tels que Microsoft Teams, Zoom et Cisco Webex vous permet de gérer et d'initier un appel directement à partir d'un incident de sécurité.

Fonctionnalités principales

- Démarrez et terminez les téléconférences directement à partir de n'importe quel incident de sécurité.
- Ajoutez ou supprimez des participants à une téléconférence.
- Suivez et rapportez les détails de la réunion, tels que la durée de la réunion et les participants, pour une analyse plus approfondie.

Prérequis

Vérifiez que vous avez installé les modules d'extension Integration Hub suivants sur votre instance ServiceNow.

- Module d'extension Notification (com.snc.notify). Pour plus d'informations, voir Configurer Notification
- Composants de l'interface utilisateur de notification pour les espaces de travail configurables
- Pour intégrer Microsoft Teams en tant que canal de communication :
  - Module d'extension Spoke Microsoft Teams Communications (sn_msteams_com_spk).
  - Module d'extension Mappage de l'utilisateur Azure Active Directory (sn_now_azure).
- Pour intégrer Zoom comme canal de communication :
  - Spoke Zoom (sn_zoom_spoke)
  - Zoom Notification (sn_notify_zoom)
- Pour intégrer Cisco Webex en tant que canal de communication :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Connecteur Cisco Webex de Notification (sn_notify_webex)
- Spoke Cisco Webex Teams (sn_cisco_teams_spk)

Pour plus d'informations, consultez Demander le Centre d'intégration .

Configuration

Effectuez la configuration suivante pour les canaux de communication que vous souhaitez utiliser :

- Pour configurer l'intégration de Cisco Webex lors de la téléconférence à l'aide du canal de communication Notification, reportez-vous à la section Configurer Notification Cisco le connecteur Webex .
- Pour configurer l'intégration Zoom de la téléconférence à l'aide du canal de communication Notification, reportez-vous à la section Configurer le connecteur Zoom de Notification dans Notification .
- Pour configurer l'intégration de Microsoft Teams lors de la téléconférence à l'aide de l'application préconfigurée, reportez-vous à la rubrique Intégrer l'application prépubliée du connecteur Notification à Microsoft Teams .
- Pour configurer l'intégration de Microsoft Teams lors de la téléconférence à l'aide de l'application autoconfigurée, reportez-vous à la section Intégrationde l'application autoconfigurée du connecteur Notification avec Microsoft Teams .

Configurer des modèles de rapport dans Réponse aux incidents de sécurité

Vous pouvez créer des modèles de rapport qui peuvent être utilisés pour générer un résumé d'incident ou un résumé exécutif à des fins d'analyse et de partage.

Utilisez Réponse aux incidents de sécurité la fonctionnalité Modèles de rapport pour créer des modèles de rapport afin de générer des rapports fournissant un résumé au niveau analyste ou exécutif d'un incident. Vous pouvez formater et configurer le rapport en fonction de vos besoins à l'aide de différents champs d'incident.

Le tableau suivant explique les modèles de rapport qui sont mis en service dans le système de base.

Modèles de rapports dans Réponse aux incidents de sécurité

Nom	Description
Rapports sur le statut de l'analyste	Fournit des informations complètes sur un incident de sécurité pour un analyste.
Résumé du cadre	Fournit une vue d'ensemble de l'état d'un incident de sécurité pour la direction.

Remarque : Par défaut, ces rapports sont à l'état brouillon et en lecture seule. Vous devez réutiliser ces modèles par défaut pour créer et publier des modèles de rapport.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un modèle de rapport dans Réponse aux incidents de sécurité

Créez un nouveau modèle de rapport pour le résumé de l'analyste ou un résumé exécutif pour un incident.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Espaces de travail** > **Espaces de travail de Réponse aux incidents de sécurité** > **Administration**.
2. Sélectionnez **Rapports**, puis **Modèles de rapport**.
   La page Modèles de rapport s'affiche avec tous les modèles disponibles dans le système de base.
3. Sélectionnez **Nouveau**.
   Affiche la page **Détails** du modèle.
4. Saisissez le nom et la description du modèle.
5. Sélectionnez **Enregistrer**.
6. Sélectionnez **l'onglet Contenu** .
   Affiche la page de contenu du modèle avec un rapport vide.
7. Sélectionnez **Développer** et insérez les champs souhaités dans le corps du modèle.
   - **Champs SIR communs** : liste des champs les plus utilisés pour un incident.
   - **Tous les champs SIR** : tous les champs associés à un incident. Par exemple, lorsque vous générez un rapport d'incident et que vous souhaitez ajouter un champ appelé Description brève, vous pouvez sélectionner ce champ dans Tous les champs SIR. Le champ Brève description est ajouté en tant que variable dans le modèle de rapport. Lorsque vous générez un rapport pour l'analyste, la brève description de l'incident est affichée dans le rapport.
   - **Enregistrements connexes** : les enregistrements connexes d'un incident particulier. Par exemple, si vous souhaitez ajouter des observables associés dans le rapport, vous pouvez les ajouter à votre modèle de rapport. Ces enregistrements connexes sont affichés au format de table
   - **Scripts** : pour ajouter la date et l'heure du rapport, vous pouvez ajouter le script Date et heure actuelles à votre modèle de rapport. Cela ajoutera la date et l'heure de création du rapport dans le rapport.
   -
8. Sélectionnez **Enregistrer le contenu** pour enregistrer le contenu de votre modèle de rapport.
9. Sélectionnez **Aperçu** pour prévisualiser le format de votre rapport.

   Une fois que vous avez ajouté tous les champs obligatoires à votre modèle de rapport, vous devez publier votre modèle de rapport.
10. Sélectionnez **Publier** pour publier le modèle.

    Un message de confirmation s'affiche si vous souhaitez publier le modèle de rapport.
11. **Facultatif :** Sélectionnez l'icône **Actions supplémentaires** , puis sélectionnez **Supprimer** pour supprimer le modèle de rapport.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés système pour les rapports

Les propriétés système des Réponse aux incidents de sécurité rapports sont expliquées ci-dessous.

Propriétés système pour les rapports

Propriété	Description	Valeur
sn_si.sn_si_incident.load_all_records	Charge tous les enregistrements des listes du rapport créé à partir d'un modèle. vrai : charge tous les enregistrements et faux : charge un nombre spécifique d'enregistrements défini par la propriété sn_si.sn_si_incident.reporting_list_records_count.	Faux
sn_si.sn_si_incident.max_colonnes_liste_autorisé	Le nombre de colonnes pouvant être ajoutées lors du rendu des listes dans les pdf de rapport. Cela utilisera les colonnes depuis le début, de la vue jusqu'à la limite autorisée.	5
sn_si.sn_si_incident.report_default_style_object	Utilisez cette propriété pour contrôler le css des champs de formulaire libre, du panneau de gauche, des listes de rapports.	(objet JSON)
sn_si.sn_si_incident.reporting_list_records_count	Charge un nombre spécifique d'enregistrements dans l'éditeur de rapports.	200
sn_si_reporting_email_template_sn_si_incident	ID système du modèle de client de messagerie pour la table SIR (sn_si_incident) qui sera utilisé dans le rapport partagé.	9ce97ae643461210416896ed3ab8f258
sn_si.sn_si_incident.ctx_menu_field_header	En-tête de champ	sn_si_incident_report_field_header sn_si_incident_report_list_header
sn_si.sn_si_incident.defang_record_list_urls	Contrôlez si les URL de la liste sont neutralisées ou non.	Faux
sn_si.sn_si_incident.reporting_dot_walk_tables	Liste des tables disponibles pour la remontée pas à pas dans les rapports.	(objet JSON)

Dupliquer un modèle de rapport dans Réponse aux incidents de sécurité

Dupliquez un modèle de rapport pour le modifier ou réutilisez un modèle existant pour créer un nouveau modèle.

Avant de commencer

Remarque : Vous devez créer une copie des modèles Executive Summary et Analyst Status Reporting pour les réutiliser.

Pour réutiliser le résumé exécutif et le rapport d'état de l'analyste, vous devez en créer une copie, puis

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Espaces de travail** > **Espaces de travail de Réponse aux incidents de sécurité** > **Administration**.
2. Sélectionnez **Rapports**, puis **Modèles de rapport**.
   La page Modèles de rapport s'affiche avec tous les modèles disponibles dans le système de base.
3. Sélectionnez le modèle.
4. Sélectionnez **Dupliquer**.

Résultats

Les contenus du modèle sélectionné sont dupliqués et une copie du modèle sélectionné est disponible dans la liste des modèles. Le modèle en double est à l'état Brouillon. Vous pouvez personnaliser le contenu, puis renommer le modèle selon vos besoins.

Que faire ensuite

Modifier un modèle de rapport dans Réponse aux incidents de sécurité

Modifier un modèle de rapport dans Réponse aux incidents de sécurité

Modifiez un modèle de rapport pour réutiliser un modèle existant afin de créer un nouveau modèle.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Espaces de travail** > **Espaces de travail de Réponse aux incidents de sécurité** > **Administration**.
2. Sélectionnez **Rapports**, puis **Modèles de rapport**.
   La page Modèles de rapport s'affiche avec tous les modèles disponibles dans le système de base.
3. Sélectionnez le modèle.
   Affiche l'onglet **Détails** du modèle en mode d'édition.
4. Mettez à jour le nom et la description du modèle.
5. Sélectionnez **Enregistrer**.
6. Sélectionnez **l'onglet Contenu** .
   Affiche la page de contenu du modèle avec un rapport vide.
7. Sélectionnez **Développer** et insérer/supprimer les champs souhaités.
   - **Champs SIR communs** : liste des champs les plus utilisés pour un incident.
   - **Tous les champs SIR** : tous les champs associés à un incident. Par exemple, lorsque vous générez un rapport d'incident et que vous souhaitez ajouter un champ appelé Description brève, vous pouvez sélectionner ce champ dans Tous les champs SIR. Le champ Brève description est ajouté en tant que variable dans le modèle de rapport. Lorsque vous générez un rapport pour l'analyste, la brève description de l'incident est affichée dans le rapport.
   - **Enregistrements connexes** : les enregistrements connexes d'un incident particulier. Par exemple, si vous souhaitez ajouter des observables associés dans le rapport, vous

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pouvez les ajouter à votre modèle de rapport. Ces enregistrements connexes sont affichés au format de table

- **Scripts** : pour ajouter la date et l'heure du rapport, vous pouvez ajouter le script Date et heure actuelles à votre modèle de rapport. Cela ajoutera la date et l'heure de création du rapport dans le rapport.

8. Sélectionnez **Enregistrer le contenu** pour enregistrer le contenu de votre modèle de rapport.
9. Sélectionnez **Aperçu** pour prévisualiser le format de votre rapport.

   Une fois que vous avez ajouté tous les champs obligatoires à votre modèle de rapport, vous devez publier votre modèle de rapport.

10. Sélectionnez **Publier** pour publier le modèle.

    Un message de confirmation s'affiche si vous souhaitez publier le modèle de rapport.

Planification d'astreinte dans Réponse aux incidents de sécurité

Utilisez Planification d'astreinte dans afin d'afficher Réponse aux incidents de sécurité et de gérer les équipes de vos analystes.

Avec la fonctionnalité Planification d'astreinte, vous pouvez afficher et gérer les équipes, approuver ou rejeter des demandes d'absence. Vous pouvez également gérer les préférences de notification, les canaux de livraison, les règles de déclencheur d'escalade et les politiques de votre groupe.

Fonctionnalités principales de sn_si.manager/rota_manager

- Consulter la planification des astreintes, y compris les éventuels écarts et les demandes de congé de votre groupe.
- Approuver ou rejeter des demandes de congé.
- Passer en revue et gérer les écarts et les conflits.
- Fournir, remplacer ou supprimer une couverture et supprimer les demandes de congé.
- Créer une équipe et y ajouter ou en supprimer des membres.
- Afficher les rapports d'escalade, de groupe et de performances.

Fonctionnalités principales de sn_si.analyst/oc_read

- Consulter les calendriers de vos astreintes et voir les autres membres de votre équipe.
- Soumettre une demande de congé et désigner un autre membre du groupe pour vous remplacer.
- Préciser votre disponibilité et vos méthodes de contact préférées.
- Affichez les détails des membres et de l'escalade pour une équipe.

Documentation pour Planification d'astreinte

Pour plus d'informations sur la configuration et l'utilisation des fonctionnalités de Planification d'astreinte, consultez la Gestion des services IT Planification d'astreinte documentation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser Espace de travail SIR

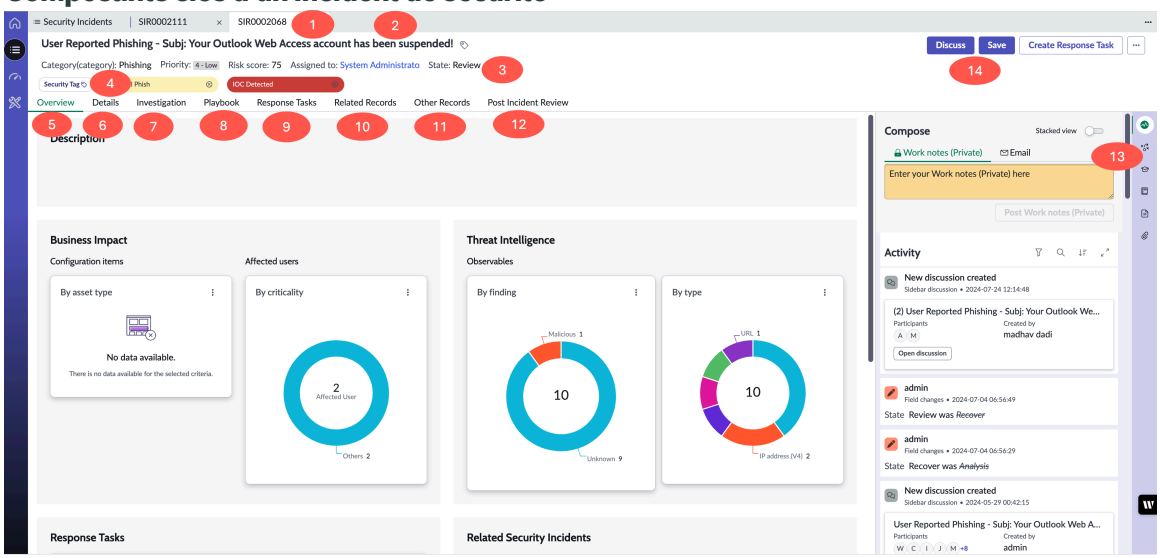
Les analystes et les gestionnaires de sécurité effectuent les Espace de travail SIR opérations quotidiennes avec une expérience utilisateur améliorée, effectuent des enquêtes complètes sur les incidents et obtiennent une vue d'ensemble.

Utilisation des enregistrements d'incidents de sécurité

L'enregistrement des incidents de sécurité comprend les éléments suivants.

Composants clés disponibles dans un enregistrement d'incident de sécurité :

Composants clés d'un incident de sécurité



Numéro	Nom	Description
1	Numéro de l'incident de sécurité	Le numéro de l'incident de sécurité est disponible en regard du nom de l'onglet.
2	Description brève	Brève description de l'incident de sécurité qui s'affiche au-dessus de la bannière du formulaire.
3	Bannière de formulaire	Il s'agit d'une section en lecture seule, qui contient les champs clés tels que la catégorie, la priorité, le score de risque, l'état et les détails d'affectation de l'incident. **Remarque :** Les balises de plate-forme régulières peuvent également être appliquées ici.
4	Balises de sécurité	Affiche les balises de sécurité associées à un incident de sécurité.
5	Vue d'ensemble	Fournit une vue d'ensemble instantanée de l'incident de sécurité, par exemple la description, l'impact sur l'entreprise, comprenant les détails des actifs par type, les utilisateurs affectés par criticité, les éléments de veille sur les menaces, comprenant les observables par résultat et par type, les tâches de réponse, les incidents de sécurité connexes, y compris les incidents de sécurité enfants et les incidents de sécurité similaires.
6	Détails	L'onglet Détails affiche le formulaire d'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro	Nom	Description
7	Examen	L’onglet Examiner affiche l’expérience d’enquête sur les incidents.
8	Playbook	Playbook est déclenché via Concepteur d’automatisation de processus (PAD). Si un processus est créé et si une condition de déclenchement est définie pour déclencher le playbook d’un incident de sécurité. Puis un playbook apparaît.
9	Tâches de réponse	Les tâches de réponse capturent toutes les tâches de réponse associées à un incident de sécurité.
10	Enregistrements connexes	L’onglet Enregistrements connexes comprend toutes les listes connexes de l’interface utilisateur classique sous cette section. Les listes connexes sont regroupées sous différentes sections telles que l’impact sur l’entreprise, les informations sur les menaces, etc. pour faciliter la navigation.
11	Autres enregistrements	L’onglet Autres enregistrements contient des enregistrements informatiques tels que les demandes de changement, les incidents et les e-mails, regroupés et affichés dans cette section.
12	Onglet Revue post-incident	Au fur et à mesure que l’incident de sécurité progresse vers l’état d’examen, l’onglet Revue post-incident s’affiche avec les évaluations et les rapports post-incident dans l’onglet.
13	Menu contextuel	Fournit un accès facile aux actions rapides et est disponible dans tous les onglets pour que l’analyste puisse y accéder à tout moment. Le menu contextuel permet de naviguer facilement vers les multiples ressources telles que : **1.** Flux d'activité **2.** Playbook **3.** Assistant analyste **4.** Runbook **5.** Modèles **6.** Pièces jointes
14	Actions d’interface utilisateur du formulaire	Les différentes actions d’interface utilisateur du formulaire d’incident de sécurité sont affichées en haut à droite du formulaire d’incident. Les actions d’interface utilisateur de formulaire disponibles sont : • Discuter • Enregistrer • Créer une tâche de réponse • Rédiger un e-mail • Ajouter un Playbook • Ouvrir les workflows associés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro	Nom	Description
		• Incident en Crète • Créer un problème • Créer une demande de changement • Créer une panne • Calculer la gravité • Lier à Incident de sécurité majeur • Proposer en tant que Incident de sécurité majeur • Promouvoir à Incident de sécurité majeur • Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison • Associer la technique MITRE ATT&CK • Basculer vers l'interface utilisateur classique • Ajouter au ticket de sécurité • Supprimer Pour plus d'informations, consultez Utiliser les actions d'interface utilisateur du formulaire.

Section Vue d'ensemble de l'incident de sécurité

La section Vue d'ensemble de l'espace de travail présente les informations clés associées à l'incident de sécurité.

Les graphiques en anneau sont activés. Lorsqu'un analyste sélectionne l'un des éléments de graphique, il vous dirige vers l'enregistrement respectif avec une vue de liste filtrée des éléments dans cet onglet correspondant. Par exemple, si **Observables malveillants** est sélectionné, vous accédez aux observables avec une vue de liste filtrée des observables malveillants dans l'onglet **Enregistrements connexes** .

La section Vue d'ensemble affiche les éléments suivants :

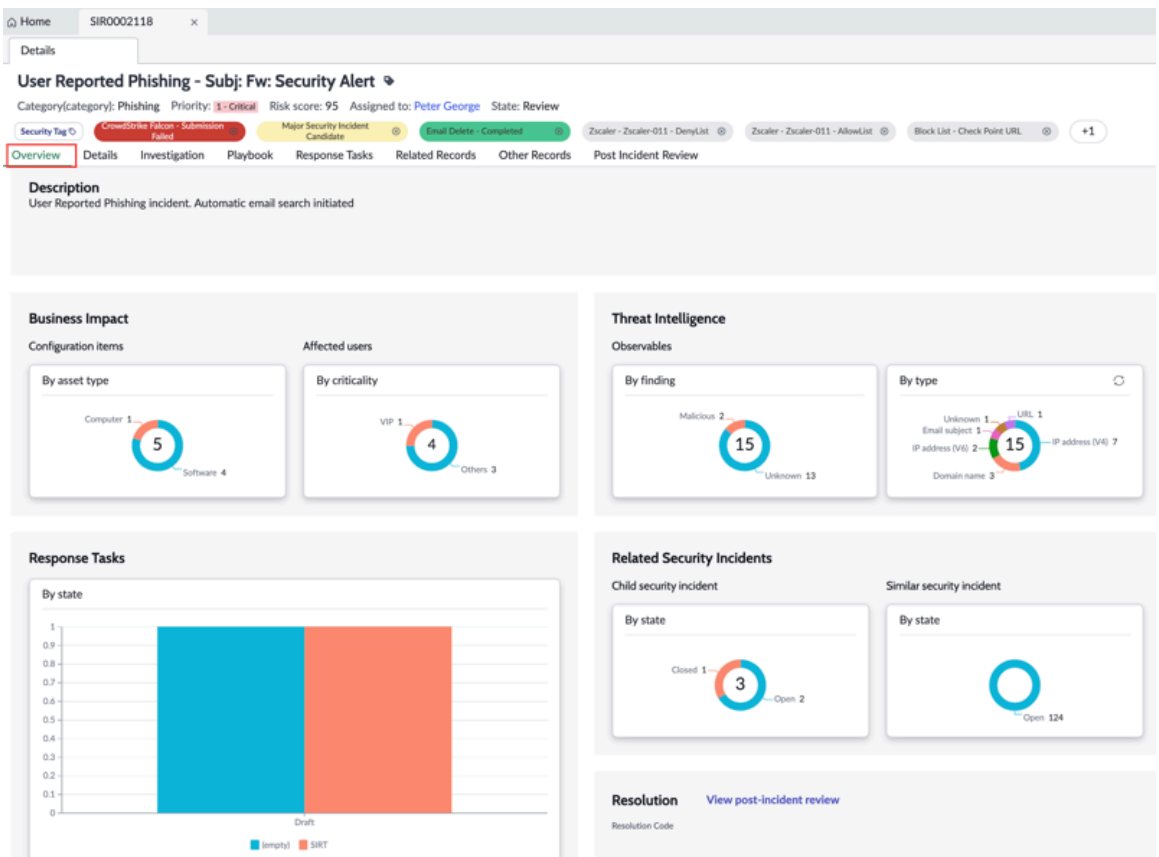
- Description de l'incident de sécurité.
- Détails de l'impact sur l'entreprise, tels que les éléments de configuration par type d'actif et les utilisateurs affectés par criticité, qu'il s'agisse d'utilisateurs VIP ou d'autres utilisateurs.
- Éléments de veille sur les menaces, tels que les observables, en déterminant s'ils sont malveillants ou inconnus, et par type.
- Tâches de réponse par état et groupe d'affectation.
- Les incidents de sécurité connexes comprenant les incidents de sécurité enfants par État - ouverts ou fermés, et les incidents de sécurité similaires par État - ouverts ou fermés.
- La section Résolution s'affiche lorsqu'un incident passe à l'état Réviser, puis la section Résolution s'affiche dans la section **Vue d'ensemble** avec la possibilité d'afficher la revue post-incident.
- Résolution : afficher la revue post-incident : sélectionnez le lien pour naviguer vers la page de **revue post-incident** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Une fois l'incident fermé, la section Résolution affiche le code de résolution, les notes de résolution et Résolu par (utilisateur), ainsi que les détails de la revue post-incident.
- Initiales de tous les utilisateurs qui accèdent actuellement au même incident.

Section Vue d'ensemble



Incident de sécurité Section Détails

Cette section affiche les champs du formulaire d'incident de sécurité restitués à partir de l'interface utilisateur classique de l'incident de sécurité.

Une vue appelée **vue SIRW** a été créée dans l'interface utilisateur classique. Cette vue est mappée à l'onglet **Détails** dans le nouvel espace de travail. Toutes les personnalisations requises doivent être implémentées dans cette vue.

Les champs de formulaire sont regroupés dans les sections suivantes et affichés dans la vue de formulaire de l'onglet Détails, cliquez sur l'une des sections ou passez à la section respective dans le formulaire :

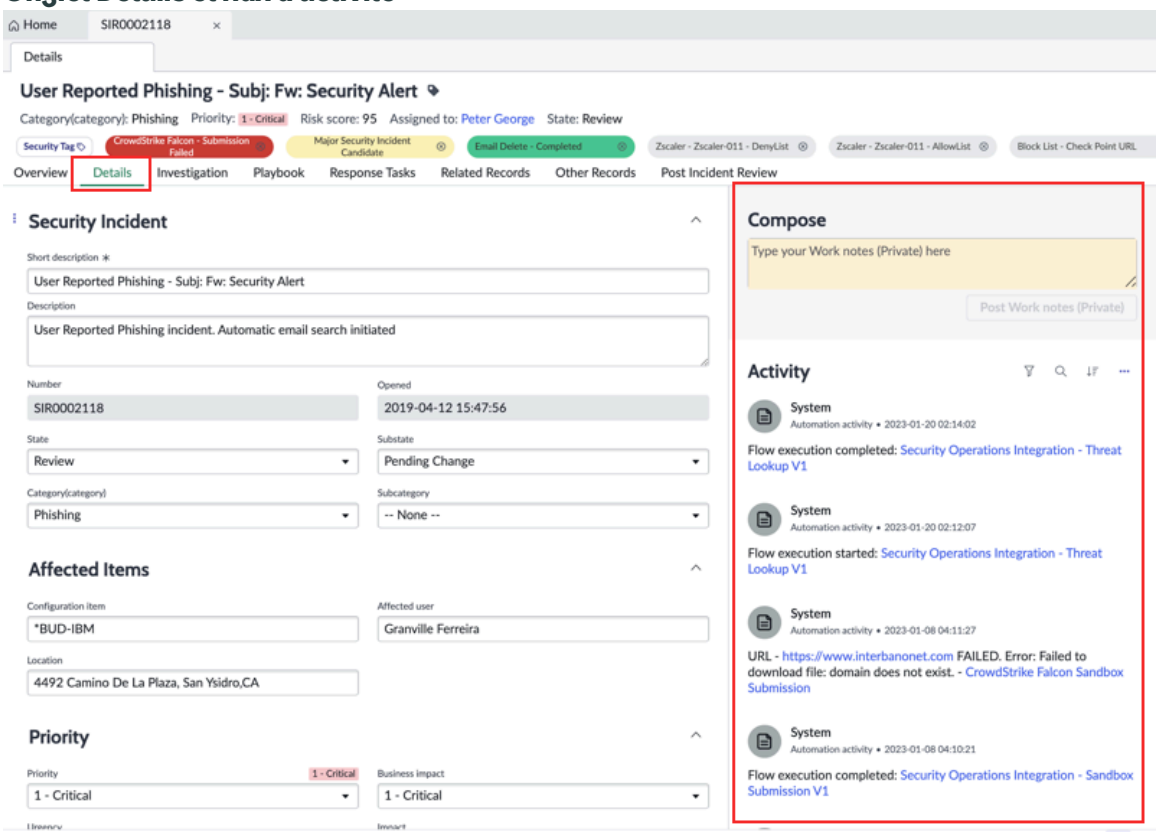
- Incident de sécurité
- Priorité
- Source
- Parent
- Affectation
- Contrôles des accès
- Éléments affectés
- Résolution

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'onglet **Détails** contient la section **Flux d'activité** dans le formulaire de détails lui-même pour un accès rapide aux analystes de sécurité qui peuvent ajouter des commentaires et les publier.

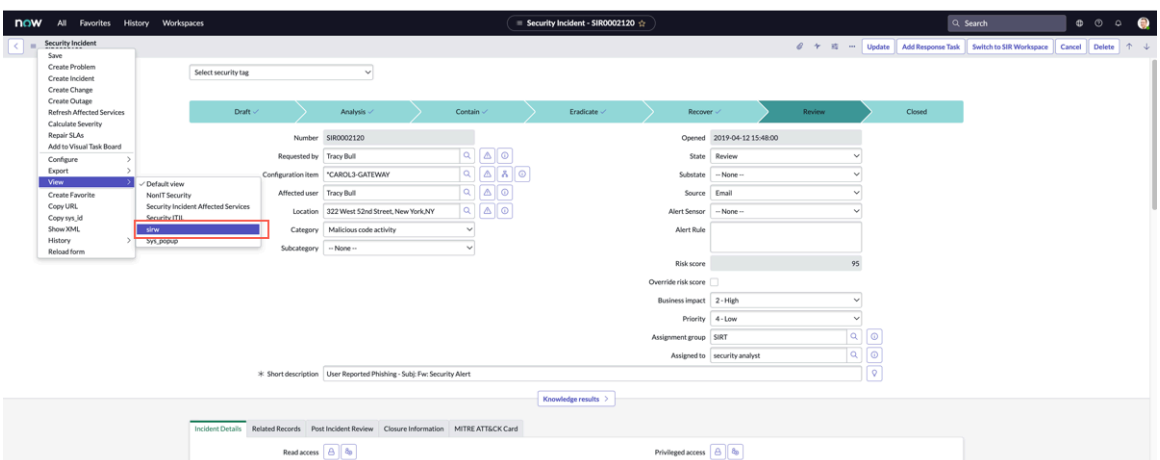
Onglet Détails et flux d'activité



Affichez la vue Espace de travail de l'analyste SIR :

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. Sélectionnez n'importe quel enregistrement d'incident de sécurité.
3. Cliquez sur le menu contextuel et sélectionnez **Vue** > **SIRW**.

> **Remarque :** Vous pouvez personnaliser à l'aide de la vue de l'espace de travail **sirw** dans le formulaire de l'interface utilisateur classique.

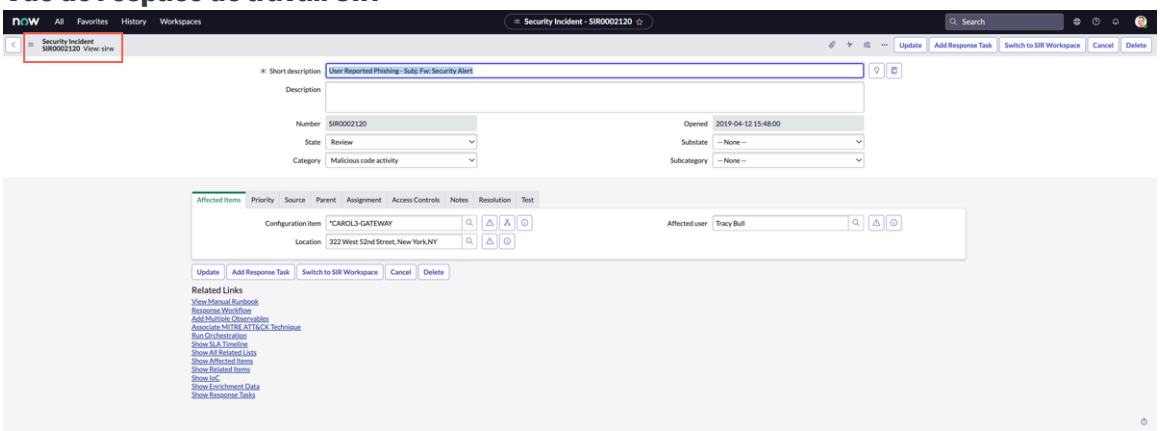


4. La vue de l'espace de travail de l'incident de sécurité s'affiche comme indiqué ci-dessous.

Traduction automatique

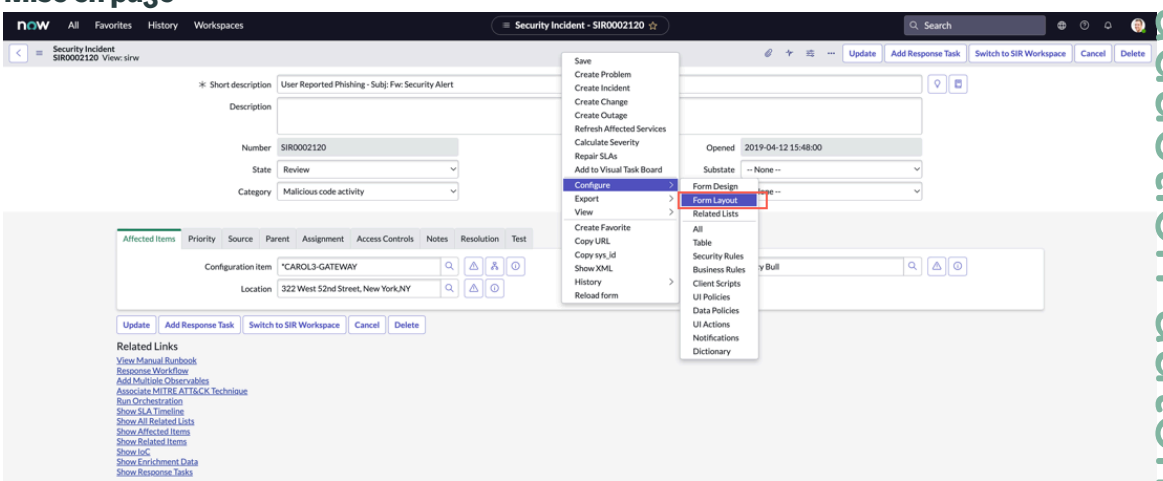
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue de l'espace de travail SIR



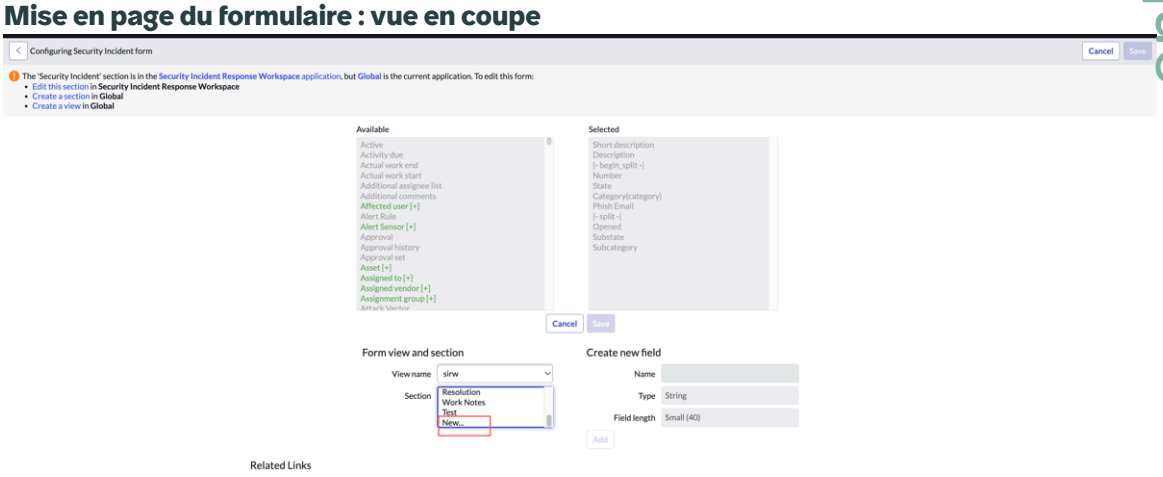
5. Sur l'enregistrement de l'incident de sécurité, cliquer avec le bouton droit et accéder à **Configurer** > **Mise en page**.

Mise en page



6. Explorez la vue et la **section Formulaire** , puis sélectionnez **Nouveau** dans la **section** pour créer une section.

Mise en page du formulaire : vue en coupe



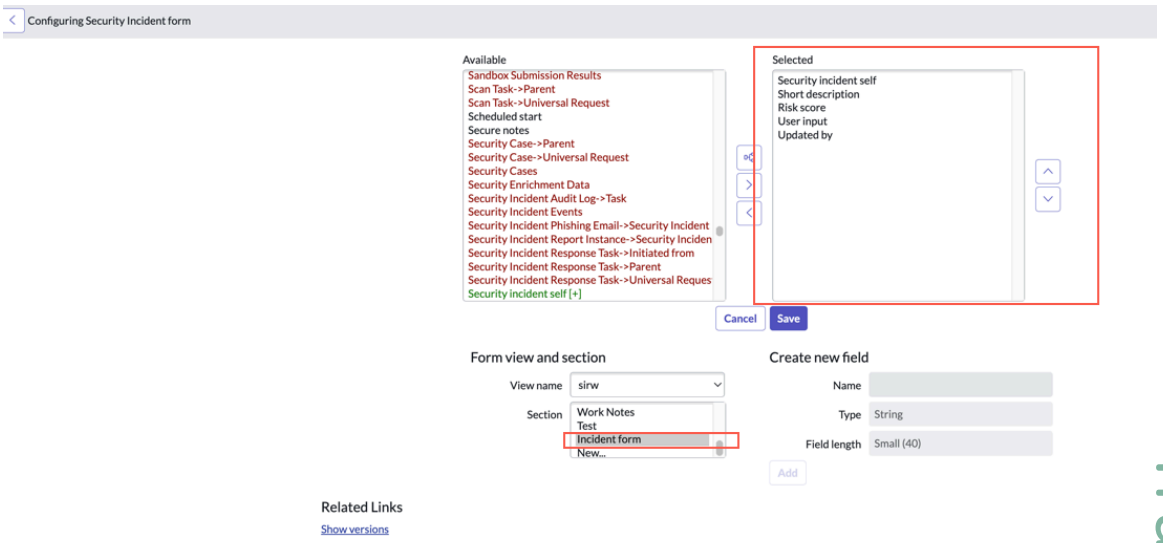
7. Indiquez le nom de la nouvelle section et cliquez sur **OK**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

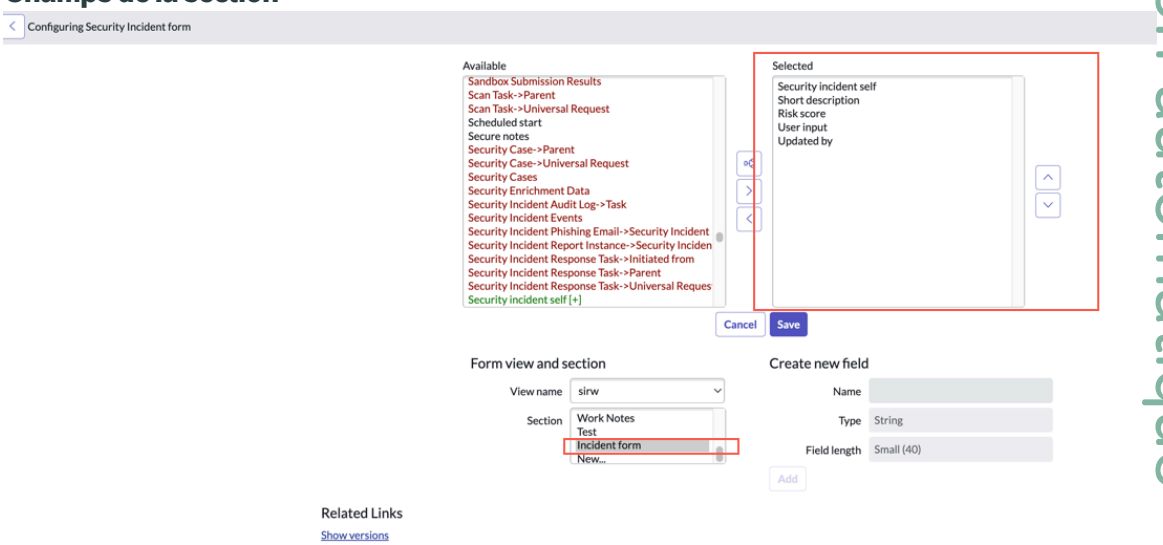
Par exemple, Formulaire d'incident.

8. La nouvelle section est créée et ajoutée à la **section**.



9. Sélectionnez votre nouvelle section et ajoutez les champs de section requis à la zone de sélection, puis cliquez sur **Enregistrer**.

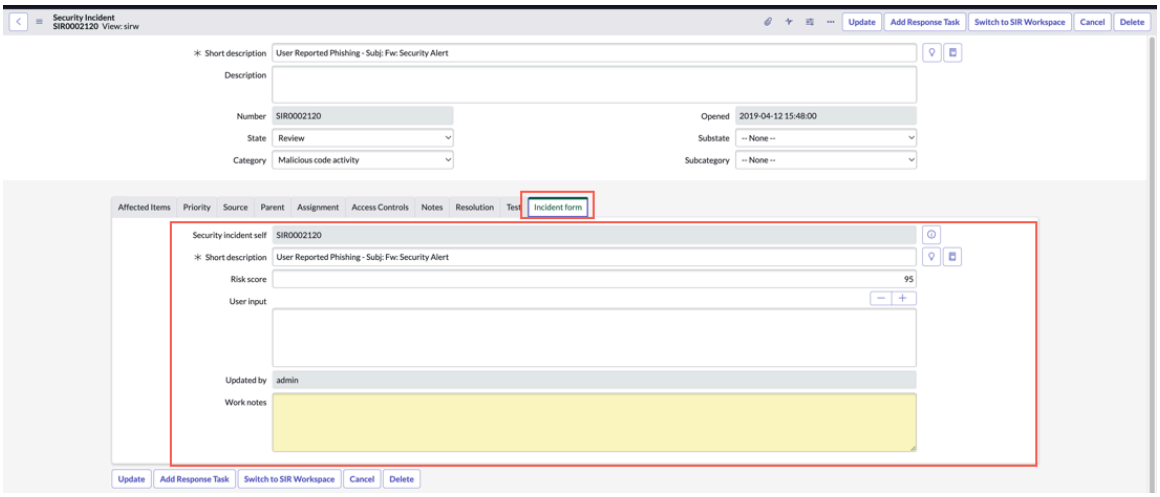
Champs de la section



10. La section nouvellement ajoutée s'affiche avec la disposition de section existante dans le formulaire d'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Cliquez maintenant sur **Basculer vers l'espace de travail SIR** pour accéder au formulaire d'incident de sécurité et à la section personnalisée dans l'onglet **Détails** de l'espace de travail.

Espace de travail SIR Orchestration

Espace de travail de la Réponse aux incidents de sécurité Les activités d'orchestration aideront les analystes de sécurité à visualiser le canevas d'examen et à effectuer diverses actions applicables.

Espace de travail SIR Canevas d'examen

Espace de travail de la Réponse aux incidents de sécurité permet aux analystes de la sécurité de consulter les informations clés associées à l'incident de sécurité pendant le processus de correction de l'incident. Les informations clés comprennent également les listes connexes telles que Observables, Résultats de la recherche de menaces, Recherche de perception, Enrichissement des observables, etc.

Dans l'interface utilisateur classique, la plupart des actions d'orchestration associées aux intégrations prêtes à l'emploi sont disponibles par rapport aux listes connexes. Par exemple, Exécuter une recherche de menace, Exécuter l'enrichissement de l'observable, etc. sont présents par rapport à la liste connexe Observables associés. De même, Obtenir les détails de l'hôte, Obtenir les statistiques réseau, etc., sont disponibles par rapport à la liste connexe Éléments de configuration.

Lorsqu'un analyste de sécurité effectue ces actions, les résultats sont renseignés dans une liste connexe différente. Par exemple, lorsqu'un utilisateur exécute Exécuter une recherche de menace, les résultats sont disponibles dans la table Résultats de la recherche de menace. Parfois, les résultats sont disponibles dans plusieurs tables différentes. Au cours de ce processus, les analystes de la sécurité ont une expérience utilisateur décousue et désorganisée en reliant les informations provenant de plusieurs endroits.

Dans la nouvelle Espace de travail SIR version réimaginée, le canevas **d'enquête** (onglet) fournit toutes les informations nécessaires regroupées logiquement en un seul endroit pour que l'analyste effectue l'enquête.

Explorer le canevas d'examen

L'objectif principal du canevas d'enquête est de présenter les données d'incident de sécurité nécessaires en un seul endroit commun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le Espace de travail SIR, l'enquête sur les incidents de sécurité s'articule principalement autour de quelques points d'entrée clés.

Voici quelques points d'entrée clés qui sont mis en service pour les analystes de sécurité dans le système de base :

- Observables associés
- Éléments de configuration
- Utilisateurs affectés
- E-mails associés Phish
- Recherche d'e-mail

Vous pouvez également configurer les points d'entrée ci-dessus en ajoutant, modifiant ou supprimant les points d'entrée, le cas échéant. Pour plus d'informations, consultez Configurer l'examen du temps de conception SI.

Dans l'onglet **Examen** , la table de points d'entrée fait office de table parente. Toutes les tables qui contiennent les résultats d'une action d'orchestration effectuée sur la table parente sont présentées comme tables enfants dans le point d'entrée.

Par exemple, pour le point d'entrée **Observables associés** , la table **Associer les observables** est la table parente, et les autres tables telles que Résultats de la recherche de menace, Résultats de soumission du bac à sable, etc. sont la table enfant.

L'analyste de la sécurité peut effectuer toutes les actions d'orchestration sur la table des observables associés et pourra afficher toutes les informations associées sur la même page, sans avoir besoin de naviguer dans plusieurs endroits.

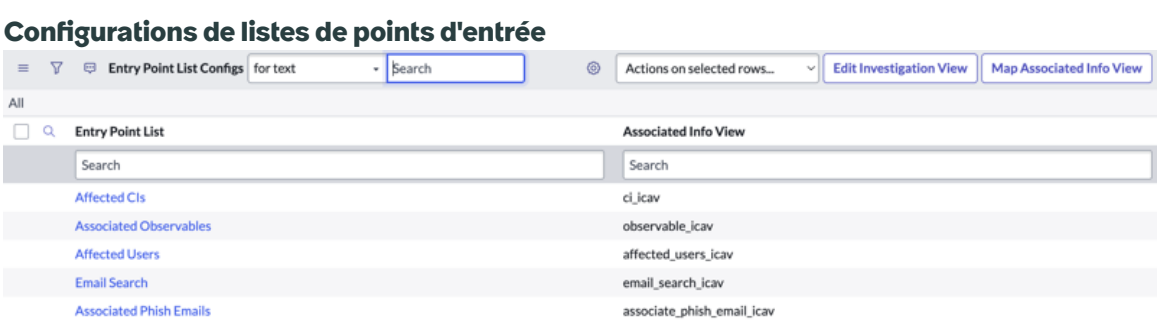
Remarque : Lorsqu'un utilisateur clique sur les graphiques interactifs de la page **Vue d'ensemble** , tels que les observables malveillants, il accède à la vue filtrée des observables malveillants dans le canevas d'examen. L'utilisateur peut également commencer directement l'enquête en accédant au canevas d'enquête qui contient toutes les données.

La liste des tables enfants sous un point d'entrée est également configurable. Pour plus d'informations, consultez Configurer l'examen du temps de conception SI.

Voici un exemple détaillé d'un point d'entrée (observable associé) configuré et mis en service dans le système de base :

1. Sélectionnez le point d'entrée **Observables associés** dans la liste déroulante.

   Ici, la table parente est également **un observable associé**.



2. Sélectionnez un ou plusieurs observables dans la table parente.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

3. Exécutez l'aptitude souhaitée.

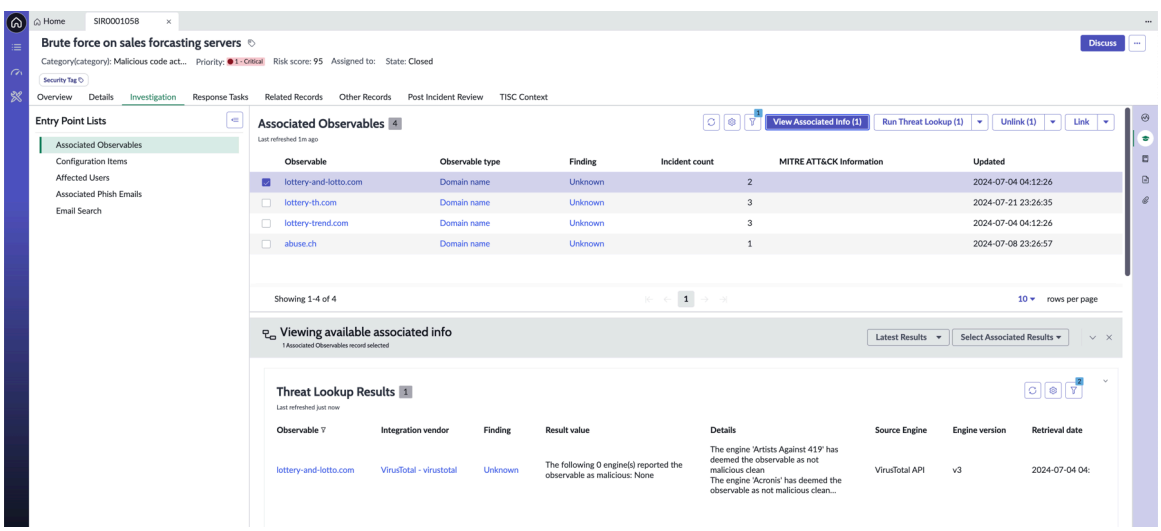
   Par exemple, sélectionnez **Exécuter une recherche de menace** pour extraire les résultats de la recherche de menace pour un observable sélectionné.

   Remarque : Lorsqu'une action observable correspondante est exécutée, le processus est exécuté dans le back-end et les résultats sont affichés sous la liste Observables.

4. Cliquez sur **Afficher les informations associées** pour afficher les résultats des observables. Les résultats sont affichés sur la même page.

   Remarque : Vous pouvez afficher les résultats à l'aide de filtres par résultats, sélectionner **Tous les résultats** ou **Derniers résultats**, selon la vue souhaitée. Par défaut, les derniers résultats s'affichent. S'il existe plusieurs implémentations (d'intégrations), les derniers résultats par implémentation s'affichent.

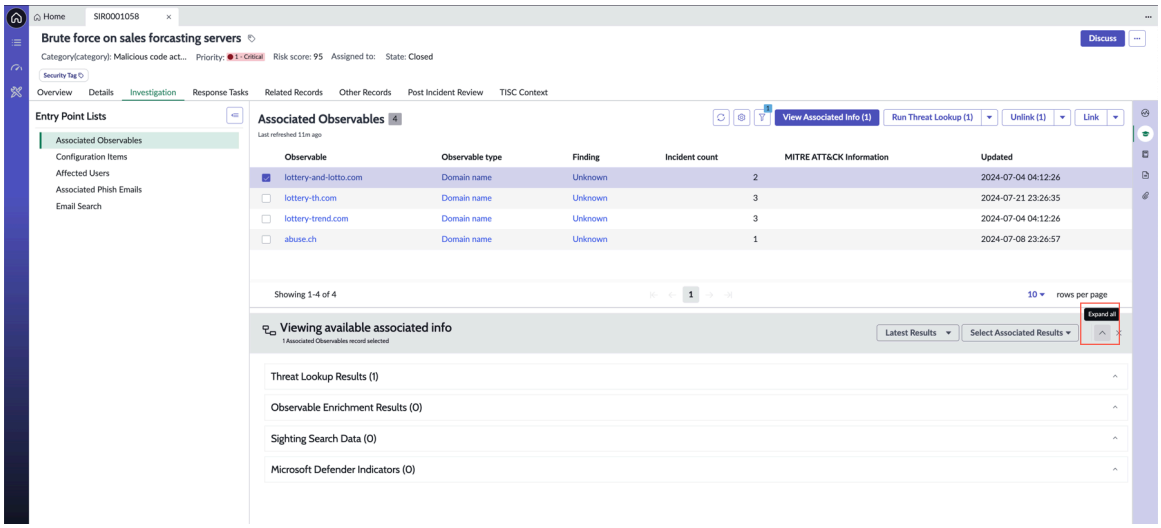
   En outre, vous pouvez filtrer les résultats **par listes connexes associées** qui sont les résultats de la table enfant. Par défaut, toutes les listes connexes de la table enfant configurée s'affichent. Pour plus d'informations, consultez Configurer l'examen du temps de conception SI. Toutefois, vous pouvez choisir de sélectionner uniquement les tables enfants requises.



5. En cliquant sur **Afficher les informations associées** , vous pouvez afficher toutes les données de la table enfant associée au même endroit. Cependant, vous pouvez fermer la vue des listes connexes en sélectionnant le bouton **Fermer la vue** . Une fois la vue fermée, vous ne pouvez voir que la table parente des observables comme précédemment.
6. Cliquez sur l'icône **Développer tout** vers le haut dans la table Affichage des résultats **d'informations associées disponibles** pour développer toutes les données de la table enfant des listes connexes.

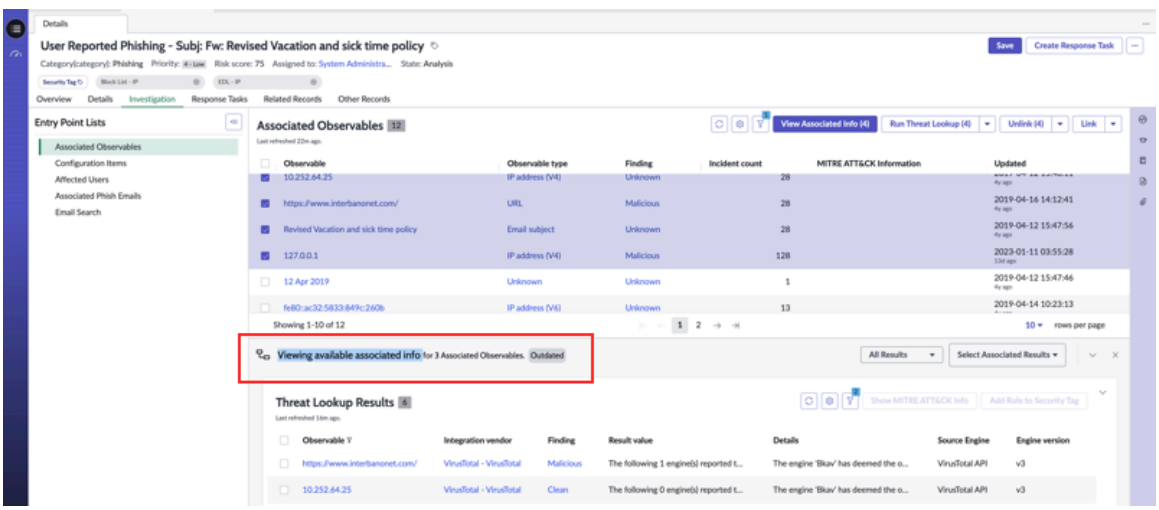
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Cliquez sur l'icône **Réduire tout** dans la direction descendante pour réduire toutes les données de table enfants des listes connexes.

Remarque : La bannière située en haut de la section des informations associées, qui contient toutes les données de la table enfant, indique le nombre d'informations connexes observables présentées à l'utilisateur. Par exemple, initialement, si vous sélectionnez deux observables et cliquez sur **Afficher les informations associées**, la bannière affiche : **Affichage des informations associées disponibles pour 2 observables associés**. Si vous sélectionnez par exemple un autre observable, la bannière indique que les informations sont obsolètes (capture d'écran ci-dessous). Vous devrez cliquer à nouveau sur **Afficher les informations associées** pour obtenir les données les plus récentes.



En plus de la vue complète des informations associées aux observables ci-dessus, cliquez sur l'observable et le formulaire d'enregistrement de la table parente s'ouvre dans un onglet différent avec une vue plus détaillée de l'enregistrement sélectionné. Toutes les données de table enfants associées de cet enregistrement sélectionné particulier sont également présentées dans la section **Informations associées** .

Toutefois, la section d'informations associée affiche uniquement les derniers résultats de la table enfants, tels qu'ils apparaissent dans le canevas d'examen, en mode lecture seule. Aucune action n'est possible dans cette vue. La page de formulaire de la table enfant peut être ouverte dans un nouvel onglet qui rendra la page entièrement fonctionnelle avec toutes les actions, le cas échéant.

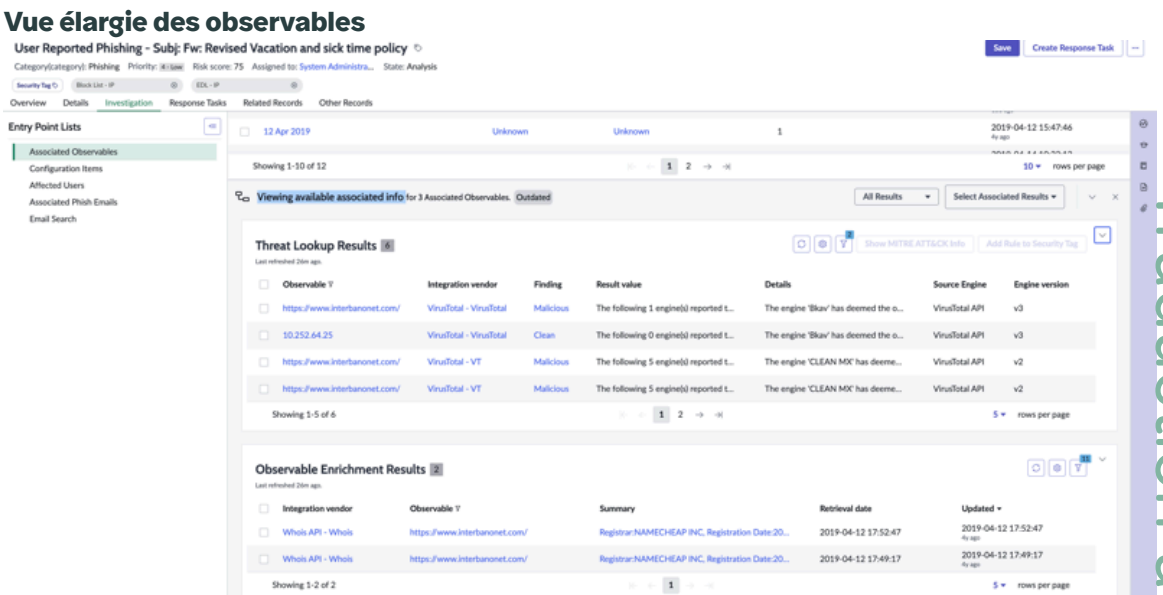
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez passer d'une table à l'autre à l'aide de la liste déroulante. Vous pouvez également développer ou réduire chaque formulaire dans la section des informations associée.

Dans la page **du formulaire Observable** (page du formulaire d'enregistrement de la table parente), vous pouvez effectuer certaines actions selon les disponibilités. Chaque fois que vous effectuez une action, vous pouvez cliquer sur Actualiser sur la bannière d'informations associée pour actualiser les données.

8. Cliquez sur **Développer tout** pour développer toutes les listes connexes de la table enfants. Par défaut, tous les enfants sont développés.



Information associée

Configurer l'examen du temps de conception SI

Cadre de travail d'expérience unifiée pour les intégrations optimisées par le cadre de travail d'aptitude

Dans l'interface utilisateur classique, l'expérience est décousue lors de l'exécution d'activités d'orchestration telles que l'exécution d'une recherche de menace, la recherche de perception, et ainsi de suite. Chaque option a sa propre expérience lors de son exécution. Le nouvel espace de travail offre une expérience unifiée pour toutes les options.

L'expérience unifiée ne s'applique qu'aux activités d'intégration et d'orchestration qui s'inscrivent dans le cadre de travail d'aptitude. Il peut y avoir des actions spécifiques à l'intégration, par exemple, Créer des indicateurs dans Microsoft Defender. Ces actions auront leur propre expérience en fonction des besoins du cas d'utilisation.

Le nouveau cadre consiste en des écrans modaux en trois étapes, comme expliqué ci-dessous.

1. **Implémentations** : la première étape consiste à sélectionner une ou plusieurs implémentations présentes par rapport à l'aptitude sélectionnée.

   Par exemple, lorsque l'analyste clique sur **Exécuter la recherche de menace**, il peut sélectionner une ou plusieurs implémentations présentes pour **l'aptitude Exécuter la recherche de menace**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chaque implémentation aura les détails de la source d'intégration. Reportez-vous au tableau ci-dessous. Des informations supplémentaires sont également présentées pour chaque implémentation.

Les informations supplémentaires peuvent inclure, par exemple, des informations sur les filtres, les types d'observables pris en charge, etc. Les informations supplémentaires peuvent être configurées comme vous le souhaitez. Pour plus d'informations, à la procédure de configuration technique du cadre de travail UX.

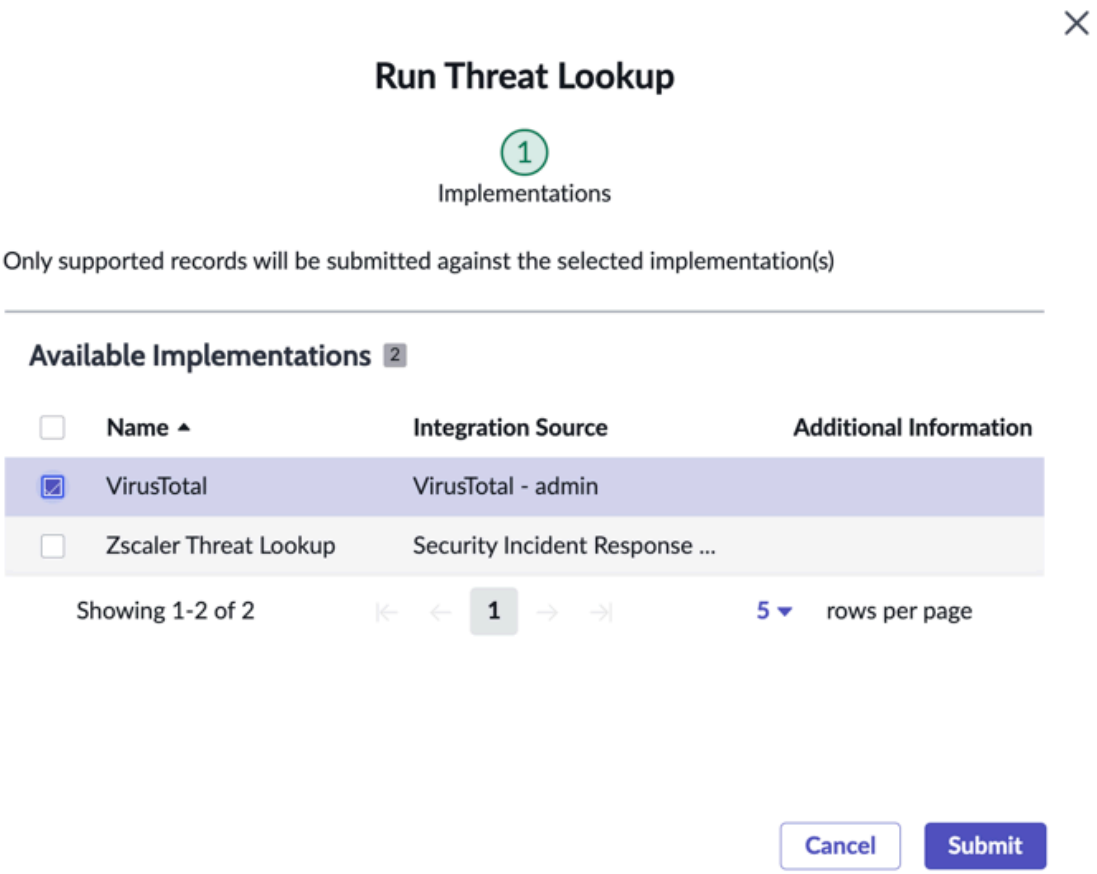
Modal du cadre de travail d'implémentation unifié

Implémentation	Description
Nom	Nom de l'implémentation.
Source d'intégration	La source de l'implémentation, telle que la configuration utilisée.
Information supplémentaire	Cette colonne capture les informations statiques, ce qui ajoute plus de contexte à l'analyste de sécurité par rapport à la ou aux implémentations sélectionnées pour procéder à une action. Par exemple, informations de prise en charge ou filtrées. En outre, si une implémentation ne prend en charge qu'un certain type d'observables tels que le domaine ou l'URL, vous pouvez ajouter ces informations supplémentaires ici dans cette colonne pour fournir le contexte à l'utilisateur. **Remarque :** Le cadre de travail de l'interface utilisateur permettrait essentiellement de sélectionner n'importe quel type d'implémentation et n'importe quel type d'observables. Lors de la soumission, les intégrations de système de base existantes qui sont expédiées prennent en charge le filtrage dans le back-end et soumettent uniquement le type d'observables pris en charge. Les autres enregistrements qui ne correspondent pas à la prise en charge seront ignorés. Par conséquent, un message d'information d'interface utilisateur s'affiche lorsque vous sélectionnez l'option : **Seuls les enregistrements pris en charge seront soumis sur la ou les implémentations sélectionnées.**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Écran 1 : Implémentation(s)

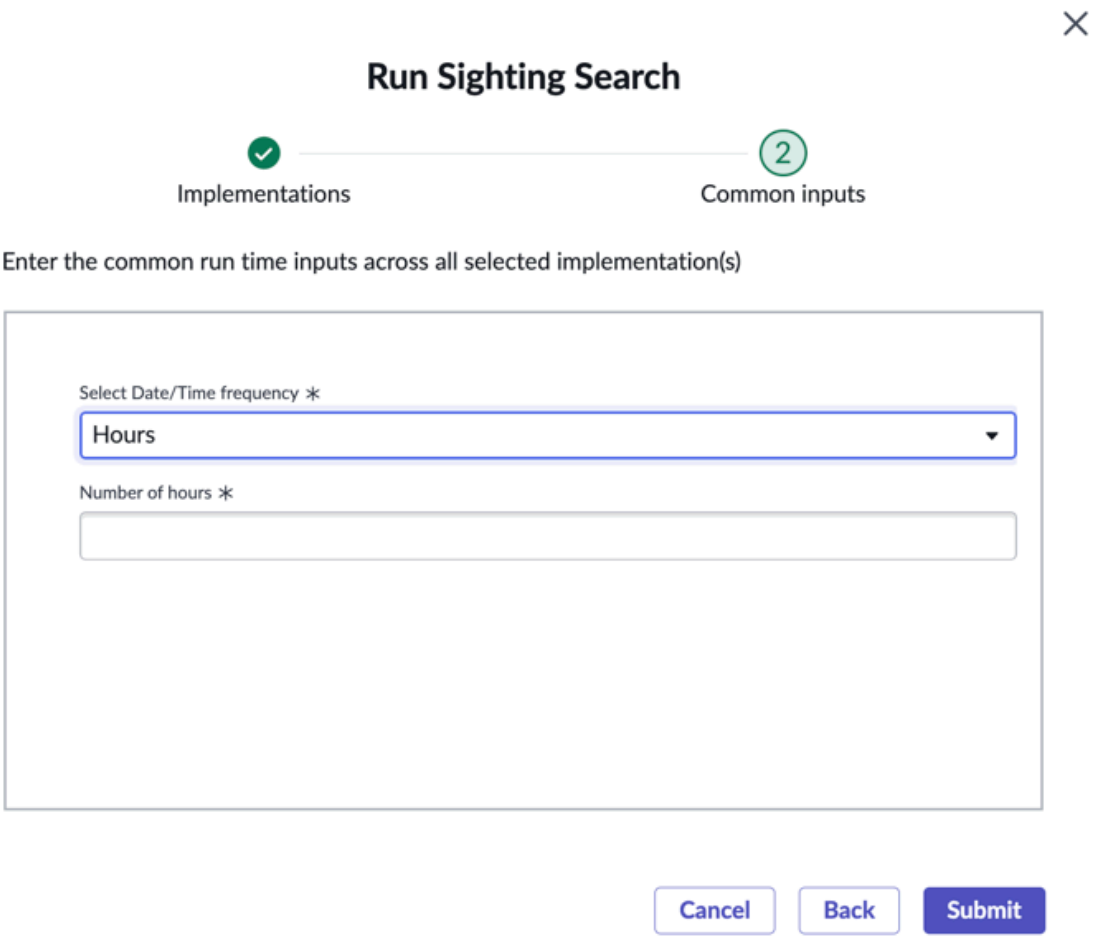


2. **Entrées communes** : ajoutez des entrées communes pour les implémentations sélectionnées ou pour toutes les implémentations applicables sélectionnées. Il s'agit de l'écran 2 de votre implémentation. Par exemple, pour l'instant, seule **la recherche de perceptions** dispose de l'écran d'entrées commun. Cette implémentation est une combinaison de l'écran 1 (Implémentations) et de l'écran 2 (Entrées communes).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Écran 1 + Écran 2



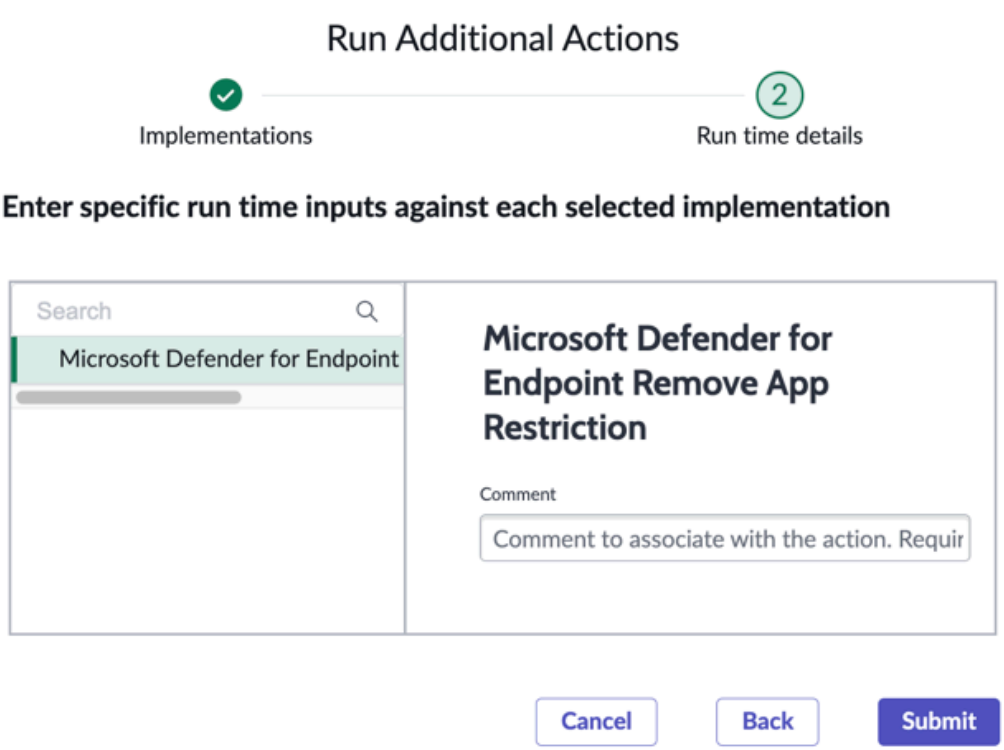
3. **Détails de la durée d'exécution** : ajoutez des entrées de durée d'exécution spécifiques pour les implémentations sélectionnées qui sont différentes les unes des autres. Il s'agit

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de l'écran 3 de votre implémentation. Cette implémentation est une combinaison de l'écran 1 (Implémentations) et de l'écran 3 (Entrées de temps d'exécution spécifiques).

Entrées spécifiques



Remarque : Les trois étapes ne sont pas toujours nécessaires. Selon l'aptitude et le type d'entrées requises, l'étape des détails de l'exécution et l'étape des entrées communes seront visibles.

Options d'expérience unifiées et écrans modaux

Le tableau ci-dessous décrit les capacités et les écrans applicables.

Table des options et des écrans applicables

Option	Écrans de cadres de travail UX applicables	Intégrations prises en charge
Exécuter une recherche de menace	Seul l'écran 1 – Sélectionner des implémentations est applicable. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour l'exécution de la recherche de menace. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste	• Virus Total • Hybrid Analysis • Intégration de Réponse aux incidents de sécurité avec Zscaler • Phistank • Métadéfenseur • Menace • Ai-je été mis en gage ? • Crowd Strike Falcon Intelligence

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des options et des écrans applicables (suite)

Option	Écrans de cadres de travail UX applicables	Intégrations prises en charge
	de la sécurité sera en mesure de soumettre l'action.	
Exécuter l'enrichissement de l'élément observable	Seul l'écran 1 – Sélectionner des implémentations est applicable Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Exécuter l'enrichissement de l'élément observable. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité sera en mesure de soumettre l'action.	• MISP • Point de terminaison Microsoft Defender • Shodan • RiskIQ (en anglais seulement) • WHOIS (en anglais seulement) • WHOIS inversé
Exécuter la recherche de perception/Exécuter la recherche de perception en ligne/Exécuter la recherche de perception des e-mails	Écran 1 – **Sélectionner Implémentations** et Écran 2 – **Entrées communes** sont applicables. La recherche de perception utilise la date et la fréquence comme entrées communes dans plusieurs implémentations de Splunk et d'autres intégrations. Cet écran sera présenté à l'analyste de la sécurité pour capturer les fréquences de date et d'heure. Pour les intégrations qui ne nécessitent pas ces entrées, par exemple FireEye HX, elles seront ignorées. Après avoir sélectionné une ou plusieurs implémentations et fourni des entrées communes, l'analyste de la	• Enrichissement d'incident Splunk • Carbon Black • Recherche élastique • FireEye HX • McaFee ESM • MSFT Defender pour point de terminaison • Perception Splunk • Recherche de perception Qradar • MISP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des options et des écrans applicables (suite)

Option	Écrans de cadres de travail UX applicables	Intégrations prises en charge
	sécurité sera en mesure de soumettre l'action.	
Soumettre à Sandbox (bac à sable)	Écran 1 – Sélectionner Implémentations et Écran 3 – Entrées spécifiques à l'implémentation sont applicables. L'envoi au bac à sable prend différentes entrées pour différentes implémentations. Il n'existe actuellement aucune entrée commune pour cette option. Par exemple, lorsque l'analyste sélectionne Crowdstrike Falcon X Quick Scan, Crowdstrike Falcon X Windows 64, Crowdstrike Falcon X Linux et Zscaler, les entrées varient. L'analyse rapide de Crowdstrike Falcon X et Zscaler n'ont pas besoin d'autres entrées de temps d'exécution. Crowdstrike Falcon X Windows 64 accepte des entrées d'exécution facultatives qui diffèrent de Crowdstrike Falcon X Linux. Ainsi, ceux-ci peuvent être fournis dans l'écran 3 spécifiquement pour les implémentations sélectionnées individuellement, le cas échéant.	• Intégration de CrowdStrike Falcon X Sandbox • Intégration de Réponse aux incidents de sécurité avec Zscaler
Publier dans la liste de surveillance	Seul l'écran 1 – Sélectionner des implémentations est applicable. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour **la publication dans la liste de surveillance**. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour	Hôte Crowdstrike Falcon

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des options et des écrans applicables (suite)

Option	Écrans de cadres de travail UX applicables	Intégrations prises en charge
	sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité sera en mesure de soumettre l'action.	
Demande d'autorisation/de blocage	Seul l'écran 1 – Sélectionner des implémentations est applicable. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour **la demande d'autorisation/de blocage**. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité sera en mesure de soumettre l'action.	• Réseau Palo Alto NGFW • Check Point NGFW • Intégration de Réponse aux incidents de sécurité avec Zscaler
Obtenir les détails de l'hôte	Seul l'écran 1 – Sélectionner des implémentations est applicable. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour obtenir les détails de l'hôte. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité sera en mesure de soumettre l'action.	• FireEye HX • Microsoft Defender pour point de terminaison
Obtenir un fichier	Écran 1 – Sélectionner Implémentations et Écran	FireEye HX

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des options et des écrans applicables (suite)

Option	Écrans de cadres de travail UX applicables	Intégrations prises en charge
	2 – Entrées communes sont applicables. Obtenir un fichier prend le nom du fichier et le chemin d'accès comme entrées courantes. Après avoir sélectionné une ou plusieurs implémentations et fourni des entrées communes, l'analyste de la sécurité sera en mesure de soumettre l'action.	
Obtenir les statistiques réseau	Seul l'écran 1 – Sélectionner des implémentations est applicable. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Obtenir les statistiques réseau. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité sera en mesure de soumettre l'action.	• FireEye HX • NetStat
Obtenir les processus en cours d'exécution	Seul l'écran 1 – Sélectionner des implémentations est applicable. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Obtenir l'exécution des processus. Ainsi, seul l'écran 1 est présenté à l'analyste de la sécurité pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste de la sécurité sera en	• FireEye HX • Carbon Black • Commande système

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des options et des écrans applicables (suite)

Option	Écrans de cadres de travail UX applicables	Intégrations prises en charge
	mesure de soumettre l'action.	
Obtenir les services d'exécution	Seul l'écran 1 – Sélectionner des implémentations est applicable. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Obtenir l'exécution des services. Ainsi, seul l'écran 1 est présenté à l'analyste pour sélectionner une ou plusieurs implémentations. Après avoir sélectionné les implémentations, l'analyste pourra soumettre l'action.	FireEye HX
Isoler l'hôte / Annuler l'isolement de l'hôte	Écran 1 – Sélectionner Implémentations et Écran 3 – Entrées spécifiques à l'implémentation sont applicables. Isoler l'hôte/Annuler l'isolement de l'hôte utilise différentes entrées pour différentes implémentations. Il n'existe actuellement aucune entrée commune pour cette option. Par exemple, lorsque l'analyste sélectionne FireEye HX et Microsoft Defender pour point de terminaison, les entrées varient. FireEye HX n'a pas besoin d'entrées de temps d'exécution. D'autre part, Microsoft Defender prend des entrées telles que le type d'isolement et les commentaires. Ainsi, ceux-ci peuvent être fournis dans l'écran 3 spécifiquement pour les implémentations sélectionnées	• FireEye HX • Point de terminaison Microsoft Defender • Carbon Black

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des options et des écrans applicables (suite)

Option	Écrans de cadres de travail UX applicables	Intégrations prises en charge
	individuellement, le cas échéant.	
Exécuter des actions supplémentaires	Écran 1 – Sélectionner Implémentations et Écran 3 – Entrées spécifiques à l'implémentation sont applicables. Exécuter des actions supplémentaires L'hôte utilise différentes entrées pour différentes implémentations. Il n'existe actuellement aucune entrée commune pour cette option. Par exemple, lorsque l'analyste sélectionne le script de détails d'enquête standard FireEye HX, l'acquisition de triage FireEye HX et le déchargement d'enregistrement de Crowdstrike Falcon Insight, les entrées varient. Le script de détails d'enquête standard FireEye HX et l'acquisition de triage FireEye HX prennent en compte les commentaires comme entrée qui peuvent être différents pour les deux. Le déchargement d'enregistrement de Crowdstrike Falcon Insight prend Subkey comme entrée. Ainsi, ceux-ci peuvent être fournis dans l'écran 3 spécifiquement pour les implémentations sélectionnées individuellement, le cas échéant.	• FireEye HX • Microsoft Defender pour point de terminaison • Aperçu de Crowdstrike Falcon

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table des options et des écrans applicables (suite)

Option	Écrans de cadres de travail UX applicables	Intégrations prises en charge
	Remarque : Ne prend actuellement en charge qu'une seule sélection d'implémentation. Dans les versions futures, la sélection multiple d'implémentation sera prise en charge.	

Exemples d'expérience unifiée

Cet exemple illustre les options du cadre de travail de l'expérience unifiée.

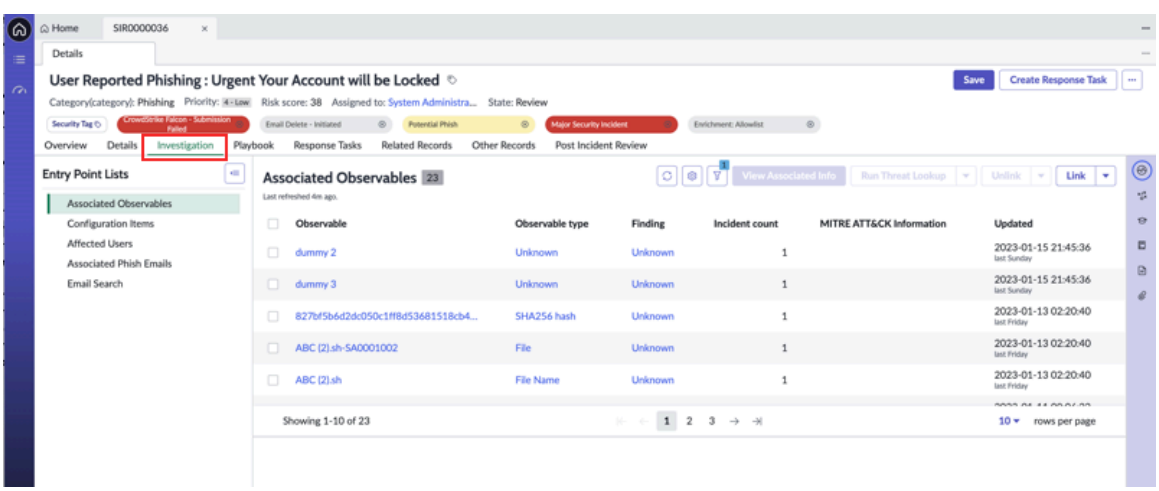
Exemple 1 : Sélectionner des implémentations : Recherche de menace

L'exemple ci-dessous illustre la ou les implémentations.

Exemple 1 : Écran uniquement 1 : Recherche de menace

Vous pouvez exécuter **l'action Exécuter les options d'intégration** connexes à la recherche de menace à l'aide de l'onglet **Examiner** du Espace de travail SIR.

1. Dans l'onglet **Examiner** , accédez à la section **Listes de points d'entrée** affichée sur le côté gauche de la page.
2. Sélectionnez n'importe quel point d'entrée et exécutez l'action d'aptitude d'intégration.



Remarque : Vous pouvez également accéder à l'onglet **Enregistrements connexes** dans l'espace de travail pour effectuer l'action des options d'intégration.

La recherche de menace est l'un des exemples qui est décrit en détail sur la façon d'effectuer les intégrations.

Sélectionner des implémentations

Sélectionnez une ou plusieurs implémentations le cas échéant.

Avant de commencer
Rôle requis : sn_si.analyst

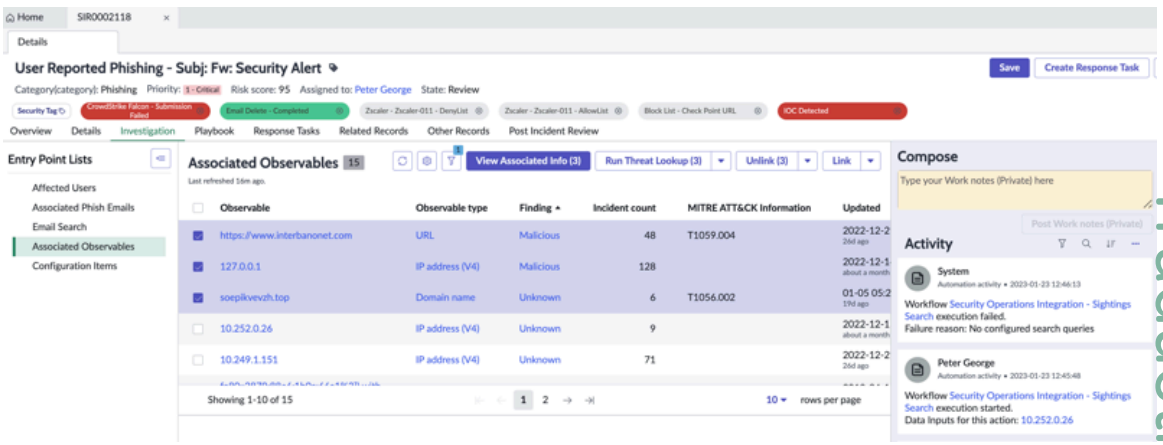
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les implémentations disponibles sont répertoriées. Sélectionnez la ou les implémentations. Une fois que vous les avez sélectionnées, seuls les enregistrements pris en charge sont soumis sur chaque implémentation sélectionnée.

Procédure

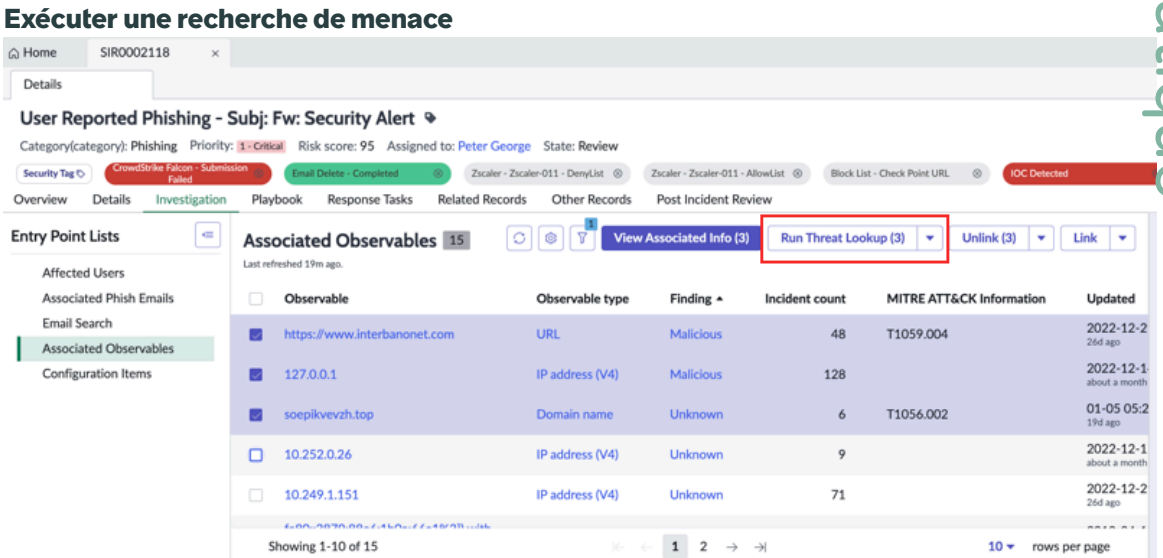
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Accédez à l'onglet **Examiner** de l'espace de travail.
   L'onglet Examiner avec les listes de points d'entrée s'affiche.



4. Sélectionnez l'observable associé dans les listes de points d'entrée.
   Par exemple, sélectionnez **Observables associés** liste connexe. Les enregistrements observables correspondants s'affichent.

> **Remarque :** Vous pouvez sélectionner une implémentation pour effectuer une recherche sur les observables sélectionnés, ou vous pouvez effectuer la recherche en sélectionnant toutes les implémentations.

Exécuter une recherche de menace



5. Cochez la case de n'importe quel observable pour lequel vous souhaitez effectuer la recherche de menace.
6. Accédez à la liste déroulante des actions des listes connexes qui s'affiche en haut de la page des listes connexes.

Traduction automatique

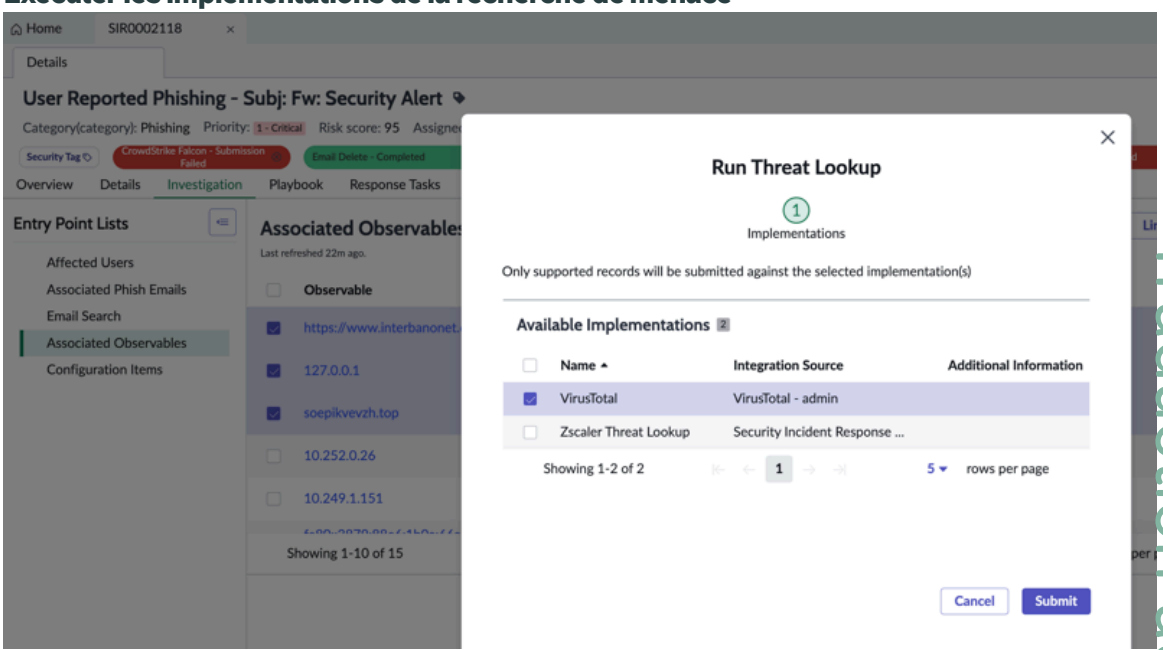
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Sélectionnez Exécuter la recherche de menace pour effectuer une action des options **d'intégration** liées aux informations sur les menaces.

   Remarque : L'aptitude Exécuter des recherches de menaces effectue des recherches de renseignements sur les menaces pour déterminer si un ou plusieurs observables sont associés à des menaces de sécurité connues.

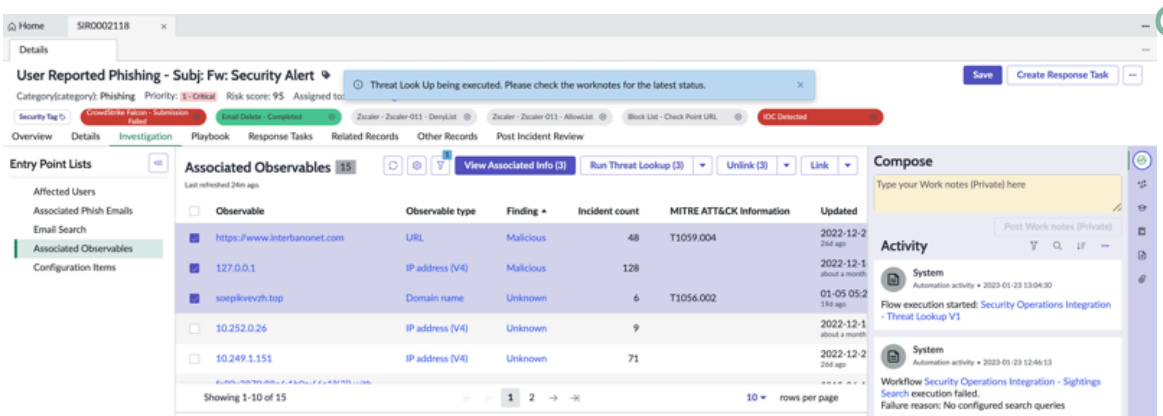
   L'écran modal Exécuter les implémentations de la recherche de menace s'affiche.

   Exécuter les implémentations de la recherche de menace



8. Sélectionnez une ou plusieurs implémentations dans la liste.

9. Cliquez sur **Envoyer**.
   Une fois les enregistrements sélectionnés envoyés, un message s'affiche indiquant que la recherche est en cours d'exécution. Une fois l'implémentation traitée dans le back-end, les résultats sont affichés dans la section de liste connexe Résultats **de la recherche de menace** . En outre, l'activité d'implémentation respective est affichée dans la section **Activité** . Deux activités s'affichent, l'une lorsque l'exécution de l'implémentation est commencée et l'autre lorsque l'exécution est terminée.



   Remarque : Les listes connexes **de Renseignements sur les menaces** , telles que les listes connexes Observables associés, sont affichées dans la section **Résultats de la recherche de menace** , et les listes connexes **Recherche de perceptions** sont affichées dans la section **Résultats de recherche de perceptions** sous Enregistrements connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple 2 : Entrées courantes : Recherche de perception

L'exemple ci-dessous illustre l'action d'aptitude d'entrées courantes.

Vous pouvez exécuter l'action **Exécuter les options d'intégration liées à la recherche de perception** à l'aide de l'onglet **Examiner** du .Espace de travail SIR

1. Dans l'onglet **Examiner** , accédez à la section **Listes de points d'entrée** affichée sur le côté gauche de la page.
2. Sélectionnez le point d'entrée respectif et exécutez l'action d'aptitude d'intégration.

> **Remarque :** Vous pouvez également accéder à l'onglet **Enregistrements connexes** dans l'espace de travail pour effectuer l'action des options d'intégration.

Ajouter des entrées communes à une implémentation

Ajoutez des entrées de temps d'exécution communes qui s'appliquent à toutes les implémentations sélectionnées, le cas échéant.

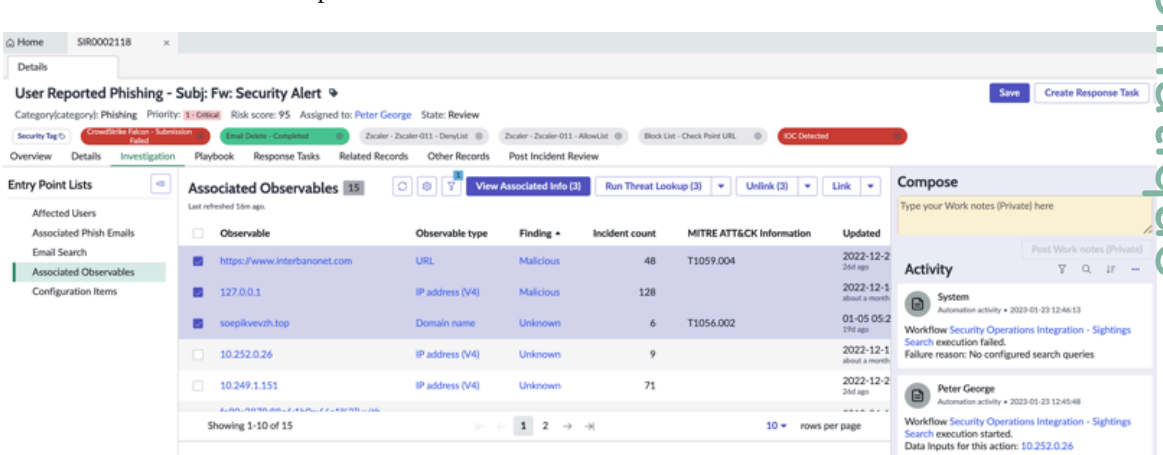
Avant de commencer

Rôle requis : sn_si.analyst

Les implémentations disponibles sont répertoriées. Sélectionnez la ou les implémentations. Une fois que vous les avez sélectionnées, seuls les enregistrements pris en charge sont soumis sur chaque implémentation sélectionnée.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Accédez à l'onglet **Examiner** de l'espace de travail.
   L'onglet Examiner avec les listes de points d'entrée s'affiche.



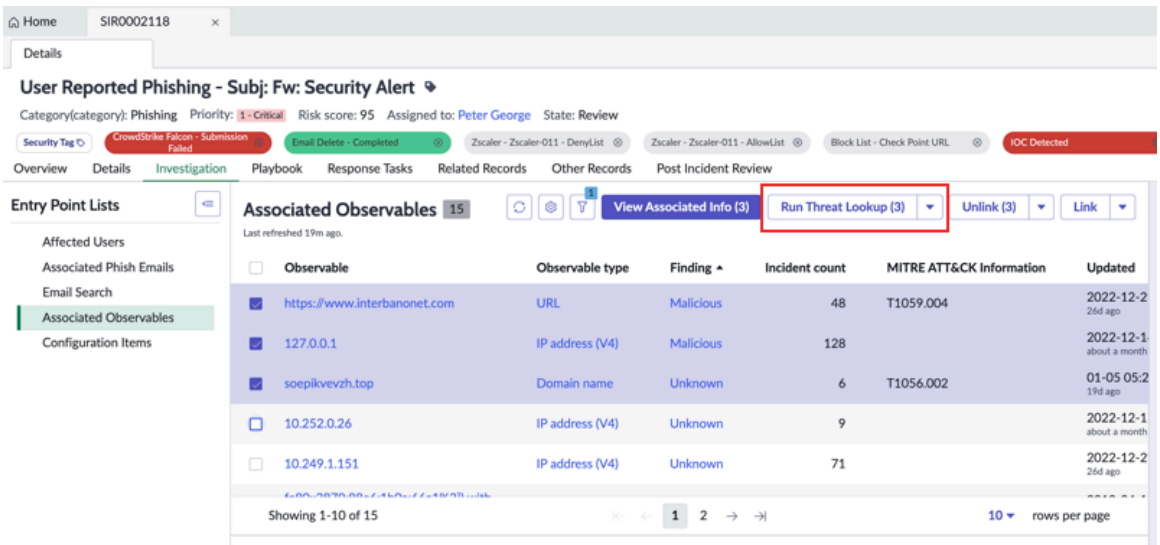
4. Sélectionnez l'observable associé dans les listes de points d'entrée.
   Par exemple, sélectionnez **Observables associés** liste connexe. Les enregistrements observables correspondants s'affichent.

> **Remarque :** Vous pouvez sélectionner une implémentation pour effectuer une recherche de perception pour les observables sélectionnés, ou en sélectionnant plusieurs implémentations.

Traduction automatique

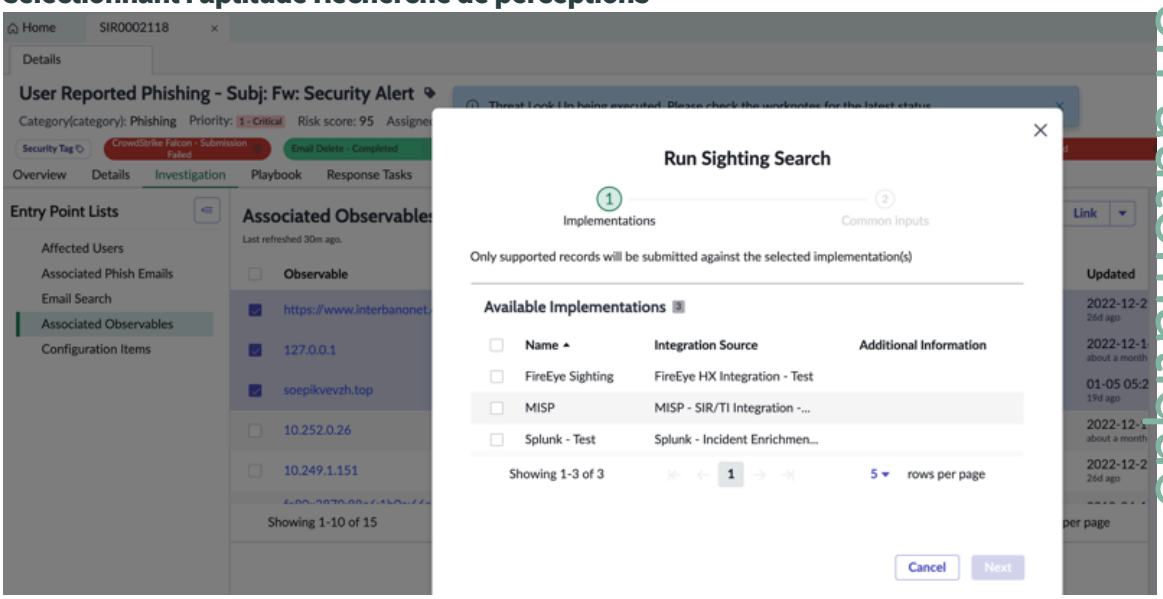
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exécuter une recherche de menace



5. Cochez la case de n'importe quel observable pour lequel vous souhaitez effectuer la recherche de menace.
6. Sélectionnez **Exécuter la recherche de perception** pour effectuer une recherche d'e-mail.
   La boîte de dialogue modale Exécuter les implémentations de recherche de perception s'affiche.

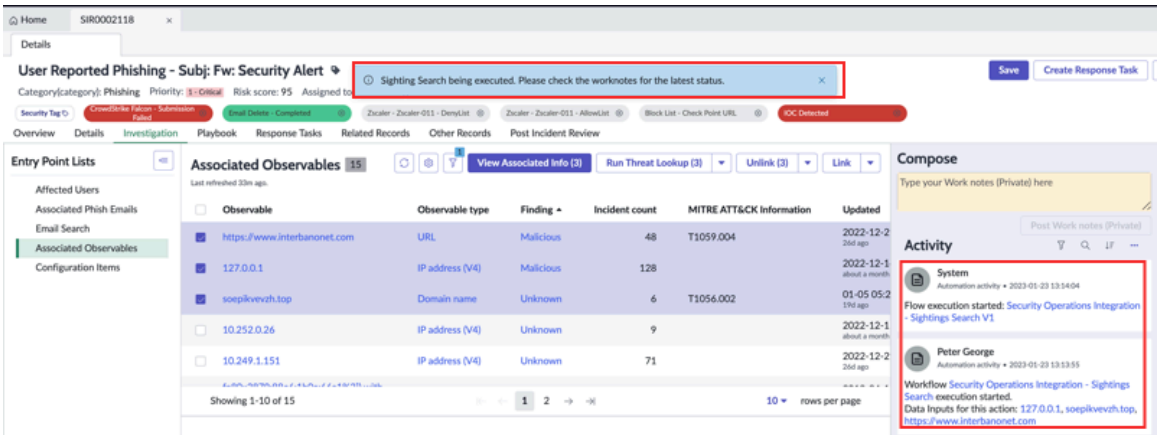
Un exemple qui montre comment ajouter des entrées d'exécution courantes en sélectionnant l'aptitude Recherche de perceptions



7. Sélectionnez une ou plusieurs implémentations dans la liste.
8. Cliquez sur **Suivant**.
   Une fois les enregistrements sélectionnés envoyés, un message s'affiche indiquant que la recherche de perception est demandée. Une fois l'implémentation traitée dans le back-end, les résultats sont affichés dans la section de liste connexe **Recherche de perception** . En outre, l'activité d'implémentation respective est affichée dans la section Activité. Deux activités s'affichent, l'une lorsque l'exécution de l'implémentation est commencée et l'autre lorsque l'exécution est terminée.
9. Sélectionnez la valeur d'entrée de temps d'exécution commune.
10. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois les enregistrements sélectionnés envoyés, un message s'affiche indiquant que la recherche de perception est demandée. Une fois l'implémentation traitée dans le back-end, les résultats sont affichés dans la section de liste connexe **Résultats de recherche de perceptions** . En outre, l'état de traitement de l'activité d'implémentation respective est affiché dans la section **Activité** .

Exemple 3 : Ajouter des entrées de détails d'exécution spécifiques à une implémentation : Exécuter des actions supplémentaires

Ajoutez des entrées de détails d'exécution spécifiques à une implémentation, exécutez des actions supplémentaires.

Vous pouvez **exécuter des actions supplémentaires** liées aux options d'intégration à l'aide de l'onglet **Examiner** du Espace de travail SIR.

1. Dans l'onglet **Examiner** , accédez à la section **Listes de points d'entrée** affichée sur le côté gauche de la page.
2. Sélectionnez le point d'entrée respectif et exécutez l'action d'aptitude d'intégration.

> **Remarque :** Vous pouvez également accéder à l'onglet **Enregistrements connexes** dans l'espace de travail pour effectuer l'action des options d'intégration.

Ajouter des entrées spécifiques à une implémentation

Ajoutez des entrées de temps d'exécution spécifiques pour chacune des implémentations sélectionnées, le cas échéant.

Avant de commencer

Rôle requis : sn_si.analyst

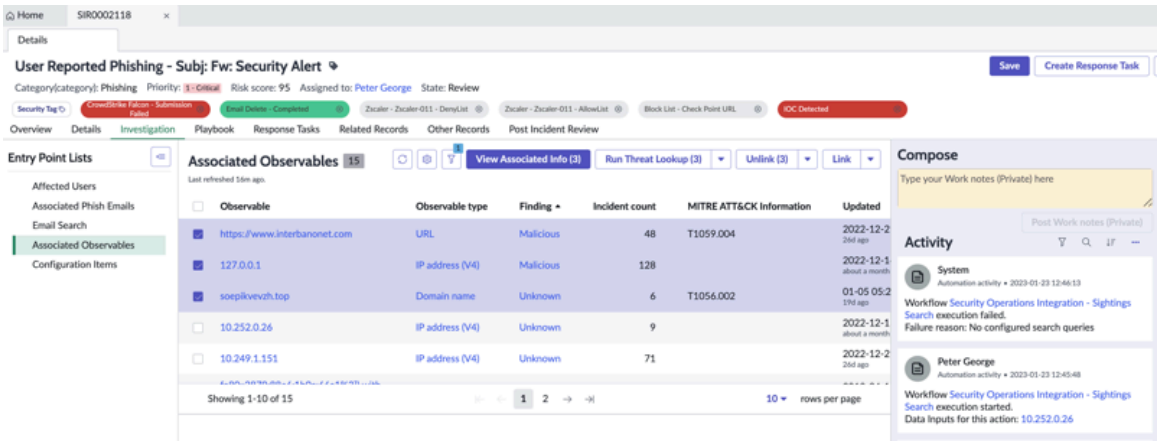
Les implémentations disponibles sont répertoriées. Sélectionnez la ou les implémentations. Une fois que vous les avez sélectionnées, seuls les enregistrements pris en charge sont soumis sur chaque implémentation sélectionnée.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Accédez à l'onglet **Examiner** de l'espace de travail.
   L'onglet Examiner avec les listes de points d'entrée s'affiche.

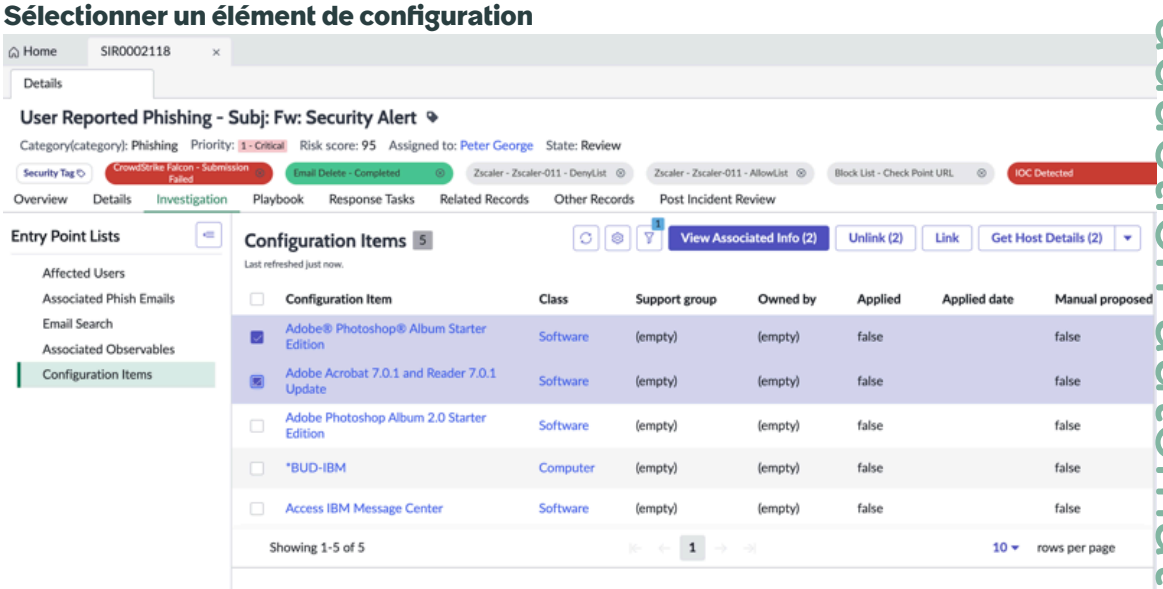
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez l’élément de configuration dans la liste des points d’entrée.
   Par exemple, sélectionnez la liste des points **d’entrée de l’élément de configuration** . Les enregistrements d’éléments de configuration correspondants s’affichent.

Sélectionner un élément de configuration



5. Sélectionnez **n’importe quel élément de configuration**.

6. Accédez à la liste déroulante des listes connexes qui s’affiche en haut de la page.
   Pour l’élément de configuration (CI) d’incident de sécurité, les listes déroulantes contiennent la liste suivante d’actions d’options. Les actions de CI répertoriées collectent les résultats et les stockent en tant que données d’enrichissement sur un incident de sécurité :

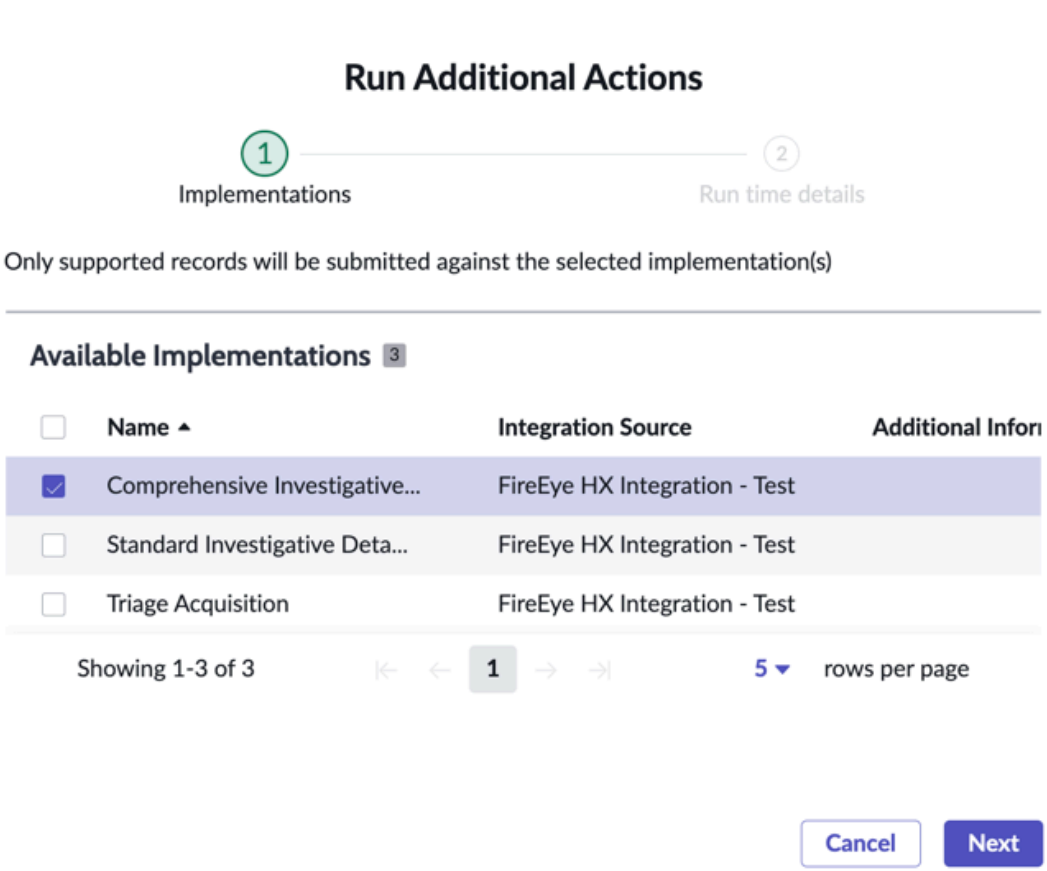
   - Obtenir un fichier : cette aptitude effectue l’action pour obtenir des fichiers avec une valeur de hachage spécifique ou un nom de fichier.
   - Isoler l’hôte : cette fonctionnalité limite les connexions système à d’autres appareils.
   - Obtenir les détails de l’hôte : cette aptitude récupère les détails de l’hôte, les détails des utilisateurs connectés et d’autres options d’enrichissement.
   - Exécuter des actions supplémentaires : cette aptitude exécute les actions supplémentaires au-delà des actions standard.
   - Obtenir les statistiques réseau : cette aptitude récupère les statistiques réseau d’une ressource affectée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Obtenir l'exécution du processus : cette aptitude récupère une liste des processus en cours d'exécution sur un élément de configuration (CI) à partir d'un hôte.
- Obtenir les utilisateurs connectés : cette fonctionnalité collecte les données des utilisateurs connectés et les relie à l'incident de sécurité.

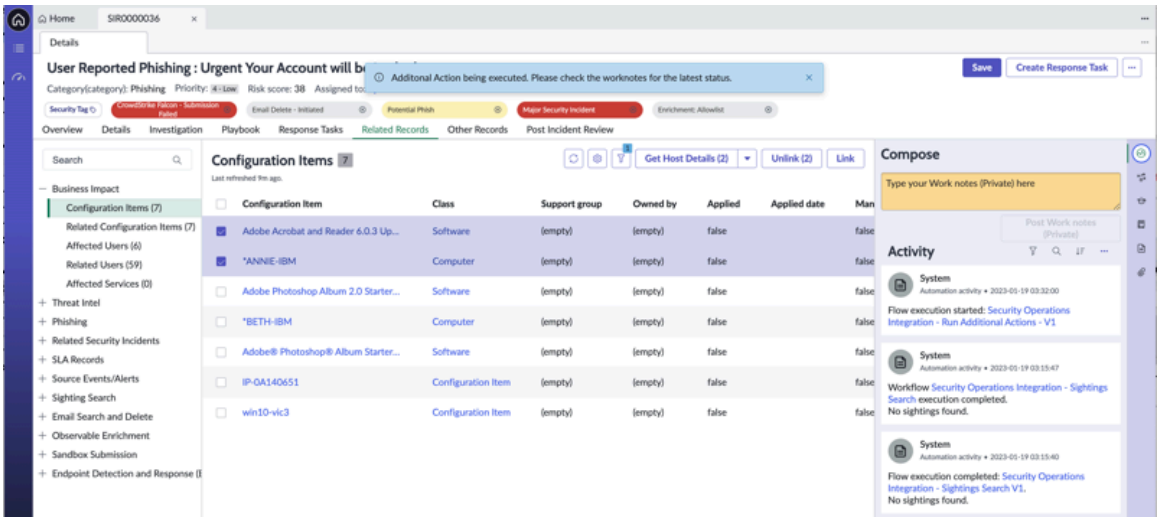
7. Sélectionnez **Exécuter des actions supplémentaires** pour effectuer une action d'options d'intégration liées aux informations sur les menaces.
   La boîte de dialogue modale Exécuter des implémentations supplémentaires s'affiche.
8. Sélectionnez une ou plusieurs implémentations dans la liste.



9. Cliquez sur **Suivant**.
   Vous allez maintenant passer à l'étape suivante pour ajouter les détails de la durée d'exécution.
10. Saisissez un commentaire à associer à l'action.
11. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois les enregistrements sélectionnés soumis, un message s'affiche indiquant que la demande d'action supplémentaire est en cours d'exécution. En outre, la progression respective des actions d'implémentation est affichée dans la section **Activité** .

12. Affichez les résultats de la section de la liste connexe EDR.

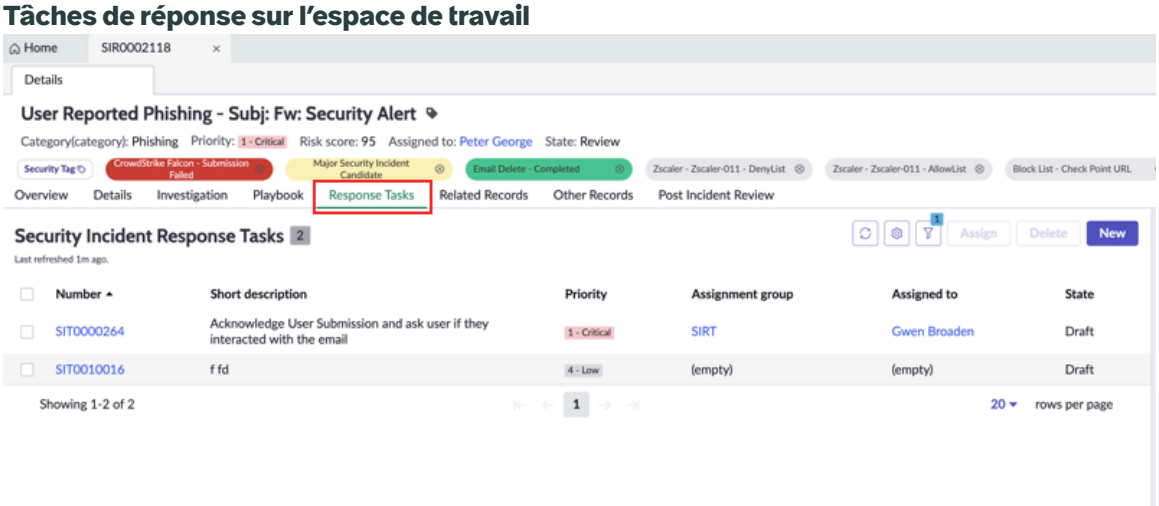
Tâches Réponse aux incidents de sécurité

Toutes les tâches de réponse associées à un incident de sécurité sont affichées dans la section Tâches de réponse.

L'analyste sera en mesure de :

- Créer une nouvelle tâche de réponse
- Affecter des tâches de réponse à soi-même ou à d'autres personnes
- Supprimer les tâches de réponse

Tâches de réponse sur l'espace de travail



Remarque : Pour apporter des modifications rapides aux tâches de réponse. Sélectionnez la tâche de réponse et une liste de tâches de réponse s'affiche, sélectionnez l'enregistrement, apportez des modifications et enregistrez la tâche de réponse.

Créer une tâche de réponse

Créez des tâches de réponse pour suivre les actions distinctes à effectuer pour répondre au problème de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

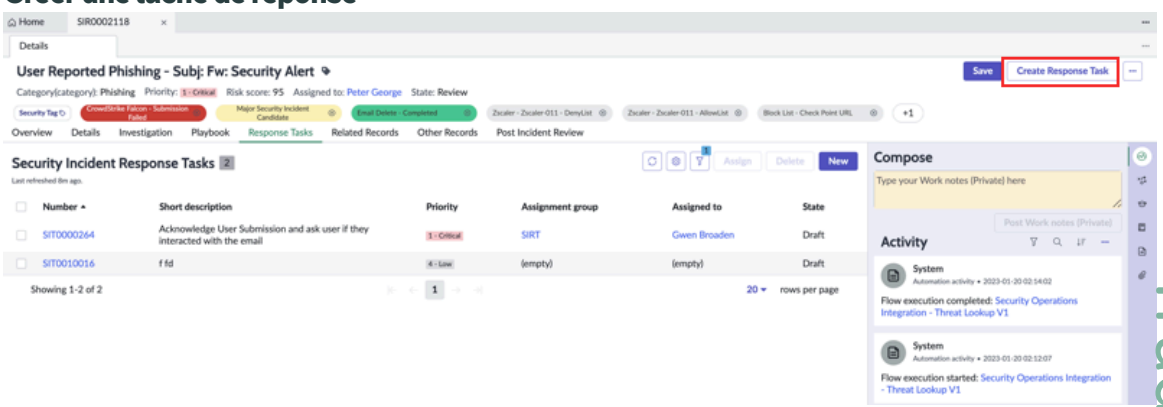
Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Cliquez sur Créer une **tâche de réponse** à partir des actions d'interface utilisateur.

Créer une tâche de réponse



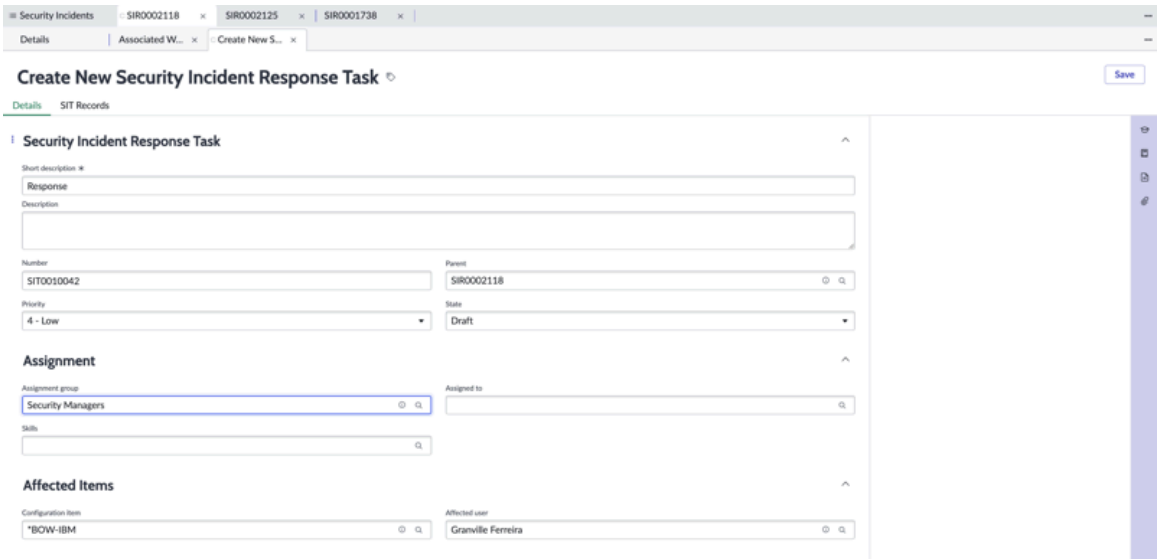
3. Renseignez les champs du formulaire comme il convient.

Incident de sécurité

Champ	Description
Description brève	Description de la Réponse aux incidents de sécurité tâche.
Description	Description de la tâche sélectionnée.
Numéro	Numéro unique généré automatiquement pour un incident de sécurité.
Parent	Numéro de l'incident de sécurité connexe.
Priorité	Priorité utilisée pour déterminer quand cette tâche est exécutée.
État	État actuel de la tâche de réponse de sécurité. Par défaut, l'état initial est **Brouillon**.
Groupe d'affectation	Groupe d'affectation à partir duquel l'agent affecté est sélectionné.
Affecté à	Personne affectée à l'exécution de la tâche.
Compétences	Compétence requise pour effectuer cette tâche. Recherchez dans la recherche et sélectionnez la compétence requise.
Éléments affectés	Les éléments affectés par le problème de sécurité.
Élément de configuration	Élément de configuration affecté par le problème de sécurité.
Utilisateur affecté	Personne affectée par le problème de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



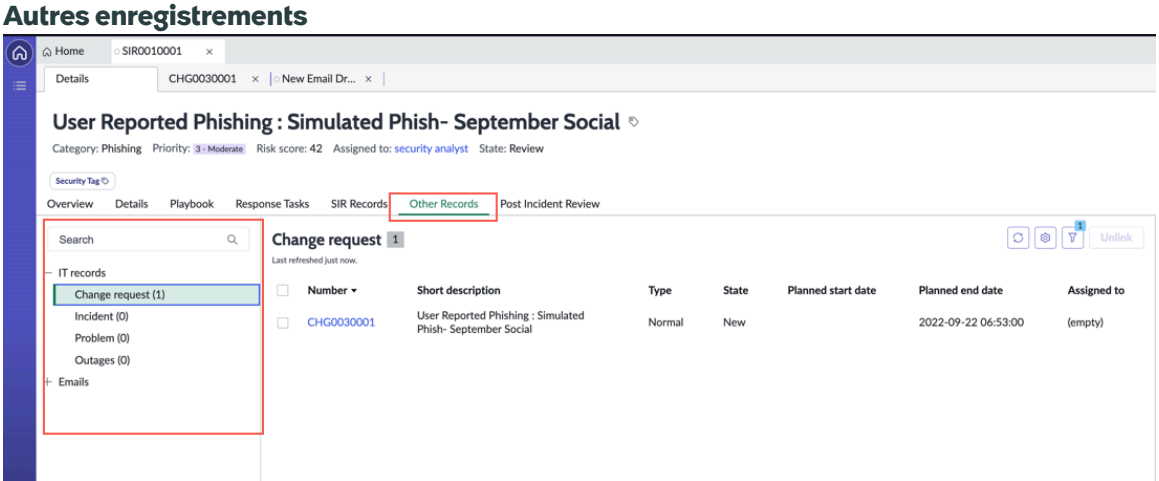
4. Cliquez sur **Enregistrer**.
   La nouvelle tâche de réponse (SIT) est créée.

Autres enregistrements de Réponse aux incidents de sécurité

Cette section affiche les autres enregistrements tels que les enregistrements liés au service informatique et les enregistrements d'e-mails. Sous Les enregistrements informatiques, Incident, Demande de changement, Problème et Pannes sont affichés.

Sous E-mail, Brouillon, E-mails envoyés et E-mails reçus sont affichés.

Autres enregistrements



Créer un incident

Créez un incident dans un incident de sécurité.

Avant de commencer
Rôle requis : sn_si.analyst.

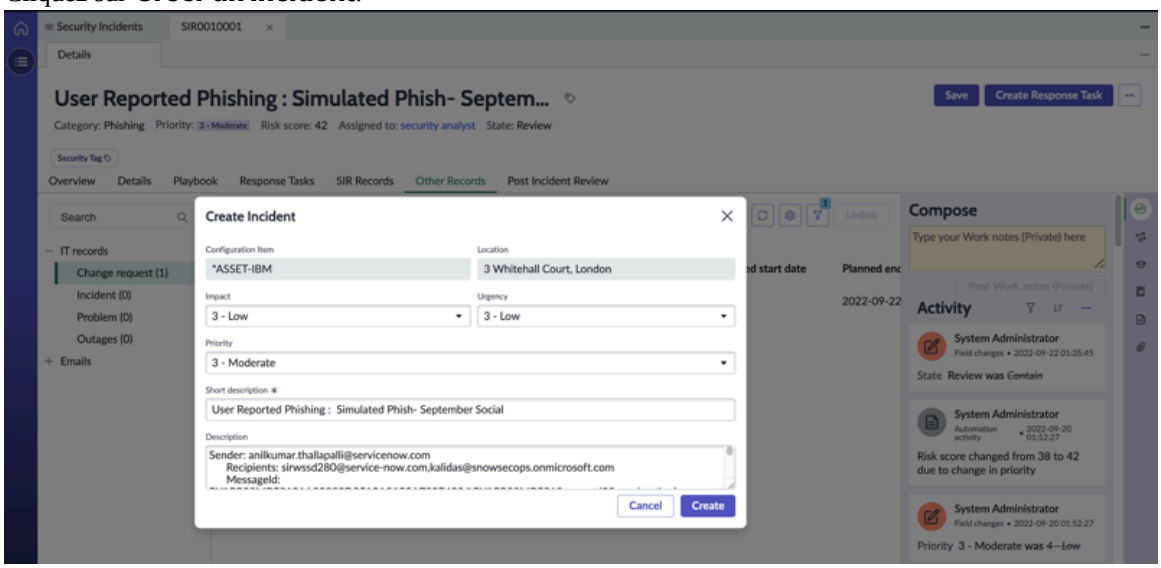
Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel enregistrement d'incident.

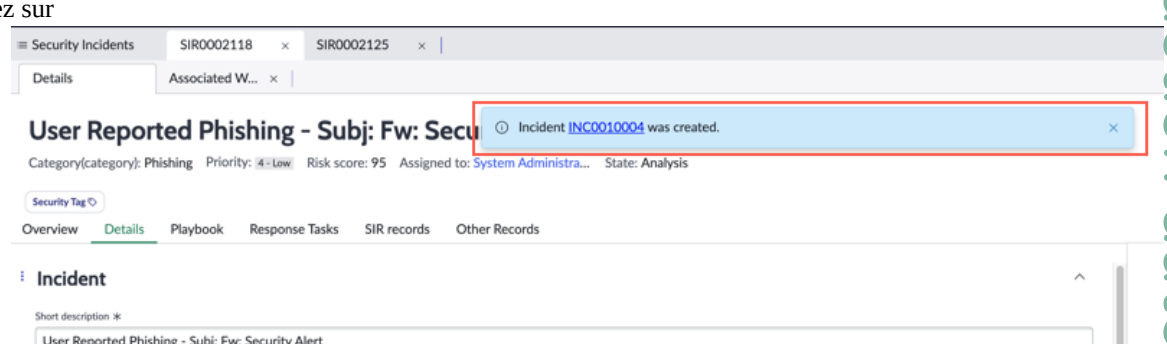
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Créer un incident**.



4. Saisissez les détails tels que l'élément de configuration, l'impact, l'urgence, l'emplacement, la priorité et la description courte.
5. Cliquez sur **Créer**.



6. Un incident est créé.

Lier plusieurs incidents ITSM

Lier Gestion des services IT (ITSM) les incidents liés à un incident de sécurité.

Avant de commencer

Remarque : Vous pouvez également créer un ITSM incident pour le lier à un incident de sécurité. Pour plus d'informations, consultez Créer un incident.

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez l'icône Liste (icône).
3. Ouvrez l'enregistrement de l'incident .
4. Sélectionnez l'onglet **Autres enregistrements** .
5. Sous **Enregistrements informatiques**, sélectionnez **Incident**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous passez à l'interface utilisateur classique, sous l'onglet **Enregistrements connexes** , le champ **Incident** est supprimé.

6. Sélectionnez **un lien**.
7. Sélectionnez les ITSM incidents que vous souhaitez lier à l'incident de sécurité sélectionné.
8. Sélectionnez **un lien**.

Résultats

Les incidents sélectionnés ITSM sont répertoriés dans la section Enregistrements informatiques de l'enregistrement d'incident de sécurité sélectionné.

Création d'une tâche de problème

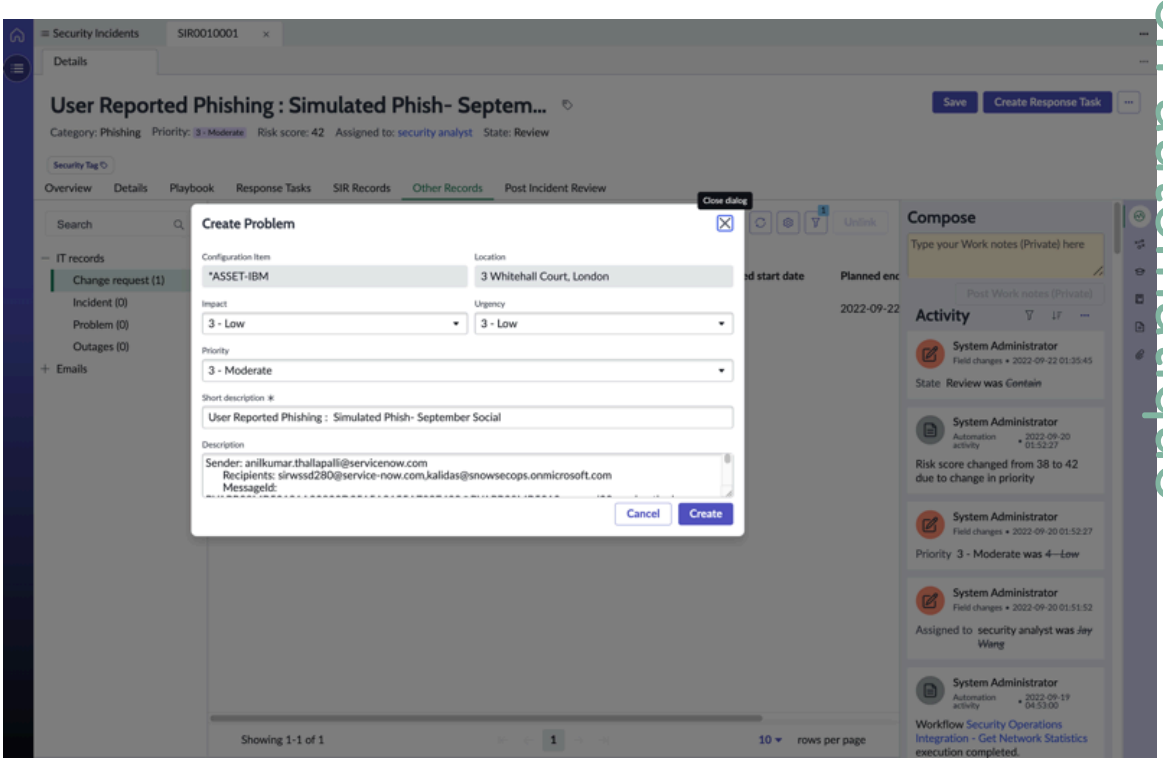
Créez une tâche de problème.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

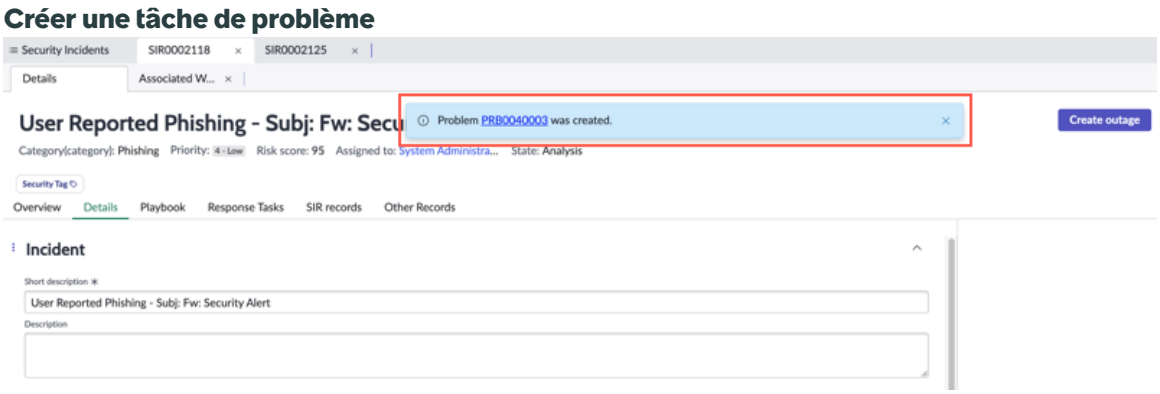
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel enregistrement d'incident.
3. Cliquez sur **Créer un problème**.



4. Renseignez les détails tels que l'élément de configuration, l'emplacement, l'impact, l'urgence, la priorité et la description courte.
5. Cliquez sur **Créer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Une tâche de problème est créée.

Créer une demande de changement

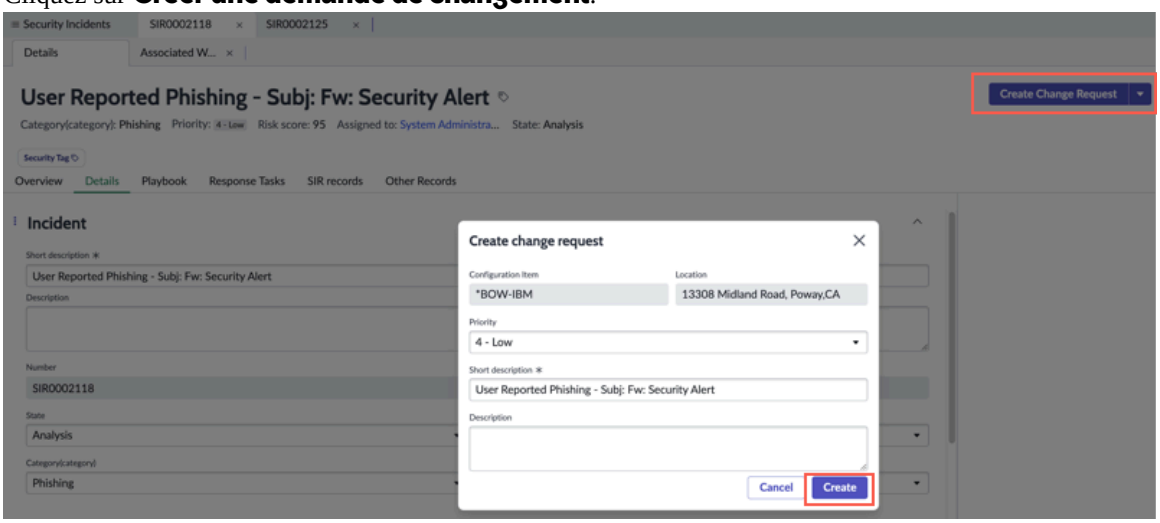
Créez une demande de changement.

Avant de commencer

Rôle requis : sn_si.analyst.

Procédure

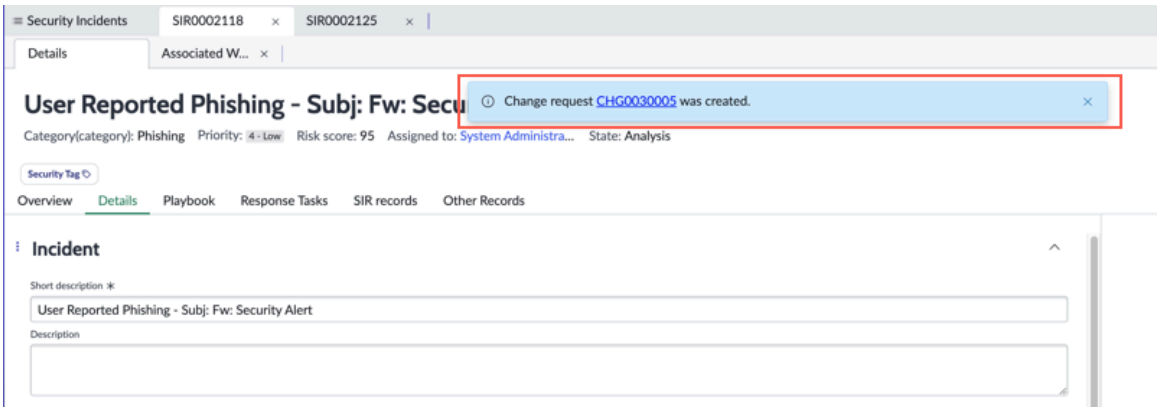
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel enregistrement d'incident.
3. Cliquez sur **Créer une demande de changement**.



4. Saisissez les détails tels que l'élément de configuration, l'emplacement, la priorité et la brève description.
5. Cliquez sur **Créer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Une demande de changement est créée.

Créer une panne

Crète une panne à partir d'un incident pour suivre le temps d'arrêt d'un élément de configuration.

Avant de commencer

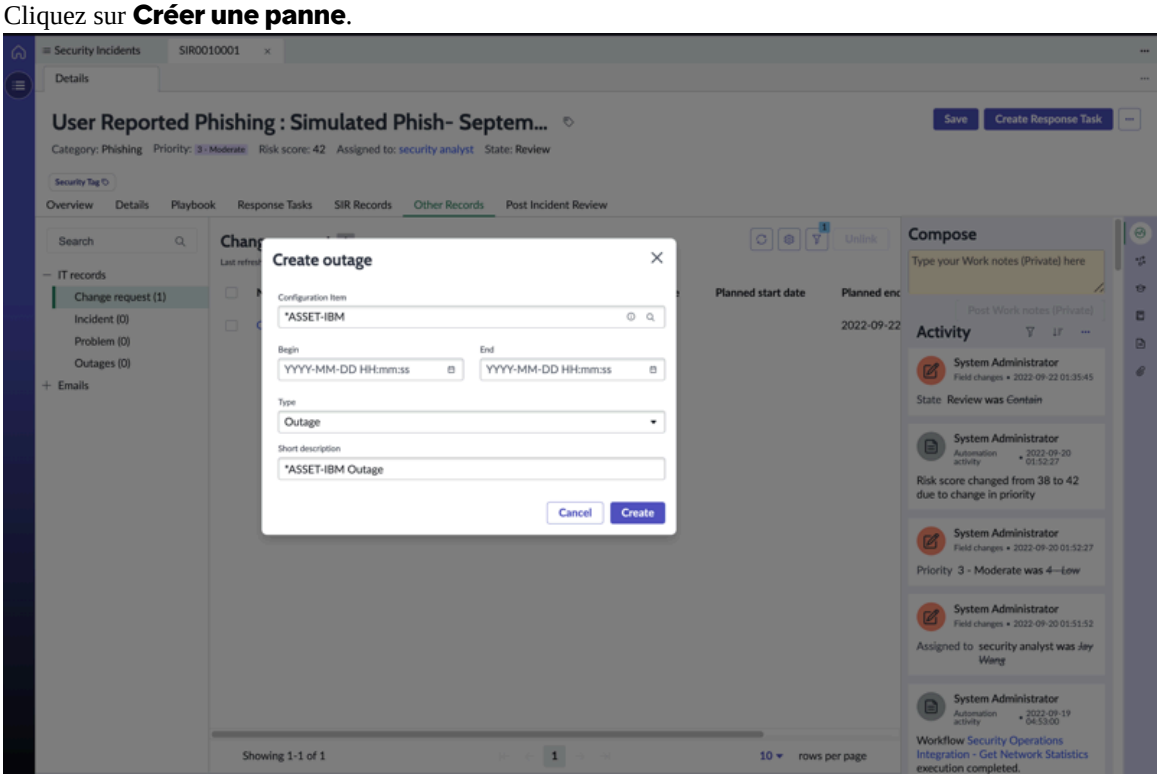
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.

2. Ouvrez n'importe quel enregistrement d'incident.

3. Cliquez sur **Créer une panne**.

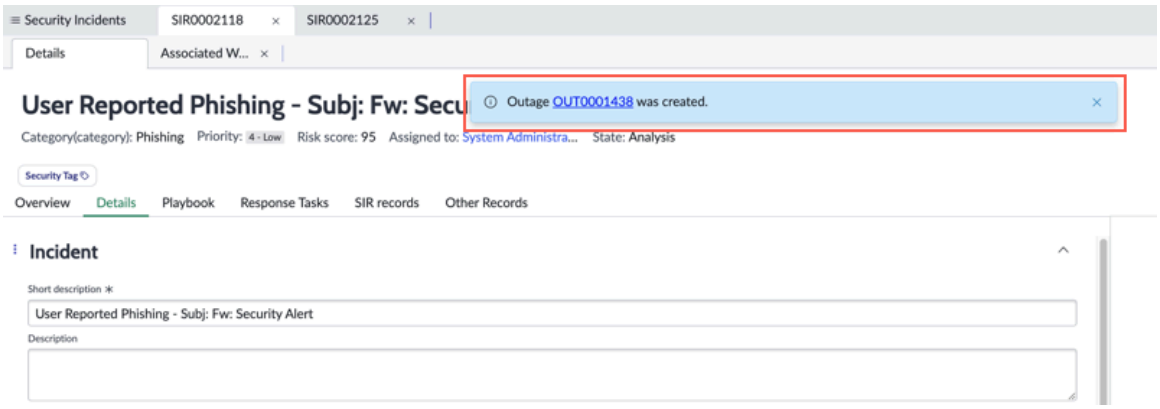


4. Entrez les détails tels que Élément de configuration, Date de début, Date de fin, Type et Description courte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Créer**.



Composer des e-mails

En tant qu'analyste, vous pouvez composer des e-mails directement à partir d'incidents de sécurité.

Avant de commencer

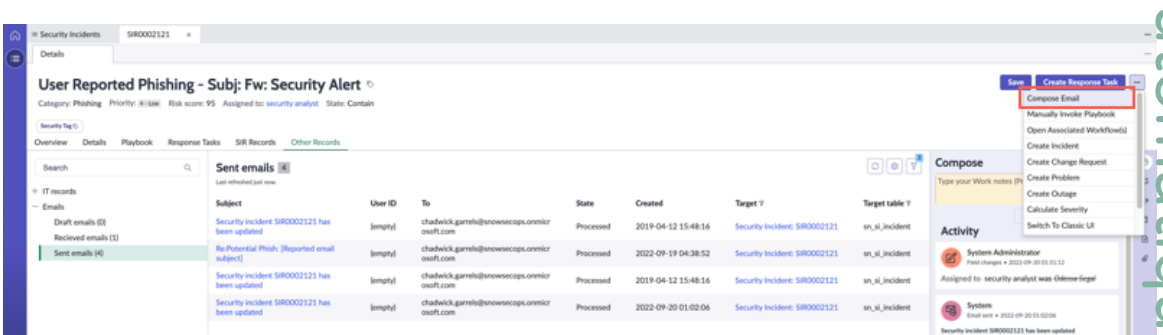
Rôle requis : sn_si.analyst

Procédure

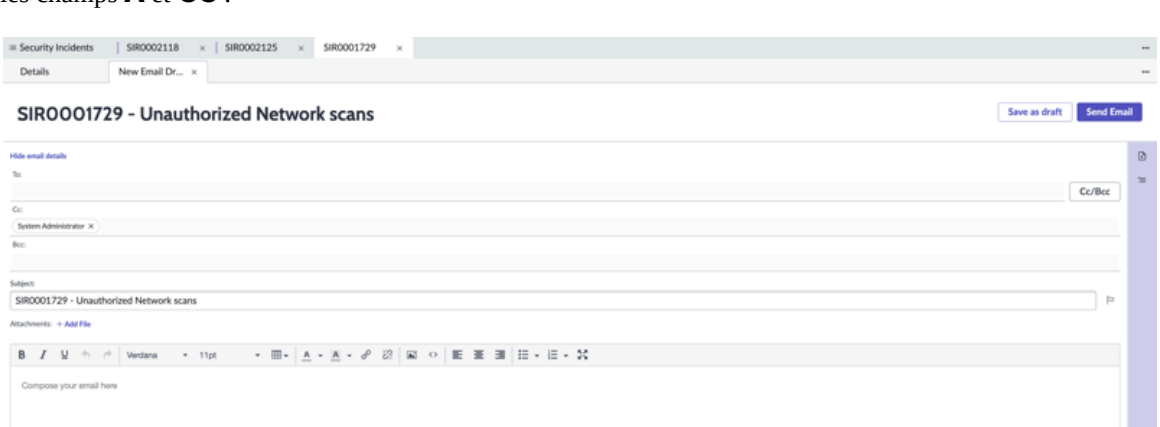
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.

2. Sélectionnez et ouvrez l'incident pour lequel vous souhaitez composer un e-mail.

3. Cliquez sur le débordement et sélectionnez **Composer un e-mail**.



4. Entrez les champs **À** et **CC** .

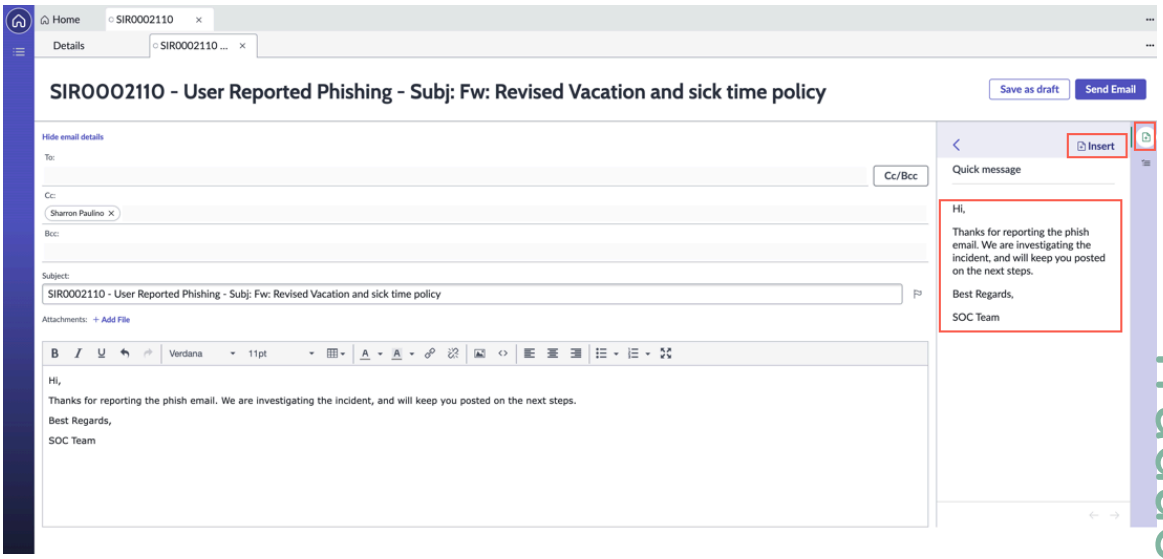


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Ajoutez** des pièces jointes, le cas échéant.

6. Dans le formulaire E-mail, cliquez sur **Messages rapides** pour afficher les messages rapides qui s'affichent sur le côté droit de la section **Composer des e-mails** .
   Les messages rapides disponibles s'affichent. Sélectionnez le message et cliquez sur **Insérer**. Les messages sont insérés dans le corps de l'e-mail.



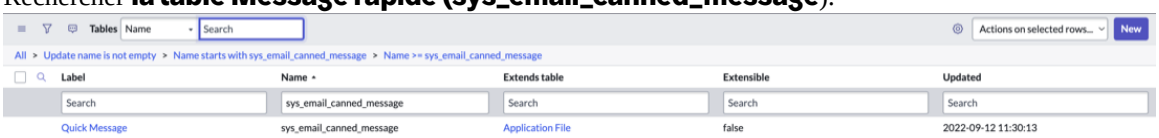
7. Composez votre e-mail et cliquez sur **Envoyer un e-mail**.

> **Remarque :** Vous pouvez enregistrer un e-mail en tant que brouillon. Ces brouillons d'e-mails sont disponibles sous l'onglet Autres enregistrements.

Comment configurer les messages rapides :

a. Accédez à la **Définitions des systèmes** > **Tables**.

b. Rechercher **la table Message rapide (sys_email_canned_message)**.



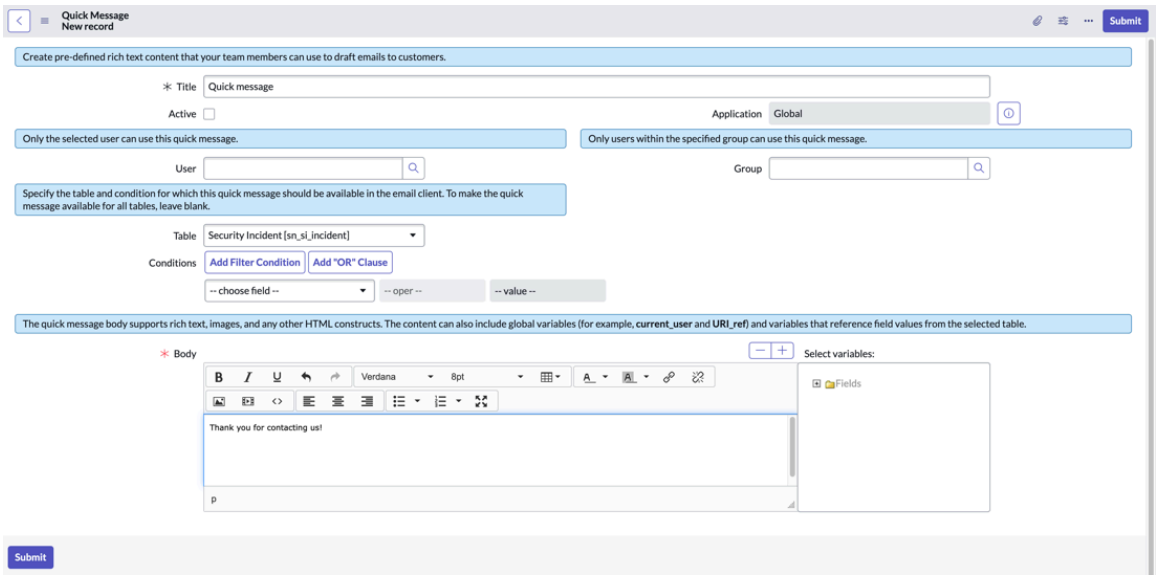
c. Accéder à **Liens connexes** > **Afficher la liste**.

d. Créer **nouveau**.

e. Saisissez le **titre**, **le corps du message**, cochez la case **Table : Incident de sécurité (sn_si_incident)** et **Actif** .

Traduction automatique

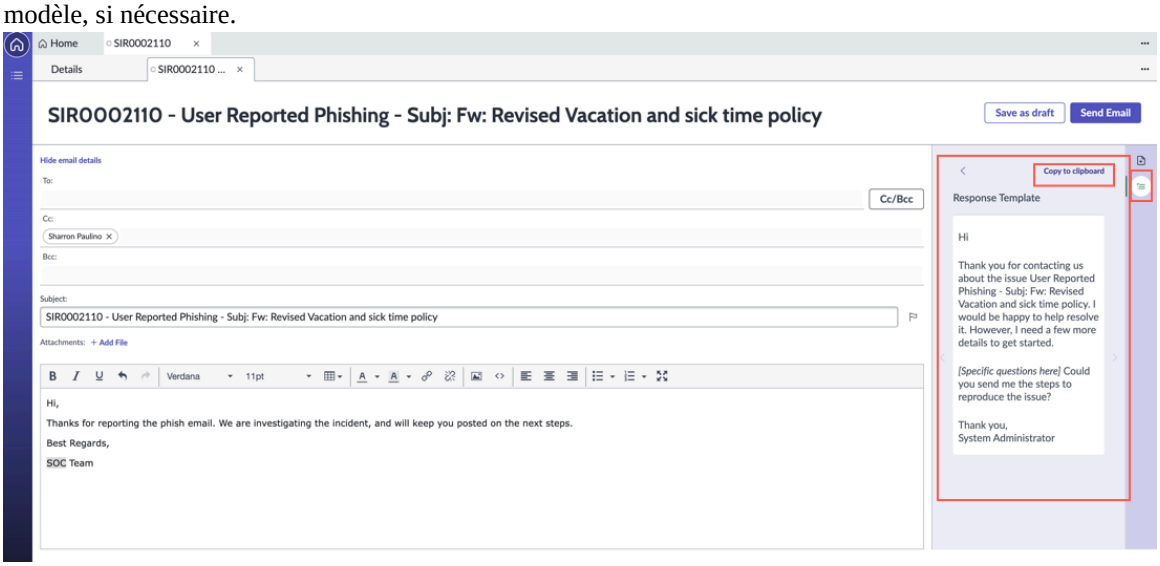
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



f. Cliquez sur **Envoyer**.
Une fois qu'une nouvelle entrée est créée dans la table, le message rapide apparaît dans le menu contextuel.

8. Cliquez sur **Modèles** pour ajouter un modèle si nécessaire.

9. Sélectionnez le **modèle de réponse** , cliquez sur **Copier dans le presse-papiers** et appliquez le modèle, si nécessaire.



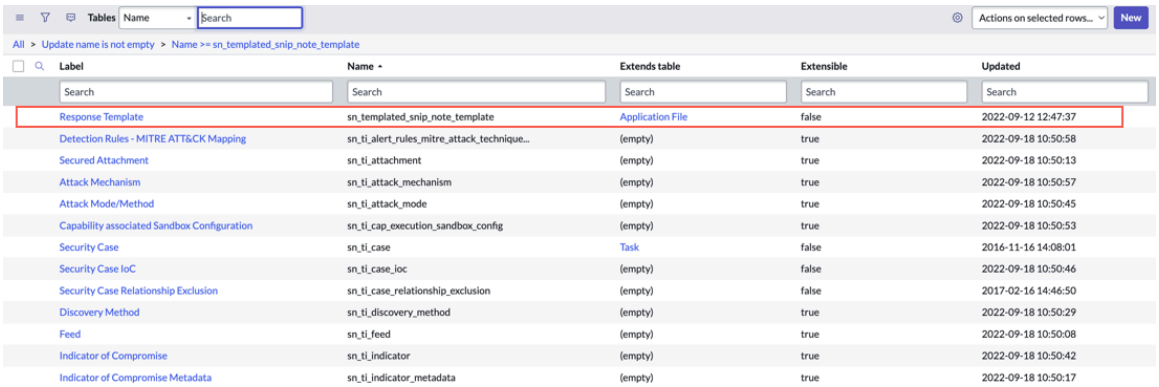
Comment configurer les modèles de réponses :

a. Accédez à la **Définitions des systèmes** > **Tables**.

b. Recherchez la table **Modèle de réponse (sn_templated_snip_note_template).**

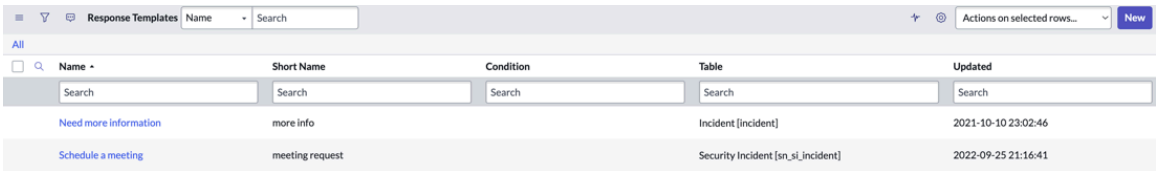
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

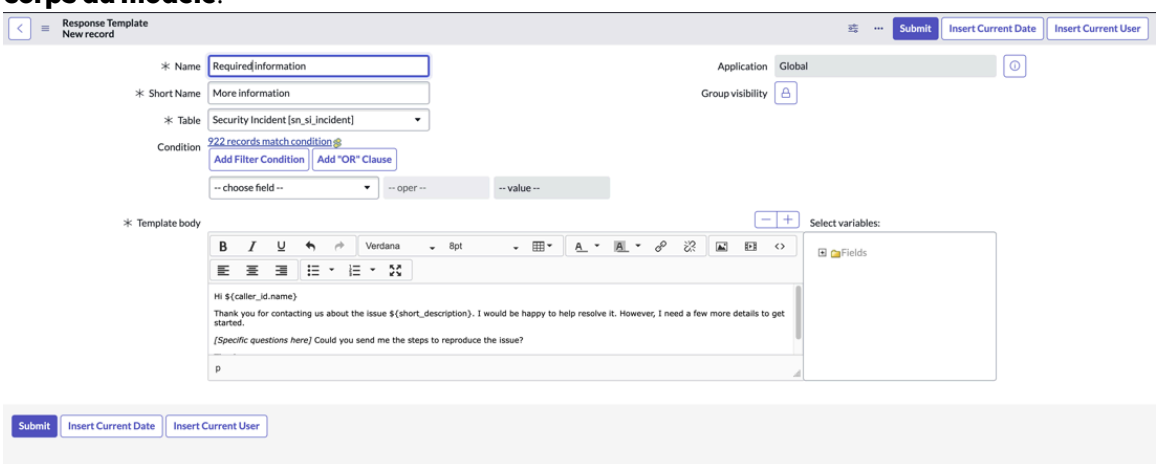


c. Accéder à **Liens connexes** > **Afficher la liste**.

d. Créer **nouveau**.



e. Saisissez le **nom**, le **nom court**, sélectionnez la **table : Incident de sécurité (sn_si_incident)** et **le corps du modèle**.



f. Cliquez sur **Envoyer**.
Une fois qu'une nouvelle entrée est créée dans la table, le nouveau modèle apparaît dans le menu contextuel.

Revue post-incident de Security Incident Response

La revue post-incident apparaît lorsqu'un incident passe à l'état Revue.

Pour plus d'informations sur la conduite des activités post-incident, voir Rapport d'examen post-incident

La revue post-incident comprend les sections suivantes :

1. Évaluations
2. Rapports

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'espace de travail Réponse aux incidents de sécurité, vous pourrez demander et effectuer des évaluations à l'aide de ces deux nouvelles actions d'interface utilisateur.

Nom	Description
Évaluations	L'évaluation affiche toutes les évaluations associées à l'incident de sécurité et les autres évaluations. L'analyste pourra effectuer des évaluations et demander des évaluations. • **Effectuer des évaluations** : cliquez sur **Effectuer des évaluations** pour effectuer les évaluations (le cas échéant) et terminer l'évaluation. Avant de terminer l'évaluation, l'état de l'incident de sécurité est Prêt à prendre et la date d'échéance de l'incident est indiquée en rouge. • Évaluations de demandes : cliquez sur **Évaluation** de demande pour toute évaluation supplémentaire et vous pouvez ajouter les nouveaux utilisateurs que vous souhaitez demander. **Remarque :** Les utilisateurs qui avaient déjà fait une demande n'apparaîtront pas dans cette section. Toute évaluation de cet incident a été configurée en fonction des conditions définies lors de la revue post-incident, elle doit être obligatoire ou facultative.
Rapports	Modifiez les configurations d'exécution et générez le rapport. Sélectionnez l'instance de rapport, modifiez les filtres et enregistrez le rapport. L'analyste peut prévisualiser et télécharger le rapport PIR.

Intégration TISC dans l'espace de travail SIR

La section suivante comprend des informations sur l'intégration du Centre de sécurité des renseignements sur les menaces dans le contexte de l'espace de travail SIR.

Envoyer les données de l'espace de travail SIR à TISC

Découvrez comment les données sont collaborées et partagées entre le Centre de sécurité des renseignements sur les menaces (TISC) et les espaces de travail Réponse aux incidents de sécurité (SIR) en suivant les procédures expliquées dans les sections suivantes.

Propriétés système pour envoyer des données

Examinez les propriétés système pour les intégrations TISC à combiner avec SIRW. Vous pouvez configurer ces propriétés pour contrôler la façon dont les deux applications gèrent les intégrations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Considérations clés

Les propriétés système pour les intégrations TISC fournissent des options de configuration avancées sur la façon dont l'application gère les observables et les enrichissements.

1. Pour définir les propriétés système des intégrations TISC dans SIRW, accédez aux **propriétés système** pour Renseignements sur les menaces et accédez à la table [sys_properties].
2. Les propriétés système contrôlent et gèrent le comportement de chaque opération de transmission de données individuelle.
3. Lorsque la propriété est activée, les données sont transmises automatiquement lorsque les données observables ou d'enrichissement sont générées dans l'espace de travail SIR.
4. Si la propriété est désactivée, les données sont transmises manuellement et les utilisateurs peuvent transmettre des données à l'aide des actions d'interface utilisateur à partir de l'espace de travail SIR.

La liste suivante affiche les propriétés système pour l'intégration TISC - SIR :

- Transmettre automatiquement et manuellement les données des observables à partir de SIR : activez la propriété sn_ti.allow_observable_and_enrichment_records_push pour transmettre les données automatiquement ou manuellement par push. Si elle est désactivée, cette propriété désactivera les modes automatique et manuel pour toutes les transmissions de données provenant de SIR.
- Transmettre par push les résultats de la recherche de menaces : activez cette propriété système sn_ti.automatic_push_threat_lookup_results pour transmettre automatiquement les données de recherche de menaces à TISC. Si cette option est désactivée, les analystes de sécurité peuvent toujours transmettre manuellement les données de recherche de menaces.
- Transmettre les résultats de la recherche de perception à TISC : activez sn_ti.automatic_push_sighting_results_to_tisc cette propriété système pour transmettre automatiquement les données de recherche de perception à TISC. Si cette option est désactivée, les analystes de sécurité peuvent toujours envoyer manuellement les données de recherche de perception.
- Push des observables : activez sn_ti.automatic_push_observable_to_tisc cette propriété système pour transmettre automatiquement les données des observables à TISC. Si cette option est désactivée, les analystes de sécurité peuvent toujours transférer les données des observables manuellement.
- Transmettre les résultats de l'enrichissement par push : activez sn_ti.automatic_push_enichment_results cette propriété système pour transmettre automatiquement les données des résultats d'enrichissement à TISC. Si cette option est désactivée, les analystes de sécurité peuvent toujours transférer manuellement les données des résultats d'enrichissement.

Ajouter un incident de sécurité au ticket TISC

Ajouter des incidents de sécurité aux enregistrements de tickets TISC.

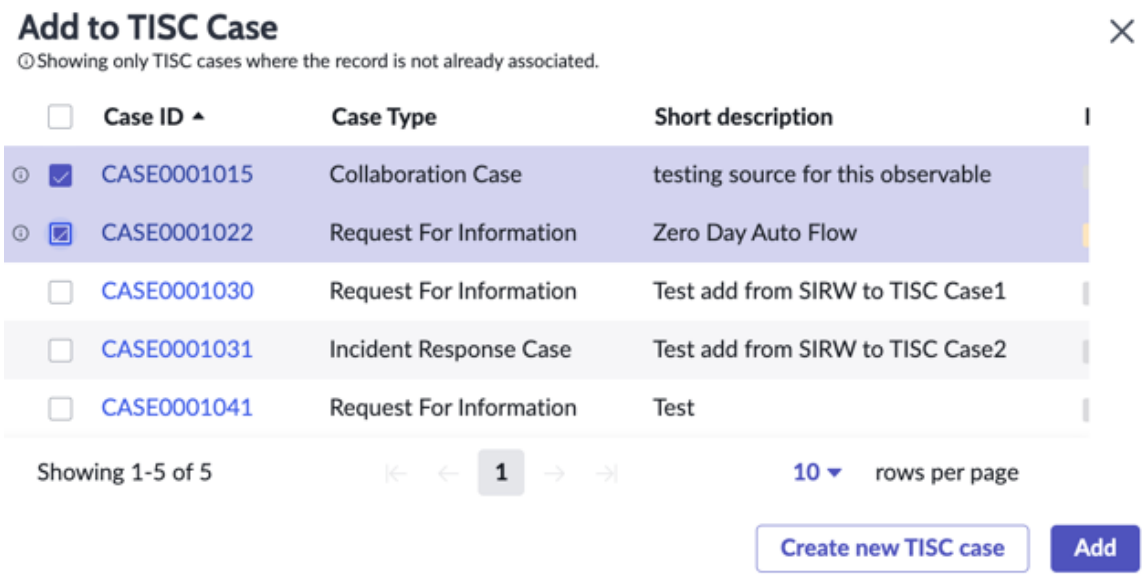
Avant de commencer
Rôle requis : sn_si.analyst, sn_sec_tisc.case_write

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tous**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.
   Cela peut également être fait en recherchant l'ID de l'incident, en naviguant à partir de la section Filtres rapides ou en filtrant l'état de l'incident.
3. Cliquez sur **l'icône Plus d'actions** .
4. Cliquez sur **l'action Ajouter au ticket TISC** .
   La boîte de dialogue Ajouter au ticket TISC s'affiche et affiche uniquement les tickets TISC pour lesquels l'incident n'est pas déjà associé.
5. Sélectionnez le ou les cas dans la boîte de dialogue **Ajouter au ticket** .



> **Remarque :** Créez un nouveau ticket TISC s'il n'y a pas d'enregistrement de ticket. Pour en savoir plus sur la création d'un ou de plusieurs tickets, reportez-vous à la section Création de tickets à l'aide de la Console d'analyste de menaces.

6. Cliquez sur **Ajouter**.
7. Cliquez sur l'enregistrement du ticket pour afficher le ticket dans TISC à partir du message d'informations affiché ou du flux **d'activité** .

> **Remarque :** Pour afficher les incidents de sécurité liés, cliquez sur l'enregistrement de ticket particulier à partir du flux **d'activité** d'incident de sécurité. Un clic dessus vous permet d'accéder à l'enregistrement du ticket dans l'espace de travail TISC et les incidents de sécurité sont ajoutés sous l'onglet **Artefacts** du module Gestion des tickets.

Ajouter des observables au ticket TISC

Ajouter des observables aux enregistrements de tickets TISC.

Avant de commencer
Rôle requis : sn_si.analyst, sn_sec_tisc.case_write

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

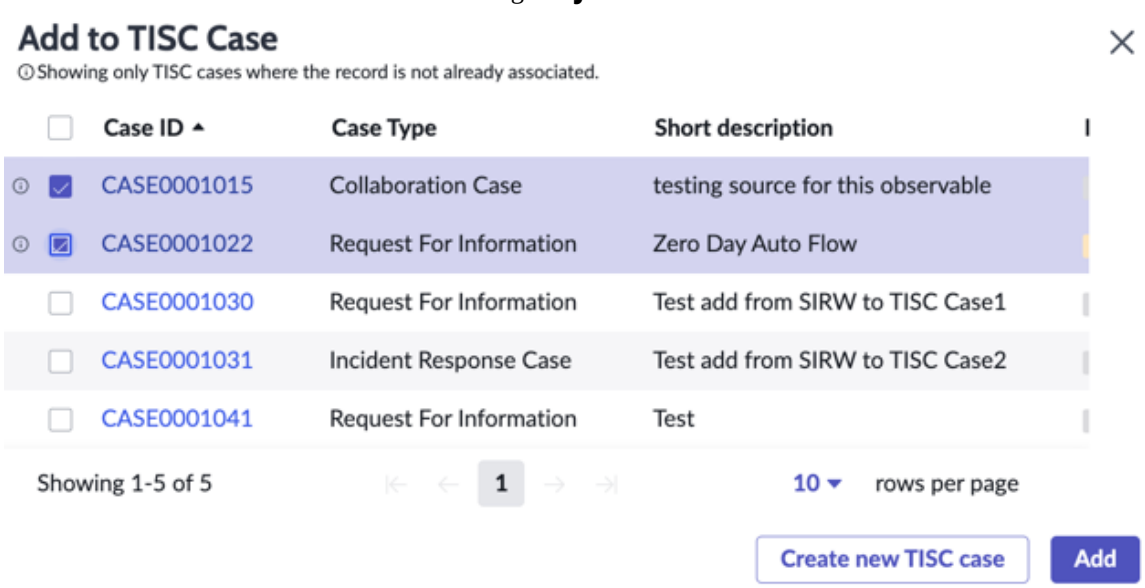
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tous**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.
   Cela peut également être fait en recherchant l'ID de l'incident, en naviguant à partir de la section Filtres rapides ou en filtrant l'état de l'incident.
3. Cliquez sur l'onglet **Enregistrements connexes** dans l'espace de travail.
   Vous pouvez effectuer l'action d'ajout d'observables au(x) ticket(s) TISC à l'aide de différents onglets de l'espace de travail Réponse aux incidents de sécurité.

   Remarque : Vous pouvez accéder au modèle suivant :
   - Page Détails des observables dans l'onglet Enregistrements connexes.
   - **Examiner** , accédez à la section Listes de **points d'entrée** affichée sur le côté gauche de la page et sélectionnez **Observables associés** pour ajouter des observables au ticket TISC.

4. Par exemple, sélectionnez **Connaissance de la menace** > **Observables associés**.
5. Sélectionnez un ou plusieurs observables pour ajouter les observables sélectionnés aux enregistrements de ticket.

   Remarque : Vous pouvez également cliquer sur l'un des enregistrements d'observables pour ouvrir la page de détails des observables dans un autre onglet. Vous pouvez ajouter des enregistrements de tickets à partir d'ici en cliquant sur Ajouter au ticket TISC.

6. Cliquez sur le bouton **Fractionner les actions d'aptitude** .
7. Sélectionnez **Ajouter au ticket TISC**.
8. Sélectionnez le ou les cas dans la boîte de dialogue **Ajouter au ticket** .



   Remarque : Créez un nouveau ticket TISC s'il n'y a pas d'enregistrement de ticket. Pour en savoir plus sur la création d'un ou de plusieurs tickets, reportez-vous à la section Création de tickets à l'aide de la Console d'analyste de menaces.

9. Cliquez sur **Ajouter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Cliquez sur l'enregistrement du ticket pour afficher le ticket dans TISC à partir du message d'informations affiché ou du flux **d'activité** .

> **Remarque :** Si l'observable n'a pas d'observable TISC correspondant, l'observable sélectionné dans l'espace de travail SIR est automatiquement envoyé à TISC et est ensuite ajouté à l'/aux enregistrement(s) de tickets TISC sélectionné(s). Pour afficher les observables liés, cliquez sur l'enregistrement de ticket particulier à partir du flux **d'activité** . En cliquant dessus, vous accédez à l'enregistrement du ticket dans l'espace de travail TISC et les observables sont ajoutés sous l'onglet **Artefacts** du module Gestion des tickets.

Résultats

Vous avez correctement envoyé les données des observables à la gestion des tickets du Centre de sécurité des renseignements sur les menaces.

Envoyer des observables à TISC

À l'aide de cette fonctionnalité, l'analyste de sécurité peut transférer les données des observables de SIR vers TISC. À l'aide du contexte TISC, vous pouvez vérifier si les observables sont présents dans TISC. Dans le cas contraire, l'analyste de sécurité peut transmettre les données par push chaque fois que nécessaire.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

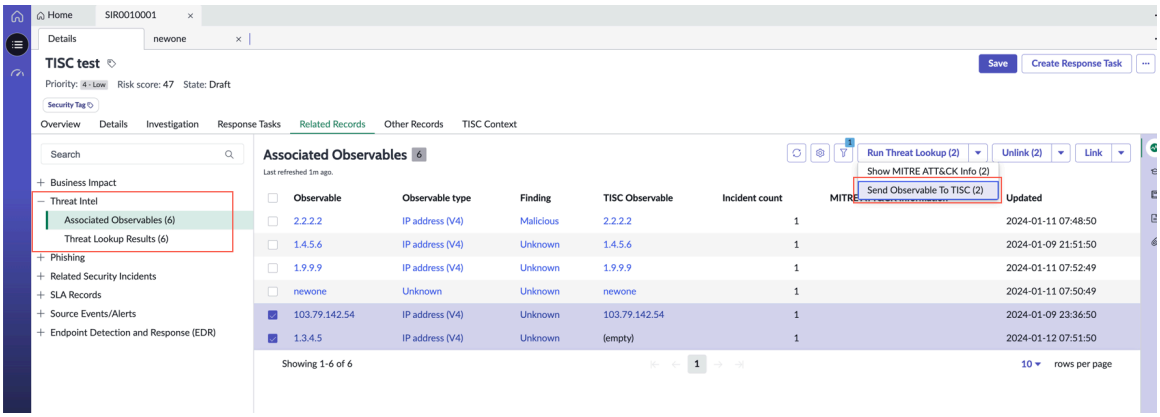
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tous**.
2. Ouvrez un incident de sécurité.
3. Sélectionnez l'onglet **Enregistrements connexes** pour effectuer l'action d'aptitude d'intégration TISC.

> **Remarque :**
>
> - Vous pouvez également accéder à l'onglet **Examiner** , à la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionner **Observables associés** pour effectuer l'opération push.
> - Dans l'onglet **Examiner** , sélectionnez **Afficher les informations connexes** pour afficher toutes les données associées de recherche de menace, de recherche de perception et d'enrichissement pour l'observable sélectionné. Pour plus d'informations, consultez Explorer le canevas d'examen.

4. Par exemple, sélectionnez **Connaissance de la menace** > **Observables associés** pour effectuer l'opération push et transmettre manuellement les données dans TISC.
5. Sélectionnez un ou plusieurs enregistrements d'observables pour effectuer l'opération **Envoyer l'observable à TISC** afin de transmettre les données par push.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Sélectionnez **Envoyer l'observable à TISC**.
7. Dans l'écran Envoyer des observables à TISC, indiquez les éléments suivants :

Ajouter des informations aux observables TISC

Champ	Description
Fiabilité	Score de confiance pour les observables.
TLP	La valeur TLP (Traffic Light Protocol) pour les observables.
Notes	Notes pour les observables.
Balises TISC	Balises pour les observables à envoyer. Vous pouvez ajouter des balises personnalisées qui sont ajoutées aux observables.

8. Sélectionnez **Envoyer**.

Remarque :

- Si l'observable sélectionné n'est pas présent dans TISC, l'observable est d'abord créé en tant que source d'observable. Une fois que l'observable source a créé un enregistrement d'observable TISC, l'enregistrement de l'observable est automatiquement associé à l'observable nouvellement créé.
- Une fois l'opération push d'observable effectuée, un message d'information s'affiche.

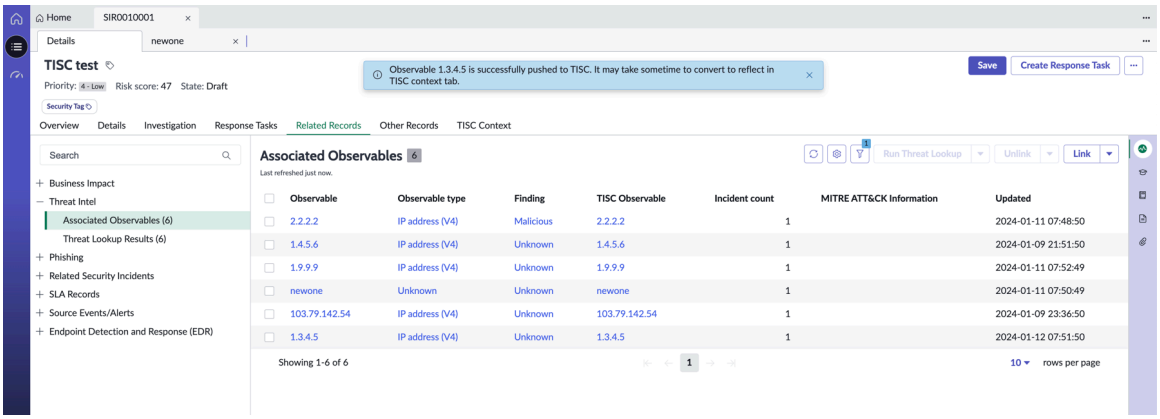
  Les observables suivants sont transmis avec succès à TISC. La réflexion dans l'onglet de contexte TISC peut prendre un certain temps. 0.0.0.0

- Si un observable existe déjà au format TISC, un message d'erreur s'affiche.

  Les observables suivants existent déjà dans TISC : 0.0.0.0

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



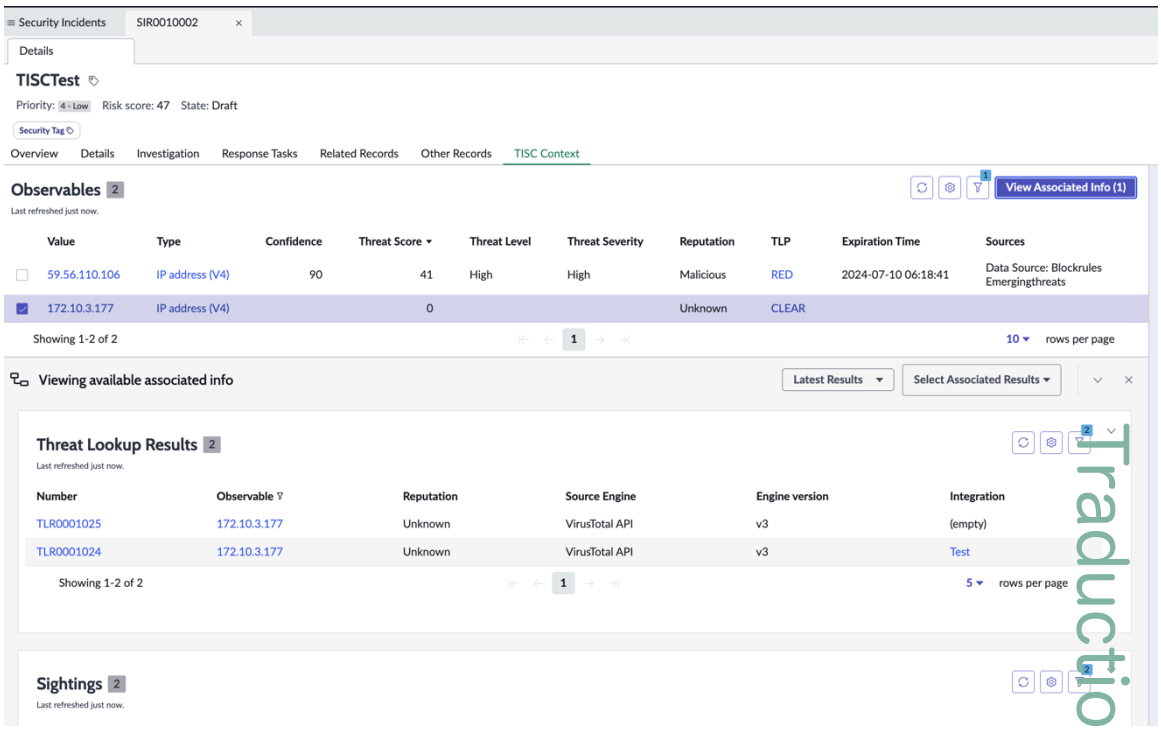
9. Sélectionnez **un contexte TISC**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : :

- Vous voyez maintenant l'observable qui est transmis à TISC à partir de l'application SIR.



- **Dans le cas d'une opération push manuelle** : les données observables ne peuvent être transmises par push que si elles sont liées aux incidents de sécurité. Une fois que l'observable est transmis par push depuis SIR, ces données peuvent être identifiées à l'aide de sources qui feront référence à l'incident de sécurité lié à l'observable.
- **Dans une opération push automatique** : l'observable ou les données d'enrichissement seront automatiquement transmises lorsqu'ils seront associés à un incident de sécurité.

  Remarque : L'option Envoyer l'observable à TISC disparaît une fois le flux automatisé activé.

- **Le contexte TISC** affiche tous les observables SIR associés qui sont également présents dans TISC.
- En utilisant le contexte TISC, les analystes SIR peuvent voir toutes les données d'enrichissement TISC, y compris les recherches de menaces, la recherche de perception et les résultats d'enrichissement des observables.
- **Afficher les informations associées** affiche toutes les données d'enrichissement observables associées des observables sélectionnés.

10. Affichez les résultats.

Envoyer une recherche de menace à TISC

À l'aide de cette fonctionnalité, l'analyste de sécurité peut transmettre les données de recherche de menaces de SIR à TISC. À l'aide du contexte TISC, vous pouvez vérifier si

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les résultats de la recherche de menaces sont présents dans TISC. Dans le cas contraire, l'analyste de sécurité peut transmettre les données par push chaque fois que nécessaire.

Avant de commencer

Rôle requis : sn_si.analyst

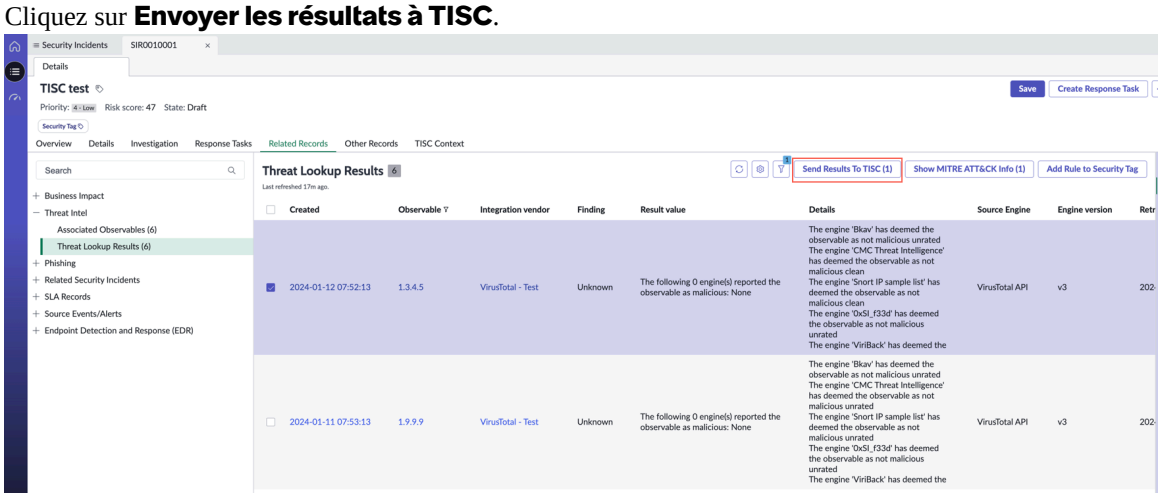
Procédure

1. Accédez à l'onglet **Enregistrements connexes** dans l'espace de travail SIR pour effectuer l'action d'aptitude d'intégration TISC.

   Remarque :

   - Vous pouvez également accéder à l'onglet **Examiner** , à la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionner **Observables associés** pour effectuer l'opération push.
   - Dans l'onglet **Examiner** , cliquez sur **Afficher les informations associées** pour afficher toutes les données de recherche de menaces, de recherche de perception et d'enrichissement associées à l'observable sélectionné. Pour plus d'informations, consultez Explorer le canevas d'examen.

2. Sélectionner **Connaissance de la menace** > **Résultats de la recherche de menace** pour effectuer l'opération push et transmettre manuellement les données dans TISC.
3. Sélectionnez un ou plusieurs enregistrements des résultats de la recherche de menace.
4. Cliquez sur **Envoyer les résultats à TISC**.



Remarque :

- Si l'observable de recherche de menace sélectionné n'est pas présent dans TISC, en mode manuel, l'observable est d'abord créé en tant que source d'observable, puis une fois que l'observable source a créé un enregistrement d'observable TISC, l'enregistrement de l'observable est automatiquement associé à l'observable nouvellement créé. En outre, la recherche de menaces sélectionnée sera également transmise à l'observable de recherche de menaces nouvellement créé en mode manuel.
- En mode automatique, les observables ne seront pas transmis par push si l'observable est présent, les recherches de menaces seront alors transmises automatiquement. Si les observables ne sont pas présents, les recherches de menaces ne sont pas transmises.

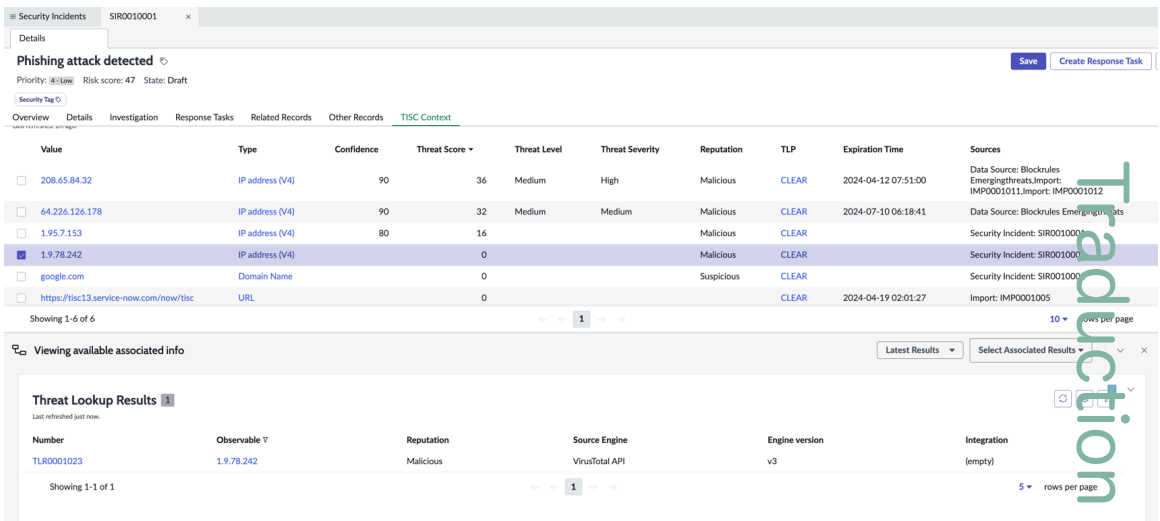
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Un message de confirmation s'affiche que l'observable (1.9.78.242) pour l'enregistrement de recherche de menace sélectionné n'existe pas dans TISC. La création d'un observable et l'association automatique de l'enregistrement de recherche de menace observable dans TISC prennent un certain temps.
   Une fois traité et transmis, vous pouvez voir les résultats.
6. Sélectionnez **un contexte TISC**.

Remarque : :

- Vous voyez maintenant l'observable qui est transmis à TISC à partir de l'application SIR.



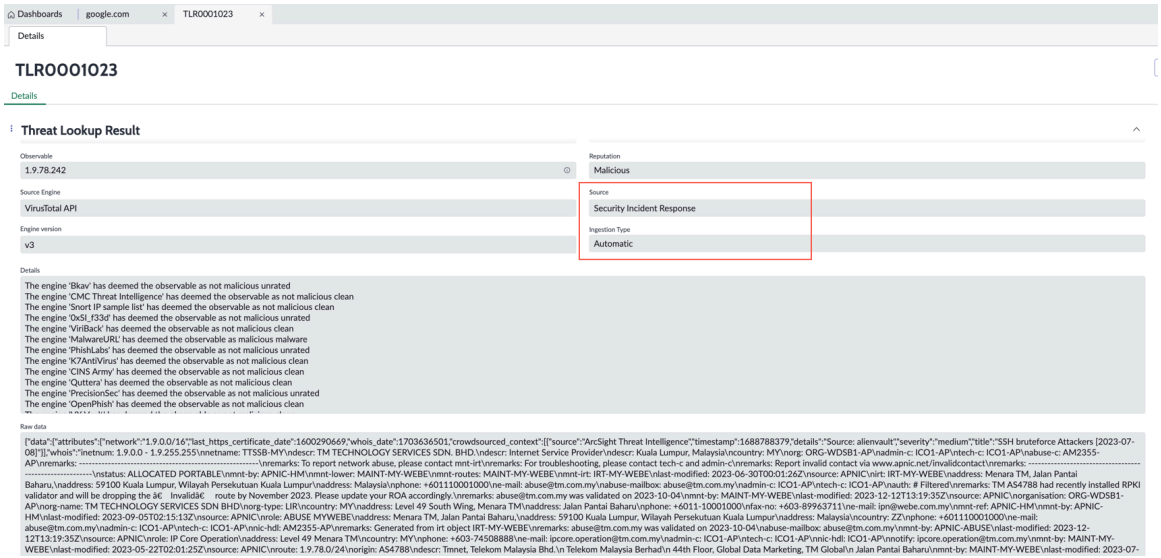
- **Dans le cas d'une opération push manuelle** : les données observables ne peuvent être transmises par push que si elles sont liées aux incidents de sécurité. Une fois que l'observable est transmis par push depuis SIR, ces données peuvent être identifiées à l'aide de sources qui feront référence à l'incident de sécurité lié à l'observable.
- **Dans une opération push automatique** : l'observable ou les données d'enrichissement sont automatiquement transmises lorsqu'elles sont associées à un incident de sécurité.
- **Le contexte TISC** affiche tous les observables SIR associés qui sont également présents dans TISC.
- En utilisant le contexte TISC, les analystes SIR peuvent voir toutes les données d'enrichissement TISC, y compris les recherches de menaces, la recherche de perception et les résultats d'enrichissement des observables.
- **Afficher les informations associées** affiche toutes les données d'enrichissement observables associées des observables sélectionnés.

7. La vue de liste affiche tous les résultats de la recherche de menaces. Cependant, sélectionnez n'importe quel enregistrement et cliquez sur le bouton **Afficher les informations associées** .
8. Affichez les résultats de la recherche de menaces.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Cliquez sur un enregistrement de résultats de recherche de menaces pour l'afficher dans la vue de formulaire, qui affiche également le type d'envoi ou **d'ingestion** (automatique ou manuelle) et la **source** sera Réponse aux incidents de sécurité.



Envoyer la recherche de perception à TISC

Grâce à cette fonctionnalité, l'analyste de sécurité peut transférer les données de recherche de perception de SIR vers TISC. À l'aide du contexte TISC, l'analyste peut vérifier si les données de recherche de perception sont présentes dans TISC. Dans le cas contraire, l'analyste de sécurité peut transmettre les données par push chaque fois que nécessaire.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à l'onglet **Enregistrements connexes** dans l'espace de travail SIR pour effectuer l'action d'aptitude d'intégration TISC.

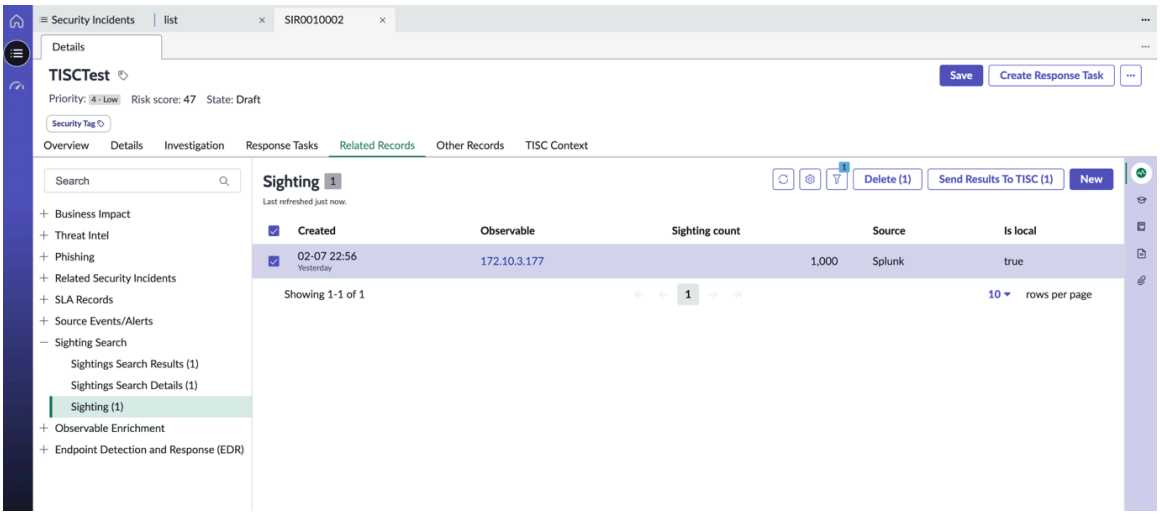
   Remarque :

   - Vous pouvez également accéder à l'onglet **Examiner** , à la section **Listes de points d'entrée** affichée sur le côté gauche de la page et sélectionner **Observables associés** pour effectuer l'opération push.
   - Dans l'onglet **Examiner** , cliquez sur **Afficher les informations associées** pour afficher toutes les données de recherche de menaces, de recherche de perception et d'enrichissement associées à l'observable sélectionné. Pour plus d'informations, consultez Explorer le canevas d'examen.

2. Sélectionner **Recherche de perception** > **Résultats de recherche de perception** pour effectuer l'opération push et transmettre manuellement les données dans TISC.
3. Sélectionnez un ou plusieurs enregistrements Résultats de recherche de perception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

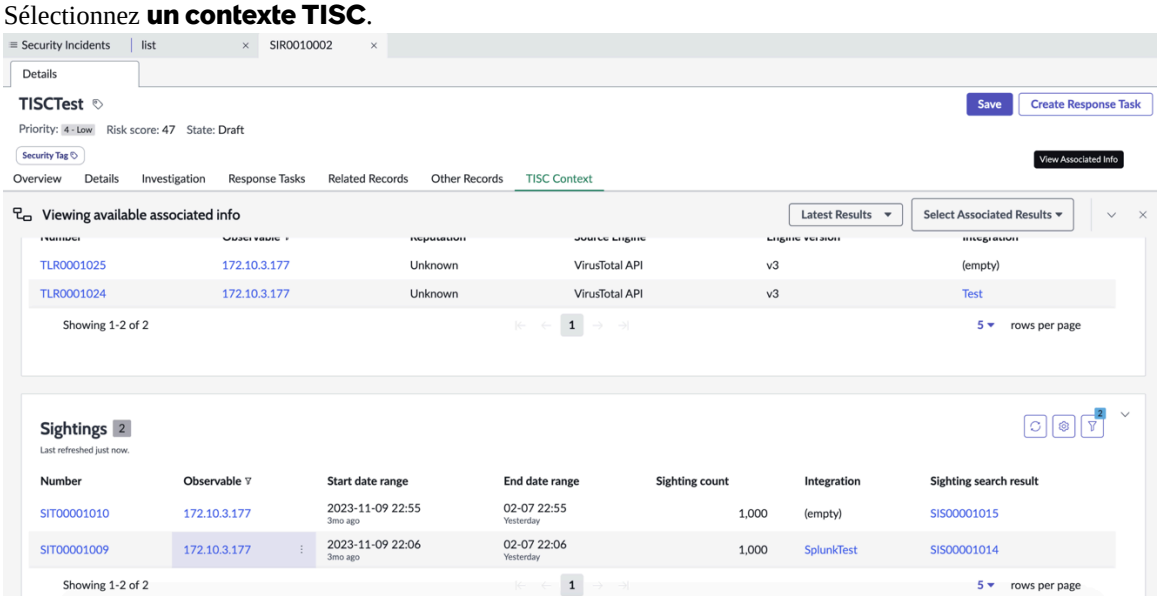


4. Cliquez sur **Envoyer les résultats à TISC**.

Remarque :

- Si l'observable de recherche de perceptions sélectionné n'est pas présent dans TISC, en mode manuel, l'observable est d'abord créé en tant que source d'observable, puis une fois que l'observable source a créé un enregistrement d'observable TISC, l'enregistrement de l'observable est automatiquement associé à l'observable nouvellement créé. En outre, la recherche de perception sélectionnée sera également poussée vers l'observable de recherche de menace nouvellement créé en mode manuel.
- En mode automatique, les observables ne seront pas transmis par push si l'observable est présent, les recherches de menaces seront alors transmises automatiquement. Si les observables ne sont pas présents, les recherches de menaces ne sont pas transmises.

5. Sélectionnez **un contexte TISC**.



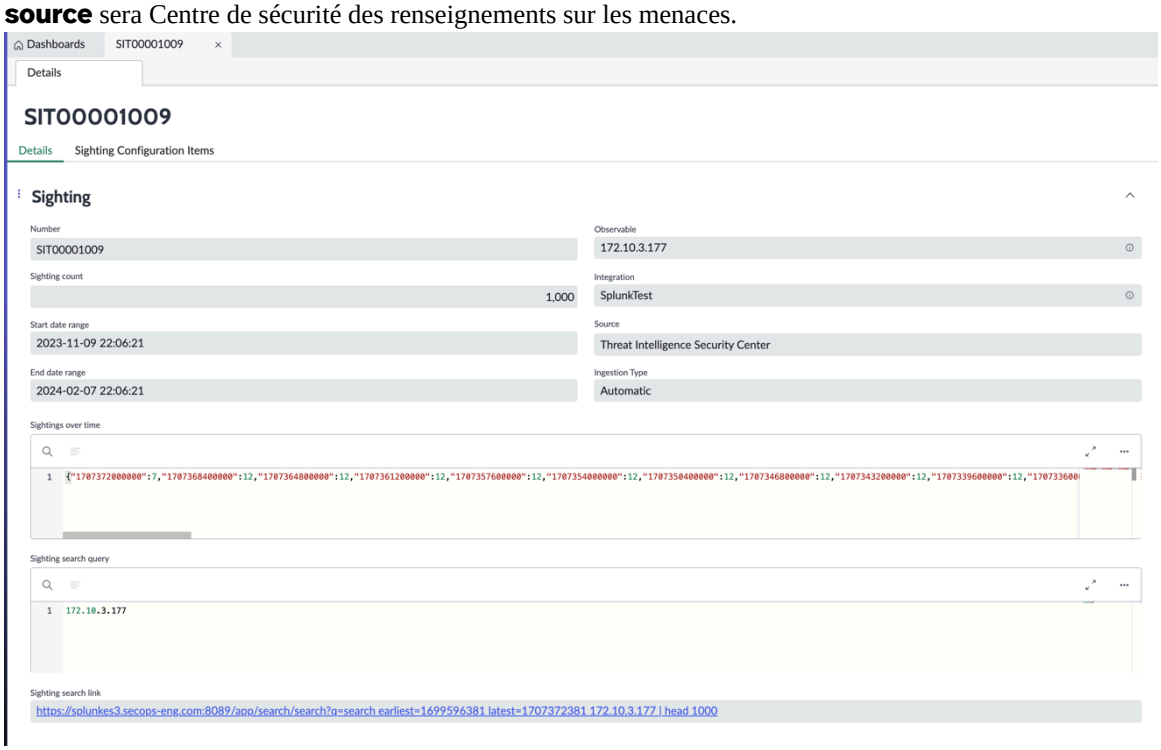
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : :

- Vous voyez maintenant l'observable qui est transmis à TISC à partir de l'application SIR.
- **Dans le cas d'une opération push manuelle** : les données observables ne peuvent être transmises par push que si elles sont liées aux incidents de sécurité. Une fois que l'observable est transmis par push depuis SIR, ces données peuvent être identifiées à l'aide de sources qui feront référence à l'incident de sécurité lié à l'observable.
- **Dans une opération push automatique** : l'observable ou les données d'enrichissement seront automatiquement transmises lorsqu'ils seront associés à un incident de sécurité.
- **Le contexte TISC** affiche tous les observables SIR associés qui sont également présents dans TISC.
- En utilisant le contexte TISC, les analystes SIR peuvent voir toutes les données d'enrichissement TISC, y compris les recherches de menaces, la recherche de perception et les résultats d'enrichissement des observables.
- **Afficher les informations associées** affiche toutes les données d'enrichissement observables associées des observables sélectionnés.

6. Une fois l'enregistrement traité, sélectionnez-le, puis cliquez sur **Afficher les informations associées**.
7. Affichez les résultats.
8. Cliquez sur n'importe quel enregistrement des résultats de recherche de perception pour l'afficher dans la vue de formulaire, qui affiche également le type d'envoi ou **d'ingestion** (automatique ou manuelle) et la **source** sera Centre de sécurité des renseignements sur les menaces.



Envoyer l'enrichissement de l'observable à TISC

Grâce à cette fonctionnalité, l'analyste de sécurité peut transférer les données de recherche de perception de SIR vers TISC. À l'aide du contexte TISC, l'analyste peut vérifier si les données de recherche de perception sont présentes dans TISC. Dans le cas

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

contraire, l’analyste de sécurité peut transmettre les données par push chaque fois que nécessaire.

Avant de commencer

Rôle requis : sn_si.analyst

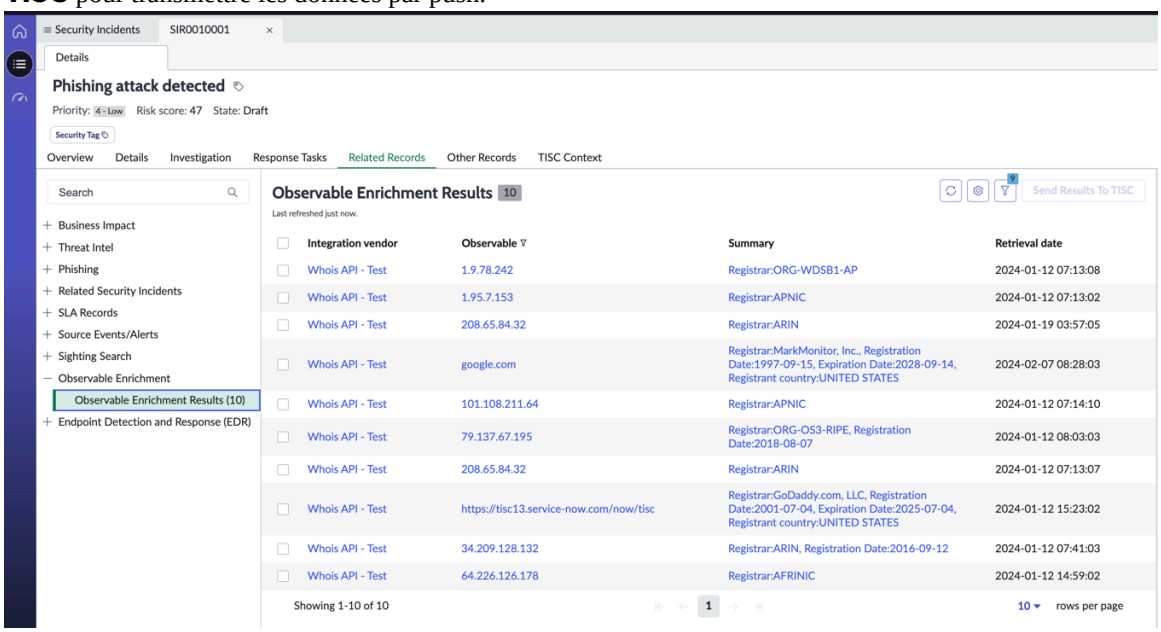
Procédure

1. Accédez à l’onglet **Enregistrements connexes** dans l’espace de travail SIR pour effectuer l’action d’aptitude d’intégration TISC.

   Remarque :

   - Vous pouvez également accéder à l’onglet **Examiner** , à la section **Listes de points d’entrée** affichée sur le côté gauche de la page et sélectionner **Observables associés** pour effectuer l’opération push.
   - Dans l’onglet **Examiner** , cliquez sur **Afficher les informations associées** pour afficher toutes les données de recherche de menaces, de recherche de perception et d’enrichissement associées à l’observable sélectionné. Pour plus d'informations, consultez Explorer le canevas d’examen.

2. Sélectionner **Enrichissement des éléments observables** > **Résultats de l'enrichissement de l'observable** pour effectuer l’opération push et transmettre manuellement les données dans TISC.
3. Sélectionnez un ou plusieurs enregistrements observables à effectuer l’opération **Envoyer les résultats à TISC** pour transmettre les données par push.



4. Cliquez sur **Envoyer les résultats à TISC**.

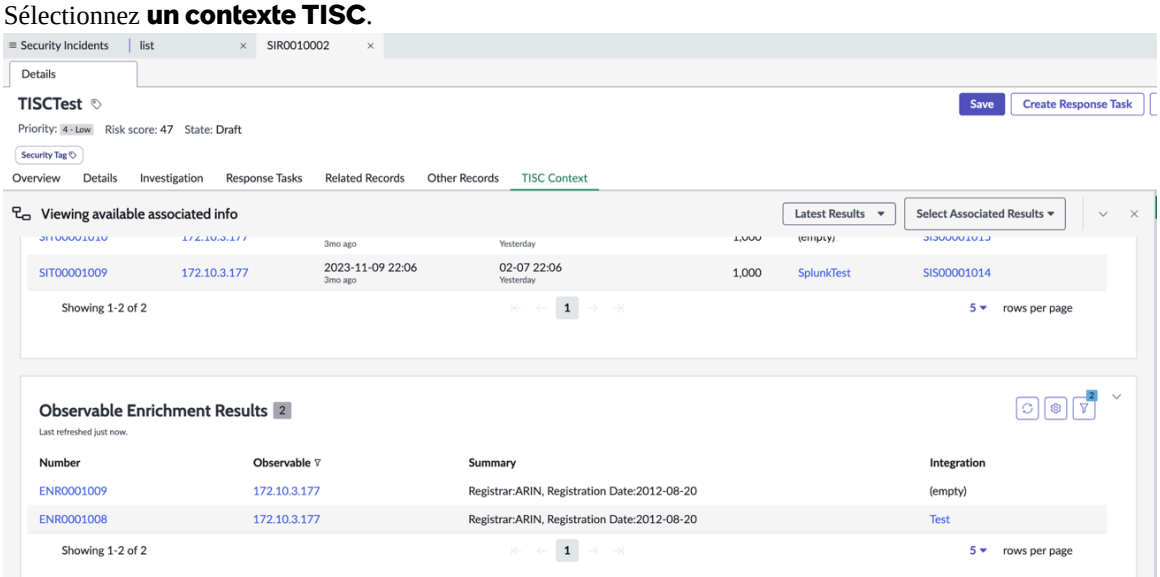
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si l'observable sélectionné n'est pas présent dans TISC, l'observable est d'abord créé en tant que source d'observable. Une fois que l'observable source a créé un enregistrement d'observable TISC, l'enregistrement de l'observable est automatiquement associé à l'observable nouvellement créé.
- Une fois l'opération push d'observable effectuée, un message d'information s'affiche indiquant que l'observable 0.0.0.0 est transmis avec succès à TISC. La conversion pour refléter dans l'onglet de contexte TISC peut prendre un certain temps.

5. Sélectionnez **un contexte TISC**.



Remarque : :

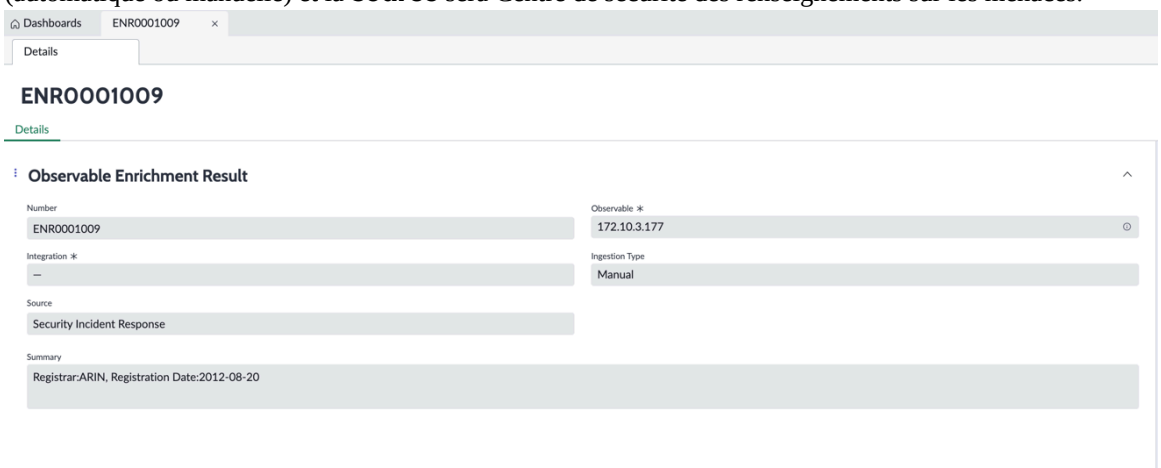
- Vous voyez maintenant l'observable qui est transmis à TISC à partir de l'application SIR.
- **Dans le cas d'une opération push manuelle** : les données observables ne peuvent être transmises par push que si elles sont liées aux incidents de sécurité. Une fois que l'observable est transmis par push depuis SIR, ces données peuvent être identifiées à l'aide de sources qui feront référence à l'incident de sécurité lié à l'observable.
- **Dans une opération push automatique** : l'observable ou les données d'enrichissement seront automatiquement transmises lorsqu'ils seront associés à un incident de sécurité.
- **Le contexte TISC** affiche tous les observables SIR associés qui sont également présents dans TISC.
- En utilisant le contexte TISC, les analystes SIR peuvent voir toutes les données d'enrichissement TISC, y compris les recherches de menaces, la recherche de perception et les résultats d'enrichissement des observables.
- **Afficher les informations associées** affiche toutes les données d'enrichissement observables associées des observables sélectionnés.

6. Affichez les résultats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur n'importe quel enregistrement des résultats d'enrichissement d'observables pour afficher l'enregistrement dans la vue de formulaire, qui affiche également le type d'envoi ou **d'ingestion** (automatique ou manuelle) et la **source** sera Centre de sécurité des renseignements sur les menaces.



Utilisation du contexte TISC

Le contexte TISC facilite l'affichage des données Threat Intelligence telles que les observables dans l'espace de travail de la Réponse aux incidents de sécurité.

Cela aide les analystes de sécurité à détecter, examiner et répondre plus efficacement aux incidents de sécurité à partir de l'espace de travail.

Le contexte TISC dans l'espace de travail Réponse aux incidents de sécurité permet aux analystes de sécurité d'ajouter des incidents de sécurité ou des observables au ou aux tickets TISC directement à partir de l'espace de travail, d'afficher également les résultats de l'enrichissement et d'afficher les informations connexes des observables, à savoir les acteurs de menace, les modèles d'attaque, les campagnes, et ainsi de suite.

À l'aide de cette section, vous pouvez effectuer les opérations suivantes :

1. Associez des observables à un ticket TISC.
2. Affichez les informations observables associées.
3. Affichez les résultats de l'enrichissement des observables.

Pour en savoir plus sur la procédure et la procédure, reportez-vous aux sections suivantes. Pour en savoir plus sur le fonctionnement de l'intégration entre les espaces de travail TISC et SIR, reportez-vous Intégration TISC à l'espace de travail SIR à la section Centre de sécurité des renseignements sur les menaces.

Ajouter des observables au ticket TISC

Utilisez cette section pour ajouter des incidents de sécurité ou des observables à un ticket TISC.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

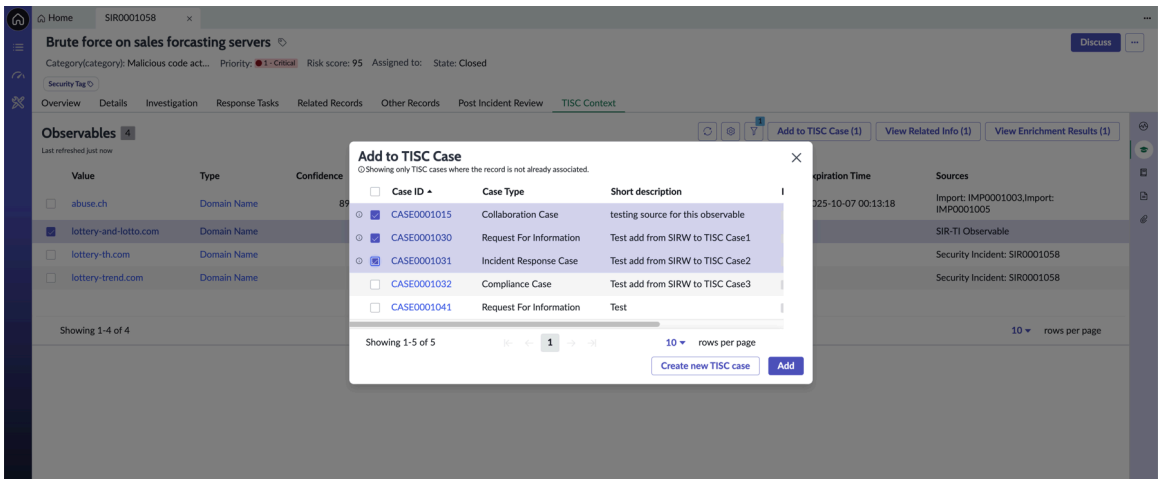
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tous**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez également rechercher l’ID de l’incident, filtrer à l’aide de la section Filtres rapides ou parcourir un état d’incident.

3. Sélectionnez **l’onglet Contexte TISC** .
4. Cliquez sur **le bouton Ajouter au ticket TISC** .
   La boîte de dialogue Ajouter au ticket TISC s’affiche et affiche uniquement les tickets TISC pour lesquels l’enregistrement n’est pas déjà associé.
5. Sélectionnez les observables.
6. Sélectionnez un ou des tickets et cliquez sur **Ajouter** pour ajouter les tickets aux observables et les associer à l’incident de sécurité.



Remarque : Vous pouvez également créer un nouveau ticket en cliquant sur **Créer un nouveau ticket TISC**, au cas où vous n’auriez pas de tickets existants.

Les messages de confirmation suivants s’affichent :

- Les observables suivants sont ajoutés avec succès en tant qu’artefacts.
- Les observables suivants sont envoyés à TISC et ajoutés par la suite aux enregistrements de tickets TISC sélectionnés.

Remarque : Le traitement et l’association des activités observables sont publiés dans le flux d’activité au fur et à mesure que l’association est terminée.

7. Affichez les enregistrements de tickets associés en vous connectant à l’espace de travail du Centre de sécurité des renseignements sur les menaces pour connaître les étapes suivantes.
   Pour plus d'informations, reportez-vous à la section Intégration TISC à l’espace de travail SIR.

Remarque :

Dans l’espace de travail Réponse aux incidents de sécurité, vous pouvez également associer des observables à des enregistrements de tickets à partir des onglets **Enquête** et **Enregistrements connexes** .

Remarque : Pour associer des observables à partir de **l’enquête**, suivez la procédure ci-dessous et pour associer des observables à partir des **enregistrements connexes** expliqués ici Ajouter des observables au ticket TISC. Vous pouvez également accéder à l’onglet **Examiner** , à la section **Listes de points d’entrée** affichée sur le côté gauche de la page et sélectionner **Observables associés** pour ajouter des observables au ticket TISC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les informations connexes à partir de TISC

Utilisez cette section pour afficher les informations connexes, telles que les acteurs de menace associés, les modèles d'attaque, les campagnes et les tickets de TISC dans l'espace de travail SIR.

Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tous**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.
   Cela peut également être fait en recherchant l'ID de l'incident, en naviguant à partir de la section Filtres rapides ou en filtrant l'état de l'incident.
3. Une fois l'incident ouvert, accédez à l'onglet **Contexte TISC** .
   Affichage des informations connexes :

   Dans les détails de l'incident, vous pouvez afficher les informations connexes dans plusieurs sections.

   a. Sélectionnez un ou plusieurs observables.

   b. Cliquez sur **le bouton Afficher les informations connexes** .
   Cette section affiche les informations associées aux observables sélectionnés.

Nom	Description
Acteurs de menace	Affiche les informations de TISC pour les acteurs de menace liées aux observables sélectionnés.
Schémas d'attaque	Affiche les informations de TISC relatives aux schémas d'attaque liés aux observables sélectionnés.
Campagnes	Affiche les informations de TISC pour les campagnes associées aux observables sélectionnés.
Tickets	Affiche les informations de TISC pour les tickets TISC liés aux observables sélectionnés.

Afficher les résultats de l'enrichissement

Utilisez cette section pour afficher les résultats de l'enrichissement des observables, tels que les résultats de la recherche de menace, les observations et les résultats d'enrichissement des observables de TISC dans l'espace de travail SIR.

Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Tous**.
2. Localisez et ouvrez tout incident de sécurité spécifique sur lequel vous enquêtez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cela peut également être fait en recherchant l'ID de l'incident, en naviguant à partir de la section Filtres rapides ou en filtrant l'état de l'incident.

3. Une fois l'incident ouvert, accédez à l'onglet **Contexte TISC** .
Affichage des résultats de l'enrichissement :

   Dans les détails de l'incident, vous pouvez afficher les informations connexes dans plusieurs sections.

   a. Sélectionnez un ou plusieurs observables.

   b. Cliquez sur le bouton **Afficher les résultats de l'enrichissement** .
   Cette section affiche les détails associés aux observables sélectionnés.

Nom	Description
Résultats de la recherche de menace	Répertorie tous les résultats de la recherche de menaces associées pour les observables TISC sélectionnés.
Perceptions	Répertorie toutes les perceptions associées pour les observables TISC sélectionnés.
Résultats de l'enrichissement de l'observable	Répertorie tous les résultats d'enrichissement d'observables associés pour les observables TISC sélectionnés.

Rapports dans Réponse aux incidents de sécurité

Tous les rapports associés à un incident de sécurité sont disponibles dans la section Rapports à des fins d'analyse et de partage.

L'analyste sera en mesure de :

- Créer un rapport
- Modifier un rapport
- Supprimer un rapport

Créer un rapport

Les analystes peuvent créer un rapport pour Réponse aux incidents de sécurité inclure le statut d'un incident et le partager par e-mail.

Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez un incident de sécurité.
3. **Sélectionnez Rapports**.

   La page **Rapport** affiche une liste de tous les rapports créés pour l'incident sélectionné.

4. Sélectionnez **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La page **Sélectionner un modèle** s'affiche avec une liste de tous les modèles publiés. La liste des modèles n'est disponible que lorsque l'administrateur a publié des modèles de rapports. Pour plus d'informations, consultez Créer un modèle de rapport dans Réponse aux incidents de sécurité.

5. Sélectionner un modèle de rapport.
   Le rapport s'ouvre en mode d'édition avec les données d'incident configurées dans le modèle.
6. Sélectionnez **Développer** et insérer/supprimer les champs souhaités.
   - **Champs SIR communs** : liste des champs les plus utilisés pour un incident.
   - **Tous les champs SIR** : tous les champs associés à un incident. Par exemple, lorsque vous générez un rapport d'incident et que vous souhaitez ajouter un champ appelé Description brève, vous pouvez sélectionner ce champ dans **Tous les champs SIR**. Lorsque vous ajoutez un champ, la description brève de l'incident est affichée dans le rapport.
   - **Enregistrements connexes** : les enregistrements connexes d'un incident particulier. Par exemple, si vous souhaitez ajouter des observables associés dans le rapport, vous pouvez l'ajouter à votre rapport. Ces enregistrements connexes sont affichés au format de table
   - **Scripts** : pour ajouter la date et l'heure du rapport, vous pouvez ajouter le script Date et heure actuelles à votre rapport. Cela ajoutera la date et l'heure de création du rapport dans le rapport.
7. Sélectionnez **Aperçu** pour afficher un aperçu du rapport.
8. Sélectionnez **Enregistrer le contenu** pour enregistrer les modifications.
9. **Facultatif :** Sélectionnez l'icône Modifier les détails du rapport pour mettre à jour le nom et la description du rapport.
10. Sélectionnez **Publier** pour publier le rapport.
11. Sélectionnez l'icône Partager le rapport par e-mail.
    a. Saisissez les e-mails du destinataire dans les champs **À** et **Cc/Cci** .
    b. Mettez à jour **l'objet et le corps de l'e-mail**.
    c. Sélectionnez **Envoyer** pour partager le rapport par e-mail.

Modifier un rapport

Les analystes peuvent modifier un rapport non publié et Réponse aux incidents de sécurité le partager par e-mail.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez un incident de sécurité.
3. **Sélectionnez Rapports**.

   La page **Rapport** affiche une liste de tous les rapports créés pour l'incident sélectionné.
4. Ouvrez le rapport pour le mettre à jour.
   Le rapport s'ouvre en mode d'édition avec les données d'incident configurées dans le modèle.
5. Modifiez le rapport selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez **Aperçu** pour afficher un aperçu du rapport.
7. Sélectionnez **Enregistrer le contenu** pour enregistrer les modifications.
8. **Facultatif :** Sélectionnez l'icône Modifier les détails du rapport pour mettre à jour le nom et la description du rapport.
9. Sélectionnez **Publier** pour publier le rapport.
10. Sélectionnez l'icône Partager le rapport par e-mail icône  .
    a. Saisissez les e-mails du destinataire dans les champs **À** et **Cc/Cci** .
    b. Mettez à jour **l'objet et le corps de l'e-mail**.
    c. Sélectionnez **Envoyer** pour partager le rapport par e-mail.

Supprimer un rapport

Vous pouvez supprimer un rapport dont Réponse aux incidents de sécurité l'état est publié ou brouillon.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez un incident de sécurité.
3. **Sélectionnez Rapports**.

   La page **Rapport** affiche une liste de tous les rapports créés pour l'incident sélectionné.
4. Ouvrez le rapport à supprimer.
5. Sélectionnez **Supprimer**.
   Un message de confirmation s'affiche.
6. Sélectionnez **Supprimer** pour supprimer le rapport.

Collaborer par téléconférence ou messagerie instantanée dans Réponse aux incidents de sécurité

Vous pouvez collaborer avec des analystes et des utilisateurs affectés pour résoudre un incident Réponse aux incidents de sécurité dans l'application ou en discuter.

Information associée

Commencer une téléconférence dans Security Incident Response

Lancer une conversation dans la barre latérale dans Security Incident Response

Commencer une téléconférence dans Security Incident Response

Grâce à la téléconférence, les analystes de sécurité peuvent collaborer en temps réel avec d'autres analystes et les utilisateurs concernés. Ces appels facilitent l'échange d'informations pour aider à résoudre les incidents.

Avant de commencer

Assurez-vous d'avoir installé et activé les applications et modules d'extension suivants :

Traduction automatique

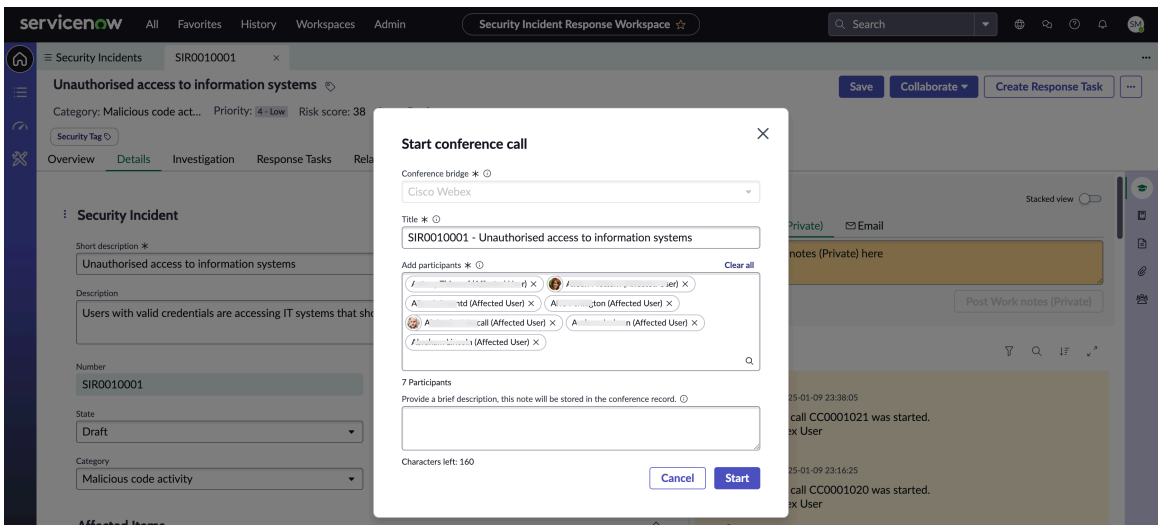
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Module d’extension Notification (com.snc.notify).
- Composants d’interface utilisateur de notification pour l’application Espaces de travail configurables.
- Module d’extension Visual Task Board (com.devsnc.snb_vtb)

Rôle requis : sn_si.analyst ou sn_si.manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez un incident de sécurité pour lequel vous souhaitez lancer une téléconférence.
3. Sélectionnez **Collaborer**, puis **Démarrer un appel**, ou vous pouvez sélectionner l’icône , puis sélectionner l’icône +.



La fenêtre contextuelle Démarrer la téléconférence s’affiche.

4. Sélectionnez un pont de conférence dans le champ **Pont de conférence** .
5. Donnez un titre à la téléconférence dans **Titre**.

> **Remarque :** Par défaut, le titre de l’incident est renseigné comme titre de l’appel. Vous pouvez modifier le titre par défaut.

6. Ajoutez ou supprimez des participants à un appel dans **Ajouter des participants**.

> **Remarque :** Selon la configuration dans les paramètres de Téléconférence, une liste préremplie de participants est ajoutée à **Ajouter des participants** ou une liste de participants **de recommandations** est disponible. Pour plus d'informations, consultez Gérer les utilisateurs et les groupes de téléconférence.

7. Fournissez une brève description du début de la téléconférence.
8. Sélectionnez **Démarrer**.

La téléconférence commence sur le pont de conférence sélectionné. Tous les participants reçoivent une notification par e-mail et via le pont de conférence. Les participants peuvent utiliser le lien ou la notification pour rejoindre l’appel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Ouvrez l'incident associé dans Réponse aux incidents de sécurité l'application pour afficher les détails de la téléconférence.
10. **Facultatif :** Sélectionnez **Copier l'invitation** pour ajouter des participants à un appel actif.
11. Sélectionnez **Mettre fin à l'appel**.
    Lorsque le dernier participant quitte la téléconférence, l'appel prend fin
12. **Facultatif :** Pour redémarrer une téléconférence, accédez à la section **Terminé** et sélectionnez l'option **Réinitier** de la téléconférence requise.

Ajouter des participants à la téléconférence active

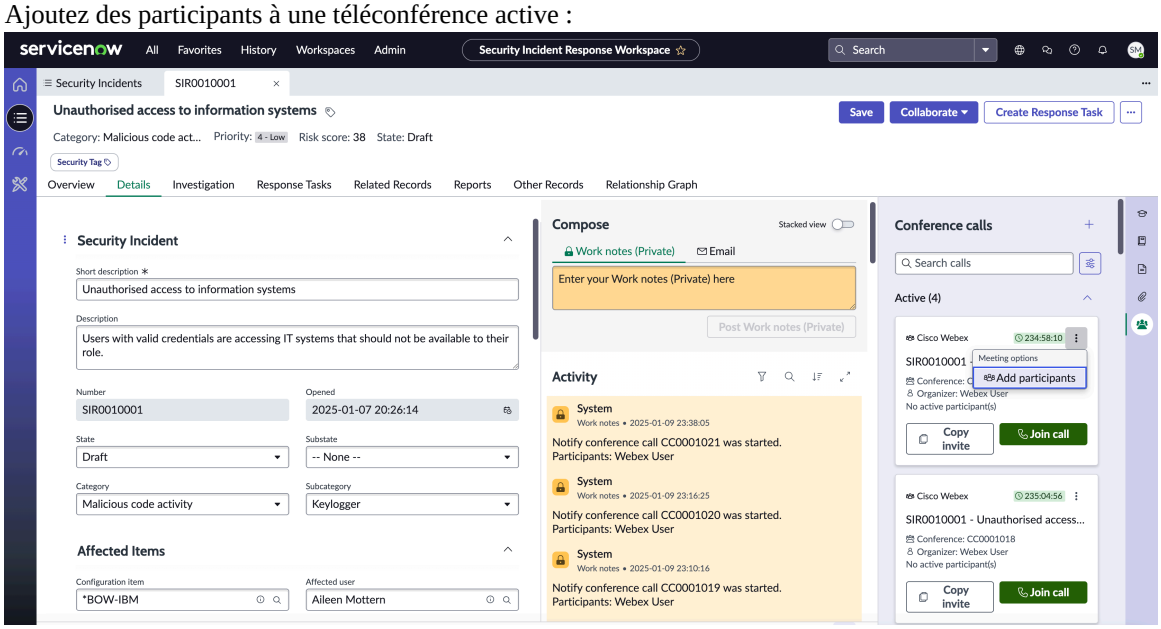
Vous pouvez ajouter des participants à une téléconférence active si vous ne les avez pas ajoutés avant de commencer la téléconférence.

Avant de commencer

Rôle requis : sn_si.analyste,sn_si.manager

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez l'incident de sécurité pour lequel vous souhaitez lancer une téléconférence.
3. Sélectionnez l'icône Téléconférence pour afficher les détails des téléconférences.
4. Ajoutez des participants à une téléconférence active :



   - Sélectionnez l'icône Options de la réunion ⋮ pour la téléconférence active et sélectionnez **Ajouter des participants**.
   - Sélectionnez **Copier l'invitation** dans la section **Téléconférences** et partagez l'invitation avec les participants requis.

Lancer une conversation dans la barre latérale dans Security Incident Response

À l'aide de Sidebar, les analystes de sécurité peuvent collaborer avec d'autres personnes en temps réel sur la base d'un enregistrement basé sur l'interaction ou une tâche de l'espace de travail. Ces discussions facilitent l'échange d'informations et de connaissances pour aider à résoudre les problèmes plus rapidement et avec des résultats de meilleure qualité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_si.read

Vérifiez que vous avez activé le module d'extension Ensemble de fonctionnalités standard omni-expérience. Pour plus d'informations, consultez Installer Barre latérale .

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez l'icône Vue de liste de la vue de .
3. Ouvrez un incident de sécurité pour lequel vous souhaitez lancer une discussion dans la barre latérale.
4. Sélectionnez **Collaborer**, puis **Démarrer la messagerie instantanée**.
   La boîte de dialogue Démarrer une discussion dans la barre latérale s'affiche.

   Remarque : L'intégration de Sidebar à Microsoft Teams permet aux utilisateurs de Sidebar et de Microsoft Teams de communiquer entre eux à partir de leurs plateformes respectives. Pour plus d'informations, consultez Barre latérale et Microsoft Teams .

5. Dans la boîte de dialogue Démarrer une discussion dans la barre latérale, renseignez les champs.

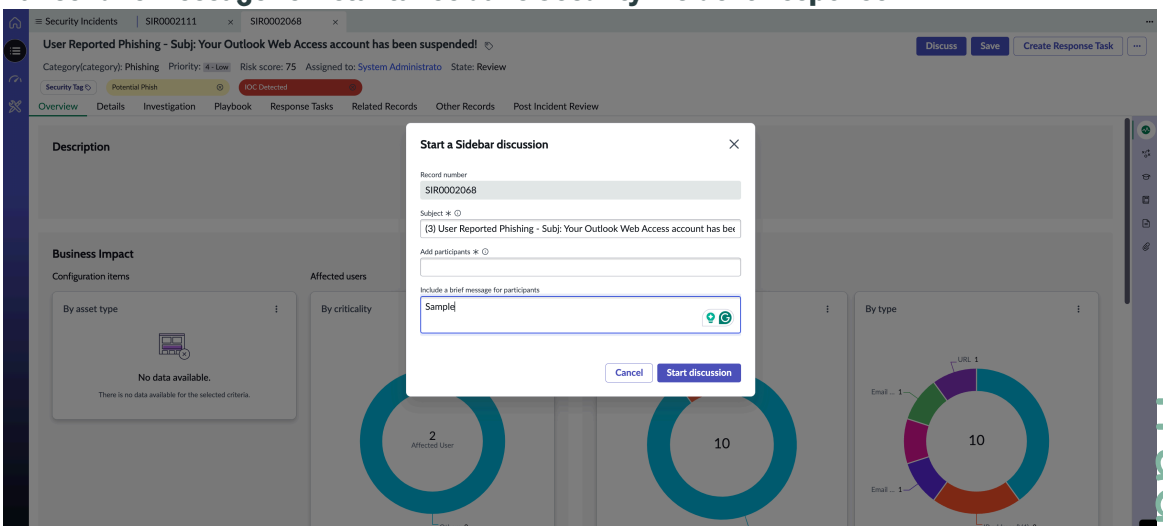
Champ	Description
Numéro d'enregistrement	Le numéro de tâche ou d'incident associé à la discussion dans la barre latérale.
Objet	Donnez un titre à la discussion dans la barre latérale.
Ajouter des participants	Option permettant d'ajouter des participants à la discussion dans la barre latérale. Si vous avez intégré la messagerie instantanée Sidebar à Microsoft Teams, vous pouvez également ajouter des participants à partir de Microsoft Teams. **Remarque :** ○ Vous devez ajouter au moins un participant pour créer une nouvelle discussion. ○ Si Sidebar et Microsoft Teams sont intégrés, les utilisateurs de Microsoft Teams sont différenciés des utilisateurs de Sidebar par une icône Microsoft Teams. ○ Par défaut, tous les utilisateurs disposant d'un accès en lecture aux enregistrements SIR auront également accès aux messageries instantanées de barre latérale, mais cela peut être contrôlé à l'aide de la requête de membre. Pour plus d'informations, consultez Configuration de la Barre latérale requête de membre .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Inclure un bref message	Résumez brièvement la question qui sera abordée dans la discussion de la barre latérale.

Lancer une messagerie instantanée dans Security Incident Response



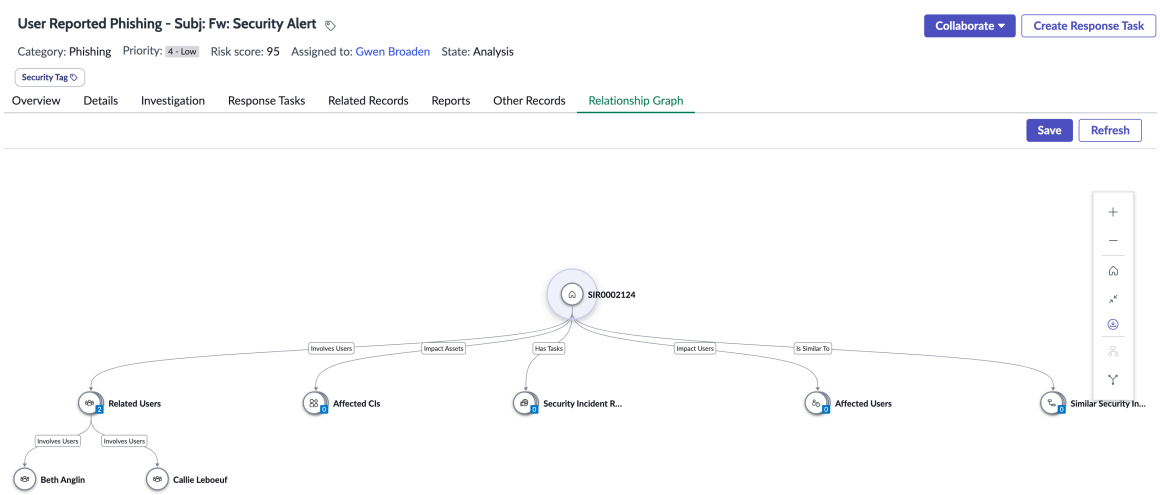
6. Sélectionnez **Démarrer une discussion**.
7. Vous pouvez effectuer une configuration supplémentaire comme des actions rapides.
   Pour limiter l'utilisation de l'action, vous pouvez utiliser le champ **Appliquer au groupe** sur la page d'action rapide. Pour plus d'informations, consultez Création d'une action rapide .

Afficher les détails d'un incident avec un graphique des relations

Les graphiques de relations dans l'espace de Réponse aux incidents de sécurité travail affichent visuellement les connexions entre un incident de sécurité et ses éléments connexes pour vous aider à analyser le contexte complet d'un incident de sécurité.

Les éléments associés à un incident de sécurité peuvent inclure des observables associés, des éléments de configuration (CI), des incidents de sécurité similaires (SIR), des tâches de réponse et d'autres listes connexes.

L'exemple de graphe des relations suivant affiche les détails d'un incident de sécurité.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous ouvrez un graphe de relations pour un incident de sécurité, les configurations disponibles sont visibles par défaut. Vous pouvez interagir avec le graphique comme suit :

- Zoomez sur n'importe quel objet, entrez dans l'écran et faites glisser les nœuds.
- Ajoutez des sous-nœuds pour chaque nœud, si disponible, et affichez les détails des sous-nœuds.
- Masquez tout nœud ou sous-nœud du graphique.
- Affichez les détails d'un sous-nœud.

Personnaliser un graphique relationnel

Visualisez et analysez les incidents de sécurité et leurs données associées dans un graphe des relations.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Espaces de travail** > **Espaces de travail de Réponse aux incidents de sécurité** > **Administration**.
2. Sélectionnez **Graphe des relations**, puis **Configurations des graphes des relations**.
3. Sélectionnez **Nouveau**.
4. Remplissez les champs du formulaire.

Configurations des graphes des relations

Champ	Description
Nom de la table connexe	Table à partir de laquelle vous souhaitez extraire les données observables de l'incident de sécurité, par exemple la table Associer l'observable [sn_ti_observable] ou la table Incident de sécurité [sn_si_incident].
Étiquette du nœud	L'étiquette de nœud de l'observable qui apparaît sur le graphe des relations. La valeur fournie automatiquement dépend de la table connexe sélectionnée.
Actif	Option permettant d'activer la configuration.
Étiquette du nœud de données	Étiquette primaire et étiquette secondaire à afficher sur le nœud pour la liste connexe sélectionnée.
Visible par défaut	Option permettant d'afficher l'étiquette du nœud de données.
Étiquette de la relation	La relation entre un nœud et le nœud de lien à afficher sur le graphe des relations.

5. Sélectionnez **Enregistrer**.

Créer un graphe des relations pour un incident

Créez un graphe Réponse aux incidents de sécurité de relations de nœud afin de mieux analyser un incident de sécurité en le corrélant avec des observables malveillants, des éléments

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de configuration (CI), des incidents de sécurité similaires (SIR), des tâches de réponse et d'autres informations connexes.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Pour plus d'informations sur la création d'un graphe relationnel personnalisé plutôt que d'utiliser un graphe prédéfini, reportez-vous à la section Personnaliser un graphique relationnel.

Remarque : Les changements apportés au graphe des relations ne sont pas enregistrés automatiquement.

Procédure
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez un incident de sécurité.
3. Sélectionnez l'onglet **Graphe des relations** .
4. Dans le graphe de relations, sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) sur le nœud parent, puis sélectionnez **Ajouter des nœuds**.
5. Sélectionnez un ou plusieurs nœuds de catégorie à afficher dans le graphique des relations, tels que Utilisateurs associés, CI affectés, Incidents de sécurité similaires (SIR) ou Utilisateurs affectés.

   Remarque : Vous pouvez sélectionner plusieurs nœuds de catégorie.

6. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) un nœud de catégorie, puis sélectionnez **Lier les nœuds** pour ajouter des données associées au nœud de catégorie.

   Remarque : Vous pouvez appliquer des filtres pour réduire le nombre d'éléments dans la liste.

   Une liste de tous les enregistrements connexes pour le nœud de catégorie sélectionné s'affiche. Par exemple, si vous sélectionnez **Utilisateurs affectés** dans la catégorie de nœud, la liste de tous les utilisateurs affectés par cet incident s'affiche.
7. Sélectionnez les enregistrements souhaités dans la liste et sélectionnez **Ajouter**.
8. Sélectionnez **Ajouter**.
9. **Facultatif :** Effacez les changements si nécessaire en sélectionnant **Actualiser**.
10. Sélectionnez **Enregistrer**.

    Remarque : Les changements apportés aux filtres sont également enregistrés lorsque vous enregistrez le graphique des relations.

11. **Facultatif :** Affichez les détails d'un sous-nœud.
    a. Sélectionnez un sous-nœud.
    b. Sélectionnez **Afficher les détails**.
12. **Facultatif :** Téléchargez la carte sur votre système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Si seule une partie de la carte est visible à l'écran et que vous souhaitez que tout l'écran soit inclus dans le PDF, sélectionnez l'icône Adapter à l'écran ( ).

> **Remarque :** Seule la partie de la carte qui apparaît à l'écran est incluse dans le fichier PDF.

b. Sélectionnez l'icône Exporter la carte (icône).

Example: Vidéo montrant comment modifier un graphe de relations pour ajouter des nœuds et des sous-nœuds de catégorie

https://player.vimeo.com/video/1095955062?h=593c16e2b6&badge=0&autopause=0&player_id=0&app_id=58479

Playbook d'incident de sécurité

Appeler le flux du playbook d'incident de sécurité automatiquement ou manuellement.

Un Playbook n'est visible que si au moins un Playbook est associé à un incident de sécurité. Le composant Playbook fonctionne uniquement pour les processus créés par Process Automation Designer (PAD) et non pour les flux créés par Flow Designer. Les flux existants activés par Flow Designer continuent de fonctionner et les activités continuent d'être restituées en tant que tâches de réponse.

Il existe deux façons d'associer le playbook à l'incident de sécurité :

- Invoquer automatiquement le playbook
- Ajouter manuellement un playbook

Appeler automatiquement le playbook

Pour qu'un Playbook soit appelé automatiquement, un processus doit être défini à l'aide de **Process Automation Designer (PAD)** et, lorsque la condition de déclenchement est remplie, l'onglet Playbook est automatiquement affiché avec les activités du playbook affichées.

Ajouter un playbook manuellement

Pour qu'un Playbook soit invoqué manuellement, accédez à la liste déroulante Action d'interface utilisateur du formulaire et sélectionnez **Ajouter un Playbook**. Pour plus d'informations, reportez-vous à la section Ajouter un Playbook

> **Remarque :** Si un playbook est déjà disponible, les nouveaux playbooks ajoutés s'exécuteront en parallèle des playbooks existants.

- Dans le playbook, l'analyste peut filtrer les cartes du playbook par état.
- L'analyste peut annuler un playbook en le sélectionnant à partir de l'icône Ellipse.
- Au sein de chaque activité, l'analyste pourra effectuer les actions définies dans les cartes d'activité telles que Ignorer, Marquer comme terminé, Annuler ou des actions d'orchestration telles que Soumettre au bac à sable, Rechercher des e-mails, etc.
- Chacune de ces actions est définie dans la définition d'activité, et la carte complète visible est personnalisable au moment de la création de la définition d'activité elle-même.

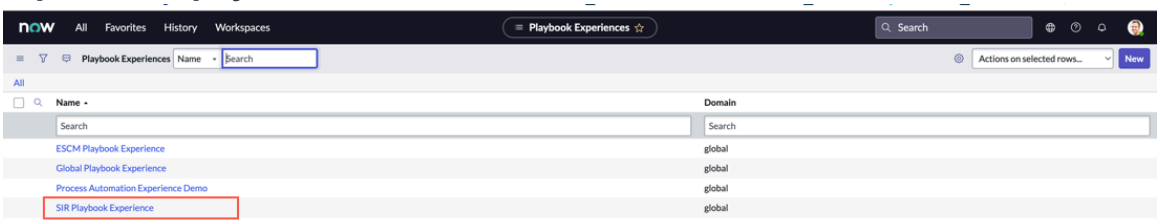
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Toutes les définitions d'activités futures et les prochaines étapes à effectuer sont affichées avec une icône de verrou et sont en mode lecture seule pour l'utilisateur. Le mode d'affichage du playbook est contrôlé par une configuration comme expliqué ci-dessous.

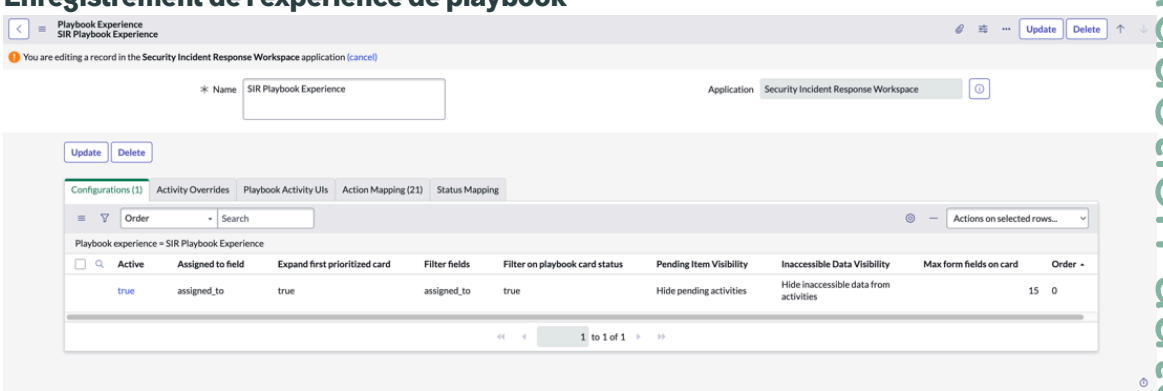
1. Accédez à la **Tous** > **Expériences Playbook**.
2. Sur la page Expériences de playbook, sélectionnez une **expérience de playbook SIR**.

Expérience de playbook

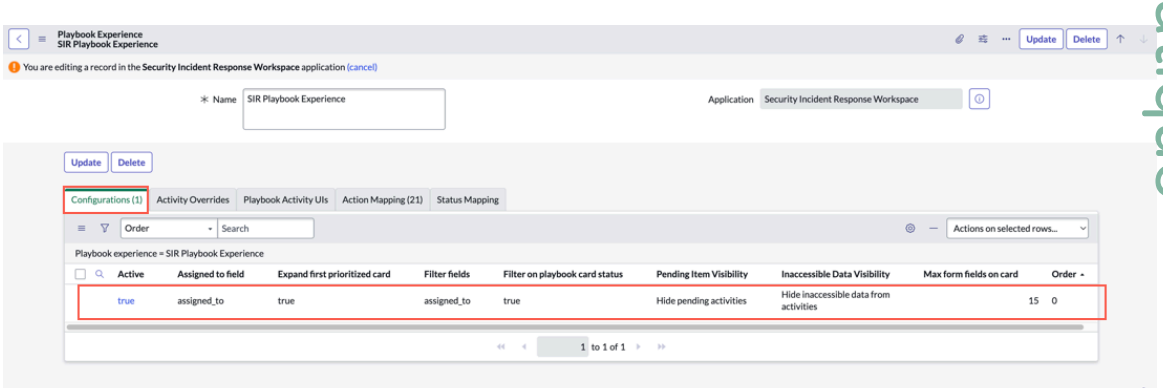


La page **Expérience de playbook SIR** s'affiche.

Enregistrement de l'expérience de playbook



3. Cliquez sur l'enregistrement de **configuration** .

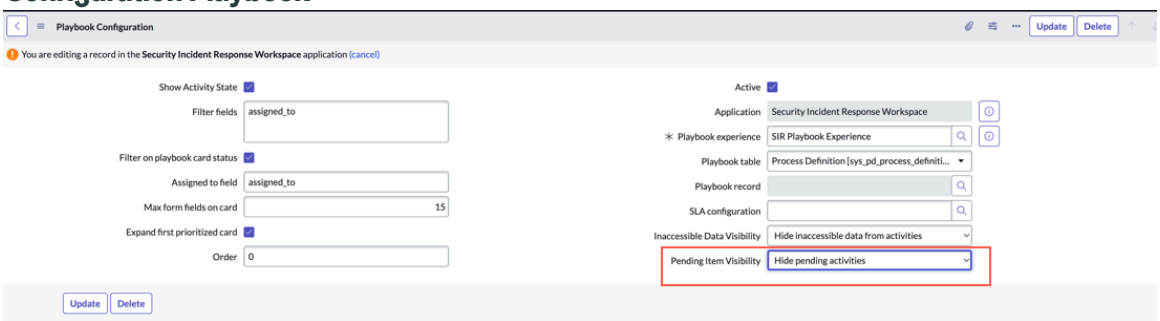


4. Dans l'onglet Configuration, cliquez sur Configuration de l'expérience de playbook SIR.

Traduction automatique

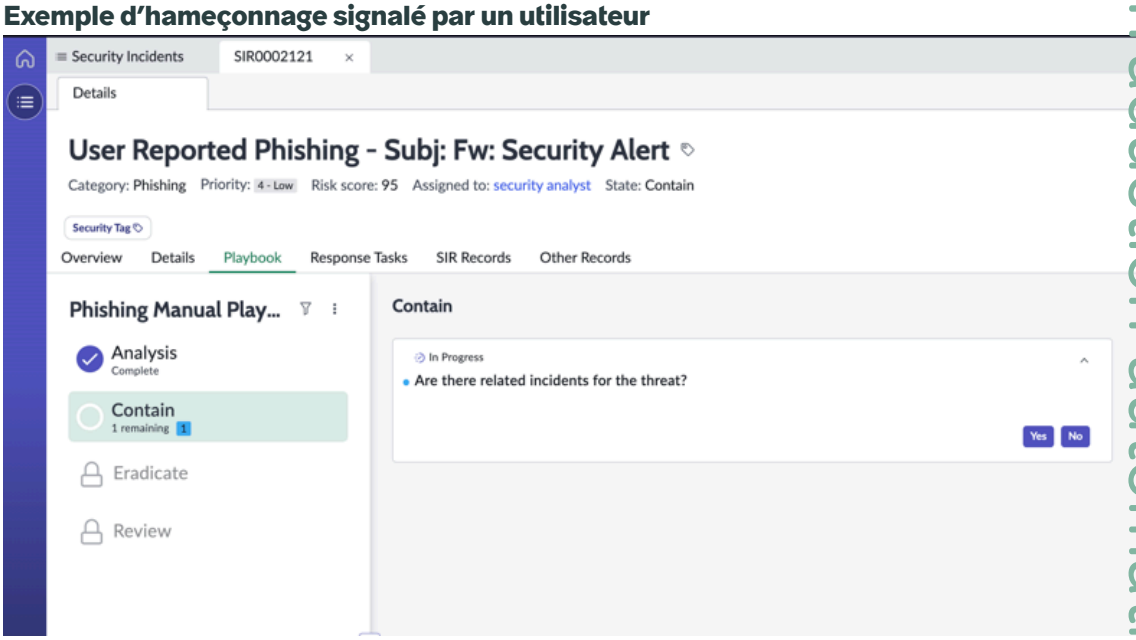
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration Playbook



5. Accédez à la liste déroulante du champ **Visibilité de l'élément en attente** , sélectionnez l'option souhaitée et enregistrez l'enregistrement. Choisissez parmi les options suivantes :
   - **Masquer les activités en attente** : sélectionnez cette option pour masquer les activités en attente que vous souhaitez afficher dans la section playbook de l'espace de travail.

Exemple d'hameçonnage signalé par un utilisateur

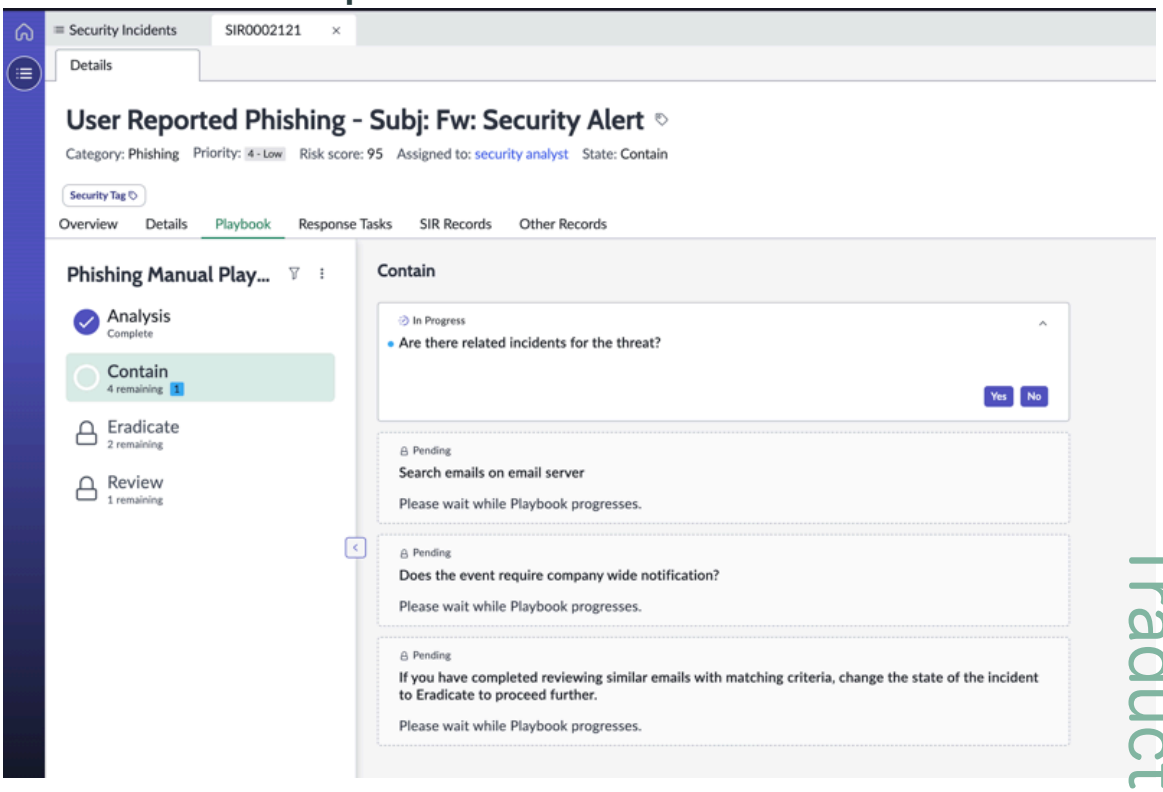


   - **Afficher les activités et étapes en attente** : sélectionnez cette option pour afficher les étapes et activités en attente que vous souhaitez afficher dans la section playbook de l'espace de travail.

Traduction automatique

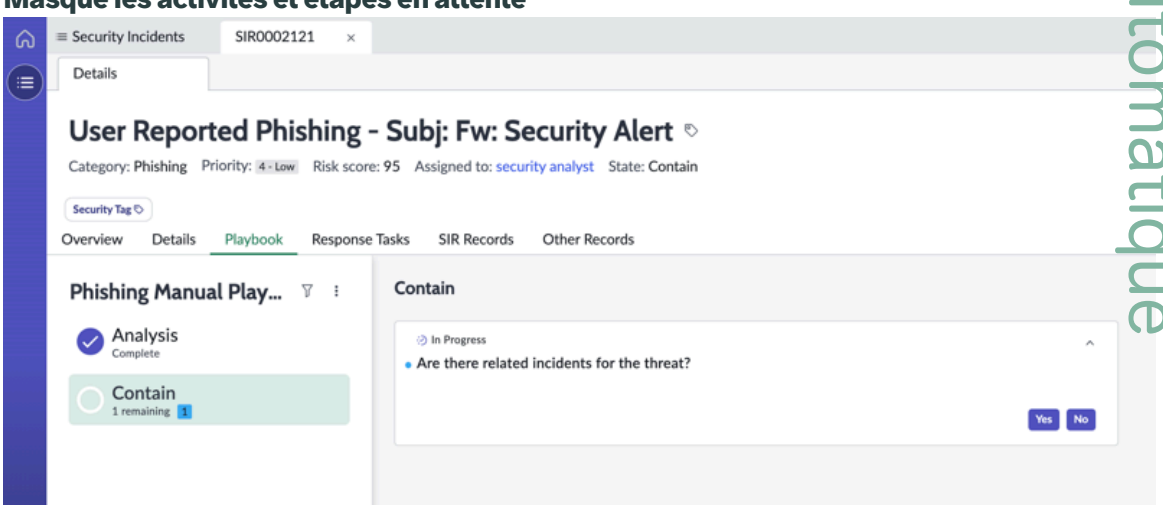
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les activités et étapes en attente



- **Masquer les activités et étapes en attente** : sélectionnez cette option pour masquer les activités et étapes en attente que vous souhaitez afficher dans la section playbook de l'espace de travail.

Masque les activités et étapes en attente

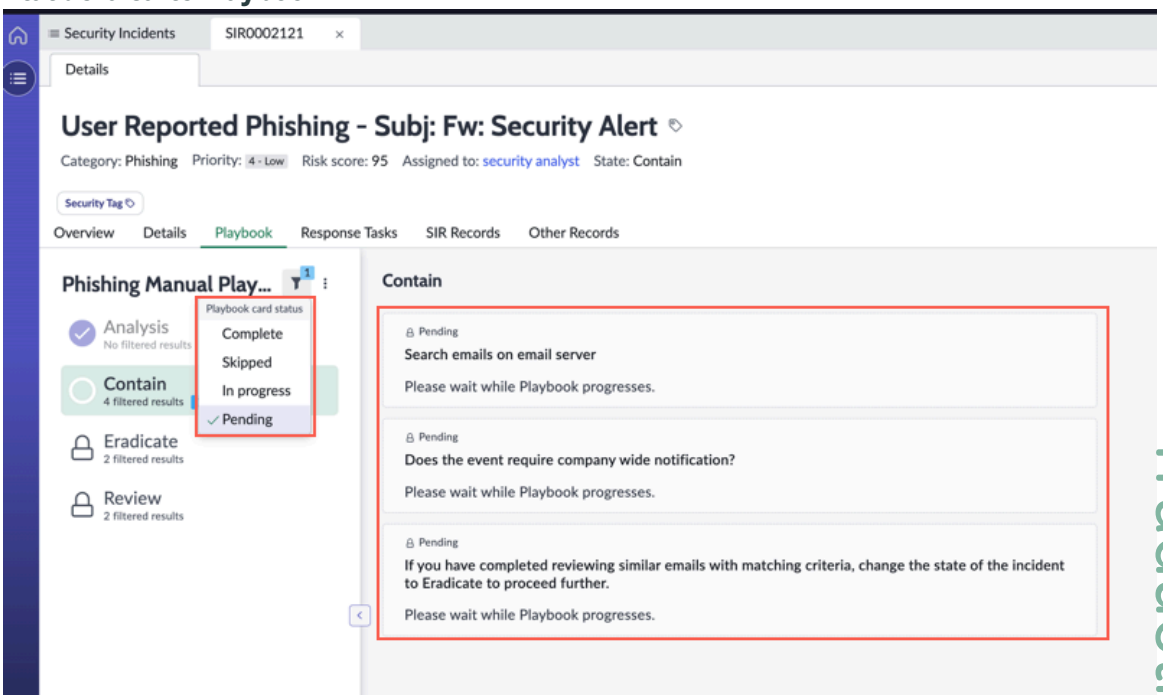


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans la section Playbook, utilisez l'option de filtre pour filtrer les activités par état de la carte Playbook (définition d'activité).

État de la carte Playbook



Ajouter un Playbook

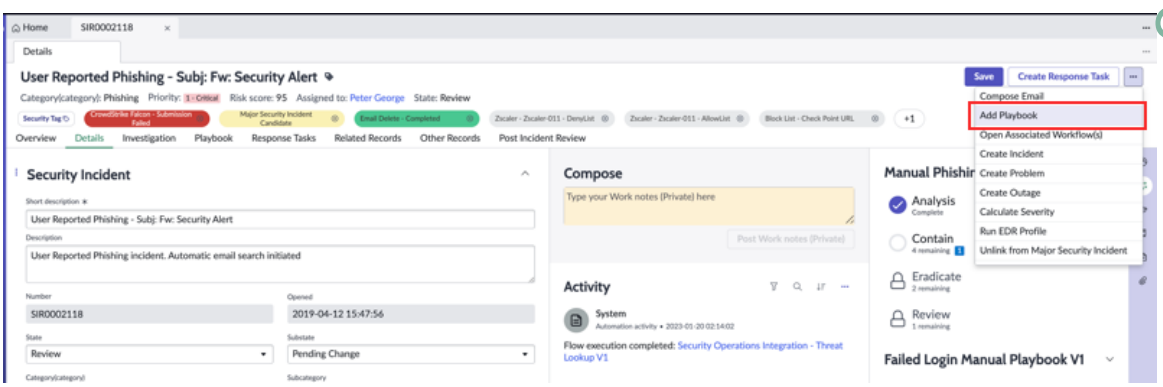
Utilisez cette section pour ajouter un playbook manuellement.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

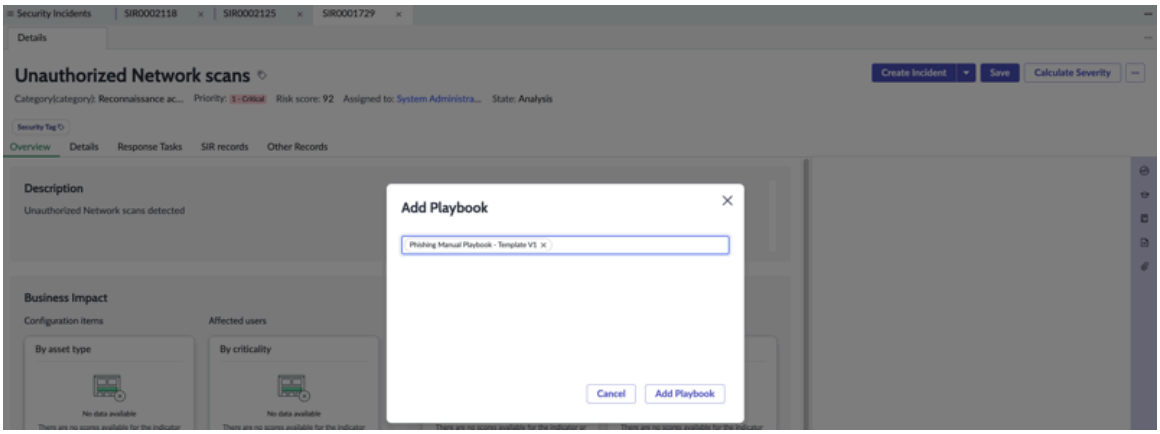
1. Accédez à la **Tous** > **Incident de sécurité** > **Security Analyst Workspace**.
2. Ouvrez un enregistrement d'incident.
3. Cliquez sur **Ajouter un playbook**.



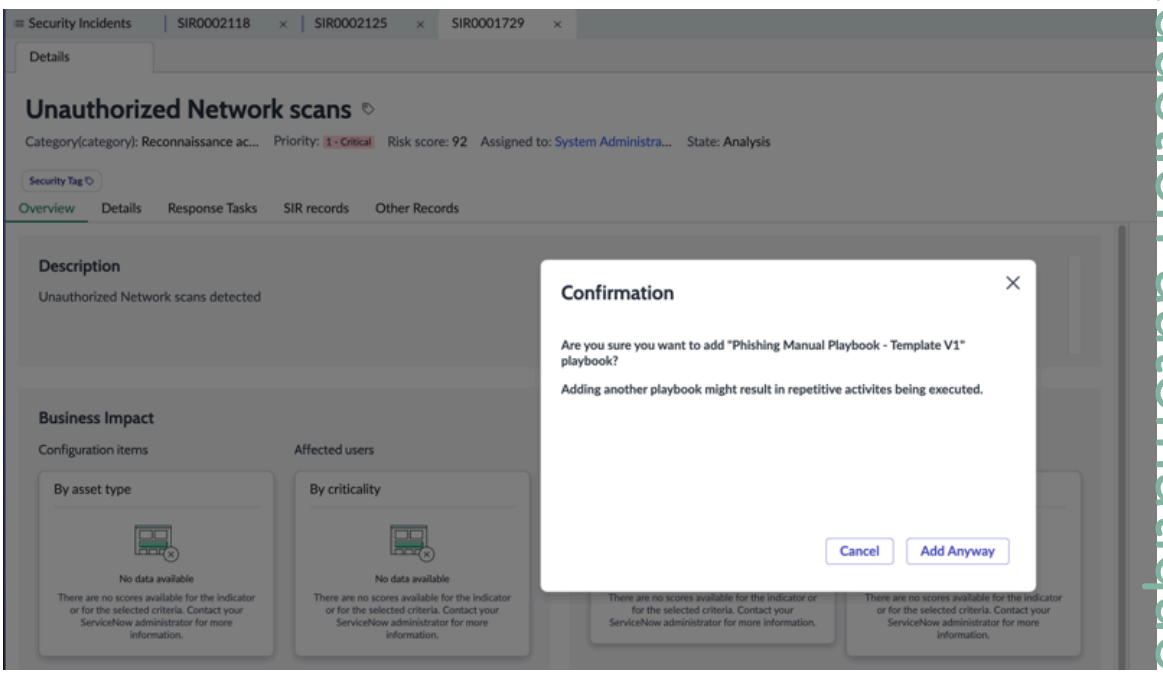
La boîte de dialogue **Ajouter un playbook** s'affiche.

Traduction automatique

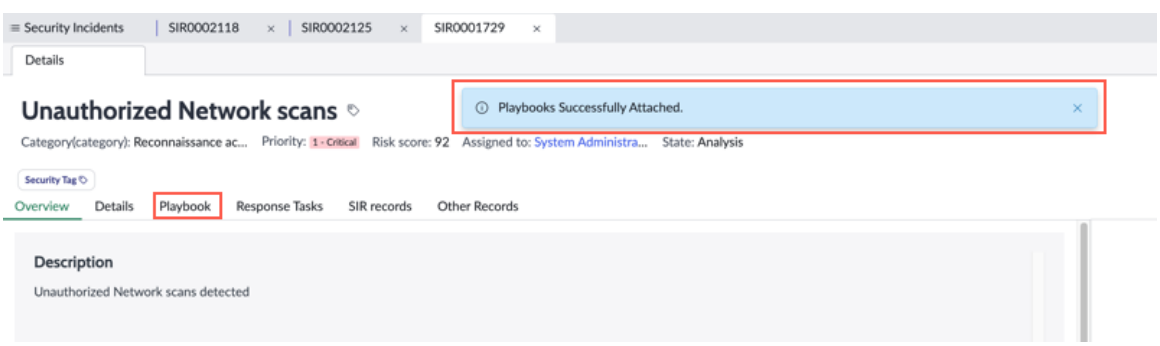
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez le modèle de playbook.
5. Cliquez sur **Ajouter un playbook**.
   Une boîte de dialogue de message de confirmation s'affiche pour que vous confirmiez.
6. Cliquez sur **Ajouter quand même**.



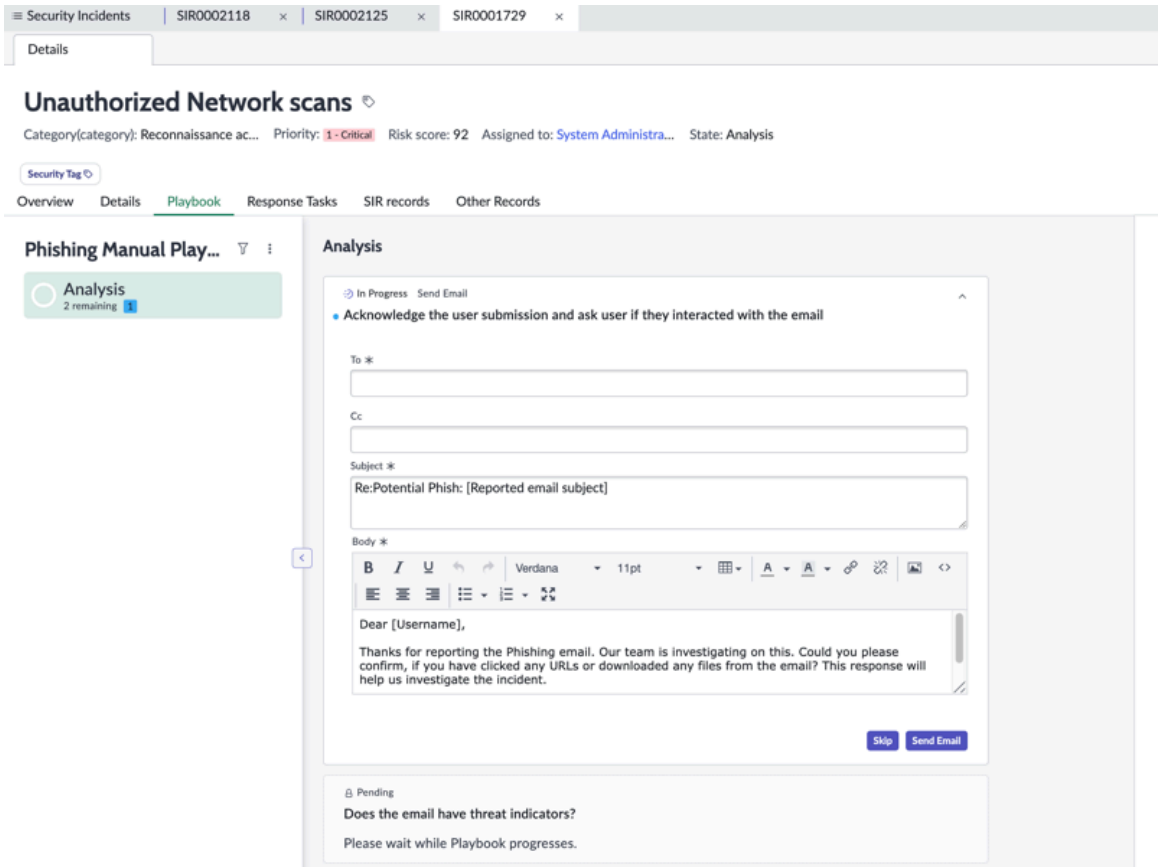
7. Le **Playbook** est ajouté à côté de l'onglet **Détails** .



8. Cliquez sur l'onglet **Playbook** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Effectuez la série d'activités telle que listée pour passer au niveau suivant.

Remarque : Si un incident de sécurité est associé à un playbook, tant que le playbook associé n'est pas fermé ou annulé, l'utilisateur ne peut plus associer le même playbook au même incident de sécurité.

Prérequis pour les Playbooks

Vous avez besoin des rôles et modules d'extension suivants pour créer les Playbooks.

Rôle requis : admin.

- Activez le module d'extension Concepteur d'automatisation de processus (PAD) [com.glide.pad.license].
- Activez les modules d'extension suivants pour une expérience de playbook :
  - com.playbook_experience
  - now_playbook_exp
  - com.glide.playbook_experience.config
- Activer le spoke Security Operations pour accéder aux flux [com.snc.secops.spoke].
- Gestion des tickets de sécurité d'entreprise PAD Commons.

Assurez-vous d'avoir lu la documentation de la plateforme et Explorer les playbooks Process Automation Designer avant de commencer avec ce guide.

Reconstruction des playbooks existants dans Studio de workflow

Vous ne pouvez pas convertir les flux existants directement en playbooks dans Studio de workflow. Chaque étape du Flow Designer qui crée une tâche de réponse pour guider l'analyste doit être divisée en actions ou flux secondaires distincts.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous n'êtes pas autorisé à convertir des flux existants directement en playbooks dans Studio de workflow. Chaque étape du Flow Designer qui crée une tâche de réponse pour guider l'analyste doit être divisée en actions ou flux secondaires distincts. À l'aide de ces flux secondaires ou actions granulaires, vous devez créer des définitions d'activité. Une fois ces définitions d'activité créées, elles sont ajoutées en tant qu'activités dans l'étape de la définition du processus. Vous pouvez réutiliser les définitions d'activité dans plusieurs playbooks.

Vous pouvez personnaliser chaque activité pour afficher les actions requises qu'elles contiennent et l'apparence de la carte lors de la création de la définition d'activité. L'activité peut afficher les clients de messagerie, les tables, les actions, les articles de la base de connaissances, les URL, etc. Vous pouvez définir la façon dont la définition d'activité et l'action ou les flux secondaires sous-jacents sont créés.

Pour plus d'informations, reportez-vous aux sections suivantes.

- Définitions d'activité
- Process Automation Designer

Définitions d'activités

Le ServiceNow AI Platform fournit quelques définitions d'activité dans le système de base. En outre, pour les playbooks que le système de base de l'espace de travail SIR, il existe quelques définitions d'activité définies dans le système de base sous l'application PAD Commons Enterprise Security Case Management.

Rôle requis : sn_si.admin.

Voici la liste des définitions d'activité qui font partie du système de base :

Définition d'activité	Table	Description	Application
Attendre une condition sans expérience	Global[global]	Attendre une condition sans expérience	Gestion des tickets de sécurité d'entreprise PAD Commons
Soumettre au bac à sable CSF X	Incident de sécurité [sn_si_incident]	Soumettre à Sandbox	Gestion des tickets de sécurité d'entreprise PAD Commons
Envoyer un e-mail	Incident de sécurité [sn_si_incident]	Activité d'envoi d'e-mail pour les playbooks SIR.	Gestion des tickets de sécurité d'entreprise PAD Commons
Rechercher un e-mail	Incident de sécurité [sn_si_incident]	Rechercher des e-mails sur le serveur de messagerie	Gestion des tickets de sécurité d'entreprise PAD Commons
Mettre à jour l'état de la tâche	Incident de sécurité [sn_si_incident]	Mettre à jour l'état de la tâche	Gestion des tickets de sécurité d'entreprise PAD Commons
Supprimer l'e-mail	Incident de sécurité [sn_si_incident]	Supprimer les e-mails	Gestion des tickets de sécurité d'entreprise PAD Commons
Résultat avec oui/non	Tâche [task]	Résultat attendu	Gestion des tickets de sécurité d'entreprise PAD Commons

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de définition d'activité : Envoyer un e-mail

Voici un exemple de définition d'activité Envoyer un e-mail.

Élémentaire

Les détails de base capturent le nom (étiquette), l'application, la description, la table et à partir de toutes les applications à partir desquelles il est accessible.

Ajoutez le plan d'automatisation, l'expérience de l'activité et soumettez. Après l'envoi, modifiez le document pour ajouter plus de détails à chaque onglet.

Plan d'automatisation

Le plan d'automatisation associe l'action back-end ou les flux secondaires créés à l'aide du concepteur de flux. Cet exemple utilise : **Envoyer un e-mail : flux secondaire d'activité ESCM** .

Ce flux secondaire permet l'envoi d'un e-mail. Il a la logique de base pour envoyer un e-mail. Tous les champs d'entrée et de sortie sont définis.

Tous les champs d'entrée sont affichés dans la section du plan d'automatisation. Chaque champ d'entrée peut être activé pour être visible uniquement par l'administrateur, dans le modal standard, dans le modal standard et le panneau de configuration :

- **Visibilité de l'administrateur uniquement** : lorsque la valeur est définie sur administrateur, seul l'administrateur peut la consulter.
- **Inclure dans le modèle standard** : lorsqu'il est défini sur Afficher dans la fenêtre modale Standard, il n'apparaît que dans la fenêtre modale Propriétés.
- **Inclure dans le modèle standard et le panneau de configuration** : lorsqu'il est défini sur Afficher dans le modal standard et le panneau de configuration, il apparaît dans le panneau de configuration PAD ainsi que dans le modal des propriétés. Pour plus d'informations, voir Définitions d'activité

Vous pouvez définir les champs d'entrée au moment de la définition de l'activité elle-même, à condition que vous n'ayez pas besoin de modifier ces valeurs au moment de la configuration. Cela permet au propriétaire du processus business de gagner du temps lors de la configuration d'une activité au sein d'un processus.

Expérience de l'activité

L'onglet Expérience d'activité définit la façon dont la carte d'activité est rendue au moment de l'exécution. Le système de base fournit les types d'expérience suivants :

- Approbation
- Élément de catalogue
- Créer un enregistrement
- Pédagogique
- Base de connaissances
- Liste
- Notification
- Enregistrement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En fonction du type d'expérience que vous sélectionnez, les champs suivants sont renseignés. Pour plus d'informations, consultez la ServiceNow AI Platform documentation.

Dans cet exemple, le type **d'enregistrement** est sélectionné.

Remarque : Par exemple, si vous souhaitez afficher une table, vous pouvez choisir la liste comme type d'expérience.

Enregistrement associé

Utilisez cet enregistrement pour stocker les données associées relatives à l'activité en cours. Cela capturerait les données de temps d'exécution, ainsi que l'état de l'expérience.

- Table associée : Données de flux
- Enregistrement associé : VL
- Table de l'état de l'expérience : données de flux
- Enregistrement de l'état de l'expérience : VL

Dans cet exemple, la table de données de flux est utilisée pour capturer les données de temps d'exécution. Les données de temps d'exécution peuvent varier en fonction du cas d'utilisation. Dans cet exemple, les données d'exécution sont des champs tels que À, cc, Objet et corps. Pour chaque cas d'utilisation, une définition de données de flux doit être créée pour définir le type des données de temps d'exécution.

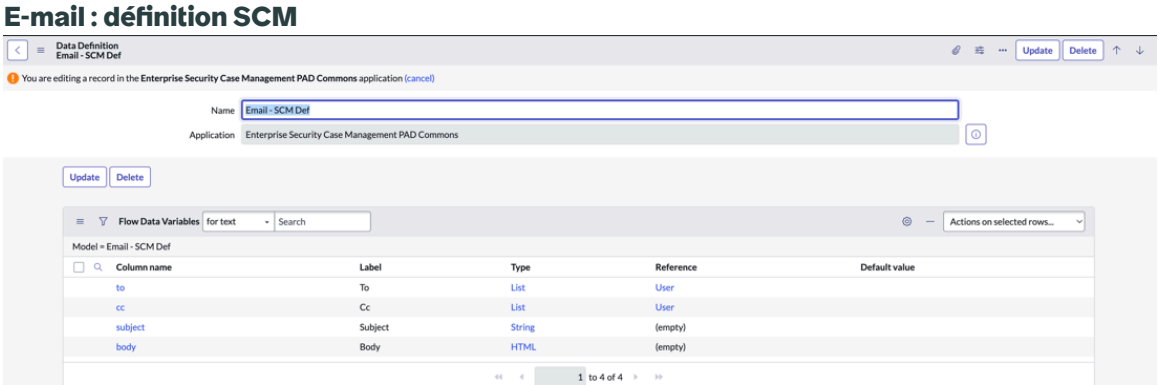
1. Accédez au volet gauche et saisissez **sys_flow_data_definition.list**. Il affiche la liste des définitions créées pour la table de données de flux.

Associer l'enregistrement



2. Ouvrez **E-mail : définition SCM** pour afficher la définition associée à cet exemple.

E-mail : définition SCM

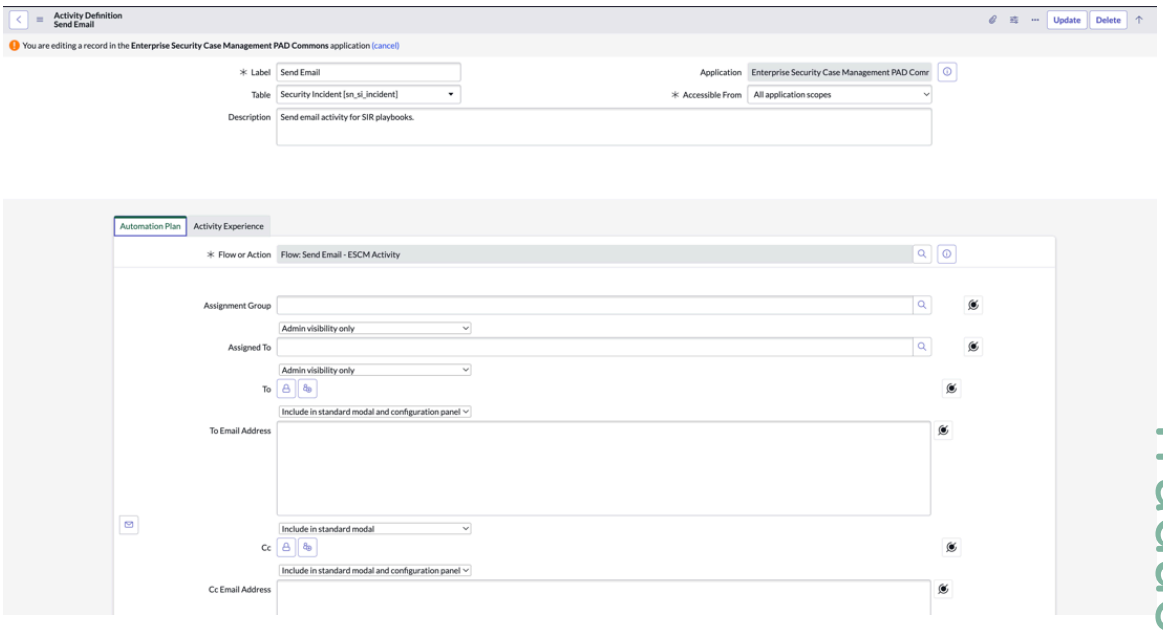


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

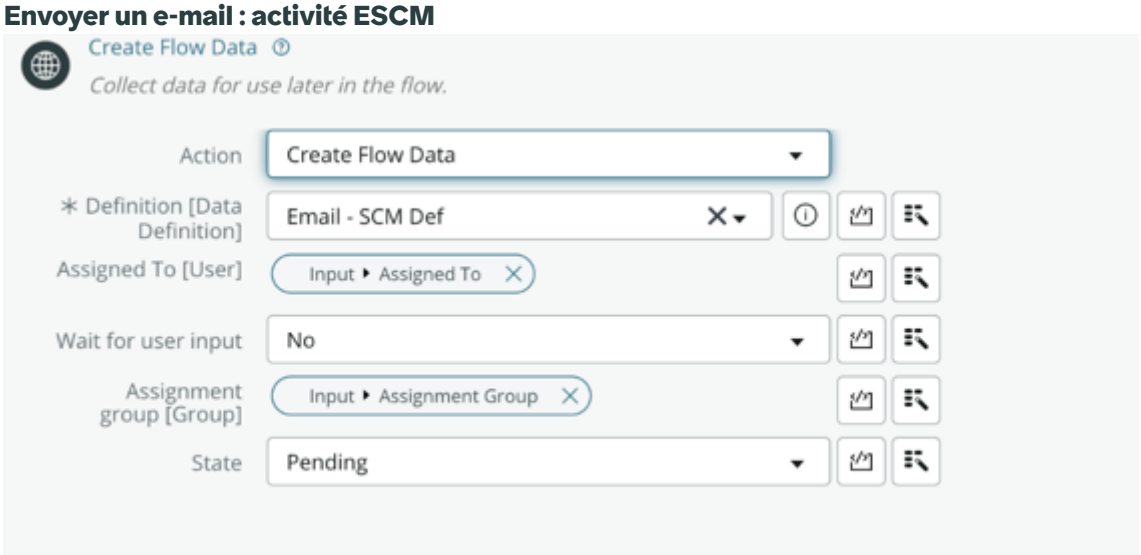
Cette définition de données de flux doit être utilisée par le flux secondaire ou l'action associée à cette définition d'activité (se référer au plan d'automatisation) pour capturer les données d'exécution.

Définitions d'activités



3. Dans cet exemple, ouvrez le flux secondaire : **Envoyer un e-mail - Activité ESCM**. Sous **l'étape Créer des données de flux** , la définition des données de flux que vous avez créée est mappée par rapport au champ **Définition** . Cet enregistrement de données de flux est utilisé dans le flux secondaire. Dans cet exemple, l'état de la carte d'activité (état de l'expérience) est capturé dans la table de données de flux.

Envoyer un e-mail : activité ESCM



Remarque : Si vous souhaitez capturer les données d'exécution dans un enregistrement de table différent de la table de données de flux, par exemple dans une tâche de réponse. Vous pouvez sélectionner la table associée en tant que table de tâches de réponse. L'enregistrement associé doit être défini sur l'enregistrement de tâche de réponse créé par le flux secondaire.

De même, la table de l'état de l'expérience capture l'état de la carte d'activité. Dans le système de base, le champ d'état de la table de données de flux est mappé à l'état de la

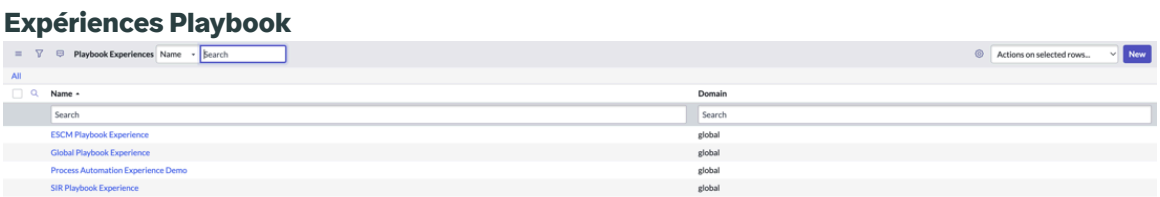
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

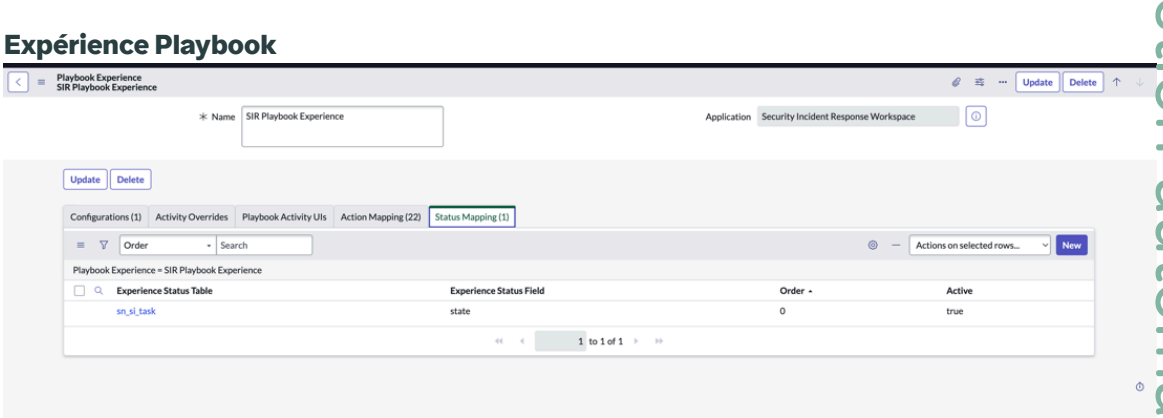
carte d'activité. Ainsi, lorsque la table de données de flux est utilisée pour capturer l'état de l'expérience, elle met automatiquement à jour l'état de la carte d'activité. Vous pouvez également utiliser une autre table que la table de données de flux pour capturer l'état de l'expérience.

Par exemple, si vous souhaitez mapper l'état de la tâche de réponse à l'état de la carte d'activité, cela est possible. Pour ce faire :

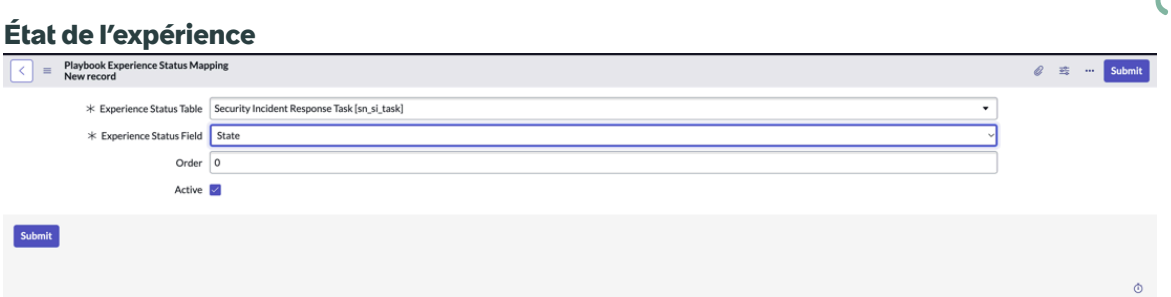
1. Accédez à la **Tous** > **Expériences Playbook**.



2. Ouvrez **l'expérience Playbook SIR**.
3. Ouvrez la liste connexe **Mappage de statut** .



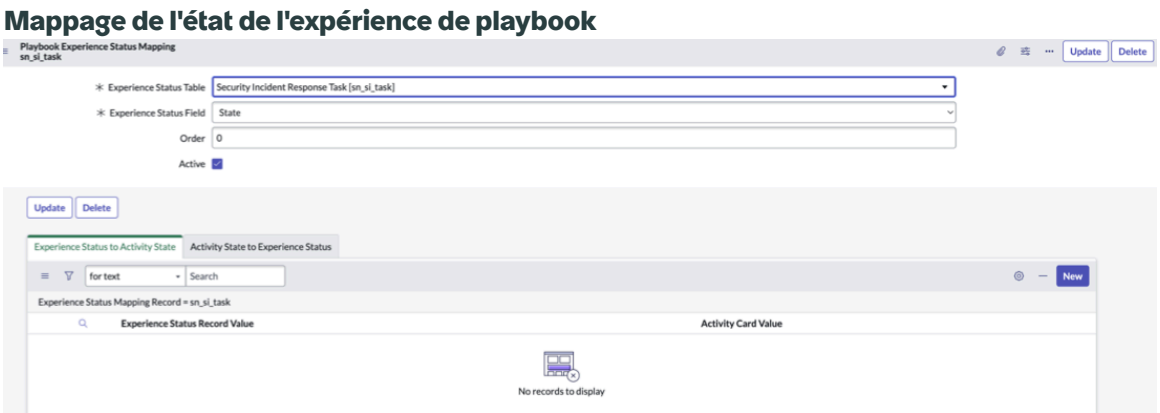
4. Saisissez la **tâche de réponse** par rapport au champ Table de l'état de l'expérience.
5. Saisissez le champ **État** par rapport au statut de l'expérience.



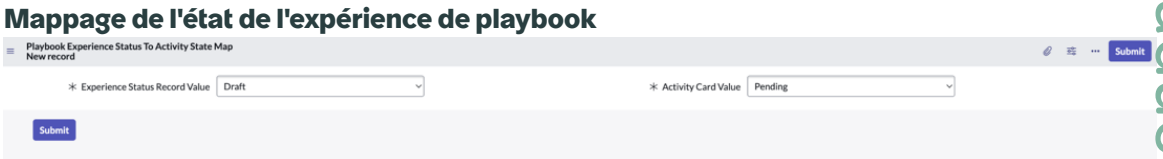
6. Cliquez sur **Envoyer**. L'enregistrement est créé.

Traduction automatique

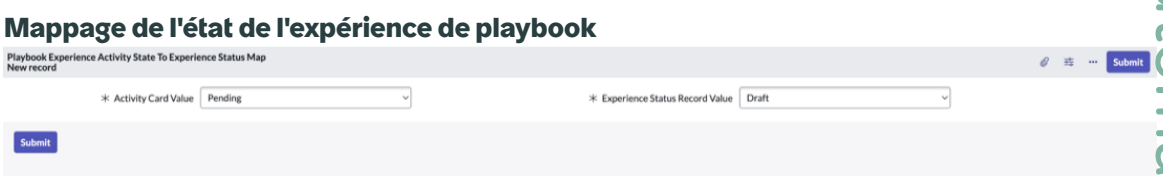
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Sous État de l'expérience à État de l'activité, mappez les états de la tâche de réponse à l'état de la carte d'activité.
8. Le côté gauche affiche les états de la tâche de réponse et le côté droit affiche l'état de la carte d'activité.



9. Le mappage peut être bidirectionnel. Sous État de l'activité vers la liste connexe Expérience également, mappez correctement les états. Cette étape est l'inverse de l'étape précédente. Dans ce cas, le côté gauche affiche l'état de la carte d'activité et le côté droit affiche l'état de la tâche de réponse.



Détails

- Ligne de balise : Envoyer un e-mail
- Icône : contour de l'enveloppe (non affiché dans l'interface utilisateur)
- Titre : **Activité** > **Instance d'activité** > **Étiquette**. Ici, nous avons sélectionné l'étiquette de l'instance d'activité. Cette remontée pas à pas remplace la valeur de l'étiquette en tant que titre de manière dynamique au moment de l'exécution.
- Description : **Activité** > **Instance d'activité** > **Description**. Ici, nous avons sélectionné la description de l'instance d'activité. Cette remontée pas à pas remplace la valeur de l'étiquette en tant que titre de manière dynamique au moment de l'exécution.
- Titre de l'état en attente : envoyer une notification par e-mail. Il s'agit du titre lorsque l'activité est à l'état En attente.
- Description d'état en attente : demande la confirmation de l'objet et du corps de l'e-mail avant l'envoi. Il s'agit de la description de la carte d'activité lorsque l'état est en attente Champs d'enregistrement : certains champs d'enregistrement sont sélectionnés dans cet exemple.

Traduction automatique

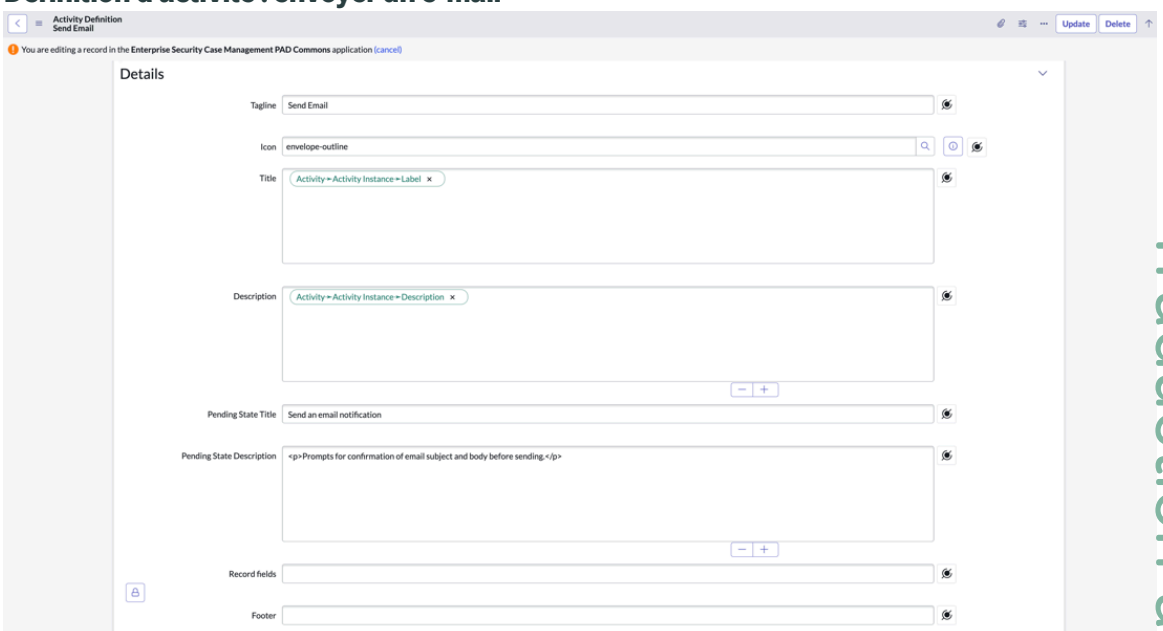
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les champs d'enregistrement sont des listes séparées par des virgules de noms de champs à afficher pour l'enregistrement associé dans une liste de paires nom-valeur. Les données sont pré-récupérées sur le serveur, la remontée pas à pas est prise en charge et les autorisations **canRead()** sont évaluées sur chaque champ.

- Pied de page : aucun pied de page n'est défini pour cet exemple.

  Le pied de page est un texte situé dans une zone grise du pied de page de la carte. Vous pouvez ajouter des informations significatives à afficher.

Définition d'activité : envoyer un e-mail

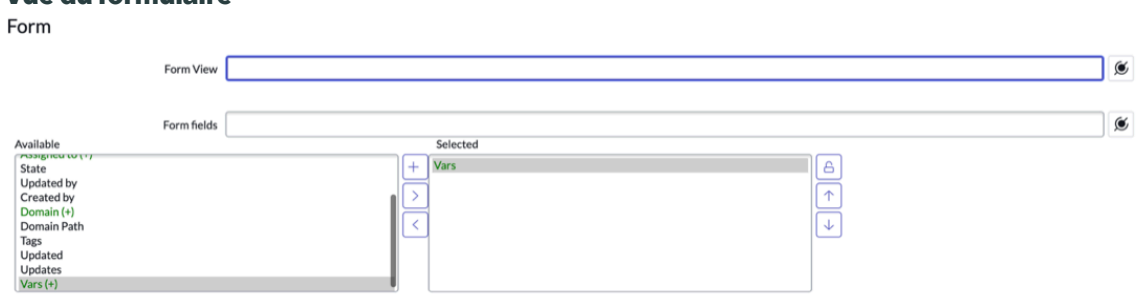


Formulaire

- Vue du formulaire : collect_data
- Champs de formulaire :

Cet exemple utilise collect_data vue pour afficher les champs qui doivent être présentés à l'utilisateur pour entrer des entrées. Collect_data vue est une vue fournie par la plateforme correspondant à la table de données de flux. Vous pouvez également laisser la vue de formulaire vide et sélectionner Variables dans la liste des valeurs disponibles en regard des champs de formulaire. (cliquez sur l'icône de verrou pour ouvrir la liste des valeurs disponibles).

Vue du formulaire



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

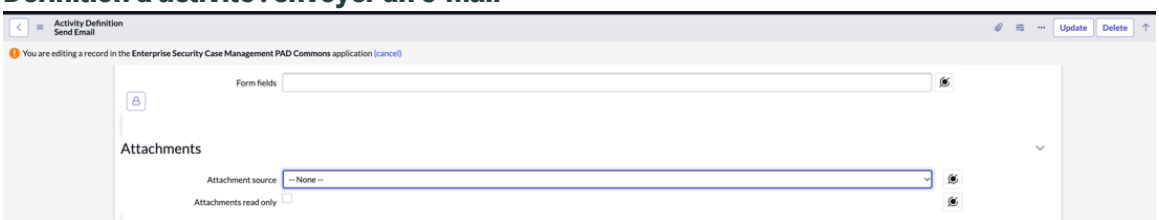
Pièces jointes

Dans cet exemple :

- La source de la pièce jointe est vide.
- Pièce jointe en lecture seule non sélectionnée.

1. Source de la pièce jointe : liste déroulante. Quelles pièces jointes afficher sur la carte : celles jointes à l'enregistrement parent, à l'enregistrement associé ou aucune.
2. Pièce jointe en lecture seule : vrai ou faux. Empêchez l'utilisateur de renommer ou de supprimer les pièces jointes existantes.

Définition d'activité : envoyer un e-mail



Fonctionnalités

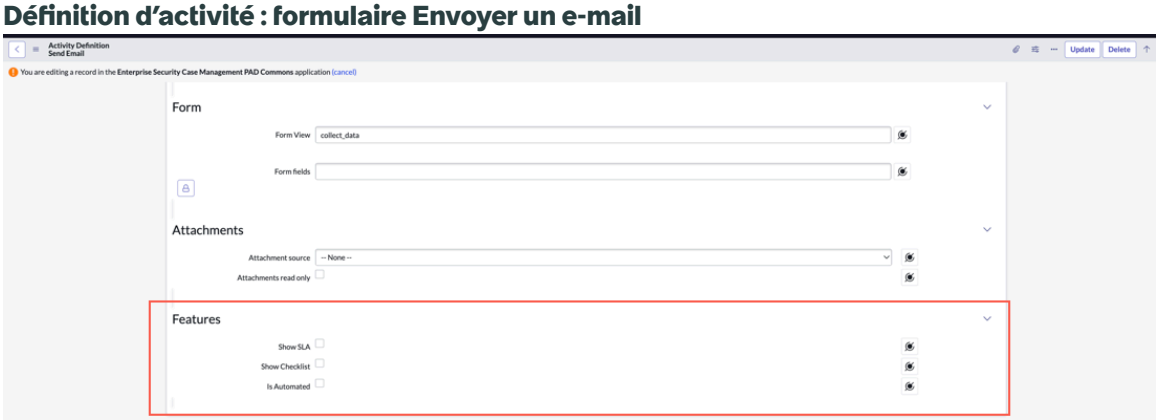
Dans cet exemple,

- Afficher le SLA : effacé
- Afficher la liste de vérification : effacé
- Est automatisé : effacé

Afficher le SLA : vrai/faux. Affiche un minuteur SLA dans l'en-tête de la carte pour l'enregistrement associé. Le SLA est choisi en fonction de l'enregistrement de configuration SLA spécifié dans la configuration du Playbook.

1. Afficher la liste de vérification : vrai ou faux. Affiche toute liste de vérification jointe à l'enregistrement associé. La liste de vérification est modifiable et les changements sont enregistrés sans nécessiter d'action déclarative.
2. Est automatisé : vrai ou faux. Si vrai, le **slogan** et **l'icône** seront remplacés par le texte **Tâche automatisée** et une icône automatisée.

Définition d'activité : formulaire Envoyer un e-mail



Traduction automatique

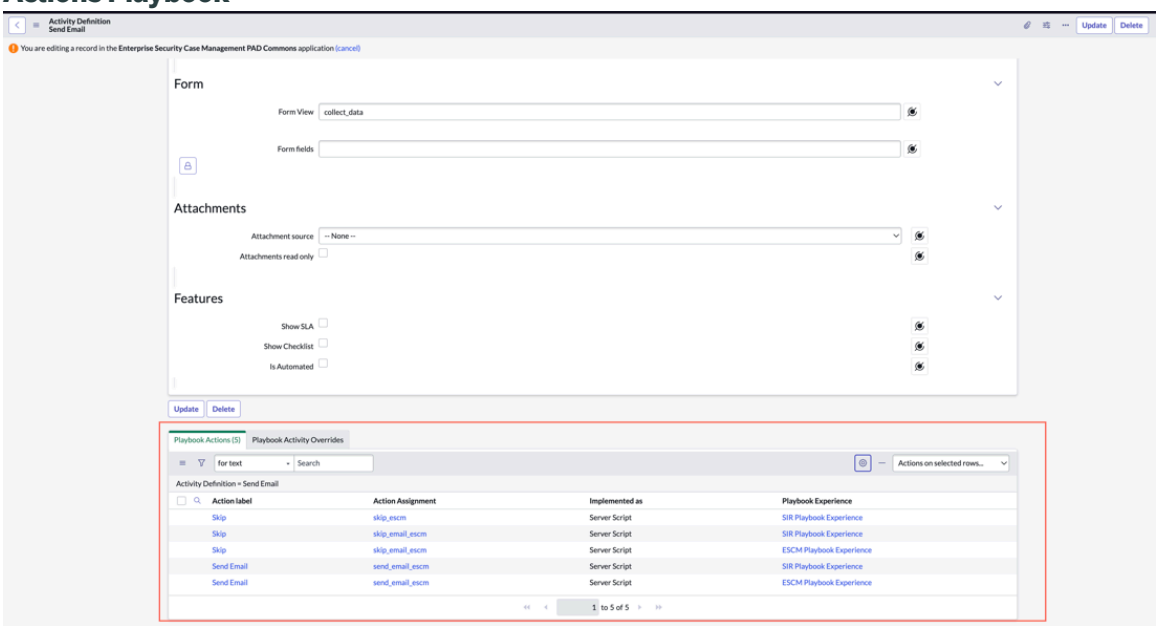
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions Playbook dans la définition d'activité

Cette section contient les actions qui seront affichées sur la carte d'activité. Cet exemple comporte **les actions Ignorer** et **Envoyer un e-mail** .

Pour ajouter une nouvelle action à la carte d'activité, vous devez créer un enregistrement dans la liste connexe **Actions Playbook** présente en bas de la page.

Actions Playbook



1. Cliquez sur **Nouveau**.
2. Sélectionnez une action d'activité existante par rapport au champ Affectation d'action.
3. Sélectionnez **Expérience de playbook SIR** en regard du champ Expérience de playbook.

Créer une action d'activité

La procédure de création d'une action d'activité est la suivante.

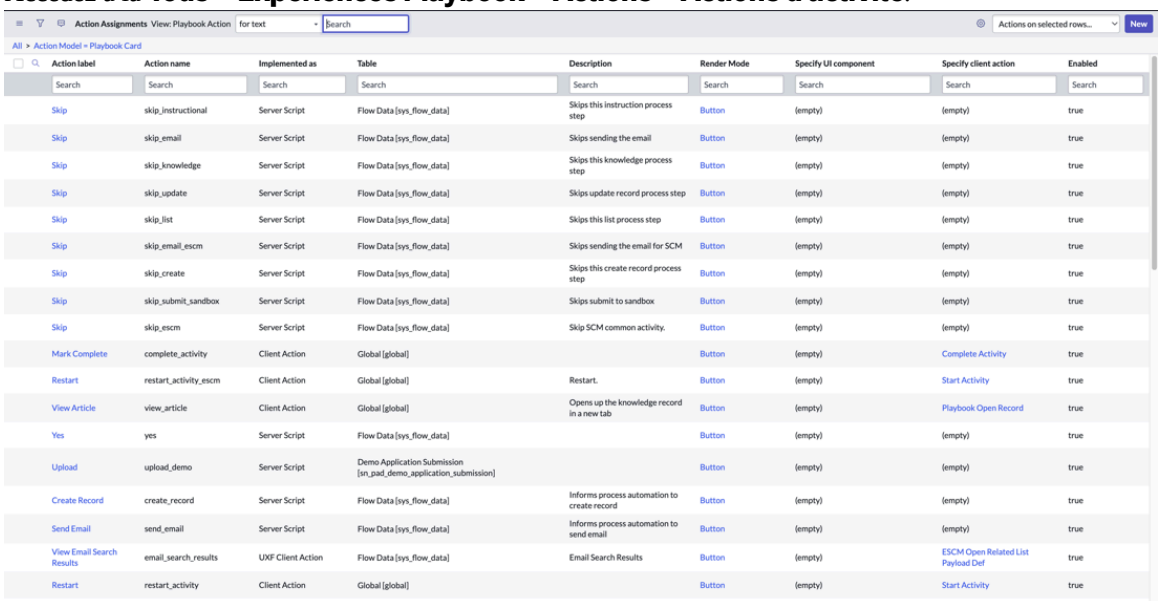
Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Expériences Playbook** > **Actions** > **Actions d'activité**.



Action label	Action name	Implemented as	Table	Description	Render Mode	Specify UI component	Specify client action	Enabled
Skip	skip_instructional	Server Script	Flow Data [sys_flow_data]	Skips this instruction process step	Button	(empty)	(empty)	true
Skip	skip_email	Server Script	Flow Data [sys_flow_data]	Skips sending the email	Button	(empty)	(empty)	true
Skip	skip_knowledge	Server Script	Flow Data [sys_flow_data]	Skips this knowledge process step	Button	(empty)	(empty)	true
Skip	skip_update	Server Script	Flow Data [sys_flow_data]	Skips update record process step	Button	(empty)	(empty)	true
Skip	skip_list	Server Script	Flow Data [sys_flow_data]	Skips this list process step	Button	(empty)	(empty)	true
Skip	skip_email_escm	Server Script	Flow Data [sys_flow_data]	Skips sending the email for SCM	Button	(empty)	(empty)	true
Skip	skip_create	Server Script	Flow Data [sys_flow_data]	Skips this create record process step	Button	(empty)	(empty)	true
Skip	skip_submit_sandbox	Server Script	Flow Data [sys_flow_data]	Skips submit to sandbox	Button	(empty)	(empty)	true
Skip	skip_escm	Server Script	Flow Data [sys_flow_data]	Skip SCM common activity.	Button	(empty)	(empty)	true
Mark Complete	complete_activity	Client Action	Global [global]		Button	(empty)	Complete Activity	true
Restart	restart_activity_escm	Client Action	Global [global]	Restart.	Button	(empty)	Start Activity	true
View Article	view_article	Client Action	Global [global]	Opens up the knowledge record in a new tab	Button	(empty)	Playbook Open Record	true
Yes	yes	Server Script	Flow Data [sys_flow_data]		Button	(empty)	(empty)	true
Upload	upload_demo	Server Script	Demo Application Submission [sn_pad_demo_application_submission]		Button	(empty)	(empty)	true
Create Record	create_record	Server Script	Flow Data [sys_flow_data]	Informs process automation to create record	Button	(empty)	(empty)	true
Send Email	send_email	Server Script	Flow Data [sys_flow_data]	Informs process automation to send email	Button	(empty)	(empty)	true
View Email Search Results	email_search_results	UXF Client Action	Flow Data [sys_flow_data]	Email Search Results	Button	(empty)	ESCM Open Related List Payload Def	true
Restart	restart_activity	Client Action	Global [global]		Button	(empty)	Start Activity	true

2. Cliquez sur **Nouveau**.

   Consultez la ServiceNow AI Platform documentation pour savoir comment créer ces actions. Dans cet exemple, Skip est implémenté en tant que script serveur.

3. **Remplacement du Playbook :**

   Si vous souhaitez remplacer le type d'expérience d'activité existant, c'est possible. Pour plus d'informations, consultez la ServiceNow AI Platform documentation. Aucun remplacement de Playbook pour cet exemple.

Soumettre au bac à sable CSF X

Soumettre au bac à sable CSF X est un exemple de processus de définition d'activité.

Élémentaire

Les détails de base capturent le nom (étiquette), l'application, la description, la table et toutes les applications à partir desquelles il est accessible.

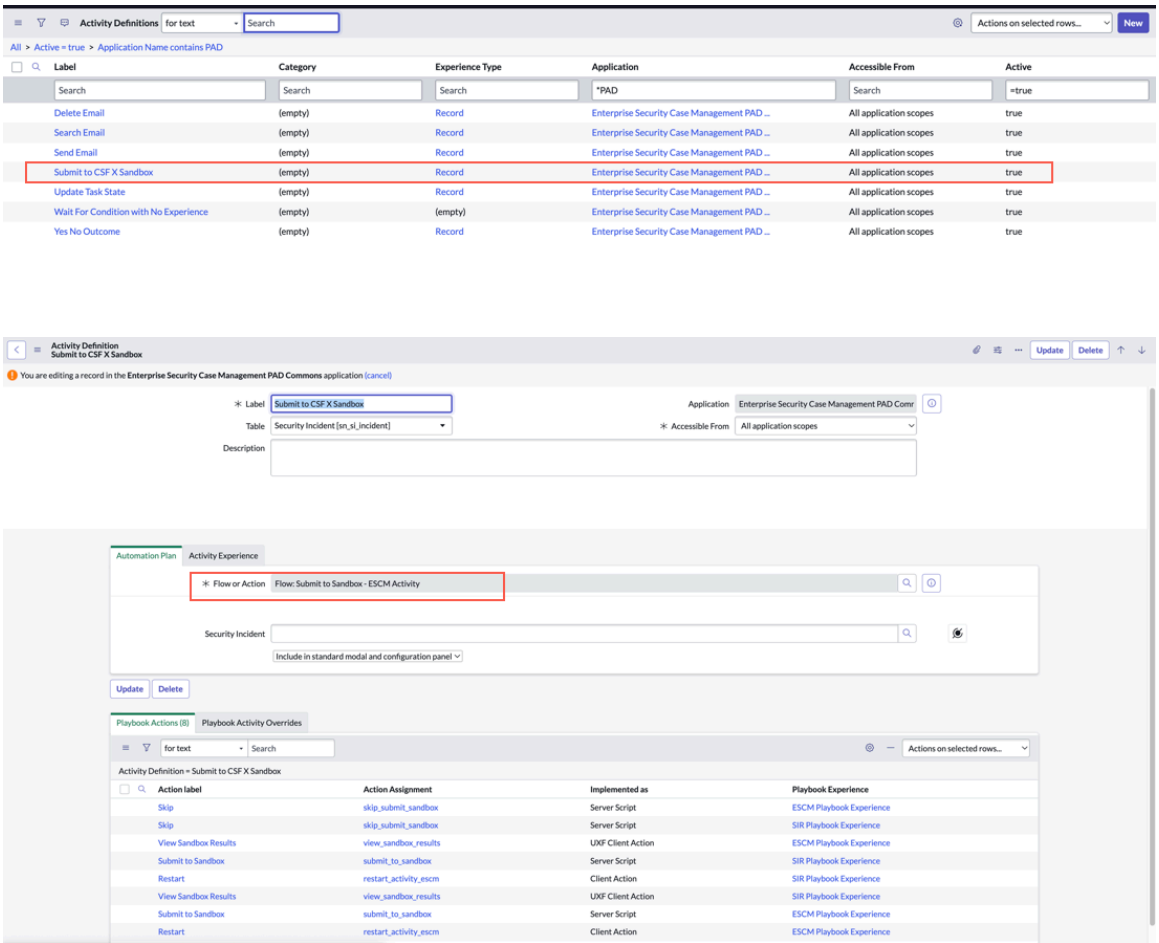
Ajoutez le plan d'automatisation, l'expérience de l'activité et soumettez. Une fois soumis, modifiez le document pour ajouter plus de détails sur chaque onglet.

Plan d'automatisation

Le plan d'automatisation associe l'action/le flux secondaire principal créé à l'aide du concepteur de flux. Cet exemple utilise le flux secondaire **Soumettre au bac à sable - ESCM Activité**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Ce flux secondaire permet de soumettre les observables malveillants au bac à sable. Tous les champs d'entrée et de sortie sont définis.

L'incident de sécurité est le champ d'entrée.

Expérience de l'activité

Dans cet exemple, le type **d'enregistrement** est sélectionné.

Enregistrement associé

L'enregistrement associé sert à stocker les données associées relatives à l'activité en cours. Cela capturerait les données de temps d'exécution, ainsi que l'état de l'expérience.

- Table associée : Données de flux
- Enregistrement associé : VL
- Table de l'état de l'expérience : données de flux
- Enregistrement de l'état de l'expérience : VL

Détails

- Ligne de balise : Envoyer un e-mail
- Icône : contour de l'enveloppe
- Titre : **Activité** > **Instance d'activité** > **Étiquette**. Ici, nous avons sélectionné l'étiquette de l'instance d'activité. Cette remontée pas à pas remplace la valeur de l'étiquette en tant que titre de manière dynamique au moment de l'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Description : VL (la sortie du flux secondaire est mappée)
- État en attente Titre : vide
- Description de l'état en attente : vide
- Champs d'enregistrement
- Pied de page

Formulaire

- Vue du formulaire : vide
- Champs de formulaire : vides

Pièces jointes

Dans cet exemple :

- Source de la pièce jointe : aucune
- Pièce jointe en lecture seule : non coché

1. Source de la pièce jointe : il s'agit d'une liste déroulante. Quelles pièces jointes afficher sur la carte : celles associées à l'enregistrement parent, à l'enregistrement associé ou aucune.
2. Pièce jointe en lecture seule : il s'agit d'un vrai/faux. Empêchez l'utilisateur de renommer ou de supprimer les pièces jointes existantes.

Fonctionnalités

Dans cet exemple,

- Afficher le SLA : non vérifié
- Afficher la liste de vérification : non vérifié
- Est automatisé : décoché

Actions Playbook dans la définition d'activité

Cette section contient les actions qui seront affichées sur la carte d'activité.

Cet exemple comporte des actions Ignorer, Afficher les résultats du bac à sable, Soumettre au bac à sable et Redémarrer.

Pour ajouter une nouvelle action à la carte d'activité, vous devez créer un nouvel enregistrement dans la liste connexe Actions Playbook présente en bas de la page.

Remplacement de Playbook

Aucun remplacement de Playbook pour cet exemple.

Exemples de playbooks pour l'espace de travail SIR

Vous pouvez créer ou configurer des playbooks pour l'espace de travail SIR rapidement et facilement sans écrire de code compliqué. Vous pouvez utiliser ces playbooks pour résoudre les menaces de sécurité étape par étape. Vous pouvez invoquer le flux de playbook d'incident de sécurité automatiquement ou manuellement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Incident Response fournit les playbooks suivants avec le système de base :

- Playbook pour l'hameçonnage manuel
- Playbook pour l'hameçonnage automatisé
- Playbook pour les programmes malveillants manuels
- Playbook pour les programmes malveillants automatisés
- Playbook pour l'échec de la connexion manuelle

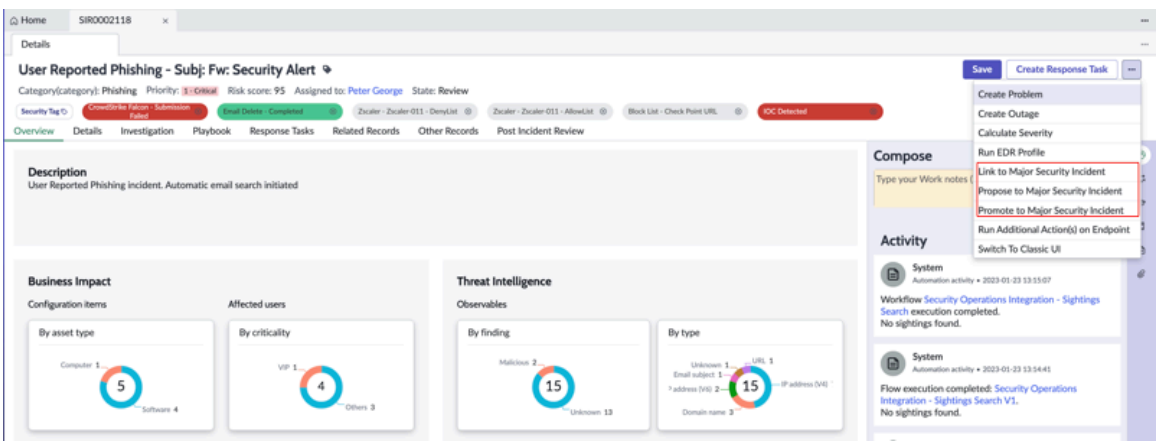
Utilisation des enregistrements MSI

À l'aide de l'espace de travail Réponse aux incidents de sécurité, vous pouvez proposer, promouvoir ou lier des incidents de sécurité en tant qu'incidents de sécurité majeurs lorsque les incidents sont identifiés comme une menace critique pour l'organisation.

Après avoir installé Gestion des incidents de sécurité majeurs (MSIM) sur votre ServiceNow AI Platform instance, vous pouvez gérer la transition des incidents de sécurité vers les incidents majeurs.

Les Gestion des incidents de sécurité majeurs actions d'interface utilisateur (MSIM) sont affichées en haut à droite de la bannière du formulaire d'incident de sécurité de l'espace de travail SIR. Sélectionnez l'action d'interface utilisateur le cas échéant.

Remarque : Certaines actions sont contextuelles. Par exemple, l'action Dissocier n'est disponible que lorsque l'incident de sécurité est déjà proposé, promu ou lié à un incident de sécurité majeur.



Proposer comme incident de sécurité majeur

Proposez un incident de sécurité en tant qu'incident de sécurité majeur (MSI).

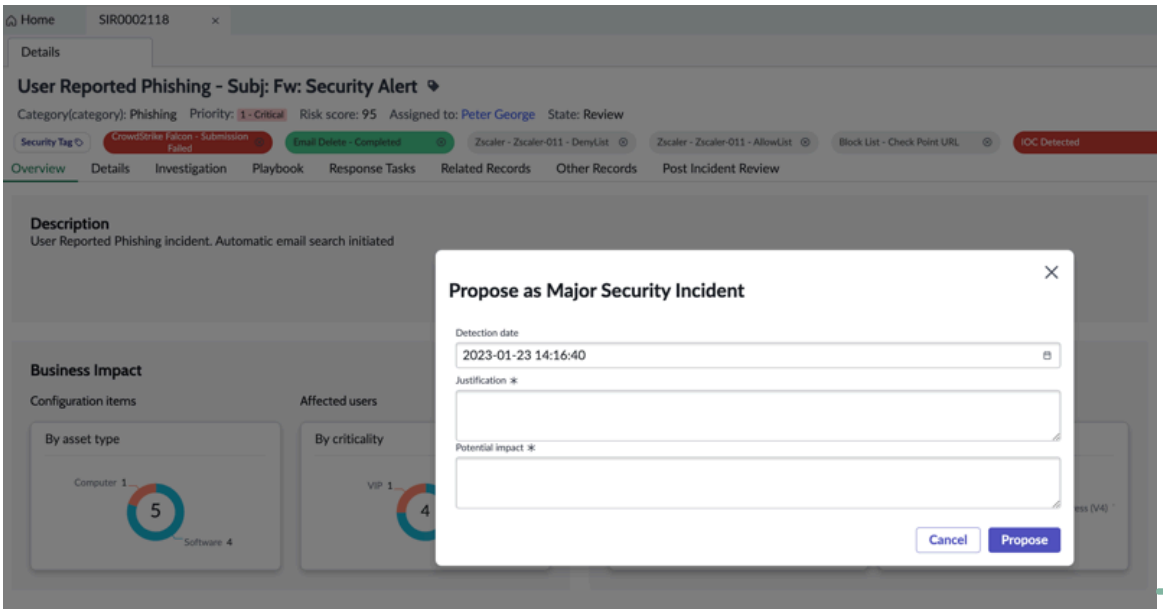
Avant de commencer
Rôle requis : sn_si.analyst.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Cliquez sur **Proposer un incident de sécurité majeur**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Renseignez les champs du formulaire, tels que Date de détection, Justification et Impact potentiel.
5. Cliquez sur **Proposer**.
   L'enregistrement d'incident est proposé comme candidat à un incident de sécurité majeur.
   Une fois que l'enregistrement d'incident est proposé comme candidat à un incident de sécurité majeur, la balise **de candidat à l'incident de sécurité majeur** est appliquée et affichée sur la bannière du formulaire d'incident de sécurité.

> **Remarque :** Cliquez sur **Dissocier d'un incident de sécurité majeur** pour dissocier l'incident si vous ne souhaitez pas proposer ou s'il n'a pas d'impact critique. L'incident sera dissocié et listé sous la vue de liste à l'analyste de sécurité pour correction.

Promouvoir en incident de sécurité majeur

Promouvoir un incident de sécurité en incident de sécurité majeur.

Avant de commencer

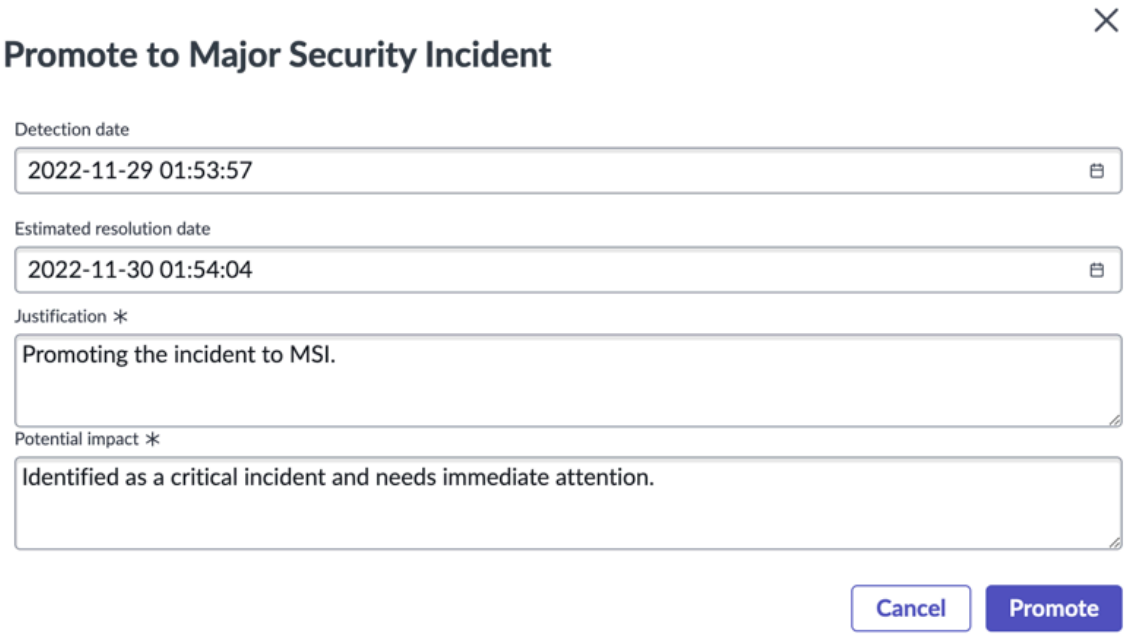
Rôle requis : sn_si.analyst.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Cliquez sur **Promouvoir en incident de sécurité majeur**.
4. Renseignez les champs du formulaire, tels que Date de détection, Date de résolution estimée, Justification et Impact potentiel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Promouvoir**.
   L'enregistrement d'incident est promu comme un incident de sécurité majeur.
   Une fois que l'enregistrement d'incident est promu en incident de sécurité majeur, la balise **d'incident de sécurité majeur** est appliquée et affichée sur la bannière du formulaire.

   Remarque : Vous pouvez également dissocier l'incident de sécurité majeur si l'incident n'est pas critique, l'incident sera alors dissocié et listé sous la vue de liste pour le rattrapage par l'analyste de sécurité.

Lier à l'incident de sécurité majeur

Liez un incident de sécurité à un incident de sécurité majeur en tant qu'incident de sécurité enfant.

Avant de commencer

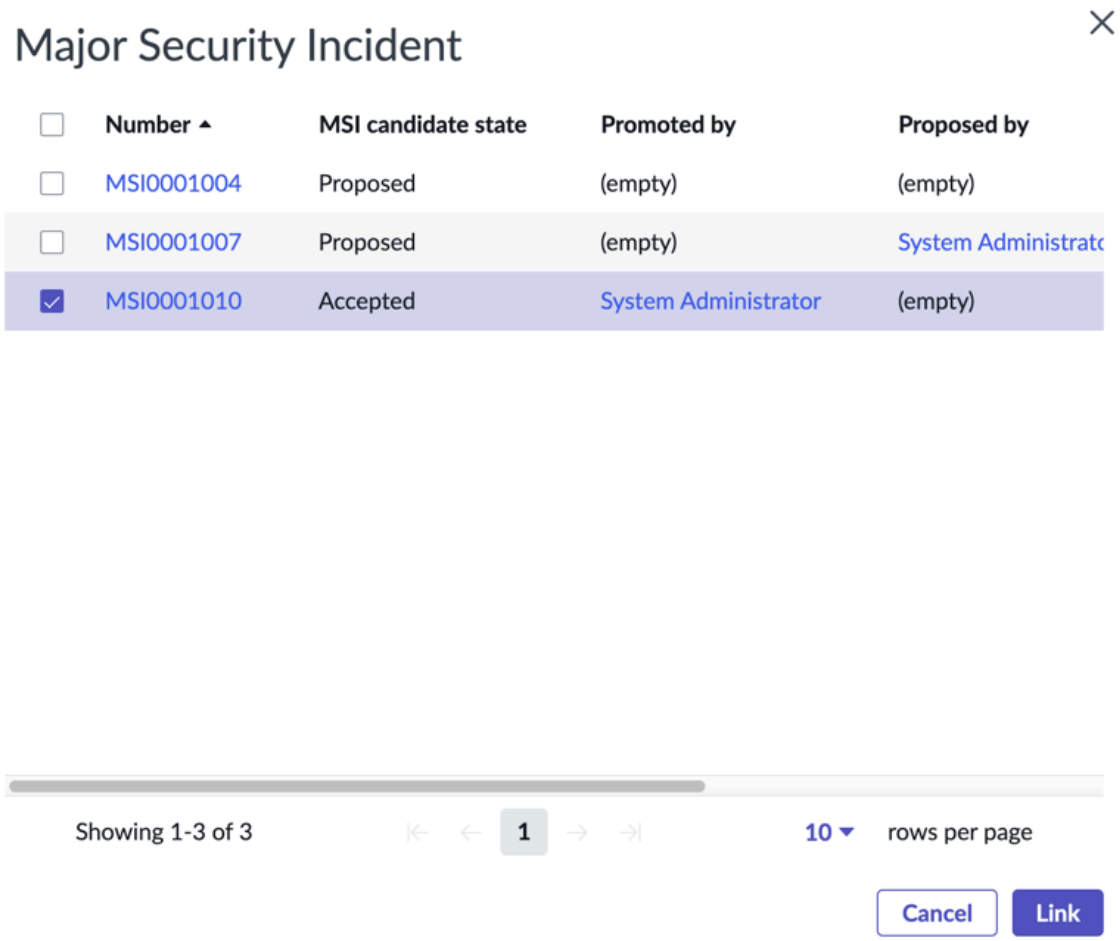
Rôle requis : sn_si.analyst.

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Ouvrez n'importe quel incident de sécurité.
3. Cliquez sur **Lien vers l'incident de sécurité majeur**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

4. Sélectionnez le ou les incidents à lier à un incident de sécurité majeur.
5. Cliquez sur **un lien**.
6. L'enregistrement d'incident est lié en tant qu'incident enfant de l'incident de sécurité majeur.
   Une fois que l'incident est lié en tant qu'incident enfant à un incident de sécurité majeur, la balise **d'incident de sécurité majeur** est appliquée et affichée sur la bannière du formulaire.

Utiliser les actions d'interface utilisateur du formulaire

Les actions d'interface utilisateur affichées sur le formulaire d'incident de sécurité sont les suivantes.

Pour accéder aux actions d'interface utilisateur du formulaire :

1. Accéder à **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez un incident de sécurité dans la vue de liste.
3. Toutes les actions d'interface utilisateur sont présentes dans le coin supérieur droit du formulaire d'incident de sécurité.

Actions d'interface utilisateur du formulaire d'espace de travail

Nom de champ	Description
Discuter	Créez ou démarrez une discussion dans la barre latérale de l'incident de sécurité.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description
Enregistrer	Enregistrez ou mettez à jour l'enregistrement Réponse aux incidents de sécurité après avoir apporté des modifications.
Créer une tâche de réponse	Créez une tâche de réponse pour l'incident de sécurité.
Composer des e-mails	Composez des e-mails pour l'incident de sécurité.
Ajouter un Playbook	Ajoutez manuellement le playbook pour l'incident de sécurité.
Créer un incident	Créez un incident au sein de l'incident de sécurité.
Créer un ticket du service clientèle	Créez un ticket du service clientèle pour l'incident de sécurité qui sera suivi par l'équipe Gestion du service client (CSM). **Remarque :** Cette option est disponible uniquement si Gestion du service clientèle (CSM) est installé.
Ouvrir le(s) Wokflow(s) associé(s)	Ouvrez n'importe quel contexte de workflow associé à l'incident de sécurité. Cette option n'est visible que s'il existe des workflows.
Créer une demande de changement	Créez une demande de changement au sein de l'incident de sécurité.
Créer un problème	Créez un problème dans l'incident de sécurité.
Créer une panne	Créer une panne au sein de l'incident de sécurité.
Calculer la gravité	Calculez la gravité d'un incident de sécurité à l'aide de calculateurs prédéfinis. La gravité est calculée en fonction des règles prédéfinies dans les calculateurs. La gravité d'un incident est basée sur le score de risque, l'impact sur l'entreprise et la priorité.
Exécuter le profil PEPT	Sélectionnez et exécutez le profil PEPT pour l'intégration requise. **Remarque :** Cette option n'est disponible que lorsque des intégrations sont installées.
Lier à l'incident de sécurité majeur	Liez un incident de sécurité à un incident de sécurité majeur.
Signaler un événement à risque	Signalez cet incident de sécurité comme événement à risque à l'équipe de gestion des risques. L'équipe de gestion des risques analyse l'événement et s'assure que de tels événements et les pertes associées ne se reproduisent pas. **Remarque :** Cette option n'est disponible que lorsque Risk Management est installé.
Dissocier d'un incident de sécurité majeur	Dissocier d'un incident de sécurité majeur.
Proposer comme incident de sécurité majeur	Proposez un incident de sécurité en tant qu'incident de sécurité majeur.
Promouvoir en incident de sécurité majeur	Promouvoir un incident de sécurité comme un incident de sécurité majeur.

Traduction automatique

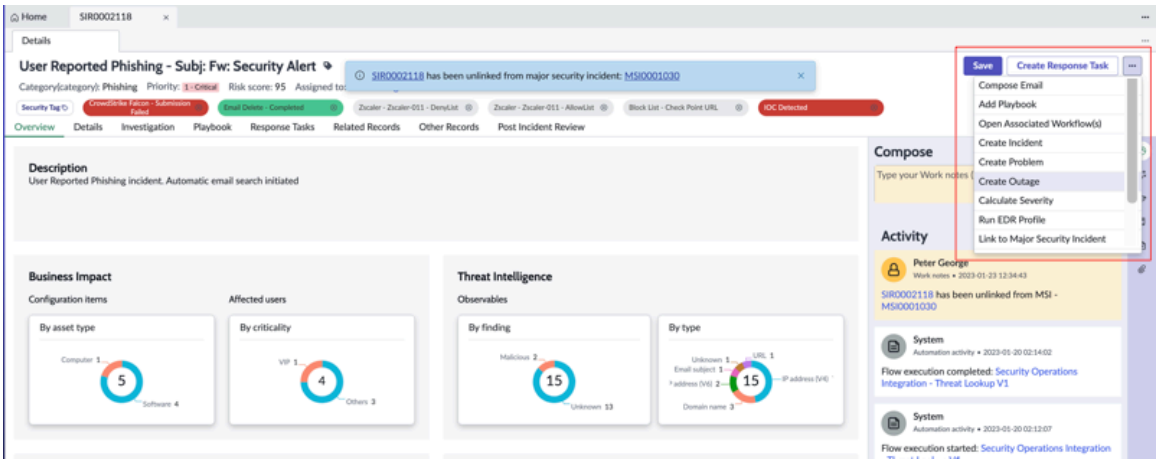
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description
Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison	Exécutez des actions supplémentaires sur le point de terminaison. **Remarque :** Cette option n'est disponible que lorsque des intégrations de point de terminaison sont installées. Par exemple : FireEye HX
Créer un nouvel événement dans MISP	Créez et modifiez des événements dans MISP automatiquement ou manuellement. **Remarque :** Cette option n'est disponible que lorsque l'intégration MISP est installée.
Associer la technique MITRE ATT&K	Associer les techniques MITRE ATT&K à l'incident de sécurité. **Remarque :** Cette option est disponible lorsque MITRE ATT&K est installé.
Afficher l'info MITRE ATT&K	Affiche les informations MITRE ATT&K associées à l'incident de sécurité. **Remarque :** Cette option est disponible lorsque MITRE ATT&K est installé.
Ajouter au ticket de sécurité	Ajoutez l'incident de sécurité à un ticket de sécurité existant ou nouveau. **Remarque :** Cette option est disponible lorsque Renseignements sur les menaces est installé.
Basculer vers l'interface utilisateur classique	Permettez à l'analyste de basculer entre l'interface utilisateur classique et la nouvelle interface utilisateur afin qu'il puisse également travailler sur les fonctionnalités existantes qui ne sont pas encore disponibles dans le nouvel espace de travail.
Abolir	Annuler un incident de sécurité. Une fois que vous avez sélectionné **Annuler** tous les enregistrements connexes tels que les tâches de réponse, les incidents de sécurité enfants sont également annulés.
Supprimer	Supprimer un enregistrement d'incident de sécurité.

4. Cliquez sur le numéro d'un incident de sécurité pour afficher l'enregistrement de l'incident de sécurité. Vous pouvez voir les actions d'interface utilisateur en haut de la page.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Workflow de fermeture d'incident de sécurité

Fermez l'incident de sécurité en mettant à jour l'état de l'incident.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

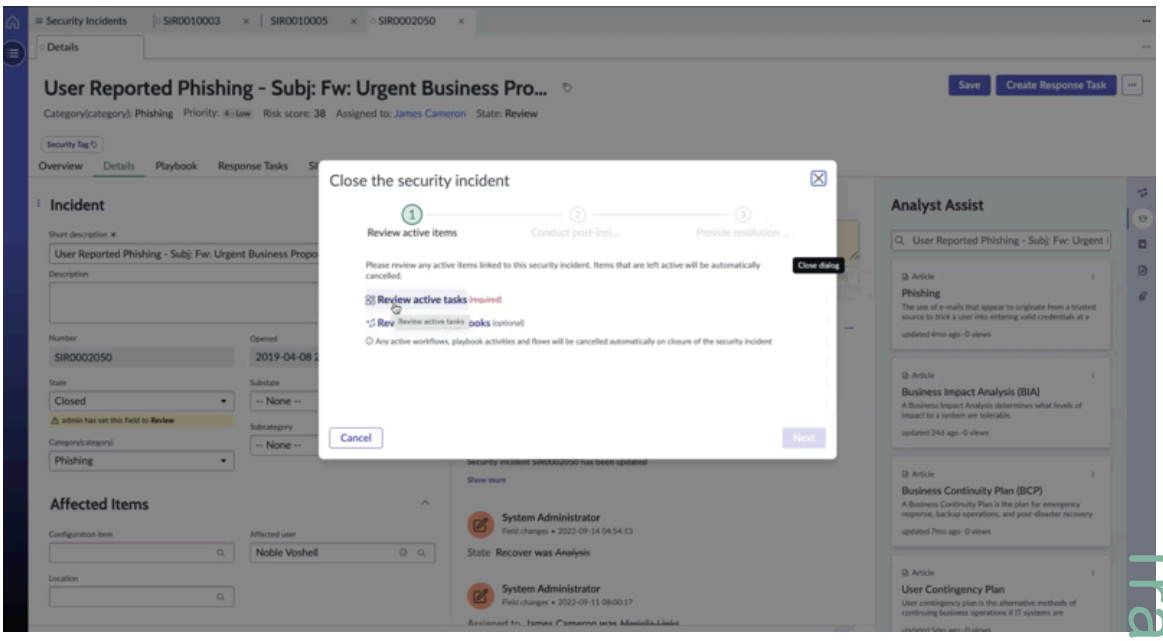
1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Par exemple, accédez à **Listes** > **Incidents de sécurité** > **Incidents ouverts**.
3. Ouvrez un incident que vous souhaitez fermer.
4. Accédez à l'onglet **Détails** .
5. Explorez l'état de l'incident et sélectionnez **Fermer**.
6. Effectuez les activités de clôture.

    - Il s'agit d'une étape obligatoire pour examiner n'importe quelle tâche avant de fermer un incident de sécurité. Toutes les tâches de réponse doivent être examinées par l'analyste et fermées ou annulées avant d'être fermées en tant qu'incident de sécurité. Lorsque l'analyste clique sur Examiner les **tâches actives**, il dirige l'utilisateur vers l'onglet **Tâches de réponse** . Un message de session s'affiche et indique que vous êtes sur le point de fermer un incident de sécurité. Cliquez sur **Continuer**.
    - Cliquez sur **Continuer**. La première étape – examiner les tâches actives lors de la fermeture de l'incident de sécurité – est terminée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

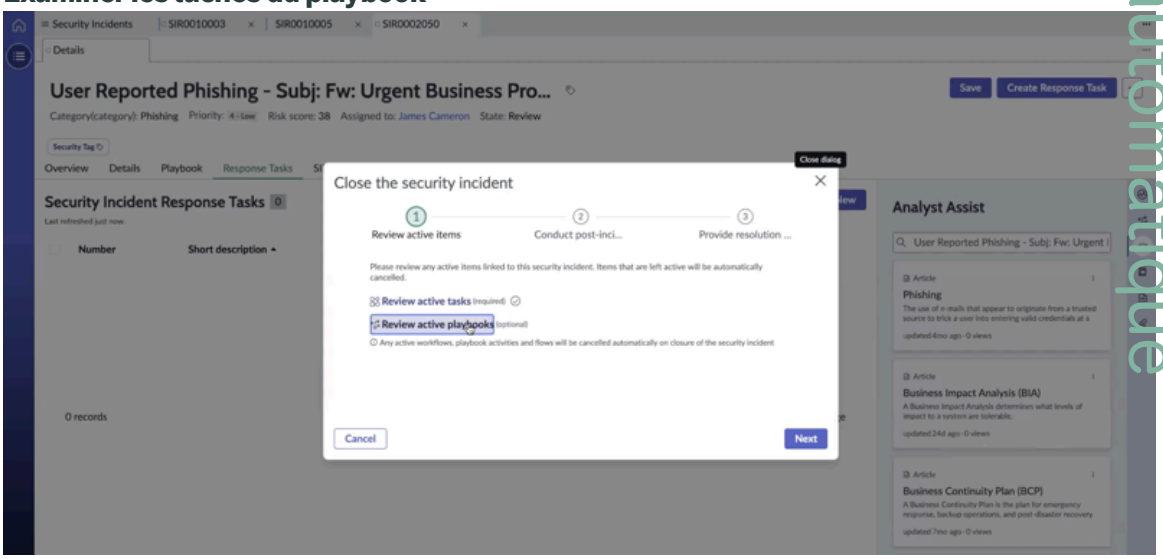
Examen des tâches de fermeture



- Passez à l'étape suivante pour examiner les playbooks actifs pour que l'analyste les examine, qui est une étape facultative. Vous pouvez cliquer sur le lien pour examiner les tâches Playbook actives et les fermer si nécessaire.

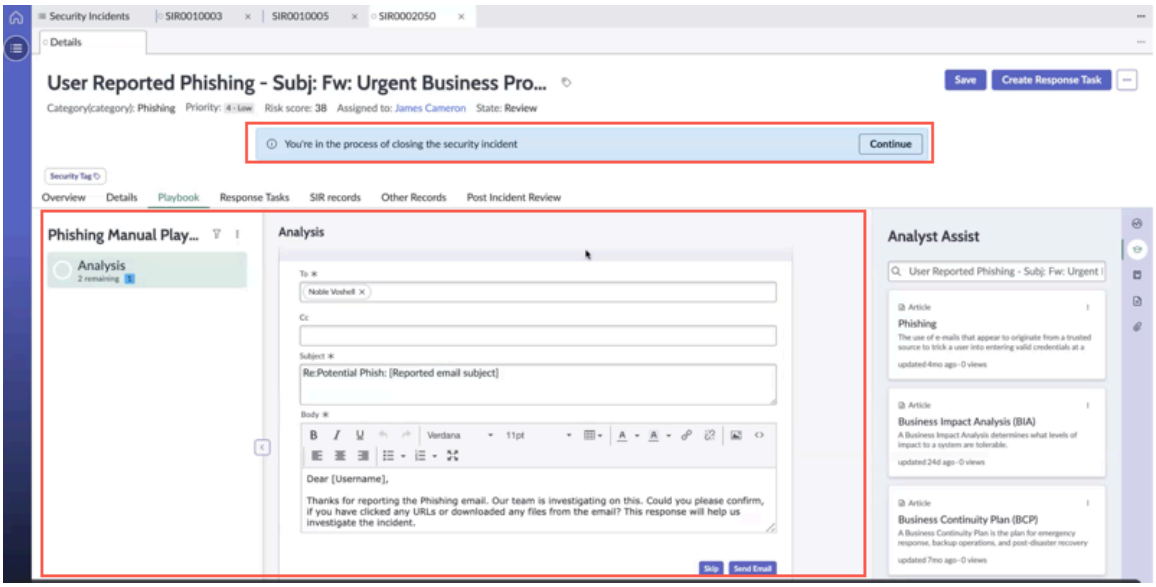
  Remarque : Tous les workflows, activités de Playbook et flux actifs seront automatiquement annulés lors de la fermeture de l'incident de sécurité.

Examiner les tâches du playbook



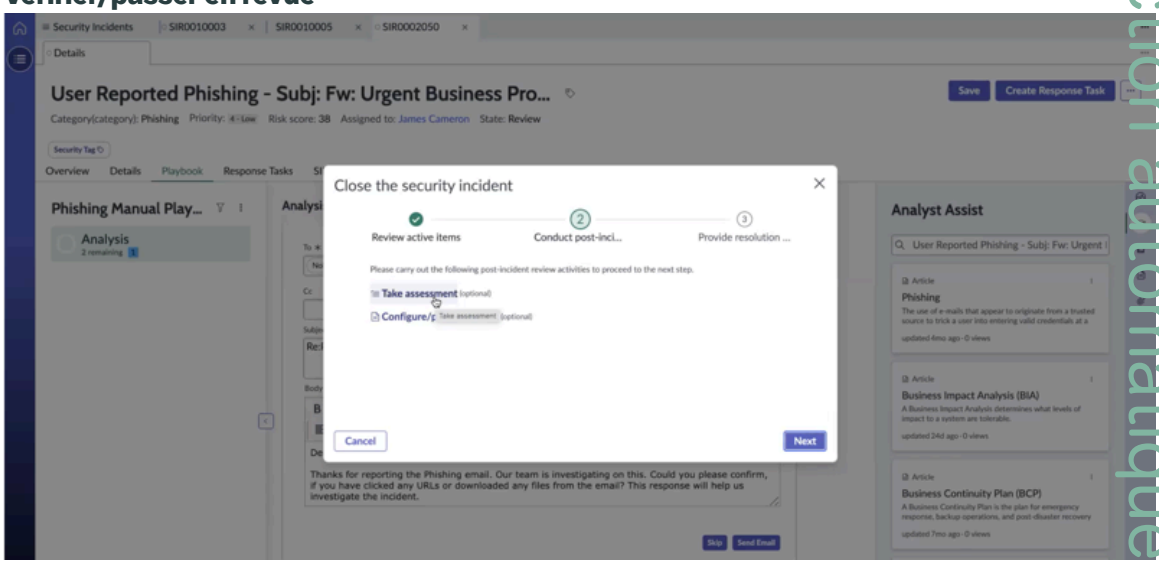
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



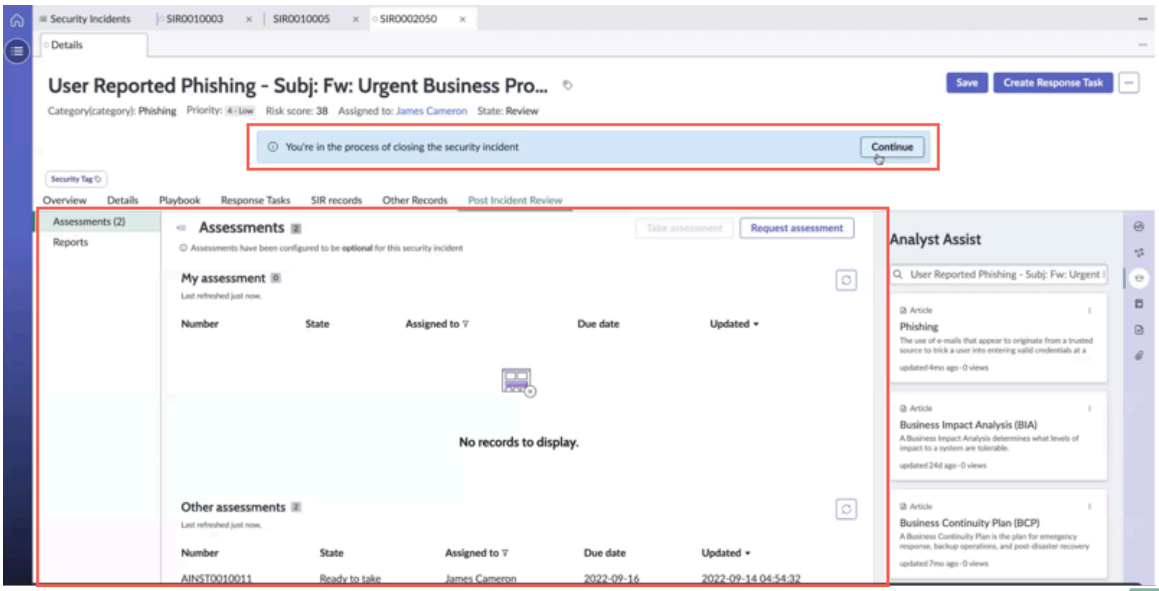
- Rapport d'examen post-incident : vous allez maintenant passer en revue les activités post-incident pour poursuivre la fermeture. Si l'évaluation est facultative, ignorez l'étape ou, si l'évaluation est obligatoire, passez l'évaluation et terminez-la.

Vérifier/passer en revue

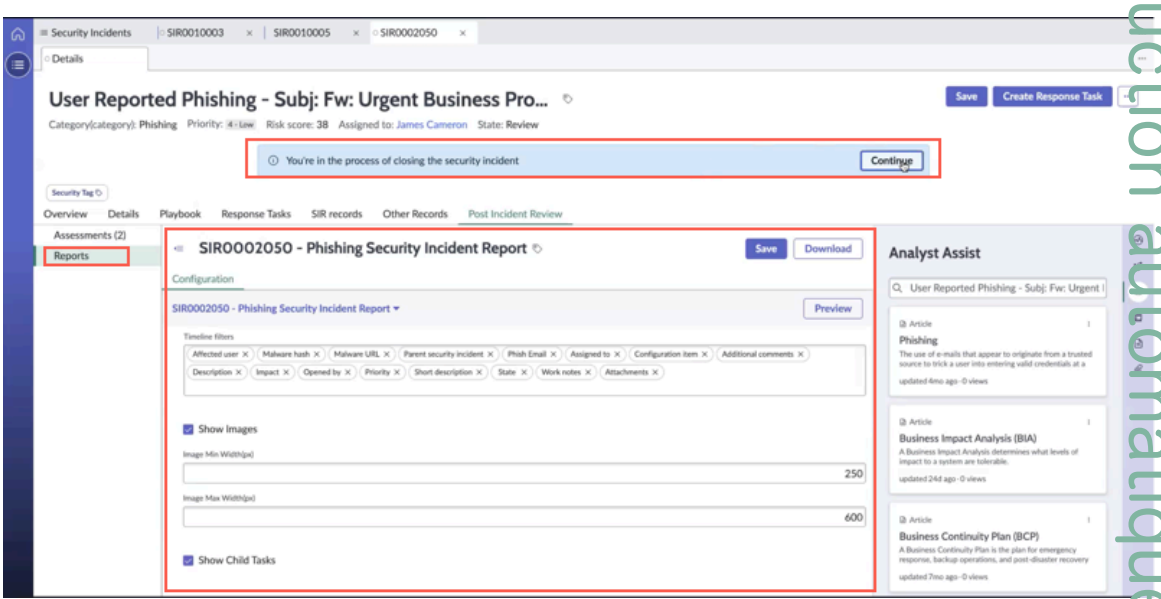


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- Configurer/prévisualiser le rapport : Il s'agit à nouveau d'une étape facultative. Cliquez sur le lien pour examiner le rapport et passer à l'étape **suivante** .

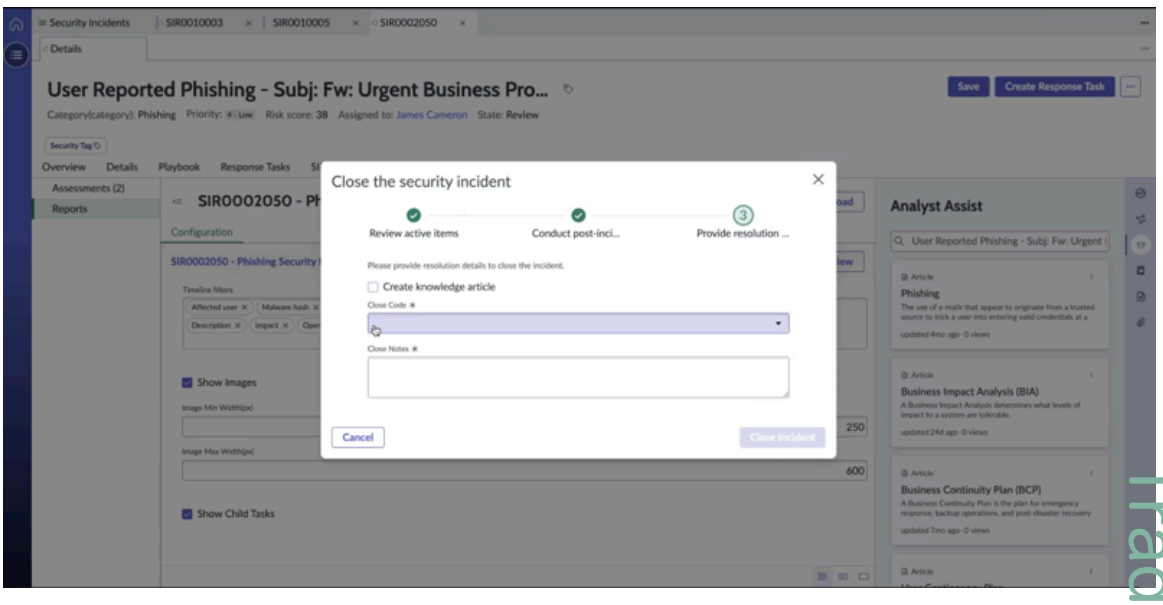


- Fournir les détails de la résolution : l'analyste peut cocher la case pour créer automatiquement des articles de la base de connaissances.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Fournissez le code de fermeture, les notes de fermeture et cliquez sur **Fermer l'incident**.



Remarque : Si l'analyste annule la boîte de dialogue **Fermer l'incident de sécurité** , il peut accéder à l'onglet **Détails** et changer l'état de l'incident sur **Fermé** pour poursuivre la fermeture.

Affichage des tableaux de bord de l'espace de travail SIR

Cette section présente les mesures importantes pour analyser votre Réponse aux incidents de sécurité processus, telles que les nouveaux incidents de sécurité ou l'ancienneté moyenne des incidents de sécurité ouverts.

Dans l'interface utilisateur classique, il existe quelques tableaux de bord standard disponibles sous la page d'accueil et Analyse des performances Tableaux de bord disponibles lorsque Analyse des performances le module d'extension Réponse aux incidents de sécurité est installé. Tous ces éléments seront désormais disponibles dans le nouvel espace de travail sous la section **Tableaux de bord SIR** .

Tableaux de bord standard sous la page d'accueil :

- Aperçu de Security Incident Response
  - Vue d'ensemble des analystes
  - Vue d'ensemble du gestionnaire (prise en charge dans les versions futures)
  - Vue d'ensemble du CISO (prise en charge dans les versions futures)
- **Platform Analytics pour** *`Réponse aux incidents de sécurité`*
  - Explorateur des incidents de sécurité
  - Tableau de bord des CISO (version future)
  - Sécurité – Gestion des incidents
  - KPI de gestion des incidents de sécurité de premier plan
  - Efficience de Opérations de sécurité
  - Analyse contextuelle : tableau de bord SI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Il peut y avoir une répétition des tableaux de bord dans l'analyse standard et de plateforme pour les tableaux de bord de Réponse aux incidents de sécurité tels que le Tableau de bord CISO. Lorsque le module d'extension est installé, il y a du contenu supplémentaire dans ces tableaux de bord et il n'est pas disponible en tant que doublon.

Les utilisateurs doivent installer le module d'extension pour que les tableaux de bord répertoriés sous Analyse de la plateforme pour les tableaux de bord Réponse aux incidents de sécurité soient présents dans l'espace de travail. Sinon, seuls les tableaux de bord standard seront disponibles.

Dans la version actuelle du , les tableaux de bord suivants sont disponibles dans la section Tableaux de Espace de travail SIR**bord SIR**. Les autres tableaux de bord manquants seront disponibles dans les versions ultérieures.

Tableaux de bord Security Incident Response

Tableau de bord	Description
Tableau de bord standard	
Vue d'ensemble des analyses de sécurité	Grâce à ce tableau de bord, les analystes de sécurité peuvent afficher les incidents de sécurité résumés en fonction du travail prioritaire critique de l'analyste, du travail prioritaire, des incidents de sécurité affectés à l'analyste, des tâches affectées aux analystes et du nombre d'incidents.
Analyse des performances (PA) pour les tableaux de bord Security Incident Response	
Explorateur des incidents de sécurité	Grâce à ce tableau de bord, les gestionnaires et les analystes de sécurité peuvent afficher les incidents de sécurité résumés et regroupés par catégorie, sous-catégorie, emplacement, priorité et impact sur l'entreprise. Ces vues permettent aux gestionnaires et aux analystes d'avoir rapidement une idée de la fréquence à laquelle les attaques se produisent et des services aux entreprises touchés.
Sécurité – Gestion des incidents	Grâce à ce tableau de bord, les responsables de la sécurité peuvent facilement suivre le volume, les performances et la progression des incidents de sécurité, de l'analyse et de la détection initiales au confinement, à l'éradication et à la récupération.
Tableau de bord des CISO	Proposition de prise en charge dans une version future.
Efficience de Opérations de sécurité	Grâce à ce tableau de bord, les gestionnaires et les analystes peuvent consulter les mesures d'efficacité globales et mesurer les performances du SOC.
KPI de gestion des incidents de sécurité de premier plan	Grâce à ce tableau de bord, les responsables de la sécurité peuvent suivre et visualiser le volume, les performances et la progression des incidents de sécurité, de l'analyse initiale/détection au confinement, à l'éradication et à la récupération.
Analyse contextuelle :	Grâce à ce tableau de bord, les gestionnaires et les analystes peuvent afficher les incidents de sécurité ouverts, l'âge moyen des incidents de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableaux de bord Security Incident Response (suite)

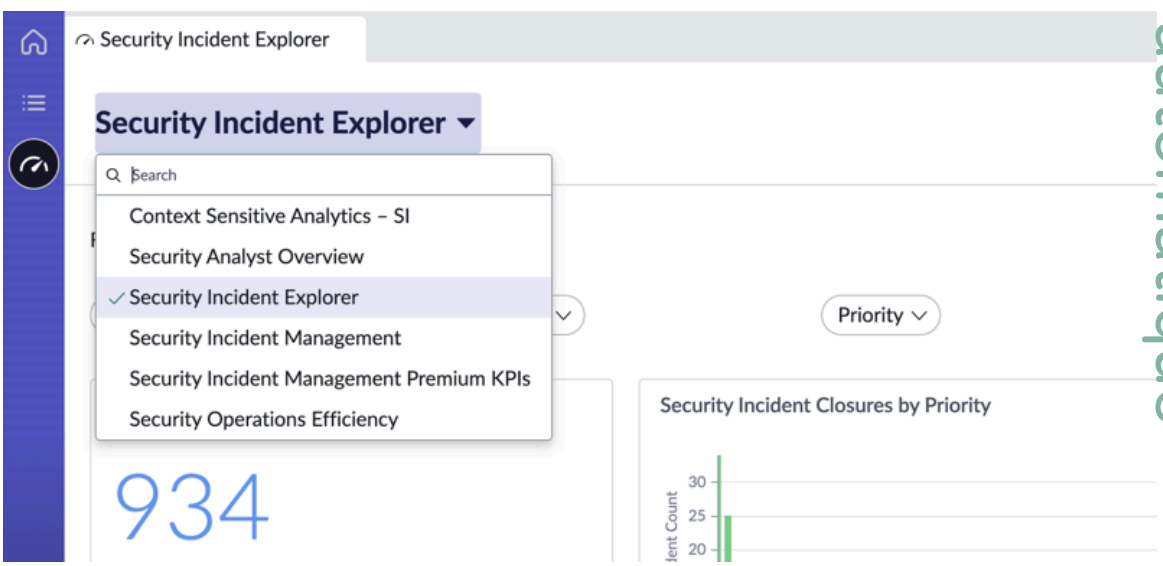
Tableau de bord	Description
	ouverts, le délai moyen de clôture des incidents de sécurité, le pourcentage d'incidents de sécurité qui ont été ouverts et fermés le même jour et le pourcentage d'incidents qui n'ont pas été mis à jour au cours des 5 derniers jours et des 30 derniers jours.

Accéder aux tableaux de bord SIR et PA

L'icône **Tableaux de bord SIR** affichée sur le côté gauche de la page d'accueil de l'espace de travail.

Remarque : Les utilisateurs disposant de l'accès sn_si.manager ou sn_si.admin peuvent modifier les tableaux de bord. Les utilisateurs doivent être dans le même champ d'application des tableaux de bord que l'utilisateur essaie d'apporter des modifications. Par exemple, le tableau de bord de vue d'ensemble des analystes de sécurité est disponible dans l'espace de travail SIR. L'utilisateur doit alors également se trouver dans le même champ d'application de l'espace de travail SIR pour apporter les modifications au tableau de bord.

1. Accédez à la **Espaces de travail** > **Espace de travail de la Gestion des incidents de sécurité**.
2. Cliquez sur l'icône du **de bord des tableaux de bord SIR**.
3. Sélectionnez le tableau de bord souhaité dans la liste déroulante.



Vous pouvez modifier les tableaux de bord, y ajouter de nouveaux éléments et créer vos propres tableaux de bord. Pour plus d'informations sur l'utilisation des tableaux de bord, voir Utilisation de tableaux de bord réactifs

Afficher le tableau de bord Vue d'ensemble des analystes de la sécurité

Grâce à ce tableau de bord, les analystes de sécurité peuvent afficher les incidents de sécurité résumés en fonction du travail prioritaire critique et du travail prioritaire des analystes, des incidents de sécurité affectés à l'analyste, des tâches affectées aux analystes et du nombre d'incidents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

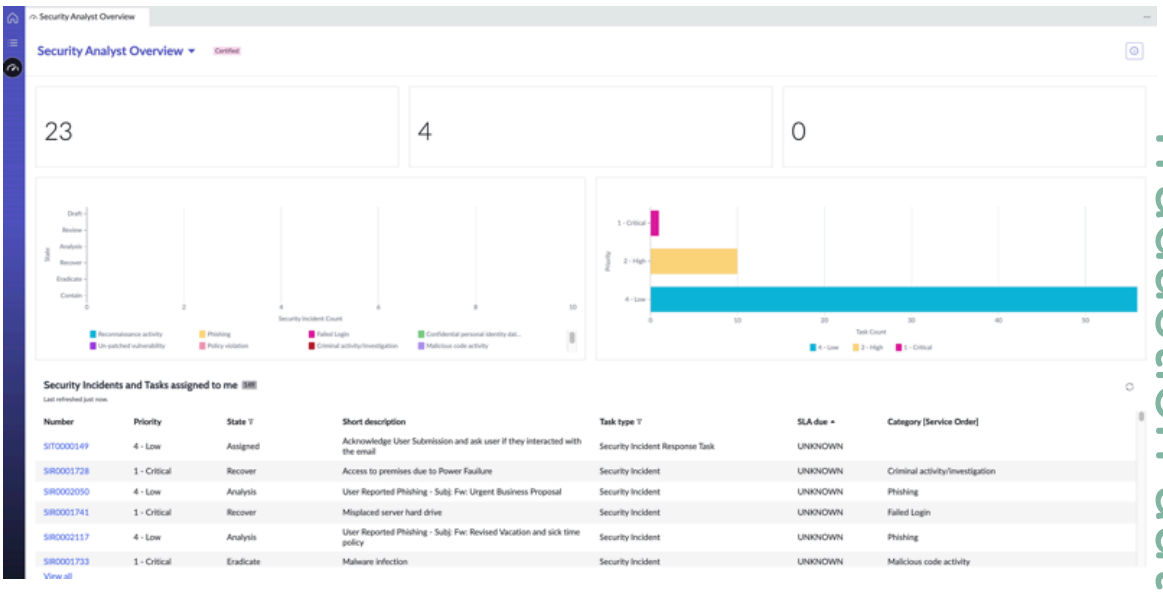
Avant de commencer

Par défaut, le tableau de bord Vue d'ensemble des analystes de la sécurité s'affiche pour les utilisateurs disposant d'un accès sn_si.analyst.

Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , qui s'affiche sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Vue d'ensemble des analystes de sécurité** dans la liste déroulante.



Consultez le tableau de bord Vue d'ensemble de l'analyste de la sécurité pour d'autres actions. Pour en savoir plus sur le tableau de bord Vue d'ensemble des analystes de la sécurité, reportez-vous à la section Réponse aux incidents de sécurité Platform Analytics et Reporting.

Afficher le tableau de bord de l'explorateur des incidents de sécurité

Grâce à ce tableau de bord, les responsables de la sécurité peuvent visualiser les incidents de sécurité résumés et regroupés par catégorie, sous-catégorie, emplacement, priorité et impact sur l'entreprise.

Avant de commencer

Par défaut, le tableau de bord Explorateur des incidents de sécurité s'affiche pour les utilisateurs disposant d'un accès sn_si.manager.

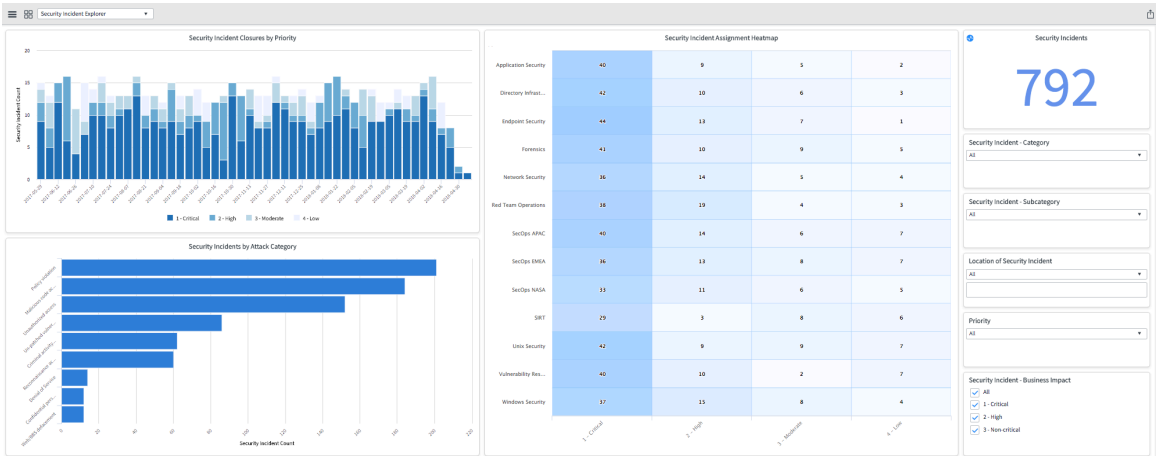
Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , qui s'affiche sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **l'Explorateur des incidents de sécurité** dans la liste déroulante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Consultez le tableau de bord de l'explorateur d'incidents de sécurité pour les actions ultérieures. Pour des informations détaillées sur le tableau de bord de l'explorateur des incidents de sécurité, voir le tableau de bord de l'explorateur des incidents de sécurité

Dans la version actuelle, la liste de rapports suivante n'est pas prise en charge dans le tableau de bord de l'explorateur d'incidents de sécurité :

- Carte thermique d'affectation des incidents de sécurité : la visualisation de la carte thermique n'est pas disponible.
- Carte des incidents de sécurité : la visualisation de la carte n'est pas disponible.

Afficher le tableau de bord Gestion des incidents de sécurité

Grâce à ce tableau de bord, les responsables de la sécurité peuvent facilement suivre le volume, les performances et la progression des incidents de sécurité, de l'analyse et de la détection initiales au confinement, à l'éradication et à la récupération.

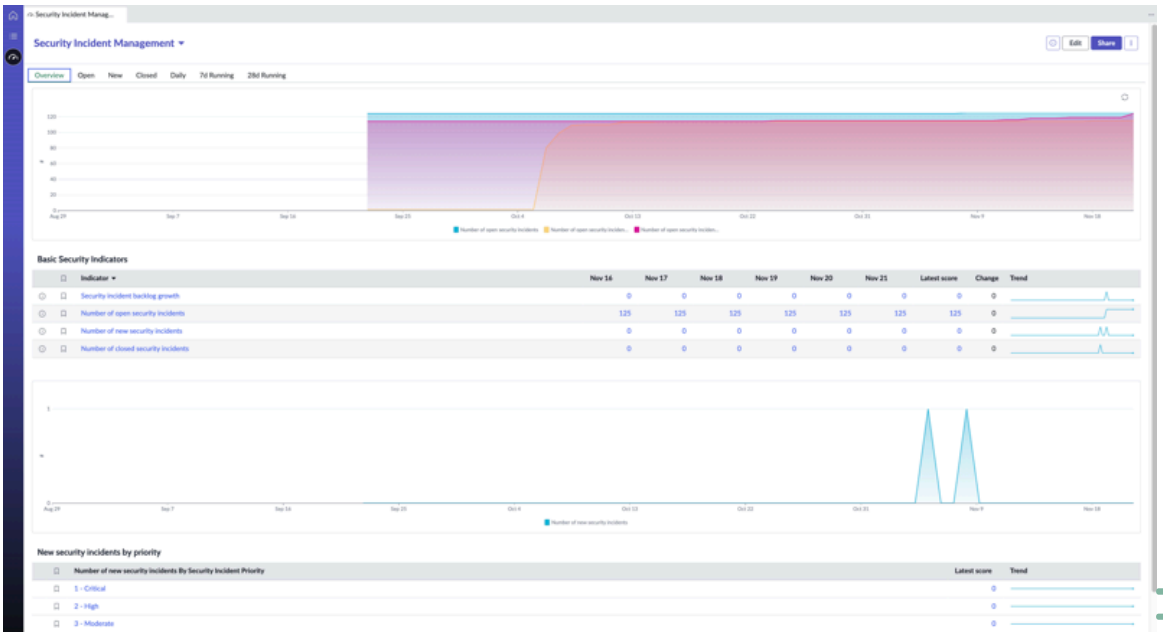
Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , qui s'affiche sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Gestion des incidents de sécurité** dans la liste déroulante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Consultez le tableau de bord de la gestion des incidents de sécurité pour une action ultérieure. Pour des informations détaillées sur le tableau de bord Gestion des incidents de sécurité, voir Tableau de bord Gestion des incidents de sécurité

Afficher le tableau de bord Efficacité de Security Operations

Les gestionnaires du centre des opérations de sécurité (SOC) peuvent afficher les mesures d'efficacité globales et mesurer les performances individuelles des membres de l'équipe SOC au sein de l'organisation.

Avant de commencer

Dans la version actuelle, le rapport suivant n'est pas pris en charge dans le tableau de bord Efficacité de Security Operations :

- Analyse de l'étape de l'incident de sécurité - La console n'est pas disponible

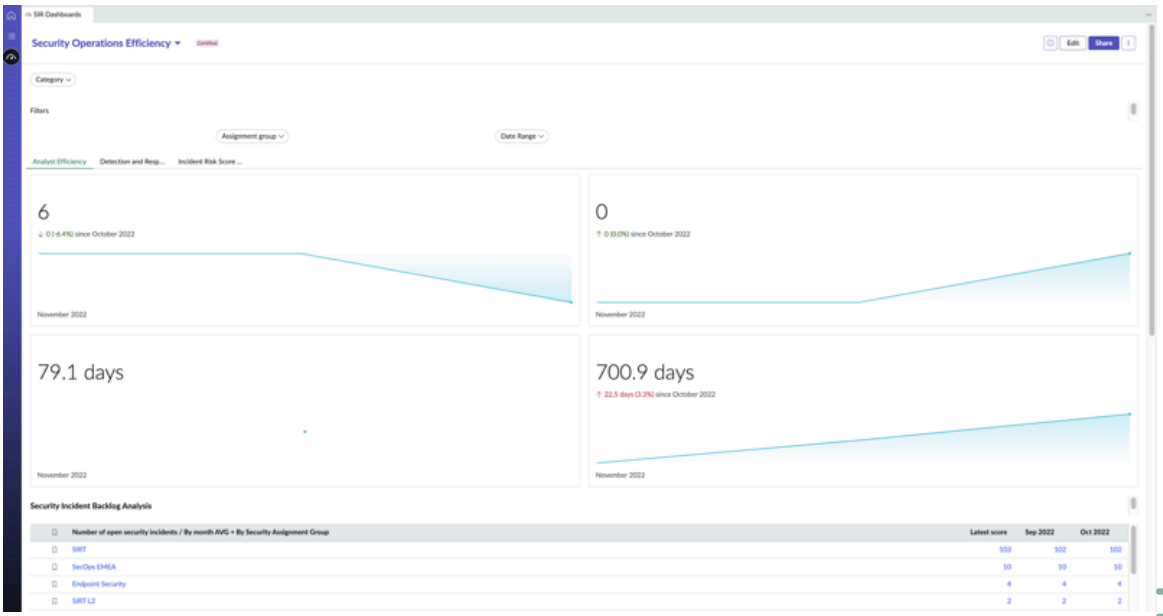
Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , qui s'affiche sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Efficacité de Security Operations dans** la liste déroulante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Consultez le tableau de bord Efficacité de Security Operations pour une action ultérieure. Pour des informations détaillées sur le tableau de bord Efficacité de Security Operations, consultez le tableau de bord Efficacité de Security Operations

Afficher le tableau de bord des KPI de Security Incident Response Premium

Grâce à ce tableau de bord, les responsables de la sécurité peuvent suivre et visualiser le volume, les performances et la progression des incidents de sécurité, de l'analyse initiale/détection au confinement, à l'éradication et à la récupération.

Avant de commencer

Dans la version actuelle, la liste de rapports suivante n'est pas prise en charge dans le tableau de bord KPI Premium de Security Incident Response :

- Processus par état : la console n'est pas disponible
- Processus par âge : la console n'est pas disponible
- Incidents de sécurité ouverts depuis plus de 30 jours par groupe d'affectation et par état : la visualisation de la carte thermique n'est pas disponible.
- Incidents de sécurité non mis à jour pendant plus de 30 jours par groupe d'affectation et par état : la visualisation de la carte thermique n'est pas disponible.
- Incidents de sécurité avec un délégataire qui n'est pas actif : la visualisation de la carte thermique n'est pas disponible.

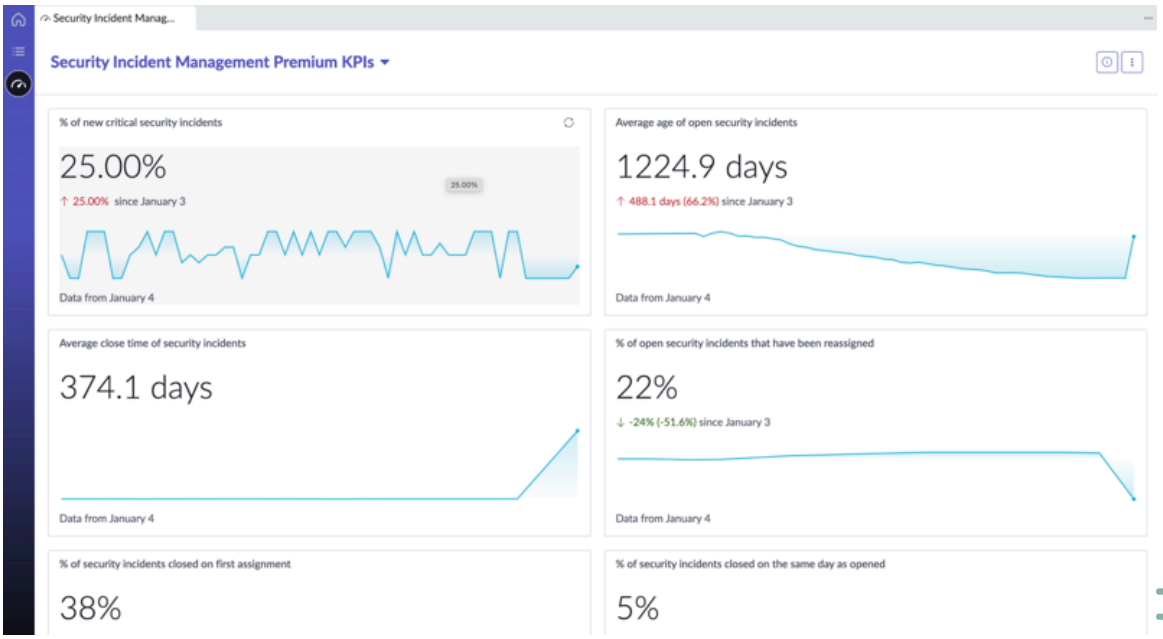
Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , qui s'affiche sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **les KPI Premium de Security Incident Response** dans la liste déroulante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Consultez le tableau de bord des KPI Premium de Security Incident Response pour connaître les prochaines actions.
   Pour des informations détaillées sur le tableau de bord KPI de Security Incident Response Premium, consultez le tableau de bord de Security Incident Management Premium

Afficher l'analyse contextuelle : tableau de bord SI

Grâce à ce tableau de bord, les gestionnaires et les analystes peuvent afficher les incidents de sécurité ouverts, l'âge moyen des incidents de sécurité ouverts, le délai moyen de clôture des incidents de sécurité, le pourcentage d'incidents de sécurité qui ont été ouverts et fermés le même jour et le pourcentage d'incidents qui n'ont pas été mis à jour au cours des 5 derniers jours et des 30 derniers jours.

Avant de commencer

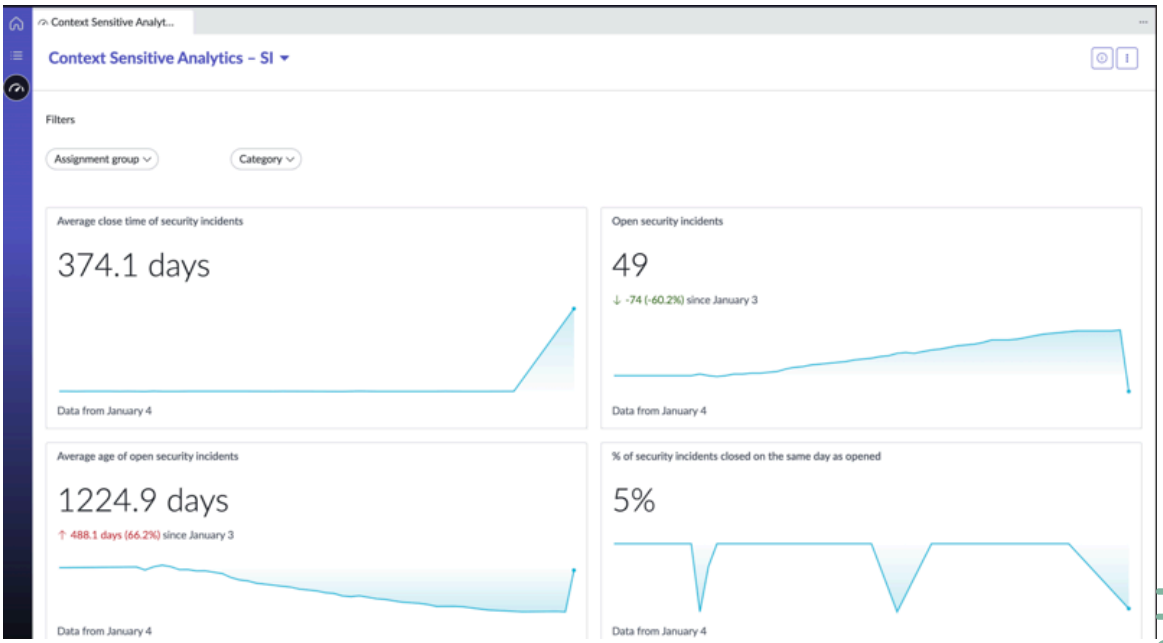
Rôle requis : sn_si.analyst (lecture), sn_si.manager ou sn_si.admin (écriture)

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** , qui s'affiche sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez **Analyse contextuelle – SI** dans la liste déroulante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Consultez le tableau de bord Analyse contextuelle – SI pour d'autres actions.

Afficher le tableau de bord des CISO

Ce tableau de bord fournit aux responsables de la sécurité de l'information (CISO) une vue d'ensemble de haut niveau des incidents de sécurité et des tendances des incidents hebdomadaires sur l'instance sous la forme de graphiques graphiques. Ces graphiques vous aident à visualiser et à analyser efficacement les performances du centre des opérations de sécurité (SOC).

Avant de commencer

- Rôle requis : sn_si.admin et sn_si.ciso - Modifiez et affichez les incidents.
- Assurez-vous que l'application Analyse des performances pour Réponse aux incidents de sécurité est installée.

Pourquoi et quand exécuter cette tâche

Remarque : Le tableau de bord du CISO et le tableau de bord Vue d'ensemble du CISO étaient deux tableaux différents dans l'interface utilisateur classique. Mais maintenant, les capacités des deux tableaux de bord ont été fusionnées sous le tableau de bord CISO.

Le tableau de bord CISO fournit des informations clés sur vos incidents de sécurité chaque semaine. Vous pouvez configurer des indicateurs et collecter des instantanés de données des incidents correspondant aux conditions des propriétés de l'indicateur. Les données collectées sont ensuite visualisées à l'aide de widgets dans le tableau de bord.

Vous pouvez visualiser les tendances hebdomadaires à l'aide des widgets du tableau de bord CISO. Les données ou les statistiques relatives aux tendances de vos incidents de sécurité sont collectées à partir des propriétés de l'indicateur d'incidents hebdomadaires qui sont définies par l'organisation. Vous pouvez obtenir des aperçus clés à l'aide des graphiques suivants :

- **Durée moyenne pour l'identification (hebdomadaire)** : ce graphique illustre la durée hebdomadaire moyenne nécessaire pour identifier un incident de sécurité.
- **Durée moyenne pour contenir (hebdomadaire)** : ce graphique illustre la durée hebdomadaire moyenne nécessaire pour contenir un incident de sécurité.

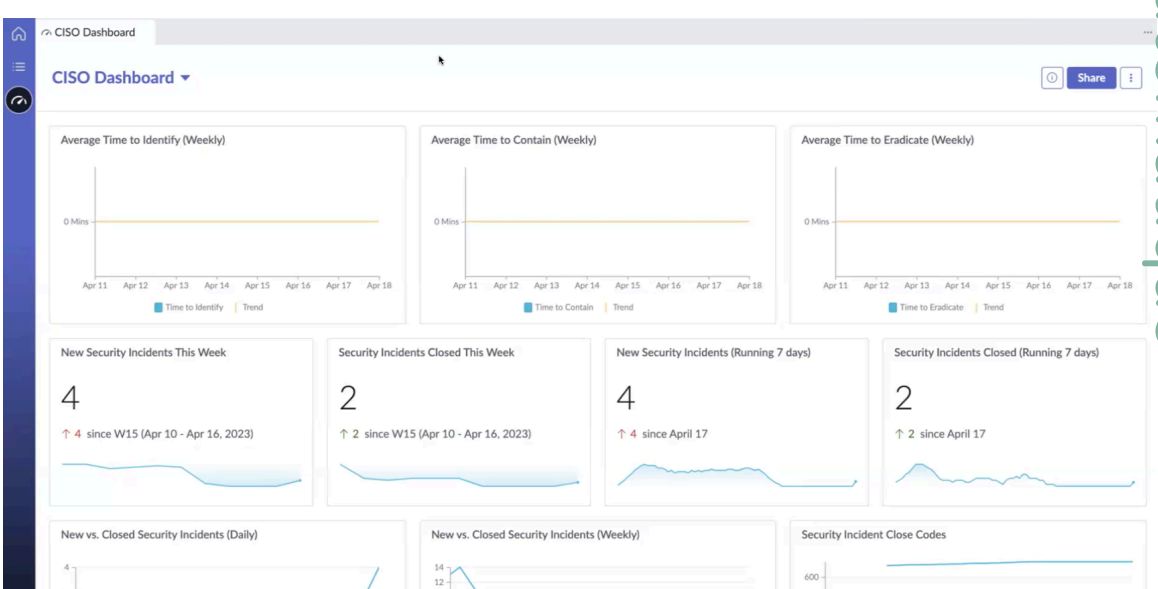
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Durée moyenne pour éradiquer (hebdomadaire)** : ce graphique illustre la durée hebdomadaire moyenne nécessaire pour supprimer un incident de sécurité.
- **Nouveaux incidents de sécurité cette semaine** : ce graphique illustre le nombre de nouveaux incidents de sécurité cette semaine.
- **Incidents de sécurité fermés cette semaine** : ce graphique illustre le nombre d'incidents de sécurité fermés cette semaine.
- **Nouveaux incidents de sécurité (sur 7 jours)** : ce graphique illustre le nombre de nouveaux incidents de sécurité qui s'exécutent pendant une semaine.
- **Incidents de sécurité clôturés (sur 7 jours)** : ce graphique illustre le nombre de nouveaux incidents de sécurité qui sont fermés mais qui s'exécutent pendant une semaine.
- **Incidents nouveaux par rapport aux incidents fermés (quotidien)** : ce graphique illustre la comparaison entre les nouveaux incidents de sécurité quotidiens et les incidents de sécurité fermés quotidiens.
- **Incidents nouveaux par rapport aux incidents fermés (hebdomadaire)** : ce graphique illustre la comparaison entre les nouveaux incidents de sécurité hebdomadaires et les incidents de sécurité fermés chaque semaine.
- **Codes fermés d'incidents de sécurité** : ce graphique illustre les codes fermés des incidents de sécurité.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez le **tableau de bord des CISO** dans la liste déroulante.



4. Consultez le tableau de bord des CISO pour les actions à suivre.

Afficher le tableau de bord de la vue d'ensemble de la génération de rapports CISO

Ce tableau de bord fournit aux responsables de la sécurité de l'information (CISO) une vue d'ensemble des rapports de haut niveau sur les incidents de sécurité et les tendances des incidents hebdomadaires sur l'instance sous la forme de graphiques graphiques. Ces

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

graphiques vous aident à visualiser et à analyser efficacement les performances du centre des opérations de sécurité (SOC).

Avant de commencer

Rôle requis : sn_si.admin et sn_si.ciso - Modifiez et affichez les incidents.

Pourquoi et quand exécuter cette tâche

Le tableau de bord Vue d'ensemble de la génération de rapports CISO fournit des informations clés sur les incidents de sécurité chaque semaine, et vous pouvez visualiser les tendances hebdomadaires à l'aide de widgets. Vous pouvez obtenir des aperçus clés sur la génération de rapports CISO à l'aide des graphiques suivants :

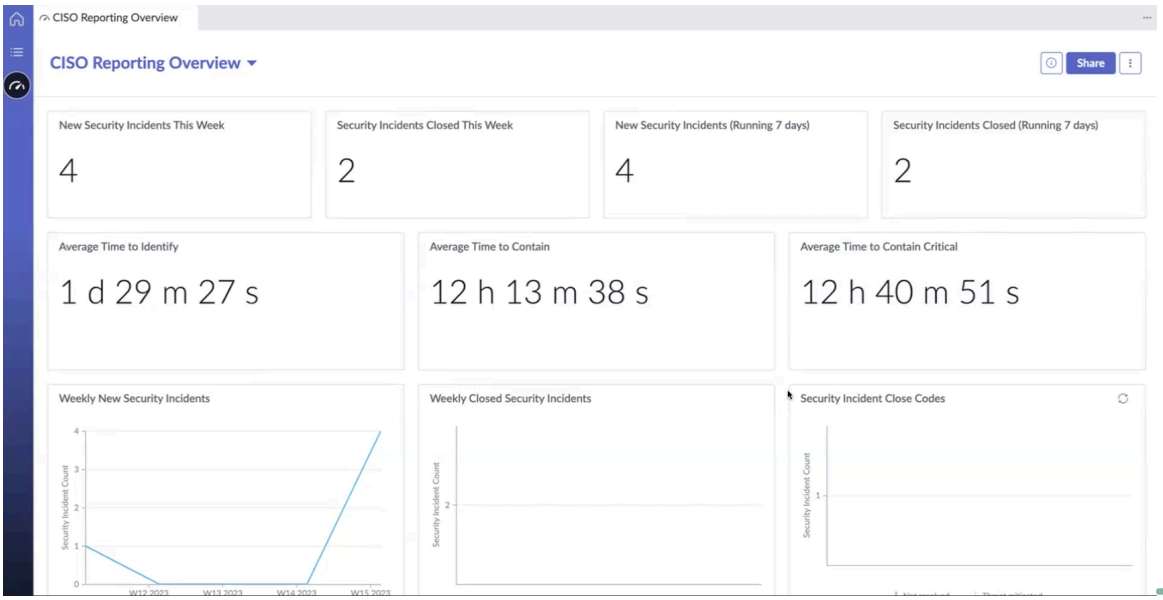
- **Nouveaux incidents de sécurité cette semaine** : cette tuile affiche le rapport du nombre de nouveaux incidents de sécurité cette semaine.
- **Incidents de sécurité fermés cette semaine** : cette vignette affiche le rapport du nombre d'incidents de sécurité fermés cette semaine.
- **Nouveaux incidents de sécurité (sur 7 jours)** : cette vignette affiche le rapport du nombre de nouveaux incidents de sécurité qui s'exécutent pendant une semaine.
- **Incidents de sécurité clôturés (sur 7 jours)** : cette vignette affiche le rapport du nombre de nouveaux incidents de sécurité clôturés mais en cours d'exécution depuis une semaine.
- **Durée moyenne pour l'identification** : cette vignette affiche le rapport du temps hebdomadaire moyen nécessaire pour identifier les incidents de sécurité.
- **Durée moyenne pour contenir** : cette vignette affiche le rapport du temps hebdomadaire moyen nécessaire pour contenir les incidents de sécurité.
- **Délai moyen pour contenir** critique : cette vignette affiche le rapport du temps hebdomadaire moyen nécessaire pour contenir les incidents de sécurité critiques.
- **Nouveaux incidents de sécurité hebdomadaires** : ce graphique illustre le rapport des nouveaux incidents de sécurité hebdomadaires.
- **Incidents de sécurité fermés chaque semaine** : ce graphique illustre le rapport des incidents de sécurité fermés chaque semaine.
- **Codes fermés d'incidents de sécurité** : ce graphique illustre le rapport des codes fermés des incidents de sécurité.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez Vue **d'ensemble de la génération de rapports CISO** dans la liste déroulante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Consultez le tableau de bord des reporting CISO pour les actions à suivre.

Afficher le tableau de bord de la vue d'ensemble du gestionnaire d'incidents de sécurité

Ce tableau de bord fournit aux gestionnaires une vue d'ensemble de haut niveau des incidents de sécurité critiques ou haute priorité au niveau de l'équipe, des SLA sur le point d'expirer dans 24 heures et des tendances des incidents hebdomadaires sur l'instance sous la forme de rapports et de graphiques graphiques.

Avant de commencer

Rôle requis :

- sn_si.admin : modifier et afficher le tableau de bord.
- sn_si.manager : afficher le tableau de bord.

Pourquoi et quand exécuter cette tâche

Vous pouvez analyser les incidents de sécurité critiques ou haute priorité, ou SLA nécessitant une attention immédiate. Vous pouvez également visualiser les tendances hebdomadaires à l'aide des widgets du tableau de bord Vue d'ensemble du gestionnaire d'incidents de sécurité. Les données ou statistiques des tendances hebdomadaires ou mensuelles de vos incidents de sécurité sont collectées à partir des tables d'incidents définies par l'organisation. Vous pouvez obtenir des aperçus clés à l'aide des graphiques suivants :

- **Incidents de sécurité critiques de l'équipe** : cette vignette affiche le nombre d'incidents de sécurité critiques pour l'équipe cette semaine.
- **Incidents de sécurité élevée de l'équipe** : cette tuile affiche le nombre d'incidents de sécurité élevée pour l'équipe cette semaine.
- **SLA arrivant à expiration dans les 24 heures** : cette tuile affiche le nombre de SLA venant à expiration dans les 24 heures.
- **Durée moyenne pour identifier** : cette vignette affiche le temps hebdomadaire moyen nécessaire pour identifier les incidents de sécurité.
- **Délai moyen pour contenir** : cette vignette affiche le temps hebdomadaire moyen nécessaire pour contenir les incidents de sécurité.

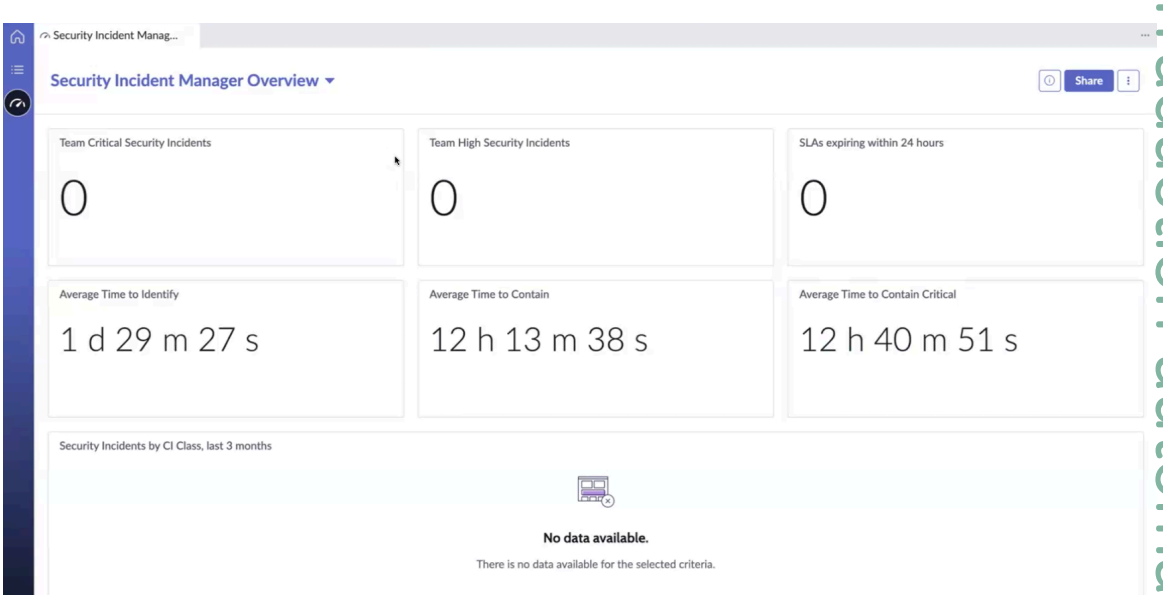
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Délai moyen pour contenir** critique : cette vignette affiche le temps hebdomadaire moyen nécessaire pour contenir les incidents de sécurité critiques.
- **Incident de sécurité par classe CI, 3 derniers mois** : ce graphique illustre les tendances de tous les incidents de sécurité basés sur la classe CI pour les trois derniers mois.
- **Tendance de tous les incidents de sécurité par catégorie** : ce graphique illustre les tendances de tous les incidents de sécurité en fonction de la catégorie.
- **Tendance de tous les incidents de sécurité par priorité** : ce graphique illustre les tendances de tous les incidents de sécurité en fonction de la priorité.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Security Incident Response**.
2. Cliquez sur l'icône **Tableaux de bord SIR** sur le côté gauche de la page d'accueil de l'espace de travail.
3. Sélectionnez Vue **d'ensemble du gestionnaire d'incidents de sécurité** dans la liste déroulante.



4. Consultez la vue d'ensemble du gestionnaire d'incidents de sécurité pour une action ultérieure.

Traduction automatique

Afficher le tableau de bord Intégrité de Security Incident Response

La fonctionnalité du tableau de bord Intégrité de Réponse aux incidents de sécurité fournit une vue centralisée des aspects critiques liés à l'implémentation du processus de réponse aux incidents, des problèmes/erreurs rencontrés et des mesures de performances. Il s'agit d'un outil essentiel pour surveiller et optimiser l'efficacité des options de réponse aux incidents de sécurité d'une organisation.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst ou sn_si.analytics_read : afficher le tableau de bord.

Pourquoi et quand exécuter cette tâche

Vous pouvez surveiller l'intégrité des incidents de sécurité à l'aide des widgets et des graphiques de tendances de chaque application. Ces statistiques présentent un score d'intégrité complet détaillant l'état de la configuration et l'efficacité du rattrapage au sein des applications SIR. Le tableau de bord Intégrité de Security Incident Response prend en charge les quatre onglets suivants :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Processus** : l'onglet affiche un résumé de tous les incidents provenant de différents capteurs d'alerte regroupés une fois par semaine.
- **Implémentation** : cet onglet affiche les personnalisations que les clients effectuent dans leurs instances, notamment les includes de script, les règles métier, les flux et les mises à niveau.
- **Problèmes/Erreurs** : l'onglet affiche les widgets mettant en évidence les erreurs dans les processus d'intégration, les divergences lors de l'ingestion des données brutes d'incident, les erreurs HTTP sortantes dans les applications SIR et tout problème survenant lors de l'exécution des playbooks.
- **Performance** : cet onglet affiche les problèmes de performances dans les applications SIR, notamment la lenteur des requêtes de performances, des règles métier et des scripts.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. Sélectionnez l'icône **Tableaux de bord SIR** sur la page d'accueil de l'espace de travail SIR.
3. Sélectionnez le **tableau de bord Intégrité de Security Incident Response** dans la liste déroulante.
4. Sélectionnez l'onglet **Processus** pour afficher le nombre d'incidents de sécurité qui ont été déclenchés sur une base hebdomadaire pour chaque capteur d'alerte sur le graphique.

Onglet Traitement



Vous pouvez effectuer les tâches suivantes :

a. Sélectionnez un capteur d'alerte sur le graphique pour afficher les détails des KPI du nombre d'incidents de sécurité déclenchés par les capteurs d'alerte en une semaine.

b. Pour obtenir les détails des KPI pour une semaine particulière, utilisez l'option **Calendrier** .

c. Pour comparer les incidents de sécurité déclenchés par le capteur d'alerte, sélectionnez l'option **Comparer les enregistrements** .

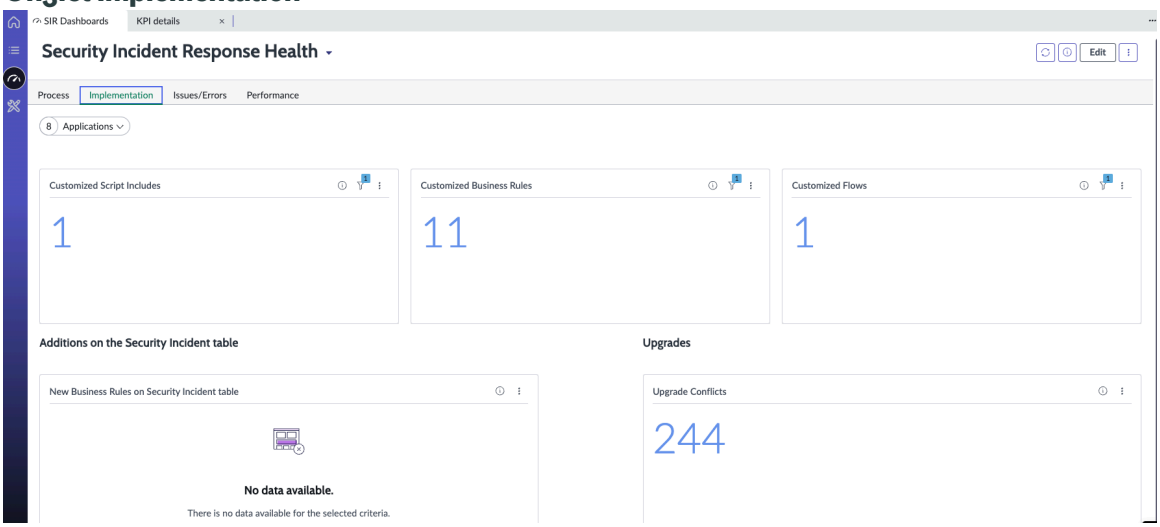
d. Pour utiliser le type de graphique, la série chronologique ou l'analyse, sélectionnez les **options de graphique**.

5. Sélectionnez l'onglet **Implémentation** pour afficher le nombre de personnalisations créées pour les incidents de sécurité dans les applications Security Incident Response.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Implémentation



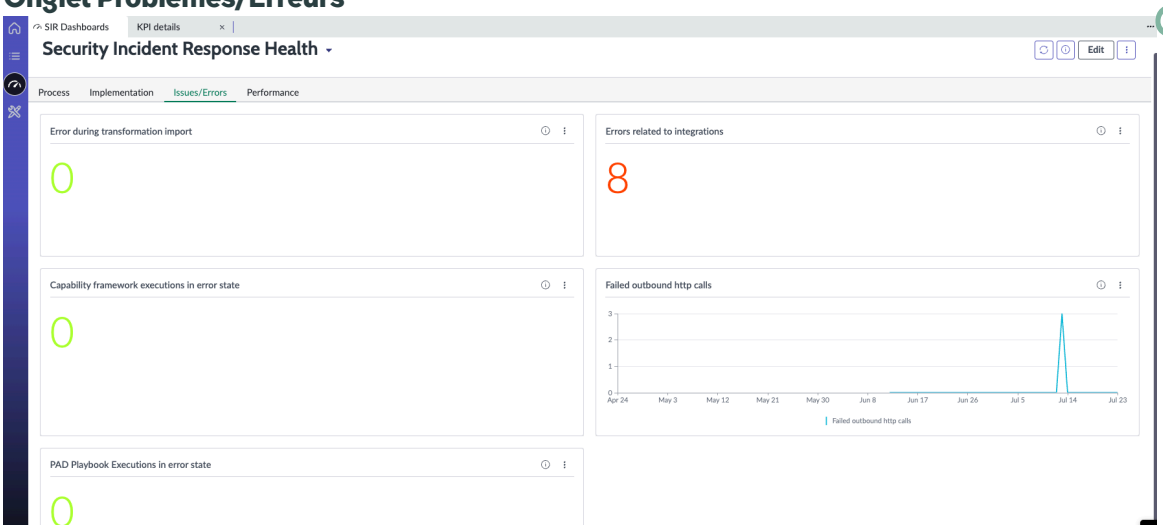
Onglet Implémentation :

Vous pouvez afficher le tableau de bord agrégé pour le nombre de personnalisations qui ont été créées pour chaque application Réponse aux incidents.

- **Includes de script personnalisé** : ce widget affiche le nombre de scripts personnalisés qui ont été ajoutés en fonction de vos besoins dans les applications SIR.
- **Règles métier personnalisées** : ce widget affiche le nombre de règles métier personnalisées qui ont été ajoutées en fonction de vos besoins dans les applications SIR.
- **Flux personnalisés** : ce widget affiche le nombre de flux personnalisés qui ont été ajoutés en fonction de vos besoins dans les applications SIR.
- **Nouvelle règle métier sur la table Incident de sécurité** : ce widget affiche le nombre de règles métier qui ont été créées dans la table Incident de sécurité.
- **Conflits de mise à niveau** : ce widget affiche le nombre de conflits qui ont été déclenchés lors de mises à niveau dans les applications SIR.

6. Sélectionnez l'onglet **Problèmes/Erreurs** pour afficher le nombre de problèmes ou d'erreurs qui ont été déclenchés dans les applications Security Incident Response.

Onglet Problèmes/Erreurs



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

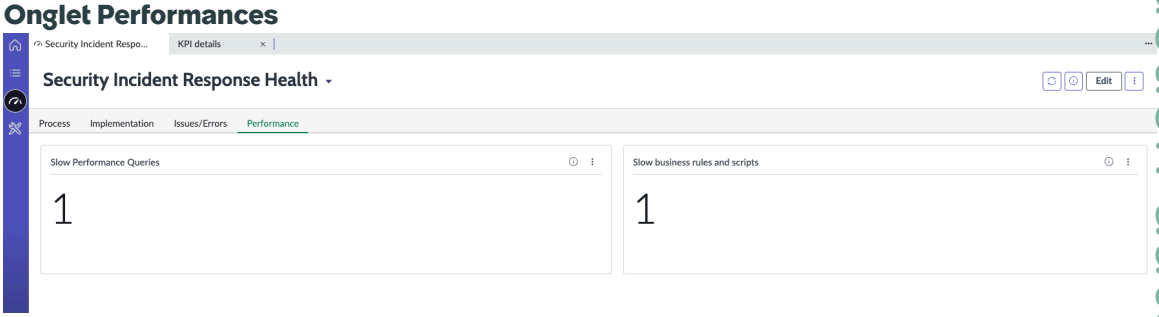
Onglet Problèmes/Erreurs :

Vous pouvez afficher le tableau de bord agrégé des problèmes ou des erreurs dans les applications Réponse aux incidents de sécurité.

- **Erreurs lors de l'importation** de transformation : ce widget affiche le nombre d'erreurs qui ont été déclenchées lors de l'importation de transformation dans les applications SIR.
- **Erreurs liées aux intégrations** : ce widget affiche le nombre d'erreurs qui ont été déclenchées pendant les intégrations SIR.
- **Exécutions du cadre de travail d'aptitude en état d'erreur** : ce widget affiche le nombre d'erreurs qui ont été déclenchées lors des exécutions du cadre de travail d'aptitude dans les applications SIR.
- **Échec des appels HTTP sortants** : ce widget affiche le nombre d'appels HTTP sortants ayant échoué qui ont été déclenchés dans les applications SIR.
- **Exécutions du Playbook PAD en état d'erreur** : ce widget affiche le nombre d'erreurs d'exécution du Playbook PAD qui ont été déclenchées dans les applications SIR.

7. Sélectionnez l'onglet **Performances** pour afficher le nombre de problèmes de performances qui ont été déclenchés dans les applications Réponse aux incidents de sécurité.

Onglet Performances



Onglet Performances :

Vous pouvez afficher le tableau de bord regroupé des problèmes de performances dans les applications Security Incident Response.

- **Requêtes de performances lentes** : ce widget affiche le nombre de requêtes de performances dans les applications SIR dont le temps d'exécution moyen est supérieur à 10 ms et en moyenne sur 1 000 exécutions ou plus.
- **Règles métier et scripts lents** : ce widget affiche le nombre de règles métier et de scripts dans les applications SIR dont le temps d'exécution moyen est supérieur à 10 ms et en moyenne sur 1 000 exécutions ou plus.

8. Vous pouvez utiliser l'icône **Actualiser** pour actualiser les données du tableau de bord Intégrité de Réponse aux incidents de sécurité.
9. Vous pouvez utiliser l'icône **Afficher les détails du tableau de bord** pour afficher les détails du tableau de bord Intégrité de Réponse aux incidents de sécurité.
10. Vous pouvez utiliser l'option **Modifier** pour modifier les détails du tableau de bord Intégrité de Réponse aux incidents de sécurité.
11. Vous pouvez utiliser l'option **Plus** pour effectuer des actions supplémentaires sur le tableau de bord Intégrité de Security Incident Response.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Création d'un incident de sécurité

Les incidents de sécurité peuvent être créés manuellement à partir du formulaire ou automatiquement via les événements de sécurité reçus à partir d'outils de surveillance des alertes tiers intégrés, tels que Splunk.

Important : Les dernières fonctionnalités de sont Réponse aux incidents de sécurité exclusivement disponibles dans le Espace de travail de la Réponse aux incidents de sécurité. Veuillez installer ou mettre à niveau vers la dernière Réponse aux incidents de sécurité version pour Espace de travail de la Réponse aux incidents de sécurité accéder aux fonctionnalités telles que le transfert d'équipe, le calculateur de score de risque, entre autres.

Si vous disposez d'un rôle de sécurité, vous pouvez utiliser l'une des méthodes suivantes pour créer manuellement des incidents de sécurité.

Méthodes de création manuelle des incidents de sécurité

Fonction de message REST	Description
Créé manuellement à partir de la liste des incidents de sécurité	Dans la liste des incidents de sécurité, cliquez sur **Nouveau** pour créer un nouvel incident de sécurité.
Créé manuellement à partir du catalogue des incidents de sécurité	Vous pouvez créer des incidents de sécurité en sélectionnant parmi les catégories de menaces à la sécurité définies dans le catalogue des incidents de sécurité.
Gestion des incidents	Dans le formulaire Incident de Gestion des incidents, cliquez sur **Créer un incident de sécurité** pour créer un nouvel incident de sécurité.
Converti manuellement à partir d'une demande de sécurité	Dans le formulaire de demande de sécurité, cliquez sur **Convertir en incident de sécurité** pour créer un nouvel incident de sécurité.
Créé manuellement à partir d'une alerte de gestion des événements	Dans le formulaire Alertes de Gestion des événements, cliquez sur **Créer un incident de sécurité** pour créer un nouvel incident de sécurité à partir d'une alerte.
Créé manuellement à partir d'une alerte	Dans le formulaire Alerte de Gestion des événements, cliquez sur **Créer un incident de sécurité** pour créer un nouvel incident de sécurité.
Converti manuellement à partir d'un enregistrement de vulnérabilité (si le module d'extension Vulnerability Response est activé)	Dans le formulaire Éléments de vulnérabilité, cliquez sur **Créer un incident de sécurité** pour créer un nouvel incident de sécurité.

Création automatique d'incidents de sécurité

En règle générale, les administrateurs de sécurité sont chargés de configurer des règles d'alerte utilisées pour générer automatiquement des incidents de sécurité.

Méthode de l'administrateur de sécurité pour la création des incidents de sécurité

Fonction de message REST	Description
Créé automatiquement à l'aide des règles d'alerte	Les incidents de sécurité peuvent être créés en fonction des règles d'alerte définies dans la gestion des événements de votre application Centre de données .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Création manuelle d'un incident de sécurité

Vous pouvez créer un incident de sécurité à partir du formulaire d'incident de sécurité, ainsi qu'à partir de plusieurs autres formulaires.

Vous pouvez créer des incidents de sécurité basés sur un enregistrement existant à partir des formulaires suivants :

- À partir de n'importe quelle liste d'incidents de sécurité
- Formulaire d'incident
- Gestion des événements Formulaire d'alerte
- Formulaire Éléments vulnérables
- Formulaire de demande de sécurité

Créer un incident de sécurité à partir de la liste des incidents de sécurité

Outre les méthodes automatiques de création d'incidents de sécurité, vous pouvez les créer manuellement, selon vos besoins.

Cette vidéo montre une vue d'ensemble de la façon dont vous pouvez créer un incident de sécurité à partir de la liste des incidents de sécurité.

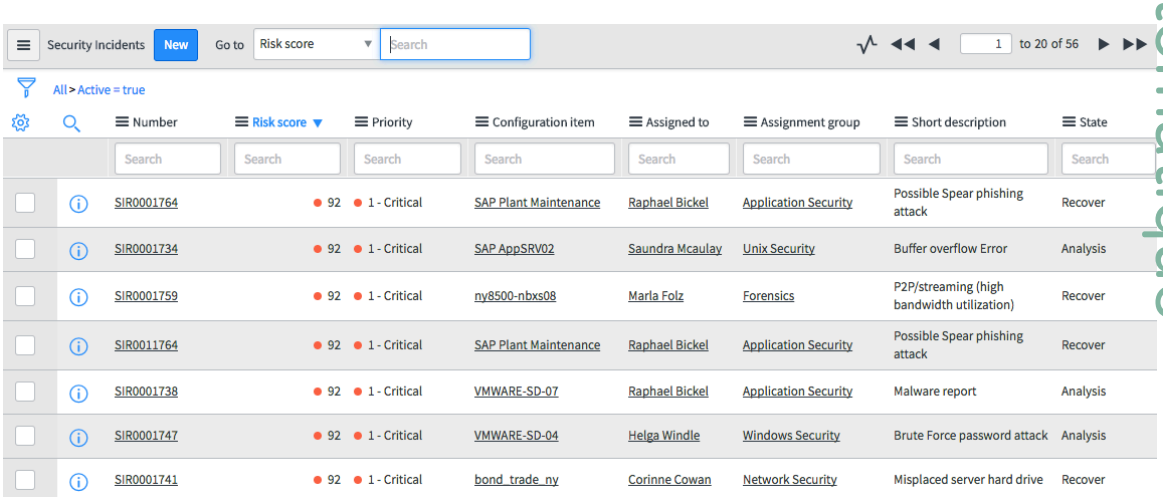
Créer un incident de sécurité à partir de la liste des incidents de sécurité

Avant de commencer

Rôle requis : sn_si.basic

Procédure

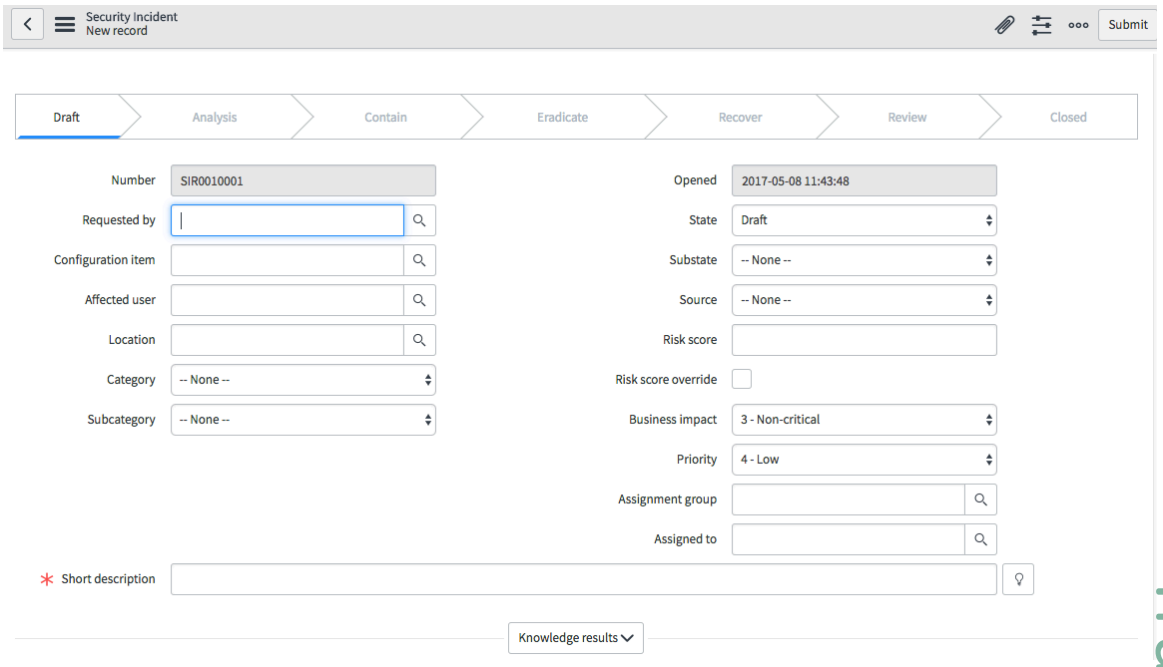
1. Accédez à une liste d'incidents de sécurité (par exemple, **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**).



2. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Remplissez les champs du formulaire.

Champ	Description
Sélectionner une balise de sécurité	Si nécessaire, sélectionnez une balise de sécurité pour ajouter des métadonnées à l'enregistrement ou identifiez qui doit avoir accès à cet enregistrement d'incident de sécurité. Ce champ n'apparaît qu'une fois l'incident de sécurité enregistré.
Numéro	[Lecture seule] Le numéro de l'incident de sécurité.
Demandé par	Personne demandant l'exécution du travail.
Élément de configuration	Serveur, ordinateur, routeur ou autre élément de configuration affecté par le problème de sécurité.
Utilisateur affecté	Personne affectée par le problème de sécurité.
Emplacement	L'emplacement du demandeur ou de la ressource. Si un **élément de configuration** n'est pas sélectionné, ce champ est pré-rempli avec l'emplacement du demandeur.
Catégorie	Catégorie qui identifie le type de problème de sécurité. Si une catégorie est sélectionnée, un workflow d'analyse de ce problème est exécuté lorsque l'enregistrement est enregistré. Par exemple, si vous sélectionnez **Déni de service**, le workflow Incident de sécurité - Déni de service - Modèle est exécuté. Pour plus d'informations, consultez Modèles de workflows Réponse aux incidents de sécurité.
Sous-catégorie	Sous-catégorie qui précise le problème.
Ouvert	[Lecture seule] Affiche la date et l'heure d'ouverture de l'incident.
État	L'état actuel de l'incident de sécurité. Lors de la création d'un incident de sécurité, ce champ est défini par défaut sur **Brouillon**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sous-état	Détermine si l'incident de sécurité inclut un problème ou un changement en attente.
Source	Identifie la source de l'incident de sécurité, par exemple un e-mail, un appel téléphonique ou la surveillance du réseau.
Capteur d'alerte	Intégration de sécurité par laquelle vous ingérez les données d'alerte ou d'événement, par exemple CarbonBlack, CrowdStrike, McAfee, etc.
Règle d4alerte	Règle du produit de sécurité qui a déclenché la création de cet incident de sécurité.
Score du risque	Affiche le score de risque calculé pour cet incident de sécurité. La valeur est basée sur la priorité de l'incident de sécurité, le type d'incident de sécurité (déni de service, harponnage ou activité de code malveillant) et le nombre de sources qui ont déclenché un score d'échec de réputation sur un indicateur. Le score de risque aide à hiérarchiser le travail d'incident de sécurité pour les analystes. Trois propriétés d'incident de sécurité vous permettent de désigner un point à code couleur à afficher à côté du score de risque dans la vue de listes afin de les rendre plus facilement identifiables. Si vous apportez des modifications à certains champs de l'incident de sécurité, tels que **l'impact sur l'activité** ou la **priorité**, et que vous sauvegardez l'enregistrement, le **score de risque** est automatiquement recalculé et affiché. Le changement est également reflété dans les notes de travail et dans la liste connexe des audits des scores de risque. **Remarque :** Le score de risque est également recalculé lorsque les utilisateurs affectés sont associés à un incident de sécurité, à des services affectés ou à des éléments vulnérables. Vous pouvez également saisir manuellement un nouveau **score de risque**. Cela peut être utile si vous souhaitez conserver un incident de sécurité particulier en haut de la liste des incidents de sécurité que vous analysez. Si vous entrez un nouveau **score de risque**, la case **Remplacement du score de risque** est automatiquement cochée. Quels que soient les changements apportés à l'incident de sécurité, un score de risque saisi manuellement n'est pas automatiquement recalculé. **Remarque :** Si vous avez mis à niveau votre instance à partir d'une version antérieure, les scores de risque ont été calculés pour tous vos incidents de sécurité ouverts. Pour plus d'informations, consultez Comprendre les calculateurs d'incidents de sécurité.
Remplacement du score du risque	Cochez cette case pour remplacer la mise à jour automatique du score de risque. Le remplacement sera reflété dans les notes de travail.
Impact sur l'activité	Sélectionnez l'importance de cet incident de sécurité pour votre entreprise. La valeur par défaut est Non critique. Si, après avoir sauvegardé l'enregistrement de l'incident de sécurité, vous modifiez la valeur dans les champs **Priorité** fand/ou **Risque** , **l'impact sur l'activité** est recalculé.
Priorité	Sélectionnez l'ordre dans lequel traiter cet incident de sécurité, en fonction de l'urgence. Si cette valeur est modifiée après la sauvegarde de l'enregistrement, cela peut affecter le calcul de **l'impact sur l'entreprise** .
Groupe d'affectation	Groupe auquel cet incident de sécurité est affecté.

Traduction automatique

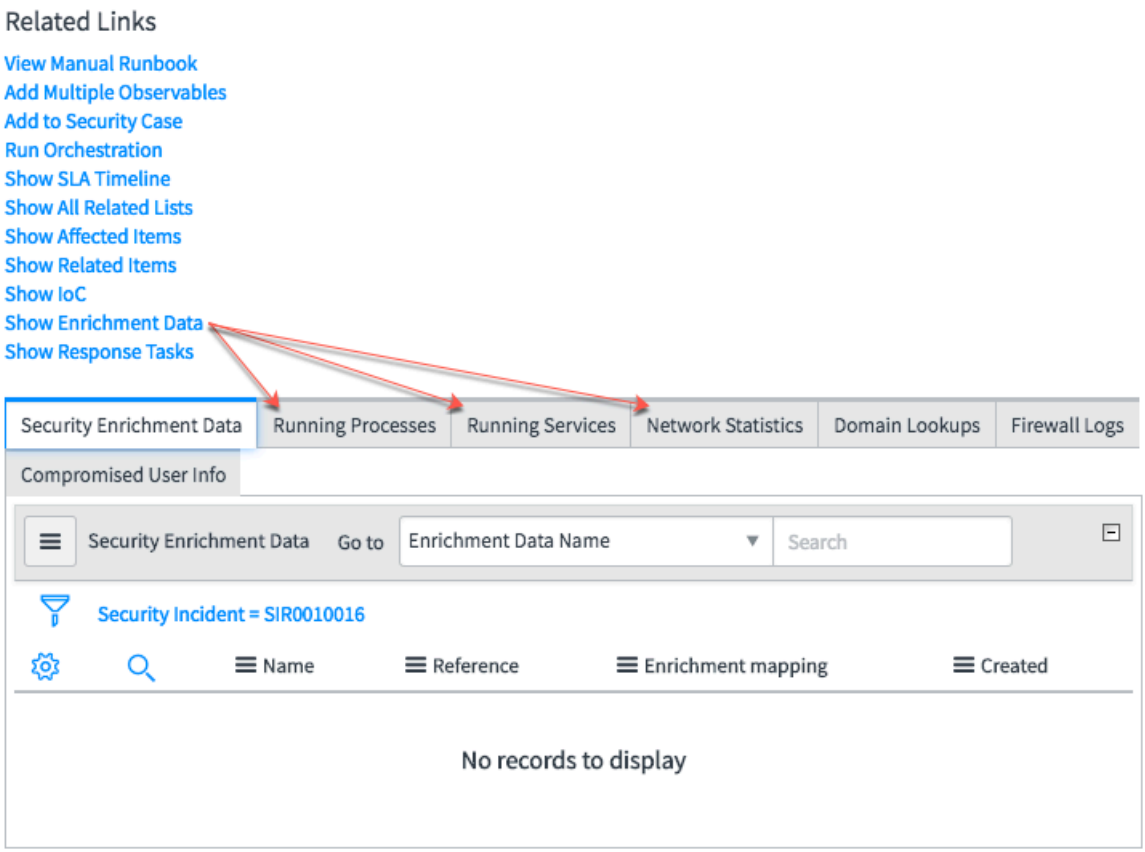
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Affecté à	Personne affectée à l'analyse de cet incident de sécurité. Les affectations peuvent être effectuées manuellement ou automatiquement. Pour plus d'informations, consultez Affectation d'analystes de la sécurité.
Description brève	Brève description de l'incident de sécurité.
Résultats de recherche dans la base de connaissances	Au fur et à mesure que vous saisissez la brève description, des liens vers des articles connexes de la base de connaissances s'affichent. L'analyse des informations pourrait résoudre votre problème.

4. Cliquez avec le bouton droit dans l'en-tête de l'enregistrement, puis sélectionnez **Enregistrer**.
   Si vous avez ajouté un nouveau CI à l'incident de sécurité, les workflows d'intégration suivants sont automatiquement exécutés :
   - Opérations de sécurité : obtenir le flux d'exécution des processus. Ce workflow récupère une liste des processus en cours d'exécution sur un élément de configuration (CI) à partir d'un hôte ou d'un point de terminaison.
   - Workflow Security Incident Response - Get Running Services. Ce workflow récupère une liste des services en cours d'exécution à partir des CI Windows.
   - Intégrations Security Operations : obtenir le flux des statistiques réseau. Ce workflow récupère une liste des connexions réseau actives à partir d'un hôte ou d'un point de terminaison.
5. Pour afficher les informations récupérées par ces workflows, cliquez sur le lien connexe **Afficher les données d'enrichissement** , puis sur l'un des onglets indiqués.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Des workflows supplémentaires sont exécutés en fonction des intégrations tierces que vous avez activées, comme suit Intégration de Security Operations Carbon Black : obtenir le flux d'exécution des processus

Information associée

Configurer Réponse aux incidents de sécurité

Créer un incident de sécurité à partir du catalogue des incidents de sécurité

Les utilisateurs de votre entreprise peuvent utiliser le catalogue des incidents de sécurité pour demander divers types d'analyses liées à la sécurité.

Avant de commencer

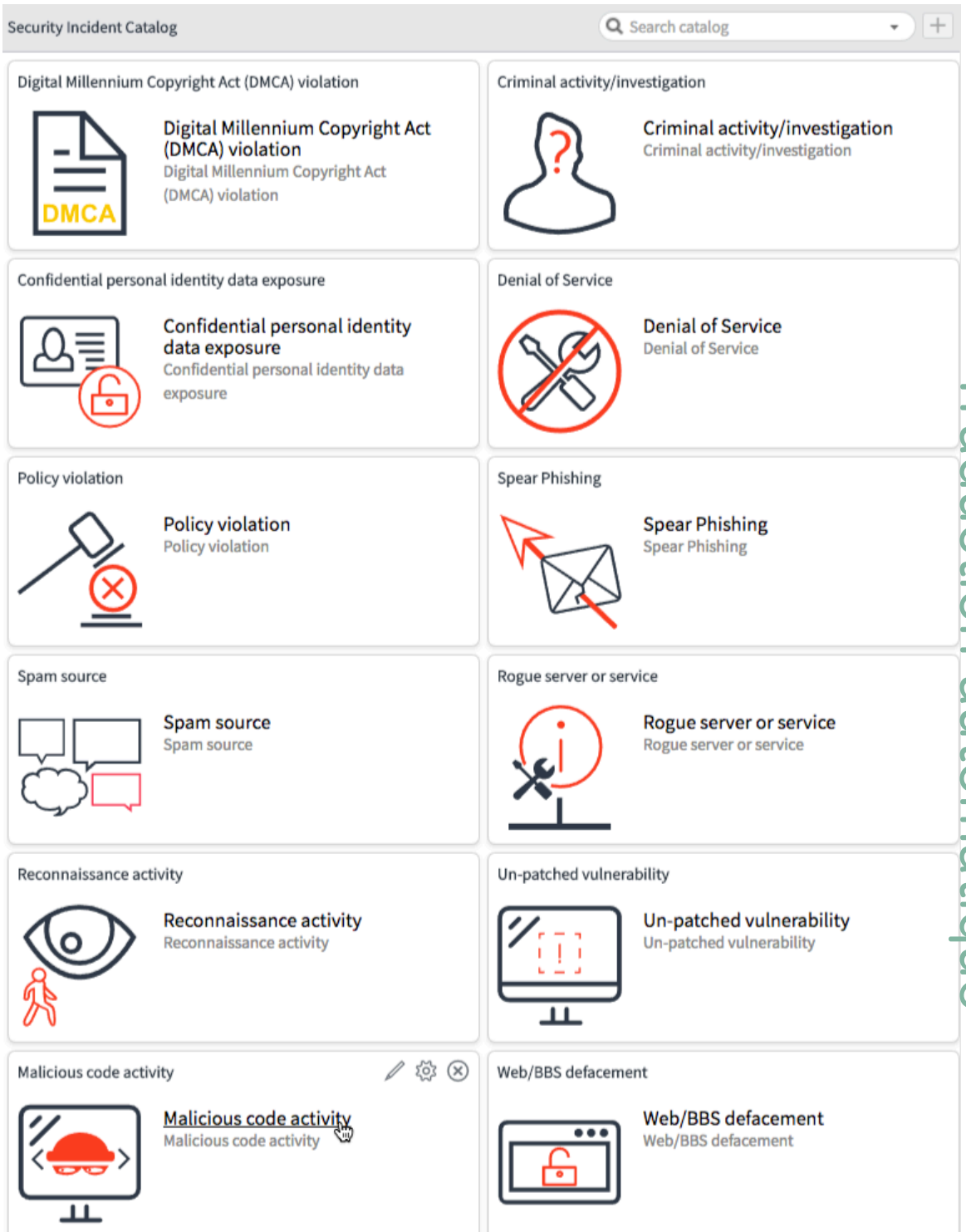
Rôle requis : aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

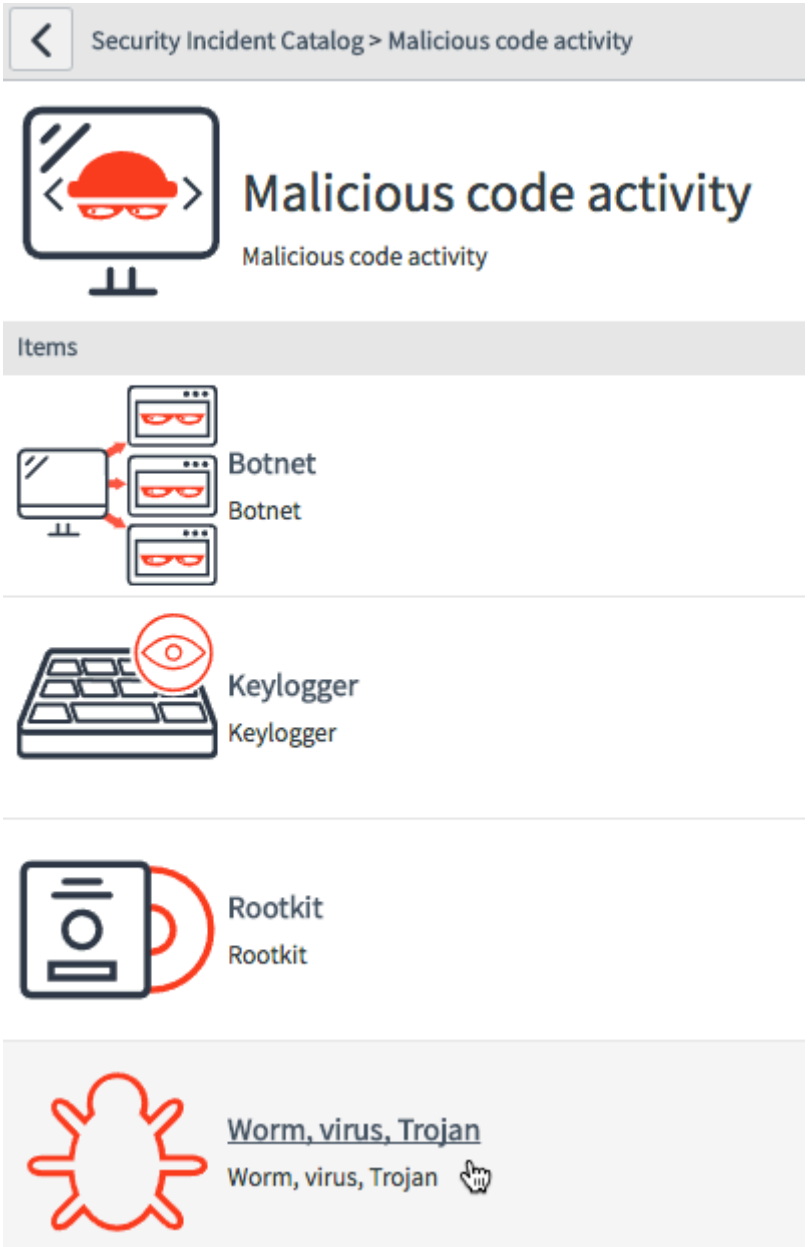
1. Accédez à la **Tous** > **Libre-service** > **Catalogue des incidents de sécurité**.



2. Cliquez sur l'élément de catalogue pour lequel vous souhaitez effectuer une demande.
   Si l'élément que vous avez sélectionné dans le catalogue principal contient des sous-catégories, la liste s'affiche. Dans l'exemple suivant, **L'activité du code malveillant** a été sélectionnée.

Traduction automatique

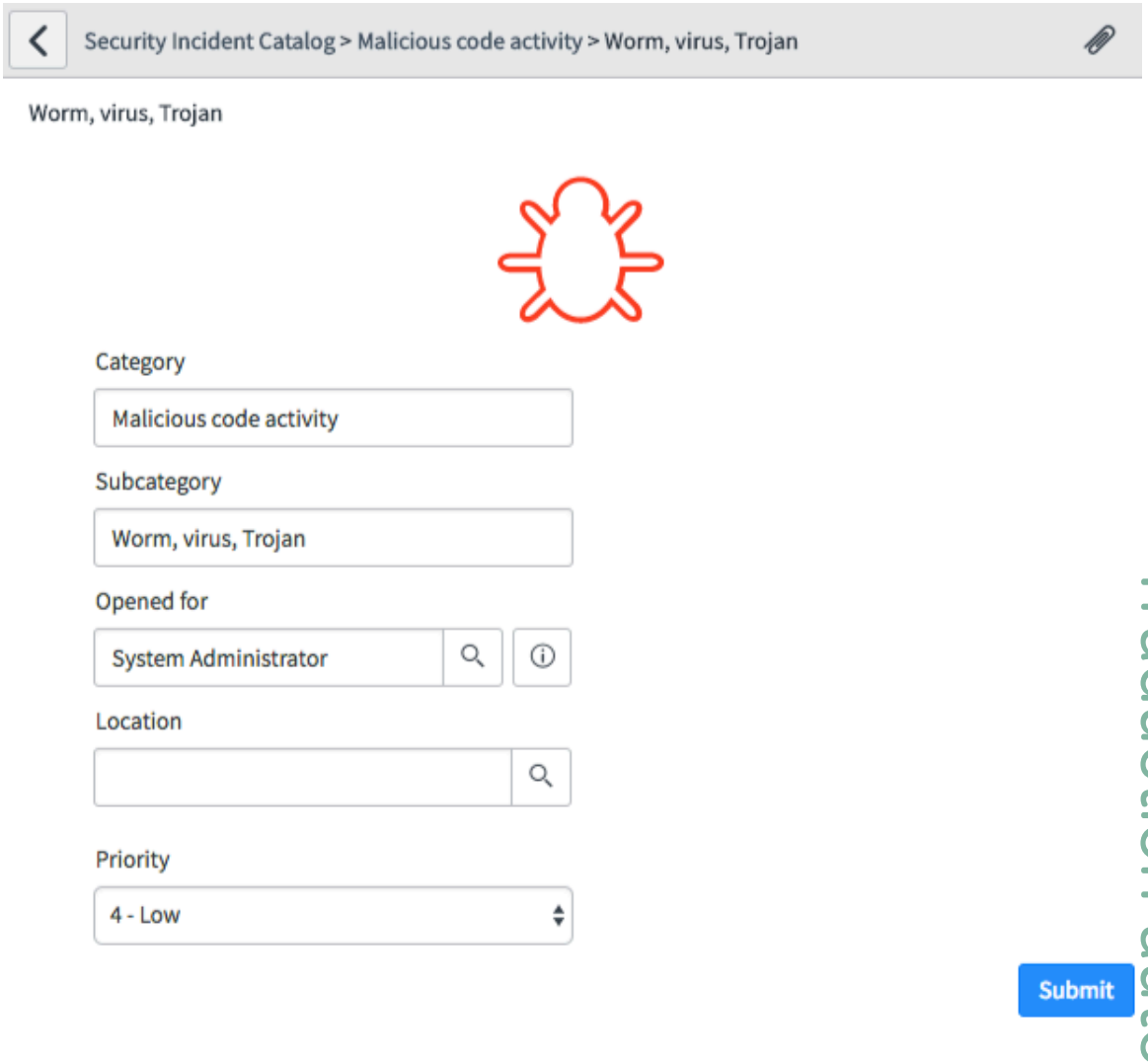
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur la sous-catégorie qui correspond le mieux au type de demande que vous souhaitez effectuer. Dans cet exemple, la sous-catégorie **Ver, virus, cheval de Troie** a été sélectionnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Saisissez les informations relatives à la demande, puis cliquez sur **Soumettre**.
   La demande est envoyée à votre service des incidents de sécurité.
5. Une fois que vous avez envoyé la demande, vous pouvez suivre sa progression en accédant à **Libre-service** > **Mes demandes**et en saisissant le numéro de demande.

Créer un incident de sécurité à partir d'une alerte de gestion des événements

Lorsque Gestion des événements est activé, vous pouvez créer manuellement des incidents de sécurité à partir du formulaire Alerte.

Avant de commencer

Le module d'extension Gestion des événements nécessite un abonnement distinct et doit être activé par le personnel ServiceNow. Ce module d'extension inclut des données de démonstration et active les modules d'extension connexes s'ils ne sont pas déjà activés. L'analytique de services est activée automatiquement lorsque Gestion des événements est activée.
Rôle requis : evt_mgmt_admin, evt_mgmt_operator ou evt_mgmt_user

Procédure

1. Accédez à la **Tous** > **Gestion des événements** > **Toutes les alertes**.
2. Cliquez sur le **numéro** d'alerte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Créer un incident de sécurité**.
4. Cliquez sur **Mettre à jour**.

Création automatique d'un incident de sécurité

Des outils de surveillance tiers, tels que Splunk, peuvent être intégrés Réponse aux incidents de sécurité afin que les événements de sécurité importés à partir de ces outils génèrent automatiquement des incidents de sécurité. Vous pouvez également importer des données à partir d'outils tiers dans des alertes de sécurité.

Pour intégrer des outils de surveillance des alertes dans Réponse aux incidents de sécurité, vous devez utiliser l'API REST pour écrire dans la table d'importation des incidents de sécurité [sn_si_incident_import]. Ensuite, à l'aide des cartes **de transformation d'incident de sécurité**, la table source du jeu d'importation est mappée aux champs de la table Incident de sécurité [sn_si.incident] cible.

Si vous tentez d'importer des enregistrements de CI qui ne sont pas reconnus par la carte de transformation, le script de carte de transformation vérifie dans l'enregistrement les éléments suivants (dans cet ordre) pour tenter d'établir une correspondance :

- sys_id
- Nom CI :
- nom de domaine pleinement qualifié
- Adresse IP

Remarque : Si vous trouvez que la carte de **transformation d'incident de sécurité** n'est pas adéquate pour l'outil de surveillance d'alerte tiers que vous utilisez, dupliquez la carte de transformation, créez-en une nouvelle et modifiez les champs, selon vos besoins.

Incidents de sécurité créés à partir d'événements et d'alertes

Les événements importés à partir d'outils de surveillance des alertes sont d'abord traités Event Management et regroupés en alertes. Ces alertes peuvent être utilisées pour créer des incidents de sécurité basés sur des règles d'alerte personnalisables, ou examinées manuellement pour sélectionner les alertes à examiner en tant qu'incident de sécurité.

Vous pouvez trouver un exemple de règle d'alerte appelée **Créer des incidents de sécurité à partir d'alertes critiques** dans le Règles d'alerte module de l'application Event Management . Cette règle d'alerte crée automatiquement des incidents de sécurité lorsque des événements critiques liés à la sécurité sont reçus à l'intérieur ServiceNow ou à partir d'applications de surveillance tierces. Une fois l'incident de sécurité créé, il est mis à jour au fur et à mesure que de nouveaux événements sont reçus. Vous pouvez modifier le modèle de tâche dans la règle d'alerte pour modifier les valeurs initiales de l'incident de sécurité créé par cette règle d'alerte. Pour gérer chaque type distinct d'incident de sécurité que vous souhaitez créer, vous pouvez définir d'autres règles d'alerte avec des conditions différentes.

Si vous êtes un utilisateur disposant du rôle d'administrateur de sécurité, vous pouvez également créer manuellement un incident de sécurité en cliquant sur le bouton **Créer un incident de sécurité** à partir d'une alerte suspecte.

Il est important que les événements reçus d'outils externes incluent les informations suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le nœud est défini sur le nom, l'adresse IP ou le sys_id du CI qui devient la ressource affectée.
- La classification des événements est définie sur Sécurité pour les distinguer des autres événements informatiques.
- Description de l'événement, qui remplit la description de l'incident de sécurité.
- Les informations supplémentaires peuvent inclure toute information supplémentaire qui ne rentre pas dans les champs précédemment répertoriés ou dans d'autres champs d'événement, tels que la catégorie, les vecteurs d'attaque, l'URL de retour ou l'ID de corrélation. Le format est une chaîne qui répertorie les noms de champs ainsi que leurs valeurs, à l'aide du format JSON suivant :

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Remarque : Pour chaque paire champ-valeur, si le champ de l'incident de sécurité dans lequel le nom de colonne correspond au fieldName est vide, il est défini sur fieldValue. Si le champ de l'incident de sécurité n'est pas vide, il n'est pas modifié. Dans les deux cas, l'événement ainsi que tous les champs et valeurs codés dans les informations supplémentaires sont enregistrés dans une entrée de notes de travail décrivant l'événement. Si rien ne change dans l'incident de sécurité, aucune entrée de note de travail n'est créée. Tous les champs d'un incident de sécurité, y compris les champs personnalisés que vous ajoutez à la table, peuvent être définis.

Données importées dans les alertes de sécurité

Lorsqu'un événement est créé avec davantage de données codées JSON, ces données sont importées dans n'importe quel champ dont le nom correspond au fieldName de cette valeur dans les données JSON.

Si vous avez des données dans votre logiciel de surveillance tiers (par exemple, Splunk) qui ne sont pas communes au système de base, vous pouvez ajouter de nouveaux champs à la table Alerte pour prendre en charge l'importation de données. Le format JSON pour l'importation de données dans les alertes est le même que celui utilisé pour la création d'incidents de sécurité à partir d'événements et d'alertes :

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

La seule différence est que les données du champ sont toujours remplacées par fieldValue.

Lorsque les données d'événement de sécurité sont importées, les champs de la table Alerte sont renseignés avec les noms de champs correspondants. Si l'alerte est ultérieurement transformée en incident de sécurité, les mêmes données d'information supplémentaires renseignent les champs correspondants de l'incident de sécurité.

Créer des incidents de sécurité à partir d'e-mails d'hameçonnage signalés par un utilisateur

Utilisez cette fonctionnalité pour créer des incidents de sécurité à partir des e-mails d'hameçonnage signalés par un utilisateur.

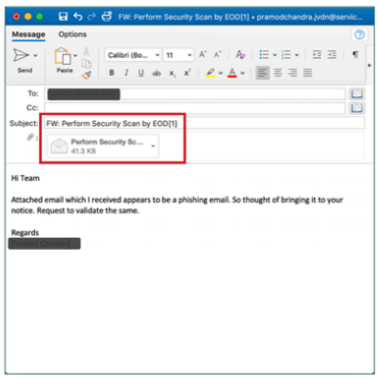
La fonctionnalité améliorée User Reported Phishing comprend des options d'agrégation, d'extraction d'en-tête d'e-mail et de configuration.

- Les utilisateurs peuvent signaler les e-mails d'hameçonnage de plusieurs manières :
  - Les e-mails peuvent être transférés en tant que pièces jointes.
  - Si le module d'extension **PhishAlarm** (anciennement connu sous le nom de Wombat) a été configuré avec le client Microsoft Outlook, les utilisateurs peuvent :

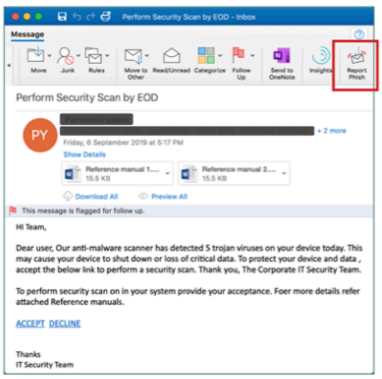
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cliquez sur le bouton **Signaler un hameçonnage** .
- Transférer des e-mails d'hameçonnage à partir d'un appareil mobile à l'aide de l'option **Signaler un hameçonnage** .



Desktop

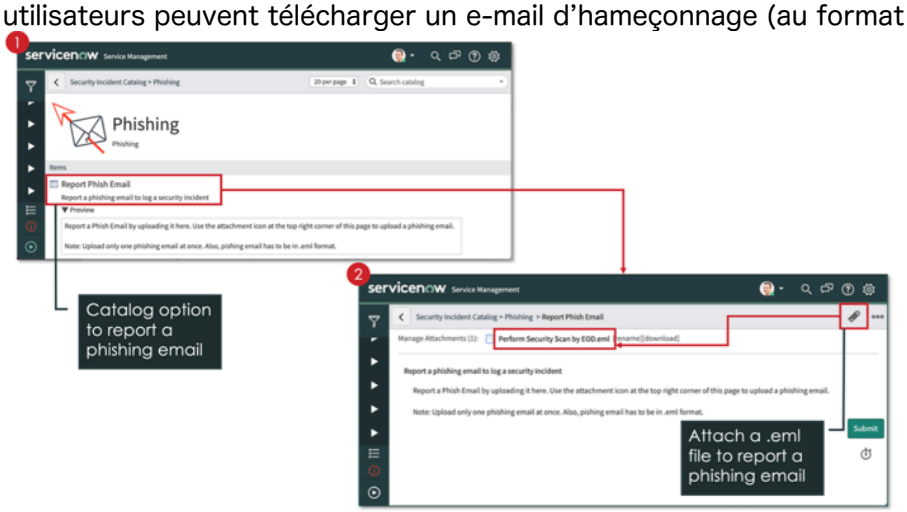


Desktop



Mobile

- Les utilisateurs peuvent télécharger un e-mail d'hameçonnage (au format .eml).



- L'hameçonnage signalé par un utilisateur comprend **une logique métier d'agrégation** qui identifie les e-mails d'hameçonnage en double signalés par les utilisateurs d'une organisation. Les utilisateurs peuvent utiliser cette fonctionnalité pour :
  - Regroupez les incidents d'hameçonnage en double ou similaires signalés par un utilisateur (campagnes d'hameçonnage initiées par l'entreprise).
  - Évitez de trier les incidents d'hameçonnage en double signalés par les utilisateurs et réduisez l'effort manuel nécessaire à la consolidation des incidents.
  - Permettez aux analystes de sécurité de travailler sur un seul incident d'hameçonnage signalé par un utilisateur.
- Fournit des en-têtes d'e-mail d'hameçonnage dans l'incident d'hameçonnage signalé par l'utilisateur.
  - Les analystes de sécurité peuvent rechercher des informations clés sur l'en-tête des e-mails au sein de l'incident.
  - Il n'est plus nécessaire de faire un effort manuel pour recueillir des informations d'en-tête à partir d'autres sources.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'e-mail d'hameçonnage d'origine envoyé est stocké en tant **qu'enregistrement d'e-mail d'hameçonnage** dans une nouvelle table.
- Les analystes de sécurité peuvent consulter les détails de l'e-mail d'hameçonnage d'origine, tels que le contenu, les en-têtes et l'origine de l'e-mail d'hameçonnage.
- Les administrateurs de sécurité peuvent configurer et apporter certaines améliorations, notamment :
  - Configurations permettant d'extraire les en-têtes des e-mails du corps de l'e-mail (signaler les soumissions **d'hameçonnage**).
  - Filtres pour capturer les en-têtes sélectionnés.
  - Configurations pour gérer l'association parent-enfant d'incident lorsque des enregistrements d'e-mail d'hameçonnage en double sont identifiés.
  - Configurations de Concepteur de flux pour modifier la logique métier d'agrégation en fonction des besoins.

Configurer des règles d'intégration pour le hameçonnage signalé par l'utilisateur

En tant qu'utilisateur disposant du rôle `sn_si.admin` , vous pouvez définir des règles de correspondance d'e-mails pour filtrer les e-mails d'hameçonnage signalés par un utilisateur en fonction de critères spécifiques. Par exemple, vous pouvez définir une règle selon laquelle tous les e-mails envoyés directement ou via le bouton Signaler un hameçonnage à *`security@acme.com`* sont classés comme des e-mails d'hameçonnage signalés par un utilisateur. Pour plus d'informations, consultez Configurer des règles d'intégration pour l'hameçonnage signalé par un utilisateur.

Définir les propriétés de hameçonnage signalé par un utilisateur

Définissez les informations d'en-tête à capturer à partir des e-mails d'hameçonnage signalés par l'utilisateur. Pour plus d'informations, voir Définir les propriétés de hameçonnage signalé par un utilisateur

Enregistrements d'e-mails d'hameçonnage créés à partir d'e-mails d'hameçonnage signalés par un utilisateur

Les e-mails d'hameçonnage signalés par un utilisateur sont convertis en incidents de sécurité en fonction des règles de correspondance d'e-mail qui ont été définies. Pour plus d'informations, consultez Enregistrements d'e-mails d'hameçonnage créés à partir d'e-mails d'hameçonnage signalés par un utilisateur.

Transformer l'e-mail d'hameçonnage en incident de sécurité

Le flux Transformer l'e-mail d'hameçonnage en incident de sécurité convertit ou transforme les enregistrements d'e-mails d'hameçonnage en incidents de sécurité. Pour plus d'informations, consultez Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité.

Enregistrements d'incidents de sécurité créés à partir d'enregistrements d'e-mails d'hameçonnage

Affichez les détails de l'enregistrement de l'incident de sécurité, y compris les listes connexes, les notes de travail et d'autres informations importantes. Pour plus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'informations, consultez Enregistrements d’incidents de sécurité créés à partir d’enregistrements d’e-mails d’hameçonnage.

Composants et modules d’extension requis

La fonctionnalité User Reported Phishing disponible dans cette version est une version améliorée de la fonctionnalité User Reported Phishing existante disponible dans la version London. Pour plus d’informations, consultez la rubrique **Créer des règles pour valider les attaques de phishing signalées** par un utilisateur dans la documentation London.

Instructions d’installation importantes

Cette amélioration remplace la conception existante de hameçonnage signalé par un utilisateur. Le nouveau design comprend les mises à jour suivantes :

- Les actions entrantes des e-mails de **hameçonnage signalés** par un utilisateur existantes (Type = Transfert et Type = Nouveau) ont été désactivées.
- Une nouvelle action Créer **un e-mail d’hameçonnage** entrant est désormais disponible.
- Il s’agit Transformer les e-mails d’hameçonnage signalés par un utilisateur en incidents de sécurité d’un nouveau flux qui contient la logique métier de création et d’agrégation des incidents de sécurité pour la nouvelle conception. Vous devez activer ce flux pour que la nouvelle conception prenne effet.
- Les règles existantes de hameçonnage signalé par un utilisateur ont été conservées pendant la mise à niveau.

> **Remarque :** Si vous utilisez des actions entrantes d’e-mail personnalisées et des workflows personnalisés pour les soumissions d’hameçonnage signalées par les utilisateurs, vous devez examiner les anciennes et les nouvelles conceptions pour détecter les fonctionnalités en conflit ou qui se chevauchent.

Hameçonnage signalé par un utilisateur Détails de l’amélioration : Voici les détails de l’amélioration :

- Signalez l’e-mail d’hameçonnage de plusieurs façons : consultez la section Créer des incidents de sécurité à partir d’e-mails d’hameçonnage signalés par un utilisateur pour en savoir plus. L’e-mail d’hameçonnage est ensuite déplacé vers la table `sn_si_phishing_email` .
- Création d’enregistrements d’e-mails d’hameçonnage : si les règles de correspondance d’e-mail sont respectées (voir Configurer des règles d’intégration pour l’hameçonnage signalé par un utilisateur), l’action **Créer un e-mail entrant d’hameçonnage** crée un enregistrement d’e-mail d’hameçonnage. Les en-têtes d’e-mail analysés sont stockés dans la table cm`sn_si_phishing_email_header` et associés à l’e-mail d’hameçonnage en tant que liste connexe.
- Agrégation d’enregistrements d’hameçonnage similaires en un seul incident de sécurité : le Transformer les e-mails d’hameçonnage signalés par un utilisateur en incidents de sécurité flux crée des incidents de sécurité à partir des enregistrements d’e-mails d’hameçonnage et agrège des enregistrements similaires en un seul incident. Les conditions d’agrégation peuvent être modifiées selon les besoins de ce flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Les actions entrantes de **Hameçonnage signalé** par un utilisateur disponibles avant la version 9.0 de Réponse aux incidents de sécurité sont désormais désactivées. Les incidents de sécurité ne sont plus créés via les actions entrantes désactivées.
- L'application Spoke Security Operations doit être installée pour que la nouvelle conception prenne effet. Cela inclut le Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité flux qui est disponible à l'état inactif par défaut. Activez ce flux pour créer des incidents de sécurité à partir des enregistrements d'e-mails d'hameçonnage.

L'image suivante montre les différences entre l'ancien et le nouveau design :



Pour utiliser la fonctionnalité améliorée User Reported Phishing, les modules d'extension et composants suivants sont requis :

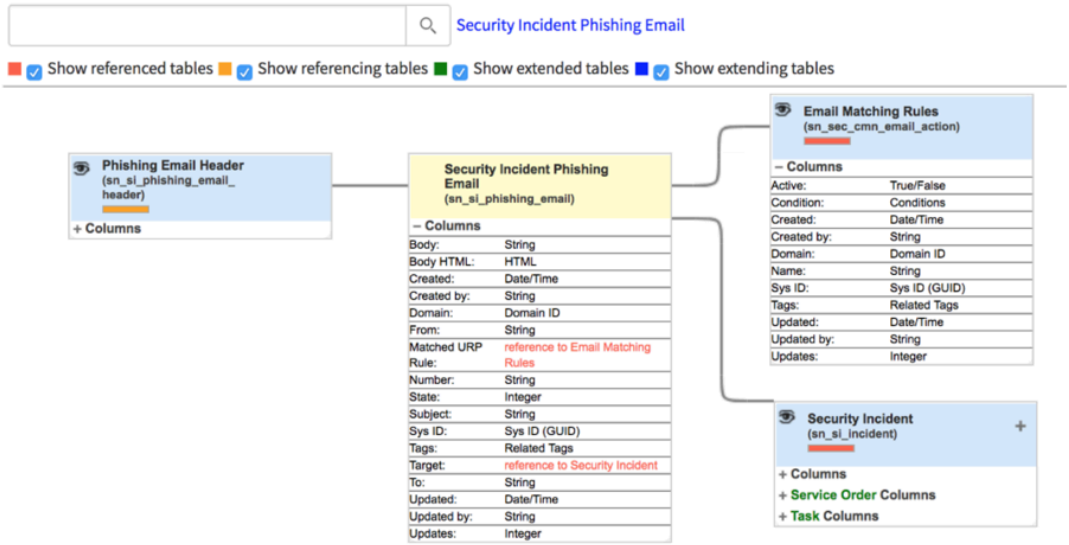
- Support de sécurité commun (`sn_sec_cmn`) : comprend :
  - Action entrante
  - Nouveau script EmailUserReportedPhishing
  - Table Règles d'ingestion
- Réponse aux incidents de sécurité (sn_si) : comprend :
  - Table des incidents de sécurité (sn_si_incident)
  - Table des e-mails d'hameçonnage de sécurité (sn_si_phishing_email)
  - Table des en-têtes d'e-mails d'hameçonnage de sécurité (sn_si_phishing_email_header)
  - Créateur d'enregistrement de chargement EML
- Spoke Security Operations

  Flux et flux secondaires pour l'agrégation des e-mails et la transformation des e-mails d'hameçonnage en incidents de sécurité.

La figure suivante montre la nouvelle table d'e-mails d'hameçonnage avec des références à la règle URP correspondante et à l'enregistrement d'incident de sécurité cible (sn_si_incident).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Configurer des règles d'intégration pour l'hameçonnage signalé par un utilisateur

En tant qu'utilisateur disposant du rôle `sn_si.admin` , vous pouvez définir des règles de correspondance d'e-mails pour filtrer les e-mails d'hameçonnage signalés par un utilisateur en fonction de critères spécifiques. Par exemple, vous pouvez définir une règle selon laquelle tous les e-mails envoyés directement ou via le bouton Signaler un hameçonnage à *`security@acme.com`* sont classés comme des e-mails d'hameçonnage signalés par un utilisateur.

Avant de commencer

Rôle requis : sn_si.admin

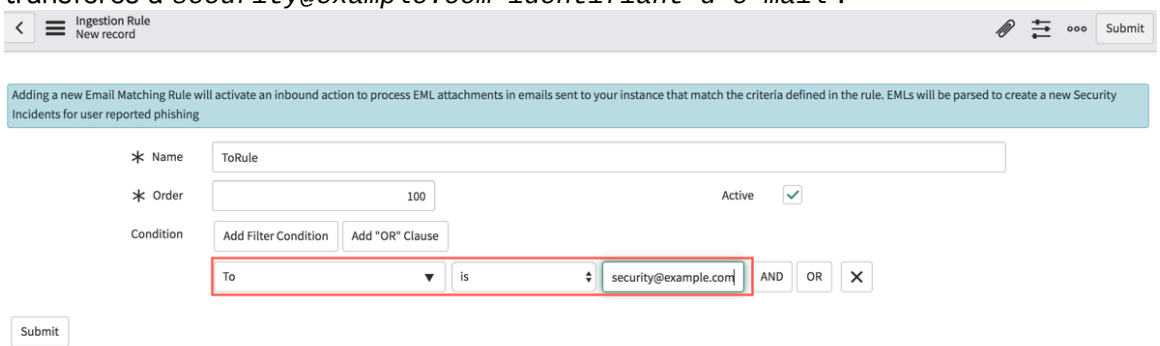
Procédure

1. Accédez à la **Tous** > **Security Operations** > **Traitement des e-mails** > **Règles d'intégration : hameçonnage signalé par un utilisateur**.
2. Cliquez sur **Nouveau** pour créer une règle de correspondance d'e-mail.
3. Entrez un nom et définissez une ou plusieurs conditions pour la règle.
4. Cliquez sur **Soumettre** pour enregistrer la règle.
   Voici quelques exemples de règles :

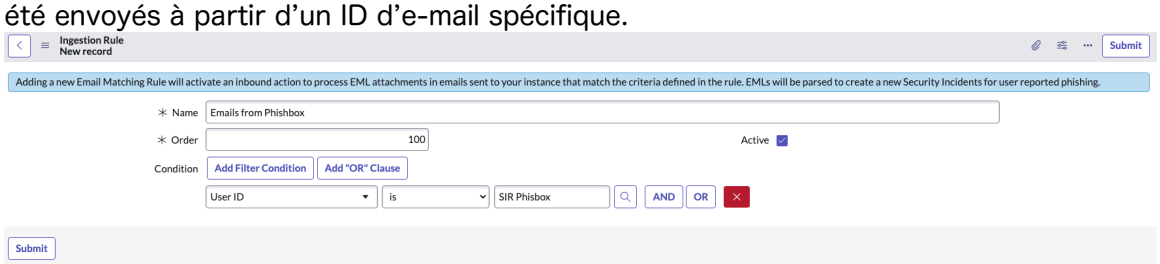
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **ToRule** : filtrez les e-mails qui ont été envoyés directement ou transférés à *security@example.com identifiant d'e-mail*.



- **Règle d'ID d'utilisateur** : filtrez les e-mails qui ont été envoyés à partir d'un ID d'e-mail spécifique.



Définir les propriétés de hameçonnage signalé par un utilisateur

Définissez les informations d'en-tête qui doivent être capturées à partir des e-mails d'hameçonnage signalés par un utilisateur.

Avant de commencer

Rôle requis : sn_si.admin

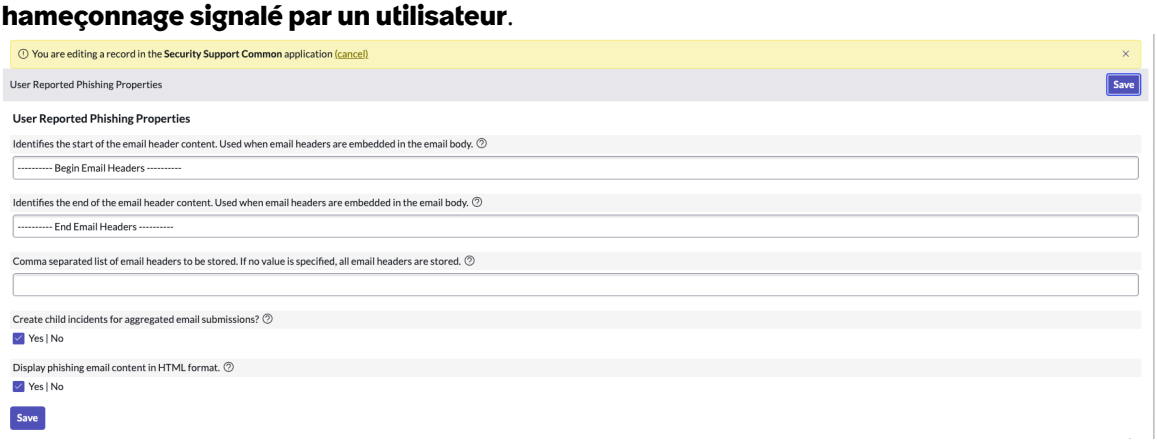
Pourquoi et quand exécuter cette tâche

Utilisez ces options pour configurer les paramètres de hameçonnage signalé par l'utilisateur suivants.

- Configuration permettant d'extraire les en-têtes des e-mails du corps de l'e-mail. (Signaler les soumissions **d'hameçonnage** .)
- Filtrez pour sélectionner des en-têtes.
- Activer ou désactiver l'association parent-enfant.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Traitement des e-mails** > **Propriétés de hameçonnage signalé par un utilisateur**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Spécifiez la configuration d'extraction des en-têtes d'e-mail du corps de l'e-mail :
   - Saisissez une chaîne qui identifie le début de l'en-tête de l'e-mail.
   - Saisissez une chaîne qui identifie la fin de l'en-tête de l'e-mail.

   Remarque : Appliquez ces paramètres uniquement aux en-têtes capturés dans le corps de l'e-mail d'hameçonnage. Par exemple, si le module d'extension **PhishAlarm** (anciennement connu sous le nom de Wombat) a été configuré avec le client Microsoft Outlook, lorsque l'utilisateur clique sur le bouton **Signaler un hameçonnage** , les en-têtes des e-mails sont capturés selon la configuration définie ici. Les informations d'en-tête ne sont pas capturées si l'e-mail d'hameçonnage est transféré en tant que pièce jointe.

3. Spécifiez des filtres pour éliminer les en-têtes qui ne sont pas nécessaires pour enquêter sur l'incident de sécurité.

   Saisissez une liste d'en-têtes séparés par des virgules qui doivent être capturés à partir de l'e-mail d'hameçonnage signalé par l'utilisateur. Si vous ne spécifiez aucune valeur ici, toutes les informations d'en-tête sont capturées.

4. Activer ou désactiver l'association parent-enfant.
   Par défaut, l'option **Oui** est activée. Sélectionnez **Oui** pour indiquer que les incidents de sécurité enfants doivent être créés lorsque les e-mails d'hameçonnage signalés par un utilisateur sont regroupés. Si vous sélectionnez **Non**, les incidents de sécurité enfants ne sont pas créés, mais les e-mails d'hameçonnage signalés par l'utilisateur sont associés à l'incident de sécurité et l'enregistrement de l'incident de sécurité est mis à jour. Pour en savoir plus sur la façon dont les incidents de sécurité enfants sont créés, reportez-vous à la rubrique Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité .
5. Activez ou désactivez l'option permettant d'afficher le contenu de l'e-mail d'hameçonnage au format HTML.
   Par défaut, l'option **Oui** est activée. Sélectionnez **Oui** pour afficher le contenu de l'e-mail d'hameçonnage au format HTML. Si vous sélectionnez **Non**, le contenu de l'e-mail au format HTML ne sera pas visible dans un enregistrement d'hameçonnage.

Enregistrements d'e-mails d'hameçonnage créés à partir d'e-mails d'hameçonnage signalés par un utilisateur

Les e-mails d'hameçonnage signalés par un utilisateur sont convertis en incidents de sécurité en fonction des règles de correspondance d'e-mails qui ont été définies.

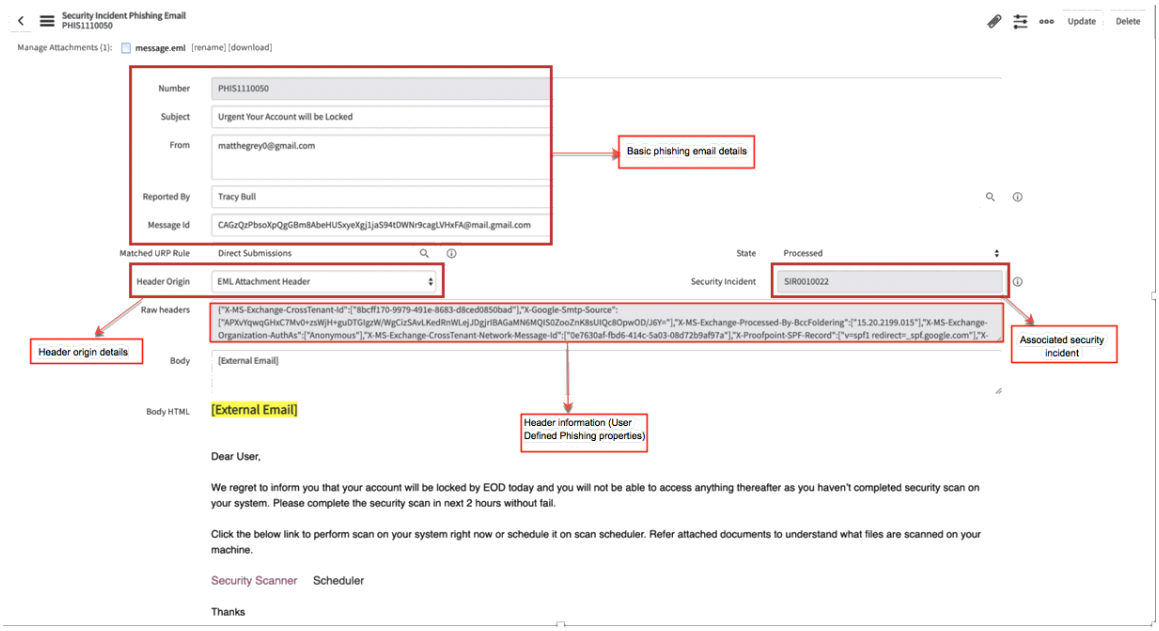
Lorsqu'un nouvel e-mail d'hameçonnage est signalé, les actions suivantes ont lieu :

- Un enregistrement d'e-mail est créé dans la table `sys_email` .
- L'action **Créer un e-mail entrant d'hameçonnage** s'exécute sur l'enregistrement de l'e-mail et utilise les règles de correspondance d'e-mail (voir Configurer des règles d'intégration pour l'hameçonnage signalé par un utilisateur) pour déterminer s'il s'agit d'un e-mail d'hameçonnage.
- Lorsqu'il a été identifié comme un e-mail d'hameçonnage, un enregistrement d'e-mail d'hameçonnage est créé dans la table `sn_si_phishing_email` .
- Enfin, le Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité flux est appliqué pour convertir l'enregistrement de l'e-mail d'hameçonnage en incident de sécurité.

Pour afficher les détails de l'e-mail, accédez à **Incident de sécurité** > **Afficher tous les e-mails d'hameçonnage**. Une liste des enregistrements d'e-mails d'hameçonnage s'affiche. Cliquez sur le lien de date dans la colonne Créé pour afficher l'enregistrement d'e-mail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



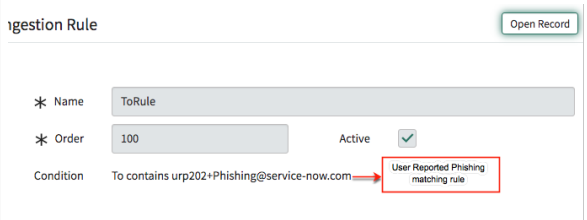
Détails de l’e-mail d’hameçonnage de l’incident de sécurité

Nom de champ	Description
Numéro	Numéro attribué à l’e-mail d’hameçonnage signalé par l’utilisateur.
Objet	Objet de l'e-mail. La règle d’objet est utile dans les simulations de campagnes ou de tests d’hameçonnage. Dans ce cas, les organisations envoient des e-mails trompeurs à leur propre personnel pour tester leur réponse au phishing et aux attaques par e-mail similaires. Dans les tests d’e-mails d’hameçonnage simulés, si le client de messagerie Microsoft Outlook avec le module d’extension **PhishAlarm** (précédemment connu sous le nom de Wombat) est utilisé, l’utilisateur peut cliquer sur le bouton **Signaler un hameçonnage** pour signaler l’e-mail d’hameçonnage. L’e-mail est envoyé à l’équipe Security Operations avec la **fonctionnalité Simulated Phishing** ajoutée à l’objet de l’e-mail. Cela est utilisé pour identifier l’e-mail comme un e-mail d’hameçonnage simulé.
De	Adresse e-mail à partir de laquelle provient cet e-mail d’hameçonnage. Ces informations sont disponibles si l’e-mail d’hameçonnage est transféré comme . Pièce jointe du fichier EML ou si les en-têtes d’origine sont intégrés dans l’e-mail. Si l’utilisateur a transféré l’e-mail d’hameçonnage directement, l’adresse de l’appelant peut ne pas être disponible.
Reporté par	L’ID d’e-mail de l’utilisateur qui a signalé cet e-mail d’hameçonnage. Cliquez sur l’icône **Informations** pour afficher des détails supplémentaires.
ID de message	ID affecté au message.
Règle URP correspondante	La règle User Reported Phishing qui doit être appliquée à cet e-mail. Cliquez sur l’icône Informations pour afficher des détails supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

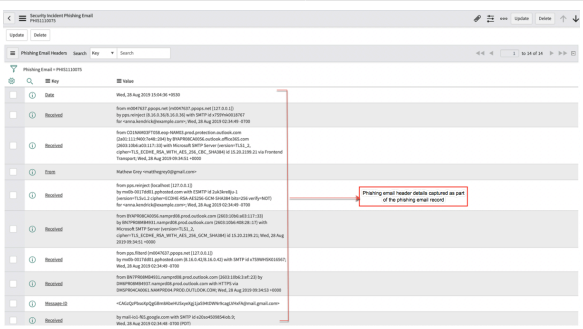
Détails de l'e-mail d'hameçonnage de l'incident de sécurité (suite)

Nom de champ	Description
	Comme vous pouvez le voir, dans cet exemple, le champ **Condition** montre que la ToRule est appliquée sur cet e-mail et qu'un incident de sécurité est créé. Voir Configurer des règles d'intégration pour l'hameçonnage signalé par un utilisateur pour plus d'informations sur la définition de règles de correspondance d'e-mail.
État	Lorsqu'un nouvel enregistrement d'e-mail d'hameçonnage est créé dans la table sn_si_phishing_email , le champ État est défini sur **Nouveau**. Lorsque cet enregistrement d'e-mail est converti en incident de sécurité (voir Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité), le champ État est mis à jour sur **Traité**.
Origine de l'en-tête	Ce champ indique l'origine des en-têtes de l'e-mail ou la manière dont l'utilisateur a signalé l'e-mail d'hameçonnage : • **En-tête d'e-mail** : l'utilisateur a transféré l'e-mail d'hameçonnage à l'équipe des opérations de sécurité. • **Corps du texte de l'e-mail :** ◦ L'utilisateur a cliqué sur l'option **Signaler un hameçonnage** (si le module d'extension **PhishAlarm** (précédemment connu sous le nom de Wombat) a été configuré avec le client de messagerie). ◦ En fonction de la règle User Reported Phishing définie, l'e-mail d'hameçonnage est transmis à l'équipe des opérations de sécurité. • **En-tête de pièce jointe EML** : ◦ Pièce jointe : l'utilisateur a transféré l'e-mail sous forme de pièce jointe (. EML). ◦ Soumission de Catalogue de services : l'utilisateur a téléchargé l'e-mail en tant que . EML sur le bureau, puis téléchargé vers un emplacement spécifié. L'incident de sécurité est ensuite créé à partir de l'e-mail. • **Corps de pièce jointe EML** : ◦ L'utilisateur a cliqué sur l'option **Signaler un hameçonnage** (si le module d'extension **PhishAlarm** (précédemment connu sous le nom de Wombat) a été configuré avec le client de messagerie). ◦ En fonction de la règle User Reported Phishing définie, l'e-mail d'hameçonnage est transmis en pièce jointe à l'équipe des opérations de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de l'e-mail d'hameçonnage de l'incident de sécurité (suite)

Nom de champ	Description
Incident de sécurité	Ce champ est vide lorsque l'e-mail d'hameçonnage signalé par l'utilisateur est signalé pour la première fois. Lorsque le Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité flux a été exécuté, cet e-mail est converti en enregistrement d'incident de sécurité et le numéro de cet enregistrement est affiché ici.
En-têtes bruts	Ce champ affiche les informations d'en-tête complètes extraites de l'e-mail, telles que définies dans la Définir les propriétés de hameçonnage signalé par un utilisateur page. Les en-têtes sont analysés en paires de valeurs clés et affichés dans la liste En-têtes des e-mails d'hameçonnage.
	
Détails	Il s'agit du corps de l'e-mail d'hameçonnage signalé par l'utilisateur.

Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité

Le flux **Transformer l'e-mail d'hameçonnage en incident de sécurité** est un nouveau flux qui convertit ou transforme les enregistrements d'e-mails d'hameçonnage en incidents de sécurité.

Avant de commencer

Remarque : Pour activer la fonctionnalité User Reported Phishing, vous devez créer une copie du flux et l'activer . Si vous avez créé des actions entrantes personnalisées et des flux personnalisés pour gérer les soumissions d'hameçonnage signalées par les utilisateurs, les modifications de flux suggérées ici ne sont pas requises.

- Rôle requis : sn_si.admin
- Le spoke Flow Designer doit être installé.

Pourquoi et quand exécuter cette tâche

Ce flux est automatiquement lancé lorsqu'un enregistrement d'e-mail de hameçonnage signalé par un utilisateur avec l'état défini sur **Nouveau** est créé. Ce flux contient la logique pour :

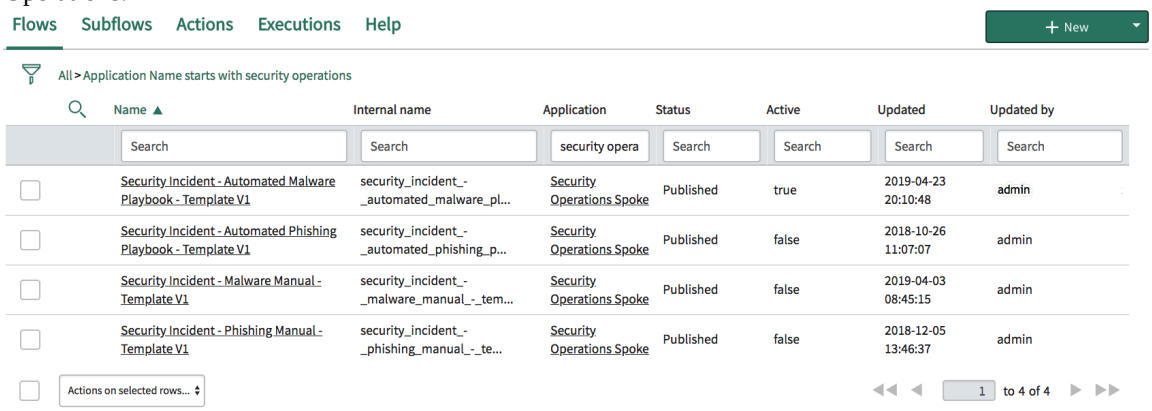
- Regrouper les incidents de sécurité.
- Mettez à jour les incidents de sécurité avec les notes pertinentes.
- Ajoutez des données d'en-tête.
- Créez des incidents enfants selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

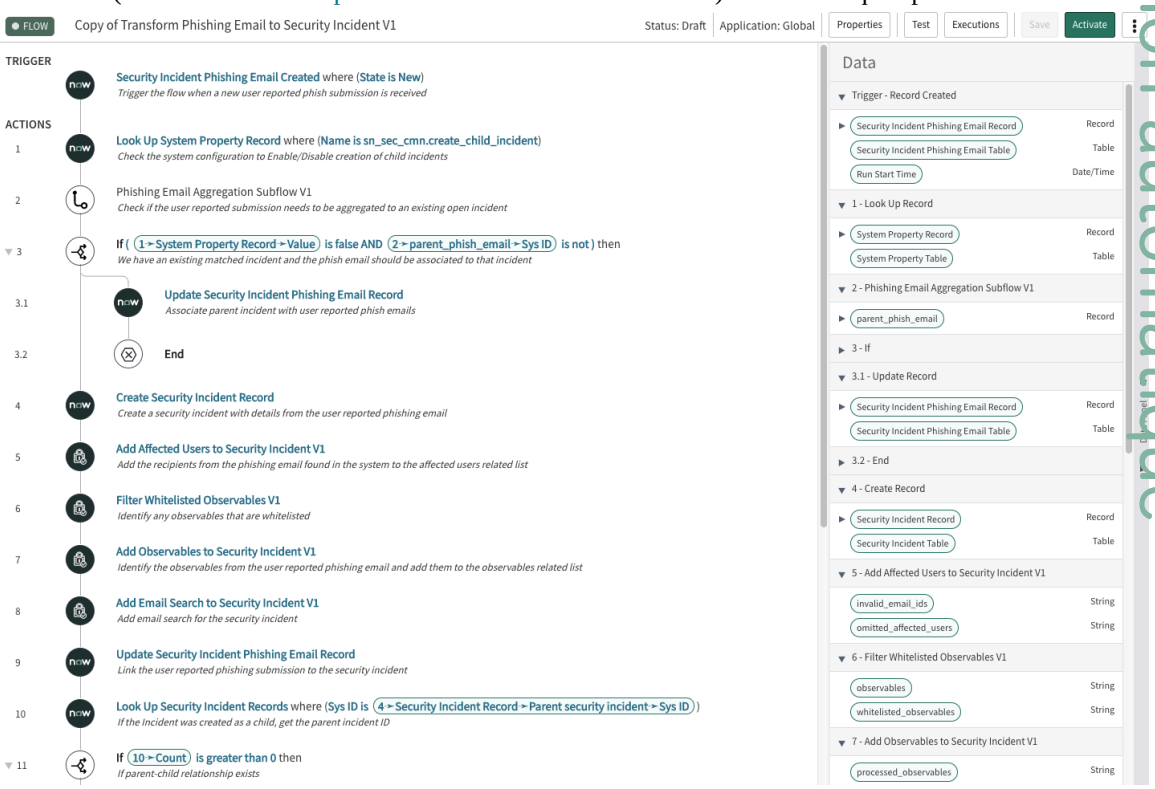
Procédure

- Accédez à la **Concepteur de flux** > **Concepteur** pour afficher les flux disponibles avec le spoke Security Operations.



- Cliquez sur le lien **Transformer l'e-mail d'hameçonnage en incidents de sécurité** pour afficher le flux.
- Ce flux est fourni avec le système de base et est en mode **lecture seule** et ne peut pas être utilisé.

  Cliquez sur , faites une copie du flux et ouvrez-le pour votre utilisation. Vous pouvez maintenant apporter des changements à votre flux, tels que la modification des conditions ou des actions de déclenchement, ou l'ajout et la suppression d'actions. Après avoir apporté les modifications nécessaires, vous devez activer (Voir Activer un Réponse aux incidents de sécurité flux) le flux afin qu'il puisse être exécuté.



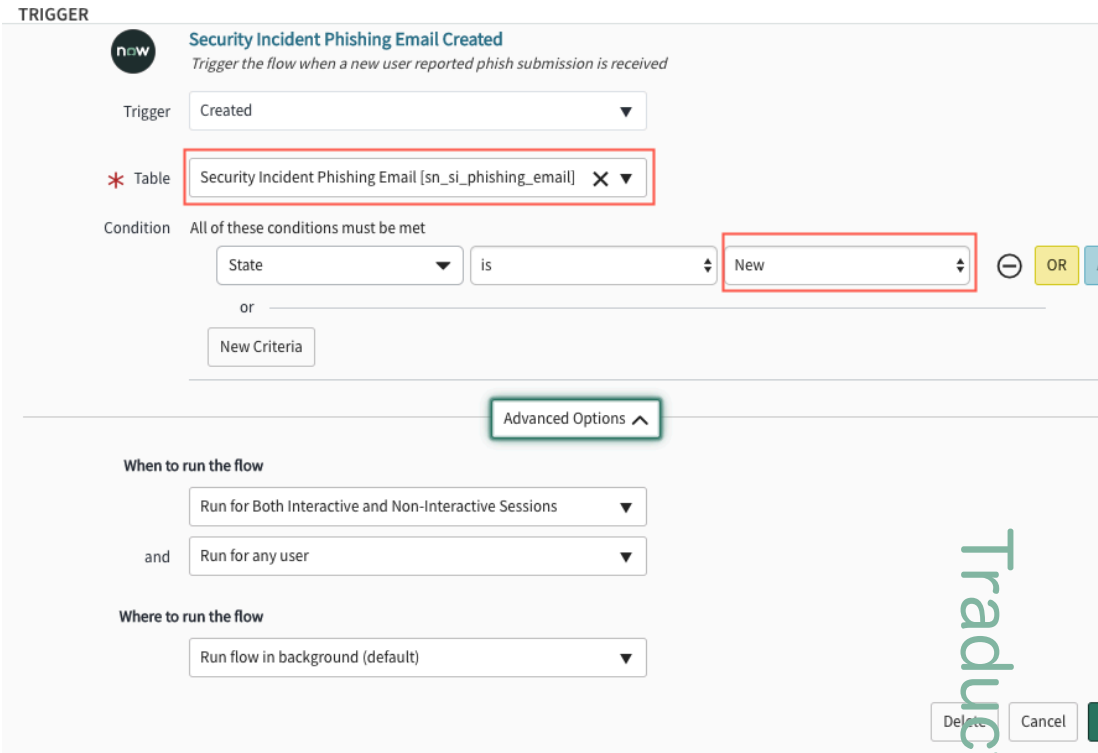
  Cette figure illustre le déclencheur et les étapes exécutées avec le flux. Le panneau de droite affiche le flux de données. Cliquez sur une icône pour développer l'étape et afficher les détails.

- Cliquez sur l'icône **Déclencher** .
  Dans la première étape, vous définissez ou définissez le déclencheur du flux. Spécifiez les conditions pour le déclencheur et la tâche à effectuer lorsque les conditions sont

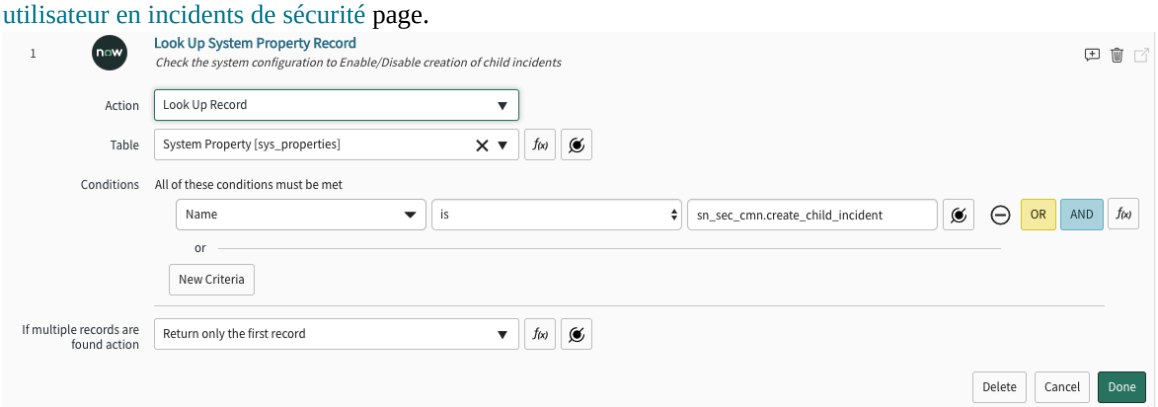
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

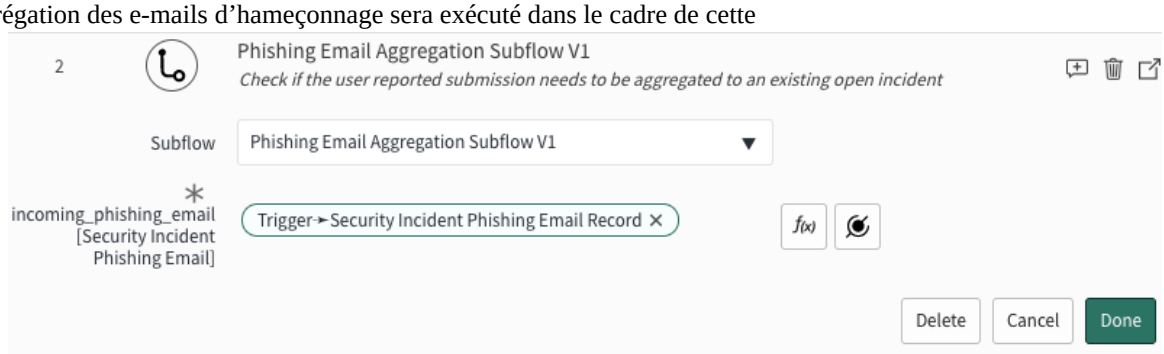
remplies. Ce flux est lancé lorsqu'un **nouvel** enregistrement est chargé dans la table sn_si_phishing_email .



- À l'étape 1, le flux vérifie si le marqueur **Créer des incidents enfants pour les soumissions d'e-mails agrégées ?** est activé ou désactivé dans la Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité page.



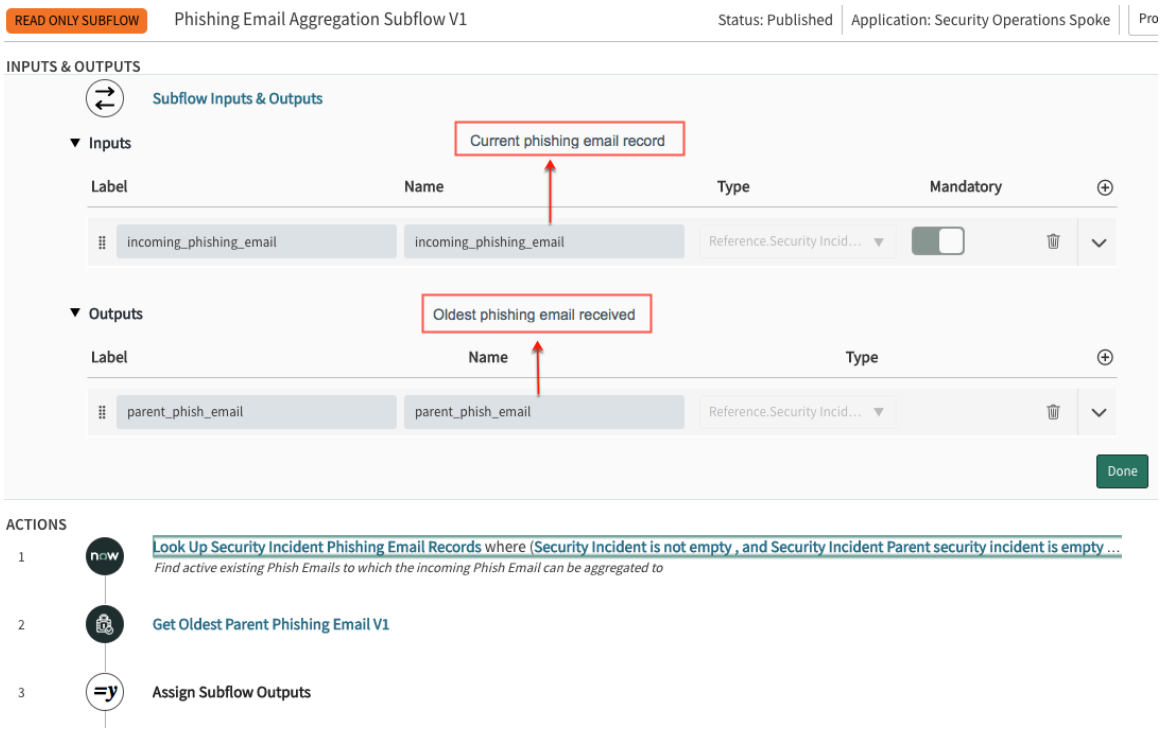
- À l'étape 2, l'incident de sécurité parent le plus ancien est identifié.
  Remarquez l'icône à l'étape 2. Cela indique que le flux secondaire d'agrégation des e-mails d'hameçonnage sera exécuté dans le cadre de cette étape.



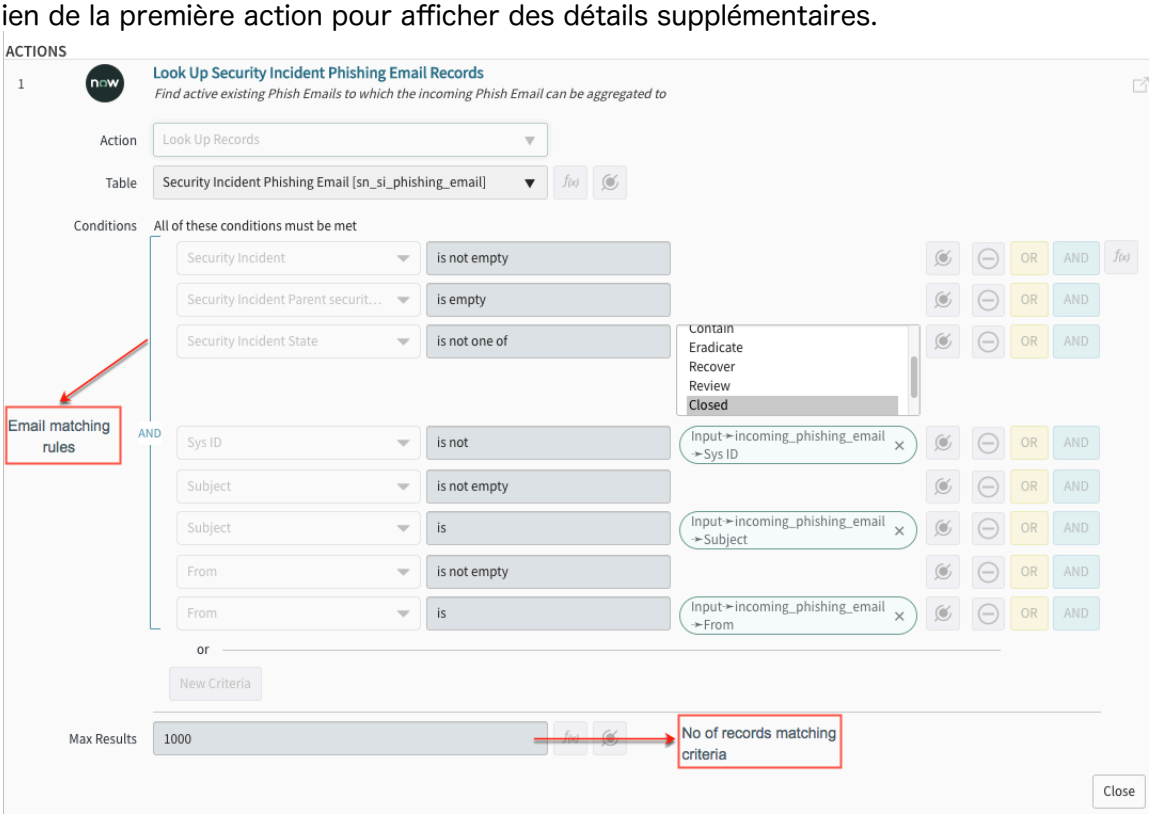
Cliquez sur l'icône du concepteur d'action pour afficher une vue détaillée de l'action. Ce flux secondaire vérifie l'e-mail d'hameçonnage et le met en correspondance avec un incident de sécurité existant en fonction des critères spécifiés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Ces deux actions sont effectuées lorsque ce flux secondaire est exécuté. Cliquez sur le lien de la première action pour afficher des détails supplémentaires.



Cette action vérifie les e-mails qui correspondent aux critères du nouvel e-mail entrant en fonction de conditions telles que :

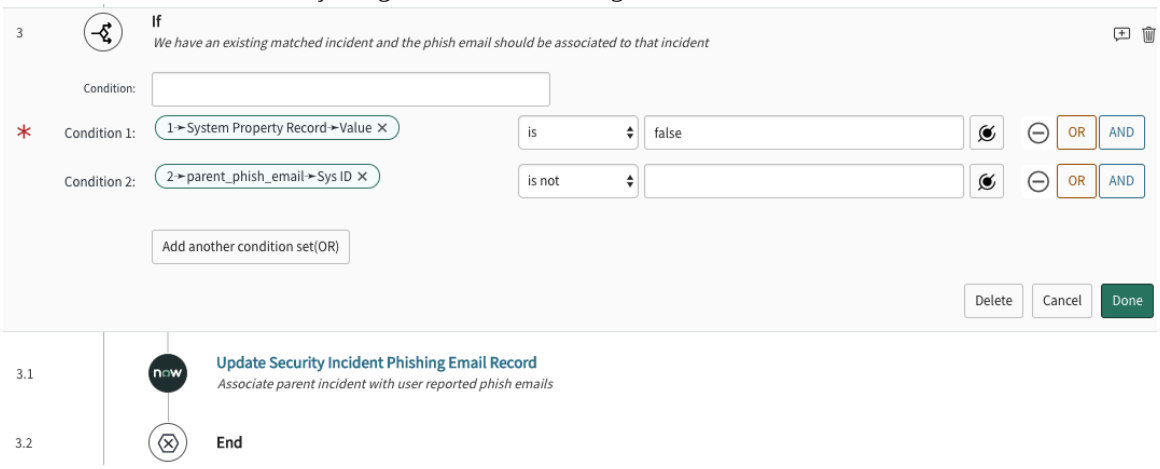
- L'état de l'incident de sécurité n'est pas **Fermé**.
- La valeur Objet ou De correspond aux conditions de règle de correspondance d'e-mail définies (voir Configurer des règles d'intégration pour l'hameçonnage signalé par un utilisateur).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si ces conditions sont remplies, vous pouvez voir le nombre d'enregistrements qui correspondent aux critères dans le champ Nombre maximal de résultats. L'enregistrement le plus ancien ou le premier de la liste est désigné comme l'enregistrement parent par rapport auquel les incidents de sécurité seront regroupés.

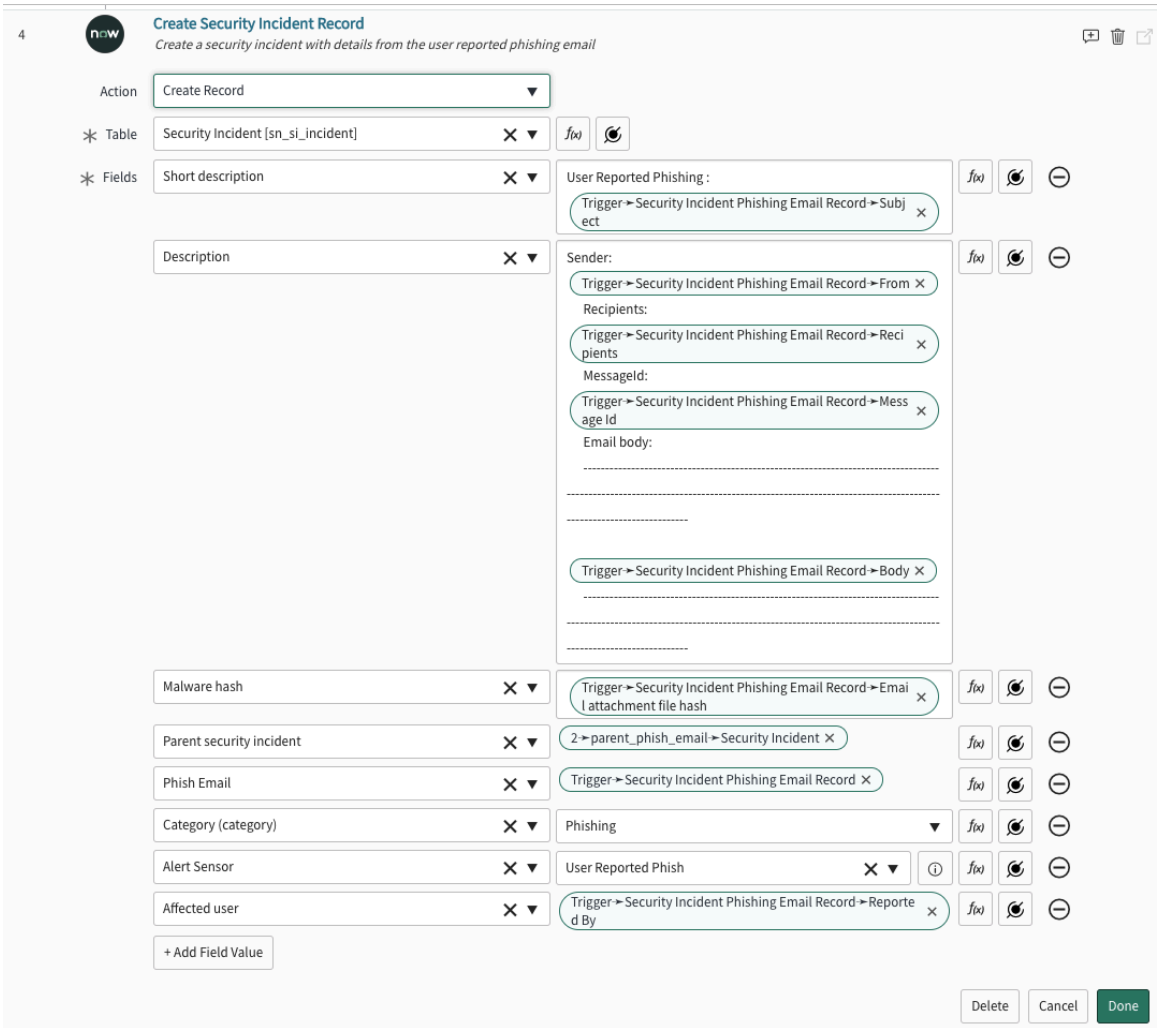
- L'étape 3 s'applique uniquement si le marqueur **Créer des incidents enfants pour les soumissions d'e-mails agrégées ?** a été défini sur **Non** dans la Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité page.
  Dans ce cas, l'e-mail d'hameçonnage est associé à l'enregistrement d'incident de sécurité et le flux s'arrête.



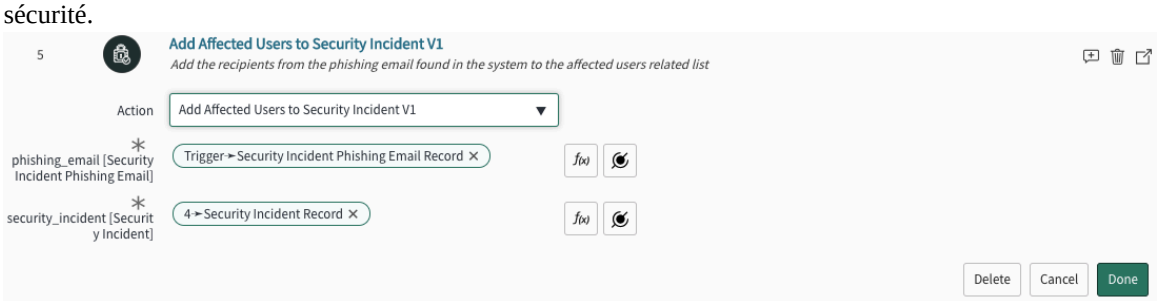
- Si l'option **Créer des incidents enfants pour les soumissions d'e-mails agrégées ?** a été définie sur **Oui**, le flux continue de s'exécuter et un nouvel incident de sécurité est créé en fonction de l'e-mail d'hameçonnage signalé par l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- À l’étape 5, les utilisateurs qui ont reçu l’e-mail d’hameçonnage (employés dans la liste À et CC de l’e-mail d’hameçonnage) sont ajoutés à la liste connexe Utilisateurs affectés dans l’enregistrement d’incident de sécurité.



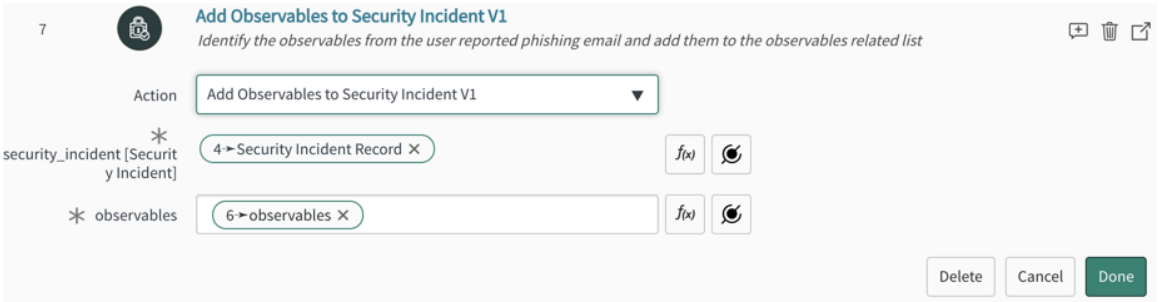
- À l’étape 6, les observables sur la liste d’autorisation sont filtrés à partir de la liste des observables dans l’incident de sécurité.
  Ces éléments observables répertoriés comme autorisation ne seront pas ajoutés à l’incident de sécurité.



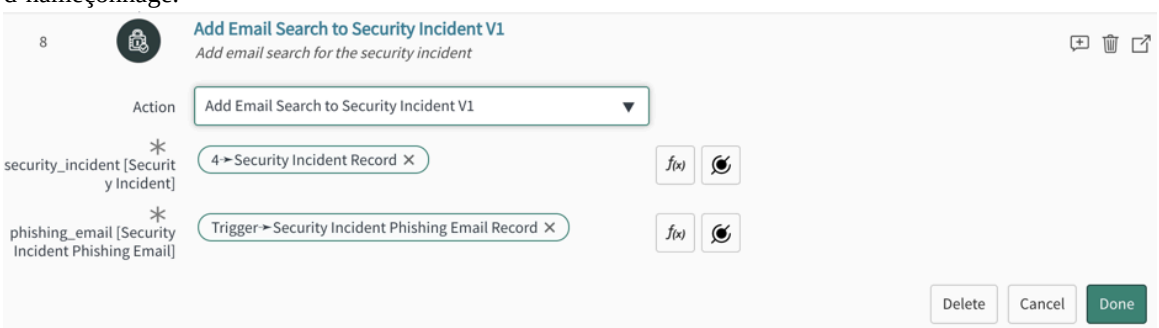
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

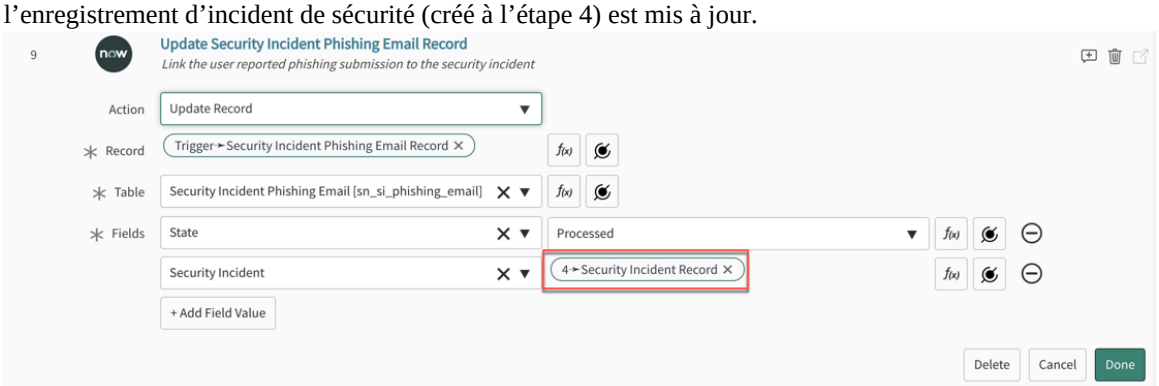
- À l'étape 7, les observables inconnus de l'e-mail d'hameçonnage signalé par l'utilisateur sont identifiés et ajoutés à la liste connexe Observables.



- À l'étape 8, une requête de recherche d'e-mails est générée, qui est une combinaison de l'objet et de l'adresse De de l'e-mail.
  Ces informations sont utiles pour identifier les employés de l'organisation qui ont été victimes d'hameçonnage.



- À l'étape 9, l'e-mail d'hameçonnage signalé par l'utilisateur est associé à l'incident de sécurité et l'enregistrement d'incident de sécurité (créé à l'étape 4) est mis à jour.



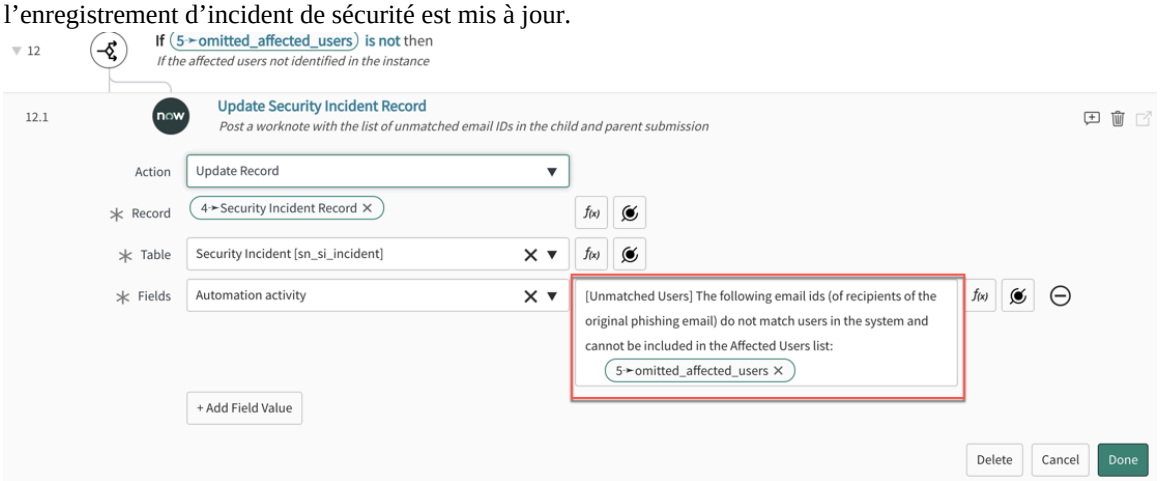
- À l'étape 10, l'incident de sécurité parent est identifié et une vérification est effectuée pour voir s'il s'agit d'un enregistrement d'incident de sécurité ouvert.



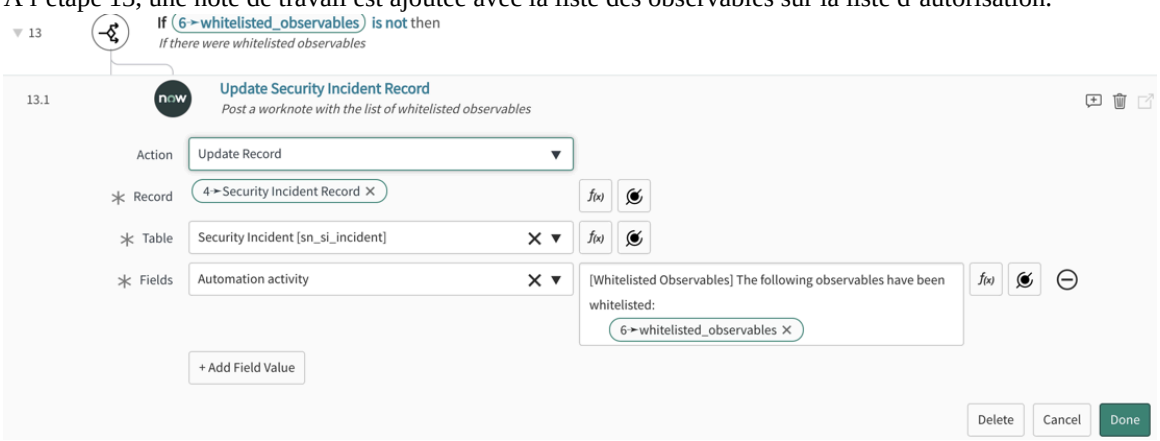
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si la sécurité parent est active, des notes sont ajoutées aux enregistrements d'incident de sécurité enfant et parent, indiquant comment ils sont associés les uns aux autres.
- À l'étape 12, si aucun utilisateur affecté n'est trouvé (à l'étape 5 du flux), une note de travail est ajoutée et l'enregistrement d'incident de sécurité est mis à jour.



- À l'étape 13, une note de travail est ajoutée avec la liste des observables sur la liste d'autorisation.



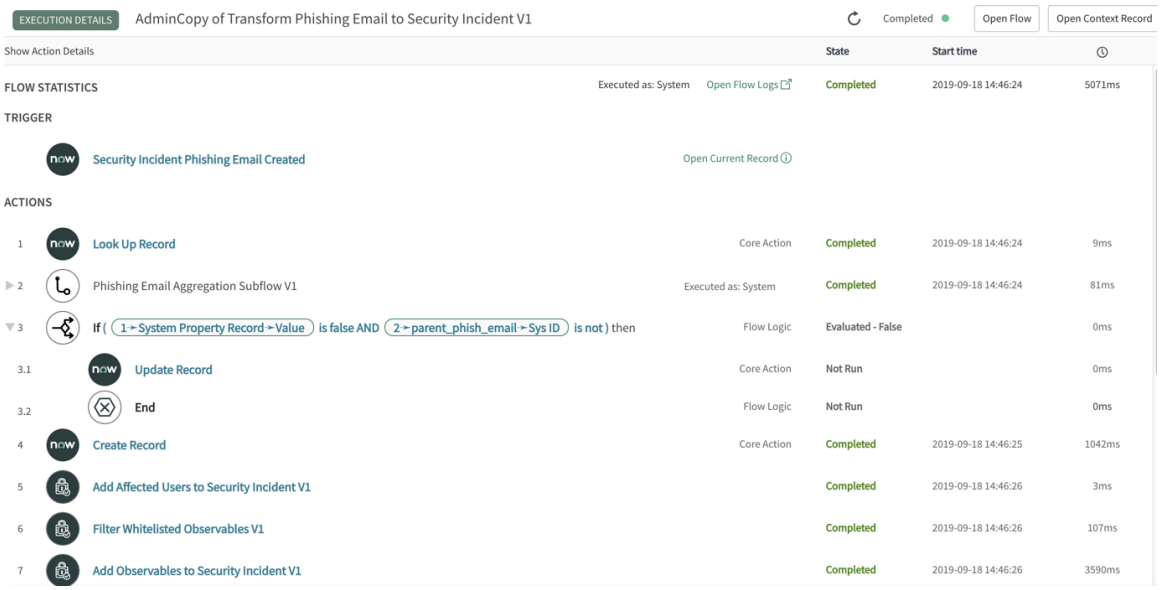
Que faire ensuite

Vous pouvez cliquer sur **Tester** pour simuler les actions dans le flux avant sa publication. Après avoir testé le flux, cliquez sur **Activer** pour activer le flux afin qu'il puisse être exécuté.

Cliquez sur **Exécutions** pour afficher les détails d'exécution du flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

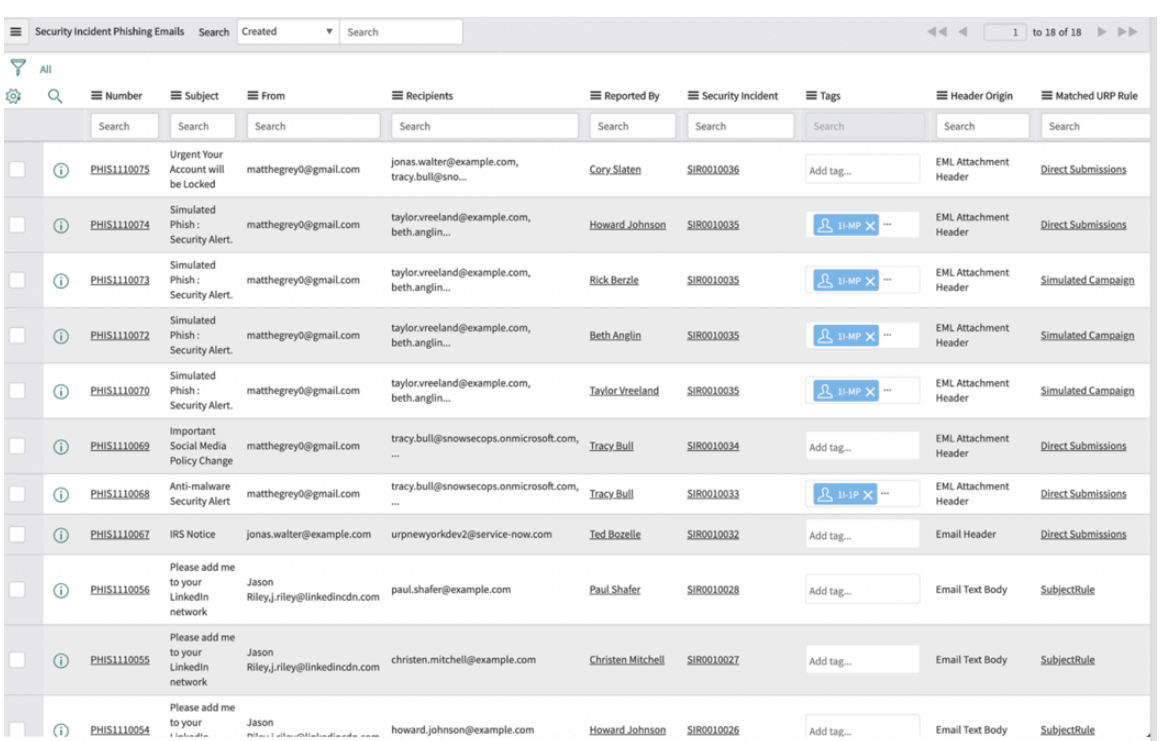


Lorsque le flux a été exécuté, l'enregistrement de l'e-mail d'hameçonnage est converti en incident de sécurité. Reportez-vous à la rubrique Enregistrements d'incidents de sécurité créés à partir d'enregistrements d'e-mails d'hameçonnage.

Enregistrements d'incidents de sécurité créés à partir d'enregistrements d'e-mails d'hameçonnage

Les enregistrements d'e-mails d'hameçonnage stockés dans la table `sn_si_phishing_email` sont convertis en enregistrements d'incidents de sécurité.

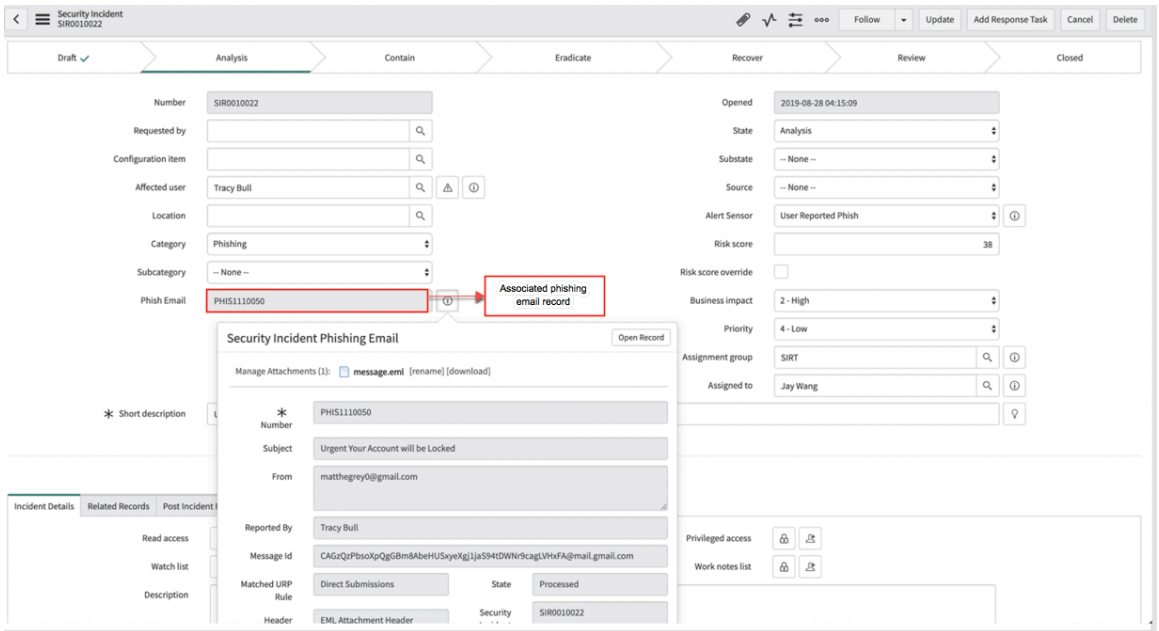
Pour afficher l'incident de sécurité associé à l'enregistrement de l'e-mail d'hameçonnage, cliquez sur **Incident de sécurité** > **E-mail de hameçonnage** > **Afficher tous les e-mails d'hameçonnage**.



Cliquez sur le lien dans la colonne Incident de sécurité associé à l'enregistrement de l'e-mail d'hameçonnage. Les détails de l'incident de sécurité s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



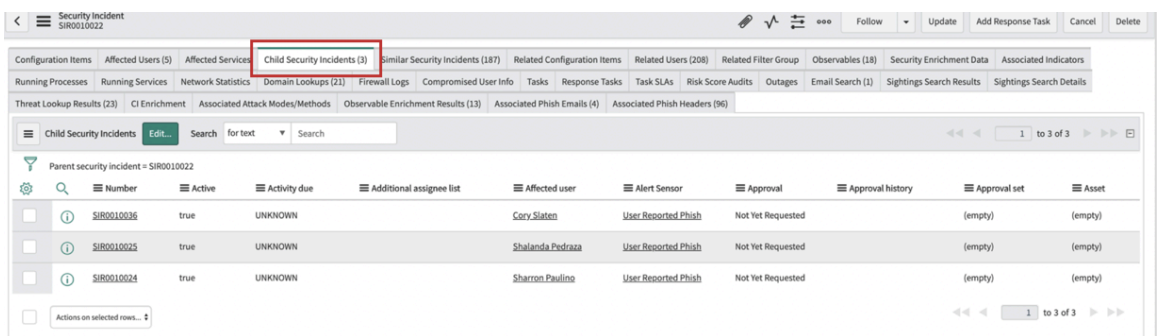
Listes connexes

Faites défiler la page vers le bas jusqu'à la section Liens connexes de l'incident de sécurité et cliquez sur **la liste connexe Afficher tout**. Affichez des détails tels que les incidents de sécurité enfants, les utilisateurs affectés, les e-mails d'hameçonnage associés.

Incidents de sécurité enfants

Cliquez sur l'onglet **Incidents de sécurité enfants** . Vous pouvez consulter une liste des incidents de sécurité enfants associés à l'incident de sécurité parent en fonction de la logique d'agrégation qui a été appliquée. Pour chaque enregistrement enfant ajouté, une activité système automatisée est ajoutée (dans la section Worknote) à l'enregistrement parent. L'analyste de sécurité est informé de l'enregistrement enfant regroupé.

Remarque : Vous pouvez voir les incidents de sécurité enfants ici uniquement si le marqueur **Créer des incidents enfants pour les soumissions d'e-mails agrégées** est défini sur **Oui** dans la page Propriétés de hameçonnage signalé par un utilisateur. Consultez Définir les propriétés de hameçonnage signalé par un utilisateur pour en savoir plus.

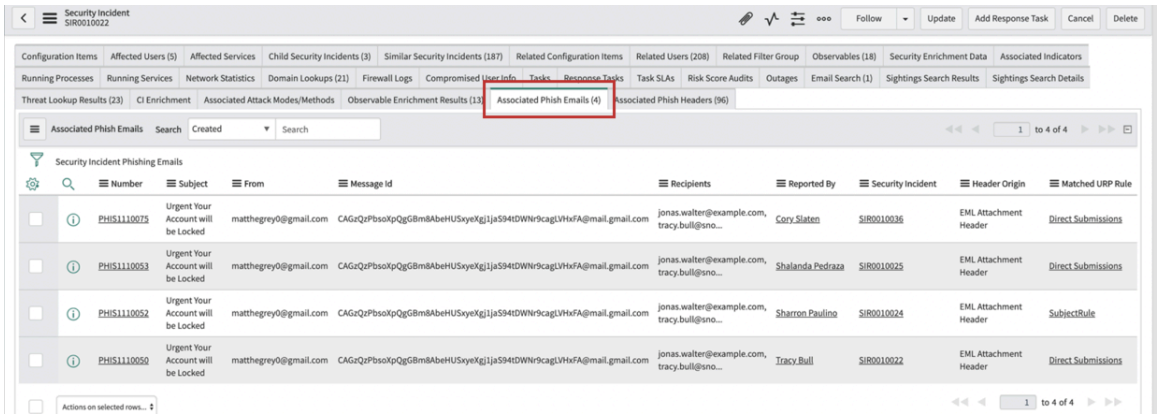


E-mails d'hameçonnage associés

Cliquez sur l'onglet **E-mails d'hameçonnage associés** . Une liste d'enregistrements d'e-mails d'hameçonnage (enregistrements en double) associés à l'enregistrement d'e-mail d'hameçonnage parent s'affiche.

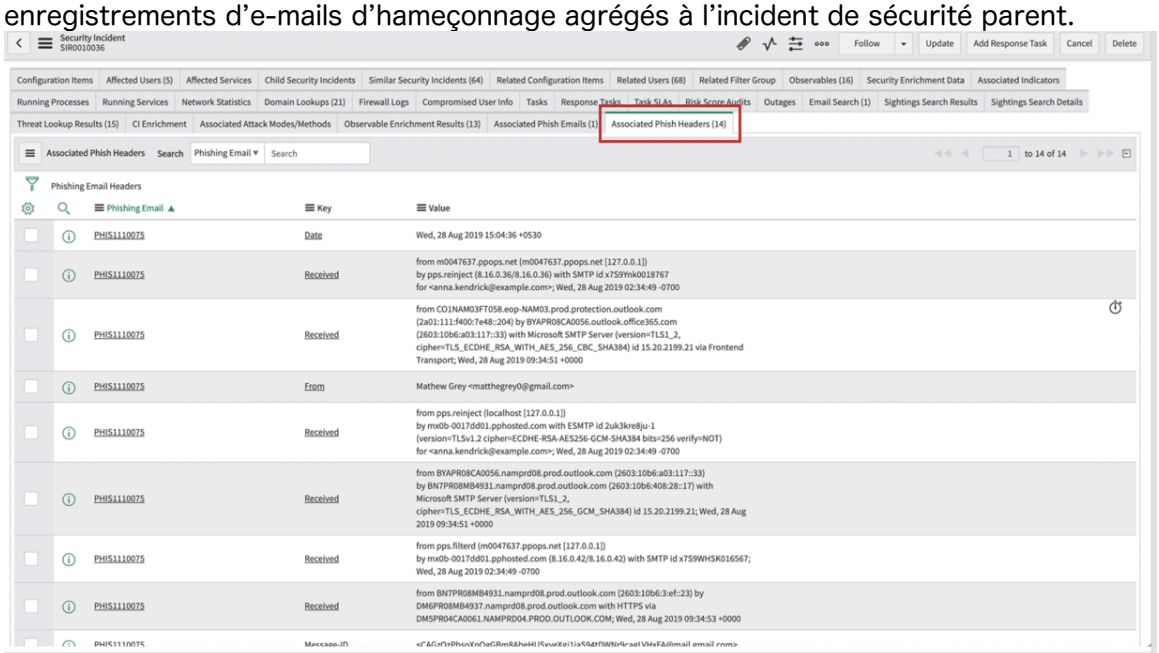
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



En-têtes d'e-mails d'hameçonnage associés

Cliquez sur l'onglet **E-mails d'hameçonnage associés** . Vous voyez les détails de l'en-tête de l'e-mail d'hameçonnage qui ont été capturés dans le cadre de l'incident de sécurité. Vous pouvez afficher les en-têtes cumulés de tous les enregistrements enfants et les enregistrements d'e-mails d'hameçonnage agrégés à l'incident de sécurité parent.



Observables de liste d'autorisation

Pendant l'exécution du Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité flux, vous pouvez surveiller l'état de l'incident de sécurité. Lorsque certains observables sont marqués comme observables de liste d'autorisation, ils ne sont pas ajoutés à la liste connexe des observables. En marquant les observables sur la liste d'autorisation, vous pouvez vous assurer que seuls les détails importants sont affichés. Par exemple, s'www.google.com une des URL qui a été balisée comme liste d'autorisation, le message système suivant s'affiche. La liste d'autorisation des observables garantit que seuls les observables importants sont surveillés.

Capture des utilisateurs sans correspondance

Certains ID d'e-mail de la liste À et CC de l'e-mail d'hameçonnage peuvent ne pas appartenir à des utilisateurs de l'organisation. Ces ID d'e-mail sont classés comme des utilisateurs sans correspondance et ne sont pas inclus dans la liste connexe des utilisateurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

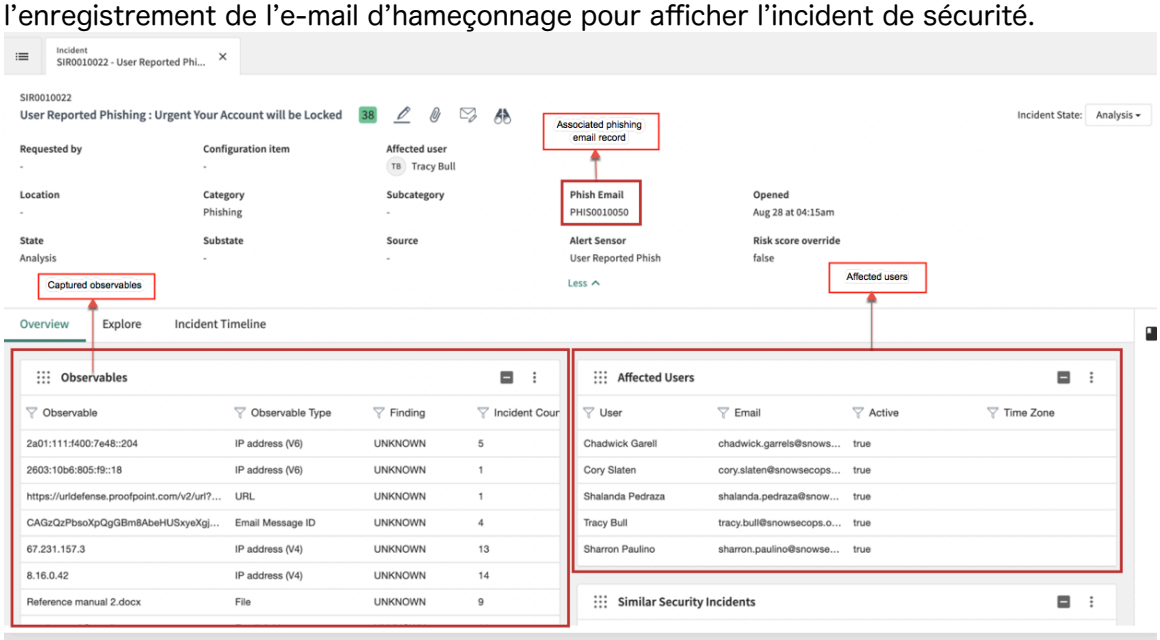
affectés. Une note de travail indiquant qu'il s'agit d'utilisateurs sans correspondance s'affiche.



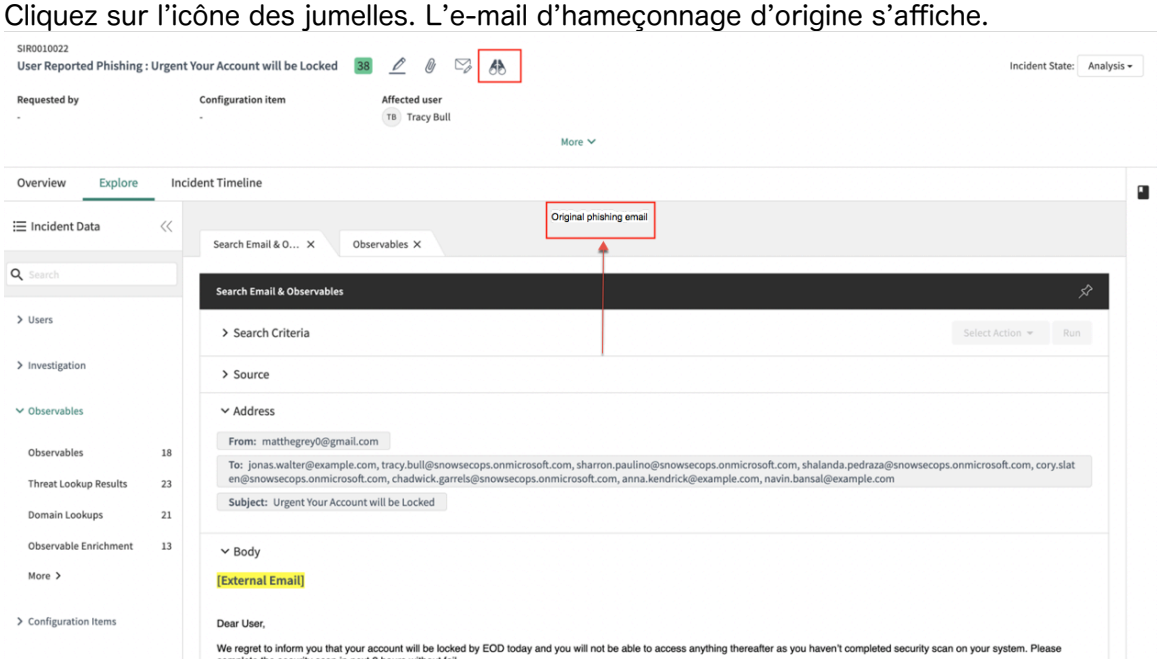
Hameçonnage signalé par un utilisateur dans Security Analyst Workspace

Vous pouvez afficher les incidents de sécurité associés aux enregistrements d'e-mails d'hameçonnage dans l'Espace de travail de l'analyste de la sécurité.

Accédez à la **Incident de sécurité** > **Nouvelle interface utilisateur**. L'espace de travail s'ouvre dans un onglet de navigateur distinct. Cliquez sur l'incident de sécurité associé à l'enregistrement de l'e-mail d'hameçonnage pour afficher l'incident de sécurité.



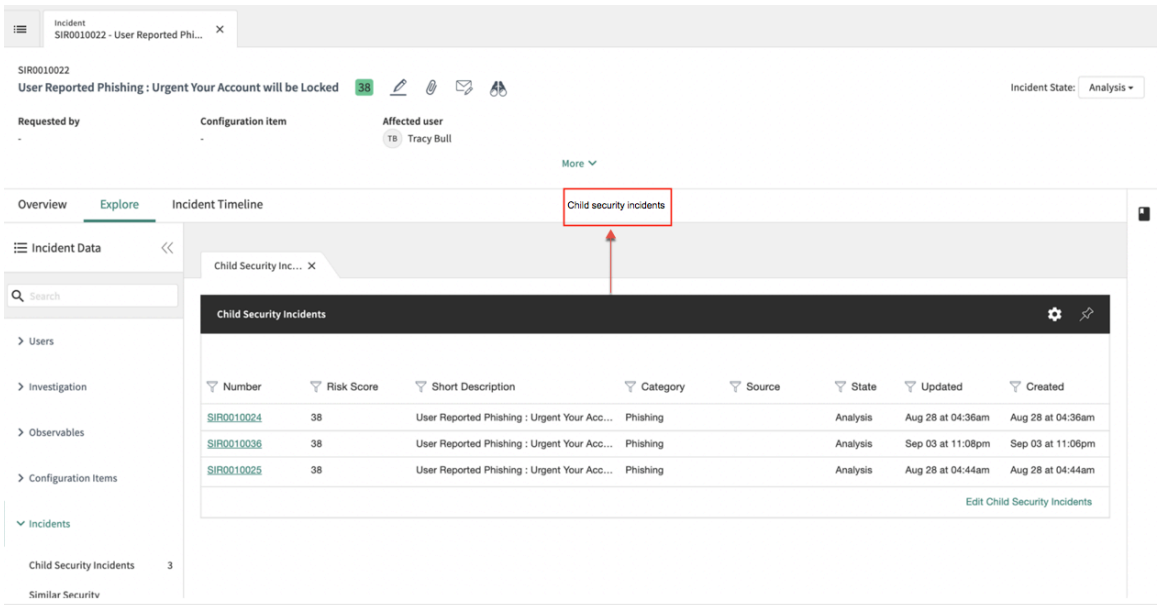
Cliquez sur l'icône des jumelles. L'e-mail d'hameçonnage d'origine s'affiche.



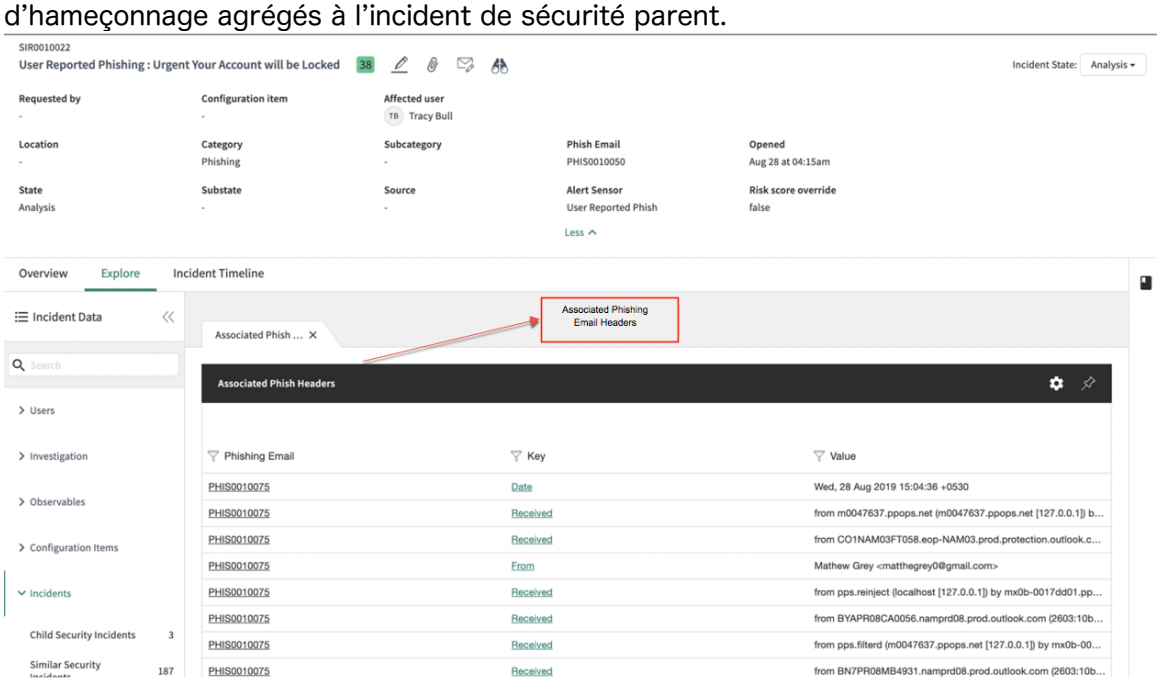
Dans l'onglet **Explorer** , cliquez sur **Incidents** > **Incidents de sécurité enfants**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



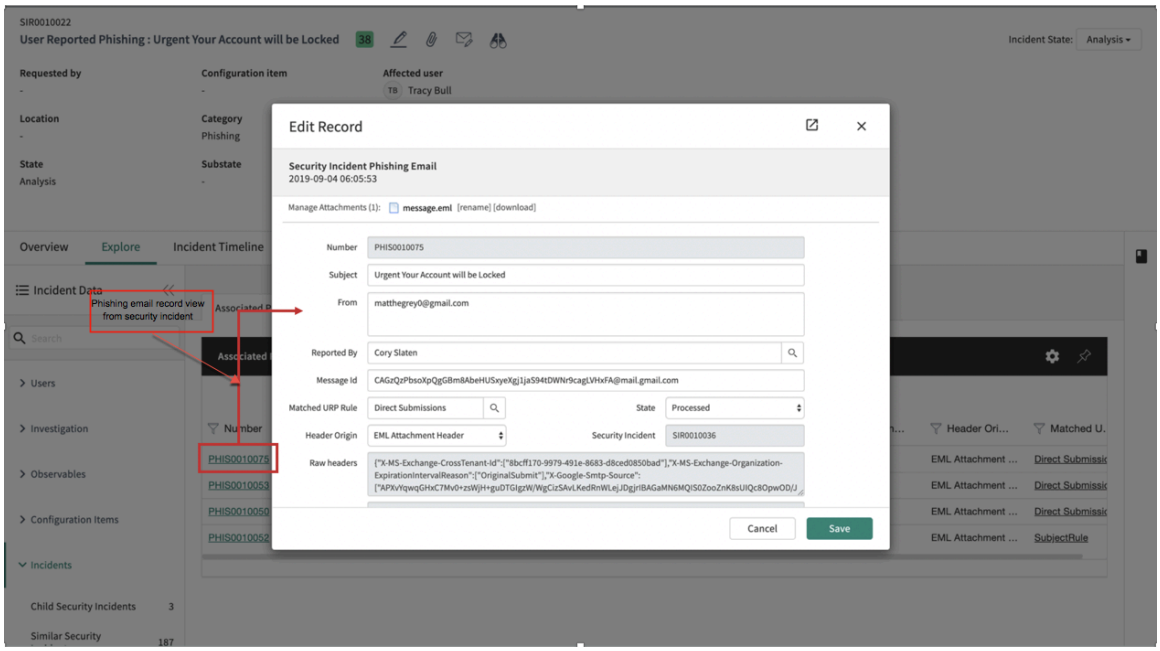
Cliquer sur **Incidents** > **En-têtes d'hameçonnage associés** > . Vous pouvez afficher les en-têtes cumulés de tous les enregistrements enfants et les enregistrements d'e-mails d'hameçonnage agrégés à l'incident de sécurité parent.



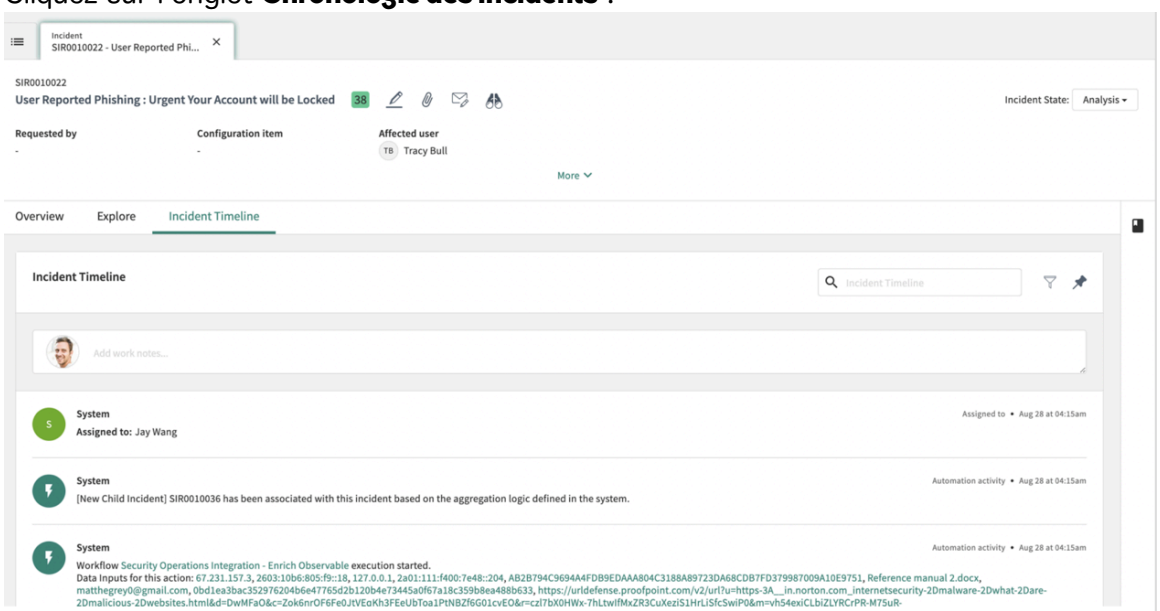
Cliquez sur le lien de l'e-mail d'hameçonnage pour afficher l'enregistrement de l'e-mail d'hameçonnage associé à l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cliquez sur l'onglet **Chronologie des incidents** .



Traduction automatique

Vous pouvez consulter les mises à jour système qui mettent en évidence :

- Identifier les enregistrements enfants en double.
- Observables sur liste d'autorisation.
- Utilisateurs sans correspondance ayant reçu l'e-mail d'hameçonnage, mais n'appartenant pas à la liste des utilisateurs affectés.

Forum aux questions

Cette section couvre certaines des questions fréquemment posées sur la fonctionnalité améliorée d'hameçonnage signalé par un utilisateur.

1. J'ai installé le nouveau spoke Réponse aux incidents de sécurité, mais je ne peux afficher aucun incident d'hameçonnage signalé par un utilisateur.

   Par défaut, la fonctionnalité User Reported Phishing a été désactivée.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour activer cette fonctionnalité, vous devez faire une copie du flux en lecture seule Transformer les e-mails d'hameçonnage signalés par un utilisateur en incidents de sécurité et l'activer avant utilisation.

2. Lors de l'ingestion d'e-mails d'hameçonnage et de leur conversion en incidents de sécurité, quelles mesures de précaution sont utilisées pour gérer les liens et les pièces jointes malveillants contenus dans les e-mails d'hameçonnage ?

   L'analyseur ServiceNow antivirus analyse ces pièces jointes et ces liens malveillants. Cependant, pour s'assurer que les analystes de sécurité peuvent enquêter avec précision sur les incidents, l'application Réponse aux incidents de sécurité capture tous les artefacts qui font partie d'un e-mail d'hameçonnage. Mais la fonctionnalité User Reported Phishing désactive les liens malveillants contenus dans l'e-mail de phishing afin que les analystes de sécurité ne cliquent pas accidentellement sur ces liens. En ce qui concerne les pièces jointes malveillantes, les analystes de sécurité doivent être prudents lorsqu'ils les téléchargent.

3. Est-ce que nous capturons tous les fichiers malveillants qui font partie des e-mails d'hameçonnage pour enrichir les incidents de sécurité ?

   Oui, nous capturons tous les fichiers des e-mails d'hameçonnage. Vous pouvez afficher ces détails dans le cadre des observables d'incident de sécurité sous la forme d'un hachage de fichier.

4. Envoyons-nous des fichiers et des liens malveillants à partir d'e-mails d'hameçonnage à une instance de bac à sable pour enquête ?

   Actuellement, nous ne prenons pas en charge les intégrations de bac à sable prêtes à l'emploi pour enquêter sur les liens et les fichiers malveillants.

5. Existe-t-il une fenêtre de temps ou un déclencheur qui définit la durée pendant laquelle les enregistrements d'e-mails d'hameçonnage entrants en double sont associés à un incident de sécurité parent ?

   Les enregistrements d'e-mails d'hameçonnage en double sont regroupés uniquement en un incident de sécurité parent actif. Si l'incident parent est fermé ou annulé, le nouvel e-mail d'hameçonnage en double entrant est créé en tant que nouvel incident de sécurité. Toutefois, dans ce scénario, au sein du nouvel incident de sécurité, vous pouvez afficher l'incident de sécurité parent fermé ou annulé dans la liste connexe **Incident de sécurité similaire** .

   Remarque : Ce comportement peut être configuré à l'aide du concepteur de flux.

6. La fonctionnalité User Report Phishing prend-elle en charge l'utilisation uniquement du module d'extension Microsoft Outlook **PhishAlarm** (précédemment connu sous le nom de Wombat) pour capturer les détails d'en-tête d'e-mail ?

   La fonctionnalité Signalé par l'utilisateur a été conçue pour analyser les en-têtes d'e-mail et est conforme à la norme RFC822. Ainsi, à l'instar du plugin **PhishAlarm** (anciennement connu sous le nom de Wombat), tous les autres plugins Microsoft Outlook qui capturent les en-têtes d'e-mail basés sur les normes RFC822 sont pris en charge.

Création d'enregistrements à partir d'incidents de sécurité

Une fois que vous avez créé et enregistré un incident de sécurité, vous pouvez créer un enregistrement de demande de changement (CHG), d'incident (INC) ou de problème (PRB)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à partir de celui-ci. Vous pouvez également créer un ticket du service clientèle à partir de n'importe quel incident de sécurité.

Créer un changement, un incident ou un problème à partir d'un incident de sécurité

Une fois que vous avez créé et enregistré un incident de sécurité, vous pouvez créer un enregistrement de demande de changement (CHG), d'incident (INC) ou de problème (PRB) à partir de celui-ci.

Avant de commencer

Rôle requis : sn.si_basic ou supérieur

Procédure

1. Ouvrez un incident de sécurité à l'aide de l'une des méthodes suivantes.
   - Ouvrez un incident de sécurité existant en accédant à **Incident de sécurité** > **Non affecté** > **Incidents**, puis en cliquant sur un incident de sécurité.
   - Créer un incident de sécurité en accédant à **Incident de sécurité** > **Non affecté** > **Incidents**, cliquez sur **Nouveau**, remplissez le formulaire et enregistrez l'enregistrement.
2. Cliquez avec le bouton droit dans la barre d'en-tête de l'incident de sécurité, puis cliquez sur l'une des options suivantes :
   - **Créer un changement**
   - **Créer un incident**
   - **Créer un problème**

   Remarque : Ce choix s'applique uniquement si la propriété de fenêtre contextuelle (sn_vul.popup) est activée. Lorsque vous cliquez sur l'un de ces boutons, une fenêtre d'aperçu s'ouvre pour afficher les informations relatives à l'incident de sécurité utilisé pour créer le changement, l'incident ou le problème. C'est-à-dire l'élément de configuration, son emplacement, sa priorité et les descriptions brève et longue. Si vous créez une demande de changement, vous pouvez modifier les champs **Priorité**, **Description brève** et **Description** . Si vous créez un incident, vous pouvez modifier les champs **Impact**, **Urgence**, **Description brève** et **Description** . Les champs de l'écran d'incident de sécurité associé ne sont pas affectés.
3. Cliquez sur **Soumettre** pour créer le changement, l'incident ou le problème.

Créer un ticket du service clientèle à partir d'un incident de sécurité

Réponse aux incidents de sécurité est fourni avec un mappage de champs par défaut qui mappe un incident de sécurité à un Service client ticket (CS). Vous pouvez créer un ticket CS à partir de n'importe quel incident de sécurité, modifier la **priorité** et également ajouter des **notes facultatives**.

Avant de commencer

Rôle requis : sn_si.basic et sn_customerservice_agent

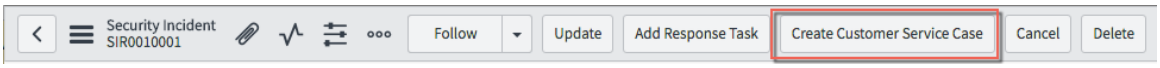
Remarque : Le Service client module d'extension doit être activé pour effectuer cette tâche.

Procédure

1. Accédez à **Incident de sécurité**.
2. Ouvrez l'incident de sécurité auquel vous souhaitez ajouter un ticket CS.
3. Cliquez sur **Créer un ticket du service clientèle** dans l'en-tête supérieur.

Traduction automatique

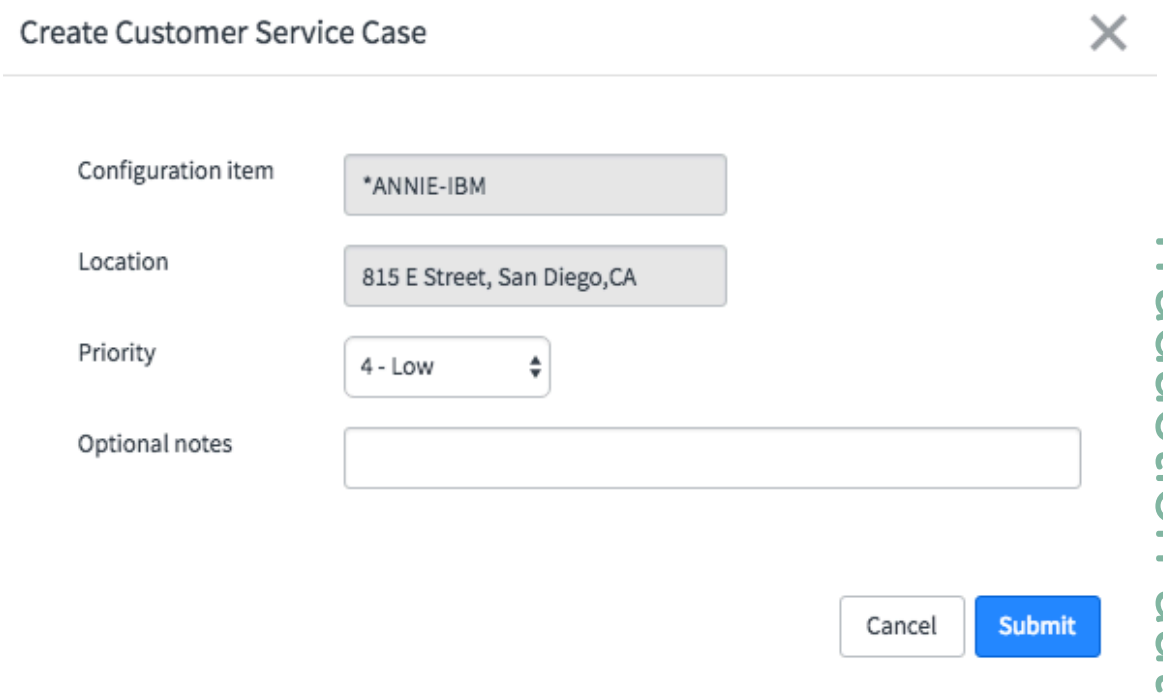
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La fenêtre contextuelle est préremplie avec les informations relatives à l'incident de sécurité en fonction de votre mappage de champs.

4. Vous pouvez sélectionner une nouvelle **priorité** et ajouter des **notes facultatives**.

Remarque : Le champ **Priorité** remplace le paramètre par défaut. Les **notes facultatives** sont annexées à l'incident.



5. Cliquez sur **Envoyer**.
   Un ticket CS est créé et affiché dans la liste connexe des tickets du service clientèle de l'incident de sécurité.
6. Vous pouvez cliquer sur le lien du ticket CS pour suivre le ticket.

Information associée

Gestion des tickets du service clientèle

Ajouter un incident de sécurité à un ticket de sécurité

Si vous déterminez qu'un incident de sécurité nécessite un niveau d'analyse plus élevé, ajoutez-le à un nouveau ticket ou à un ticket existant.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

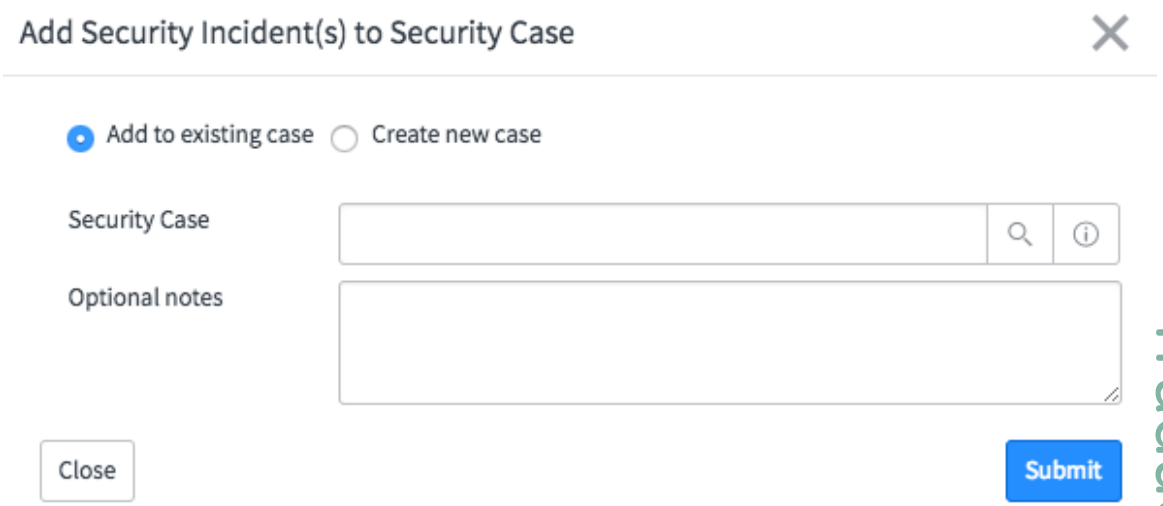
Rôle requis : sn_si.admin, sn_ti.case_user_write

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à l'incident de sécurité qui requiert une escalade en cliquant sur **Incident de sécurité** > **Incidents** > **Me l'affecter**et ouvrez l'incident de sécurité.
2. Cliquez sur le lien connexe **Ajouter au ticket de sécurité** .
   La boîte de dialogue **Ajouter un ou plusieurs incidents de sécurité au ticket de sécurité s'ouvre** .



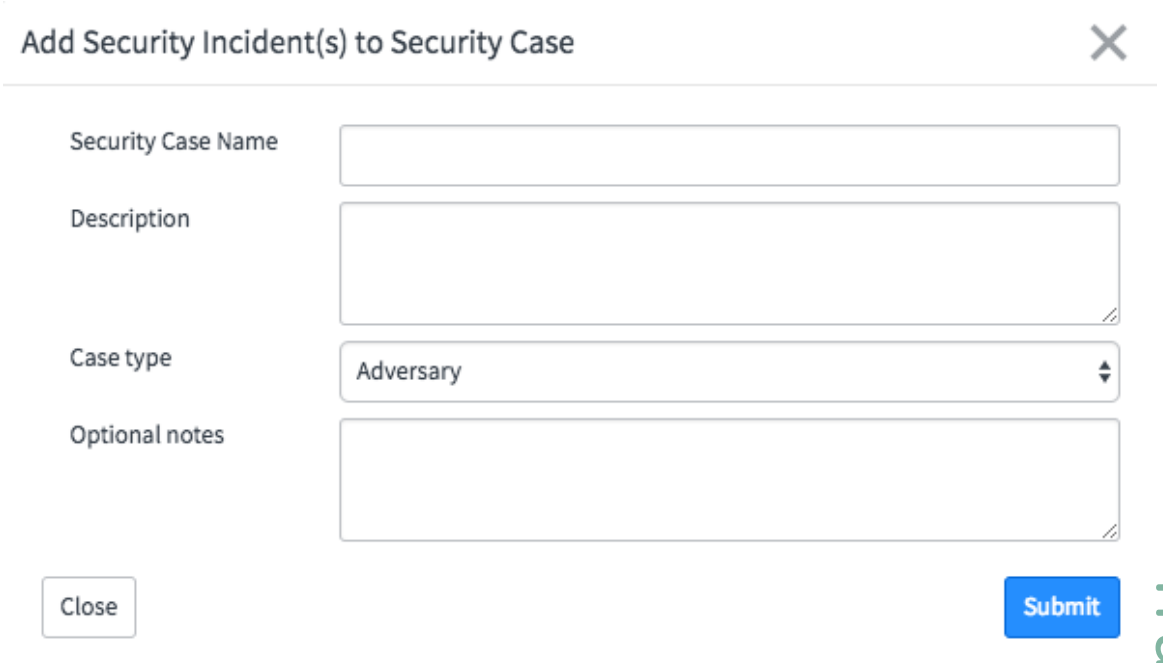
3. Si un ticket vous a été affecté et auquel vous souhaitez ajouter cet incident de sécurité, renseignez les champs comme il convient, puis cliquez sur **Soumettre**.

Champ	Description
Ticket de sécurité	Sélectionnez le ticket de sécurité.
Notes facultatives	Au besoin, saisissez des notes supplémentaires qui pourraient être utiles à l'analyste de ticket.

4. Si un ou plusieurs tickets vous sont affectés, mais que vous souhaitez créer un nouveau ticket et lui affecter l'incident de sécurité, cliquez sur **Créer un nouveau ticket** pour afficher des champs supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Si aucun ticket ne vous est affecté, l'écran ci-dessus s'ouvre en premier.

5. Renseignez les champs comme il convient.

Champ	Description
Nom du ticket de sécurité	Entrez le nom du nouveau ticket de sécurité.
Description	Saisissez une description pour le ticket.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête.
Notes facultatives	Au besoin, saisissez des notes supplémentaires qui pourraient être utiles à l'analyste de ticket.

6. Cliquez sur **Envoyer**.
   Un message apparaît en haut de l'incident de sécurité, ainsi qu'un lien vers le nouveau ticket.

Information associée

Security Case Management

Créer des tâches de réponse

Après la création d'un incident de sécurité, vous pouvez créer des tâches de réponse pour suivre les différentes actions à effectuer pour répondre au problème de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. Accédez à l'emplacement approprié pour ouvrir l'incident de sécurité pour lequel vous souhaitez créer des tâches.
   Par exemple :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour créer une tâche de réponse basée sur un incident de sécurité qui vous est affecté, sélectionnez **Incident de sécurité** > **Incidents** > **Me l'affecter**.
- Pour créer une tâche de réponse basée sur un incident de sécurité affecté à votre équipe, sélectionnez **Incident de sécurité** > **Incidents** > **Affecté à une équipe** > **Incidents**.
- Pour créer une tâche de réponse basée sur un incident de sécurité non affecté, sélectionnez **Incident de sécurité** > **Incidents** > **Incidents non affectés**.

2. Ouvrez l'incident de sécurité auquel vous souhaitez ajouter des tâches de réponse.
3. Cliquez sur le bouton **Ajouter une tâche de réponse** dans l'en-tête du formulaire.

   Remarque : Pour créer une autre tâche, cliquez sur l'onglet **Tâches** dans la liste connexe des incidents.

4. Renseignez les champs du formulaire comme il convient.

Incident de sécurité

Champ	Description
Sélectionner une balise de sécurité	Si vous avez configuré et activé des balises de sécurité, vous pouvez sélectionner une ou plusieurs balises pour ajouter des métadonnées à l'enregistrement ou spécifier le degré de sensibilité de la tâche de réponse. Si vous n'avez pas configuré ou activé les balises de sécurité, cette liste déroulante ne s'affiche pas.
Numéro	[Lecture seule] Numéro généré Réponse aux incidents de sécurité automatiquement.
Parent	[Lecture seule] Numéro de l'incident de sécurité connexe.
Élément de configuration	L'élément de configuration (ressource) affecté par le problème de sécurité.
Utilisateur affecté	Personne affectée par le problème de sécurité.
Priorité	Priorité utilisée pour déterminer quand cette tâche est exécutée.
État	État actuel de la tâche de réponse de sécurité. Lors de la création de la tâche, ce champ est défini par défaut sur **Brouillon**.
Compétences	Compétence requise pour effectuer cette tâche. Cliquez sur l'icône de verrouillage, puis sélectionnez la compétence requise. Une fois que vous avez terminé vos sélections, cliquez à nouveau sur l'icône de verrouillage.
Groupe d'affectation	Groupe d'affectation à partir duquel l'agent affecté est sélectionné.
Affecté à	Personne affectée à l'exécution de la tâche.
Description brève	Description de la Réponse aux incidents de sécurité tâche.
Description	Description de la tâche sélectionnée.
Notes sécurisées	Les notes de travail qui sont chiffrées et non visibles pour le client.
Notes de travail	Les notes de travail qui ne sont pas visibles pour le client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Commentaires supplémentaires	Commentaires que vous souhaitez rendre visibles par le client.

5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Remarque : Une fois que vous avez créé Réponse aux incidents de sécurité des tâches, vous pouvez les afficher à l'aide de l'une des applications suivantes sous le module **Tâches de réponse** :

- **Mes affectations**.
- **Affecté à une équipe**.
- **Afficher les tâches ouvertes**
- **Afficher toutes les tâches**
- **Tâches non affectées**.

Gérer Intelligence prédictive pour le hameçonnage signalé par les utilisateurs

La fonctionnalité Intelligence prédictive pour le hameçonnage signalé par les utilisateurs fournit une solution importante pour le triage et la hiérarchisation des e-mails d'hameçonnage signalés par les utilisateurs.

Cette section décrit les éléments suivants :

- Intelligence prédictive pour le hameçonnage signalé par les utilisateurs
- Composants et modules d'extension requis
- Génération d'un verdict final pour Hameçonnage signalé par un utilisateur
- Dépannage d'Intelligence prédictive pour le hameçonnage signalé par les utilisateurs

Intelligence prédictive pour le hameçonnage signalé par les utilisateurs

Cette fonctionnalité aide les analystes de sécurité à trier et à hiérarchiser les e-mails d'hameçonnage signalés par les utilisateurs.

Le cadre de travail Intelligence prédictive fournit des solutions pour former le système à prédire, recommander et organiser les résultats des données. Pour plus d'informations sur l'intelligence prédictive, reportez-vous à la section Intelligence prédictive . À l'aide de ce cadre de travail, vous pouvez créer des modèles pour prédire automatiquement si un e-mail d'hameçonnage signalé par un utilisateur est suspect ou légitime.

À l'aide des données historiques des incidents de sécurité liés au hameçonnage signalé par les utilisateurs (en-têtes des e-mails, corps des e-mails et résultats de triage capturés via les codes de fermeture des incidents de sécurité), les analystes de sécurité peuvent former le système à classer les soumissions de hameçonnage signalées par les utilisateurs entrants comme celles qui doivent être triées davantage (probablement suspectes) et celles qui sont des soumissions légitimes.

En triant automatiquement les e-mails entrants, les analystes de sécurité peuvent facilement hiérarchiser la file d'attente des incidents et se concentrer sur les incidents susceptibles de représenter un risque pour l'organisation avant tout et consacrer moins d'efforts aux e-mails qui sont très susceptibles d'être des faux positifs. Le résultat de prédiction fournit également un score de confiance sur la classification pour permettre une hiérarchisation granulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants et modules d'extension requis

Pour utiliser Intelligence prédictive pour User Reported Phishing, vous devez installer les applications suivantes

Nom du module d'extension	Version minimale
Security Incident Response	9.0.1 ou 10.0.2
Intelligence prédictive	Version Orlando
Intelligence prédictive pour le hameçonnage signalé par les utilisateurs	10.0.2

Remarque : Les nouvelles améliorations suivantes sont disponibles avec Réponse aux incidents de sécurité 10.4 :

- La possibilité de choisir des codes de fermeture dans les champs personnalisés pour la formation du modèle.
- Possibilité d'activer explicitement les prédictions après la création du modèle.
- Possibilité de générer un verdict final sur la soumission de hameçonnage signalé par un utilisateur à l'aide d'une table de décision. (nécessite Spoke Security Operations 10.3.0)

Pour utiliser les nouvelles améliorations, vous devez mettre à niveau les applications suivantes :

Nom du module d'extension	Effectuer une mise à niveau vers
Security Incident Response	10.0.4
Intelligence prédictive pour le hameçonnage signalé par les utilisateurs	10.3.1

Tables nouvelles et mises à jour

- sn_sir_ml_urp_config (nouveau) : contient la configuration de l'application ML URP.
- sn_sir_ml_urp_feature (nouveau) : enregistrements extraits de la table d'e-mail sn_si_phishing.
- sn_sir_ml_urp_feature_import (nouveau) : utilisé pour charger des données historiques d'e-mails d'hameçonnage.
- sn_si_incident (mise à jour) : Les nouveaux champs suivants ont été ajoutés :
  - Prédiction acceptée
  - Résultat de prédiction
  - Score de confiance
- **Includes de script**
  - URPMLUtil : récupère la configuration, exécute la tâche de prédiction et suit le processus de prédiction.
  - URPMLProcessor : extrait et traite les données de la table sn_si_phishing_email.
  - URPMLAction : exécute le flux pour accepter le résultat de prédiction.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Génération d'un verdict final pour Hameçonnage signalé par un utilisateur

Les équipes Security Incident Response peuvent désormais déterminer le verdict définitif d'un enregistrement d'hameçonnage signalé par un utilisateur en fonction des résultats des intégrations d'intelligence prédictive et d'enrichissement des menaces.

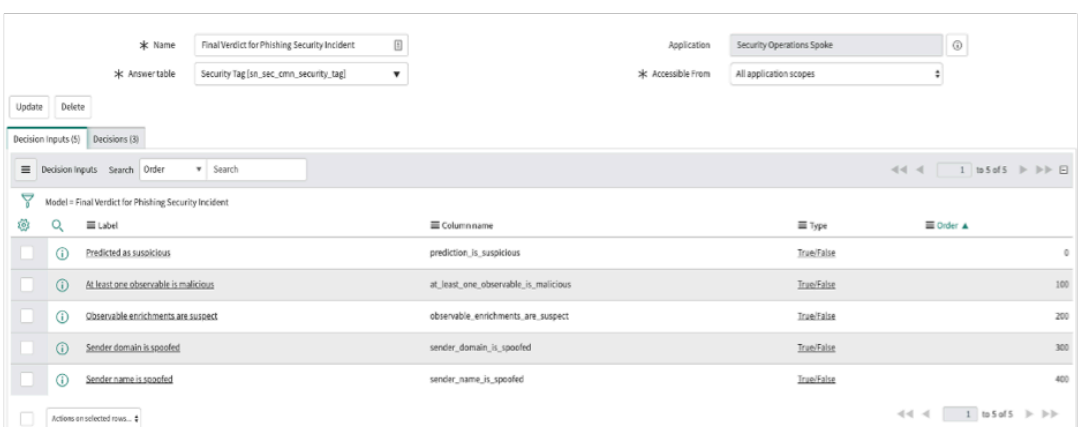
Cette génération de verdict final est activée par le biais d'une construction de table de décision et exploitée dans un flux.

Prérequis

Assurez-vous que tous les modules d'extension répertoriés dans Composants et modules d'extension requis ont été installés.

Accédez à la **Intelligence prédictive pour l'hameçonnage** > **Verdict final** > **Verdict final pour l'hameçonnage de l'incident de sécurité**.

L'onglet **Entrées de décision** affiche les différentes conditions qui ont été évaluées pour arriver au verdict final.



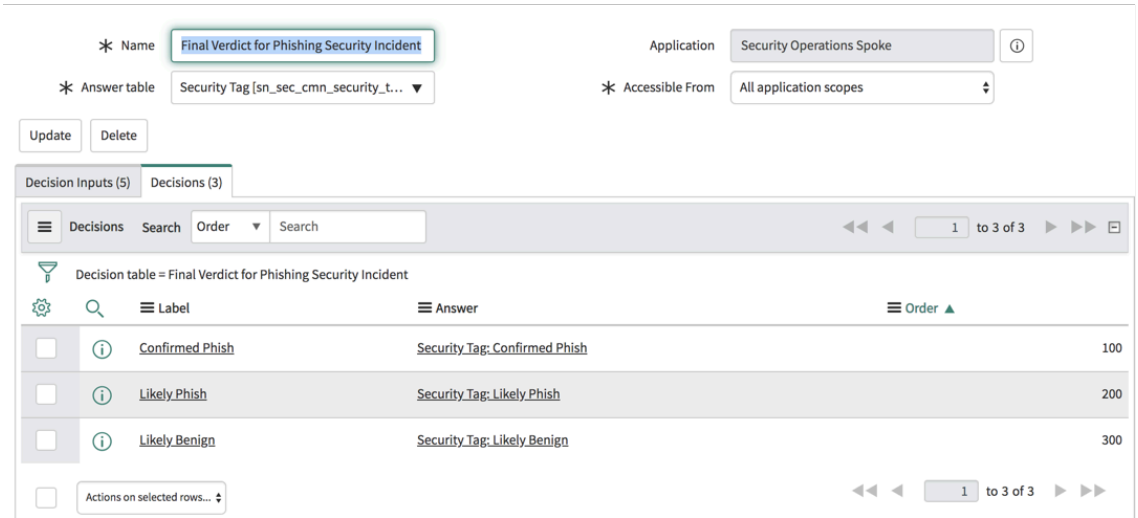
Les conditions suivantes sont disponibles avec le système de base :

- Prédit comme suspect : lorsque Predictive Intelligence a classifié l'e-mail d'hameçonnage signalé par l'utilisateur comme **suspect.**
- Au moins un observable est malveillant : lorsqu'un observable impliqué dans l'incident de sécurité (par exemple, URL, domaine, adresse IP, hachage) a été classé comme **malveillant** par les sources de renseignements sur les menaces.
- L'enrichissement des observables est suspect : lorsque l'enrichissement des observables (par exemple, récence de l'enregistrement du domaine d'hameçonnage, pays d'enregistrement du domaine d'hameçonnage) est considéré comme suspect.
- Le domaine de l'expéditeur est falsifié : lorsque le domaine de messagerie de l'hameçonneur est soupçonné d'usurper un domaine de confiance.
- Le nom de l'expéditeur est usurpé : lorsque l'adresse e-mail de l'hameçonneur est suspectée d'usurper l'identité d'un employé de confiance d'une organisation.

L'onglet **Décisions** affiche les options de verdict final qui peuvent être obtenues pour un incident de sécurité donné.

Traduction automatique

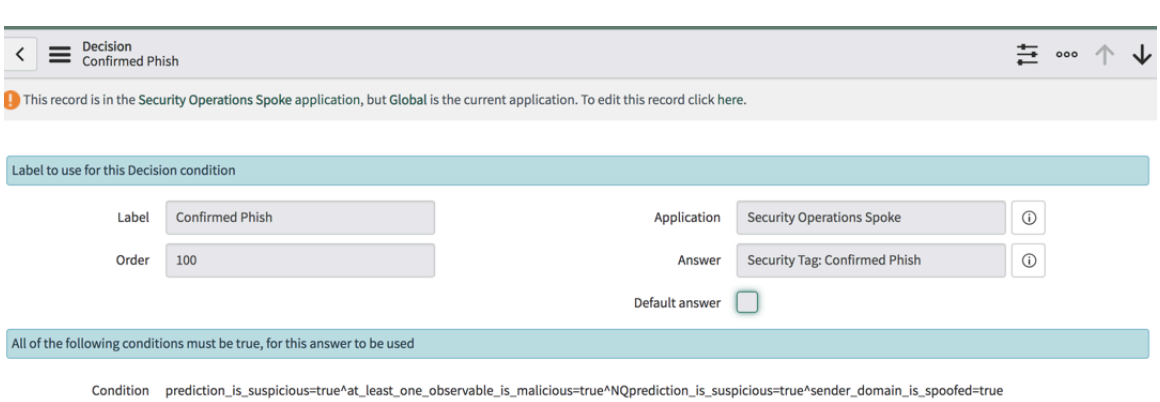
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les décisions suivantes sont disponibles avec le système de base :

- Hameçonnage confirmé : lorsque les conditions ont conduit au verdict final comme étant un e-mail de hameçonnage confirmé.
- Hameçonnage probable : lorsque les conditions ont conduit au verdict final en tant que tentative d'hameçonnage potentielle.
- Probablement bénin : Lorsque les conditions ont conduit au verdict final en tant que soumission bénigne.

Vous pouvez voir les conditions qui ont été évaluées pour chacune des options du verdict final. Cliquez sur le lien Étiquette pour voir les conditions.



Vous pouvez personnaliser la table de décision fournie avec le système de base ou créer votre propre table de décision. Cette table de décision peut être exploitée dans les playbooks Security Incident Response. Le flux secondaire **Générer un verdict final pour les incidents de sécurité d'hameçonnage** est disponible avec le système de base. Ce flux secondaire génère automatiquement le verdict final d'un incident de sécurité de hameçonnage et applique une balise de sécurité en fonction de cette décision. Vous pouvez inclure ce flux secondaire dans le cadre du playbook **d'hameçonnage automatisé** .

Les entrées de ce flux secondaire sont les suivantes :

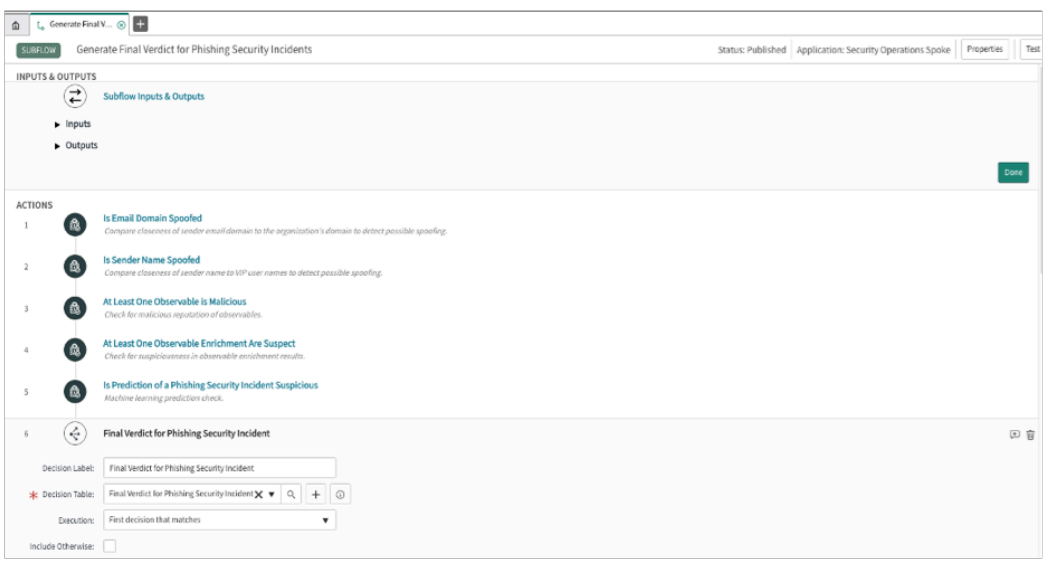
- incident_id : ID système de l'incident de sécurité de hameçonnage.
- c_level_names : liste séparée par des virgules de noms (par exemple, les noms des cadres de l'organisation) probablement usurpée dans l'attaque de phishing.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- trusted_domains : liste des domaines d'e-mail de confiance séparés par des virgules.
- enrichment_keywords : liste de mots clés séparés par des virgules qui indiquent le caractère malveillant de l'observable à partir des résultats d'enrichissement.
- sender_email (facultatif) : l'adresse e-mail de l'expéditeur de l'e-mail d'hameçonnage.

La sortie de ce flux peut être **Hameçonnage confirmé**, **Hameçonnage probable** ou **Probablement bénin.**



Dépannage d'Intelligence prédictive pour le hameçonnage signalé par les utilisateurs

Cette section couvre quelques scénarios de problèmes courants.

- Problème : je ne peux pas modifier la configuration d'Intelligence prédictive.

  Solution : vérifiez si vous avez les autorisations nécessaires. Vous devez vous connecter en tant qu'utilisateur avec le rôle ml_admin pour modifier les seuils. Certains scénarios peuvent exiger des privilèges encore plus élevés, comme, par exemple, vous devez modifier la limite des données de formation. Dans de tels scénarios, vous devez contacter le service clientèle pour obtenir de l'aide.

- Problème : échec de la formation du modèle.

  Solution : vérifiez si les URL du planificateur ML ont été configurées. Accédez à la **Propriétés système** > **Toutes les propriétés** et vérifiez si la propriété `glide.shared_service_scheduler.url` a été configurée.

- Problème : les résultats de prédiction ne sont pas disponibles pour un incident de sécurité.

  Solution:

  - Vérifiez si l'URL de prévision a été configurée dans la propriété système `glide.prediction_service.url` et assurez-vous que le centre de données correspond à l'URL.
  - Vérifiez si la tâche planifiée Prédire l'e-mail d'hameçonnage signalé par l'utilisateur est active.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Intelligence prédictive pour le hameçonnage signalé par les utilisateurs

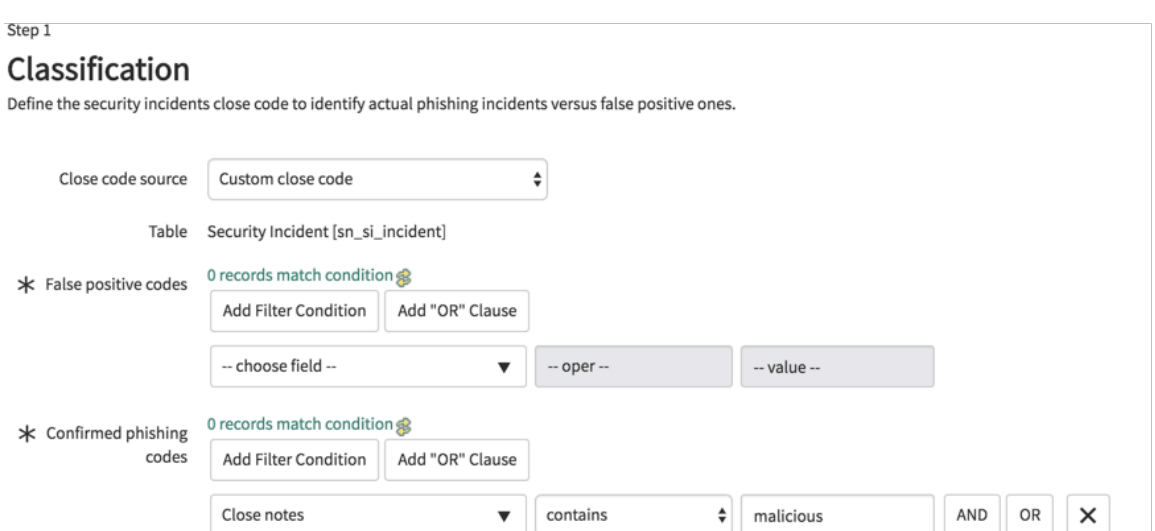
Configurez et préparez le modèle pour identifier les e-mails d'hameçonnage signalés par l'utilisateur.

Avant de commencer

Rôle requis : ml_admin

Procédure

1. Accédez à la **Tous** > **Intelligence prédictive pour l'hameçonnage** > **Configuration**.
2. À l'étape 1 de la configuration, sélectionnez l'une des options suivantes dans la liste Source du code de fermeture :
   - Code de fermeture par défaut : sélectionnez cette option pour spécifier les codes de fermeture des incidents de sécurité par défaut qui doivent être utilisés par le modèle de formation pour identifier les e-mails malveillants et les e-mails légitimes. Cliquez sur l'icône de verrou et sélectionnez un ou plusieurs codes de faux positif ou codes de hameçonnage confirmés.
   - Code de fermeture personnalisé : sélectionnez l'option Code de fermeture personnalisé si vous souhaitez définir des codes de fermeture à partir de champs personnalisés qui peuvent être utilisés dans le cadre de vos procédures de réponse aux incidents existantes. Pour définir un code de fermeture, sélectionnez un champ dans la table d'incidents de sécurité et spécifiez une ou plusieurs conditions de filtre.



3. À l'étape 2, importez des données historiques qui peuvent être utilisées pour former le modèle. Sélectionnez la source de données pour importer les données historiques. Cela peut être :
   - Tableau des e-mails de hameçonnage signalés par un utilisateur : Vous pouvez afficher le nombre d'enregistrements qui peuvent être importés en tant que données historiques. Sélectionnez cette option et cliquez sur **Importer**.
   - Source de données personnalisée : vous pouvez joindre un seul fichier CSV formaté contenant des enregistrements de données historiques. Sélectionnez le fichier et cliquez sur **Importer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le fichier CSV que vous importez doit contenir les en-têtes suivants :

- Étiquette
- En-tête
- Corps de texte

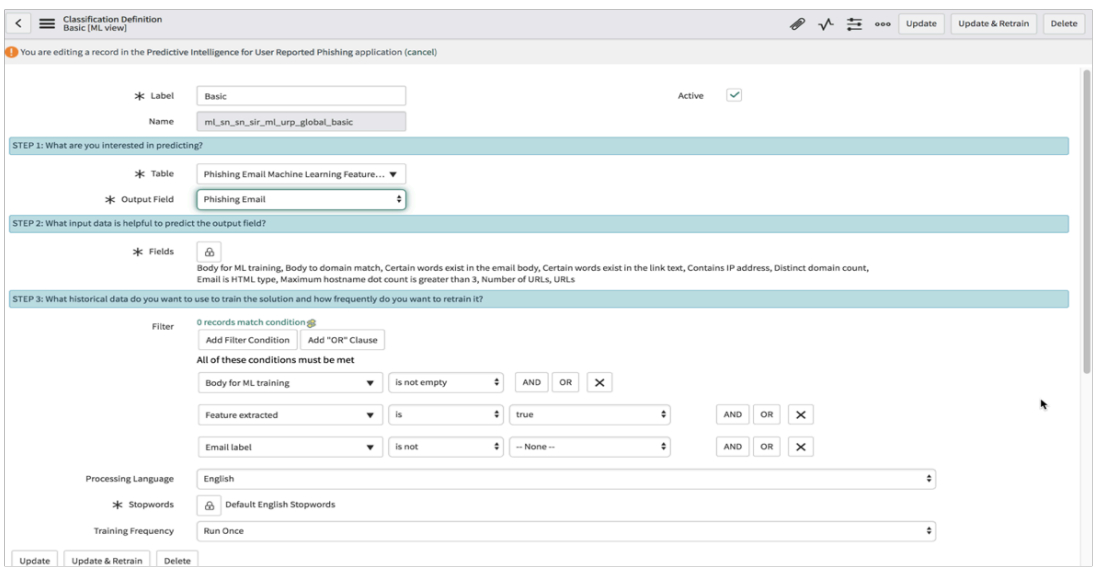
Chaque enregistrement doit contenir une balise malveillante ou légitime dans la colonne Étiquette du fichier CSV.

Cliquez sur **Annuler l'importation** pour arrêter l'importation des données. Le processus d'importation est annulé et tous les enregistrements qui ont été importés jusqu'à présent sont supprimés.

4. Une fois que vous avez importé les données historiques, cliquez sur le lien pour actualiser la page. Vous pouvez ensuite importer plus de données de formation ou passer à l'étape suivante.
5. À l'étape 3, vérifiez si le nombre d'enregistrements disponibles pour la formation répond aux exigences de seuil minimal.

Remarque : Les valeurs par défaut pour le nombre maximal et minimal d'enregistrements de formation s'affichent. Ces seuils peuvent être modifiés dans la page Propriétés d'apprentissage machine de la plateforme . Contactez le support client pour obtenir de l'aide.

6. Si les données de formation sont suffisantes, cliquez sur **Entraîner le modèle**. Vous pouvez mettre à jour les entrées de formation dans l'écran ci-dessous.



7. Les entrées de prédiction que vous pouvez modifier sont les suivantes :
   - Que souhaitez-vous prédire ?
   - Quelles données d'entrée permettent de prédire le champ de sortie ?
   - Quelles données historiques souhaitez-vous utiliser pour former la solution et à quelle fréquence souhaitez-vous la reformer ?

   Les valeurs par défaut de ces entrées s'affichent. Vous pouvez les modifier et cliquer sur l'un des éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Mettre à jour** : met à jour la définition du modèle de formation.
- **Mettre à jour et former** : met à jour la définition du modèle de formation et reforme le modèle (déclenche la fonction **Former le modèle**).

8. Enfin, une fois la formation du modèle terminée, cochez la case **Activer la prédiction** . Des prédictions sont désormais fournies sur chaque enregistrement de phishing signalé par un utilisateur à l'aide de ce modèle. Si vous souhaitez cesser de fournir des prédictions sur les enregistrements d'hameçonnage signalés par l'utilisateur, désactivez la case **à cocher Activer la prédiction** et cliquez sur **Désactiver**.

Affectation d'analystes de la sécurité

En fonction des paramètres définis dans l'écran Configuration de l'administration SIR , vous pouvez affecter des analystes de sécurité aux incidents de sécurité manuellement, automatiquement à l'aide d'un workflow ou automatiquement à l'aide de l'affectation automatique.

Affectation manuelle d'analyste

Vous pouvez configurer l'écran de configuration de l'administration Réponse aux incidents de sécurité pour exiger que les analystes de sécurité soient affectés manuellement chaque fois que quelqu'un ou l'application SIR crée un incident de sécurité ou génère une tâche de réponse de sécurité.

Si un incident de sécurité ou une tâche de réponse ne peut pas être affecté automatiquement, vous pouvez configurer l'écran de configuration de l'administration SIR pour exiger l'affectation manuelle d'analystes de sécurité. C'est un bon choix si vous avez un nombre limité d'analystes de sécurité pour traiter les demandes ou si vous ne souhaitez tout simplement pas les affecter automatiquement.

Affectation d'analyste de la sécurité basée sur les workflows

Vous pouvez configurer l'écran Configuration de l'administration Réponse aux incidents de sécurité afin d'utiliser un workflow sélectionné afin d'affecter l'analyste de sécurité chaque fois que quelqu'un ou l'application SIR crée un incident de sécurité ou une tâche de réponse de sécurité.

Dans l'écran de configuration d'Administration des incidents de sécurité, vous pouvez choisir d'utiliser un workflow pour affecter un analyste à chaque incident de sécurité ou tâche de réponse de sécurité. Cette option est un bon choix pour les organisations qui utilisent un processus personnalisé pour résoudre les problèmes de sécurité ou qui disposent d'un processus qui peut être automatisé.

Affectation automatique d'un analyste de sécurité

Vous pouvez configurer l'écran Configuration de l'administration Réponse aux incidents de sécurité pour affecter automatiquement l'analyste de sécurité chaque fois que quelqu'un ou l'application SIR crée un incident de sécurité ou une tâche de réponse de sécurité. L'affectation automatique vous permet de définir, en fonction des besoins de votre organisation, les critères selon lesquels les analystes sont affectés automatiquement aux incidents de sécurité.

Affectation automatique d'agent basée sur les évaluations d'agents

Si l'affectation automatique est activée et qu'un incident de sécurité ou une tâche de réponse est créé, les actions suivantes se produisent :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les analystes de sécurité disponibles sont évalués en fonction des critères définis dans la configuration.
- Un analyste de la sécurité approprié est automatiquement affecté à la tâche.
- La tâche passe à l'état **Affecté**.

Si la configuration est configurée pour prendre en compte plus d'un ensemble de conditions, telles que les compétences, l'emplacement, le fuseau horaire ou la zone de couverture du groupe, les analystes de sécurité sont évalués en fonction des paramètres de propriété de pondération et d'autres critères. Ces paramètres de configuration vous permettent d'affecter automatiquement des agents en fonction de propriétés facultatives. Les évaluations calculées sont utilisées pour déterminer le meilleur agent pour l'incident de sécurité ou la tâche de réponse. Toute combinaison de méthodes basées sur l'évaluation peut être activée dans l'écran de configuration de l'application.

Lorsqu'une tâche est créée, une note pour chaque type de critères de sélection activé est calculée pour chaque agent disponible. L'agent dont l'évaluation totale est la plus élevée est pris en compte pour l'affectation automatique.

Les paramètres des propriétés de pondération de l'affectation automatique, que l'on trouve dans **Incident de sécurité** > **Administration** > **Propriétés**, sont inclus dans les calculs de cote.

Ces valeurs vous aident à classer par ordre de priorité les critères de sélection des affectations automatiques qui sont les plus importants pour votre organisation. Définissez les valeurs de priorité entre 1 (moins important) et 10 (important).

Pour un exemple de la façon dont les propriétés de pondération affectent les notes des agents, consultez Affectation automatique d'agent à l'aide de critères de sélection multiples.

On-Call Scheduling

L'application Planification d'astreinte vous permet de vous assurer que les membres de l'équipe de support dédiée sont disponibles pour résoudre les problèmes à mesure qu'ils se produisent. Vous pouvez configurer des calendriers d'astreinte, des rotations de liste et des politiques d'escalade, escalader des notifications pour un groupe et déterminer le contact actuel pour une escalade. L'application identifie le membre affecté et disponible d'un groupe de support, par exemple, lors de l'affectation d'un incident. Consultez Planification d'astreinte pour plus d'informations. La planification d'astreinte pour Réponse aux incidents de sécurité fonctionne de la même manière.

Affectation automatique d'agent à l'aide de l'emplacement

Les agents peuvent être affectés automatiquement en fonction de leur emplacement d'accueil dans leur enregistrement utilisateur et de l'emplacement des tâches.

L'affectation automatique par emplacement est effectuée lorsque l'option **de configuration Sélection automatique d'agents tient compte de l'emplacement des agents** est activée.

Lorsqu'une tâche (incident de sécurité ou tâche de réponse) est créée, l'agent le plus proche de l'emplacement de la tâche est pris en compte pour la tâche. Si l'application est configurée de telle sorte que seul l'emplacement est pris en compte, l'agent le plus proche est automatiquement affecté à la tâche.

Lorsqu'une tâche est créée, les emplacements des agents sont comparés aux plages suivantes pour déterminer l'évaluation de chaque emplacement d'agent.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calcul de la note d'emplacement

Distance (miles) entre l'agent et la tâche	Évaluation
0 à 0,1	1
0,11 à 0,5	0,9
0,51 à 5	0,7
5,1 à 10	0,5
10,1 à 20	0,4
20,1 à 30	0,3
30,1 à 40	0,2
40,1 à 100	0.1
>100	0

Si l'application est configurée pour utiliser d'autres critères de sélection, tels que les compétences, le fuseau horaire ou le calendrier, les évaluations de tous les critères de sélection sont pondérées et additionnées. L'agent ayant l'évaluation globale la plus élevée est automatiquement affecté à la tâche. Consultez Affectation automatique d'agent à l'aide de critères de sélection multiples pour en savoir plus.

Affectation automatique des agents à l'aide des compétences

Les agents peuvent être affectés automatiquement en fonction de leurs compétences et des compétences requises pour effectuer la tâche. Affecter des compétences à leurs enregistrements utilisateur à l'aide de **Compétences** > **Utilisateurs**.

L'affectation automatique par compétences peut être effectuée lorsque **l'option Sélection automatique d'agents pour des tâches qui requièrent qu'ils disposent de compétences** est définie sur **tout ou certaines**.

Lorsqu'une tâche comprenant des compétences est affectée automatiquement, les compétences d'un agent sont comparées aux compétences requises pour effectuer la tâche. Une évaluation est calculée en fonction de l'option de configuration des compétences. Si l'option est définie sur **Certaines**, la tâche est automatiquement affectée à l'agent dont les compétences sont les plus proches. Si l'option est définie sur **Toutes**, seuls les agents qui possèdent toutes les compétences requises sont pris en compte. Si aucun agent ne possède toutes les compétences requises pour effectuer la tâche, aucun agent n'est affecté automatiquement.

Comment se calcule-t-on une évaluation des compétences ?

Skills_agent/Skills_task

Où :

- Skills_agent est le nombre de compétences de l'agent qui correspondent aux compétences requises pour la tâche.
- Skills_task est le nombre total de compétences requises pour la tâche.

Par exemple, une tâche exige quatre compétences, l'agent A possède trois d'entre elles et l'agent B en possède deux :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Évaluation des compétences de l'agent A = 3/4 ou 0,75
- Cote de compétence de l'agent B = 2/4 ou 0,5

Si l'application est configurée de manière à utiliser d'autres critères de sélection, tels que l'emplacement ou le fuseau horaire, les notes de tous les critères de sélection sont pondérées et additionnées. L'agent ayant la note globale la plus élevée est sélectionné pour la tâche. Consultez Affectation automatique d'agent à l'aide de critères de sélection multiples pour en savoir plus.

Affectation automatique des agents à l'aide des fuseaux horaires

Les agents peuvent être affectés automatiquement en fonction du fuseau horaire défini dans leurs enregistrements utilisateur et du fuseau horaire des tâches.

Si l'option **Sélection automatique des agents tiendra compte du fuseau horaire pour l'option de configuration de la tâche** est activée, l'affectation automatique par fuseau horaire peut être effectuée.

Lorsqu'une tâche est créée, les agents situés dans le fuseau horaire le plus proche du fuseau horaire de la tâche sont pris en compte pour la tâche. Si l'application est configurée de telle sorte que seul le fuseau horaire est pris en compte, seul un agent se trouvant dans le même fuseau horaire peut être affecté automatiquement à la tâche.

Remarque : Il est important que les fuseaux horaires de l'agent et de la tâche soient correctement définis.

Lorsqu'une tâche est créée, les agents sont évalués en fonction du fuseau horaire de la tâche et du fuseau horaire de l'agent à l'aide de la formule suivante :

1 - [abs(Task_tz – Agent_tz) ÷ 12]

où :

- abs est la fonction mathématique de calcul de la valeur absolue.
- Task_tz est le décalage entre le fuseau horaire de la tâche et le fuseau GMT.
- Agent_tz le décalage entre le fuseau horaire de l'agent et le fuseau GMT.

Par exemple, une tâche est créée à New York (GMT-4) et deux agents sont disponibles pour effectuer la tâche, l'un à Los Angeles (GMT-7) et l'autre à Paris (GMT+1).

La note de l'agent à Los Angeles est calculée comme suit :

1 - abs((-4) - (-7)) ÷ 12 ou 0,75

La note de l'agent à Paris est calculée comme suit :

1 - abs((-4) - (+1)) ÷ 12 ou 0,58

Ainsi, si l'affectation automatique de la tâche est basée uniquement sur le fuseau horaire, elle est affectée à l'agent de Los Angeles.

Si l'application est configurée pour utiliser d'autres critères de sélection, tels que les compétences ou l'emplacement, les évaluations de tous les critères de sélection sont pondérées et additionnées. L'agent ayant la note globale la plus élevée est sélectionné pour la tâche. Consultez Affectation automatique d'agent à l'aide de critères de sélection multiples pour en savoir plus.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affectation automatique d'agents à l'aide des zones de couverture de groupe

Les agents peuvent être affectés automatiquement en fonction de la zone de couverture du groupe définie dans leurs enregistrements utilisateur.

Affectation automatique d'agent à l'aide de critères de sélection multiples

Lorsqu'une tâche est créée, les évaluations des agents sont calculées. Pour en savoir plus, consultez :

- Affectation automatique d'agent à l'aide de l'emplacement
- Affectation automatique des agents à l'aide des compétences
- Affectation automatique des agents à l'aide des fuseaux horaires

L'affectation automatique est basée sur le calcul suivant :

(cote Criteria_1 x poids Criteria_1) + (cote Criteria_2 x poids Criteria_2) + (cote Criteria_3 x poids Criteria_3) / Nombre de types de critères utilisés où :

Nombre de types de critères utilisés = 1, 2 ou 3 selon les paramètres d'emplacement, de compétence et de fuseau horaire utilisés.

Cet exemple calcule l'affectation automatique de l'agent en fonction de l'emplacement et des compétences. L'exemple est basé sur les hypothèses suivantes.

- L'option de configuration **La sélection automatique d'agents tiendra compte de leur localisation** est activée pour l'application.
- L'option de configuration **La sélection automatique d'agents pour des tâches requiert qu'ils aient des compétences** est activée pour l'application.
- La propriété **Poids des compétences** est définie sur 10 pour l'application.
- La propriété **Poids de l'emplacement** est définie sur 5 pour l'application.
- Les agents A et B sont disponibles pour effectuer une tâche qui nécessite quatre compétences spécifiques.
- Agent Un emplacement se trouve à 5 miles du site de la tâche et possède trois des quatre compétences requises.
- L'emplacement de l'agent B est à un quart de mile du site et possède deux des compétences requises.

L'affectation automatique des agents utilise le calcul suivant : [(Évaluation de l'emplacement x Poids de l'emplacement) + (Évaluation des compétences x Poids des compétences)]/ 2

- Le calcul de l'affectation automatique pour l'agent A est le suivant : [(0,7 x 0,5) + (0,75 x 1)]/ 2 = 0,55
- Le calcul de l'affectation automatique pour l'agent B est le suivant : [(0,9 x 0,5) + (0,5 x 1)]/ 2 = 0,475

Dans cet exemple, la tâche est automatiquement affectée à l'agent A.

Espace de travail d'exploration de processus pour Réponse aux incidents de sécurité

Exploration de processus parcourt les journaux d'audit des incidents de sécurité et identifie les facteurs contribuant à l'inefficacité, tels que les réaffectations multiples, les

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

temps d’attente prolongés et les périodes d’inactivité pour les incidents de sécurité. Les organisations peuvent utiliser ces informations pour remédier aux inefficacités.

Grâce à l’exploration de processus, vous pouvez identifier les opportunités d’amélioration suivantes pour vos incidents de sécurité.

Opportunités avec l’exploration de processus

Opportunité	Description
Incidents avec au moins deux changements de groupe d'affectation	Incidents pour lesquels le groupe d’affectation a changé deux fois ou plus.
SIRT (le nombre maximal de répétitions est de 2)	
Les incidents ont mis plus de 5 heures pour passer à une priorité élevée	Incidents pour lesquels la priorité a été transmise à une priorité supérieure après cinq heures.
L'analyse des incidents a pris plus de 5 heures	Incidents qui étaient dans l’état Analyse depuis plus de cinq heures.
Incidents analysés dans les 30 minutes	Incidents qui ont été dans l’état d’analyse pendant moins de 30 minutes.
Révision (le nombre maximal de répétitions est de 2)	Incidents qui ont été passés à l’état Examen deux fois.
Éradiquer (le nombre maximal de répétitions est de 2)	Incidents qui ont été déplacés vers l’état Éradiquer deux fois.

Le pack Réponse aux incidents de sécurité de contenu pour l’exploration de processus ajoute un projet préconstruit qui inclut une définition de modèle de processus prédéfinie pour les incidents de sécurité. Pour créer un projet, reportez-vous à la section Créer un projet d’exploration de processus pour les incidents de sécurité.

Remarque : Pour utiliser l’exploration de processus dans Réponse aux incidents de sécurité, téléchargez et installez le pack de contenu. Pour plus d'informations, consultez Pack de contenu pour Réponse aux incidents de sécurité .

Créer un projet d’exploration de processus pour les incidents de sécurité

Créez un projet dans l’espace de travail Exploration de processus à l’aide des définitions de modèles de processus prédéfinies du pack de contenu pour parcourir les journaux d’audit des enregistrements d’incidents de sécurité et identifier les inefficacités dans le cycle de vie de votre incident de sécurité.

Avant de commencer

Rôle requis : sn_process_optimization_analyst et sn_si_read

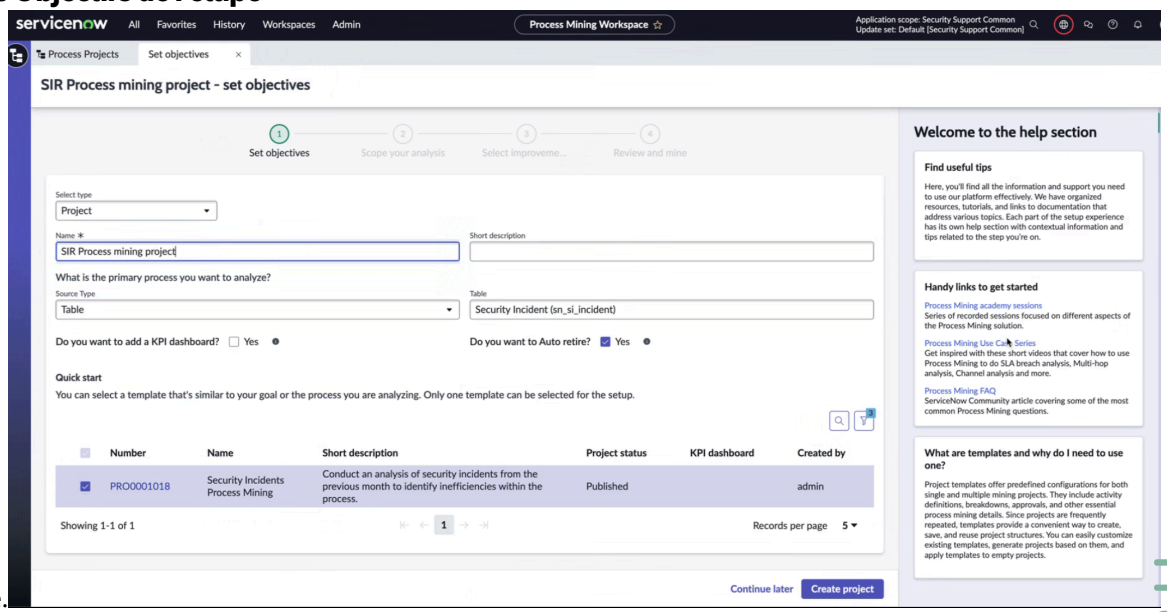
Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail d'exploration de processus**.
2. Sélectionnez **Créer un projet**.

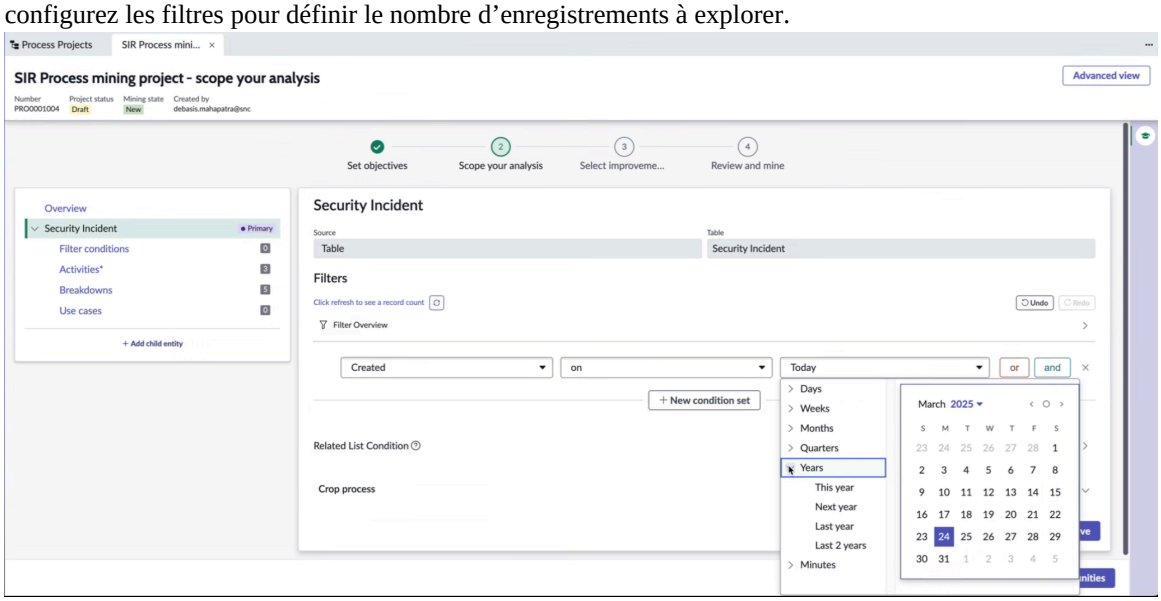
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La page **Objectifs de l'étape** s'ouvre.



3. Entrez un nom de projet d'exploration de processus dans **Nom**.
4. **Facultatif :** Ajoutez une brève description de votre projet dans **Brève description**.
5. Sélectionnez **le type de source** comme table.
6. Sélectionnez l'incident de sécurité (sn_si_incident) dans la **table**.
7. Sélectionnez le modèle par défaut, puis sélectionnez **Créer un projet**.
   Le tableau de bord du projet s'affiche avec tous les paramètres configurés.
8. Sélectionnez l'icône Modifier (icône) correspondant au **champ d'application de l'analyse** et configurez les filtres pour définir le nombre d'enregistrements à explorer.



9. Sélectionnez **Sélectionner des opportunités d'amélioration** et configurez les améliorations pour vos incidents de sécurité.
   Une liste des opportunités d'amélioration s'affiche. Pour plus d'informations sur la configuration des opportunités d'amélioration, reportez-vous à la section Utilisation des opportunités d'amélioration .
10. Sélectionnez **Examiner et explorer** , puis sélectionnez **Explorer le projet**.
11. Sélectionnez **Exemple d'exploration** ou **Exploration complète**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

12. Sélectionnez **Confirmer et explorer** pour démarrer l'exploration.
    L'exploration démarre et l'état de l'exploration s'affiche.

Cas d'utilisation de l'exploration de processus pour les incidents de sécurité

Les cas d'utilisation d'Exploration de processus suivants fournissent diverses méthodes d'analyse que vous pouvez utiliser pour identifier les inefficacités lors de la résolution de vos incidents de sécurité.

Analyse à sauts multiples

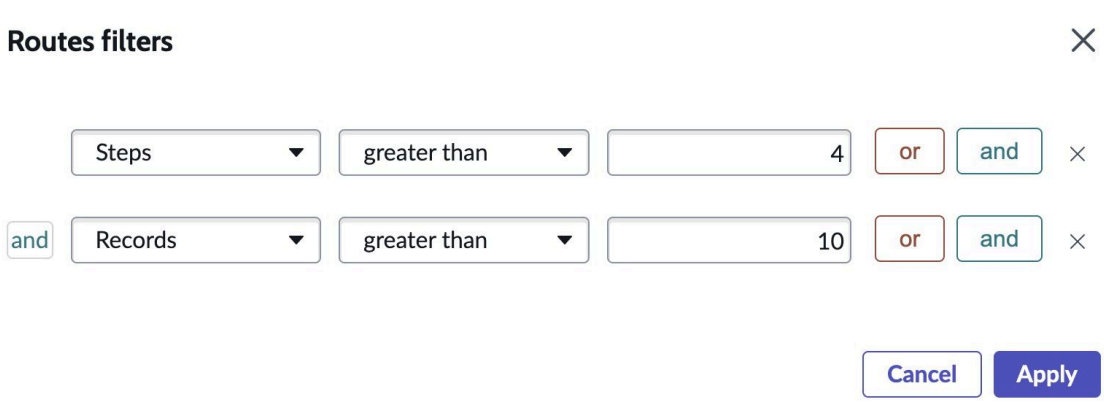
Les incidents de sécurité qui sont réaffectés plusieurs fois à différentes équipes peuvent entraîner un délai de résolution. En analysant les raisons des réaffectations pour ces incidents de sécurité et les endroits où les incidents sont bloqués pendant des durées plus longues, vous pouvez améliorer l'efficacité globale.

Voici des exemples d'étapes pour obtenir la liste des incidents de sécurité qui ont emprunté les itinéraires les plus longs :

1. Accédez à la **Espaces de travail** > **Espace de travail d'exploration de processus**.
2. **Sélectionnez un groupe d'affectation**.
3. Ouvrez un projet et accédez à **la console d'analyste**.

   Lorsque vous ouvrez un projet d'optimisation de processus exploré, la console d'analyste s'ouvre par défaut.
4. **Sélectionnez Analyse de la variation**.
5. Sélectionnez l'icône de filtre (icône) et définissez un filtre similaire à ce qui suit :
   - Étapes supérieures au nombre moyen d'étapes.
   - Enregistrements supérieurs au nombre minimal d'enregistrements qui ont emprunté un itinéraire plus long.

   Remarque : Vous pouvez configurer les valeurs selon vos besoins.



6. Sélectionnez **Appliquer**.

   Tous les enregistrements qui correspondent aux critères de filtre s'affichent. Sélectionnez un enregistrement pour afficher l'itinéraire de fermeture de l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Sélectionnez un enregistrement, puis sélectionnez **Afficher l'itinéraire**.

   L'itinéraire parcouru par l'enregistrement apparaît. Vous pouvez utiliser cet itinéraire pour identifier l'étape à laquelle les incidents ont été bloqués pendant une durée plus longue que prévu.

Analyse des violations de SLA

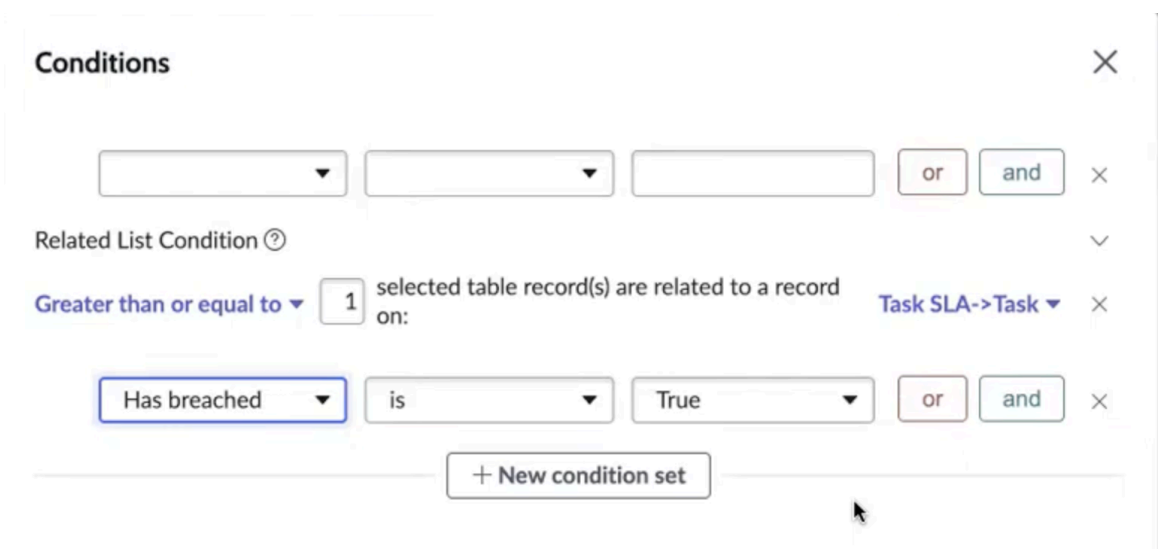
Vous pouvez utiliser l'exploration de processus pour analyser les incidents de sécurité qui ont violé un certain SLA (accord sur les niveaux de service).

Voici des exemples d'étapes pour obtenir la liste des incidents de sécurité qui ont violé le SLA :

1. Accédez à la **Espaces de travail** > **Espace de travail d'exploration de processus**.
2. Ouvrez un projet et accédez à **la console d'analyste**.

   Lorsque vous ouvrez un projet d'optimisation de processus exploré, la console d'analyste s'ouvre par défaut.

3. Dans les filtres Avancés, sélectionnez **Conditions**.
4. Sélectionnez la flèche correspondant à la **condition de liste connexe**.
5. Définissez les conditions de la même manière que :
   - Utilisez la liste **Sélectionner** pour sélectionner la table de SLA de tâche .
   - Définissez la valeur du champ **Supérieur ou égal à**sur 1.
   - Définissez la valeur de **Non respecté** sur **Vrai**.
   - Pour identifier les incidents de sécurité qui ont violé un SLA spécifique, définissez un filtre **de définition de SLA** .



6. Sélectionnez **Appliquer**.

   Tous les enregistrements qui correspondent aux conditions s'affichent. Sélectionnez un enregistrement pour afficher l'itinéraire de l'enregistrement pour analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Analyse des priorités

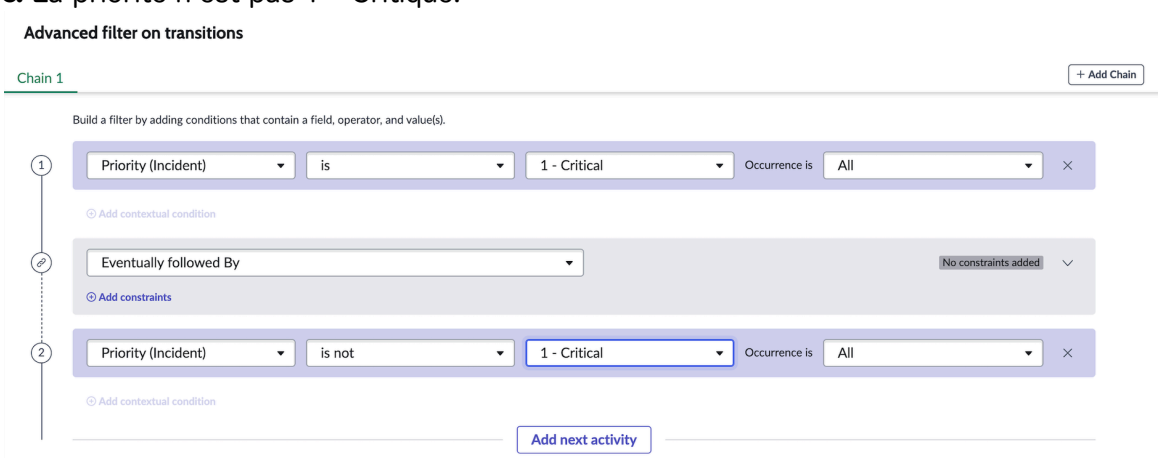
Vous pouvez utiliser l'exploration de processus pour examiner et améliorer le processus existant d'affectation des priorités à vos incidents de sécurité.

Voici des exemples d'étapes pour obtenir la liste des incidents de sécurité pour lesquels la priorité a été modifiée :

1. Accédez à la **Espaces de travail** > **Espace de travail d'exploration de processus**.
2. Ouvrez un projet et accédez à **la console d'analyste**.

   Lorsque vous ouvrez un projet d'optimisation de processus exploré, la console d'analyste s'ouvre par défaut.

3. Sélectionnez **Priorité**.
4. Dans les filtres Avancés, sélectionnez **Transitions**.
5. Dans le **filtre avancé sur les transitions**, configurez les éléments suivants :
   a. Définir la priorité est 1 : critique.
   b. **Sélectionner éventuellement suivi par**
   c. La priorité n'est pas 1 - Critique.



6. Sélectionnez **Appliquer toutes les chaînes**.

   La carte affiche tous les incidents de sécurité auxquels une priorité 1 a été affectée et dont la priorité a été abaissée par la suite.

Analyse du goulet d'étranglement

Vous pouvez utiliser l'exploration de processus pour examiner les transitions d'états de vos incidents de sécurité. Cette analyse identifie les transitions qui ne sont pas habituelles et le retard qui en résulte.

Voici des exemples d'étapes pour effectuer l'analyse du goulet d'étranglement :

1. Accédez à la **Espaces de travail** > **Espace de travail d'exploration de processus**.
2. Ouvrez un projet et accédez à **la console d'analyste**.

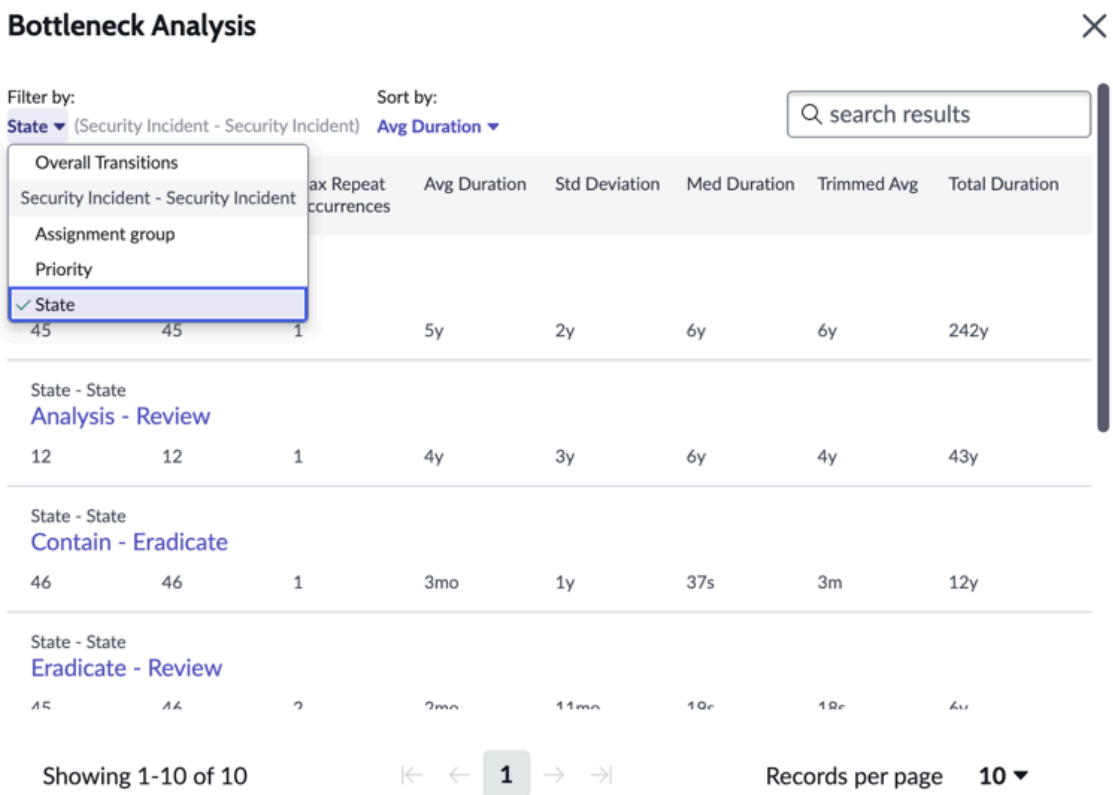
   Lorsque vous ouvrez un projet d'optimisation de processus exploré, la console d'analyste s'ouvre par défaut.

3. Sélectionnez **Analyse du goulet d'étranglement** dans les **options du modèle**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'écran affiche les transitions d'états pour les incidents de sécurité.



4. Sélectionnez **Filtrer par** pour identifier les transitions de goulet d'étranglement. Vous pouvez également utiliser la barre de recherche pour rechercher les transitions de goulet d'étranglement. Par exemple, pour identifier les incidents qui ont été déplacés vers d'autres états à partir de l'état Fermé, utilisez « Fermé » ou « Fermé - ».

Délai de démarrage long avant la résolution

Vous pouvez utiliser l'exploration de processus pour examiner les incidents qui mettent beaucoup de temps à atteindre l'état Brouillon, mais qui ont ensuite été fermés dans un délai relativement court.

Voici des exemples d'étapes pour identifier les incidents de sécurité qui étaient à l'état Brouillon pendant plus de deux jours et qui ont été fermés dans les 30 minutes suivant leur passage à l'état Analyse :

1. Accédez à la **Espaces de travail** > **Espace de travail d'exploration de processus**.
2. Ouvrez un projet et accédez à **la console d'analyste**.

   Lorsque vous ouvrez un projet d'optimisation de processus exploré, la console d'analyste s'ouvre par défaut.
3. Dans les filtres Avancés, sélectionnez **Transitions**.
4. Dans le **filtre avancé sur les transitions**, configurez les éléments suivants :
   a. Définir l'état (incident) est défini sur Brouillon.
   b. **Sélectionner éventuellement suivi par**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Sélectionnez **Ajouter des contraintes** et définissez **De sur**2 jours.

d. Sélectionnez **Ajouter une prochaine activité**.

e. Définir l'état (incident) est en cours d'analyse.

f. Sélectionner éventuellement suivi par

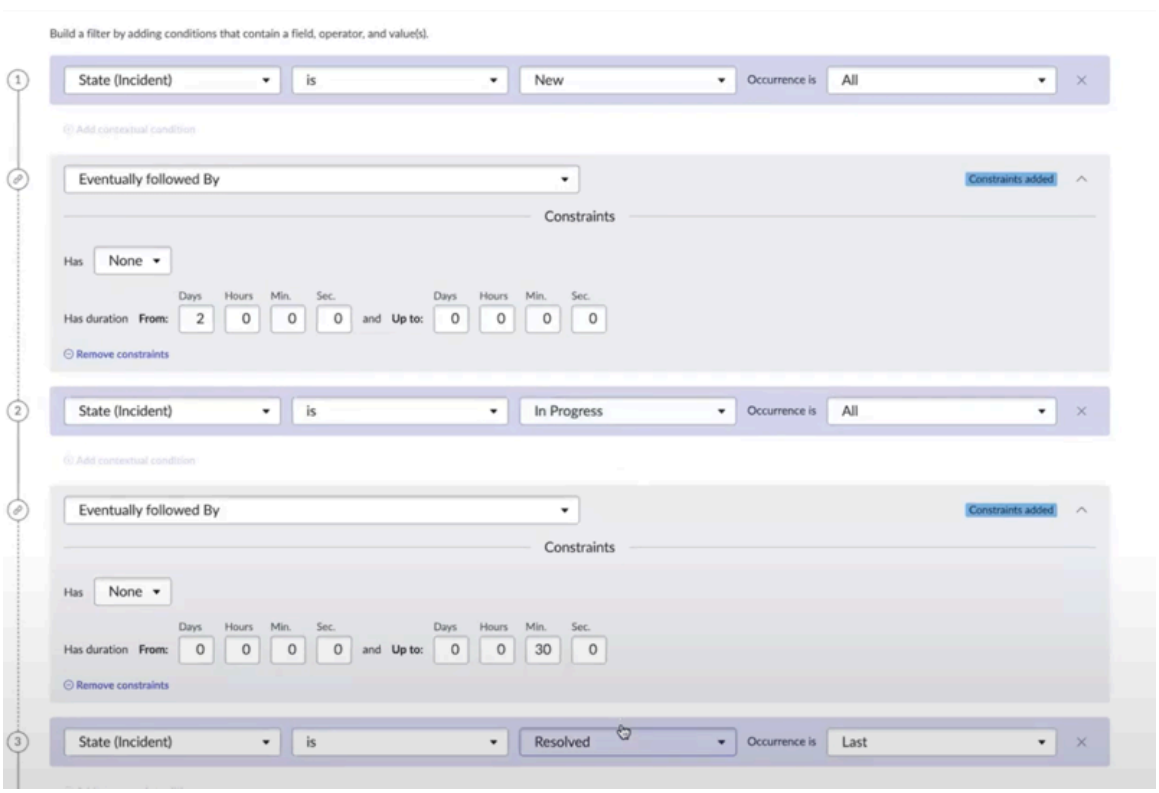
g. Sélectionnez **Ajouter des contraintes** et définissez **Jusqu'à**30 minutes.

h. Sélectionnez **Ajouter une prochaine activité**.

i. Sélectionner éventuellement suivi par

j. Sélectionnez **Ajouter des contraintes** et définissez **Jusqu'à** 30 minutes.

k. Définir l'état (incident) sur Fermé.



5. Sélectionnez **Appliquer toutes les chaînes**.

6. Sélectionnez des filtres de répartition et triez par **durée moyenne la plus longue**.

Gestion des incidents de sécurité et des demandes entrantes

Après la création d'un incident de sécurité, il existe de nombreux types d'informations qui peuvent être ajoutées et consultées au fur et à mesure que votre analyse du problème progresse vers la résolution.

Important : Les dernières fonctionnalités de sont Réponse aux incidents de sécurité exclusivement disponibles dans le Espace de travail de la Réponse aux incidents de sécurité. Veuillez installer ou mettre à niveau vers la dernière Réponse aux incidents de sécurité version pour Espace de travail de la Réponse aux incidents de sécurité accéder aux fonctionnalités telles que le transfert d'équipe, le calculateur de score de risque, entre autres.

Cette section décrit les éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Créer une demande entrante
- Gérer les observables
- Gérer les recherches et les analyses
- Calculer la gravité d'un incident de sécurité
- Gérer les activités post-incident
- Fermer les incidents de sécurité

Créer une demande entrante

Contrairement aux incidents de sécurité, les demandes entrantes sont généralement moins prioritaires. Les demandes de recherche, d'analyse ou de nouveau badge sont des exemples de demandes entrantes.

Avant de commencer

Rôles requis : rôle sn_si.basic ou supérieur

Procédure

1. Accédez à l'un des formulaires de demandes.
   Par exemple : **Tous** > **Incident de sécurité** > **Demandes entrantes** > **Me l'affecter**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Demande de sécurité

Champ	Description
Numéro	[Lecture seule] Numéro de la demande de sécurité générée automatiquement.
Société	Société du demandeur.
Emplacement	L'emplacement du CI, le cas échéant. Ce champ est pré-rempli lorsque le CI est sélectionné.
Élément de configuration	L'élément de configuration affecté par la demande.
Priorité	Priorité de la demande.
Ouvert	[Lecture seule] Date et heure d'ouverture de la demande.
État	État actuel de la demande de sécurité. Lors de la création d'une demande de sécurité, ce champ est défini par défaut sur **Brouillon**.
Groupe d'affectation	Groupe d'affectation à partir duquel l'agent affecté est sélectionné.
Affecté à	Personne affectée à l'exécution du travail.
Description brève	Brève description de la demande de sécurité, visible par le demandeur.
Description	La description complète de la demande, visible par le demandeur.
Notes de travail	Notes de travail, visibles par le demandeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.
5. Si vous devez escalader la demande en incident de sécurité, cliquez sur **Convertir en incident de sécurité**.

Gérer les observables

Les observables sont des artefacts trouvés sur un réseau ou un système d'exploitation qui sont susceptibles d'indiquer une intrusion. Les observables typiques sont les adresses IP, les hachages MD5 de fichiers malveillants ou d'URL, ou les noms de domaine. Renseignements sur les menaces Les données de la table observable sont disponibles à partir d'un incident de sécurité.

Les informations sur les observables comprennent la valeur, le type, le contexte et l'horodatage.

Vous pouvez créer ou supprimer des observables manuellement ou automatiquement par le biais de demandes de recherche.

Une nouvelle colonne **de recherche** a été ajoutée à **l'onglet Résultats de la recherche de menace** . Les valeurs possibles sont : malveillant et inconnu.

Si une demande de recherche IoC ne trouve pas d'observable d'incident de sécurité, elle est étiquetée Inconnu.

Si une demande de recherche IoC trouve un observable d'incident de sécurité, elle est étiquetée comme malveillante.

Lors d'une mise à niveau, la colonne **Recherche** des objets existants est définie sur Malicieux.

Remarque : Bien que Renseignements sur les menaces les données de table des observables fassent partie d'un incident de sécurité, aucune autre interaction avec le module n'est Renseignements sur les menaces incluse. Pour une fonctionnalité complète de menace, le module d'extension Renseignements sur les menaces est disponible par abonnement.

Information associée

Créer un observable d'incident de sécurité

Afficher les informations IoC pour un incident de sécurité

Vous pouvez afficher des informations sur l'IoC, telles que les observables et les résultats de recherche de perceptions associés à un incident de sécurité.

Avant de commencer
Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les informations relatives à l'IoC.
2. Cliquez sur le lien connexe **Afficher l'IoC** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations relatives à l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet	Description
Observables	Affichez ou ajoutez ou modifiez manuellement des observables associés à l'incident de sécurité. Pour plus d'informations, consultez Gérer les observables.
Indicateurs associés	Si Renseignements sur les menaces cette option est activée, vous pouvez afficher tous les autres indicateurs associés à l'un des mêmes enregistrements de menace.
Résultats de recherche de perceptions	Contient les résultats de la recherche de perceptions.
Détails de la recherche de perception	Contient les détails de l'enregistrement de recherche de perceptions.
Recherches de menaces	Stocke les données d'enrichissement des systèmes de détection de programmes malveillants. Cet onglet n'apparaît que lorsque le module d'extension Renseignements sur les menaces est installé.
Modes/ méthodes d'attaque connexes	S'il Renseignements sur les menaces est activé, vous pouvez afficher tous les autres types d'attaques associés à l'un des mêmes enregistrements de menace.
Demandes d'analyses de sécurité	S'il Renseignements sur les menaces est activé, vous pouvez afficher les demandes d'analyse et de recherche jointes à l'incident de sécurité.
Ressources avec IoC similaires	S'il Renseignements sur les menaces est activé, vous pouvez afficher toutes les autres ressources ayant des indicateurs similaires.
Utilisateurs avec IoC similaires	S'il Renseignements sur les menaces est activé, vous pouvez afficher tous les autres utilisateurs avec des indicateurs similaires.

4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments affectés
   - Afficher les éléments connexes
   - Afficher les données d'enrichissement
   - Afficher les tâches de réponse
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Créer un observable d'incident de sécurité

Vous pouvez créer et afficher un observable au sein d'un incident de sécurité et prendre les mesures appropriées. Le fait de disposer d'observables dans l'incident de sécurité est évolutif et réduit le temps de réponse.

Avant de commencer

Rôle requis :

- sn_ti_observable.write (écriture)
- sn_ti_observable.read (lecture)
- sn_ti_observable.admin (supprimer)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à **Incident de sécurité**.
2. Choisissez un incident.
3. Cliquez sur **l'onglet de liste connexe Observables de l'incident de sécurité** .
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire comme il convient.

Champ	Description
Sélectionner une balise de classification	Si vous avez configuré et activé des balises de sécurité pour ajouter des métadonnées à l'enregistrement, vous pouvez sélectionner une ou plusieurs balises pour spécifier le degré de sensibilité de l'observable. Si vous n'avez pas configuré ou activé les balises de sécurité, cette liste déroulante ne s'affiche pas.
Valeur	Valeur (par exemple, adresse IP ou hachage) associée à l'observable. **Remarque :** Si une analyse des menaces sur une adresse IP ou un hachage, renvoie un programme malveillant ou une autre défaillance, l'adresse IP ou la valeur de hachage est automatiquement ajoutée à la table Observable [sn_ti_observable]. En tant que tel, il peut être recherché à partir du formulaire Observables.
Type d'observable	Sélectionnez la classification de l'observable, telle qu'une adresse IP ou un hachage de fichier. Ces types d'observables sont définis dans le module **Types d'observables** .
Nombre d'incidents	Nombre de fois où la valeur de l'observable a été rencontrée.
Est une composition	Ce champ s'affiche uniquement après avoir sauvegardé l'enregistrement de l'observable. Si le **type d'observable** est défini sur autre chose que **Composition observable** et que ce nouvel observable est une composition, cochez cette case. Si le **type d'observable** est déjà défini sur **Composition de l'observable**, la case est cochée et en lecture seule. Une composition observable est un observable qui contient des observables enfants.
Résultat	Sélectionnez l'une des options suivantes : ○ **malveillant** : indique que l'observable est nuisible à l'organisation. ○ **Suspect** : indique que l'observable peut être dangereux pour l'organisation. ○ **Propre** : indique que l'observable n'est pas dangereux pour l'organisation. ○ **Inconnu** : indique que nous n'avons pas encore déterminé la conclusion de l'observable. ○ Valeur par défaut : inconnue. Pour plus d'informations, consultez Calculateurs de résultats de la recherche de menace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Après une mise à niveau, les observables existants sont marqués comme malveillants.
Opérateur	Ce champ s'affiche uniquement si la case **Est la composition** est cochée. Selon votre configuration dans ce champ, les observables et leurs enfants sont pris en compte pour décider si un indicateur associé est présent. Définissez ce champ sur **ET** si tous les observables enfants doivent être présents pour qu'un indicateur associé soit considéré comme présent. Définissez-le sur **OU** si l'un des observables enfants est présent pour qu'un indicateur associé soit considéré comme présent.
Ne doit pas être présent	Ce champ s'affiche uniquement après avoir sauvegardé l'enregistrement de l'observable. Si ce champ est sélectionné, ce champ signifie que l'absence de l'observable est le problème potentiel (par exemple, une clé de Registre manquante).
Emplacement	Vous pouvez charger Charger plus de données IoC dans ce champ à l'aide des paramètres de deux propriétés et d'une définition d'include de script.
Notes	Saisissez toutes les remarques supplémentaires sur l'observable.

6. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires.

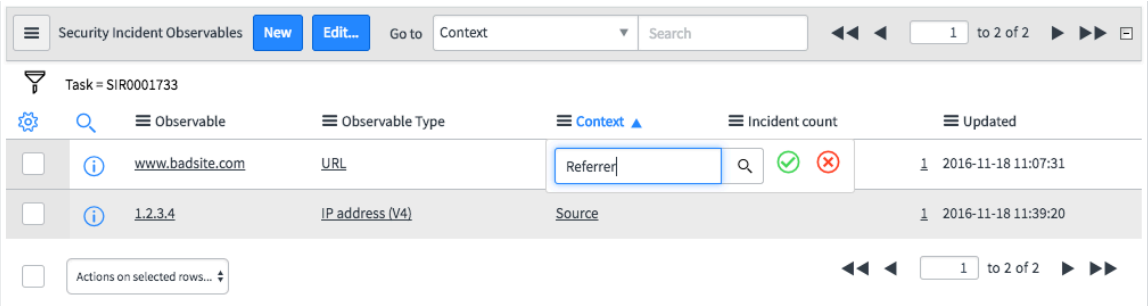
Liste connexe	Description
Indicateurs connexes	Répertorie les indicateurs qui ont été identifiés par la source de menace.
Tâches associées	Répertorie les changements associés à l'observable.
Observables enfants	Répertorie les observables associés qui ont été identifiés par la source de menace.
Ressources correspondantes pour IP	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante.
Sources des observables	Répertorie les sources de cet observable, ainsi que le niveau de confiance de la source.
Annotations de sécurité	Répertorie les annotations de sécurité ajoutées à cet observable.

7. Pour en revenir à l'incident de sécurité, les informations suivantes sont disponibles.

Remarque : Lorsque vous ajoutez un observable à l'incident de sécurité, le système recherche tout autre élément de configuration ou utilisateur qui lui est associé. Les onglets de liste connexe **Éléments de configuration associés** et **Utilisateurs associés** sont mis à jour en conséquence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Colonne	Définition
Observable	Valeur (par exemple, adresse IP ou hachage) associée à l'observable.
Type d'observable	Type spécifique d'observable.
Contexte	Sélectionné par l'utilisateur. Les choix possibles sont les suivants : ○ IP : source ou destination **Remarque :** Si Renseignements sur les menaces et Palo Alto Networks - Firewall sont activés, la modification ou l'ajout d'une valeur à ce champ entraîne l'exécution du workflow Obtenir le flux de données du journal Security Operations Palo Alto Networks - Obtenir les données du journal . Le workflow récupère les données enrichies du journal des menaces à partir du pare-feu et les joint à l'incident de sécurité. Les informations sont également analysées et affichées dans la section Journaux du pare-feu sous **l'onglet Données d'enrichissement** . ○ URL - Référent **Remarque :** Lorsque l'utilisateur clique sur un lien dans un e-mail d'hameçonnage, un référent est l'URL du dernier saut avant l'accès à l'URL du programme malveillant.
Nombre d'incidents	Nombre d'incidents dans lesquels cet observable apparaît. Cette valeur est automatiquement mise à jour lorsque l'observable est ajouté à un autre incident manuellement ou via un workflow.
Mis à jour	Données et heure de dernière mise à jour de la liste.

Remarque : Si le module d'extension Renseignements sur les menaces est installé, vous pouvez également afficher l'observable dans la liste **Observables** du **référentiel IoC**.

Information associée

Modifier une liste d'observables d'incident de sécurité

Ajouter plusieurs observablesd'incident de sécurité

Gérer les observables de fichier

La gestion des observables de fichier fournit des mesures de sécurité strictes pour stocker les fichiers suspects et active les observables de type de fichiers pour l'intégration de bac à sable.

Avant de commencer

Rôle requis : sn_ti_malicious_attachment_access (charger)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chargez les observables de type de fichier :

- Automatiquement : lorsque les incidents de sécurité sont créés pour les e-mails d'hameçonnage, les pièces jointes de l'e-mail d'hameçonnage sont créées en tant qu'observables de type fichier.

- Manuellement : un analyste de sécurité peut également charger les fichiers suspects pour créer des observables de type fichier.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer et afficher des observables de type fichier pour un incident de sécurité. Les fichiers suspects qui font partie des observables sont stockés dans un emplacement spécifique, auquel l'analyste de la sécurité peut accéder pour télécharger le fichier uniquement avec un rôle spécifique.

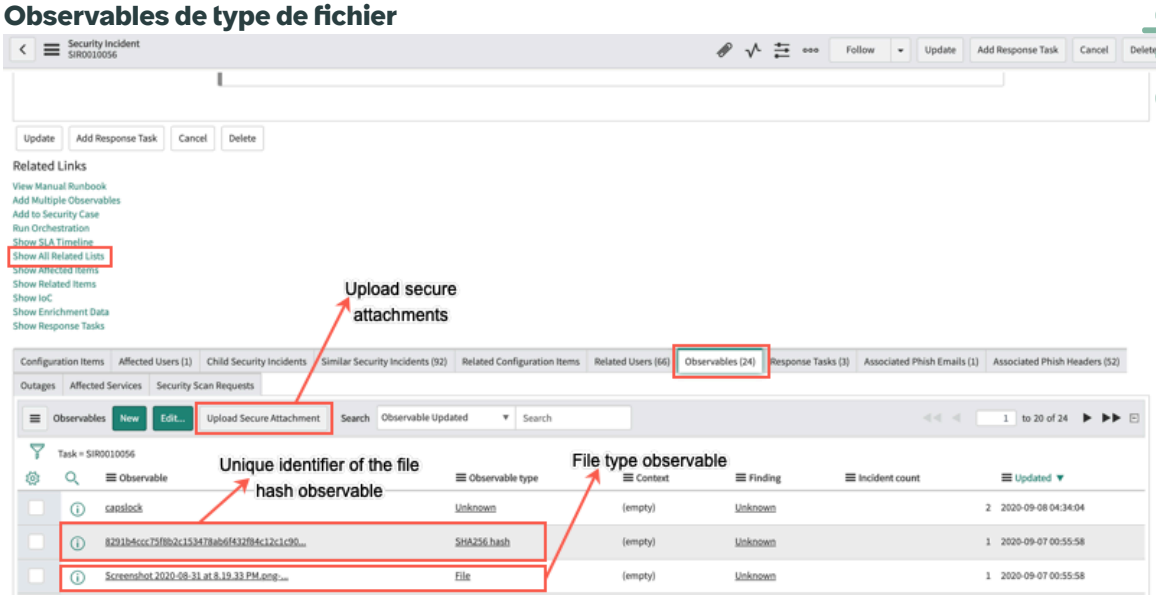
Procédure

1. Accédez à un incident de sécurité.
2. Sélectionnez des **observables** dans l'onglet **Afficher toutes les listes connexes** .

   Si l'e-mail d'hameçonnage contient des pièces jointes, celles-ci sont créées par défaut en tant qu'observables de type fichier dans l'incident de sécurité correspondant. Chaque pièce jointe est créée en tant que deux observables tels que le type de fichier et l'observable de hachage de fichier.

3. Pour charger manuellement les pièces jointes sécurisées :
   - Cliquez sur **Télécharger la pièce jointe sécurisée**.
   - Dans la section Télécharger des pièces jointes sécurisées, cliquez sur **Choisir un fichier** pour charger un ou plusieurs fichiers. Chaque fichier est considéré comme un enregistrement observable unique.
   - Cliquez sur **Créer des observables de fichier** pour créer des observables de type de fichier, par exemple un est le type de fichier et l'autre est le hachage de fichier, qui est un identificateur unique.

Observables de type de fichier



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionnez le type de fichier observable à traiter pour d'autres intégrations telles que le bac à sable, la recherche de menaces. En outre, vous pouvez également télécharger les pièces jointes à partir du type de fichier observable.

Remarque :

La recherche de menace (VirusTotal) récupère le fichier à partir des pièces jointes sécurisées pour les nouveaux observables de type de fichier et les propriétés système ci-dessous ne sont pas applicables aux nouveaux observables de type de fichier.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

Pour une référence rapide, l'observable de type fichier est mappé en tant qu'enfant à l'observable de hachage et l'observable de hachage est mappé en tant qu'enfant à l'observable de fichier.

Si les pièces jointes de l'e-mail d'hameçonnage dépassent la taille définie, les observables ne sont pas créés. Vous devez modifier les propriétés système pour prendre en charge les fichiers de plus grande taille.

Propriétés système de la taille du fichier

Propriété système	Description
glide.email.inbound.max_total_attachment_size_bytes	Si vous transférez directement l'e-mail d'hameçonnage, utilisez cette valeur de propriétés système pour augmenter la taille du fichier de 18 Mo à la taille de fichier souhaitée.
com.glide.attachment.max_get_size	Si vous transférez l'e-mail d'hameçonnage en tant que pièce jointe, utilisez cette valeur de propriété système pour créer les propriétés système ci-dessous dans le champ d'application global afin d'augmenter la taille du fichier de 5 Mo à la taille souhaitée.

Vous pouvez également créer un observable de type de fichier comme suit :

a. Cliquez sur **Nouveau**.

b. Sélectionner le **type d'observable Catégorie : fichier**

c. Cliquez sur **Charger** pour joindre un fichier.

Modifier une liste d'observables d'incident de sécurité

Vous pouvez modifier les observables de la liste associés à un incident de sécurité à afficher.

Avant de commencer

Rôle requis : sn_si.basic

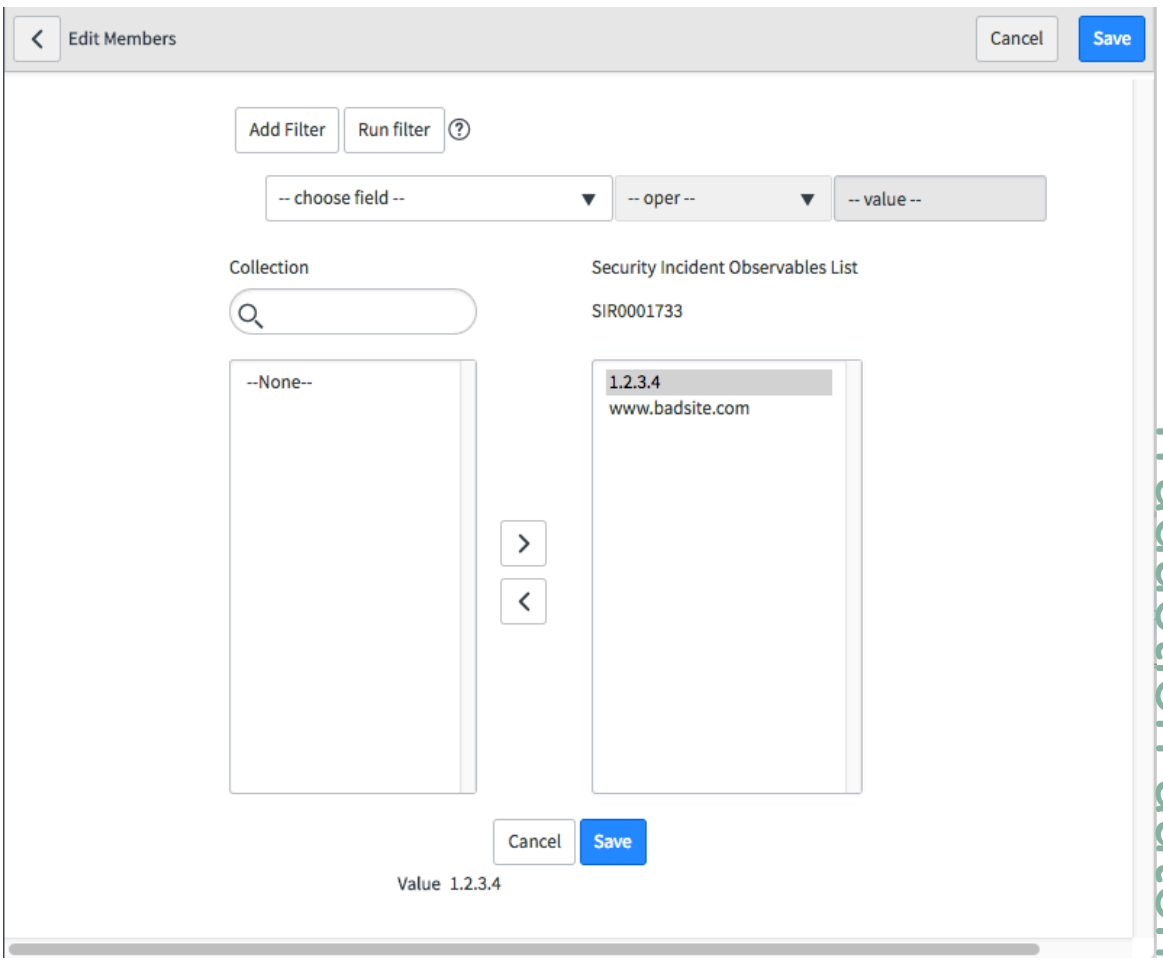
Procédure

1. Accédez à **Incident de sécurité**.
2. Choisissez un incident.
3. Cliquez sur **l'onglet de liste connexe Observables de l'incident de sécurité** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Modifier**.
5. Ajoutez ou supprimez des observables de la liste.
   Créez un filtre pour les longues listes.



6. Cliquez sur **Enregistrer**.

Remarque : Lorsque vous ajoutez un observable à l'incident de sécurité, le système recherche tout autre élément de configuration ou utilisateur qui lui est associé. Les onglets de liste connexe **Éléments de configuration associés** et **Utilisateurs associés** sont mis à jour en conséquence. En outre, si le module d'extension Renseignements sur les menaces est activé et qu'au moins une implémentation d'intégrationIntégrations de Réponse aux incidents de sécurité est activée, il Security Operations Integration - Aptitude de recherche de menace exécute un ou plusieurs workflows et des recherches de sécurité contre les menaces sont effectués sur les observables que vous avez ajoutés. Les résultats apparaissent dans **l'onglet Résultats de la recherche de menace** .

Information associée

Ajouter plusieurs observablesd'incident de sécurité

Créer un observable d'incident de sécurité

Ajouter plusieurs observablesd'incident de sécurité

Pour gagner du temps, vous pouvez ajouter plusieurs observables d'incident de sécurité à la liste des observables d'incident de sécurité.

Avant de commencer

Rôle requis : sn_ti_write

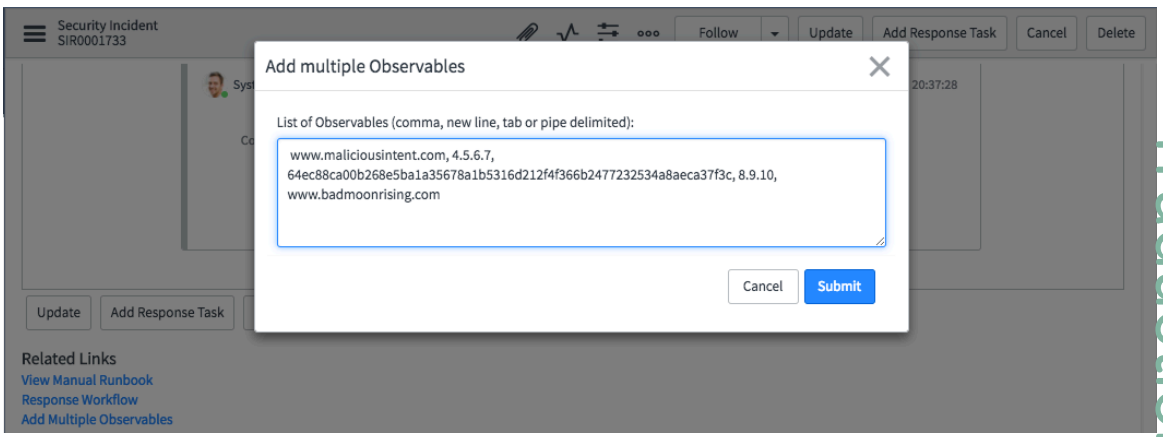
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lors de l'ajout de plusieurs observables d'incident de sécurité, les doublons sont ignorés pendant le traitement.

Procédure

1. Accédez à **Incident de sécurité**.
2. Choisissez un incident.
3. Cliquez sur le lien connexe **Ajouter plusieurs observables** .
4. Saisissez ou collez plusieurs observables.
   Les entrées peuvent être de n'importe quel type d'observable. Les formats acceptés sont : séparateurs par virgules, nouvelles lignes, tabulations ou barres verticales.



Remarque : Lorsque vous ajoutez un observable à l'incident de sécurité, le système recherche tout autre élément de configuration ou utilisateur qui lui est associé. Les onglets de liste connexe **Éléments de configuration associés** et **Utilisateurs associés** sont mis à jour en conséquence.

Remarque : les valeurs observables non détectées automatiquement sont affectées au type Inconnu.

5. Cliquez sur **Soumettre**.

Enrichissement automatique des données du journal des observables des incidents de sécurité

Lorsque certaines applications et intégrations sont configurées, y compris Renseignements sur les menaces l'intégration, les informations sur les observables d'un Palo Alto Networks - Firewall incident de sécurité peuvent être automatiquement enrichies avec les données du journal des menaces chaque fois que l'adresse IP source de ses observables est modifiée.

Lorsqu'une modification se produit, une règle métier lance un workflow qui récupère les données des journaux de menaces sur votre pare-feu et enrichit les informations des observables dans l'incident de sécurité.

Avant de pouvoir enrichir les observables, les étapes suivantes doivent être effectuées.

- Threat Intelligence doit être activé.
- L'intégration du pare-feu Palo Alto Networks doit être activée et configurée. Cela peut également inclure .Configurer les informations d'identification SSH vers le serveur MID

Une fois cette configuration terminée, le fait de modifier l'adresse IP source des observables associés à un incident de sécurité entraîne l'exécution par une règle métier du workflow **Security Operations Palo Alto Networks - Get Log Data** . Les activités du workflow mettent en file d'attente une requête de recherche sur le pare-feu et renvoient un ID de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

tâche qui est utilisé pour récupérer les données des journaux des menaces à partir du pare-feu et les joindre en tant que fichier XML à l'incident de sécurité.

Information associée

- Obtenir des informations sur la session AutoFocus Flux d'enrichissement
- Palo Alto Networks Workflow du lanceur de pare-feu
- Security Operations Palo Alto Networks : workflow de vérification et de blocage des valeurs
- Obtenir le flux de données du journal
- Obtenir le flux d'enrichissement des données WildFire

Publier des observables dans une liste de surveillance tierce

Vous pouvez publier un ou plusieurs observables ou indicateurs associés dans une liste de surveillance tierce. Actuellement, la seule implémentation qui prend en charge cette fonctionnalité est CrowdStrike Falcon Host.

Avant de commencer

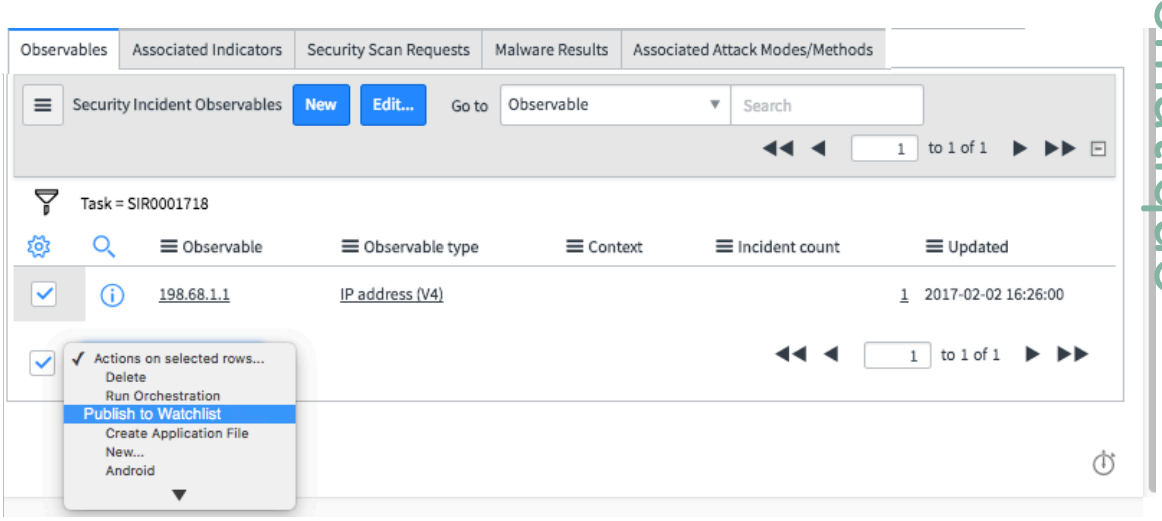
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

Procédure

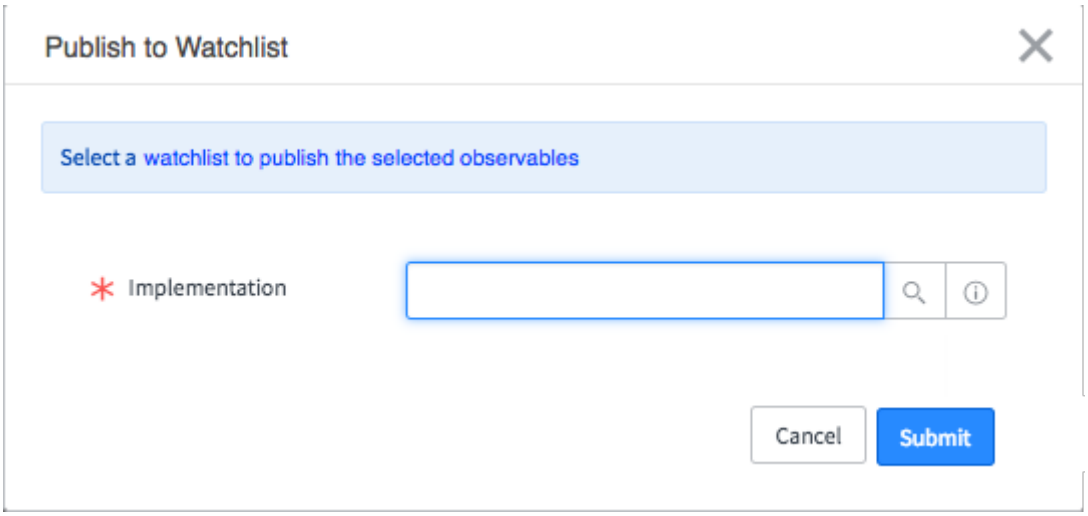
1. Accédez à un incident de sécurité.
2. Sélectionnez **Observables** dans l'onglet **Liste connexe** .
3. Cliquez sur **Publier dans la liste de surveillance** dans le menu déroulant **Actions sur les lignes sélectionnées...**



La boîte de dialogue s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Entrez ou choisissez l'implémentation.

   Remarque : Un workflow est déclenché lorsque Security Operations Integration : aptitude de publication dans la liste de surveillance vous sélectionnez l'implémentation de CrowdStrike Falcon Host.

5. Cliquez sur **Envoyer**.

Gérer les recherches et les analyses

Vous pouvez effectuer des recherches et des analyses de vulnérabilité à partir des incidents de sécurité et du catalogue des incidents de sécurité afin d'identifier les menaces et les vulnérabilités potentielles.

Soumettre une demande de recherche IoC à partir d'un incident de sécurité

Une recherche d'IoC s'exécute automatiquement chaque fois que des observables sont ajoutés à un incident de sécurité. En outre, si votre incident de sécurité comporte des pièces jointes, celles-ci peuvent être facilement trouvées en appuyant sur un bouton.

Avant de commencer

Pour les recherches automatiques IoC, le module d'extension Renseignements sur les menaces doit être activé.

Rôle requis : sn_si.basic

Remarque : Par défaut, le **type de recherche** de **fichier** est inactif.

Procédure

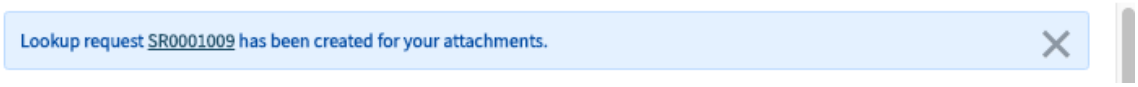
1. Créez un nouvel incident de sécurité ou ouvrez-en un existant si vous avez l'intention d'y joindre de nouveaux fichiers.
2. Cliquez sur l'icône du presse-papier dans l'en-tête du formulaire et joignez un ou plusieurs fichiers.
3. Lorsque vous avez terminé vos entrées sur le formulaire, cliquez avec le bouton droit sur l'en-tête du formulaire et cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un bouton **Rechercher des pièces jointes** s'affiche.
4. Cliquez sur **Rechercher des pièces jointes**.

   Remarque : Les notes de travail sous **Détails de l'incident** signalent la progression du processus de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Vous pouvez cliquer sur le numéro de recherche à la fin du message pour afficher l'enregistrement de recherche.
   Vous pouvez cliquer sur le lien Rechercher une référence pour afficher les résultats détaillés.



Soumettre une demande de recherche IoC à partir du Catalogue des incidents de sécurité

Si le module d'extension Réponse aux incidents de sécurité est activé, vous pouvez soumettre des recherches de menaces pour des fichiers, des valeurs de hachage, des URL et des adresses IP à partir du catalogue des incidents de sécurité. Les demandes sont soumises et vous pouvez afficher les résultats dans le module **Mes demandes** .

Avant de commencer
Rôle requis : aucun

Pourquoi et quand exécuter cette tâche
Les recherches sont automatiquement effectuées pour le type de recherche par défaut pour chaque source de recherche répertoriée dans l'enregistrement de recherche. Les résultats de la demande de recherche sont disponibles dans le module **Mes demandes** .

Procédure

1. Accédez à la **Tous** > **Libre-service** > **Catalogue des incidents de sécurité**.
2. Cliquez sur **Recherche IoC**.
3. Cliquez sur **Rechercher des fichiers, des valeurs de hachage, des URL ou des adresses IP**.
4. Entrez un ou plusieurs des éléments suivants :

Demande de recherche IoC

Élément à rechercher	Description
Fichiers	Cliquez sur l'icône du trombone, puis recherchez et joignez les fichiers que vous souhaitez rechercher. **Remarque :** Par défaut, le **type de recherche** de **fichier**est inactif. Les fichiers sont convertis et soumis en tant que valeur de hachage.
URL	Dans le champ **URL** , entrez les URL que vous souhaitez rechercher, séparées par des virgules. Par exemple : www.abc.com, www.xyz.net.
Adresses IP	Dans le champ **Adresses IP** , entrez les adresses IP que vous souhaitez rechercher, séparées par des virgules.
Valeurs de hachage	Dans le champ **Valeurs de hachage** , saisissez les valeurs de hachage que vous souhaitez rechercher, séparées par des virgules. **Remarque :** Lorsque le **type de recherche** de **fichier** est inactif, cette valeur est l'action par défaut pour les valeurs **de fichier** et **de hachage**.

5. Lorsque vous avez effectué vos sélections, cliquez sur **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Pour afficher l'état et/ou les résultats des recherches, accédez à **Libre-service** > **Mes demandes**.
7. Cliquez sur le numéro SR de la demande.
   Les notes de travail sous **Activité** énumèrent les tâches effectuées pendant la recherche, y compris la création de recherches individuelles pour chaque fichier, valeur de hachage, URL ou adresse IP, ainsi que les résultats de la recherche.

Soumettre une demande d'analyse de vulnérabilité à partir d'un incident de sécurité

Si votre incident de sécurité comporte un ou plusieurs éléments de configuration (serveurs, ordinateurs, etc.), il peut être analysé pour rechercher des Réponse aux incidents de sécurité vulnérabilités à partir du formulaire.

Avant de commencer

Le Réponse aux vulnérabilités module d'extension doit être activé.

Rôle requis : sn_si.write

Procédure

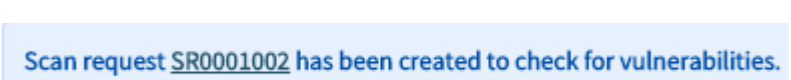
1. Créez un incident de sécurité et incluez au moins une ressource.
   Vous pouvez également ouvrir un incident existant qui comporte des éléments de configuration.
2. Lorsque vous avez terminé vos entrées sur le formulaire, cliquez avec le bouton droit sur l'en-tête du formulaire et cliquez sur **Enregistrer**.
   Une fois l'enregistrement enregistré, un lien connexe **Rechercher des vulnérabilités** s'affiche.

   Remarque : Si la liste connexe **Rechercher des vulnérabilités** n'est pas affichée, vous devez accéder à **Vulnérabilité** > **Scanners**, configurez au moins un scanner et définissez sa valeur par défaut sur **vrai**.

3. Cliquez sur **Rechercher les vulnérabilités**.

   Remarque :

   Un message apparaît en haut du formulaire d'incident de sécurité, ainsi qu'un lien vers l'enregistrement d'analyse.

4. Vous pouvez cliquer sur le numéro de demande d'analyse pour afficher l'enregistrement d'analyse.
   Les détails de l'incident affichent les résultats de l'analyse dans l'enregistrement de demande d'analyse de sécurité.

Soumettre une demande d'analyse de vulnérabilité à partir du catalogue Security Incident Response

Vous pouvez soumettre des analyses de vulnérabilité pour les CI et les adresses IP à partir du Réponse aux incidents de sécurité catalogue. Les demandes sont soumises et vous pouvez afficher les résultats dans le module **Mes demandes** .

Avant de commencer

Rôle requis : aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Libre-service** > **Catalogue des incidents de sécurité**.
2. Cliquez sur **Analyse de vulnérabilité**.
3. Cliquez sur **l'élément de configuration de l'analyse et sur les adresses IP**.
4. Entrez un ou plusieurs des éléments suivants à analyser.

Scanners de vulnérabilité

Élément à analyser	Description
Élément de configuration	Dans le champ **Élément de configuration à analyser** , sélectionnez le CI à analyser.
Adresses IP	Dans le champ **Adresses IP à analyser** , entrez les adresses IP, séparées par des virgules.

5. Lorsque vous avez effectué vos sélections, cliquez sur **Soumettre**.
   Si un observable est trouvé, un indicateur est créé, conformément aux normes STIXX.
6. Pour afficher l'état et/ou les résultats des analyses, accédez à **Libre-service** > **Mes demandes**.
7. Cliquez sur le numéro SR de la demande.
   Les notes de travail sous **Activités** répertorient les tâches effectuées pendant l'analyse, y compris la création d'analyses individuelles pour chaque CI ou adresse IP, et les résultats des analyses.

Définir de nouvelles orchestrations à la demande

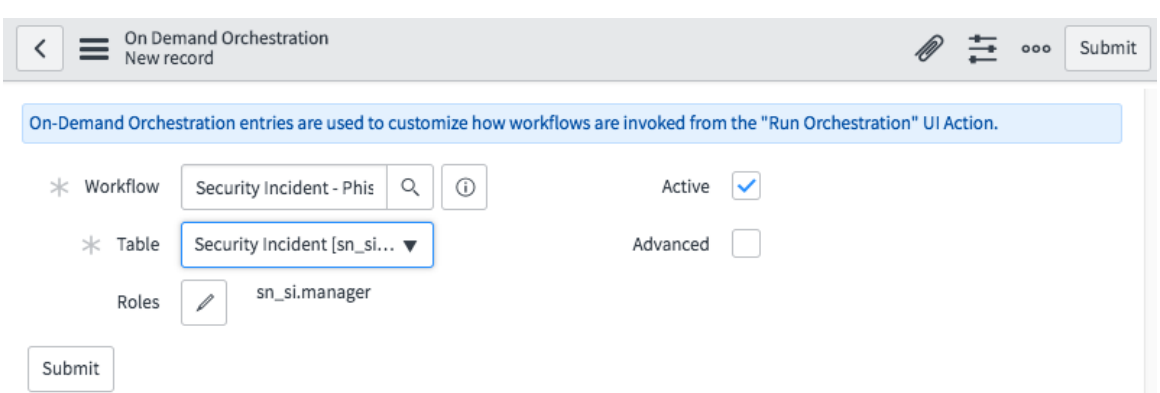
Dans le système de base, vous pouvez sélectionner des orchestrations sur demande qui exécutent des workflows prédéfinis. Vous pouvez définir de nouvelles orchestrations à la demande pour personnaliser la manière dont les workflows sont appelés à partir des listes de choix **Exécuter l'orchestration** .

Avant de commencer

Rôle requis : sn_si.write

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Orchestration sur demande**
2. Cliquez sur **Nouveau**.



3. Renseignez les champs comme il convient.

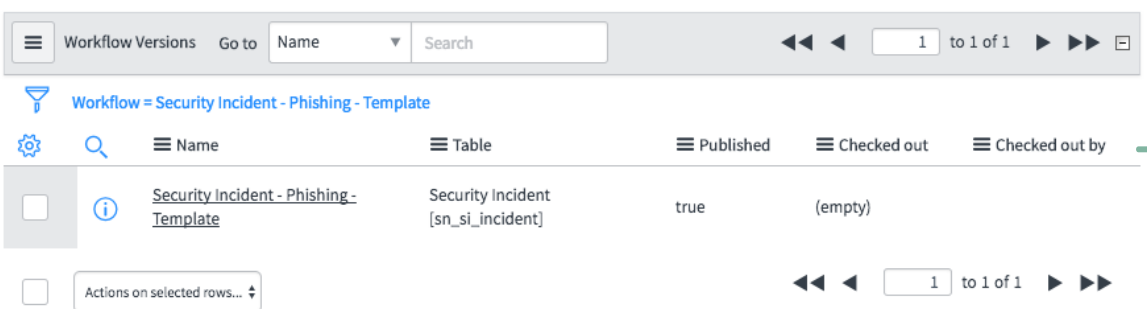
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Orchestration à la demande

Champ	Description
Workflow	Sélectionnez le workflow à inclure dans la liste de choix **Exécuter l'orchestration** .
Table	Sélectionnez la table sur laquelle le workflow sélectionné est exécuté. Si la table ne correspond pas à la table configurée pour le workflow sélectionné, vous devez cocher la case **Avancé** et modifier le **script d'exécution** pour transmettre le bon enregistrement au workflow lors de l'exécution.
Rôles	Si nécessaire, sélectionnez des rôles supplémentaires pour restreindre qui peut voir ce workflow dans la liste de choix **Exécuter l'orchestration** .
Actif	Cochez cette case pour activer cet enregistrement d'orchestration à la demande.
Avancés	Cochez cette case pour modifier le script d'exécution afin qu'il transmette l'enregistrement correct à la table sélectionnée pour ce workflow.
Script d'exécution	Modifiez le script d'exécution afin qu'il transmette l'enregistrement correct à la table sélectionnée pour ce workflow. Ce champ s'affiche uniquement si la case **Avancé** est cochée.

4. Cliquez avec le bouton droit dans l'en-tête de l'enregistrement, puis sélectionnez **Enregistrer**.
La liste connexe **Versions du workflow** s'affiche.



5. Si vous devez apporter des modifications supplémentaires au workflow, vous devez le vérifier.

Information associée

Utiliser les versions de workflow

Enregistrer les nouvelles applications Security Operations pour l'orchestration à la demande

Dans le système de base, les applications Security Operations sont automatiquement enregistrées lorsqu'elles sont activées. L'inscription permet aux workflows associés aux applications d'être disponibles pour les demandes d'orchestration à la demande. Si nécessaire, vous pouvez définir de nouvelles applications et leur associer des workflows pour l'orchestration sur demande.

Traduction automatique

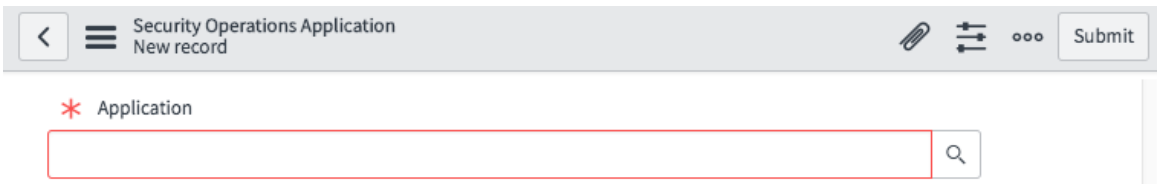
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

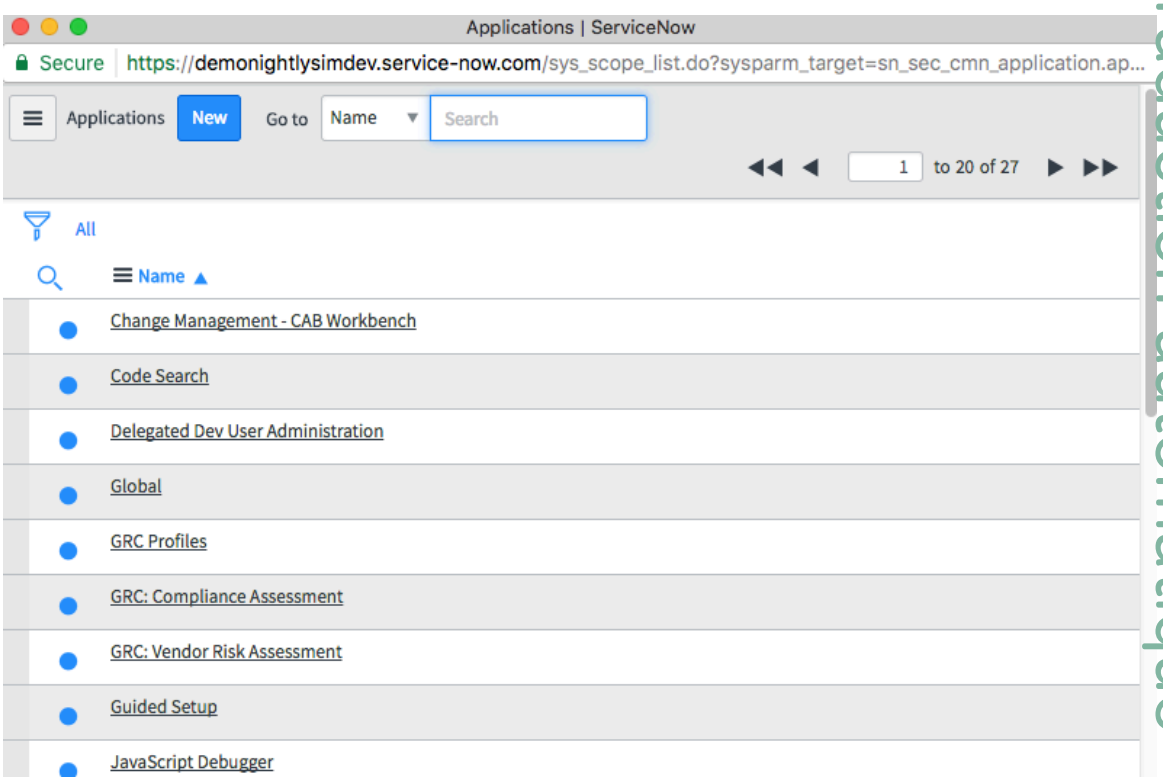
Rôle requis : sn_si.write

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Registre des applications SecOps**et cliquez sur **Enregistrer l'application**.
   L'écran de l'application Security Operations s'affiche.



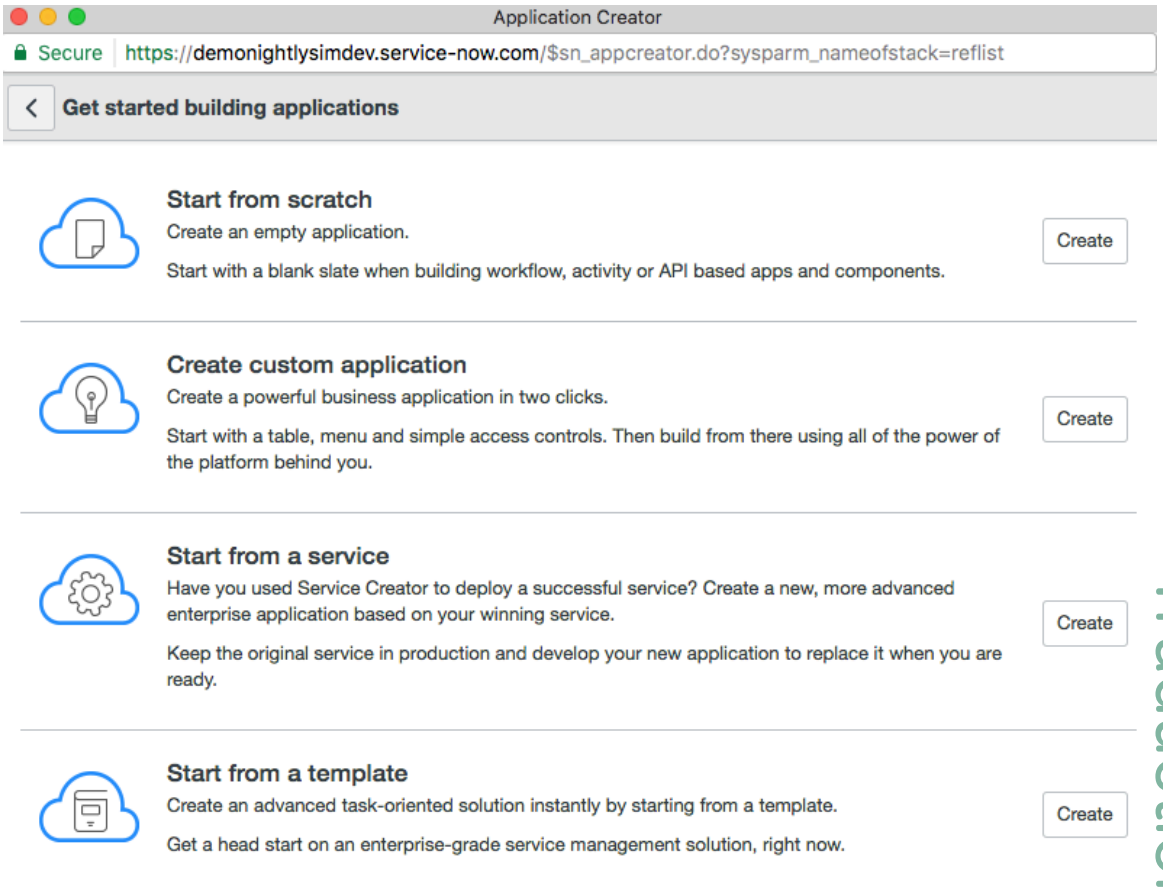
2. Dans le champ **Application** , cliquez sur l'icône de recherches (loupe).
   L'écran Applications s'affiche.



3. Cliquez sur **Nouveau**.
   L'écran Créateur d'application s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Les options qui s'affichent dépendent des applications que vous avez activées. Pour en savoir plus sur la création de nouvelles applications, consultez Création d'applications .

4. Une fois l'application générée, vous pouvez créer des scripts pour configurer l'orchestration à la demande.

Remarque : La configuration de l'orchestration à la demande pour de nouvelles applications nécessite des connaissances techniques avancées en matière de scripting et de création de déclencheurs pour les scripts (règles métier, action d'interface utilisateur, workflows...). Pour plus d'informations, contactez les ServiceNow services professionnels.

Ajouter des informations à un incident de sécurité

Après la création d'un incident de sécurité, vous pouvez ajouter d'autres détails pour faciliter l'analyse, tels que les rôles d'accès et différents types de notes.

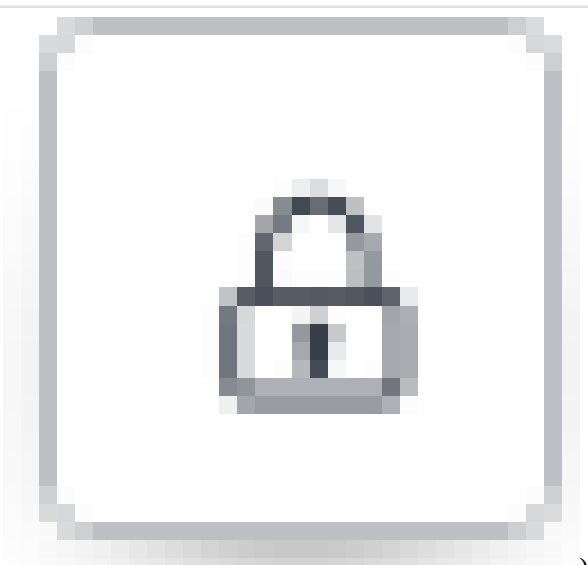
Avant de commencer
Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité que vous souhaitez mettre à jour.
2. Cliquez sur l'onglet **Détails de l'incident** .
3. Renseignez les champs nécessaires.

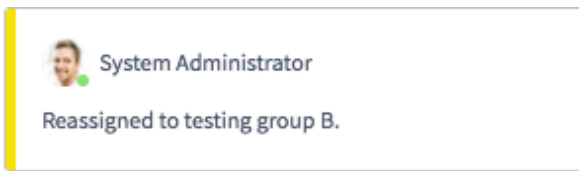
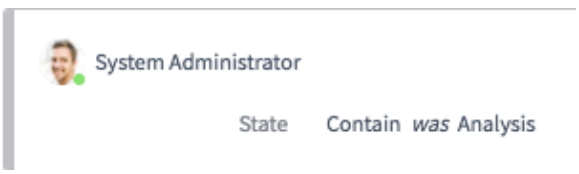
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Accès en lecture	Donne à un utilisateur disposant du rôle **d'accès spécial** un accès en lecture à l'incident de sécurité. L'utilisateur est capable de lire et d'écrire des notes de travail. **Remarque :** ◦ Si un utilisateur est ajouté à la fois à la liste **d'accès en lecture** et à **la liste d'accès privilégié** , seules les autorisations d'accès **privilégié** persistent. ◦ L'utilisateur disposant du rôle sn_si.admin peut modifier à la fois l'accès en lecture et l'accès privilégié.
Liste de surveillance	Cliquez sur l'icône de verrou pour ajouter des utilisateurs avertis lorsque des changements apportés à l'incident de sécurité se produisent. Une fois le champ déverrouillé, des options sont disponibles pour ajouter ou supprimer plusieurs utilisateurs ou saisir des adresses e-mail d'utilisateurs. Lorsque vous avez terminé vos entrées, cliquez sur l'icône de verrou pour verrouiller le champ.
Accès privilégié	Attribue à un utilisateur disposant du rôle **d'accès spécial** un accès en lecture et en écriture à tous les champs de l'incident de sécurité, à l'exception de **Affecté à**. Les utilisateurs disposant de rôles d'accès spéciaux ont leur propre module contenant tous les incidents de sécurité qui leur sont affectés. Aucun autre module n'est à leur disposition. Personne d'autre ne peut voir le module **Visible pour moi** . **Remarque :** Seul un utilisateur affecté ou une personne disposant d'un rôle de sécurité (par exemple, sn_si_analyst ou sn_si.admin) peut modifier le champ **Affecté à** . Si un utilisateur est ajouté à la fois à la liste **d'accès en lecture** et à **la liste d'accès privilégié** , seules les autorisations d'accès **privilégié** persistent.
Liste de notes de travail	 Cliquez sur l'icône de) pour ajouter des utilisateurs qui sont avertis lorsque de nouvelles notes de travail sont ajoutées. Une fois le champ déverrouillé, des options sont disponibles pour ajouter ou supprimer plusieurs

Traduction automatique

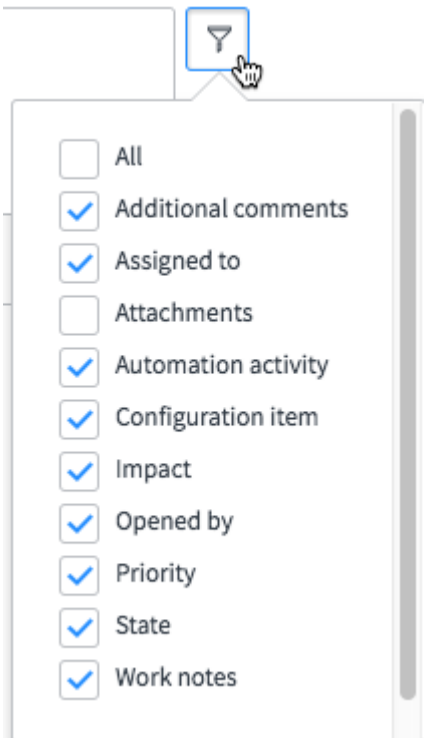
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	utilisateurs ou saisir des adresses e-mail d'utilisateurs. Lorsque vous avez terminé vos entrées, cliquez sur l'icône de verrou pour verrouiller le champ.
Description	Saisissez une description complète de l'incident de sécurité ainsi que toute information pouvant aider à trouver la cause ou à résoudre le problème.
Notes sécurisées	Seuls les rôles d'utilisateur avec sn_si.admin et sn_si.analyst peuvent afficher ou modifier les notes sécurisées.
Notes de travail	Saisissez des notes de travail qui ne sont pas visibles pour le client. Les notes de travail s'affichent dans la zone **Activité** .
Activité	Affiche les informations saisies manuellement dans les notes de travail et toutes les activités de tâches mises à jour dynamiquement (actions, commentaires, notes de travail, etc.) sur les enregistrements associés à cet incident de sécurité. Les notes de travail apparaissent avec une bande de couleur jaune.  Les notes générées automatiquement apparaissent avec une bande de couleur grise. 

4. Vous pouvez limiter les types d'informations affichées dans le champ **Activité** en cliquant sur l'icône de filtre ( ).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : La case à cocher **Activité d'automatisation** vous permet d'inclure tout enrichissement effectué par cet incident de sécurité, y compris les activités de workflow, les mises à jour du score de risque, etc.

5. Cliquez sur l'un des onglets suivants pour mettre à jour l'incident de sécurité :
   - Enregistrements connexes
   - Revue post-incident
   - Informations sur la fermeture
6. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Ajouter les problèmes, les changements et les incidents associés à un incident de sécurité

Vous pouvez ajouter des enregistrements connexes, tels que des problèmes, des changements et des incidents, aux incidents de sécurité existants.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité que vous souhaitez mettre à jour.
2. Cliquez sur l'onglet **Enregistrements connexes** .
3. Renseignez les champs nécessaires.

Champ	Description
Problème	Sélectionnez un enregistrement de problème (PRB) qui résout le problème sous-jacent à l'origine de la création de cet incident de sécurité. Les PRB pour cet incident sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	généralement créés en cliquant avec le bouton droit de la souris dans l'en-tête du formulaire d'incident de sécurité et en sélectionnant **Créer un problème**.
Parent	Sélectionnez un enregistrement de tâche lié au problème sous-jacent qui a causé la création de cet incident de sécurité.
Incident de sécurité parent	Sélectionnez un enregistrement d'incident de sécurité lié au problème sous-jacent qui a entraîné la création de cet incident de sécurité. Consultez Relations d'incident de sécurité parent et enfant.
Incident	Sélectionnez un enregistrement d'incident (INC) qui résout le problème sous-jacent à l'origine de la création de cet incident de sécurité. L'incident est généralement créé en cliquant avec le bouton droit de la souris sur l'en-tête du formulaire d'incident de sécurité et en sélectionnant **Créer un incident**.
Demande de changement	Sélectionnez un enregistrement de demande de changement (CHG) qui résout le problème sous-jacent à l'origine de la création de cet incident de sécurité. La demande de changement est généralement créée en cliquant avec le bouton droit de la souris sur l'en-tête du formulaire d'incident de sécurité et en sélectionnant **Créer un changement**.

4. Cliquez sur l'un des onglets suivants pour mettre à jour l'incident de sécurité :
   - Détails de l'incident
   - Revue post-incident
   - Informations sur la fermeture
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Appeler un vidage de processus pour un processus enrichi dans Windows

Un analyste de la sécurité peut exécuter un vidage de processus sur un processus spécifique, le vider dans un fichier et le publier sur un site partagé sur un réseau interne. Un analyste peut alors afficher un processus sur liste de refus, surligné en rouge dans un incident de sécurité, et effectuer une analyse supplémentaire.

Avant de commencer

Les éléments suivants sont requis :

- Un client exécutant Windows Vista ou une version ultérieure, ou un serveur exécutant Windows Server 2008 ou une version ultérieure.
- L'utilitaire de ligne de commande ProcDump installé, avec une variable d'environnement système qui pointe vers le chemin d'accès au fichier exécutable procdump. Le nom de la variable doit être PROCDUMP. Ce nom est utilisé dans un script PowerShell.

Rôle requis : sn_si.analyst

Procédure

1. Accédez à l'incident de sécurité avec le processus enrichi sur lequel vous souhaitez invoquer un procdump en cliquant sur **Tous** > **Incident de sécurité** > **Afficher les incidents ouverts**et ouvrez un incident de sécurité.
2. Cliquez sur **l'onglet Données d'enrichissement** .
3. Cliquez sur l'enregistrement d'enrichissement **Récupérer les processus en cours d'exécution** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cochez les cases des processus en cours d'exécution pour lesquels vous souhaitez effectuer un procdump, cliquez sur la liste déroulante Actions sur les lignes sélectionnées en bas de la liste, puis cliquez sur **Exécuter le procdump**.
   Un **workflow de prodump initié pour** le message du processus sélectionné apparaît en haut de la liste, et le workflow **Réponse aux incidents de sécurité : exécuter procdump** s'exécute.

Afficher des informations dans un incident de sécurité

Vous pouvez effectuer plusieurs autres actions sur un incident de sécurité existant à l'aide des liens connexes.

Avant de commencer
Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité que vous souhaitez mettre à jour.
2. Dans **les liens connexes**, vous pouvez effectuer les tâches suivantes :

Option	Description
Afficher le Runbook manuel	Consultez une liste des guides d'exploitation disponibles pour cet incident de sécurité.
Workflow de réponses	Affichez tout workflow associé à cet incident.
Ajouter plusieurs éléments observables	Ajoute une liste d'observables au format délimité par des virgules, des retours à la ligne, des onglets ou des barres verticales.
Ajouter au ticket de sécurité	Ajoute l'incident de sécurité à un ou plusieurs tickets de sécurité. Vous pouvez également créer un nouveau ticket de sécurité et y ajouter cet incident de sécurité.
Obtenir les résumés IP de QRadar	Si une intégration QRadar est disponible et contient des CI valides, des adresses IP source et de destination, elle déclenche les workflows QRadar et affiche les résultats dans des notes de travail.
Exécuter l'orchestration	Choisissez et exécutez un workflow Security Operations.
Afficher la chronologie SLA	Vous pouvez afficher une chronologie SLA à partir d'un enregistrement SLA de tâche ou d'une définition de SLA.
Afficher toutes les listes connexes	Affiche toutes les listes connexes standard et toutes les listes ajoutées manuellement. **Remarque :** Les éléments ajoutés manuellement sont disponibles uniquement dans cette vue.
Afficher les éléments affectés	Affiche les listes de CI, d'utilisateurs et de services directement affectés par cet incident
Afficher les éléments connexes	Affiche les listes des incidents associés, des CI, des utilisateurs et des groupes affectés par cet incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Afficher IoC	Affiche les listes des observables, des indicateurs, des programmes malveillants, des modes et des méthodes, ainsi que des demandes d'analyse de sécurité associées à cet incident.
Afficher les données d'enrichissement	Affiche les listes des données d'enrichissement, des processus, des services, des statistiques, des recherches, des journaux de pare-feu et des informations utilisateur compromises associées à cet incident.
Afficher les tâches de réponse	Affiche les listes de tâches, les SLA, les audits de score de risque, les pannes et les recherches Exchange associées à cet incident.
Afficher les détails dans le système externe	Si cet incident de sécurité a été généré à partir d'une application externe, directement ou par événements, et qu'un lien vers les données d'origine a été fourni, l'action **Afficher les détails dans le système externe** ouvre l'URL. Vous pouvez afficher et rechercher dans les journaux qui ont généré cet incident.
Rechercher des vulnérabilités	S'il Réponse aux vulnérabilités est activé et que vous avez sélectionné au moins un CI affecté pour l'incident de sécurité, vous pouvez soumettre une demande d'analyse pour déterminer quelles vulnérabilités existent sur le CI.

Relations d'incident de sécurité parent et enfant

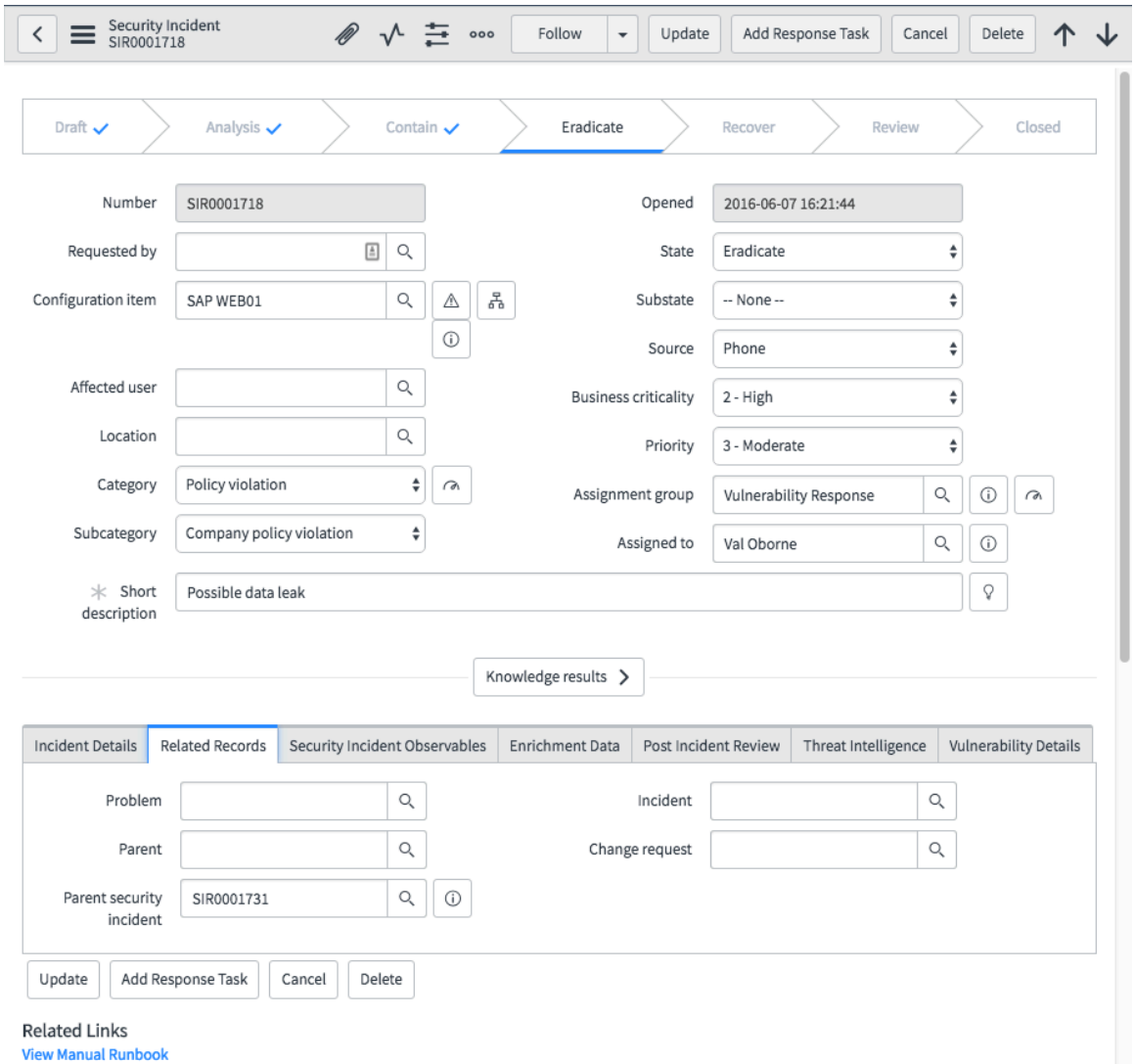
Vous pouvez associer et suivre l'impact d'un problème donné à l'aide des relations d'incident de sécurité parent et enfant dans Réponse aux incidents de sécurité.

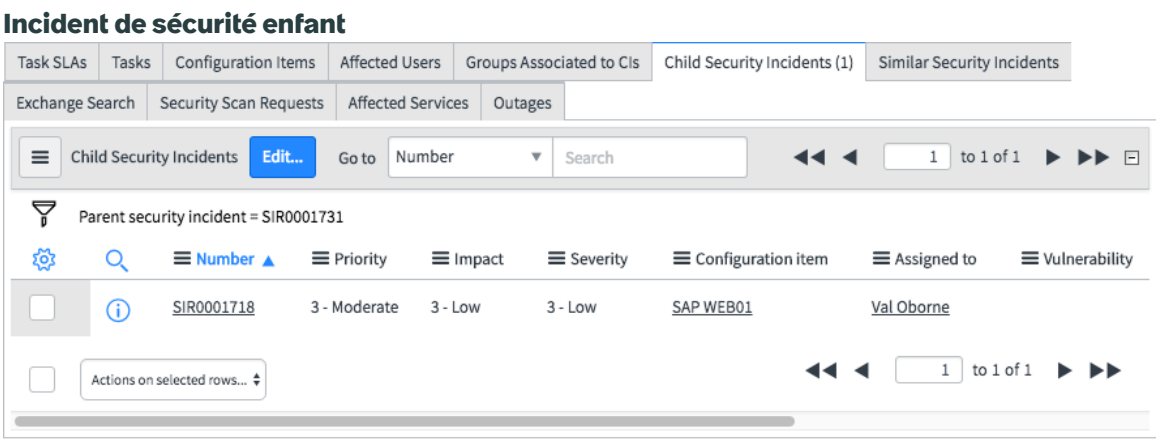
À l'aide de l'onglet **Enregistrements connexes** , vous pouvez ajouter un **problème d'incident de sécurité parent** à n'importe quel Réponse aux incidents de sécurité formulaire. Cette fonctionnalité fait automatiquement de l'incident un enfant qui apparaît dans l'onglet **Listes connexes - Incidents de sécurité enfants** du problème parent.

Remarque : Vous ne pouvez pas faire d'un incident de sécurité parent existant son propre enfant en utilisant le même numéro pour les deux incidents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



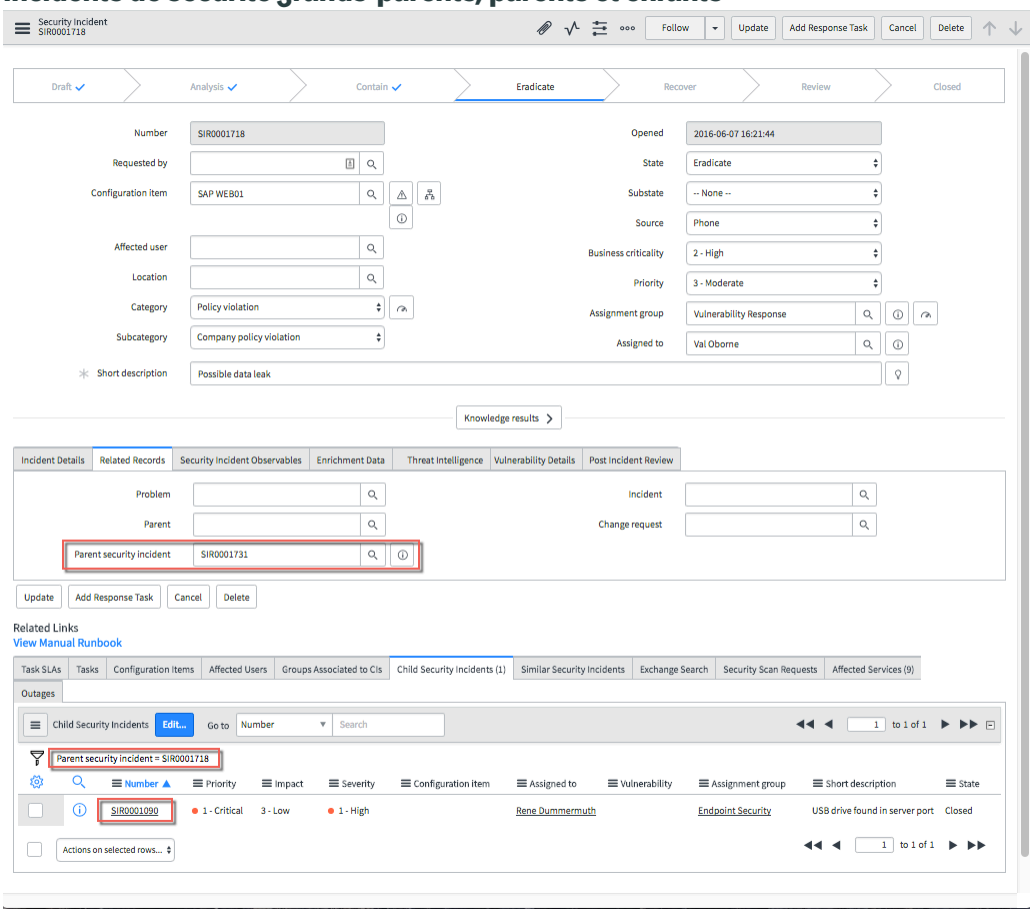


Vous pouvez également ajouter un ou plusieurs **incidents de sécurité enfants** à n'importe quel enregistrement d'incident de sécurité à l'aide du bouton **Modifier** de l'onglet **Incidents de sécurité enfants** . Dans l'exemple suivant, les trois enregistrements sont connectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incidents de sécurité grands-parents, parents et enfants



Remarque :

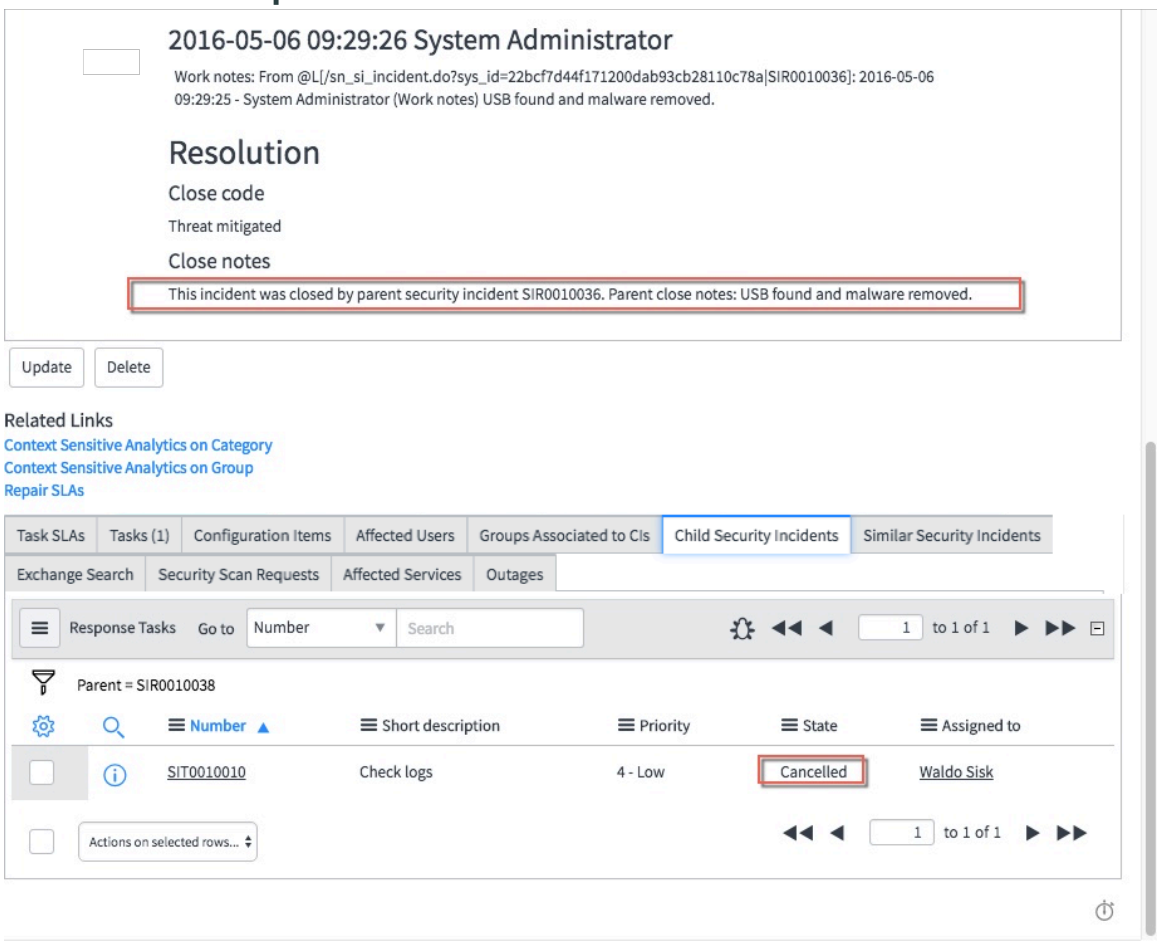
- Toutes les notes de travail enregistrées dans le parent sont propagées à tous les enfants actifs dans les **activités** sous l'onglet Détails de **l'incident** .
- Le champ **Parent** est utilisé pour associer l'incident de sécurité à un enregistrement parent, tel qu'un incident majeur, un problème ou une demande de changement, qui se trouve en dehors du module Incident de sécurité. Pour regrouper plusieurs incidents de sécurité en un incident de sécurité principal, le champ **Incident de sécurité parent** est utilisé.

Lorsqu'un parent est fermé ou annulé, tous les enfants actifs sont également fermés ou annulés. Toutes les **tâches de réponse** actives sur les incidents enfants sont annulées. **S'il** n'y a pas d'autres tâches ouvertes, l'incident enfant est fermé. Lorsqu'elle est fermée, **l'entretien post-incident** enregistre la fermeture et les informations trouvées dans l'onglet Informations sur la **fermeture** sont propagées du parent aux enfants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fermer la tâche de réponse enfant



Afficher les éléments affectés pour un incident de sécurité

Vous pouvez afficher les éléments affectés, tels que les CI, les utilisateurs affectés et les services affectés associés à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les éléments affectés.
2. Cliquez sur le lien connexe **Afficher les éléments affectés** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations relatives à l'incident de sécurité.

Onglet	Description
Éléments de configuration	Éléments de configuration (CI) affectés. Une fois les CI affectés identifiés, vous pouvez ajouter manuellement des ressources affectées à partir de cette liste connexe.
Utilisateurs affectés	Une fois les utilisateurs affectés identifiés, vous pouvez ajouter manuellement des utilisateurs affectés à partir de cette liste connexe.
Services affectés	Afficher ou ajouter des services d'entreprise associés à l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet	Description
	Remarque : Si un CI affecté est ajouté après l'ouverture de l'incident de sécurité, il est judicieux de cliquer avec le bouton droit dans l'en-tête du formulaire et de sélectionner **Actualiser les services impactés**.

Remarque : Si l'aptitude d'intégration Security Operations Integration - Obtenir l'exécution des processus est active et que vous ajoutez un CI à un incident de sécurité, le workflow Obtenir l'exécution des processus s'exécute et récupère une liste des processus en cours d'exécution sur le CI.

Si l'option d'intégration Intégration de Security Operations - Isoler l'hôte est active, vous pouvez sélectionner un ou plusieurs CI et restreindre leurs connexions système à d'autres appareils. Pour ce faire, cochez les cases correspondant aux CI et cliquez sur **Isoler l'hôte** dans la liste de choix **Actions sur les lignes sélectionnées** .

4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments connexes
   - Afficher IoC
   - Afficher les données d'enrichissement
   - Afficher les tâches de réponse
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Afficher les éléments connexes pour un incident de sécurité

Vous pouvez afficher les éléments connexes, tels que les incidents de sécurité similaires et enfants, les utilisateurs associés, les groupes de vulnérabilité et les éléments vulnérables associés à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les éléments connexes.
2. Cliquez sur le lien connexe **Afficher les éléments connexes** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations relatives à l'incident de sécurité.

Onglet	Description
Incidents de sécurité enfants	Sélectionnez un enregistrement de tâche lié au problème qui a causé la création de cet incident de sécurité.
Incidents de sécurité similaires	Affichez tout autre incident de sécurité associé à l'un des mêmes enregistrements observables.
Éléments de configuration associés	Affiche une liste des incidents de sécurité contenant des éléments de configuration avec le même observable que cet incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet	Description
	Cette liste peut être filtrée à l'aide du groupe **de filtres d'exclusions de CI** . Lorsqu'un observable est ajouté à un incident de sécurité, cette liste est automatiquement mise à jour. Par défaut, les observables dont le type de contexte est Destination sont exclus.
Utilisateurs associés	Affiche une liste des incidents de sécurité contenant des utilisateurs ayant les mêmes observables que cet incident de sécurité. Cette liste peut être filtrée à l'aide du groupe de filtres **d'exclusion d'utilisateurs** . Lorsqu'un observable est ajouté à un incident de sécurité, cette liste est automatiquement mise à jour. Par défaut, les observables dont le type de contexte est Destination sont exclus.
Groupe de filtres connexes	Une fois les éléments de configuration identifiés, tout CI ou groupe de filtres correspondant est automatiquement ajouté.
Groupes de vulnérabilité	Si Réponse aux vulnérabilités cette option est activée, vous pouvez afficher les groupes de vulnérabilité associés à cet incident de sécurité.
Éléments vulnérables	Si Réponse aux vulnérabilités cette option est activée, vous pouvez afficher les éléments de vulnérabilité associés à cet incident de sécurité.
Risques	Si l'un des modules d'extension de base de Risk Management (Policy and Compliance Management, Audit, Management ou Risk Management) est activé, vous pouvez afficher ou ajouter des risques associés à l'incident de sécurité. Vous pouvez ajouter cette liste connexe à partir du menu contextuel de l'en-tête du formulaire sous **Configurer** > **Listes connexes**.
Événements d'éléments de configuration	S'il Gestion des événements est activé, vous pouvez afficher les événements.
Alertes d'éléments de configuration	Si Gestion des événements cette option est activée, vous pouvez afficher les alertes.
Tickets du service clientèle	Si Service client cette option est activée, vous pouvez afficher les Service client informations du ticket.

Traduction automatique

4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments affectés
   - Afficher IoC
   - Afficher les données d'enrichissement
   - Afficher les tâches de réponse
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Afficher les données d'enrichissement pour un incident de sécurité

Vous pouvez afficher les données d'enrichissement, telles que les processus en cours et les services en cours d'exécution, ainsi que les statistiques réseau associées à un incident de sécurité.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité pour lequel vous souhaitez afficher les données d'enrichissement.
2. Cliquez sur le lien connexe **Afficher les données d'enrichissement** .
3. Cliquez sur l'une des listes connexes pour afficher ou ajouter des informations relatives à l'incident de sécurité.

   Remarque : Les détails des données brutes sont stockés dans une pièce jointe à l'enregistrement des données d'enrichissement. S'ils dépassent la limite de champ, les détails affichés sont tronqués.

Onglet	Description
Processus en cours	Stocke les enregistrements créés par le workflow Réponse aux incidents de sécurité **Obtenir l'exécution des processus** .
Services d'exécution	Stocke les enregistrements créés par le workflow Réponse aux incidents de sécurité **Obtenir des services d'exécution** .
Statistiques réseau	Stocke les enregistrements créés par le workflow Réponse aux incidents de sécurité **Obtenir les statistiques réseau** .
Recherches de domaine	Si le module d'extension est activé, il WhoisXML API Integration stocke les enregistrements créés par une recherche Whois.
Journaux du pare-feu	Stocke les données d'enrichissement à partir des journaux de pare-feu, tels que les journaux de pare-feu du réseau Palo Alto.
Info sur l'utilisateur compromis	Stocke les comptes identifiés comme étant compromis par un fichier Have I Been Pwned ? Recherche.

   Remarque : **L'onglet Données d'enrichissement de sécurité** affiche les données d'enrichissement brutes provenant de workflows, telles que la récupération des statistiques réseau ou l'exécution des Réponse aux incidents de sécurité processus. Cet onglet peut être affiché en cliquant sur le lien connexe **Afficher toutes les listes connexes** .
4. Cliquez sur l'un des liens connexes suivants pour mettre à jour l'incident de sécurité :
   - Afficher les éléments affectés
   - Afficher les éléments connexes
   - Afficher IoC
   - Afficher les tâches de réponse
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Afficher les informations sur la tâche de réponse pour un incident de sécurité

Vous pouvez afficher les informations sur les tâches de réponse, telles que les SLA de tâche, les audits de score de risque et les pannes associées à un incident de sécurité.

Avant de commencer
Rôle requis : sn_si.basic

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. S’il n’est pas déjà ouvert, ouvrez l’incident de sécurité pour lequel vous souhaitez afficher les tâches de réponse.
2. Cliquez sur le lien connexe **Afficher les tâches de réponse** .
3. Cliquez sur l’une des listes connexes pour afficher ou ajouter des informations relatives à l’incident de sécurité.

Onglet	Description
Tâches	Affiche les tâches déjà définies pour l’incident de sécurité. Vous pouvez créer manuellement une tâche de réponse.
Tâches de réponse	Affiche les actions à effectuer en réponse à l’incident de sécurité.
SLA de tâche	Affichez ou ajoutez des SLA de tâche actifs qui ont été définis pour l’incident de sécurité.
Audits de score du risque	Un enregistrement d’audit pour chaque instance de changement de score de risque.
Pannes	Affichez ou ajoutez manuellement de nouveaux enregistrements de panne associés à l’incident de sécurité.
Recherche d'e-mail	Liste des enregistrements contenant des critères de recherche pour exécuter des requêtes sur un serveur de messagerie, tel que Microsoft® Exchange Server (en fonction de l’implémentation installée), et stockant les résultats reçus. **Remarque :** Si le n’est Security Operations Integration : option de recherche et de suppression d’e-mails pas actif, le lien connexe **de recherche d’e-mail** n’est pas affiché.

4. Cliquez sur l’un des liens connexes suivants pour mettre à jour l’incident de sécurité :
   - Afficher les éléments affectés
   - Afficher les éléments connexes
   - Afficher IoC
   - Afficher les données d'enrichissement
5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Afficher les événements et alertes associés aux incidents de sécurité

Pendant qu’un incident de sécurité est en cours de traitement, vous pouvez afficher les détails des événements. Pour les alertes, vous pouvez les afficher et les authentifier, et créer des incidents ou des incidents de sécurité à partir de celles-ci si nécessaire.

Avant de commencer

Le module d’extension Security Incident Response Event Management Support doit être activé.

Rôle requis : si.sn_agent

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à une liste d'incidents de sécurité (par exemple, **Tous** > **Incident de sécurité** > **Incidents** > **Incidents non affectés**).
2. Si les ressources affectées par l'incident de sécurité que vous visualisez ont reçu des alertes ou des événements au cours des 24 dernières heures, l'une des listes connexes suivantes ou les deux s'affichent.
   - Alertes d'incident de sécurité CI
   - Événements CI d'incidents de sécurité
3. Cliquez sur la liste connexe que vous souhaitez afficher.

Liste connexe	Description
Alertes d'incident de sécurité CI	Vous pouvez afficher les détails des alertes reçues au cours des 24 dernières heures. Vous avez la possibilité de cliquer sur **Confirmer** pour indiquer que vous êtes au courant de l'alerte et qu'elle est traitée. Utilisez **Fermer** pour indiquer que l'alerte n'est pas importante.
Événements CI d'incidents de sécurité	Vous pouvez afficher les détails de l'événement reçu au cours des 24 dernières heures.

Afficher l'incident de sécurité vers le mappage du ticket du service clientèle

Réponse aux incidents de sécurité est fourni avec un mappage de champs par défaut qui mappe un incident de sécurité à un Service client ticket. Vous pouvez afficher la carte par défaut de l'incident de sécurité par rapport au ticket CS.

Avant de commencer

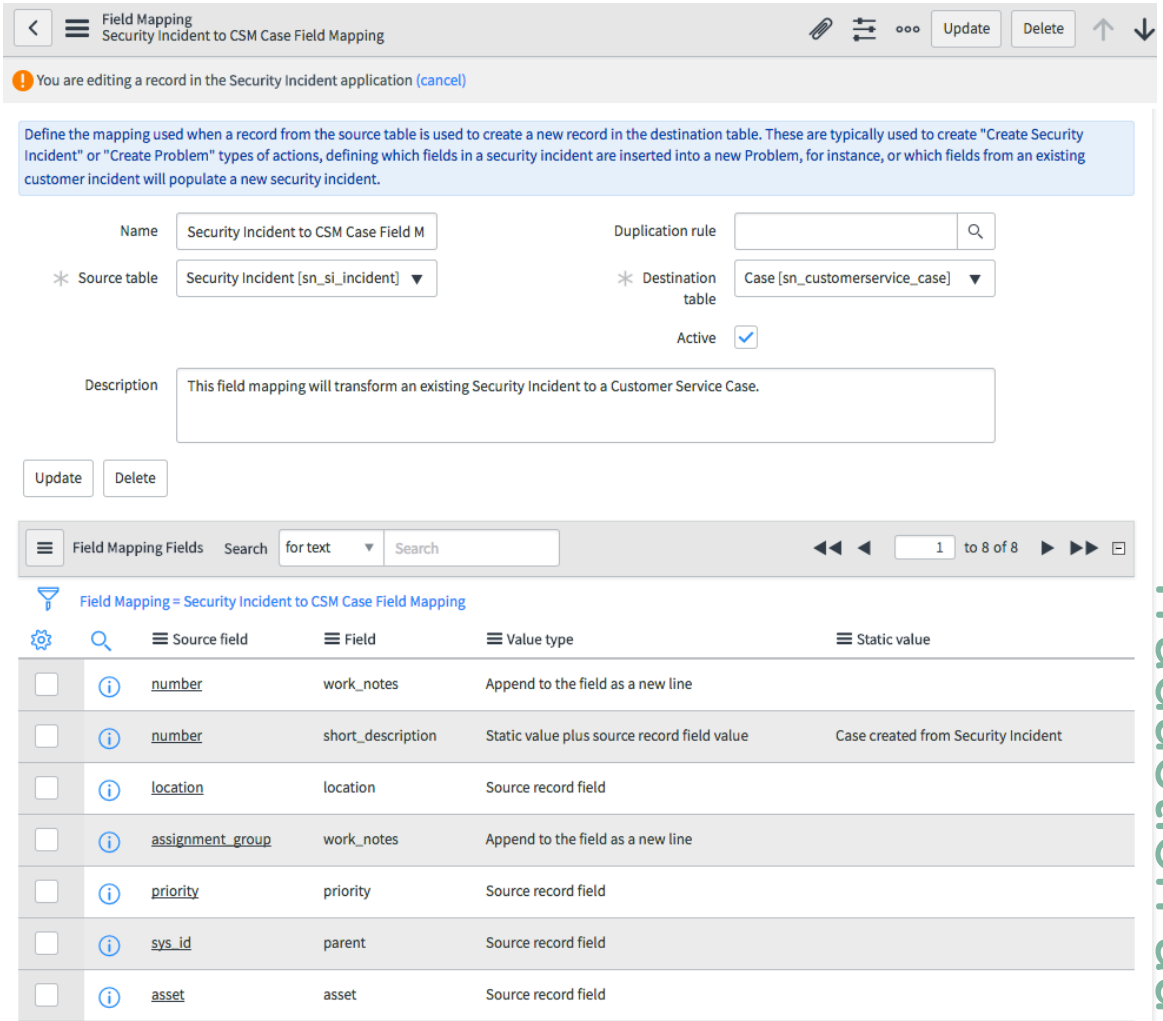
Rôle requis : sec_cmn.read

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Mappage de champs**.
2. Cliquez sur **Mappage de champ d'incident de sécurité à Mappage de champ de ticket CSM** pour afficher la carte par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Vous pouvez modifier le mappage, si nécessaire.
4. Lorsque vous avez terminé vos modifications, cliquez sur **Mettre à jour**.

Afficher un Runbook de Security Incident Response

Les Runbooks vous donnent accès aux procédures liées aux tâches sur lesquelles vous travaillez.

Avant de commencer

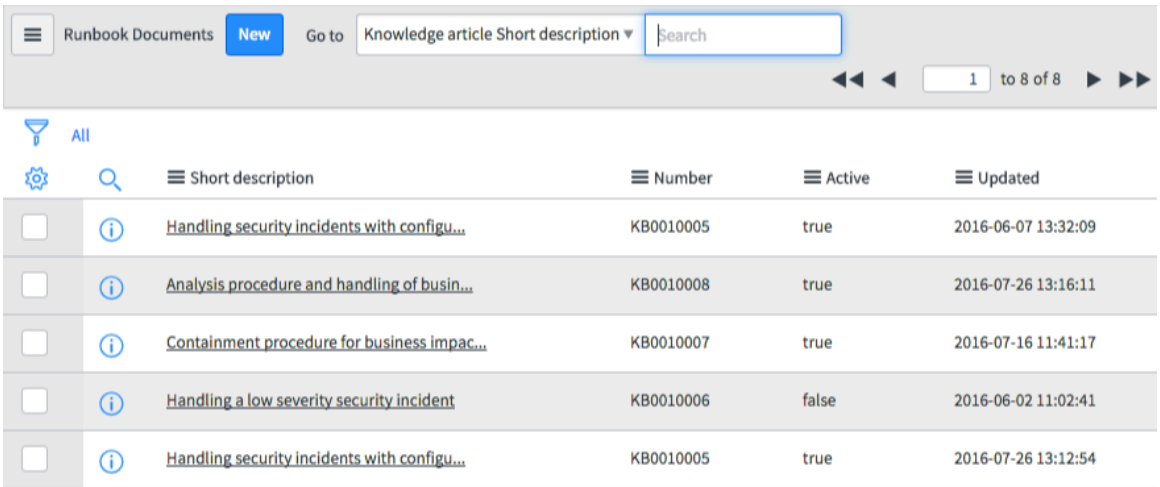
Rôle requis : sn.si.knowledge_admin

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Runbook manuel** > **Afficher les documents Runbook**.
2. Sélectionnez un runbook dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour créer un runbook, cliquez sur **Nouveau**.
   Pour plus d'informations, consultez Créer un runbook.

Identifier tous les éléments de configuration affectés par un incident de sécurité

Si vous savez quelle ressource (serveur, bureau ou autre élément de configuration) est à l'origine d'un incident de sécurité et que vous souhaitez identifier les ressources connexes et les services d'entreprise qui peuvent être affectés, vous pouvez utiliser la carte Gestion des services d'entreprise (BSM).

Avant de commencer

Rôle requis : admin ou sn_si.admin

Pourquoi et quand exécuter cette tâche

La carte BSM affiche les dépendances en amont et en aval d'un CI racine sélectionné.

Il existe deux méthodes que vous pouvez utiliser pour afficher la carte BSM d'un CI :

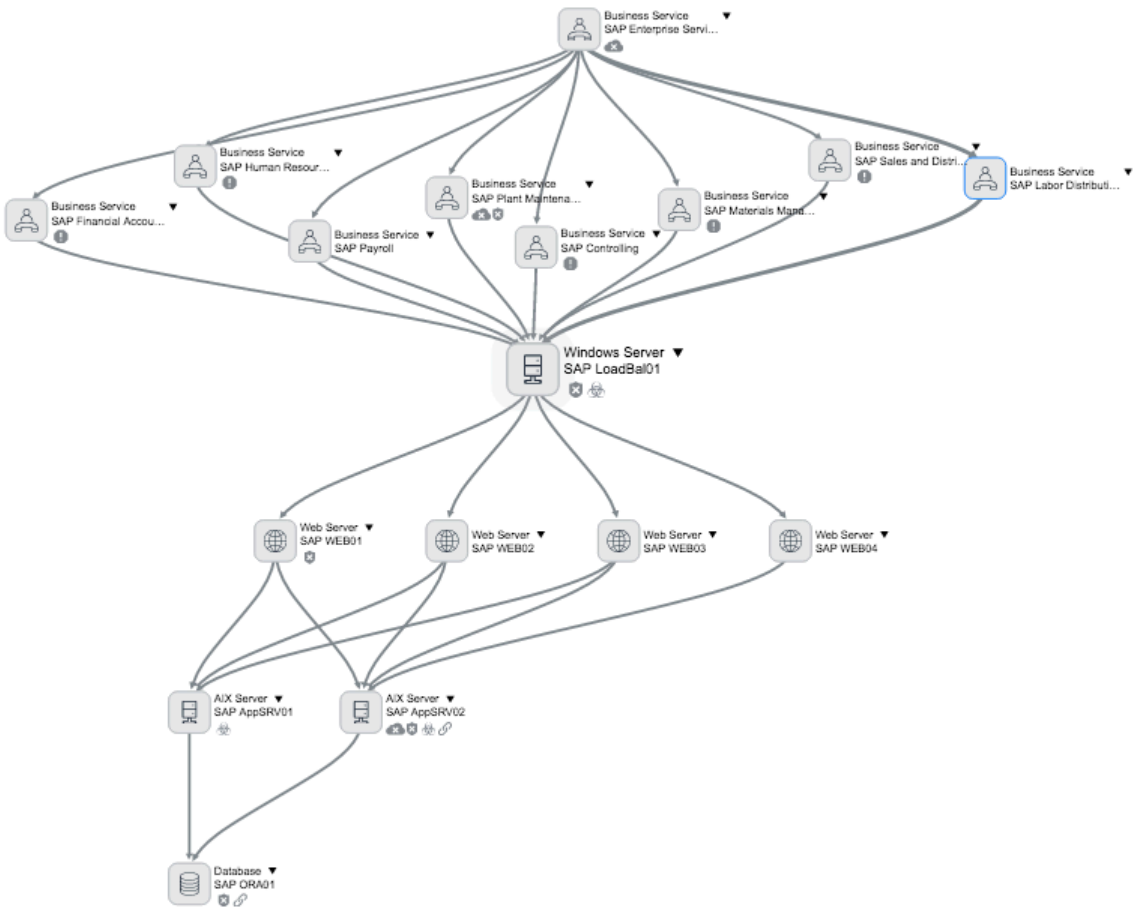
- Si vous souhaitez afficher les CI dans le contexte d'une tâche, à partir du formulaire d'incident de sécurité.
- Si vous ne souhaitez pas afficher les CI du point de vue d'une tâche, effectuez une vue à partir de la barre de navigation.

Procédure

1. Dans le formulaire Incident de sécurité, renseignez le champ **Élément de configuration** , puis cliquez sur l'icône de carte BSM ( ).
   L'écran de carte BSM affiche la carte du dernier incident auquel vous avez accédé dans Gestion des incidents ou du dernier incident de sécurité auquel vous avez accédé dans Gestion des incidents de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Cliquez sur les icônes en regard d'un élément de configuration pour afficher différents types de détails sur la ressource (serveur, bureau ou autre CI).
   Par exemple, cliquez sur (icône ⚠) pour afficher les alertes associées au CI.

   Remarque : Pour afficher une liste de toutes les icônes disponibles, cliquez sur **Filtres** au-dessus de la carte BSM et développez **Filtrer les types de tâches**.

3. Pour organiser la carte dans différentes configurations, sélectionnez l'un des formats répertoriés au-dessus de la carte (**Vertical**, **Horizontal**, **Radial**) ou cliquez sur **Filtres** pour filtrer la carte afin de faciliter l'affichage.

4. Si vous avez ouvert la carte BSM à partir du formulaire d'incident de sécurité, vous pouvez ajouter un CI dépendant à l'incident de sécurité en cliquant avec le bouton droit sur le CI et en sélectionnant **Ajouter les CI affectés**.
   Vous pouvez également ajouter plusieurs CI à la fois. Faites glisser une zone autour des CI que vous souhaitez ajouter, cliquez avec le bouton droit sur la zone et sélectionnez **Ajouter les CI affectés**.
   Les CI sont ajoutés à la liste connexe CI affectés de l'incident de sécurité.

Calculer la gravité d'un incident de sécurité

Vous pouvez calculer la gravité d'un incident de sécurité à l'aide de calculateurs prédéfinis.

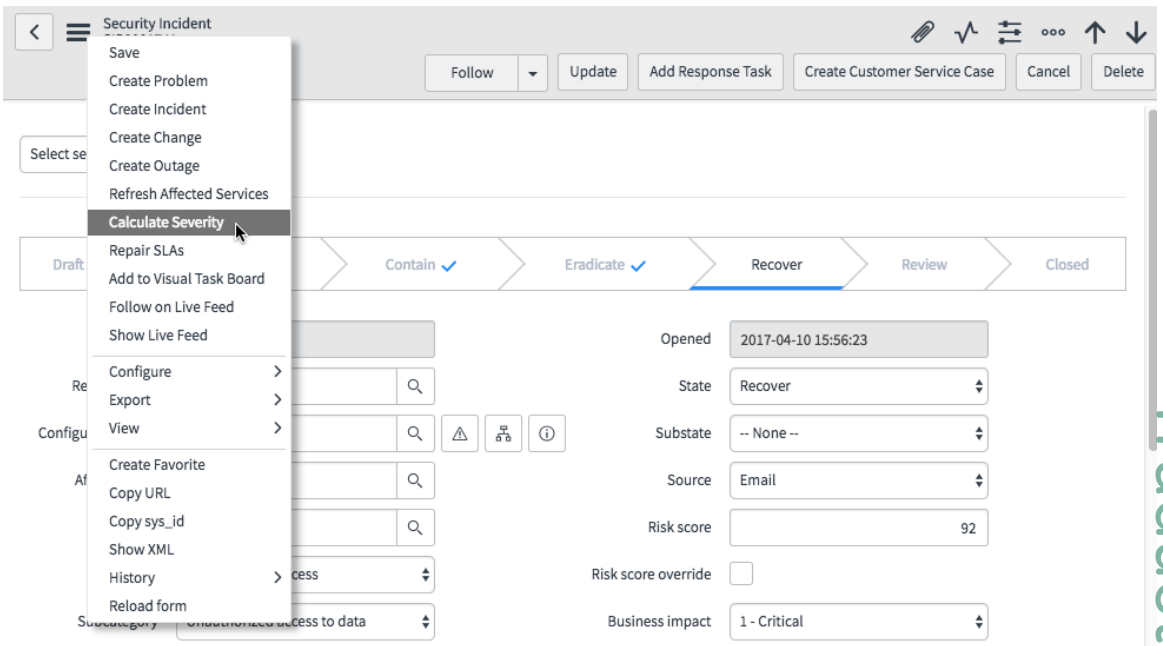
Avant de commencer
Rôle requis : sn_si.basic

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. S’il n’est pas déjà ouvert, ouvrez l’incident de sécurité dont vous souhaitez calculer la gravité.
2. Cliquez sur le menu contextuel de l’en-tête du formulaire et sélectionnez **Calculer la gravité** :



La gravité est calculée en fonction des règles prédéfinies pour les calculateurs de base. Pour plus d'informations, consultez Comprendre les calculateurs d’incidents de sécurité.

Rechercher et supprimer des e-mails d’hameçonnage

La suppression des e-mails d’hameçonnage peut aider à réduire l’exposition à une attaque spécifique au sein d’une organisation. Vous pouvez gérer les e-mails d’hameçonnage sur votre serveur de messagerie en les recherchant, en les accordant et en les supprimant.

Avant de commencer

Rôles requis : sn_sec_cmn.cap_email_read

Vous pouvez déterminer combien d’utilisateurs ont été ciblés par une attaque de phishing en interrogeant un enregistrement d’e-mail associé à un incident de sécurité.

Logiciels pris en charge :

- Serveur Microsoft® Exchange 2010

Limitation : Lorsque vous recherchez le corps des e-mails, vous pouvez rechercher un maximum de 1 500 boîtes aux lettres.

Pourquoi et quand exécuter cette tâche

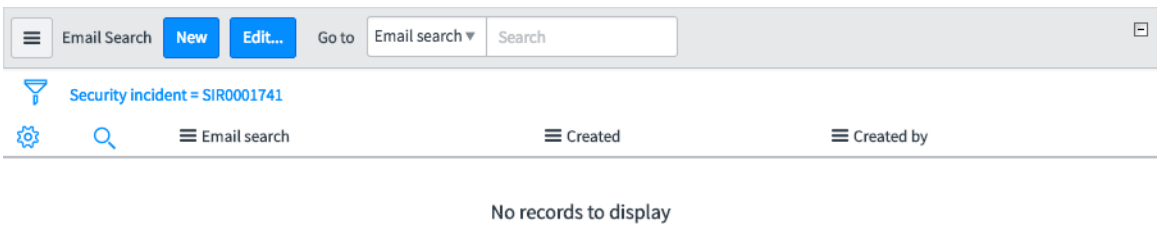
Cette fonctionnalité est utilisée par le Security Operations Integration : flux de recherche et de suppression d’e-mails pour exécuter une requête sur votre serveur de messagerie. En fonction des critères de recherche que vous sélectionnez, la recherche identifie tous les e-mails figurant dans une attaque de phishing et renvoie le nombre total d’e-mails affectés ou les détails des e-mails affectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

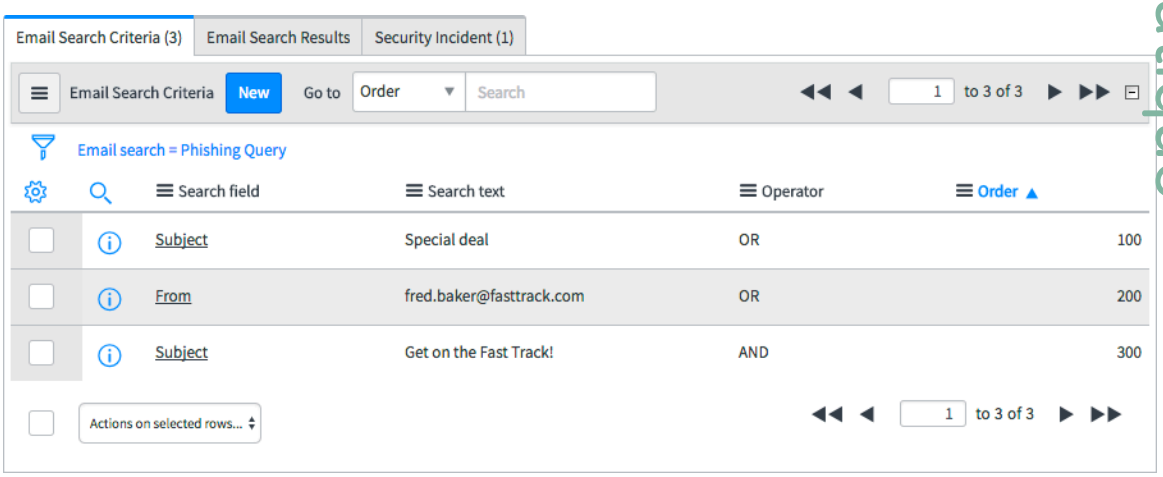
1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. Choisissez un incident de sécurité.
3. Si la liste connexe **Recherche d'e-mails** n'est pas visible, cliquez sur le lien connexe **Afficher tous les liens connexes** .
4. Cliquez sur la liste connexe **Recherche d'e-mails** .



5. Cliquez sur **Nouveau**.
6. Renseignez les champs comme il convient.

Champ	Description
Nom	Nom de la requête de recherche
Requête à partir de critères	Un aperçu de la requête exécutée sur le serveur de messagerie. Généré à partir de tous les enregistrements de critères de recherche actifs associés.
Description	Décrivez ce que la requête de recherche recherche.

7. Faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.



8. Cliquez sur l'onglet **Critères de recherche d'e-mails** , puis sur **Nouveau**.
9. Renseignez ou modifiez les champs, selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Recherche d'e-mail	Affiche le nom de la recherche d’e-mails. Vous pouvez le modifier si nécessaire.
Champ de recherche	Champ à rechercher dans le serveur de messagerie. Le champ de recherche propose les choix suivants : **Objet** Ce critère recherche les e-mails qui contiennent le texte de la ligne d’objet spécifié dans le champ **Texte de recherche** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d’e-mails d’hameçonnage et les détails de chaque e-mail, y compris la date de réception de l’e-mail, l’état de lecture de l’e-mail, le destinataire et l’ID du message, sont renvoyés. **De** Ce critère recherche les e-mails qui contiennent l’adresse e-mail complète de l’expéditeur (par exemple, jane.doe@abc.com) spécifiée dans le champ de **texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d’e-mails d’hameçonnage et les détails de chaque e-mail, y compris la date de réception de l’e-mail, l’état de lecture de l’e-mail, le destinataire et l’ID du message, sont renvoyés. **Remarque :** Vous ne pouvez pas utiliser les champs **De** et **Destinataire** dans la même requête. **Destinataire** Ce critère recherche les e-mails qui contiennent l’adresse e-mail complète du destinataire (par exemple, john.doe@abc.com) spécifiée dans le champ de **texte Rechercher** . Il recherche également les e-mails dans les champs À, Cc et Cci. Pour les e-mails qui répondent à ces critères de recherche, le nombre total d’e-mails d’hameçonnage et les détails de chaque e-mail, y compris la date de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

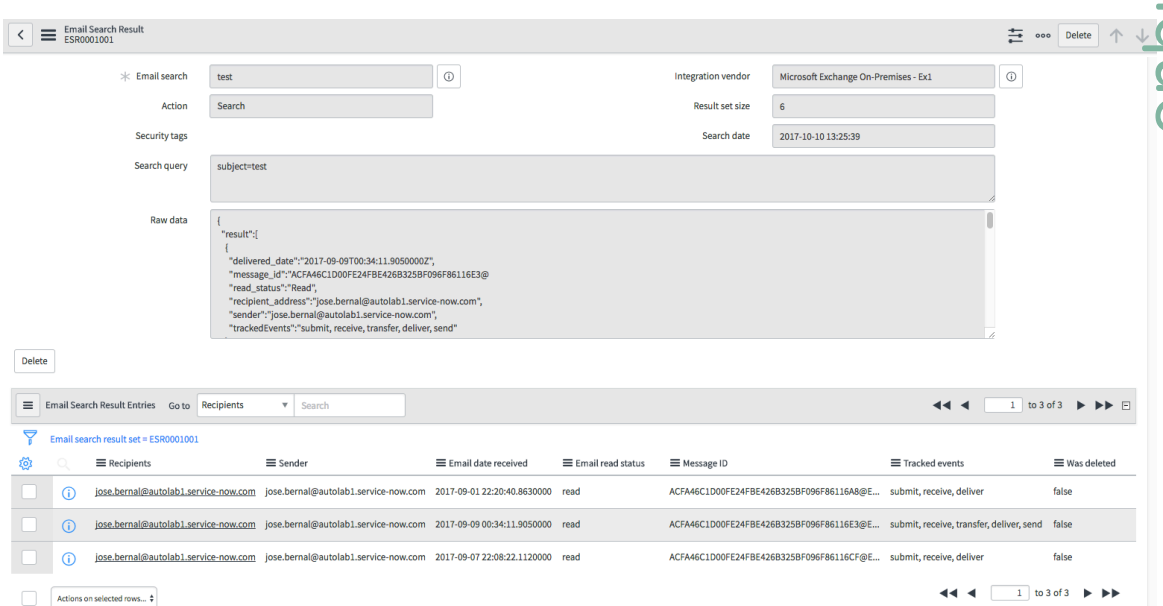
Champ	Description
	réception de l’e-mail, l’état de lecture de l’e-mail, le destinataire et l’ID du message, sont renvoyés. **Remarque :** Vous ne pouvez pas utiliser les champs **De** et **Destinataire** dans la même requête. **Détails** Ce critère recherche les e-mails qui contiennent le corps de texte spécifié dans le champ **Texte de recherche** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d’e-mails d’hameçonnage est renvoyé. **Remarque :** Lorsque vous recherchez le corps des e-mails, vous pouvez rechercher un maximum de 1 500 boîtes aux lettres. **Cc :** Ce critère recherche les e-mails qui contiennent l’adresse e-mail complète Cc (ex : jane.doe@abc.com) spécifiée dans le champ de **texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d’e-mails d’hameçonnage est renvoyé. **Bcc:** Ce critère recherche les e-mails qui contiennent l’adresse e-mail complète Cci (ex : jane.doe@abc.com) spécifiée dans le champ de **texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d’e-mails d’hameçonnage est renvoyé. **Pièce jointe** Ce critère recherche les e-mails qui contiennent le nom de fichier de la pièce jointe ou le contenu de la pièce jointe spécifié dans le champ de **texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d’e-mails d’hameçonnage est renvoyé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Seules les pièces jointes en texte brut sont prises en charge pour la recherche du contenu des pièces jointes. **Politique de rétention** Ce critère recherche les e-mails qui contiennent des numéros de politique de conservation spécifiés dans le champ **de texte Rechercher** . Pour les e-mails qui répondent à ces critères de recherche, le nombre total d'e-mails d'hameçonnage est renvoyé.
Actif	Cochez cette case pour activer cette requête de recherche d'e-mail.
Opérateur	Les valeurs possibles sont AND et OR. Vous pouvez définir comment les critères de recherche sont combinés pour s'exécuter dans le serveur de messagerie.
Ordre	Ordre dans lequel la requête de recherche est créée à partir des critères de recherche.
Texte de recherche	Le texte à rechercher. Les guillemets simples, les guillemets doubles et les deux-points ne sont pas pris en charge.

10. Cliquez sur **Envoyer**.
11. Répétez l'opération au besoin pour définir des critères de recherche supplémentaires.
12. Vous pouvez afficher les résultats de la recherche en cliquant sur l'onglet Résultats de recherche **d'e-mails** .

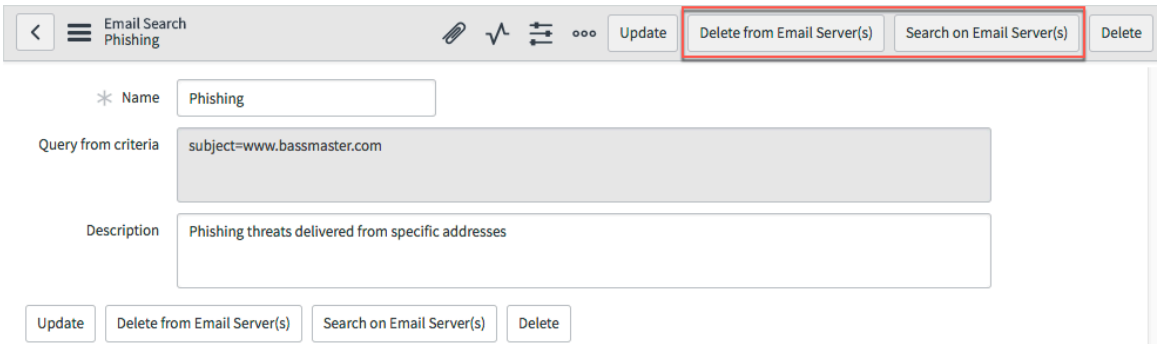


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chaque ligne du formulaire Entrées des résultats de recherche d'e-mail représente un e-mail distinct.

13. Une fois que vous avez créé un enregistrement de critères de recherche, deux boutons apparaissent dans le formulaire Recherche d'e-mail : **Supprimer des serveurs de messagerie** et **Rechercher sur les serveurs de messagerie**.



14. Pour rechercher des e-mails dans le serveur sélectionné qui répondent aux critères de recherche que vous avez définis, cliquez sur **Rechercher sur le(s) serveur(s) de messagerie**.

Créer un article de la base de connaissances sur les incidents de sécurité

Lorsque vous travaillez avec des incidents de sécurité et des tâches de réponse, les articles de la base de connaissances s'affichent automatiquement pour fournir des informations pertinentes sur la tâche que vous effectuez. Votre organisation peut créer et gérer des articles dans la base de connaissances sur les incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.knowledge_admin

Pourquoi et quand exécuter cette tâche

Les articles de la base de connaissances partagent des informations sur la sécurité, documentent les types de cybermenaces auxquelles votre organisation est confrontée et fournissent des réponses et des réponses à ces menaces.

Si nécessaire, vous pouvez organiser les articles de la base de connaissances en runbooks, qui créent des associations entre les articles et des tâches spécifiques. Par exemple, vous pouvez configurer un Runbook avec des conditions qui entraînent l'affichage d'un article de la base de connaissances sur le hameçonnage lorsque vous créez un incident de sécurité pour une attaque de hameçonnage. Pour plus d'informations, consultez Créer un Runbook de réponse aux incidents de sécurité.

Les articles de la base de connaissances dans les Runbooks peuvent également être associés à des tâches spécifiques dans un playbook. Pour plus d'informations, consultez Associer un article de la base de connaissances à une tâche de playbook.

Les avantages des articles de la base de connaissances comprennent ce qui suit.

- Les employés ont une source d'information facile à consulter.
- Les informations peuvent être tenues à jour, car les articles de la base de connaissances ont un cycle de vie défini : création, révision et mise à jour, publication et mise hors service.
- Lorsque vous créez manuellement une demande de sécurité, un incident ou une tâche de réponse, une liste d'articles pertinents s'affiche lorsque vous saisissez la brève description.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Il est important d'affecter un gestionnaire des connaissances à chaque base de connaissances sur les incidents de sécurité.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Catalogue et base de connaissances** > **Base de connaissances**.
2. Cliquez sur l'icône Créer un article ( ).
3. Renseignez les champs du formulaire comme il convient.

Formulaire de connaissances

Champ	Description
Numéro	Numéro de la base de connaissances généré automatiquement.
Base de connaissances	La base de connaissances sélectionnée pour cet article.
Catégorie	Catégorie de cet article.
Publié	Date de publication de cet article de la base de connaissances. Cette valeur est définie lors de la création de l'article et mise à jour lorsque l'article est publié.
Date de fin de validité	Lorsque cet article de la base de connaissances expire. Cet article n'apparaîtra plus dans les résultats de recherche après cette date ou si une date n'est pas sélectionnée.
Image	Image qui s'affiche à côté de l'article lors d'une recherche à partir du portail de la base de connaissances hérité.
Workflow	[Lecture seule] État de publication de l'article, tel que Brouillon ou Publié. Quand Lors de l'insertion d'un nouvel article à partir d'un article existant, l'état du nouvel article est réinitialisé à **Brouillon**.
Source	Tâche pour laquelle cet article de la base de connaissances a été créé (le cas échéant). Ce champ est défini automatiquement lorsque vous créez l'article de la base de connaissances à partir d'un enregistrement de tâche.
Lien de la pièce jointe	Cochez la case pour télécharger automatiquement un fichier joint lorsqu'un utilisateur accède à l'article, au lieu d'ouvrir la vue de l'article. Ajoutez une pièce jointe à l'article pour utiliser cette option.
Afficher les pièces jointes	Cochez la case pour afficher les pièces jointes aux utilisateurs qui consultent cet article de la base de connaissances. Les pièces jointes apparaissent sous le texte de l'article. Ajoutez une ou plusieurs pièces jointes à l'article pour utiliser cette option.
Description brève	Titre de l'article. Ce titre s'affiche lors de la navigation et de la recherche dans la base de connaissances et en haut de l'article.
Texte	Contenu de l'article. Utilisez l'éditeur HTML WYSIWYG pour créer du contenu. Un aperçu du contenu s'affiche lors du parcours et de la recherche dans la base de connaissances.

Remarque : Si vous créez un article de la base de connaissances à associer à une tâche de playbook, définissez le champ Base de **connaissances** sur **Runbook de Réponse aux incidents de sécurité**.

4. Cliquez sur **Soumettre** pour créer l'article.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Toutes les étapes supplémentaires requises pour publier l'article, telles que les approbations, dépendent des Workflow de publication de la base de connaissances.

Information associée

Créer un Runbook de réponse aux incidents de sécurité

Escalader un incident de sécurité

Si un chemin d'escalade existe pour un incident de sécurité, le bouton Escalader est disponible dans l'en-tête de l'incident de sécurité.

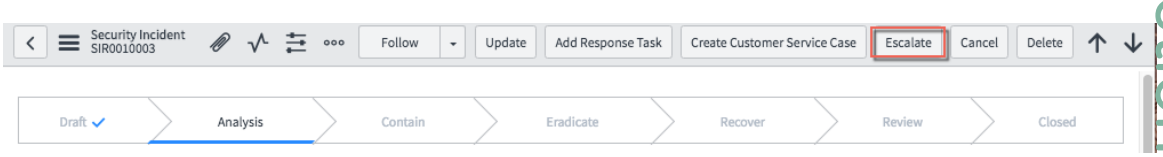
Avant de commencer

Rôle requis : sn_si.admin

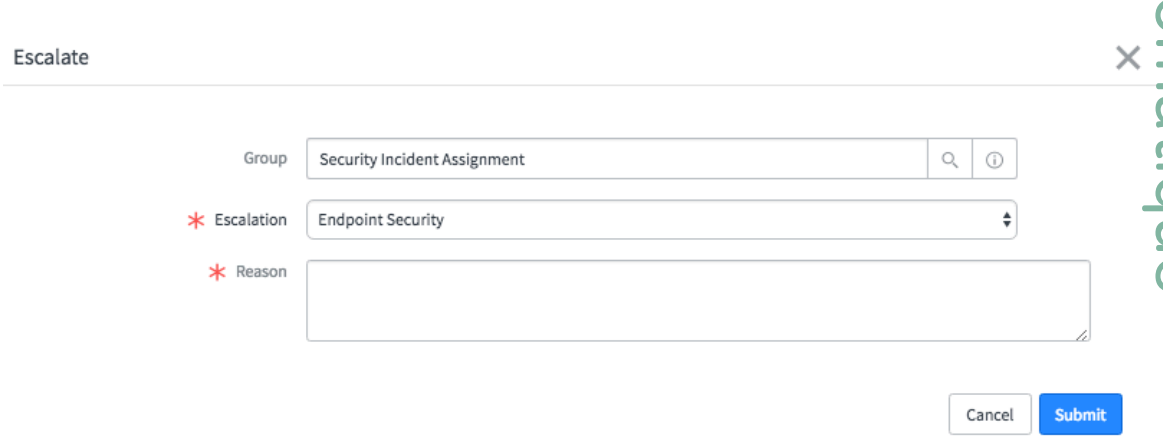
Vous devez avoir créé un groupe d'escalade pour voir ce bouton. Consultez Créer un groupe d'escalade Opérations de sécurité défini par l'utilisateur pour plus d'informations.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. Ouvrez l'incident que vous souhaitez escalader.
3. Cliquez sur le bouton **Escalader** .



4. Choisissez un groupe d'escalade.
5. Saisissez un motif pour l'escalade.



6. Cliquez sur **Envoyer**.
   Met à jour le **groupe d'affectation** et **Affecté à** sur l'incident de sécurité.

Gérer les activités post-incident

En fonction des besoins de votre entreprise, il est souvent nécessaire d'examiner l'origine et le traitement des incidents de sécurité.

La Revue post-incident fonctionnalité fournie fournit ServiceNow de nombreux outils pour automatiser, suivre, auditer et simplifier ce processus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette section décrit les éléments suivants :

- Affecter des rôles de revue post-incident
- Configurer une condition de déclenchement d'évaluation
- Effectuer une revue post-incident basée sur un questionnaire
- Créer des règles d'affectation PIR
- Rapport d'examen post-incident

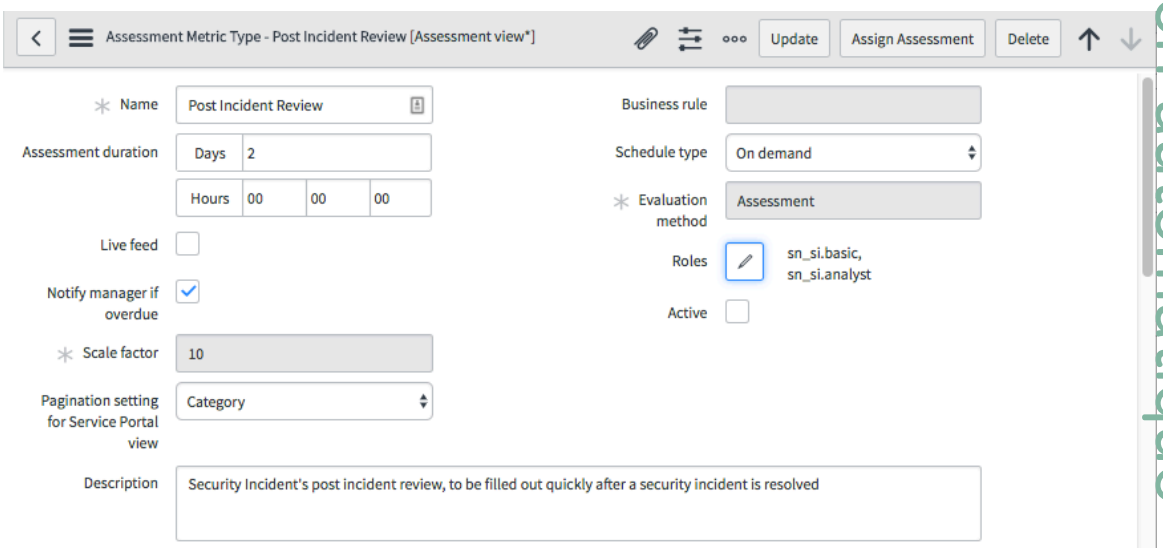
Affecter des rôles de revue post-incident

Vous pouvez cibler des questions sur des groupes prédéfinis spécifiques en affectant des rôles à des catégories de revue post-incident (PIR).

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Évaluations** > **Définition de la mesure** > **Types**.
2. Dans la colonne **Types** , recherchez un enregistrement de **revue post-incident** .
3. Ouvrez l'enregistrement.
4. Affectez un ou plusieurs rôles à cette catégorie de questions.



5. Cliquez sur **Mettre à jour**.
6. Accédez à la **Administration utilisateurs** > **Utilisateurs**.
7. Choisir un utilisateur
8. Ajoutez un ou plusieurs rôles de type mesure à l'enregistrement utilisateur.

> **Remarque :** Les rôles doivent correspondre aux rôles affectés dans la catégorie Revue post-incident.

Rapport d'examen post-incident

La fonctionnalité Rapports de revue post-incident (PIR) vous permet de configurer et de télécharger les rapports de revue post-incident à l'aide de l'onglet Revue post-incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'administrateur de sécurité peut créer et configurer les modèles de rapport et mapper ces modèles à l'incident de sécurité à l'aide de la configuration du rapport. Un analyste de sécurité peut ensuite consulter ou télécharger le rapport une fois que l'incident de sécurité est résolu et que l'état est mis à jour sur l'état Révision.

Un rapport PDF est généré et joint à l'incident de sécurité lorsque l'incident passe à l'état Fermé après une configuration réussie.

Remarque : La fonctionnalité de rapports est applicable et prise en charge à partir d'Orlando Patch9.

Pour personnaliser vos rapports de revue post-incident, vous devez effectuer la configuration suivante.

1. **Modèles de rapport** : personnalisez et configurez les fonctionnalités de modèle de rapport suivantes pour ajouter des informations supplémentaires au rapport :
   a. Chronologie
   b. Marques
   c. Scripts de modèle
2. **Configuration du rapport**

Cette section décrit la procédure de configuration :

Modèles de rapports

Utilisez la section Modèles de rapport pour créer des modèles de rapport primaires et supplémentaires appliqués aux incidents de sécurité en vue de générer le rapport de revue post-incident. Vous pouvez formater et configurer le rapport en fonction de vos besoins. Les modèles vous aident également à inclure les détails de l'évaluation dans le modèle.

Voici quelques étapes facultatives qui peuvent être effectuées lors de la création du modèle :

1. Configuration des informations de marque.
2. Configurer la taille et la marge de la page.
3. Ajout de champs liés aux incidents de sécurité (personnalisés et standard)
4. À l'aide des jetons personnalisés prédéfinis suivants :
   a. `$sessionUser`: renvoie le nom d'utilisateur connecté
   b. `$date`: renvoie la date actuelle
   c. `$if_not_null_start & $if_not_null_end`: si ces balises sont utilisées sur n'importe quel champ, les balises sont affichées uniquement si la valeur existe. Par exemple :
      - `${if_not_null_start:problem}`
      - `Problem Category: ${problem.category}`
      - `${if_not_null_end:problem}`
5. Inclusion des données de la liste connexe à l'aide des scripts de modèle. Pour plus d'informations, consultez la section ci-dessous sur les **scripts de modèle**.
6. Inclusion des informations de chronologie à l'aide des filtres de chronologie. Pour plus d'informations, consultez la section ci-dessous sur la **chronologie**.
7. Gestion et mise en forme du contenu du modèle, comme les pièces jointes, les tableaux et les images.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les fonctionnalités améliorées de la barre d'outils du modèle de rapport sont disponibles uniquement à partir de la version Paris.

Points clés des modèles de rapports :

1. Les images jointes au modèle de rapport ne sont affichées dans le rapport de revue post-incident que lorsqu'elles sont incluses dans la table sys_attachment.

   Remarque : Les images sélectionnées dans la table des db_image ne seront pas affichées dans le rapport de revue post-incident.

2. Les vidéos ne sont pas prises en charge dans le rapport de revue post-incident.
3. Les URL dans le PDF ne sont pas cliquables. Pour activer les URL, non cliquable (.) est notée (point).
4. Le rapport n'est pas généré si la taille du modèle de rapport dépasse 50 Mo.
5. La famille de polices sélectionnée pour le contenu du modèle de rapport n'est pas appliquée au PDF si elle n'est pas prise en charge par le générateur PDF.

   Remarque : Si la police correspondante n'est pas là, le générateur de PDF identifie la police alternative la plus proche, puis génère le PDF.

6. Si vous indiquez des valeurs de marge de page plus élevées, la génération du rapport de revue post-incident a échoué. Par exemple, la marge supérieure et inférieure > 450 et la marge gauche et droite > 450.
7. Si un texte volumineux est inclus dans le modèle de rapport sans espace, le texte peut être tronqué. Prévisualisez le texte et modifiez-le en conséquence.

L'administrateur de sécurité peut prévisualiser le rapport à l'aide du bouton **Afficher un aperçu du rapport** disponible sur la page Modèle de rapport.

Remarque :

Sélectionnez un incident de sécurité pour prévisualiser un rapport avec cette option de modèle, puis cliquez sur **Afficher un aperçu du rapport**.

Marques

Vous pouvez ajouter le nom du modèle de marque, l'image d'en-tête et de pied de page, le texte d'en-tête et de pied de page, générer des numéros de page et inclure l'enregistrement de marque dans le modèle de rapport après sa création.

Voici un exemple de format de rapport de marque :

Points clés de la personnalisation du modèle de rapport :

1. La taille maximale autorisée pour l'image d'en-tête et de pied de page est de 5 Mo. Si la taille dépasse la limite spécifiée, un message d'erreur « Le format d'image ne peut pas être reconnu » s'affiche dans l'incident de sécurité.
2. La longueur du texte du pied de page est limitée à 100 caractères.
   a. Si le texte de l'image du pied de page et le contenu du rapport se chevauchent lors de la prévisualisation, vous devez apporter des modifications à l'enregistrement de la marque.
   b. Si le texte du pied de page contient un lien URL, il peut se chevaucher sur l'image de pied de page. Prévisualisez-le et corrigez-le selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chronologie

La configuration de la chronologie vous permet de créer et de modifier les filtres de chronologie selon vos besoins. Vous pouvez filtrer les types d'activités à inclure dans le rapport, configurer si les tâches enfants doivent être incluses ou exclues dans le rapport, et configurer si les images doivent être incluses ou exclues du rapport.

Si vous souhaitez utiliser et remplir n'importe quelle configuration de chronologie, vous devez ajouter la balise comme indiqué ci-dessous : `${timeline:timeline name}`. Deux exemples de configurations de chronologie à titre d'exemple sont fournis dans la configuration et sont utilisés dans le modèle de rapport d'hameçonnage et le modèle de rapport par défaut. Vous pouvez modifier et réutiliser les configurations.

Scripts de modèle

Utilisez les scripts de modèle pour inclure les données des listes connexes, l'horodatage et toutes les autres données qui ne sont pas directement accessibles par une remontée pas à pas. Voici un exemple :

Construisez un script de modèle pour afficher la liste connexe sur un modèle de rapport :

1. Pour préparer les données de la liste connexe, appelez la méthode PostIncidentReportUtils.fetchRelatedListDataForReport.
2. Pour représenter les données step1 au format et au style de table, appelez la méthode ReportTemplateUtil.constructTablefunction.

Si vous souhaitez utiliser et remplir n'importe quel script de modèle, vous devez ajouter la balise de script de modèle de balise en tant que `${template_script:script name}`.

Voici quelques exemples de modèles de scripts fournis pour configurer et modifier vos rapports post-incident.

Nom de script	Description
formatted_current_date	Renvoie la date et l'heure locales actuelles au format JJMMAAA, 00,00 AM ou PM. Par exemple, 21 janv. 2021 15:51 PST.
si_affected_users	Renvoie les utilisateurs affectés de la liste connexe sous forme de tableau.
si_assessments	Renvoie les résultats de l'évaluation post-incident sous forme de tableau.
si_associated_phish_emails	Renvoie les e-mails d'hameçonnage associés de la liste connexe sous forme de tableau.
si_associated_phish_headers	Renvoie les en-têtes d'hameçonnage associés de la liste connexe sous forme de tableau.
si_business_criticality	Renvoie une valeur de criticité opérationnelle codée par couleur.
si_malicious_observables	Renvoie les observables malveillants de la liste connexe sous forme de tableau.
si_observables	Renvoie les observables de la liste connexe sous forme de tableau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

Nom de script	Description
si_priority	Renvoie une valeur de priorité codée par couleur.
si_response_tasks	Renvoie les tâches de réponse de la liste connexe sous forme de tableau.
si_time_to_identify	Renvoie la durée passée à l'état Brouillon et Analyse.
si_time_to_resolve	Renvoie le délai de résolution de l'incident.

Points clés des scripts de modèle de rapport :

1. Si une liste connexe de plus de 5 colonnes est ajoutée, les données de table sont tronquées pendant la génération du PDF. La largeur minimale de chaque colonne est définie sur 124 px.
2. Si un script de modèle n'est pas en mesure de charger le contenu du modèle de rapport en raison de problèmes techniques, un message d'erreur s'affiche sur le rapport, « Erreur lors de l'évaluation du script de modèle » et l'administrateur de sécurité doit évaluer l'exactitude du script pour résoudre le problème.
3. si_assessments : par défaut, toutes les catégories d'évaluation sont ajoutées au rapport. L'administrateur de sécurité peut filtrer les données en modifiant le script du modèle si nécessaire. Ajoutez le `categories: sys_id1,# sys_id2;` paramètre pour filtrer les données.
4. Délai de résolution et temps d'identification des scripts : utilisez les enregistrements de définition qui font partie de la liste connexe des mesures. Si les enregistrements de définition ne sont pas disponibles pour l'incident de sécurité, créez ou ajoutez ces enregistrements de définition pour renseigner les valeurs des deux champs.

Remarque :

Par défaut, l'administrateur de sécurité n'a pas accès à l'affichage des enregistrements de version d'une table. Vous devez ajouter un rôle administrateur pour accéder aux enregistrements de version et revenir à la version précédente.

Configuration du rapport

Utilisez la section Configuration du rapport pour configurer les conditions et appliquer les modèles de rapport aux incidents de sécurité. Vous pouvez ajouter un rapport primaire et un ou plusieurs modèles de rapport supplémentaires à la même condition.

Voici un exemple de condition fourni pour appliquer le modèle de rapport d'hameçonnage aux incidents de catégorie d'hameçonnage et l'autre pour appliquer le modèle de rapport par défaut à tous les incidents de sécurité. Le modèle de rapport par défaut sera appliqué aux incidents de sécurité si les conditions ne sont pas remplies.

Procédure pour désactiver la nouvelle implémentation

1. Désactivez les règles métier suivantes :
   a. Générer un PDF PIR
   b. Créer un article de base de connaissances à la fermeture Nouveau
2. Activez les règles métier suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Générer un PIR quand en cours de révision et de fermeture

b. Créer un article de base de connaissances à la fermeture

c. [Régénérer la PIR à la fermeture/l'annulation/la suppression]

3. Activez la règle d'interface utilisateur, *`Hide PIR field when empty`*.
4. Accédez à la mise en page du formulaire dans le formulaire d'incident de sécurité. Dans la section **Revue post-incident** :

a. Supprimer le sélecteur de rapport PIR de la section PIR

b. Ajouter un champ Rapport post-incident à la section PIR

Configurer les propriétés du rapport de revue post-incident (PIR) pour les incidents de sécurité enfants

Vous pouvez configurer les deux propriétés du rapport PIR suivantes pour les incidents de sécurité enfants :

- **sn_si.generate_pir_report_for_child_si**
- **sn_si.include_child_si_timeline_in_pir**

Remarque : Les utilisateurs disposant du rôle d'administrateur système [admin] peuvent afficher les propriétés. Les utilisateurs disposant du rôle d'administrateur de sécurité [sn_si.admin] peuvent les modifier.

Configurer les propriétés du rapport PIR pour les incidents de sécurité enfants

Propriété	Utilisation
sn_si.generate_pir_report_for_child_si	Option permettant d'activer la génération de rapports de revue post-incident (PIR) pour les incidents de sécurité enfants. • **Type** : vrai | faux • **Valeur par défaut** : faux • **Emplacement** : accédez à toutes les propriétés système > > toutes les propriétés.
sn_si.include_child_si_timeline_in_pir	Option permettant d'inclure la chronologie des incidents de sécurité enfants dans le rapport PIR de l'incident de sécurité parent. • **Type** : vrai | faux • **Valeur par défaut** : faux • **Emplacement** : accédez à toutes les propriétés système > > toutes les propriétés.

Gérer le rapport de revue post-incident

Le rapport Gérer la revue post-incident inclut les informations qui ont été configurées et appliquées par l'administrateur de sécurité, et les analystes de sécurité peuvent modifier les filtres de chronologie au moment de l'exécution et les télécharger.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis :sn.si_analyst

Pourquoi et quand exécuter cette tâche
L'analyste de la sécurité peut sélectionner l'un des modèles de rapport principaux ou supplémentaires disponibles, configurer les filtres de chronologie, prévisualiser et télécharger le rapport. L'analyste de la sécurité peut également télécharger directement le rapport avec la configuration de chronologie qui a été appliquée en dernier.

L'analyste de la sécurité peut accéder aux rapports à l'aide de l'onglet Revue post-incident.

Procédure

1. Accédez à l'incident de sécurité à l'état Révision.
2. Cliquez sur **l'onglet Revue post-incident** .
3. Si l'incident de sécurité est à l'état **Examen** :
   Modèle de rapport :
   - Par défaut, le modèle de rapport principal configuré sur la page de configuration est appliqué à l'incident de sécurité et peut être téléchargé.
   - L'analyste peut choisir d'autres rapports dans la liste déroulante pour configurer et télécharger le rapport.
4. **Configurer/prévisualiser :**

   Un analyste de sécurité peut prévisualiser et modifier la configuration du modèle de rapport. Dans la configuration actuelle, l'analyste de sécurité ne peut modifier que les filtres de chronologie.

   Si la configuration est modifiée pour le rapport primaire avant la fermeture de l'incident de sécurité, le rapport de revue post-incident joint à l'incident de sécurité est mis à jour en fonction des modifications apportées par l'analyste de sécurité. Après la fermeture, l'analyste pourra modifier la configuration et télécharger le rapport en déplacement. Toutefois, le rapport joint suivrait la dernière configuration avant la fermeture.

   Pour configurer/prévisualiser le rapport, procédez comme suit :

   a. Sélectionnez le modèle de rapport souhaité dans la liste déroulante **Modèle de rapport** de l'onglet **Revue post-incident** .
   b. Cliquez sur l'onglet **Configurer/Prévisualiser** .
   c. **Mettez à jour** ou configurez les filtres de chronologie selon vos besoins.
   d. Utilisez la case **à cocher Afficher les images** pour inclure ou exclure les images de la chronologie. Si cette option n'est pas cochée, seuls les noms des images sont inclus dans la section chronologie.
   e. Utilisez la case **à cocher Afficher les tâches enfants** pour répertorier toutes les tâches enfants associées à l'incident de sécurité.
5. **Enregistrez** la configuration et cliquez sur l'onglet **Aperçu** pour prévisualiser et télécharger le rapport.
6. Cliquez sur **Télécharger** pour télécharger directement le rapport.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer une condition de déclenchement d'évaluation

Définissez les conditions des règles et générez les évaluations obligatoires et facultatives pour des incidents de sécurité spécifiques.

Avant de commencer

Rôle requis : sn_si.admin

Remarque : Pour utiliser la fonctionnalité Conditions de déclenchement de l'évaluation de la revue post-incident, vous devez effectuer une mise à niveau vers Réponse aux incidents de sécurité la version 11.0. Avant de procéder à une mise à niveau, vous devez rétablir toutes les personnalisations apportées au type de mesure de revue post-incident et aux conditions de déclenchement. En outre, vous devrez peut-être rétablir les personnalisations effectuées sur les règles métier spécifiques à la revue post-incident.

- Exiger que les évaluations soient terminées
- Délégataire de la boutique

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Administration** > **Revue post-incident : configuration des évaluations**.
2. Dans la section **Conditions de déclenchement de l'évaluation Configurer** , cliquez sur **Configurer**.

   Remarque : Sur le formulaire Configurations de l'évaluation et dans la section Configurations des évaluations, la case **Générer les évaluations** est cochée par défaut.

   - Lorsque vous cochez la case, une évaluation facultative est créée pour chaque incident de sécurité.
   - Lorsque vous décochez la case, les évaluations ne sont pas générées. Les règles d'évaluation ne sont pas affichées et vous ne pouvez pas configurer les conditions pour les incidents de sécurité.

3. Dans la section Conditions du formulaire Configurations de l'évaluation, spécifiez les informations requises.

   a. Dans le champ **Nom** , spécifiez le nom de la règle.

   b. Dans le champ **Exécution** , spécifiez le type d'exécution.

   c. Pour configurer une condition, cliquez sur l'enregistrement de règle et définissez les conditions dans le champ **Condition** .

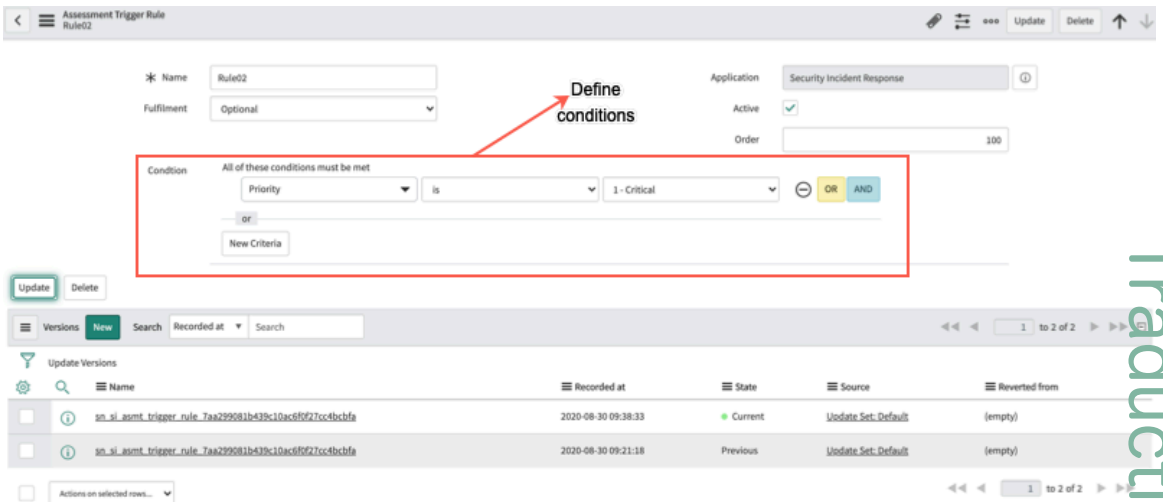
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si vous créez une règle sans définir de condition dans le champ **Condition** , la condition est évaluée comme vraie et la règle est applicable à tous les incidents de sécurité.
- Vous pouvez définir une règle spécifique pour rendre les évaluations obligatoires ou facultatives, et les évaluations ne sont pas générées pour les incidents de sécurité restants, qui ne correspondent pas aux règles définies.

Conditions de déclenchement



Exemples de conditions de déclenchement d'évaluation

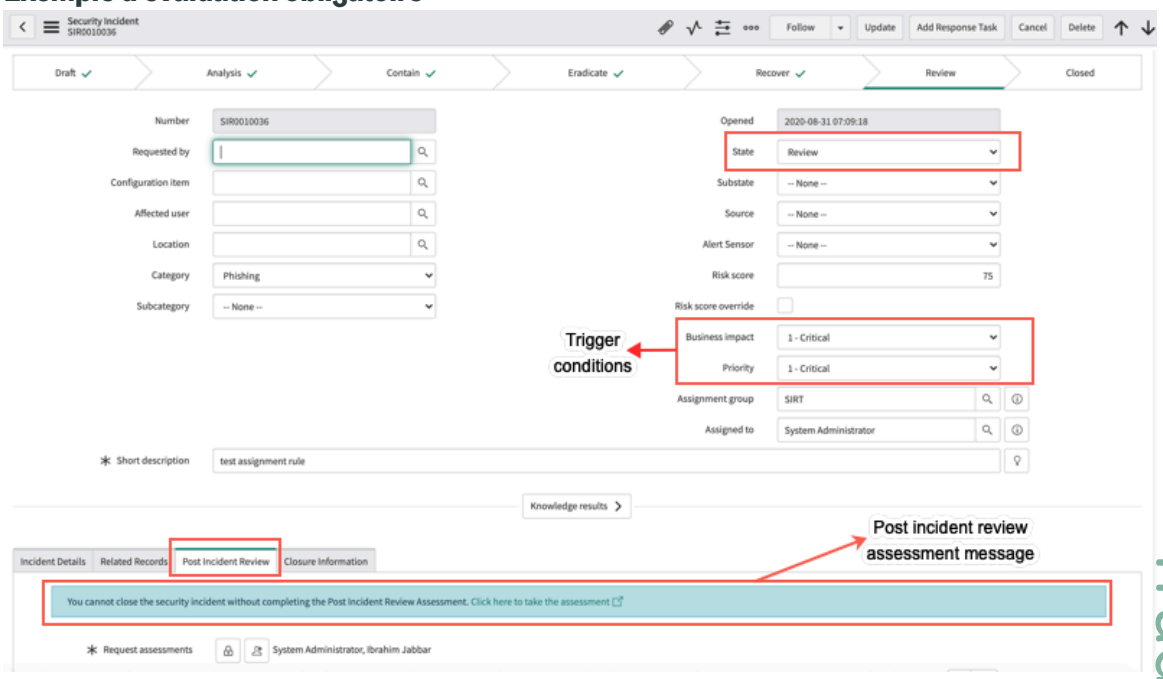
Les exemples suivants présentent différents scénarios sur la façon dont les conditions de déclenchement d'évaluation obligatoires et facultatives sont générées.

- Sur le formulaire Condition de déclenchement de l'évaluation, générez les évaluations obligatoires lorsque la **priorité** et **l'impact sur l'entreprise** d'un incident de sécurité sont définis sur **Critique** sur la page **Règle de déclencheur d'évaluation** . Dans ce scénario, les analystes de sécurité ne peuvent pas fermer l'incident tant que les évaluations obligatoires ne sont pas terminées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple d'évaluation obligatoire



- Comme vous pouvez le voir, dans cet exemple, si un incident de sécurité est à l'état **Revue** , les analystes de sécurité ne peuvent pas fermer l'incident de sécurité sans avoir terminé l'évaluation de la **revue post-incident**. Un lien d'évaluation est disponible pour transmettre l'évaluation aux analystes de sécurité qui sont affectés (ou qui avaient demandé l'évaluation) à l'incident.
- Dans le formulaire Condition de déclenchement de l'évaluation, générez des évaluations facultatives lorsque la **priorité** et **l'impact sur l'entreprise** d'un incident de sécurité sont définis sur **Élevé**. Dans cet exemple, si les analystes de sécurité ne terminent pas les évaluations et ne ferment pas l'incident de sécurité, les évaluations sont automatiquement annulées.
- Si les évaluations obligatoires ou facultatives ne correspondent pas à l'incident de sécurité, les évaluations ne sont pas générées pour ces incidents de sécurité. Un analyste de sécurité peut fermer l'incident de sécurité sans avoir terminé l'évaluation de l'examen post-incident.

Effectuer une revue post-incident basée sur un questionnaire

Vous pouvez décider qu'un examen post-incident de l'incident de sécurité est justifié. Une revue post-incident décrit ce qui s'est passé, aide à déterminer pourquoi l'incident s'est produit et identifie comment il peut être évité ou géré à l'avenir.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager, sn_si.analyst

Remarque : Quel que soit son rôle, tout utilisateur peut participer à un questionnaire de revue post-incident. Les rôles peuvent être affectés à une révision.

Pourquoi et quand exécuter cette tâche

L'application ServiceNow Réponse aux incidents de sécurité peut automatiser la collecte d'informations de revue post-incident auprès de toutes les personnes impliquées dans un incident de sécurité à l'aide de questionnaires. Si vous décidez d'utiliser un questionnaire dans le cadre d'une revue post-incident, une liste de questions pertinentes pour l'incident de sécurité est envoyée à la liste des participants définie par l'utilisateur. Au fur et à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

mesure que chaque utilisateur termine le questionnaire, le rapport post-incident est généré automatiquement. Le rapport compile toutes les informations relatives à l'incident de sécurité, ainsi que toutes les réponses à la revue post-incident.

Une liste initiale de questions est fournie avec le système de base, mais elle est personnalisable. Vous pouvez créer des catégories et y ajouter de nouvelles questions, ou vous pouvez modifier des questions individuelles dans des catégories existantes. Vous pouvez poser des questions en fonction des rôles. Vous pouvez définir quand certaines questions sont posées. Vous pouvez poser des questions uniquement pour vos serveurs UNIX, par exemple, ou uniquement en cas d'activité criminelle. Vous pouvez définir les questions posées en fonction de la réponse à une autre question ou de la valeur d'un champ du formulaire. Il peut même y avoir des questions qui sont entièrement remplies en interrogeant la base de données.

Une fois l'incident de sécurité résolu et passé à l'état **Examen** , des évaluations sont générées pour tous les utilisateurs affectés et les utilisateurs directement ajoutés à partir de la liste **d'évaluation des demandes** .

Le questionnaire peut être un outil utile pour recueillir des informations sur la gestion de l'incident de sécurité à partir de diverses sources.

Au cours de la révision, vous pouvez ajouter d'autres utilisateurs à la liste ou supprimer des utilisateurs existants de la liste, à moins qu'ils n'aient déjà commencé à remplir le questionnaire. Si vous ajoutez de nouveaux utilisateurs à la liste, ils reçoivent les questions lors de l'enregistrement enregistré. L'incident de sécurité ne peut pas être fermé tant que tous les questionnaires n'ont pas été remplis. Au fur et à mesure que les questionnaires sont remplis par chaque utilisateur, le rapport post-incident est automatiquement généré (et régénéré) et affiché dans l'onglet **Revue post-incident** .

Pour commencer une revue post-incident :

Procédure

1. Créez un incident de sécurité ou ouvrez-en un existant en accédant à **Incident de sécurité** > **Incidents** > **Affecté à moi-même (ou affecté à une équipe ou à des incidents non affectés)**.
2. Cliquez sur l'onglet **Revue post-incident** .
3. Par défaut, le champ Évaluations de la **demande** indique la personne dans le champ **Affecté à** . Cliquez sur l'icône de verrou pour ajouter d'autres utilisateurs à la liste de révision. Une fois le champ déverrouillé, des options sont disponibles pour ajouter ou supprimer plusieurs utilisateurs et rôles, ou pour saisir des adresses e-mail d'utilisateurs.
4. Lorsque vous avez terminé vos entrées, cliquez sur l'icône de verrou pour verrouiller le champ.

   Remarque : Vous pouvez également définir les conditions qui, lorsqu'elles sont réunies dans un incident de sécurité, peuvent entraîner l'ajout automatique d'utilisateurs spécifiques au champ **Évaluations des demandes** pour cet incident de sécurité. Par exemple, lorsqu'une **catégorie** d'incident de sécurité est changée en **Hameçonnage**, des personnes spécifiques qui ont une expertise en matière de menaces d'hameçonnage peuvent être ajoutées à la liste de revue post-incident. Pour plus d'informations, consultez Créer des règles d'affectation PIR.

5. Cliquez sur **Mettre à jour**.
   Lorsque l'incident passe à l'état **d'examen** (ou immédiatement, s'il est déjà à l'état **d'examen**), chacun des utilisateurs de la liste d'examen reçoit une notification initiale par e-mail . Des rappels sont envoyés à l'approche de la date d'échéance. Lorsque chaque utilisateur accède au questionnaire à partir du lien par e-mail ou en accédant à **Revue post-incident** > **Mes vérifications en attente**, les questions affichées sont tirées de toutes les catégories qui correspondent à cet incident de sécurité. Si de nouveaux utilisateurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sont ajoutés à la liste de révision avant la date d'échéance, ils reçoivent des notifications lorsque l'incident de sécurité est enregistré.

Au fur et à mesure que les utilisateurs terminent leurs questionnaires, le rapport post-incident compile les données et affiche le rapport dans l'onglet **Revue post-incident** . Les données du questionnaire sont affichées dans l'onglet **Résultats** .

Créer des catégories de questionnaire de revue post-incident

Vous pouvez utiliser les catégories de questionnaire fournies avec le système de base ou créer vos propres catégories.

Avant de commencer
Rôle requis : sn.si_admin

Pourquoi et quand exécuter cette tâche
Pour créer une nouvelle catégorie de questions :

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Revue post-incident**.
2. Cliquez sur **Passer en revue les questions**.
   Une liste de catégories s'affiche, ainsi que leur ordre et des filtres qui définissent les conditions dans lesquelles les questions sont posées (par exemple, uniquement lorsque la catégorie d'incident de sécurité est `Activité criminelle`). Chaque catégorie est une section du questionnaire de revue post-incident et les questions de chaque catégorie ne sont incluses que lorsque l'incident de sécurité correspond au filtre Condition. Par exemple, pour une catégorie de questions s'appliquant uniquement aux serveurs Linux, vous pouvez configurer un filtre qui sélectionne les incidents de sécurité dans lesquels le type de ressource affecté est Serveur Linux. Dans cette catégorie, vous créeriez ensuite toutes les questions nécessaires lorsqu'un incident de sécurité se produit sur un serveur Linux. Vous utilisez l'une des catégories fournies dans le système de base ou créez une nouvelle catégorie. Cette procédure suppose que vous souhaitiez créer une nouvelle catégorie avant de définir des questions.
3. Cliquez sur **Nouveau** dans la liste des catégories.
4. Renseignez les champs du formulaire comme il convient.

Incident de sécurité

Champ	Description
Nom	Nom de la catégorie qui apparaît dans le questionnaire sur les incidents de sécurité.
Type	La revue post-incident est la valeur par défaut.
Créer les personnes concernées	Non utilisé par Réponse aux incidents de sécurité.
Table	Ce champ est affecté automatiquement une fois le formulaire soumis.
Filtre	Entrez la condition qui détermine quand les questions de cette catégorie sont utilisées. Si un enregistrement d'incident de sécurité correspond à ce filtre, les questions sont incluses dans une revue post-incident pour cet incident de sécurité. Les filtres peuvent utiliser n'importe quelle donnée de l'enregistrement ou d'autres enregistrements liés à cet enregistrement. Par exemple, le département du gestionnaire de l'utilisateur demandeur.
Application	Application du champ d'application pour l'incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Pondération	Valeur numérique représentant l'importance de cette mesure par rapport à d'autres mesures de la même catégorie. Par défaut, le poids est de 10.
Nombre total de mesures	Nombre de mesures utilisées par la catégorie.
Description	Description du questionnaire.

5. Cliquez sur **Soumettre** pour enregistrer la catégorie.

Rédiger des questions de revue post-incident

Vous pouvez utiliser les questions fournies avec le système de base ou créer vos propres questions.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Les méthodes de collecte d'informations de revue post-incident peuvent prendre la forme de questions ou de données collectées automatiquement à l'aide de scripts.

Les questions peuvent dépendre des réponses à d'autres questions. Par exemple, vous pouvez demander si tous les journaux nécessaires étaient disponibles. Si la réponse est non, vous posez une question de suivi pour déterminer lesquels des journaux nécessaires n'ont pas été activés.

La collecte de données scriptées, également appelée mesures de script, rassemble les données relatives à l'incident de sécurité via les scripts que vous écrivez. Cette action peut aller bien au-delà des données contenues dans l'enregistrement d'incident de sécurité lui-même. Par exemple, une mesure de script peut collecter les temps de panne récents d'un serveur affecté par cet incident de sécurité.

Enfin, vous pouvez mélanger les deux types. Les questions peuvent avoir des valeurs par défaut extraites d'un script ou simplement d'un champ de l'enregistrement d'incident de sécurité. Lorsque vous utilisez un type de question Réponse par défaut de... , vous pouvez choisir si vous souhaitez que l'utilisateur réponde toujours à la question (la valeur par défaut lui fournissant une valeur initiale) ou si vous souhaitez que la question soit posée à l'utilisateur uniquement si le script ou le champ est vide.

Pour créer une nouvelle question :

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Revue post-incident**.
2. Cliquez sur la catégorie pour laquelle vous souhaitez créer une question.
3. Cliquez sur l'onglet **Mesures d'évaluation** .
4. Cliquez sur **Nouveau**.
   Vous pouvez également cliquer sur une question existante pour la modifier.
5. Renseignez les champs du formulaire comme il convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de mesure

Champ	Description
Nom	Nom de la mesure (question ou script). Si la mesure est une collecte de données scriptée, ce nom apparaît sur le rapport post-incident.
Catégorie	Catégorie à laquelle appartient la mesure. Le système remplit automatiquement cette catégorie si vous créez une nouvelle mesure à partir du formulaire Catégorie de mesure. **Remarque :** Vous ne pouvez pas changer la catégorie si le champ **Dépend du champ est** défini ou si une autre mesure dépend de cette mesure
Fonction de message REST	Indique le type de mesure, comme suit : ○ *`Assessment`*: une question qui n'a pas de valeur par défaut. Plusieurs types de données peuvent être définis dans le champ **Type de données** de l'onglet **Type de champ** , tels que les cases à cocher, les listes de choix, l'entrée de texte. ○ *`Script`*: mesure scriptée. Obtenir des valeurs en écrivant un script personnalisé. La *`Script`* méthode est compatible avec les types de données **Durée**, **Nombre** et **Pourcentage** . ○ *`Default answer from field`*: question dont la réponse par défaut provient d'un champ sélectionné dans l'incident de sécurité. La sélection de cette option ajoute deux champs à l'onglet **Général** : ▪ *`Default answer`*: sélectionnez le champ de l'incident de sécurité qui contient la réponse par défaut à la question. Par exemple, pour la question : « Qui a initialement signalé cet incident ? », le champ **Demandé par** serait un choix probable. ▪ *`Ask question`*: spécifie quand poser la question : toujours ou uniquement si le champ Réponse **par défaut** est vide. En utilisant l'exemple ci-dessus, la question serait posée si le champ **Demandé par** est vide. ○ *`Default answer from script`*: une question dont la réponse par défaut provient d'un script. La réponse peut être un nombre, une chaîne ou un pourcentage. L'onglet **Général** ajoute un champ : *`Ask question`*: comme le Spécifie quand poser la question : toujours ou seulement si le script ne fournit pas de réponse par défaut. Le script est défini dans l'onglet **Type de champ** . **Remarque :** Si vous sélectionnez un **type de données** incompatible avec la **méthode** sélectionnée, le système remplace automatiquement la **méthode** par une valeur compatible.
Pondération	[Obligatoire] Valeur numérique représentant l'importance de cette mesure par rapport à d'autres mesures de la même catégorie. Par défaut, le poids est de 10.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Ce champ est visible et obligatoire sauf si le **type de données** est **Date**, **Date/Heure** ou **Chaîne**. Ces types de données ne sont pas inclus dans les calculs de résultats.
Ordre	[Obligatoire] Valeur numérique qui détermine l'ordre de la question de mesure dans les questionnaires d'évaluation, par rapport à d'autres questions de mesure de la même catégorie. La mesure avec la valeur d'ordre la plus petite apparaît comme la première question de la section catégorie. Par défaut, la commande est de 100. **Remarque :** La valeur d'ordre que vous utilisez pour les mesures avec la méthode Script n'a pas d'importance, car elles n'apparaissent pas sur les questionnaires.
Actif	Case à cocher qui détermine si cette mesure est utilisée. Si la case n'est pas cochée, c'est comme si l'enregistrement de mesure n'existait pas.
Obligatoire	Case à cocher qui rend la question de mesure obligatoire (sélectionnée) ou facultative (décochée) dans les questionnaires d'évaluation. Les utilisateurs ne peuvent pas soumettre de questionnaires tant qu'ils n'ont pas fourni de réponses valides à toutes les questions obligatoires, qui sont indiquées par un indicateur d'état de champ rouge. Ce champ n'est visible que si le champ **Dépend du** champ est vide et que le type de données n'est pas **Case à cocher**.

6. Cliquez sur l'onglet **Général** et renseignez les champs comme il convient.

Onglet Général

Champ	Description
Question	Texte à utiliser comme question sur les questionnaires d'examen des incidents de sécurité. Saisissez une question claire, simple et à laquelle il est facile de répondre, par exemple **: Comment avons-nous maîtrisé l'incident** ?
Description	Informations sur la mesure et ce qu'elle évalue. S'il s'agit **d'une***Method* évaluation, incluez des détails qui aident les utilisateurs à comprendre comment répondre à la question. Ce texte apparaît sous forme d'indication lorsqu'un utilisateur pointe sur le texte de la question dans le questionnaire.
Dépend de et Affiché quand	Sélectionnez une question dans le champ **Dépend du** sur lequel la question actuelle dépend. Par exemple, la question « Quels journaux supplémentaires étaient nécessaires ? » dépend de la question « Tous les journaux nécessaires étaient-ils disponibles ? » Ensuite, utilisez le champ **Affiché quand** pour identifier quand vous souhaitez que la question dépendante apparaisse dans les questionnaires. Par exemple, si vous souhaitez que la question dépendante soit posée uniquement lorsque l'utilisateur répond

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Non à la question « Tous les journaux nécessaires **étaient-ils** disponibles ? », sélectionnez **Non** dans le champ Affiché quand. **Remarque :** Le système empêche la création de dépendances récursives entre les mesures. Par exemple, si la mesure A dépend de la mesure B, la mesure B ne peut pas dépendre de la mesure A.

7. Cliquez sur l'onglet **Type de champ** et renseignez les champs, selon vos besoins.

Onglet Type de champ

Champ	Description
Type de données	Le type de données de la réponse attendue dont la liste des types disponibles dépend pour la méthode sélectionnée. Si la méthode est **Évaluation**, le type de données détermine la façon dont les utilisateurs répondent à la question correspondante dans les questionnaires. Si la méthode est **Script**, le type de données détermine la manière dont le système calcule les résultats d'évaluation. **Remarque :** Si une autre mesure dépend de cette mesure, vous ne pouvez pas modifier le type de données.
Définir de façon aléatoire les réponses	Case à cocher qui détermine s'il convient de présenter les options de réponse pour cette question de mesure dans un ordre aléatoire chaque fois qu'un utilisateur ouvre un questionnaire d'évaluation contenant la question. La préférence de réponse peut être influencée par l'ordre dans lequel les options de réponse apparaissent. Cela peut entraîner des résultats biaisés. La randomisation des options de réponse peut aider à prévenir ce biais. Ce champ n'est visible que si vous sélectionnez **Échelle de Likert** ou **Choix** dans le champ **Type de données** .
Module d'extension dépendant	[Obligatoire s'il s'agit **d'un***Method* script.] Module d'extension qui contient les tables interrogées dans le script. Le système exécute le script de mesure uniquement si le module d'extension est actif. Les valeurs par défaut disponibles sont **Gestion des actifs**, **CMDB**, **Core**, **Gestion des coûts**, **Approvisionnement** et **Gestion des actifs logiciels**. Ce champ n'est visible que s'il s'agit **d'un***Method* script. **Remarque :** ○ Si la valeur Core par défaut est utilisée, le script est toujours exécuté. ○ Si vous êtes administrateur, vous pouvez ajouter d'autres choix de modules d'extension au champ.
Définition de l'échelle	Paramètre qui détermine si des valeurs numériques inférieures ou supérieures équivalent à un bon score dans les calculs de résultats

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'évaluation. Sélectionnez **Faible** si des valeurs numériques inférieures sont préférables, par exemple pour une mesure qui mesure le nombre de défauts pour un fournisseur. Sélectionnez **Élevé** si les valeurs numériques supérieures sont meilleures, par exemple pour une mesure qui mesure la satisfaction des utilisateurs sur une échelle de un à cinq. La valeur par défaut est **Élevé**. Ce champ est visible et obligatoire sauf s'il s'agit *Data type* **de Date**, **Date/Heure** ou **Chaîne**. Les résultats de ces types de données ne sont pas inclus dans les calculs de résultats.
Min.	Valeur numérique la plus basse à utiliser comme option de réponse dans les évaluations ou comme valeur adaptée dans une mesure scriptée. Ce champ est visible et requis uniquement si certains types de données sont sélectionnés. Si le type de données est **Choix** ou **Échelle de Likert**, ce champ est en lecture seule et est défini automatiquement en fonction de la plus petite définition *Value* de mesure.
Max.	Valeur numérique la plus élevée à utiliser comme option de réponse ou comme valeur mise à l'échelle. Ce champ est visible et requis uniquement si certains types de données sont sélectionnés. Si le type de données est **Choix** ou **Échelle de Likert**, ce champ est en lecture seule et est défini automatiquement en fonction de la plus grande définition *Value* de mesure.
Script	Script qui obtient les informations système souhaitées. Le script comporte une variable d'entrée, définie avec l'ID de l'incident de sécurité (primaire), et trois variables de sortie possibles définies par le script, string_result, scaled_result et actual_result. Lorsque le type de données est Chaîne, seule la string_result est requise. Ce champ est visible et requis lorsqu'il s'agit d'un *Method* **script** ou que la valeur par défaut provient d'un script.
Modèle	Un ensemble prédéfini de réponses courantes à utiliser pour la question. Par exemple, un modèle de fréquence commencera probablement par une valeur « Jamais » et montera jusqu'à la valeur supérieure « Toujours ». Ce champ est visible et requis uniquement s'il s'agit d'un *Data type* **modèle**. **Remarque :** Si une autre mesure dépend de cette mesure, vous ne pouvez pas modifier le modèle.

8. Facultatif : Lorsque vous avez terminé vos entrées, cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer des règles d'affectation PIR

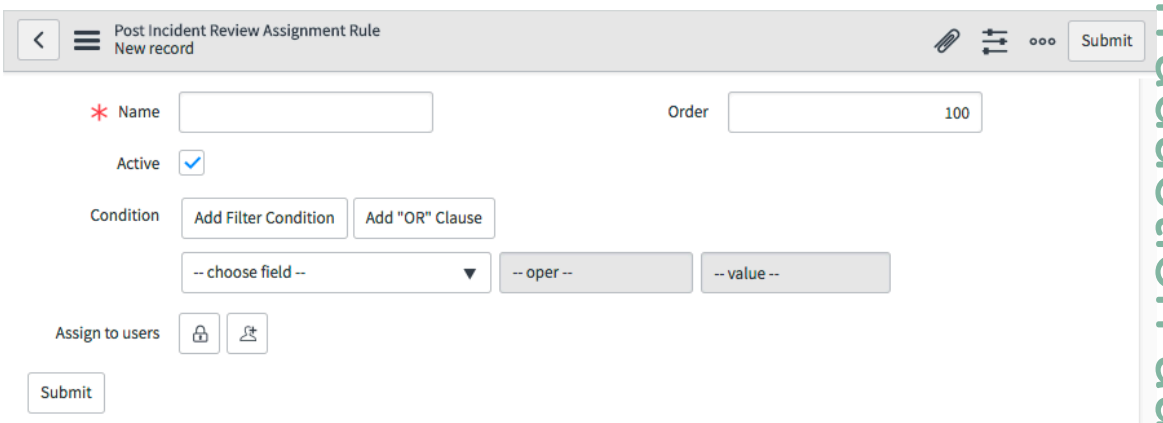
En plus d'ajouter manuellement des utilisateurs à la liste d'évaluation de la revue post-incident pour un incident de sécurité, vous pouvez définir des règles d'affectation pour ajouter automatiquement des utilisateurs à la liste.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager, sn_si.analyst

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Administration** > **Revue post-incident : configuration des évaluations**.
2. Explorez jusqu'à la section **Règles d'affectation d'utilisateur** .
3. Cliquez sur **Configurer**.
4. Cliquez sur **Nouveau**.



5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette règle d'affectation.
Actif	Cochez cette case pour activer la règle.
Ordre	Saisissez une valeur numérique pour spécifier l'emplacement où cette règle doit apparaître dans la liste des règles d'affectation. Les nombres les plus faibles apparaissent en haut de la liste. **Remarque :** Seule la première règle d'affectation correspondante est exécutée et seuls les utilisateurs définis dans cette règle sont ajoutés à la liste d'évaluation.
Condition	Utiliser le Créateur de conditions permettant de définir les conditions qui doivent être remplies dans l'incident de sécurité pour que cette règle soit exécutée. Pour plus d'informations, voir l'exemple ci-dessous.
Affecter aux utilisateurs	Cliquez sur l'icône de verrou pour ajouter des utilisateurs à la liste de révision. Une fois le champ déverrouillé, des options sont disponibles pour ajouter ou supprimer plusieurs utilisateurs et rôles, ou pour saisir des adresses e-mail d'utilisateurs.

6. Cliquez sur **Envoyer**.

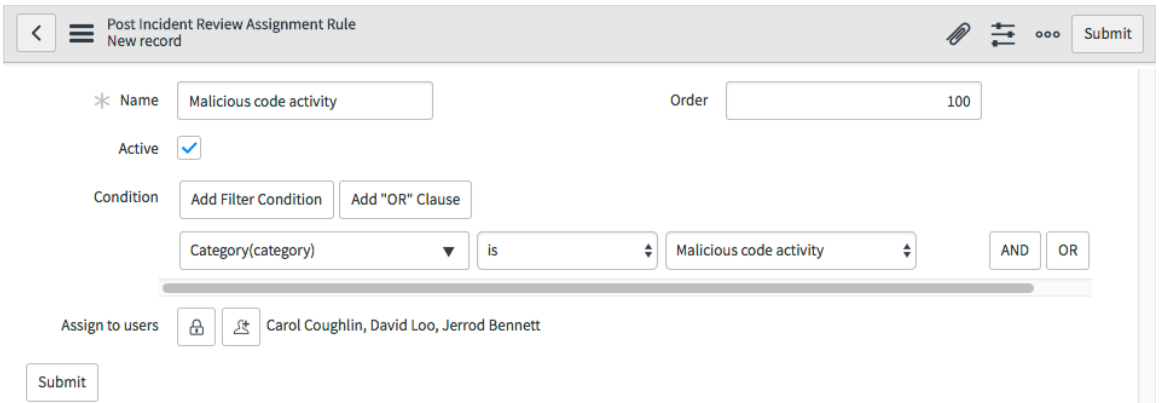
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example: Activité du code malveillant

Dans la règle d'affectation de revue post-incident illustrée ici, lorsqu'un incident de sécurité dont le champ **Catégorie** est défini sur **Activité de code malveillant** passe à l'état **Révision** , les trois utilisateurs identifiés (qui se trouvent être des experts dans la gestion de l'activité de code malveillant) sont ajoutés à la liste des utilisateurs qui recevront le questionnaire de revue post-incident pour cet incident de sécurité.

Activité du code malveillant



Fermer les incidents de sécurité

Lorsqu'un incident de sécurité est passé à l'état d'examen, il est possible de le fermer et d'entrer un code de fermeture approprié. Les codes de fermeture peuvent être recherchés ultérieurement pour faciliter la localisation.

Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Remarque : Dans les versions précédentes de Réponse aux incidents de sécurité, les utilisateurs pouvaient fermer les incidents ou les demandes de sécurité comme spam. Dans la Istanbul version, l'option spam n'est plus disponible. Les incidents ou demandes de sécurité de courrier indésirable peuvent être annulés ou supprimés, selon le cas.

Procédure

1. Si l'incident de sécurité que vous souhaitez fermer n'est pas déjà ouvert, accédez à **Incident de sécurité** > **Incidents** > **Afficher les incidents**et localisez l'incident de sécurité que vous souhaitez fermer.

   Remarque : Si des évaluations de revue post-incident n'ont pas été effectuées pour cet incident de sécurité, l'incident de sécurité ne peut pas être fermé. Retourner à **Incident de sécurité** > **Revue post-incident** > **Toutes les révisions incomplètes**, localisez les évaluations incomplètes et demandez aux évaluateurs de terminer leurs évaluations ou annulez les évaluations restantes.

2. Cliquez sur l'onglet **Informations sur la fermeture** et renseignez les champs, selon vos besoins.

Incident de sécurité

Champ	Description
Créer un article de la base de connaissances	Sélectionnez ce champ pour créer automatiquement un brouillon d'article de la base de connaissances contenant le contenu de la revue post-incident.
Code de fermeture	Sélectionnez le code de fermeture qui décrit le mieux la raison pour laquelle vous fermez cet incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	◦ Enquête terminée ◦ Menace réduite ◦ Vulnérabilité corrigée ◦ Vulnérabilité non valide ◦ Non résolu ◦ Faux positif
Fermé par	Affiche l'utilisateur qui a fermé l'incident de sécurité après la mise à jour de l'enregistrement.
Fermé	Affiche la date et l'heure de fermeture après la mise à jour de l'enregistrement.
Fermer les notes	Entrez toutes les notes supplémentaires qui décrivent le résultat de la fermeture de cet incident de sécurité.

3. Cliquez sur **Mettre à jour**.
4. L'utilisateur affecté peut changer manuellement **l'état** sur **Fermé**.
   Lorsqu'un incident parent est fermé, toutes les tâches de réponse appartenant à l'incident enfant sont annulées. S'il n'y a pas d'autres types de tâches, l'incident enfant est également fermé.

Ajouter des informations sur la fermeture à un incident de sécurité

Lorsqu'un incident de sécurité est à l'état Examiné ou Fermé, vous pouvez saisir des informations sur sa fermeture.

Avant de commencer

Rôle requis : sn_si.basic

Procédure

1. S'il n'est pas déjà ouvert, ouvrez l'incident de sécurité que vous souhaitez mettre à jour.
2. Cliquez sur l'onglet **Enregistrements connexes** .
3. Renseignez les champs nécessaires.

Champ	Description
Créer un article de la base de connaissances	Cochez cette case pour générer un article de la base de connaissances à l'aide du contenu du rapport post-incident.
Code de fermeture	Sélectionnez le code de fermeture qui décrit le mieux le motif de fermeture de l'incident de sécurité.
Fermé par	[Lecture seule] Affiche l'utilisateur qui a fermé l'incident de sécurité.
Fermé	[Lecture seule] Affiche la date et l'heure de la fermeture de l'incident de sécurité.
Fermer les notes	Comment l'incident de sécurité a été fermé, y compris les leçons apprises, la résolution, etc.

4. Cliquez sur l'un des onglets suivants pour mettre à jour l'incident de sécurité :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Détails de l'incident
- Revue post-incident

5. Lorsque vous avez terminé vos entrées, cliquez sur **Soumettre**.

Restreindre l'accès aux incidents de sécurité

Gérez l'accès aux incidents de sécurité qui contiennent des informations sensibles. Vous pouvez appliquer des restrictions d'incident de sécurité pour déterminer qui peut accéder à un incident donné et limiter l'accès uniquement à des utilisateurs ou groupes spécifiques.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Les restrictions d'incident de sécurité vous permettent de masquer les incidents de sécurité critiques pour empêcher les autres utilisateurs d'une organisation particulière d'accéder aux incidents de sécurité critiques. Ces restrictions vous permettent de fournir un moyen plus granulaire de contrôler les incidents de sécurité auxquels un utilisateur peut accéder. Vous pouvez appliquer une restriction d'incident de sécurité en cochant la case **Appliquer la restriction** , puis en sélectionnant les utilisateurs ou les groupes autorisés à accéder à l'incident de sécurité particulier.

Une fois que vous avez appliqué la restriction sur des incidents de sécurité spécifiques et limité l'accès à certains utilisateurs ou groupes, tous les autres utilisateurs restants de votre organisation ne seront pas en mesure d'accéder à ces incidents de sécurité, même s'ils recherchent un incident de sécurité restreint particulier.

Procédure

1. Ouvrez un incident de sécurité que vous souhaitez limiter.
2. Si vous utilisez l'interface utilisateur classique, procédez comme suit :

   a. Cliquez sur l'onglet **Restriction** .

   b. Cochez la case **Appliquer la restriction** pour activer la restriction de l'incident de sécurité.



   c. Dans le champ Membres autorisés, cliquez sur pour sélectionner les utilisateurs qui peuvent accéder à l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Sélectionnez pour vous ajouter en tant qu'utilisateur autorisé.

e. Sélectionnez l'icône pour ajouter ou supprimer des utilisateurs.

f. Dans le champ Groupes autorisés, cliquez sur pour sélectionner les groupes qui peuvent accéder à l'incident de sécurité.

g. Sélectionnez l'icône pour ajouter ou supprimer des groupes.

> **Remarque :** Une fois que la case **Appliquer la restriction** est cochée pour l'incident de sécurité, seuls le sn_si.admin et les membres ou groupes autorisés auront accès à l'incident de sécurité.

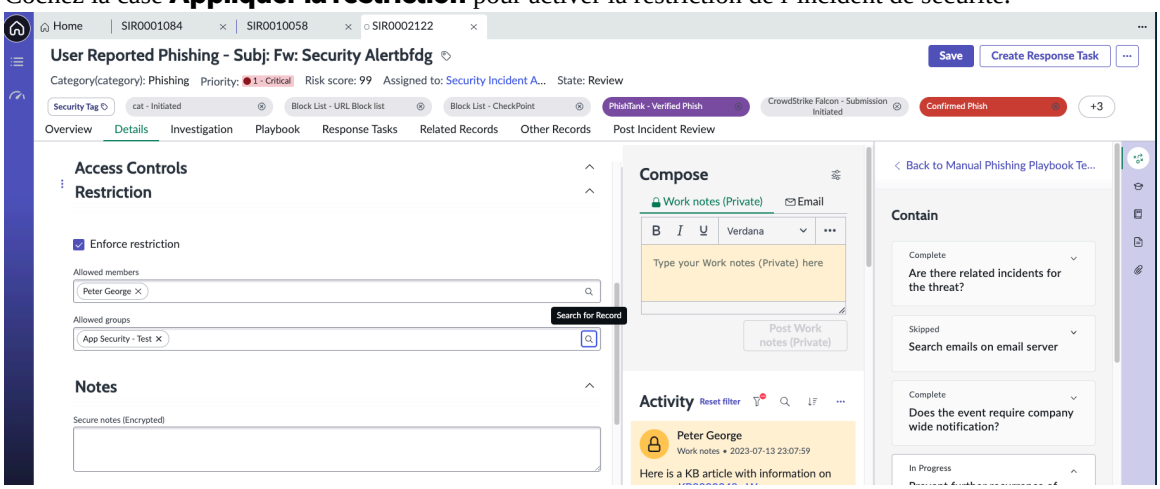
h. Cliquez sur **Mettre à jour**.

3. Si vous utilisez l'espace de travail SIR, procédez comme suit :

a. À partir de l'incident de sécurité, cliquez sur l'onglet **Détails** .

b. Faites défiler vers le bas et cliquez sur la section **Restriction** .

c. Cochez la case **Appliquer la restriction** pour activer la restriction de l'incident de sécurité.



d. Dans le champ Membres autorisés, sélectionnez les utilisateurs qui peuvent accéder à l'incident de sécurité à l'aide de l'option Rechercher.

e. Dans le champ Groupes autorisés, sélectionnez les groupes qui peuvent accéder à l'incident de sécurité à l'aide de l'option Rechercher.

> **Remarque :** Une fois que la case **Appliquer la restriction** est cochée pour l'incident de sécurité, seuls le sn_si.admin et les membres ou groupes autorisés auront accès à l'incident de sécurité.

f. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer les menaces de sécurité à l'aide de l' Security Analyst Workspace

Réponse aux incidents de sécurité inclut une nouvelle interface utilisateur appelée Qui Security Analyst Workspace propose de puissants outils d'aide à l'analyse, notamment le Playbook, la vue d'ensemble et les onglets permettant de travailler sur plusieurs incidents de sécurité.

Spécialement conçus pour les analystes de sécurité, les puissants outils de l'vous Security Analyst Workspace permettent d'analyser le volume toujours croissant de données associées aux incidents de sécurité. De plus, les actions automatisées réduisent considérablement le temps d'enquête sur les incidents de sécurité, ce qui peut faire la différence entre l'arrêt d'une attaque et une violation.

Avant d'utiliser le Security Analyst Workspace

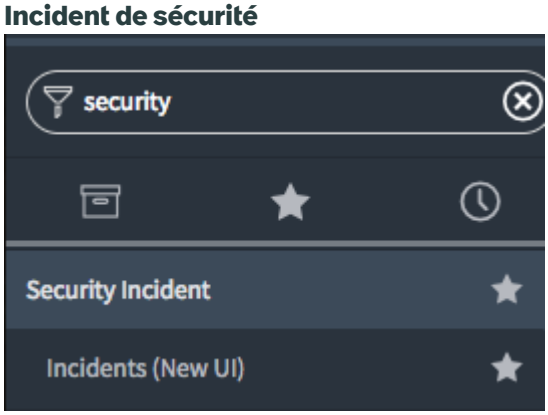
Avant de pouvoir commencer à utiliser le Security Analyst Workspace, vous devez vous assurer qu'au moins London Patch 3 est installé sur votre instance, que vous avez défini les rôles corrects et que vous avez a téléchargé l'application d'interface utilisateur Réponse aux incidents de sécurité à partir de ServiceNow Store.

Remarque : Si votre instance exécute une version antérieure à London Patch 3, vous devez demander le module d'extension Security Incident Response UI via le système HI Customer Service.

Accéder à Security Analyst Workspace

Pour accéder à ce nouvel espace de travail, accédez à **Incident de sécurité** > **Incidents (nouvelle interface utilisateur)**.

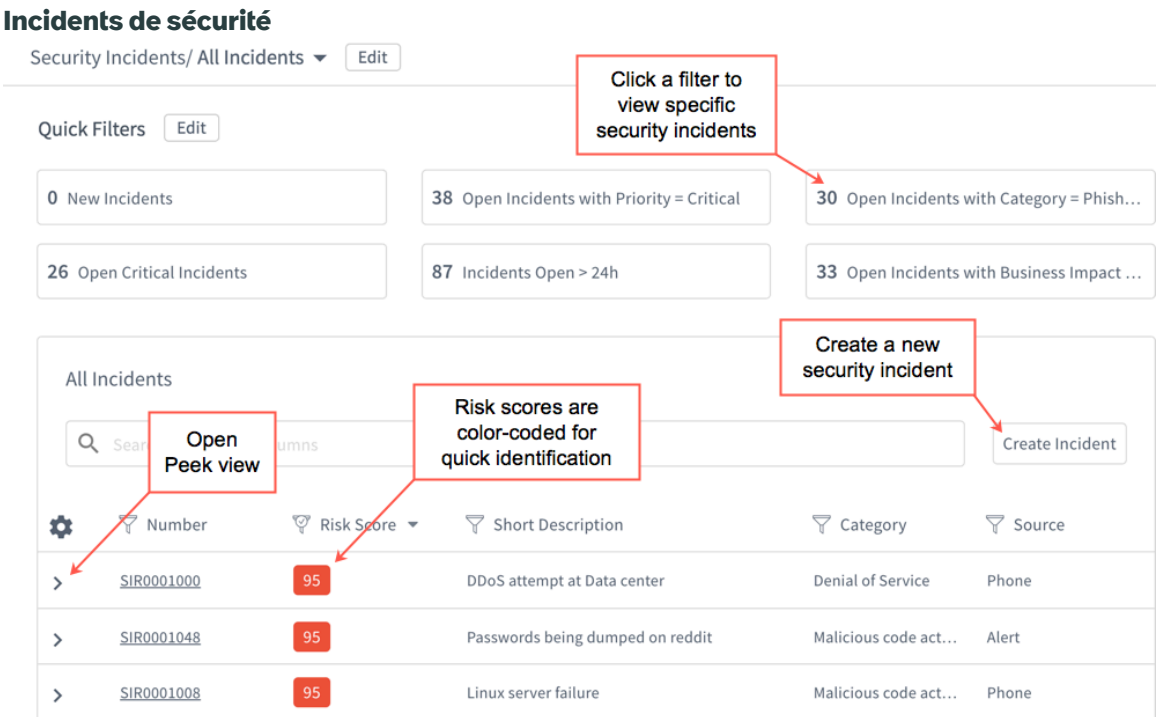
Incident de sécurité



L'espace de travail s'ouvre dans un onglet de navigateur distinct.

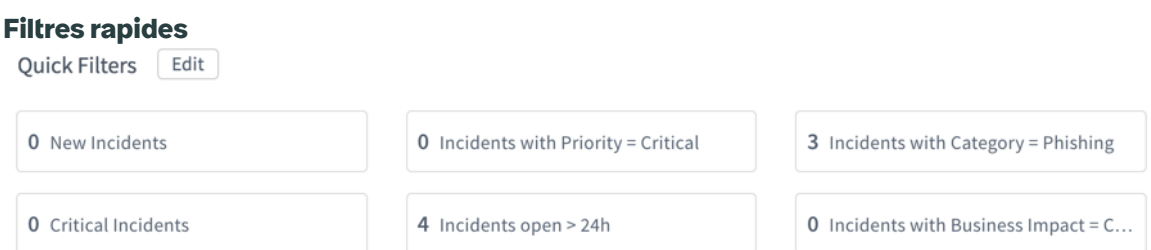
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Localisez les incidents de sécurité que vous souhaitez analyser à l'aide des filtres rapides

Le fournit Security Analyst Workspace plusieurs outils permettant de filtrer la liste des incidents de sécurité afin que vous puissiez trouver rapidement les incidents de sécurité que vous souhaitez analyser. Les filtres rapides vous permettent de sélectionner un sous-ensemble d'incidents de sécurité en fonction des critères contenus dans le filtre.



Cliquez simplement sur le filtre rapide que vous souhaitez utiliser.

Remarque : Vous pouvez cliquer sur un bouton **Modifier** pour identifier les filtres rapides que vous souhaitez afficher sur l'écran de liste. Un minimum d'un filtre doit être sélectionné, jusqu'à un maximum de six.

Vous pouvez définir des filtres rapides supplémentaires, ainsi que des filtres primaires pour le , à l'aide de l'environnement Security Analyst Workspace classique. Pour plus d'informations, consultez Configurer des filtres primaires et secondaires pour Security Analyst Workspace.

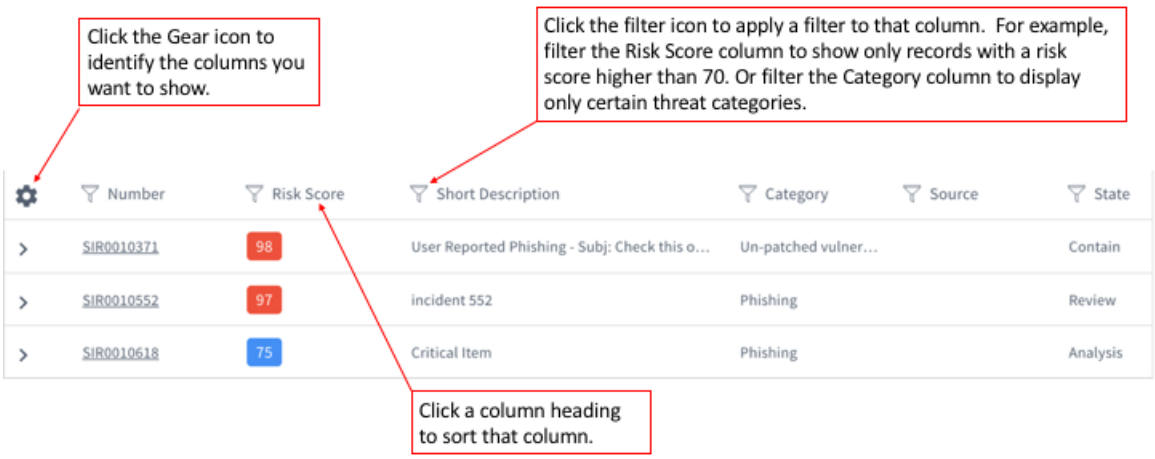
Personnaliser la liste des incidents de sécurité

Comme pour toutes les listes de votre instance, fournit Security Analyst Workspace des outils permettant de personnaliser la liste et de trier les informations affichées pour répondre à vos besoins d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

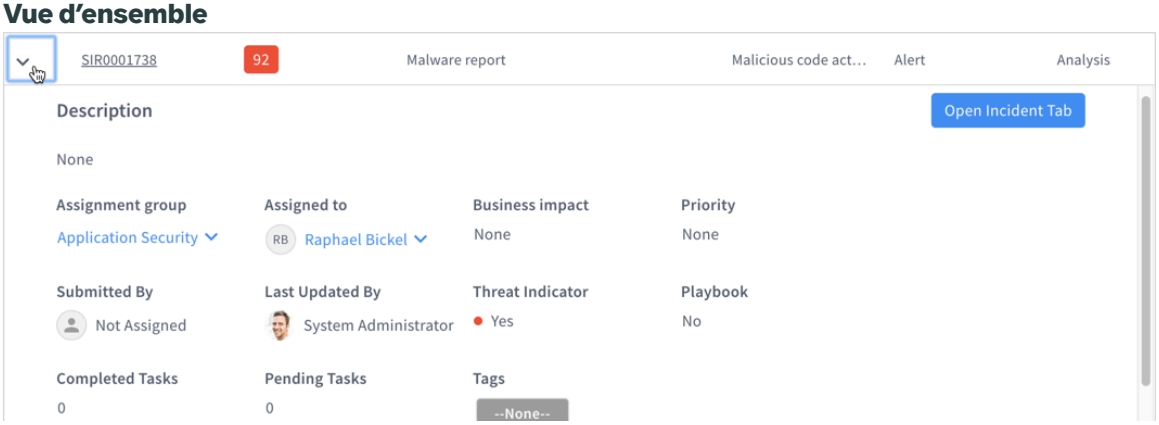
Personnaliser la liste des incidents de sécurité



Gagnez du temps avec la vue d'aperçu

Avant d'ouvrir un enregistrement d'incident de sécurité, vous pouvez gagner du temps à l'aide de la vue d'aperçu. Cette fonctionnalité vous permet de localiser rapidement les artefacts de sécurité vitaux sans avoir à recharger la page entière. Cliquez simplement sur l'icône **>** à gauche d'un numéro d'incident de sécurité pour y jeter un coup d'œil.

Vue d'ensemble

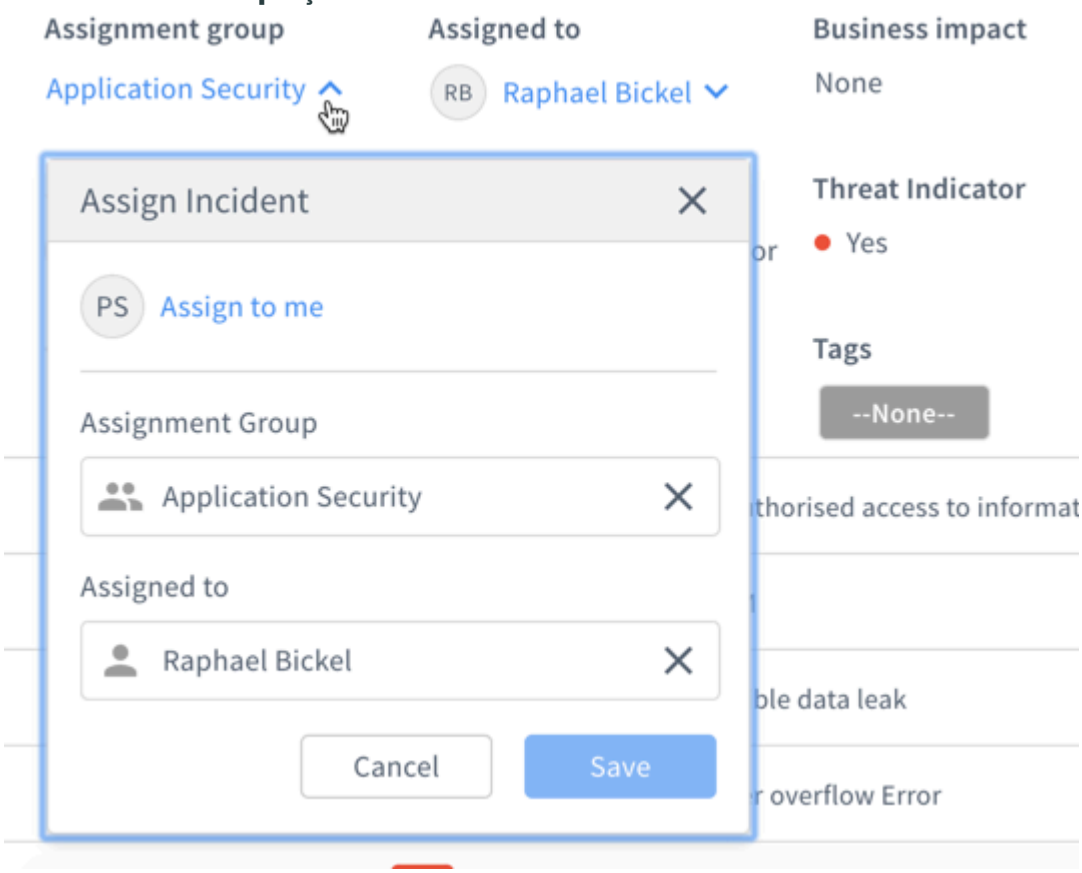


La vue d'aperçu fournit un instantané des informations vitales en une seule vue. Cette vue peut vous faire gagner un temps précieux lorsque vous travaillez avec plusieurs incidents. Vous pouvez cliquer sur les flèches vers le bas de certains champs pour effectuer des mises à jour à la volée, telles que l'affectation d'un groupe d'affectation ou d'un analyste spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de la vue d'aperçu



Effectuer des actions rapides sur un incident de sécurité

Une fois que vous avez sélectionné et ouvert un incident de sécurité spécifique, vous pouvez effectuer des actions de gain de temps sur l'enregistrement.

- Si votre incident de sécurité est ouvert, cliquez sur l'icône **Modifier l'enregistrement** pour apporter des modifications rapides à l'un de ses champs. Si l'enregistrement est fermé, vous ne pouvez modifier que sa balise.
- Cliquez sur **Gérer les pièces jointes** pour joindre des fichiers à l'incident de sécurité. Vous pouvez également télécharger ou supprimer des fichiers joints et modifier le chiffrement appliqué aux pièces jointes.
- Cliquez sur **Composer un e-mail pour envoyer un e-mail** rapide à un collègue. Les e-mails peuvent être de forme libre ou vous pouvez envoyer des e-mails prédéfinis sélectionnés dans une liste de modèles. Les e-mails envoyés et les réponses reçues sont capturés dans la chronologie des incidents.

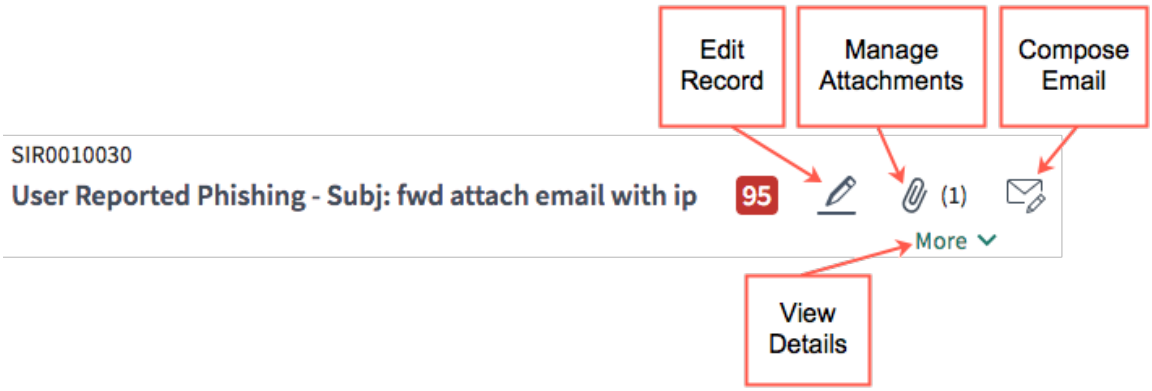
  Remarque : Vous pouvez créer des modèles personnalisés contenant du contenu réutilisable pour les e-mails et les notifications par e-mail. Les variables peuvent être utilisées pour insérer des informations spécifiques à l'incident de sécurité ou à l'alerte, telles que la ligne d'objet, la priorité ou la catégorie de menace. Utilisez la table Incident de sécurité [sn_si_incident] pour les e-mails et notifications par e-mail associés à Réponse aux incidents de sécurité. Pour plus d'informations, voir Modèles d'e-mail

- Cliquez sur **Plus** pour afficher un instantané rapide de l'incident de sécurité, tel que la description, l'impact sur l'entreprise et la priorité. Vous pouvez également cliquer sur la flèche vers le bas dans les champs **Groupe d'affectation** et **Affecté à** pour apporter des modifications à la volée à ces champs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

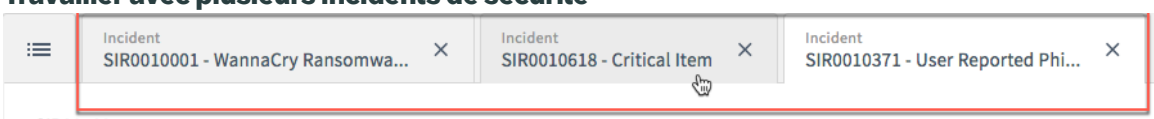
Groupe d'affectation



Travailler avec plusieurs incidents de sécurité

L'interface à onglets vous permet de conserver plusieurs incidents de sécurité ouverts simultanément afin de pouvoir passer de l'un à l'autre en un seul clic. Cela peut vous faire gagner du temps et vous permettre d'avoir une vue d'ensemble lorsque des menaces provenant de plusieurs sources sont identifiées.

Travailler avec plusieurs incidents de sécurité



Afficher les informations d'analyse dans les onglets Incident de sécurité

Lorsque vous ouvrez un enregistrement d'incident de sécurité, trois onglets s'affichent :

- Vue d'ensemble
- Explorer
- Chronologie des incidents

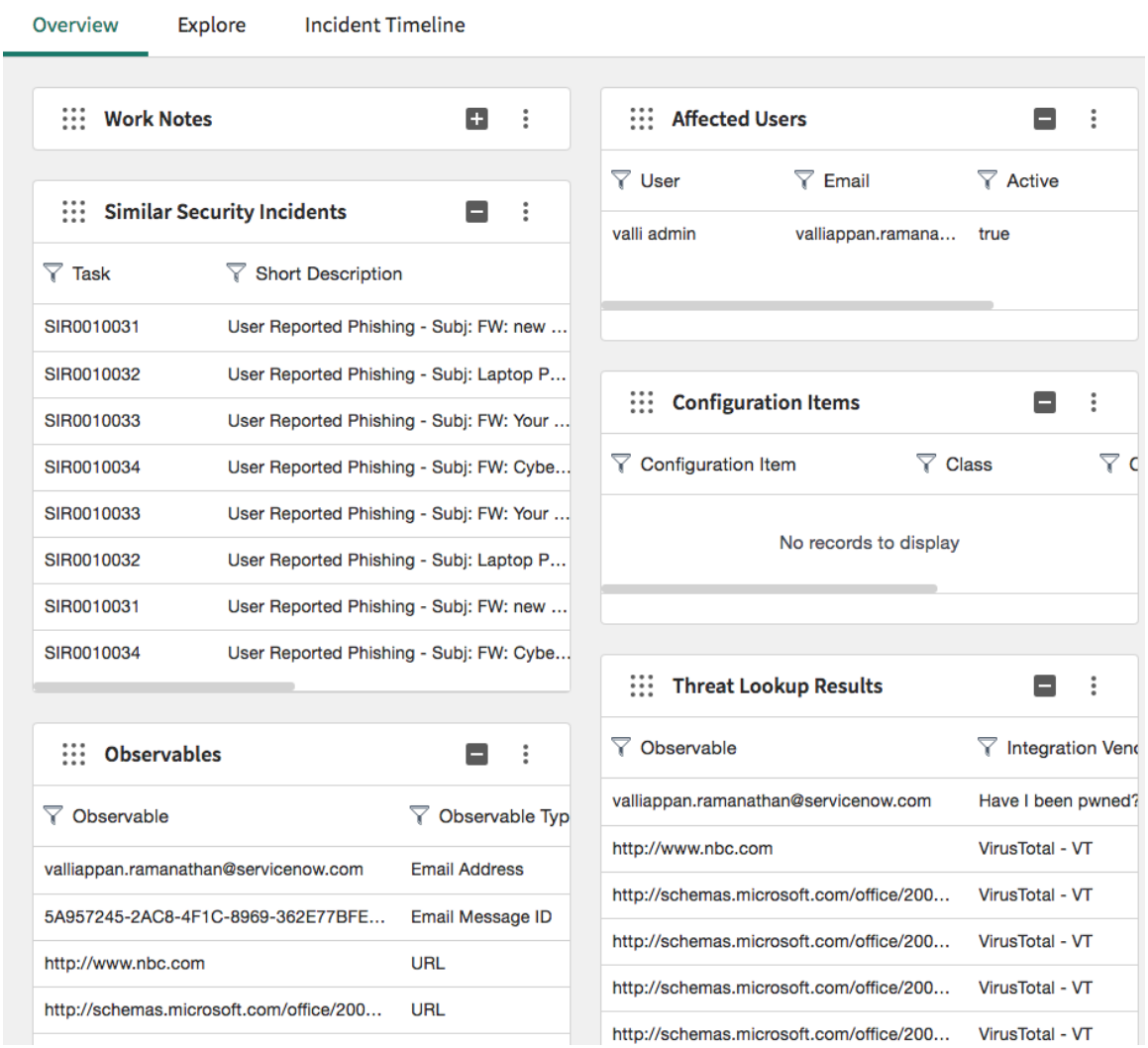
Onglet Vue d'ensemble

Utilisez l'onglet **Vue d'ensemble** pour afficher les informations relatives à un incident de sécurité dans un seul emplacement. Pas besoin d'ouvrir une autre application ou console.

Traduction automatique

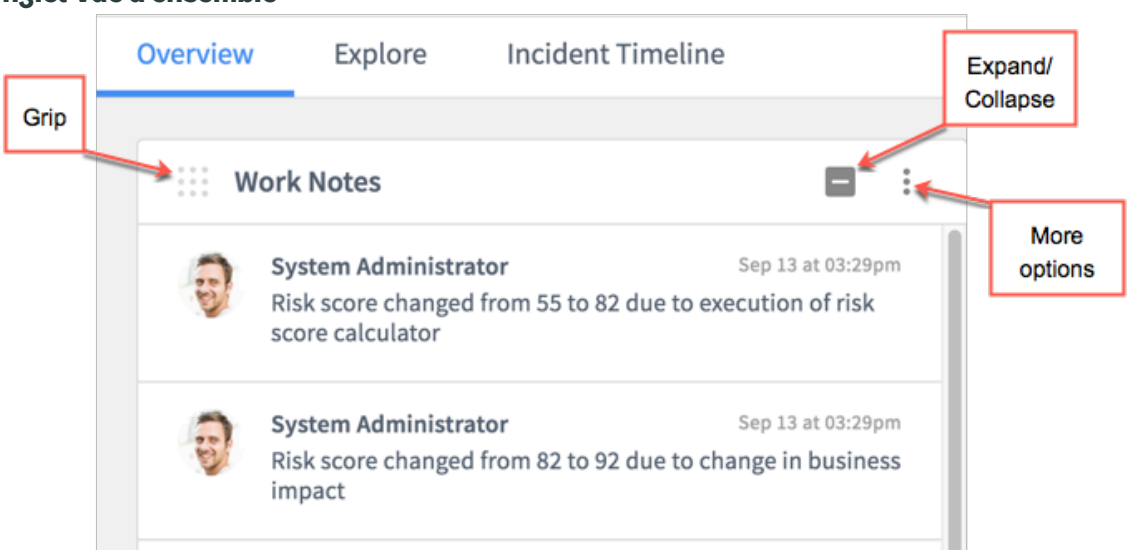
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble



Les tuiles affichées dans l'onglet **Vue d'ensemble** sont personnalisables. Vous pouvez les réduire et les développer selon vos besoins, et vous pouvez les déplacer en faisant glisser l'icône **Poignée** . Cliquez sur l'icône **Autres options** pour supprimer une tuile ou modifier son texte d'en-tête.

Onglet Vue d'ensemble



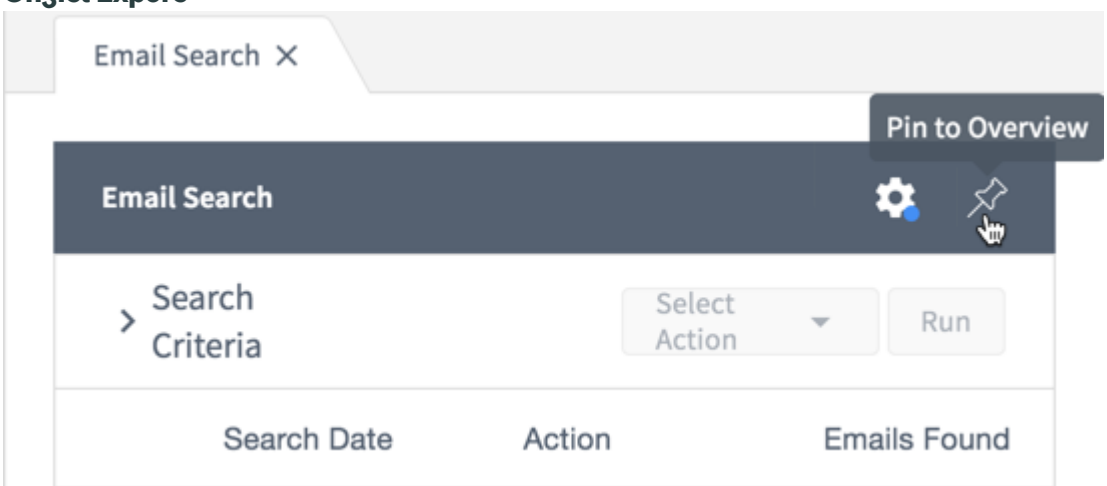
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Explorer

Configurez les tuiles affichées dans l'onglet **Vue d'ensemble à** l'aide de l'onglet **Explorer** . Sélectionnez simplement les tuiles que vous souhaitez afficher dans le volet gauche et cliquez sur l'icône **Épingler** . Les tuiles épinglées apparaissent automatiquement dans l'onglet **Vue d'ensemble** .

Onglet Expore



Le volet gauche de l'onglet **Explorer** comprend une grande variété d'informations que vous pouvez afficher dans l'onglet **Vue d'ensemble** . Par exemple, développez **Observables** pour afficher ces listes connexes.

- Observables
- Résultats de la recherche de menace
- Résultats de l'analyse de sécurité
- Recherches de domaine
- Enrichissement des éléments observables

Des listes connexes supplémentaires sont disponibles sous **Utilisateurs**, **Éléments de configuration** et **Incidents**.

Onglet Chronologie des incidents

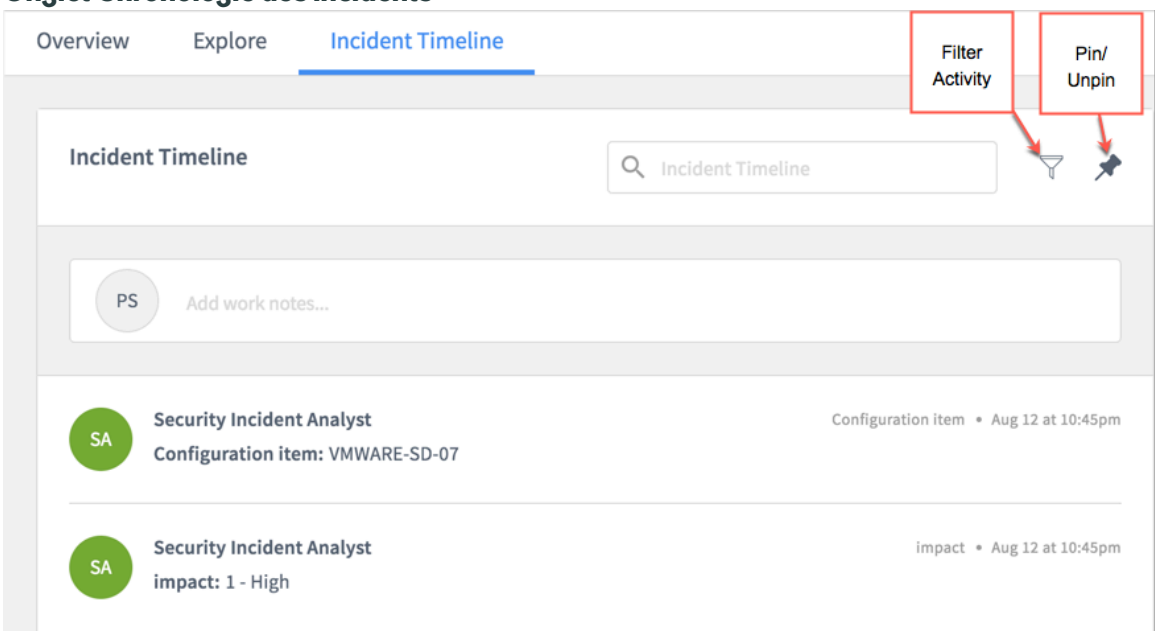
Utilisez l'onglet **Chronologie des incidents** au cours de votre enquête à des fins de suivi. Chaque fois qu'une action est effectuée sur un incident de sécurité, le système l'enregistre dans la chronologie des incidents.

- Vous pouvez également ajouter manuellement des notes de travail à la chronologie en les saisissant dans la zone **Ajouter des notes de travail** et en cliquant sur **Publier**.
- Vous pouvez rechercher une activité de chronologie spécifique à l'aide de la zone de recherche.
- L'icône **Filtrer l'activité** vous permet d'afficher uniquement les types d'activité de chronologie que vous souhaitez afficher (par exemple, uniquement les incidents créés par un analyste spécifique).
- Vous pouvez ajouter ou supprimer la chronologie des incidents à partir de l'onglet **Vue d'ensemble** à l'aide de l'icône **Épingler/Désépingler** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Chronologie des incidents



Gérer les incidents de sécurité à l'aide du Playbook

Résolvez certains types de menaces à la sécurité étape par étape à l'aide des playbooks d'analyste de sécurité intégrés. Par exemple, un analyste peut utiliser le playbook pour résoudre les attaques de phishing et les menaces causées par des activités de code malveillant. Pour plus d'informations, consultez Résoudre les menaces de sécurité avec le playbook.

Résoudre les menaces de sécurité avec le playbook

Utilisez le Playbook pour résoudre certains types de menaces à la sécurité étape par étape. Par exemple, vous pouvez résoudre les attaques de phishing et les menaces causées par l'activité de codes malveillants à l'aide de playbooks.

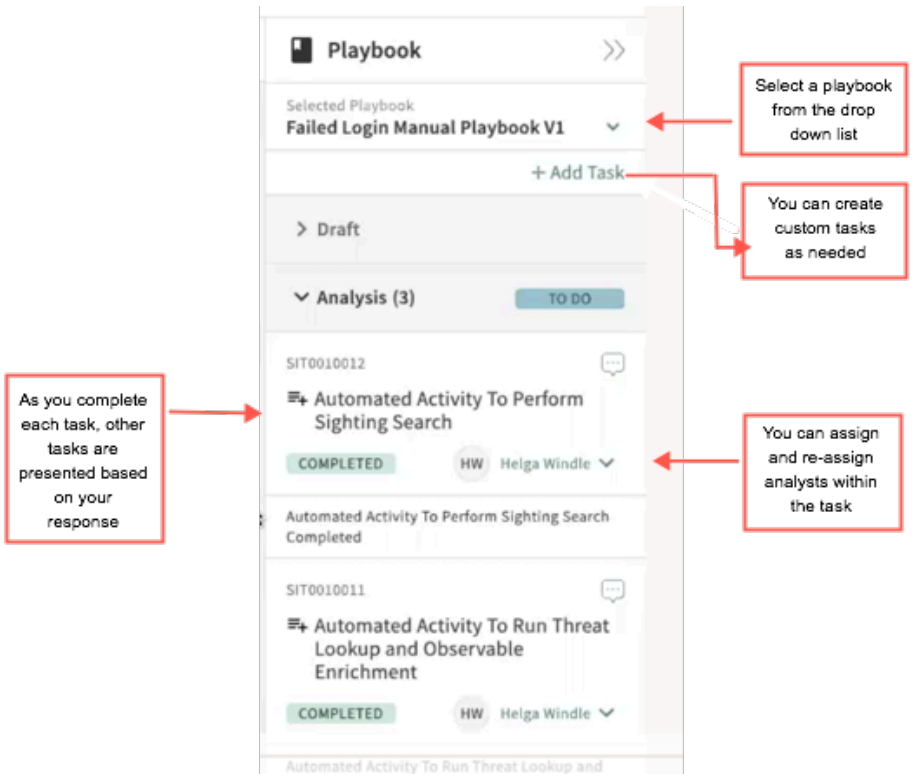
Avant de commencer
Rôle requis : sn_si.admin ou admin

Pourquoi et quand exécuter cette tâche
Chaque groupe de tâches (Analyse, Contenir, etc.) vous guide à travers une série de questions et d'autres activités pour résoudre la menace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

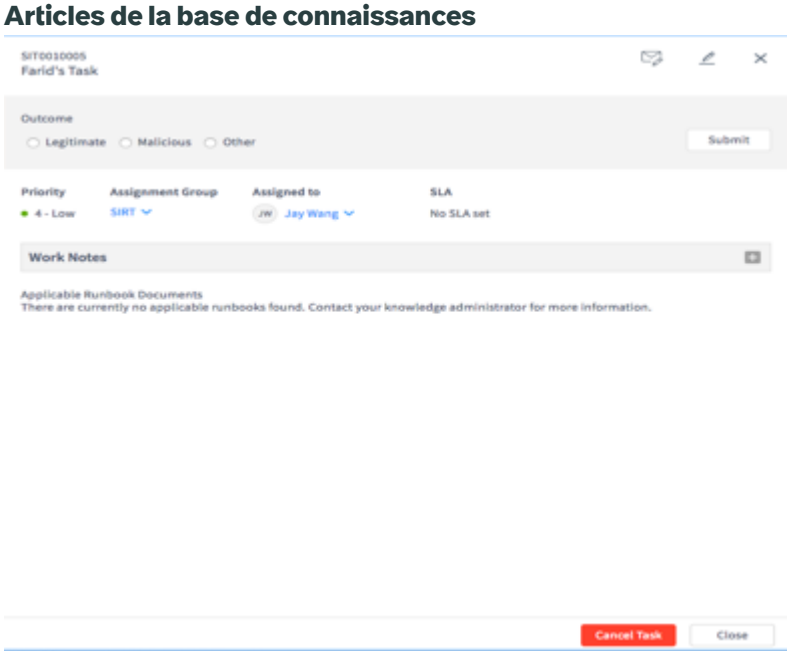
Playbook



Au fur et à mesure que vous travaillez sur chaque tâche, saisissez des notes de travail pour vous aider à analyser des attaques similaires à l'avenir. Une fois qu'une menace est identifiée, vous pouvez également utiliser les informations du playbook pour mettre la menace en quarantaine, isoler les actifs affectés de la même manière et supprimer les logiciels malveillants.

Les articles de la base de connaissances, inclus dans chaque tâche, fournissent des conseils et d'autres informations pour vous aider à effectuer les étapes nécessaires.

Articles de la base de connaissances



Traduction automatique

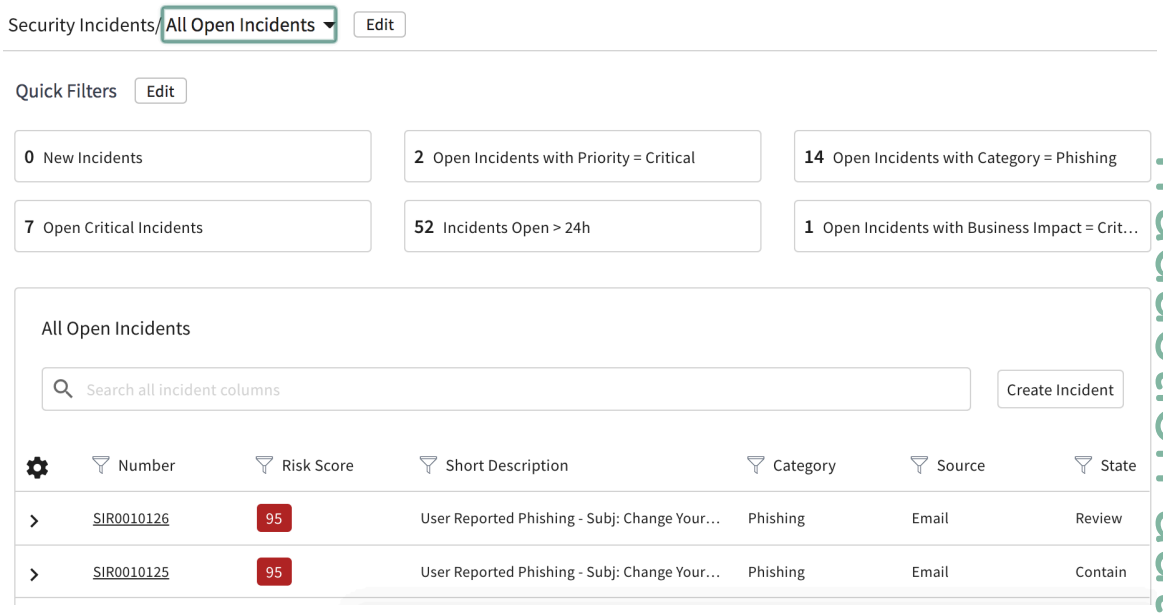
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le système de base inclut des articles de la base de connaissances pour chacune des tâches du playbook. Vous pouvez toutefois écrire vos propres articles de la base de connaissances et les associer à des tâches de playbook.

Remarque : Pour obtenir un exemple d'utilisation du playbook pour analyser et résoudre une menace spécifique, reportez-vous à la section Résoudre les attaques de phishing signalées par les utilisateurs avec le playbook.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents (nouvelle interface utilisateur)**.
   L'écran Incidents de sécurité affiche les incidents de sécurité qui vous ont été affectés.



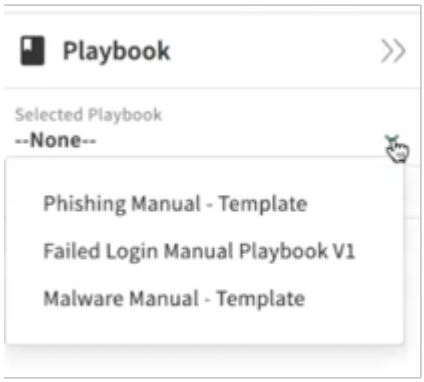
2. Vous pouvez cliquer sur la liste de choix **Mes affectations** pour sélectionner un autre filtre, tel que tous les incidents ouverts ou tous les incidents non affectés.
   Vous pouvez également cliquer sur l'un des filtres rapides pour afficher les incidents de sécurité d'un type particulier, comme uniquement les incidents critiques.
3. Cliquez sur l'incident de sécurité que vous souhaitez analyser.

   Envisagez de donner la priorité aux incidents de sécurité avec des scores de risque élevés.

4. Si le volet du playbook sur le bord droit de l'écran est fermé, cliquez sur l'icône du playbook ( ) pour l'ouvrir.
   Si aucun playbook n'est affecté à l'incident de sécurité, vous pouvez sélectionner un playbook dans la liste de choix de Playbooks sélectionnés, comme indiqué ci-dessous :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez également affecter un autre playbook à l'incident de sécurité. Pour inclure un playbook dans la liste de choix de Playbooks sélectionnés ou pour modifier le playbook en cas d'incident de sécurité, consultez la rubrique Activer les playbooks pour la sélection des analystes pour en savoir plus.

Le playbook spécifique au type de menace de sécurité s'ouvre. Il est divisé en catégories de tâches similaires. Par exemple, vous utilisez les tâches du groupe **Analyse** pour déterminer la validité et l'étendue de la menace. Le groupe **Contenir** comprend des tâches visant à isoler la menace qui pèse sur un utilisateur ou un actif spécifique. Les tâches du groupe **Éradiquer** vous guident tout au long du processus de suppression du programme malveillant ou de réimagerie de l'hôte.

5. Cliquez sur le premier groupe (**Analyse**), puis cliquez sur la première tâche dans le playbook.
6. Suivez les invites de la tâche.
   - Certaines tâches posent une question, par exemple « L'e-mail fait-il partie de la campagne ? » Effectuez l'analyse nécessaire pour répondre à la question et sélectionnez **Oui** ou **Non**.
   - Si vous avez défini des articles de la base de connaissances et que vous les avez associés à des tâches de playbook, les articles s'affichent lorsque vous commencez à travailler sur une tâche.
   - Certaines tâches sont transitoires. Ils vous demandent simplement d'effectuer une action, comme l'ajout d'observables à un incident de sécurité. Une fois l'action terminée, cliquez sur **Marquer comme terminé.**

   Au fur et à mesure que vous accomplissez des tâches, les tâches suivantes vous sont présentées en fonction des choix que vous faites. Les groupes grisés (tels que **Récupérer**, **Revoir**, etc.) peuvent être activés par vos choix.
7. Continuez à travailler sur chaque tâche qui vous est présentée jusqu'à ce que vous ayez terminé toutes les tâches visant à résoudre la menace et à fermer l'incident de sécurité.

Information associée

Ajouter une tâche personnalisée au playbook

Résoudre les attaques de phishing signalées par les utilisateurs avec le playbook

Le playbook d'hameçonnage vous guide à travers les tâches nécessaires à l'analyse et à la résolution d'une attaque d'hameçonnage signalée par l'un des employés de votre entreprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

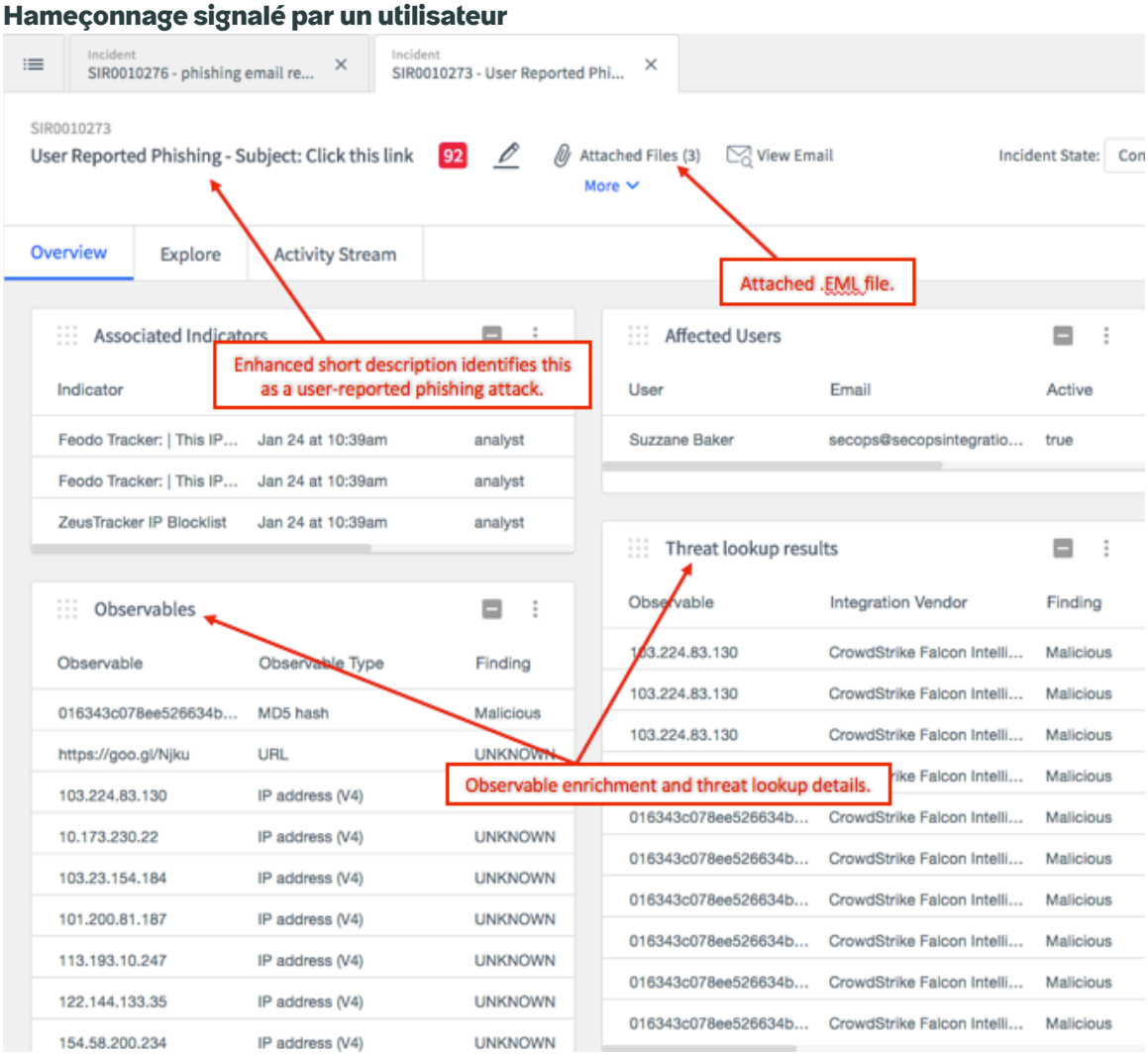
Comment les incidents de sécurité sont créés à partir d'attaques de phishing signalées par un utilisateur

Pendant la configuration de Réponse aux incidents de sécurité, votre administrateur système crée une série de règles de correspondance d'e-mails qui peuvent identifier les e-mails contenant des signes d'attaque d'hameçonnage. Lorsque les employés reçoivent un e-mail suspect contenant les signes courants d'une attaque de phishing (tels que définis par vos politiques de sécurité), ils peuvent l'envoyer sous forme de . Pièce jointe EML à l'adresse e-mail d'hameçonnage définie par votre organisation.

Lorsque l'e-mail est reçu à l'adresse e-mail d'hameçonnage, le fichier . La pièce jointe EML est analysée et ses informations sont comparées aux règles de correspondance d'e-mail. Si une correspondance est trouvée, un incident de sécurité contenant les informations suivantes est créé :

- La brève description inclut le hameçonnage signalé par un utilisateur, suivi de l'objet réel de l'e-mail d'origine.
- Le. Le fichier EML est joint à l'incident de sécurité.
- Si le . EML contient tous les observables, ils sont analysés et les recherches d'enrichissement et de menace sont automatiquement effectuées.

Hameçonnage signalé par un utilisateur

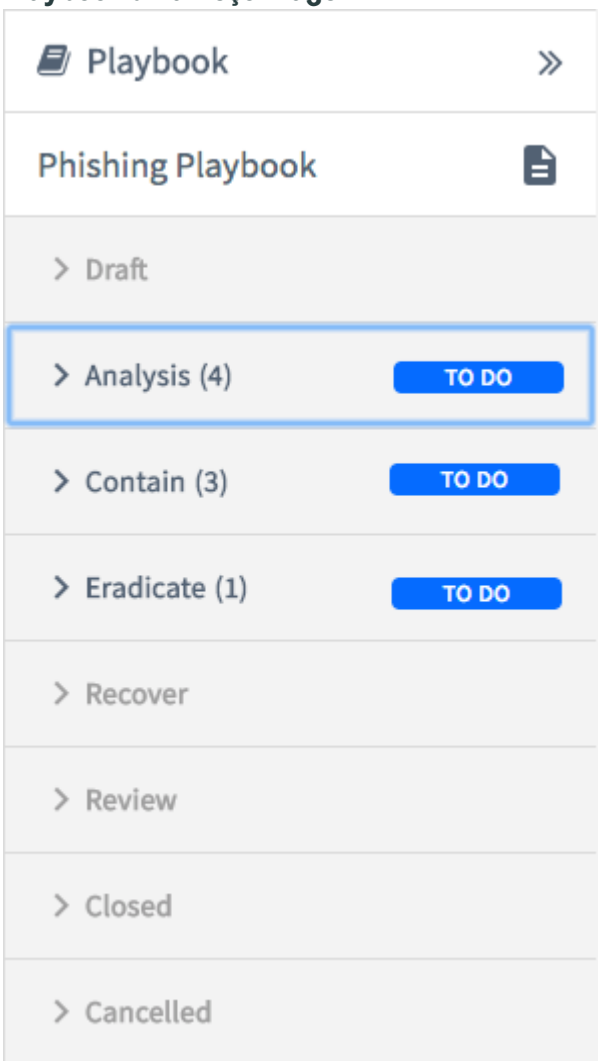


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsqu'un incident de sécurité de catégorie hameçonnage est ouvert, le Playbook d'hameçonnage est automatiquement disponible. Cliquez simplement sur l'icône du playbook ( ) pour ouvrir le playbook.

Playbook d'hameçonnage



Le playbook d'hameçonnage contient des tâches pour vous aider à analyser, contenir et éradiquer une menace d'hameçonnage. Les tâches sont organisées en états (par exemple, **Analyse**, **Contenir**, etc.). Lorsque toutes les tâches pour un état ont été terminées, le playbook vous guide vers l'état suivant.

Analyse des détails de l'incident de sécurité

Lorsque l'incident de sécurité est à l'état Analyse, vous disposez de tâches pour effectuer une enquête de base sur l'incident, notamment :

- détermination de la validité de l'incident.
- Étudier l'impact de la menace potentielle.
- Coordonner une réponse efficace à l'incident.

Au fur et à mesure que vous accomplissez les tâches :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Familiarisez-vous avec les articles de la base de connaissances.
- Ouvrez la pièce jointe de l'e-mail et examinez-la pour détecter des signes d'éléments de phishing courants.
- Examinez les résultats de la recherche de menaces.

Contenir l'incident de sécurité

Lorsque l'incident de sécurité est à l'état **Maîtriser** , vous avez pour tâche d'examiner les détails de l'e-mail. Pour vous assurer que les menaces ne peuvent pas pénétrer dans votre organisation, mettez à jour les défenses de votre réseau, sous la forme de signatures et de règles du système de défense contre les intrusions (IDS) et du système de prévention des intrusions (IPS).

Au fur et à mesure que vous accomplissez les tâches :

- Prenez des mesures pour limiter les impacts des menaces, telles que l'isolation des appareils impactés.
- Examinez les observables joints à l'e-mail.
- Déterminez si le contenu d'un e-mail est associé à une menace connue, notamment :
  - URL
  - Expéditeur d'e-mail
  - URL de hameçonnage
  - Adresse IP du serveur SMTP de l'expéditeur

Éradiquer le programme malveillant

Après avoir déployé des signatures et des règles mises à jour dans votre solution antivirus, utilisez les tâches à l'état **Éradiquer** pour déterminer la présence d'un programme malveillant et le gérer en conséquence.

Pendant que vous travaillez sur les tâches :

- Analysez les points de terminaison des appareils affectés pour détecter la présence de logiciels malveillants.
- Supprimez tout programme malveillant trouvé.
- En dernier recours, effacez et recréez l'image des appareils hôtes.

Examen de l'incident de sécurité

Si vous avez déterminé qu'une attaque d'hameçonnage était une fausse alerte lors de l'exécution des tâches d'analyse, l'incident de sécurité passe à l'état **Examen** et vous devez en informer vos utilisateurs afin qu'ils sachent qu'il est possible d'ouvrir la pièce jointe en toute sécurité.

Fermeture de l'incident de sécurité

Lorsque toutes les tâches du playbook ont été terminées, l'incident de sécurité passe à l'état **Fermé** . Vous devez saisir des commentaires de fermeture pour pouvoir fermer l'incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Annulation d'un incident de sécurité

Lorsqu'un incident de sécurité est à l'état **d'examen** et que vous avez informé vos utilisateurs que l'e-mail ne constitue pas une menace, l'état **Annulé** devient actif et vous pouvez annuler l'incident de sécurité.

Remarque : La tâche de récupération n'est pas utilisée dans le playbook d'hameçonnage.

Associer un article de la base de connaissances à une tâche de playbook

Lorsque vous analysez les menaces de sécurité à l'aide du playbook, vous pouvez consulter les articles de Réponse aux incidents de sécurité la base de connaissances pour chaque tâche si votre organisation les définit. Si les articles de la base de connaissances ne sont pas présents, vous pouvez les créer et les associer à des tâches du playbook.

Avant de commencer

Lorsque vous utilisez le playbook dans Réponse aux incidents de sécurité, notez le texte associé à chaque tâche. Par exemple, la première tâche de la catégorie Hameçonnage est **Alerte a-t-elle été envoyée par l'employé ?** Il s'agit de la brève description de la tâche et vous avez besoin de ce texte (exactement comme il apparaît dans le playbook) pour associer un article de la base de connaissances à la tâche.

Rôle requis : sn_sir.knowledge_admin et sn_si.admin ou admin

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Catalogue et base de connaissances** > **Base de connaissances**.
2. Créez et publiez un article de la base de connaissances pour une tâche Playbook spécifique.
3. Accédez à la **Incident de sécurité** > **Runbook manuel** > **Créer un nouveau Runbook**.
4. Créez un runbook en renseignant les informations suivantes :

Champ	Description
Article de la base de connaissances	Sélectionnez l'article de la base de connaissances publié que vous souhaitez associer à la tâche Playbook.
Table	Sélectionnez Réponse aux incidents de sécurité la tâche [sn_si_task].
Condition	Définissez le générateur de conditions sur : ○ **Option:** Sélectionnez **Brève description**. ○ **Opérateur:**Sélectionnez **est**. ○ **Valeur d'entrée :** Saisissez la description brève de la tâche, telle qu'elle apparaît dans le playbook.

5. Cliquez sur **Envoyer**.
   La prochaine fois que vous exécuterez le playbook et que vous sélectionnerez cette tâche, l'article de la base de connaissances associé s'affichera.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Créer un article de la base de connaissances sur les incidents de sécurité

Créer un Runbook de réponse aux incidents de sécurité

Ajouter une tâche personnalisée au playbook

Le Security Analyst Workspace système de base comprend une série de tâches pour chaque catégorie de menace. Vous pouvez créer des tâches personnalisées qui répondent aux besoins uniques de votre système ou de vos clients.

Avant de commencer

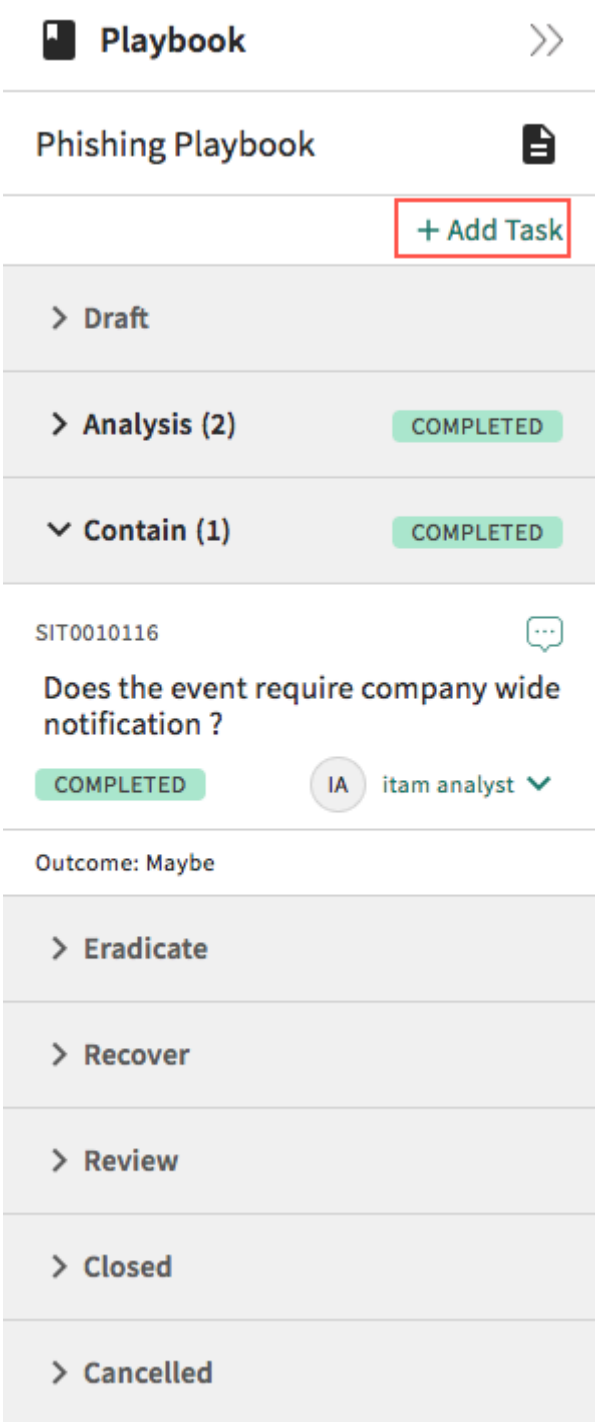
Rôle requis : sn_si.basic ou security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

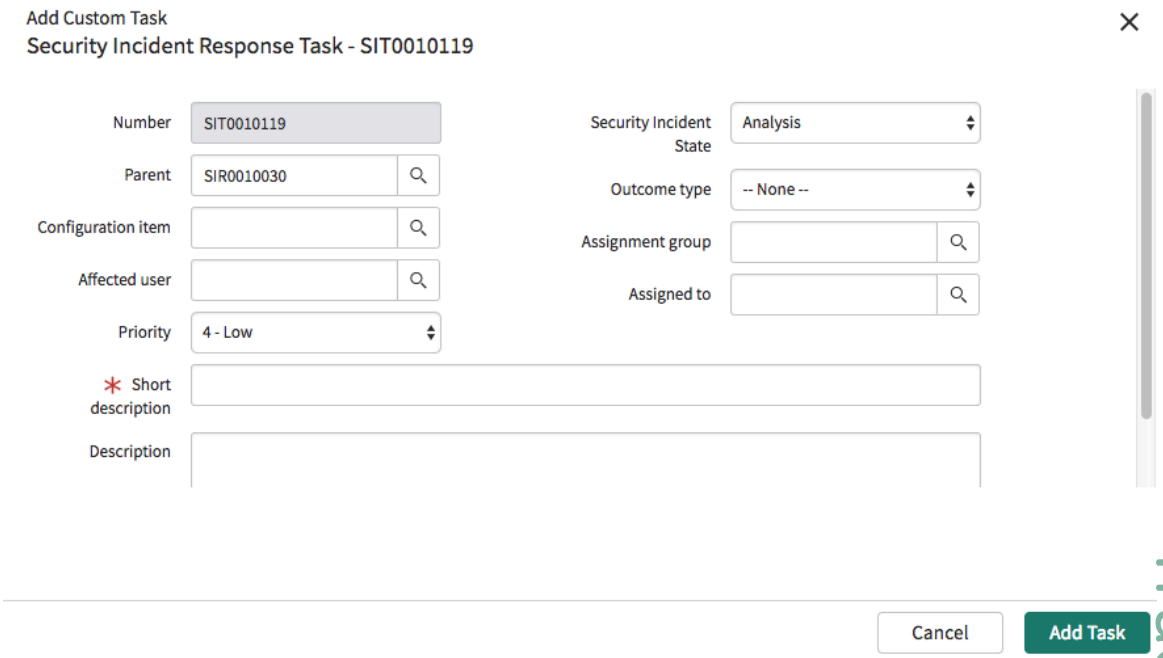
1. Une fois le playbook ouvert, cliquez sur **Ajouter une tâche**.



L’écran Ajouter une tâche personnalisée s’ouvre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Renseignez les champs nécessaires.

Champ	Description
Numéro	[Lecture seule] Numéro de tâche d'incident de sécurité généré automatiquement.
Parent	Numéro de l'incident de sécurité connexe.
Élément de configuration	Élément de configuration affecté par le problème de sécurité, le cas échéant.
Utilisateur affecté	Utilisateur affecté par le problème de sécurité, le cas échéant.
Priorité	Sélectionnez la priorité utilisée pour déterminer quand cette tâche doit être effectuée.
État de l'incident de sécurité	État actuel de la tâche de réponse de sécurité. Vous pouvez sélectionner un état futur, si nécessaire.
Type de résultat	Si vous disposez du rôle sn_si.basic, sélectionnez **Oui/Non** comme type de résultat. Si vous disposez du rôle security_admin, vous pouvez créer un type de résultat personnalisé avec plusieurs valeurs de sortie personnalisées. Par exemple, vous pouvez définir une tâche avec des valeurs dépendantes en fonction de la catégorie de menace. Pour plus d'informations, voir Listes de choix
Groupe d'affectation	Groupe d'affectation à partir duquel l'agent affecté sera sélectionné.
Affecté à	Personne affectée à l'exécution de la tâche.
Description brève	Une description de la tâche du playbook d'incident de sécurité.
Description	Saisissez une description pour la tâche sélectionnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Lorsque vous avez terminé vos entrées, cliquez sur **Ajouter une tâche**.
   La tâche est insérée dans le playbook après la tâche actuelle.

Recherches de perceptions sur les attaques de phishing et de programmes malveillants signalées par les utilisateurs

Effectuez des recherches de perception sur des e-mails ou des observables pour déterminer la fréquence à laquelle certains types d'attaques, tels que les attaques de phishing ou les communications avec une adresse IP ou une URL malveillante, se produisent sur votre réseau. Chaque occurrence est considérée comme une observation. Les recherches de perceptions pour les observables doivent être configurées pour vos magasins de journaux ou pour la gestion des informations et événements de sécurité (SIEM).

Comment utiliser la fonctionnalité de recherche de perception pour localiser les utilisateurs hameçonnés et suivre les observables de hameçonnage et de programmes malveillants dans le magasin de journaux de votre réseau.

Regardez cette vidéo de trois minutes pour découvrir comment utiliser la fonctionnalité de recherche de perception pour localiser les utilisateurs hameçonnés et suivre les observables de hameçonnage et de programmes malveillants dans le magasin de journaux de votre réseau.

Les termes suivants sont utilisés pour décrire les attaques de phishing signalées par les utilisateurs :

- Utilisateur hameçonné : utilisateur qui a reçu un e-mail d'hameçonnage.
- Utilisateur victime : utilisateur qui a interagi avec l'URL d'hameçonnage, généralement en cliquant sur un lien dans l'e-mail d'hameçonnage. Cette action expose potentiellement les informations d'identification à l'attaquant.

Lorsque vous commencez à analyser un incident d'hameçonnage, vous pouvez effectuer une recherche d'observations d'e-mails ou unerecherche d'observations d'observables pour identifier les autres utilisateurs de votre organisation qui sont impactés par la même attaque d'hameçonnage. Effectuez des recherches dans vos magasins de journaux pour identifier les utilisateurs hameçonnés et victimes. Une fois que vous avez identifié la liste des utilisateurs affectés, créez des incidents de sécurité enfants pour exécuter des procédures de réponse aux incidents complètes à l'aide des outils disponibles dans Réponse aux incidents de sécurité.

Remarque : Vous pouvez également utiliser l'approche suivante pour effectuer une recherche d'observations :

- Accédez à la **Incidents de sécurité** > **Afficher les incidents** et cliquez sur un incident de sécurité.
- Cliquez sur **Afficher l'IoC** sous Liens connexes. La liste des observables s'affiche.
- Sélectionnez un observable dans la liste et, dans la liste **Actions** , sélectionnez l'une des options suivantes :
  - Exécuter la recherche de perception du trafic web
  - Exécuter la recherche de perception du trafic des e-mails
- Spécifiez le délai et cliquez sur **Rechercher** pour effectuer une recherche de perceptions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurations de recherche de perceptions enregistrées

Configurez les recherches de perception et créez des configurations enregistrées pour les SIEM ou d'autres magasins de journaux pour les instances d'observables afin de déterminer la présence d'observables malveillants dans votre environnement.

Remarque : Les recherches enregistrées et les requêtes sur place sont prises en charge pour Splunk Integration uniquement.

Information associée

Créer des enregistrements de configuration de recherche de perceptions

Effectuer une recherche de perceptions d'e-mails pour les attaques de phishing signalées par un utilisateur

Recherchez les utilisateurs qui ont reçu des e-mails d'hameçonnage en fonction d'observables tels que l'objet de l'e-mail, le nom de l'expéditeur ou l'ID du message. Vous pouvez ensuite contenir et éradiquer ces e-mails d'hameçonnage de votre organisation.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Recherchez les journaux de trafic des e-mails Splunk pour rassembler la liste des destinataires d'un e-mail suspect. La recherche peut être effectuée en utilisant l'expéditeur de l'e-mail, l'ID de l'e-mail ou l'objet de l'e-mail associé à un incident de sécurité comme critères.

Remarque :

- Cette implémentation de la recherche de perceptions pour les observables basés sur l'e-mail a été testée uniquement avec le magasin de journaux Splunk Enterprise.
- Les événements de journal Splunk doivent être conformes au modèle CIM (Common Information Model) pour que la requête de recherche de perceptions renvoie des résultats précis.

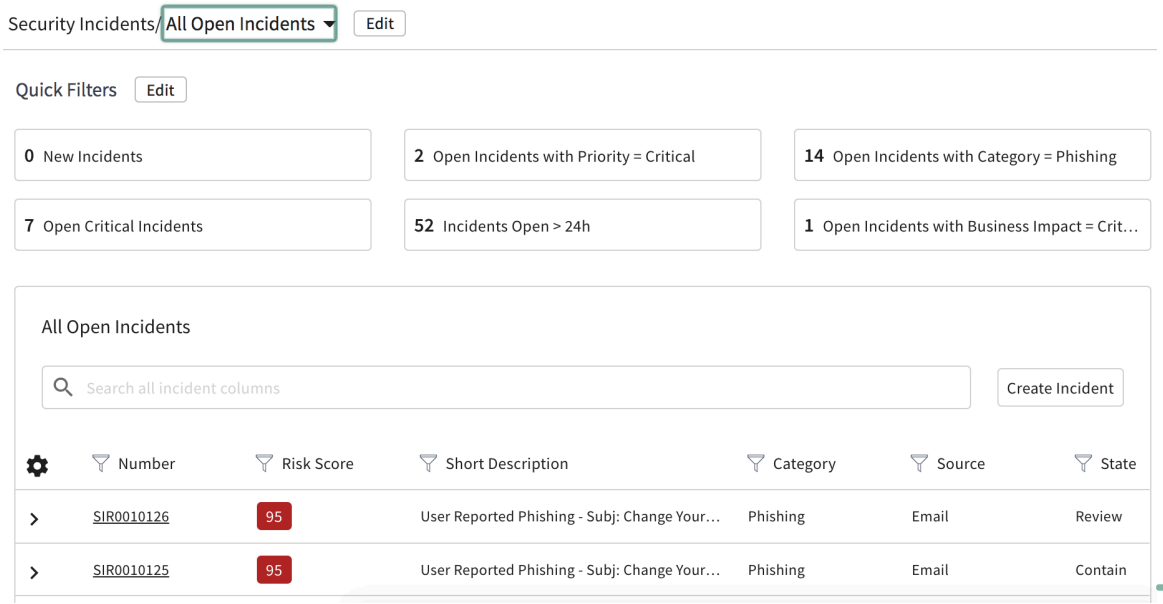
Procédure

1. Pour afficher les incidents de sécurité affectés à votre équipe, accédez à **Incident de sécurité** > **Incidents (nouvelle interface utilisateur)**.
2. Dans la liste **Incidents de sécurité** , sélectionnez l'un des filtres, tel que tous les **incidents ouverts**, **tous les incidents qui vous sont affectés** ou **tous les incidents**.

   Pour afficher les incidents de sécurité d'un type particulier, tels que les incidents critiques ou les e-mails d'hameçonnage, cliquez sur l'un des **filtres rapides**.

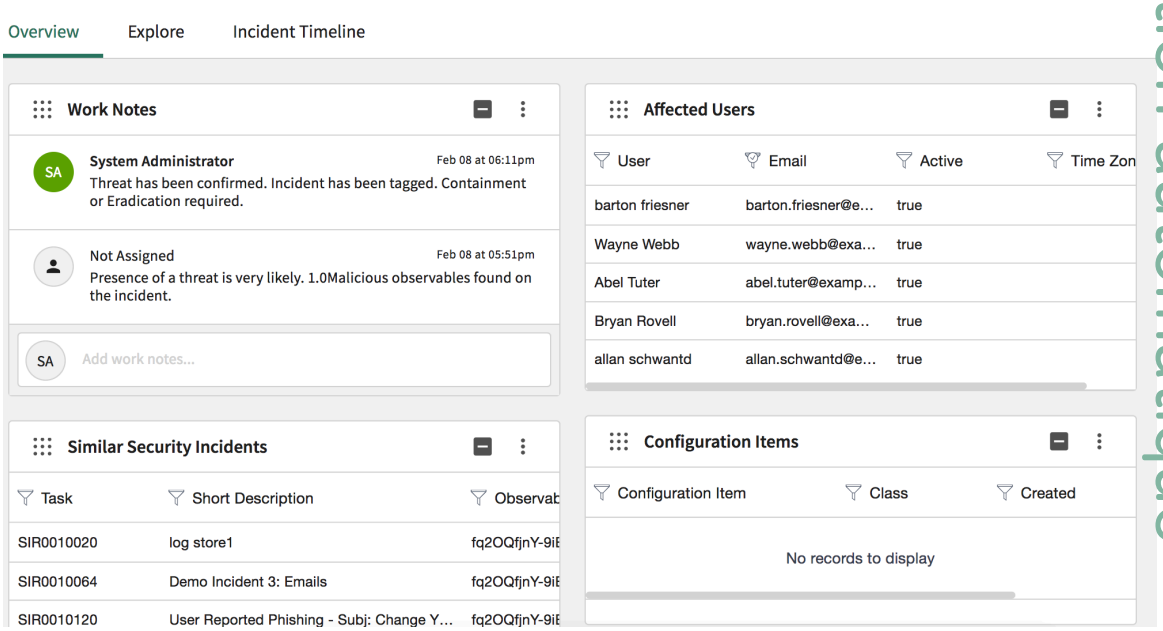
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur l'incident de sécurité que vous souhaitez analyser.

L'onglet Vue d'ensemble fournit une vue d'ensemble de l'incident de sécurité, y compris une liste des observables, des utilisateurs affectés et des incidents de sécurité similaires.

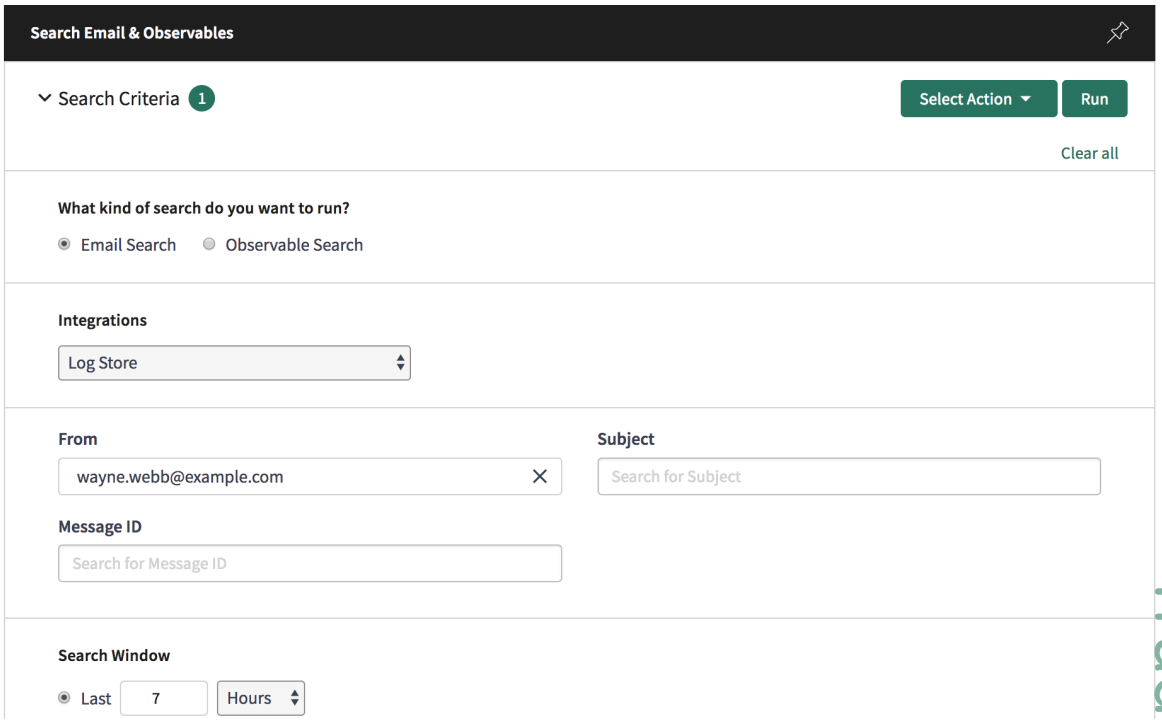


4. Cliquez sur l'onglet **Explorer** .

5. Sous **Données d'incident**, accédez à **Examen** > **Rechercher des e-mails et des observables**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Développez la section Critères de recherche.
7. Sélectionnez Recherche **d'e-mails** comme type de recherche que vous souhaitez exécuter et spécifiez le reste des critères de recherche.

Formulaire Critères de recherche

Champ	Description
Intégrations	Type d'intégration. Sélectionnez **Magasin de journaux** dans la liste. **Remarque :** Cette fonctionnalité n'est prise en charge qu'avec le magasin de journaux Splunk.
De	Adresse e-mail complète de l'expéditeur (par exemple, jane.doe@example.com).
ID de message	ID de message électronique du magasin de journaux.
Objet	Objet de l'e-mail d'hameçonnage.
Fenêtre de recherche	Intervalle de temps pour la recherche (par exemple, les dernières 24 heures).

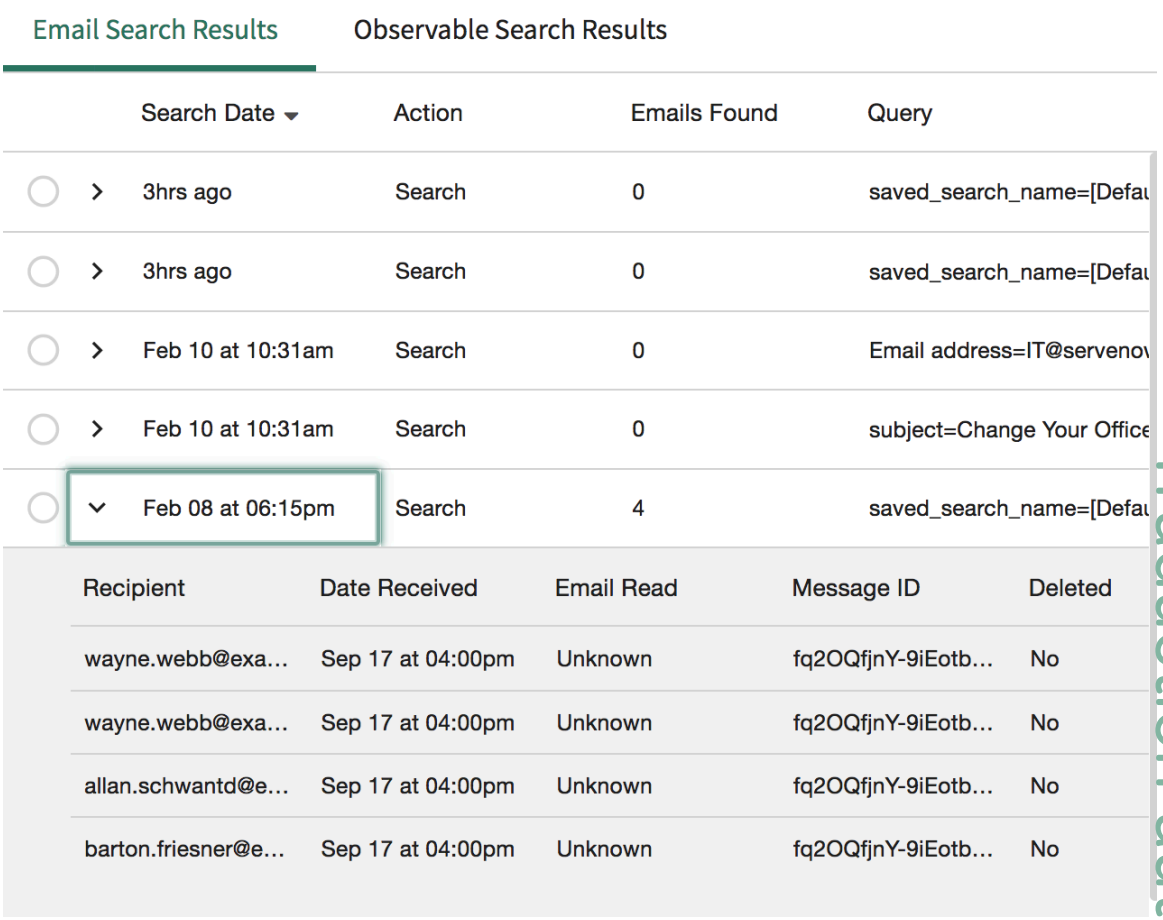
8. Dans la liste **Sélectionner une action** , sélectionnez **Rechercher** , puis cliquez sur **Exécuter**.

Les recherches dans le magasin de journaux Splunk sont effectuées à l'aide des critères que vous avez saisis, et les utilisateurs ciblés par l'attaque de phishing sont affichés dans l'onglet **Résultats de recherche d'e-mails** . Le nombre total d'e-mails d'hameçonnage et les détails de chaque e-mail, y compris la date de réception de l'e-mail, le destinataire et l'ID du message, sont affichés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Pour afficher la liste des utilisateurs qui ont reçu l'e-mail d'hameçonnage, cliquez sur le symbole de **>** dans la colonne Date de recherche.



10. Pour afficher la liste des utilisateurs qui ont reçu l'e-mail, accédez à **Utilisateurs** > **Utilisateurs affectés**.

La colonne Utilisateur hameçonné identifie les destinataires de l'e-mail.

Remarque : La page Utilisateurs affectés affiche uniquement les enregistrements utilisateur présents sur l'instance ServiceNow.

11. Pour enquêter plus en détail sur les utilisateurs cibles de l'attaque d'hameçonnage, procédez comme suit :

a. Cochez les cases en regard des noms d'utilisateurs.

b. Dans la liste, sélectionnez **Créer un incident de sécurité enfant**, puis cliquez sur **Exécuter**.
Un message s'affiche pour indiquer qu'un incident de sécurité enfant a été créé. Pour afficher les incidents de sécurité enfants associés à un incident parent, cliquez sur l'onglet **Explorer** et accédez à **Incidents** > **Incidents de sécurité enfants**.

Résultats
La liste des utilisateurs hameçonnés s'affiche.

Effectuer une recherche de perceptions observables pour les attaques de hameçonnage et de programmes malveillants signalées par un utilisateur

Effectuez des recherches de perception sur les observables pour savoir combien d'utilisateurs ont visité un site Web malveillant ou suspect au cours d'une période spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Vous pouvez effectuer une recherche de trafic réseau sur des observables tels que l'URL, l'hôte de destination ou l'adresse IP de destination associée à un incident de sécurité.

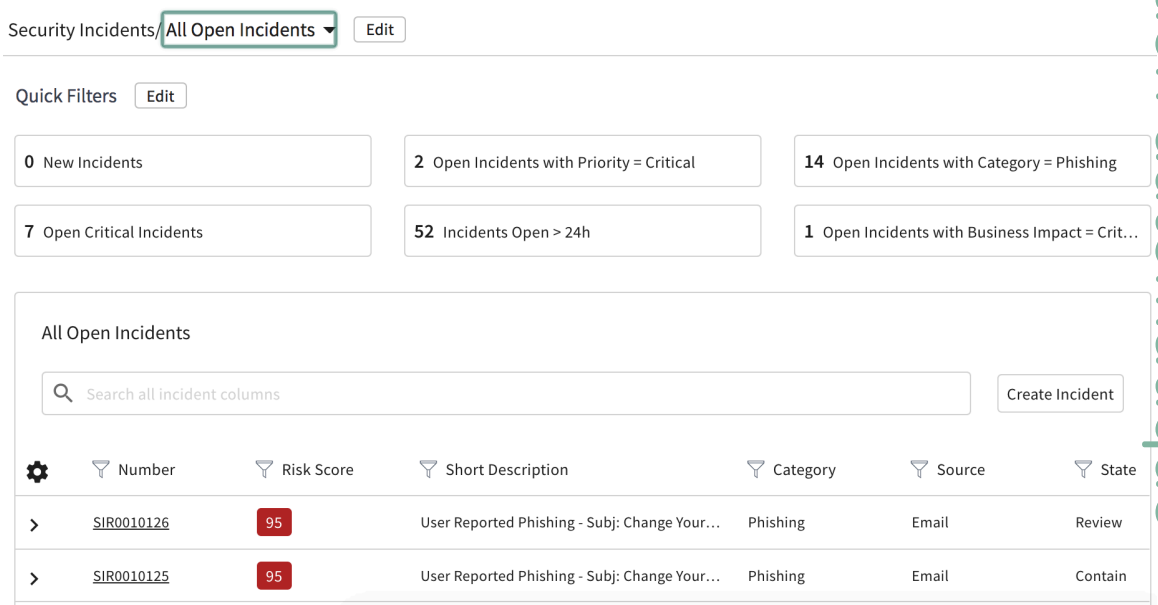
Remarque :

- Cette implémentation de la recherche de perceptions pour les observables a été testée uniquement avec le magasin de journaux Splunk Enterprise.
- Les événements de journal Splunk doivent être conformes au modèle CIM (Common Information Model) pour que la requête de recherche de perceptions renvoie des résultats précis.

Procédure

1. Pour afficher les incidents de sécurité qui sont affectés à votre équipe, accédez à **Incident de sécurité** > **Incidents (nouvelle interface utilisateur)**.
2. Dans la liste **Incidents de sécurité** , sélectionnez un autre filtre, tel que Tous les **incidents qui me sont affectés**, **Tous les incidents ouverts** ou **Tous les incidents**.

   Pour afficher les incidents de sécurité d'un type particulier, tels que les incidents critiques ou les e-mails d'hameçonnage, cliquez sur l'un des **filtres rapides**.

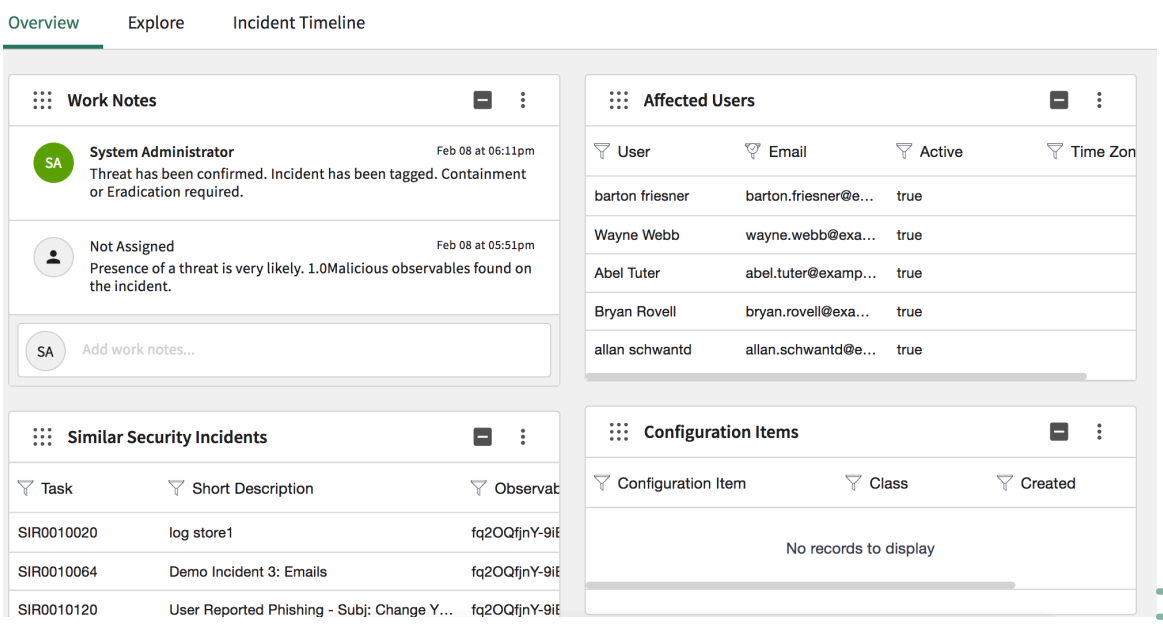


3. Cliquez sur l'incident de sécurité que vous souhaitez analyser.

   Vous pouvez voir une vue d'ensemble de l'incident de sécurité, y compris une liste des observables, des utilisateurs affectés et des incidents de sécurité similaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



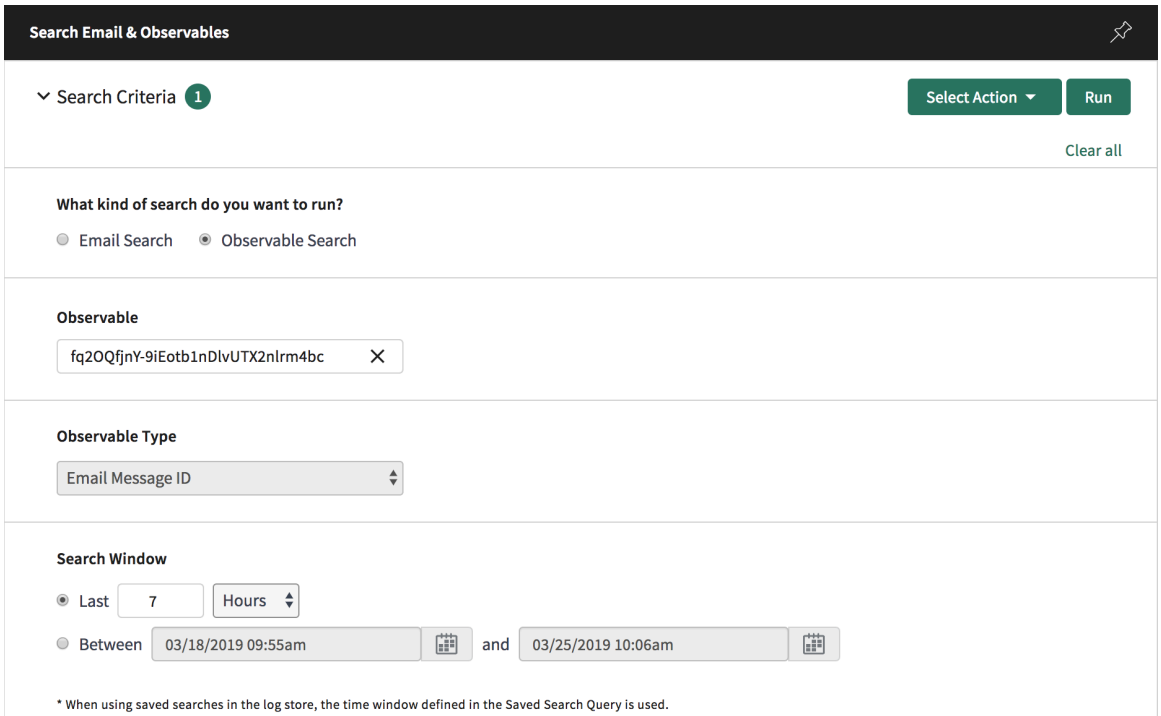
Dans la section Observables, notez que la colonne Observable affiche l'adresse e-mail, l'objet et l'URL. Notez également que la colonne Recherche indique que l'URL a été automatiquement analysée lorsque l'e-mail d'hameçonnage a été soumis et qu'il a été déterminé qu'il s'agissait d'une URL malveillante connue. La colonne Nombre d'incidents affiche les autres incidents qui partagent le même observable. Ces artefacts indiquent que vous êtes probablement prêt à passer aux procédures de maîtrise de cette attaque de phishing, notamment à déterminer combien d'utilisateurs de l'organisation ont été affectés.



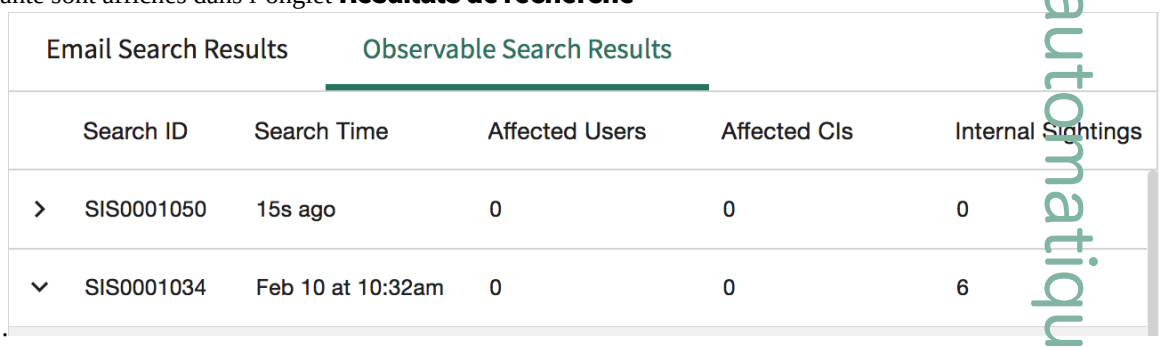
4. Accédez à la **Explorer** > **Examen** > **Rechercher des e-mails et des observables**.
5. Développez la section Critères de recherche et cliquez sur **Recherche d'observables**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Entrez l'observable que vous recherchez et une fenêtre de temps pour la recherche (par exemple, 24 dernières heures).
7. Dans la liste **Sélectionner une action** , sélectionnez **Rechercher**.
   Les recherches dans le magasin de journaux Splunk sont effectuées à l'aide des critères que vous avez entrés et les principaux utilisateurs ciblés par l'attaque malveillante sont affichés dans l'onglet **Résultats de recherche d'observables** .



8. Pour afficher les utilisateurs qui ont reçu l'e-mail, accédez à **Utilisateurs** > **Utilisateurs affectés**.

   La colonne Utilisateur hameçonné identifie les destinataires de l'e-mail d'hameçonnage et la colonne Interaction de l'utilisateur identifie les utilisateurs qui ont cliqué sur une URL d'hameçonnage ou interagi avec une adresse e-mail suspecte. La colonne Interaction de l'utilisateur est définie sur vrai ou faux, selon que l'utilisateur a cliqué sur le lien malveillant ou sur l'adresse IP.

   Remarque : La page Utilisateurs affectés affiche uniquement les enregistrements utilisateur présents sur l'instance ServiceNow.

9. Pour enquêter plus en détail sur les utilisateurs qui ont cliqué sur l'e-mail d'hameçonnage et potentiellement compromis leurs informations d'identification :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans les colonnes Utilisateur hameçonné et Interaction de l'utilisateur, cochez les cases en regard des noms d'utilisateur qui affichent **vrai**.

b. Cliquez sur **Créer un incident de sécurité enfant** , puis sur **Exécuter**.
Un message s'affiche pour indiquer qu'un incident de sécurité enfant a été créé. Pour afficher les incidents de sécurité enfants associés à un incident parent, cliquez sur l'onglet **Explorer** et accédez à **Incidents** > **Incidents de sécurité enfants**.

Résultats
La liste des utilisateurs hameçonnés s'affiche.

Créer des enregistrements de configuration de recherche de perceptions

Créez plusieurs enregistrements de configuration de recherche de perceptions et utilisez-les lors de l'interrogation de plusieurs magasins de journaux ou de la variation des paramètres de recherche.

Avant de commencer
Rôle requis : sn_si.admin

- Le module complémentaire CIM doit être installé sur l'instance Splunk.
- Les recherches enregistrées et les requêtes sur place sont prises en charge pour Splunk Integration uniquement.

Pourquoi et quand exécuter cette tâche
Vous pouvez également créer des enregistrements de configuration de recherche de perceptions pour invoquer les recherches enregistrées dans le magasin de journaux d'entreprise Splunk.

Remarque : Les requêtes de configuration de recherche s'appuient sur les données de journal Splunk pour être conformes à Splunk Common Information Model (CIM).

Avec les configurations de recherche enregistrées, vous pouvez :

- Créez des recherches personnalisées qui combinent plusieurs enregistrements d'événements.
- Des recherches efficaces et efficientes en matière de conception.
- Utiliser les entrées paramétrées dans la recherche enregistrée Splunk.

Le système de base inclut les exemples de configurations, comme illustré dans cette image :

Configurations de recherche enregistrées

Name	Observable type	Search	Is saved search
Search	Search	Search	Search
Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

Les requêtes de recherche enregistrées et de configuration sur place sont des exemples de requêtes qui peuvent être remplacées par des paramètres appropriés pour votre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

environnement. Créez des configurations de recherche enregistrées supplémentaires au besoin. Lorsque vous définissez une configuration de recherche enregistrée, le nom et les paramètres de la requête de recherche doivent correspondre à la configuration enregistrée définie sur votre instance Splunk. Si le nom et les paramètres ne sont pas identiques, vous risquez de ne pas voir de résultats précis lorsque vous effectuez une recherche d'observations.

Remarque : Sur votre instance Splunk, accédez à la page Recherches, rapports et alertes et localisez votre requête de recherche enregistrée. Cliquez sur le lien **Autorisations** pour accéder à la page Autorisations. Sélectionnez la case d'option **Toutes les applications** et activez l'option **Autorisation de lecture** pour **tout le monde**. Cela changera la valeur de la colonne de partage de Privé à Application pour votre requête de recherche enregistrée. Si cette option n'est pas définie, la requête de recherche enregistrée peut ne pas renvoyer de résultats.

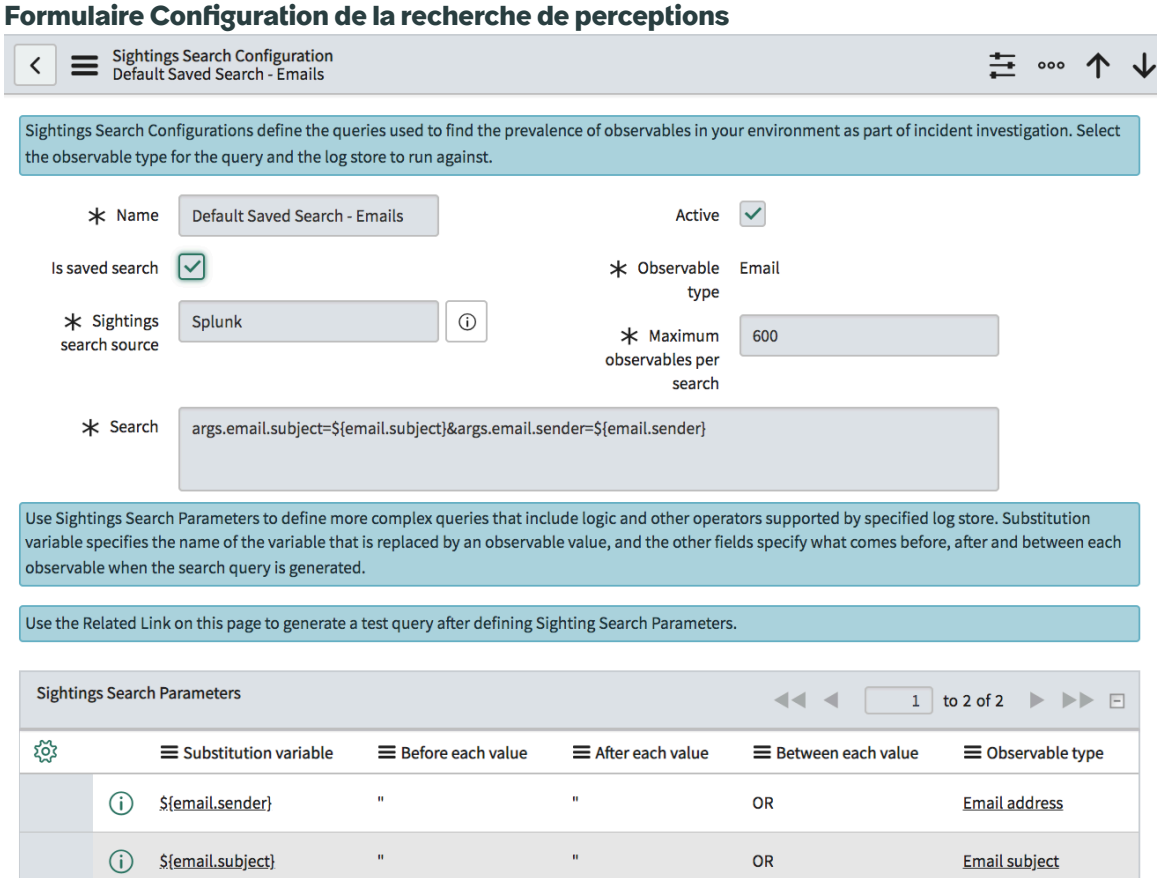
Pour vérifier si la configuration de recherche enregistrée correspond à la configuration définie sur votre instance Splunk :

1. Accédez à la **Paramètres** > **Recherches, rapports et alertes**.
2. **Modifiez le contexte de l'application** sur **Tous**.

   Une liste de rapports de recherche s'affiche.
3. Confirmez que la requête de recherche enregistrée figure dans la liste.

Par exemple, le formulaire de configuration de la recherche de perceptions contient l'adresse e-mail et l'expéditeur comme paramètres de recherche :

Formulaire Configuration de la recherche de perceptions



Dans votre instance Splunk, définissez la recherche enregistrée avec le même nom, la recherche enregistrée par défaut - E-mails, et les mêmes paramètres de recherche pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'adresse e-mail et l'objet de l'e-mail. Si le nom et les paramètres de recherche ne sont pas identiques, la recherche de perceptions ne génère pas de résultat précis.

Procédure

1. Accédez à la **Security Operations** > **Intégrations** > **Configuration de la recherche de perceptions** et créez un nouvel enregistrement (voir la table des descriptions de champ).

Formulaire Configuration de la recherche de perceptions

Champ	Description
Nom	Nom de la configuration.
Est une recherche enregistrée	La configuration de recherche enregistrée est créée si vous sélectionnez cette option.
Source de recherche de perceptions	La source de la recherche d'observations. Sélectionnez le magasin de journaux Splunk comme source.
Actif	Option pour l'état de recherche enregistré. Seules les configurations de recherche actives peuvent être utilisées pour effectuer une recherche de perceptions.
Type d'observable	Le type d'observable peut être n'importe quel type d'observable tel qu'une adresse IP, une valeur de hachage, une URL, un nom de domaine, et ainsi de suite.
Nombre maximum d'observables par recherche	Nombre maximal d'observables à renvoyer à partir de la recherche.
Rechercher	La chaîne de recherche par défaut est `$(observable)`, mais vous pouvez définir votre propre requête de recherche en spécifiant les paramètres pris en charge par le magasin de journaux Splunk.

2. Cliquez sur **Envoyer**.

Résultats
Vous avez créé un enregistrement de configuration de recherche de perceptions.

Que faire ensuite
Après avoir défini la requête de recherche, cliquez sur **Générer une requête de test de recherche de perceptions** et spécifiez une liste de valeurs observables pour générer une requête de test basée sur cette configuration de recherche enregistrée.

Ressources Playbook

Réponse aux incidents de sécurité fournit un ensemble complet de ressources de playbooks qui incluent une bibliothèque complète de playbooks, de flux secondaires et d'actions. Vous pouvez créer ou configurer des playbooks rapidement et facilement sans écrire de code compliqué. Vous pouvez utiliser ces playbooks pour résoudre les menaces de sécurité étape par étape.

Les ressources de Playbook comprennent les éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux incidents de sécurité Playbooks	Actions du playbook de Réponse aux incidents de sécurité
Les playbooks fournis avec le système de base sont conçus pour accélérer le processus d'enquête sur les incidents de sécurité en automatisant les tâches complexes et banales. Les Playbooks sont hautement configurables et créés à l'aide de la technologie Flow Designer de ServiceNow. Pour le configurer, copiez le playbook fourni avec le système de base et modifiez-le à l'aide de l'interface graphique simple par glisser-déplacer. Consultez Réponse aux incidents de sécurité Playbooks.	Les actions complexes qui sont essentielles pour générer des playbooks sont disponibles sous forme **de bibliothèques d'actions**. Ces bibliothèques d'actions permettent aux administrateurs de sécurité de créer des playbooks sans écrire de code compliqué. Consultez Actions du playbook de Réponse aux incidents de sécurité.

Activer un Réponse aux incidents de sécurité flux

Les administrateurs de sécurité et les concepteurs de flux peuvent utiliser les Réponse aux incidents de sécurité flux pour automatiser le processus de résolution des incidents de sécurité au sein de l'organisation.

Avant de commencer

Rôle requis : sn_si.admin, action_designer et flow_designer

Pourquoi et quand exécuter cette tâche

Les flux fournis avec le système de base sont à l'état inactif. Activez ces flux avant de les utiliser.

Procédure

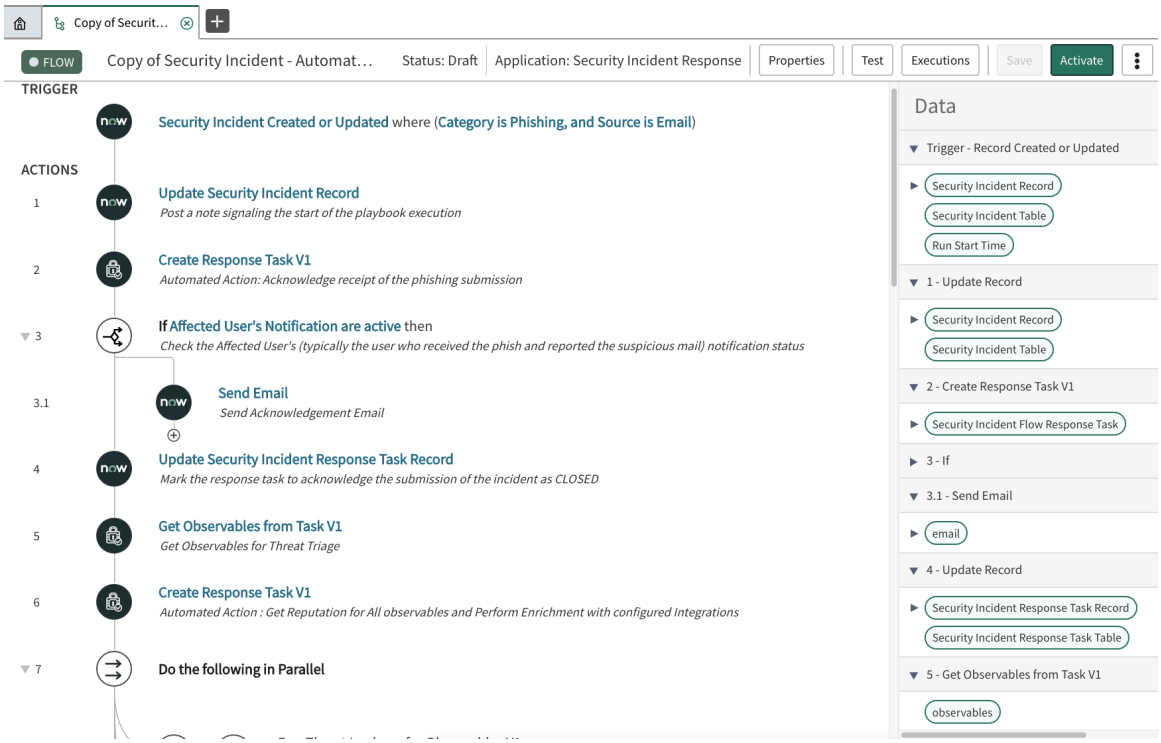
1. Téléchargez et installez l'application spoke Opérations de sécurité .
   Cette application spoke fournit des actions d'opérations de sécurité que vous pouvez utiliser lors de la définition des Réponse aux incidents de sécurité flux.
2. Accédez à la **Concepteur de flux** > **Concepteur** et la recherche de l'application Opérations de sécurité Spoke pour afficher les flux liés aux incidents de sécurité.



   Notez que les flux ont un état publié et sont inactifs.
3. Par exemple, si vous souhaitez activer le flux Playbook de programme malveillant automatisé, cliquez sur le lien **Incident de sécurité - Playbook d'hameçonnage automatisé - Modèle V1** pour afficher le flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Vous ne pouvez pas modifier les flux fournis avec le système de base, car il s'agit de flux en lecture seule. Vous pouvez utiliser ces flux tels quels ou en faire une copie et les modifier si nécessaire.

4. Cliquez sur **Activer** pour activer le flux.

Résultats

Le flux du Playbook d'hameçonnage automatisé est actif et prêt à l'emploi.

Réponse aux incidents de sécurité Playbooks

Vous pouvez invoquer le flux de playbook d'incident de sécurité automatiquement ou manuellement.

Un Playbook n'est visible que si au moins un Playbook est associé à un incident de sécurité. Le composant Playbook fonctionne uniquement pour les processus créés par Process Automation Designer (PAD) et non pour les flux créés par Flow Designer. Les flux existants activés par Flow Designer continuent de fonctionner et les activités continuent d'être restituées en tant que tâches de réponse.

Réponse aux incidents de sécurité prend en charge deux types de Playbooks :

- Playbooks basés sur les processus
- Playbooks basés sur le flux

En plus des playbooks répertoriés, il existe également des flux secondaires dans le spoke Security Operations qui peuvent être appelés à partir du playbook de flux. Les ransomwares sont l'un de ces flux secondaires.

Activez ces flux avant de les utiliser. Pour plus d'informations, consultez Activer un flux Security Incident Response.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbooks basés sur les processus

Le composant Playbook fonctionne uniquement pour les Playbooks intégrés Studio de workflow et non pour les flux. Toutefois, les playbooks existants basés sur les flux continueront de fonctionner et les activités continueront d'être présentées en tant que tâches d'intervention.

Réponse aux incidents de sécurité fournit les playbooks suivants avec le système de base.

Playbook pour l'hameçonnage manuel

Le Playbook d'hameçonnage manuel fournit des conseils étape par étape à vos analystes sur la façon dont ils peuvent résoudre manuellement des types spécifiques de menaces de sécurité dans vos activités d'hameçonnage.

Vue d'ensemble

Le modèle Playbook d'hameçonnage manuel est conçu pour effectuer manuellement les tâches de réponse d'hameçonnage et comprend une séquence d'actions qui inclut des conditions de déclenchement. Vous pouvez utiliser les modèles PAD pour effectuer les étapes du playbook de réponse d'hameçonnage et résoudre efficacement ces incidents.

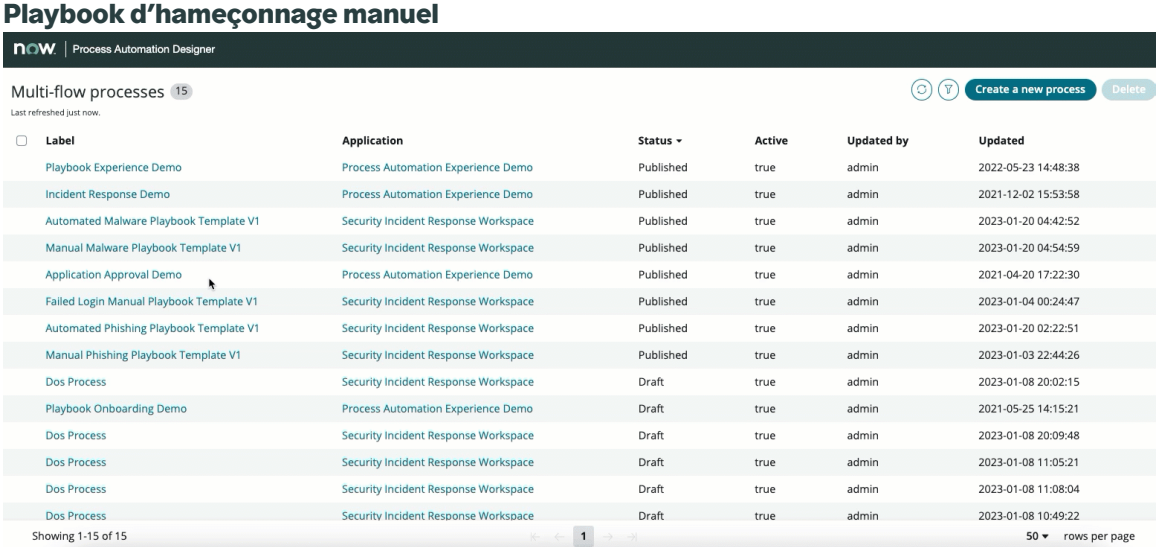
Ce playbook peut être utilisé si un incident de sécurité est créé ou mis à jour. Vous devez activer le Playbook d'hameçonnage manuel sur Process Automation Designer (PAD), puis effectuer toutes les tâches, telles que l'analyse, contenir, éradiquer et examiner.

Les étapes de la définition du processus sont les suivantes et correspondent à l'état de l'incident de sécurité :

- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Playbook d'hameçonnage manuel



Une fois que vous marquez une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche au fur et à mesure que vous terminez les tâches et les étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les détails que vous avez saisis à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des playbooks pour l'hameçonnage manuel dans Studio de workflow

Suivez ces étapes pour créer des playbooks pour l'hameçonnage manuel dans Studio de workflow.

Avant de commencer

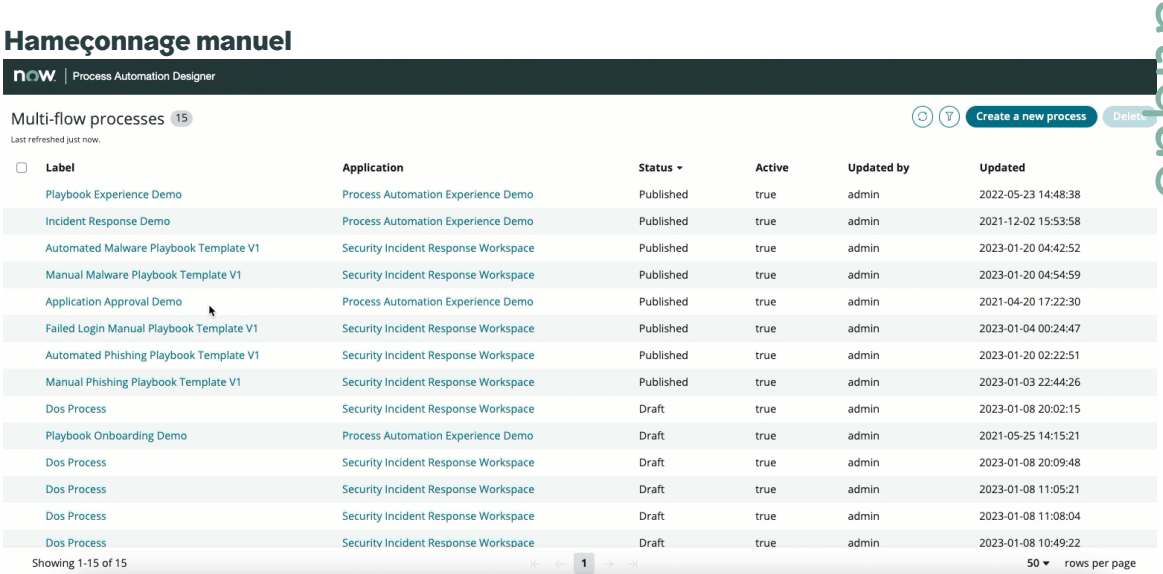
Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **Tous** > **Concepteur d'automatisation de processus** > > **Nouveau** et sélectionnez **Playbook**.

   Par exemple, Playbook d'hameçonnage manuel : modèle V1.

2. Saisissez un nom pour le playbook, la description et l'application pour laquelle le playbook est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour le moment où votre processus s'exécute**, et sélectionnez la condition de déclenchement pour le moment où votre playbook doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions pour définir quand votre playbook doit s'exécuter en sélectionnant une table et en remplissant les conditions.
   Par exemple, la condition de déclenchement est lorsqu'un incident de sécurité de catégorie Hameçonnage est créé.



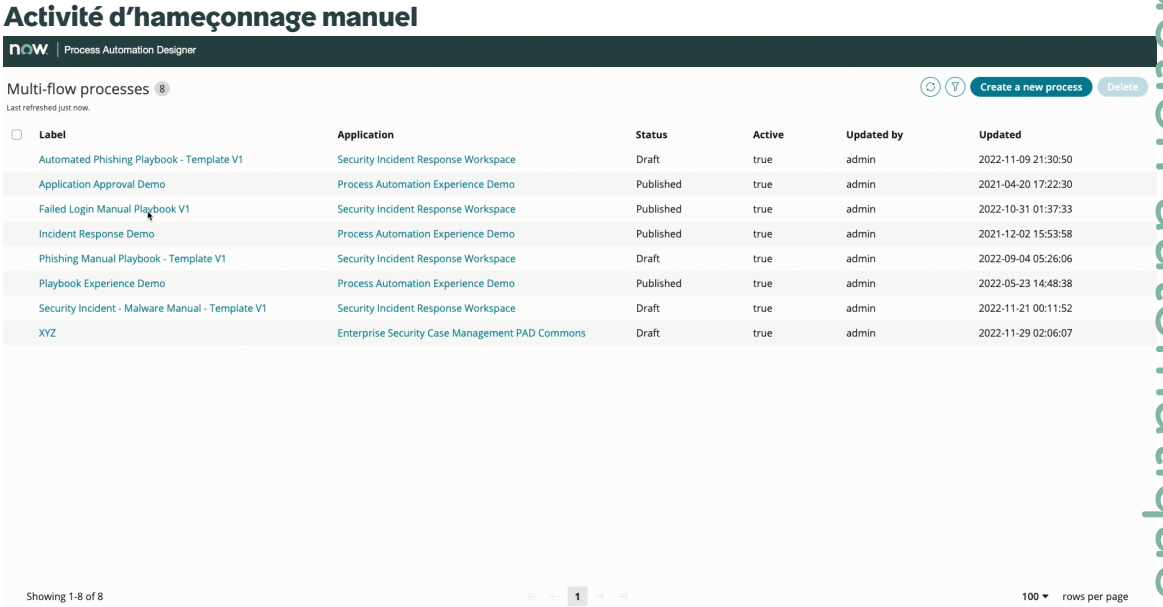
7. Cliquez sur **Accéder à Designer**.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Dans le volet des propriétés de l'étape, saisissez les détails suivants : **Nom**, **Description**, **Condition d'exécution** et **Indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer indiquent quand l'étape** doit s'exécuter.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour Analyser, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a pas de condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité** sous une étape particulière (par exemple, l'étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus pour chaque étape.

Activité d'hameçonnage manuel



14. Dans le volet des propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité de la définition d'activité.

Ajouter des activités parallèles

Si le champ **Quand démarrer** est défini sur **Avec le précédent**, des activités parallèles peuvent être lancées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour passer d'une étape à l'autre

Si aucune condition d'exécution n'est définie, les étapes et les activités sont exécutées séquentiellement.

Vous pouvez utiliser la condition d'exécution pour ignorer des activités ou des étapes. Dans cet exemple, **l'étape Contenir commence lorsque le résultat de « L'e-mail comporte-t-il des indicateurs de menace ? » est Oui**.

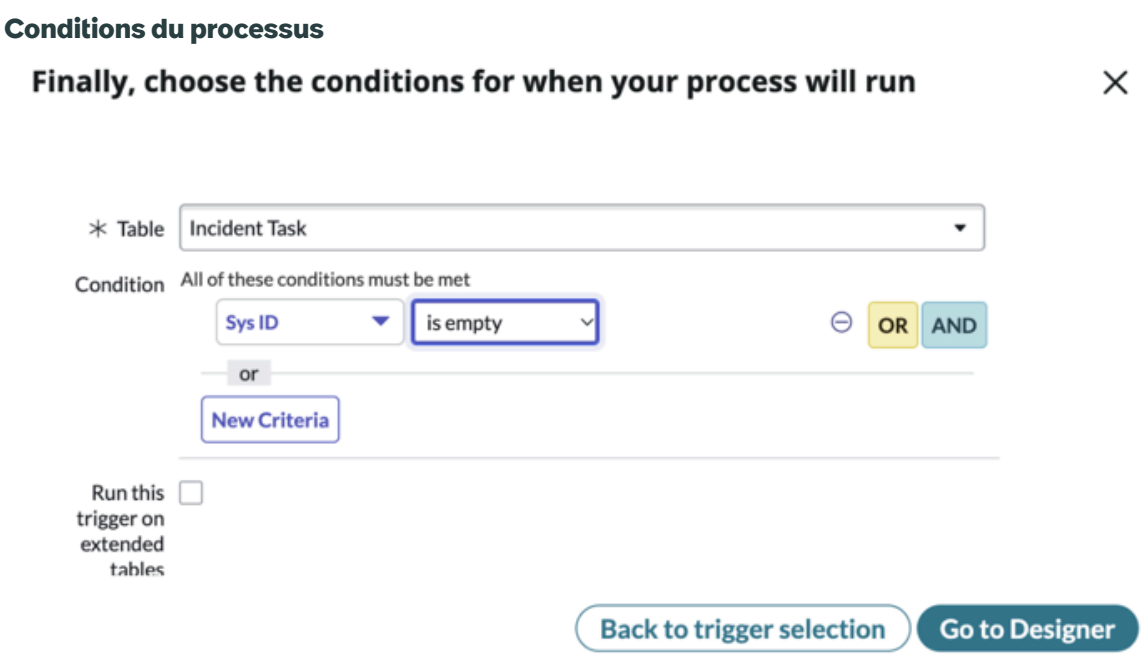
Pour passer d'une étape à une autre, vous pouvez utiliser la définition d'activité fournie par la plateforme **: Mettre à jour l'enregistrement**. Cela mettra à jour le champ d'état de l'incident de sécurité et reprendra l'exécution du playbook à l'étape suivante.

Cependant, le défi avec cette définition d'activité est que, si le playbook est à l'étape Analyse et si l'utilisateur a mis à jour manuellement l'état sur Révision, l'activité Mettre à jour l'enregistrement change à nouveau l'état sur Maîtriser pour continuer l'exécution du playbook. Cela remplacera le changement manuel effectué.

Pour surmonter ce problème, une définition d'activité appelée **Mettre à jour l'état** de la tâche est fournie dans le système de base. Cette activité ne remplacera pas l'état de l'incident de sécurité, si l'état actuel de l'état de la sécurité est antérieur à l'étape dans le playbook.

Créer une définition de processus avec une condition de déclenchement factice

Une définition de processus nécessite toujours une condition de déclenchement. Toutefois, si vous ne savez pas quand le processus doit être déclenché, vous pouvez toujours créer une définition de processus avec une condition de déclenchement factice. Définissez la condition de déclenchement, car **sys_id est vide**. Cette condition ne sera jamais remplie.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook d'hameçonnage manuel

Suivez ces étapes pour apprendre à utiliser le playbook d'hameçonnage manuel dans l'Espace de travail de l'analyste SIR et ses options.

Avant de commencer

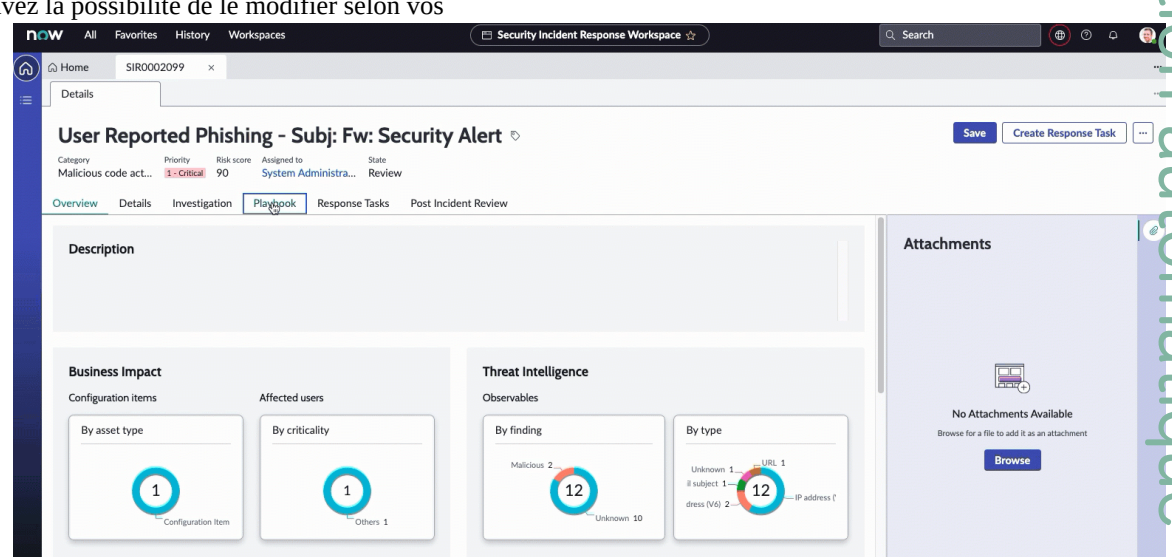
Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de l'afficher dans l'onglet **Playbook** .
3. Cliquez sur le **Playbook d'hameçonnage manuel**.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.
   Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Examiner pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action de l'utilisateur à effectuer, elle s'affiche dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase respective et effectuez l'action pour terminer l'activité.

Résumé du Playbook de l'espace de travail

Le résumé du processus est décrit ci-dessous.

- Comprendre le playbook basé sur le flux hérité.
- Répertoriez les activités possibles, les étapes après avoir analysé le flux. Recherchez les étapes dans lesquelles une véritable orchestration peut être créée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Prenez chaque activité et vérifiez si la définition d'activité fournie par le système de base peut répondre au cas d'utilisation ou non.
- Répertoriez les cas d'utilisation d'activités qui nécessitent l'implémentation de nouvelles définitions d'activité. Classez-les : interactifs, non interactifs ou automatisés. Pour créer une définition d'activité :
  - Créez un flux secondaire ou une action pour le cas d'utilisation.
  - Décidez si les données associées doivent être capturées dans une table de données de flux ou dans une table personnalisée.
  - Si vous utilisez une table de données de flux, créez **une** définition de données de flux dans sys_flow_data_definition. Lors de la création d'un enregistrement de données de flux dans le flux secondaire, sélectionnez la définition de données de flux créée.
  - Créez une **définition d'activité**.
  - Mappez le plan d'automatisation.
  - Renseignez les propriétés de **l'expérience d'activité** .
  - Créez une action sous Actions du playbook. Il doit y avoir une action d'activité existante pour l'affecter à la définition d'activité.
  - Pour remplacer l'expérience de carte par défaut en fonction du type d'expérience sélectionné, ajoutez le remplacement du playbook à l'aide du concept d'interface utilisateur d'activité.
- Certaines activités peuvent être gérées à la fois de manière automatique et interactive à l'aide du marqueur d'attente d'entrée de l'utilisateur dans le flux secondaire. Cette entrée peut être transmise lors de la configuration de l'activité dans la définition du processus.
- Une fois que vous avez toutes les définitions d'activité requises pour votre processus, commencez à créer la définition du processus à l'aide de Studio de workflow.

Playbook pour l'hameçonnage automatisé

Le playbook d'hameçonnage automatisé fournit des conseils étape par étape à vos analystes sur la façon dont ils peuvent résoudre des types spécifiques de menaces de sécurité dans vos activités d'hameçonnage automatisé.

Vue d'ensemble

Le modèle de playbook d'hameçonnage automatisé est conçu pour automatiser les tâches de réponse d'hameçonnage et contient une séquence d'actions qui inclut les conditions de déclenchement. Vous pouvez utiliser les modèles de playbook pour Studio de workflow automatiser les étapes du playbook de réponse d'hameçonnage et résoudre efficacement ces incidents. Ce modèle de playbook contient une séquence d'actions réutilisables conçues pour répondre aux attaques d'hameçonnage. Chaque flux possède un déclencheur (condition), une séquence d'actions et des flux secondaires que vous pouvez annoter.

Dans ce playbook, il n'y aura aucune interaction de l'utilisateur lorsque la catégorie d'un incident de sécurité est définie sur Hameçonnage. Ce playbook peut être utilisé si un incident de sécurité est créé ou mis à jour. Vous devez activer le Playbook d'hameçonnage automatisé dans Studio de workflow, et ce playbook effectue automatiquement toutes les tâches, telles que l'analyse, le confinement, l'éradication et l'examen.

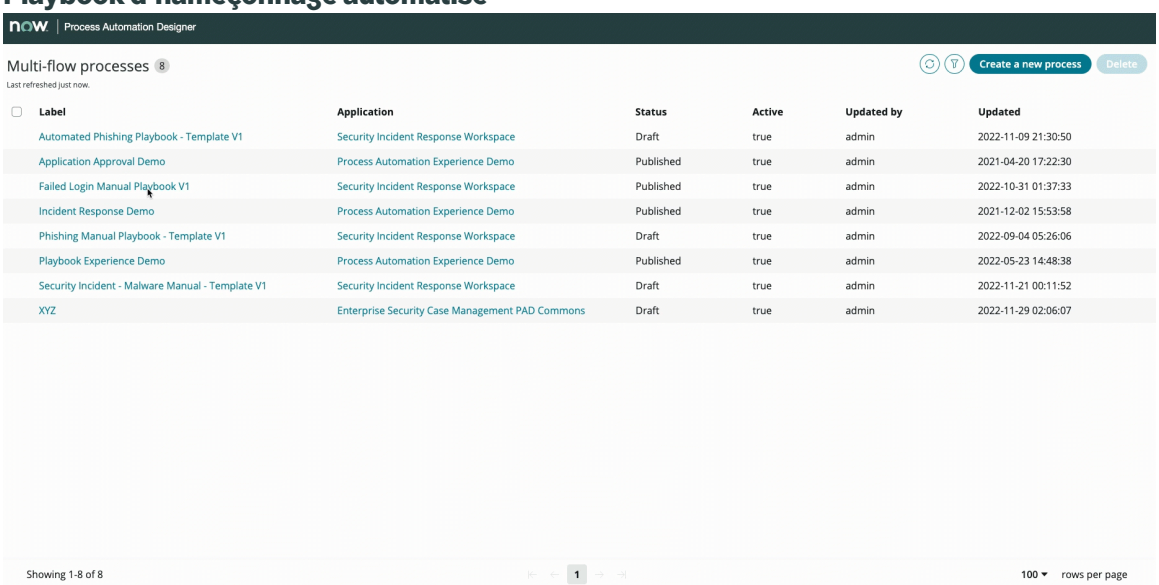
Les étapes de la définition du processus sont les suivantes et correspondent à l'état de l'incident de sécurité :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Playbook d'hameçonnage automatisé



Une fois que vous marquez une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche au fur et à mesure que vous terminez les tâches et les étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les détails que vous avez saisis à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des processus pour l'hameçonnage automatisé dans PAD

Suivez ces étapes pour créer des processus d'hameçonnage automatisé dans le Concepteur d'automatisation de processus (PAD).

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

   Par exemple, Playbook d'hameçonnage automatisé : modèle V1.

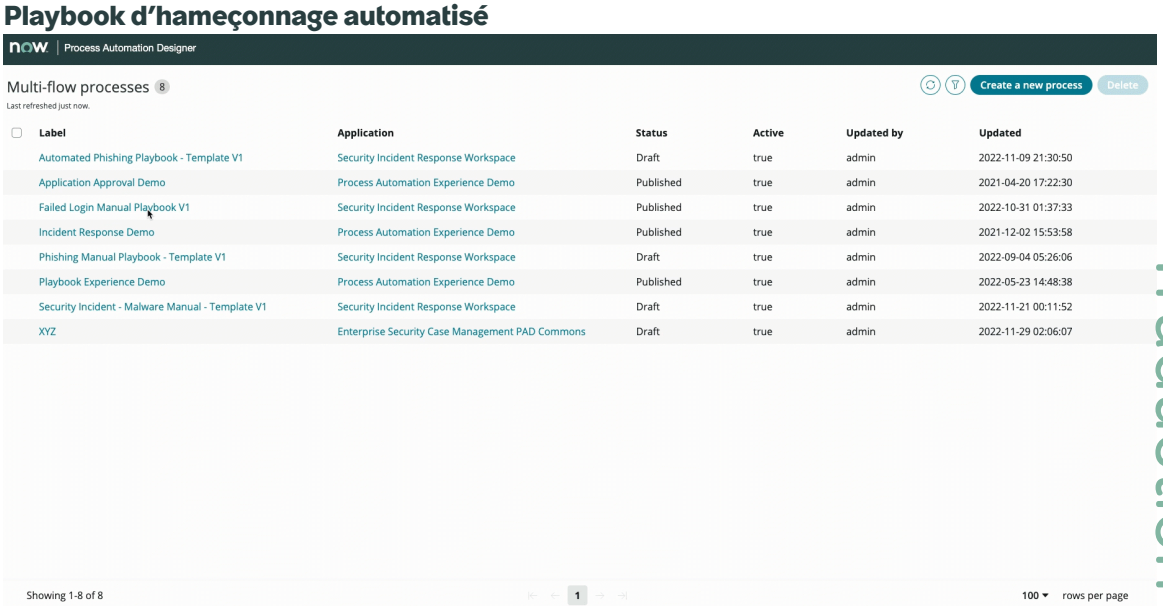
2. Saisissez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Définir vos propres conditions pour le moment où votre processus s'exécute**, puis sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions pour définir quand votre processus doit s'exécuter en sélectionnant une table et en remplissant les conditions.
   Par exemple, la condition de déclenchement est lorsqu'un incident de sécurité de catégorie Hameçonnage est créé.

Playbook d'hameçonnage automatisé

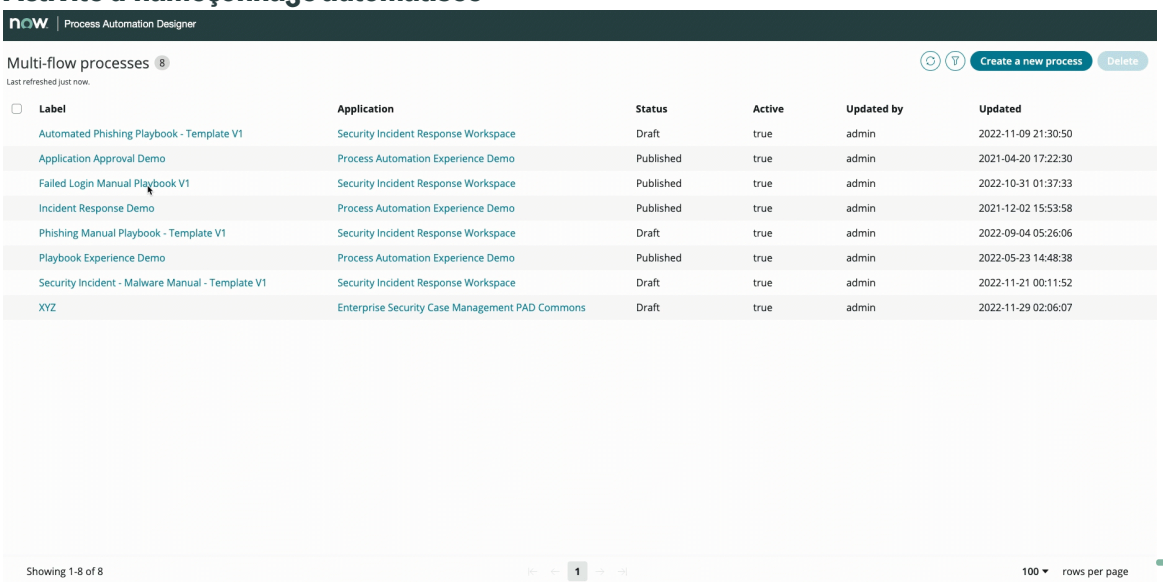


7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet des propriétés de l'étape, saisissez les détails suivants : **Nom**, **Description**, **Condition d'exécution** et **Indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer indiquent quand l'étape** doit s'exécuter.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour Analyser, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a pas de condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité de processus** à une étape particulière (par exemple, l'étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus pour chaque étape.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activité d'hameçonnage automatisée



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité de processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité de la définition d'activité.

Utilisation du playbook d'hameçonnage automatisé

Suivez ces étapes pour apprendre à utiliser le playbook d'hameçonnage automatisé dans l'Espace de travail de l'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

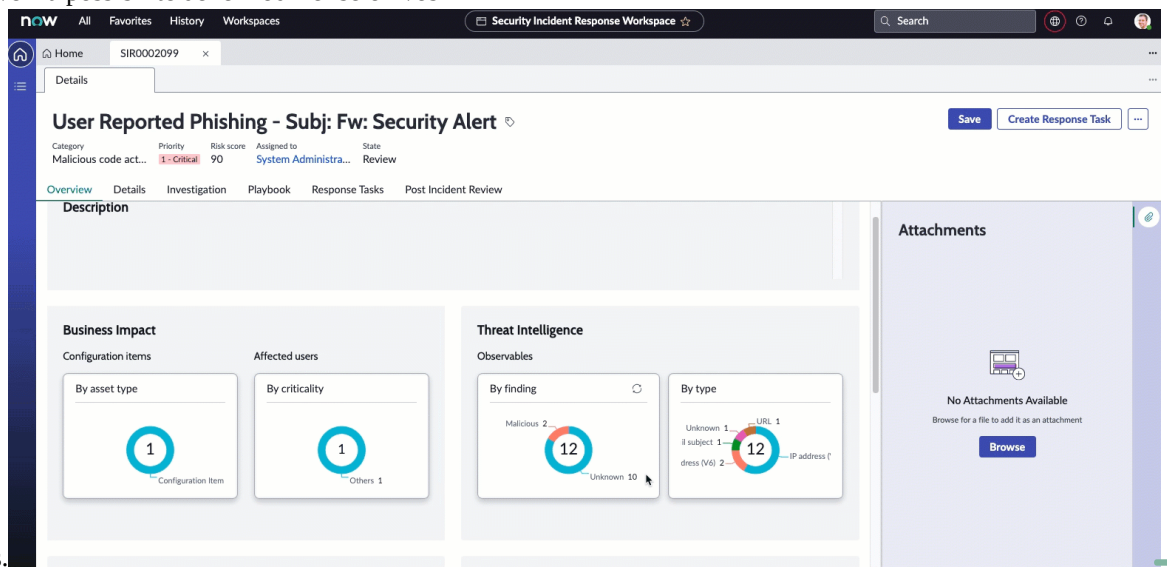
   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de l'afficher dans l'onglet **Playbook** .

3. Cliquez sur le **Playbook d'hameçonnage automatisé**.
   Pour le hameçonnage automatisé, les tâches sont automatiquement exécutées pour l'incident de sécurité.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Examiner pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action de l'utilisateur à effectuer, elle s'affiche dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase respective et effectuez l'action pour terminer l'activité.

Playbook pour les programmes malveillants manuels

Le playbook de logiciels malveillants manuels fournit des conseils étape par étape sur la façon dont les analystes peuvent résoudre manuellement plus efficacement les alertes de programmes malveillants.

Le modèle de Playbook de programme malveillant manuel est conçu pour effectuer manuellement les étapes de gestion des alertes de programme malveillant provenant du point de terminaison ou du réseau. Vous pouvez utiliser les modèles de playbook pour Studio de workflow effectuer les étapes du playbook de programme malveillant manuel et résoudre efficacement ces alertes. Ce playbook comprend des conditions de déclenchement, une séquence d'actions et des flux secondaires que vous pouvez annoter. Ce playbook contient une séquence d'actions réutilisables conçues pour répondre aux attaques de programmes malveillants. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires pour l'annotation.

Ce playbook peut être utilisé si un programme malveillant est créé ou mis à jour. Vous devez activer le Playbook de programme malveillant manuel et Studio de workflow créer toutes les tâches, telles que l'analyse, le confinement, l'éradication et la révision.

Les étapes de la définition du processus sont les suivantes et correspondent à l'état de l'alerte de programme malveillant :

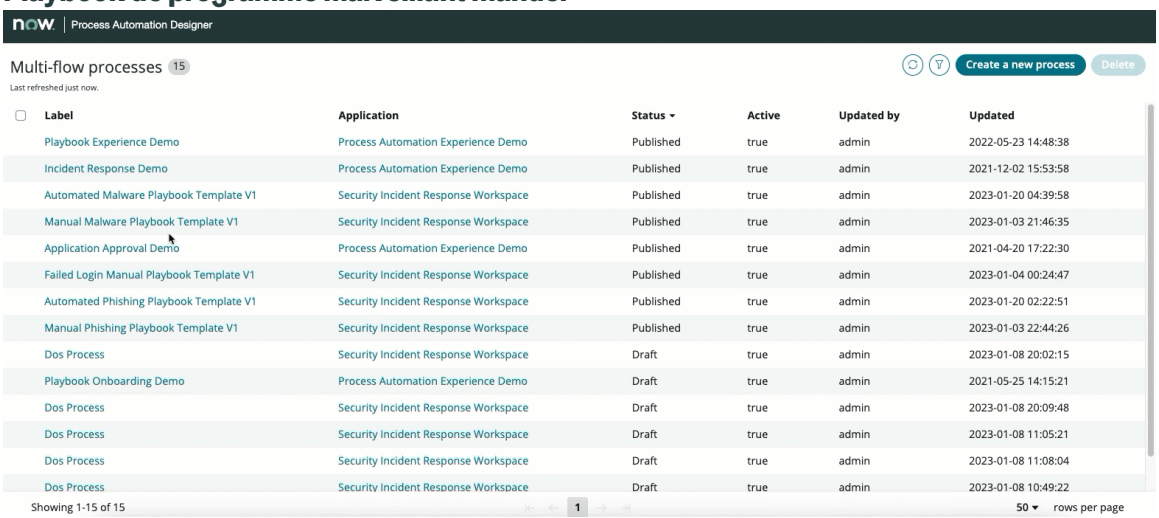
- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de programme malveillant manuel



Une fois que vous avez marqué une tâche terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche au fur et à mesure que vous terminez les tâches et les étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les détails que vous avez saisis à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des processus pour les programmes malveillants manuels dans PAD

Suivez ces étapes pour créer des processus pour les programmes malveillants manuels dans le Concepteur d'automatisation de processus (PAD).

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.manager

Procédure

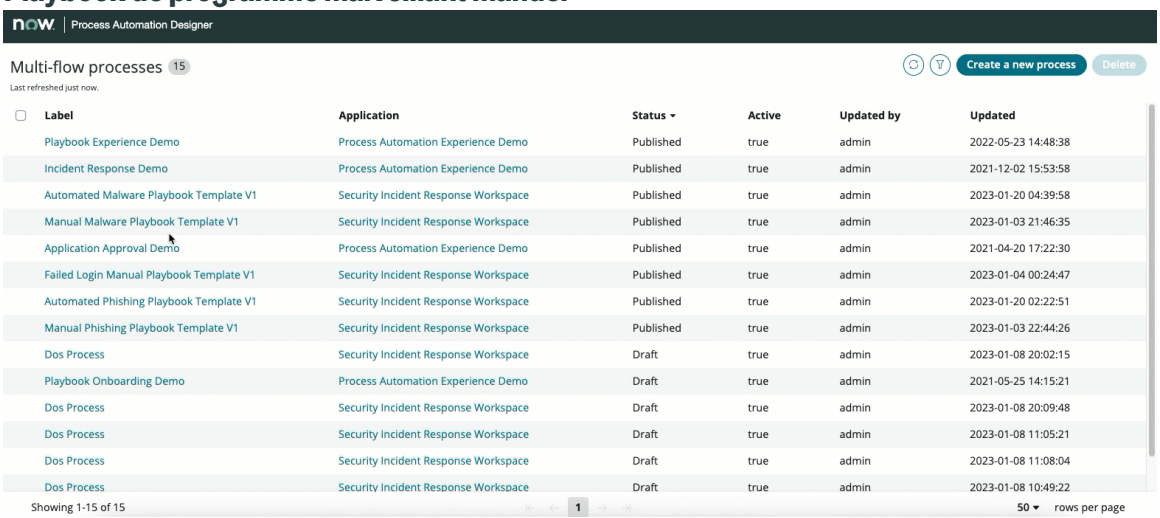
1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

   Par exemple, Playbook de programme malveillant manuel : modèle V1.
2. Saisissez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour le moment où votre processus s'exécute**, puis sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions pour définir quand votre processus doit s'exécuter en sélectionnant une table et en remplissant les conditions.
   Par exemple, la condition de déclenchement est lorsqu'un incident de sécurité de catégorie Hameçonnage est créé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de programme malveillant manuel

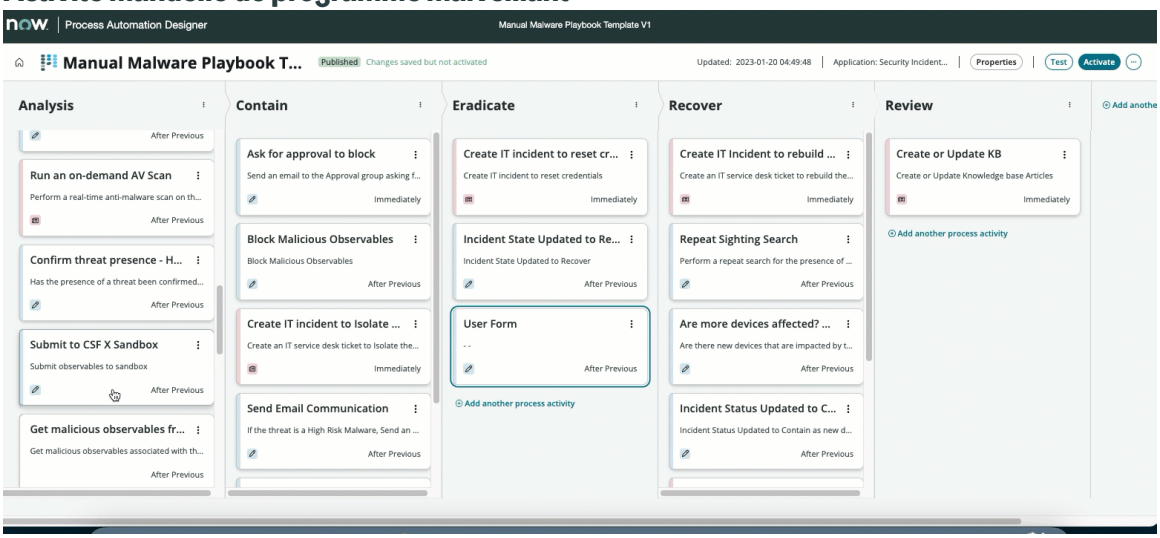


7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet des propriétés de l'étape, saisissez les détails suivants : **Nom**, **Description**, **Condition d'exécution** et **Indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer indiquent quand l'étape** doit s'exécuter.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour Analyser, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a pas de condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité de processus** à une étape particulière (par exemple, l'étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus pour chaque étape.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activité manuelle de programme malveillant



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité de processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité de la définition d'activité.

Utilisation du playbook de programme malveillant manuel

Suivez ces étapes pour apprendre à utiliser le playbook de programme malveillant manuel dans l'espace de travail de l'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

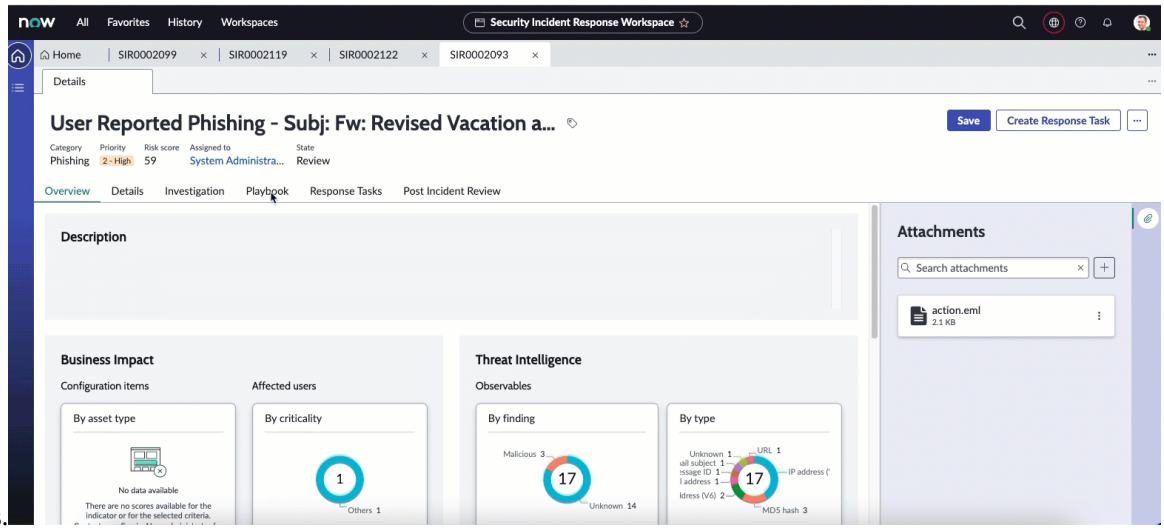
   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de l'afficher dans l'onglet **Playbook** .

3. Cliquez sur le **Playbook de programme malveillant manuel**.
   Pour les programmes malveillants manuels, les tâches sont automatiquement exécutées pour l'incident de sécurité.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Examiner pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action de l'utilisateur à effectuer, elle s'affiche dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase respective et effectuez l'action pour terminer l'activité.

Playbook pour les programmes malveillants automatisés

Le playbook de programme malveillant automatisé fournit une séquence d'étapes automatisées qui aide les analystes à résoudre plus efficacement les alertes de programme malveillant.

Le modèle de playbook de programme malveillant automatisé est conçu pour automatiser les étapes de gestion des alertes de programme malveillant provenant du point de terminaison ou du réseau. Vous pouvez utiliser les modèles de playbook pour Studio de workflow automatiser les étapes du playbook de programme malveillant automatisé et résoudre efficacement ces alertes. Ce playbook comprend des conditions de déclenchement, une séquence d'actions et des flux secondaires que vous pouvez annoter. Ce playbook contient une séquence d'actions réutilisables conçues pour répondre aux attaques de programmes malveillants. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires pour l'annotation.

Ce playbook peut être utilisé si un incident de sécurité est créé ou mis à jour. Vous devez activer le playbook de programme malveillant automatisé dans Studio de workflow, et ce playbook effectue automatiquement toutes les tâches, telles que l'analyse, le confinement, l'éradication et l'examen.

Les étapes de la définition du processus sont les suivantes et correspondent à l'état de l'incident de sécurité :

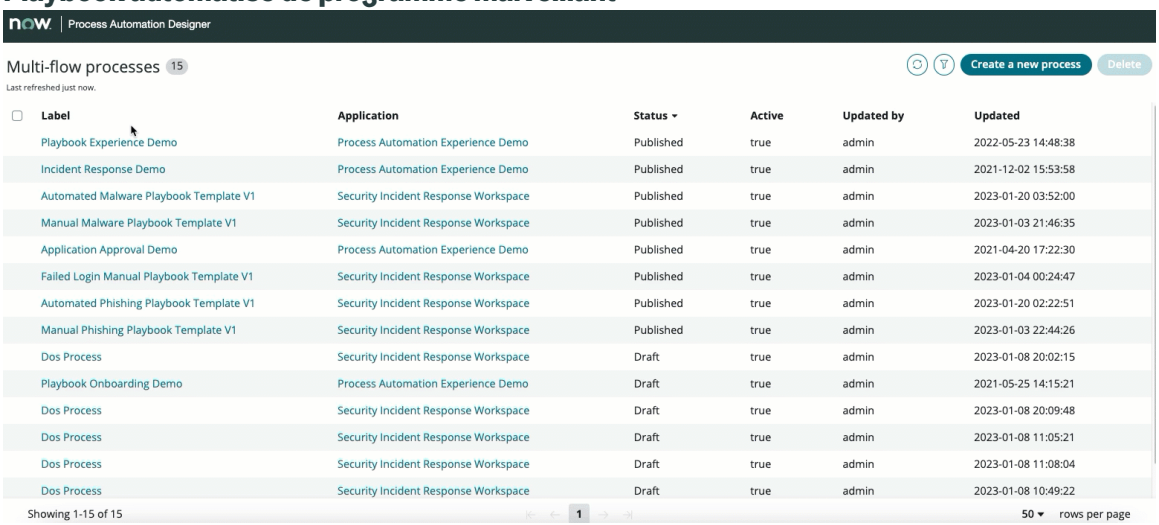
- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook automatisé de programme malveillant



Une fois que vous marquez une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche au fur et à mesure que vous terminez les tâches et les étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les détails que vous avez saisis à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des processus Programme malveillant automatisé dans PAD

Suivez ces étapes pour créer des processus pour les programmes malveillants automatisés dans le Concepteur d'automatisation de processus (PAD).

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

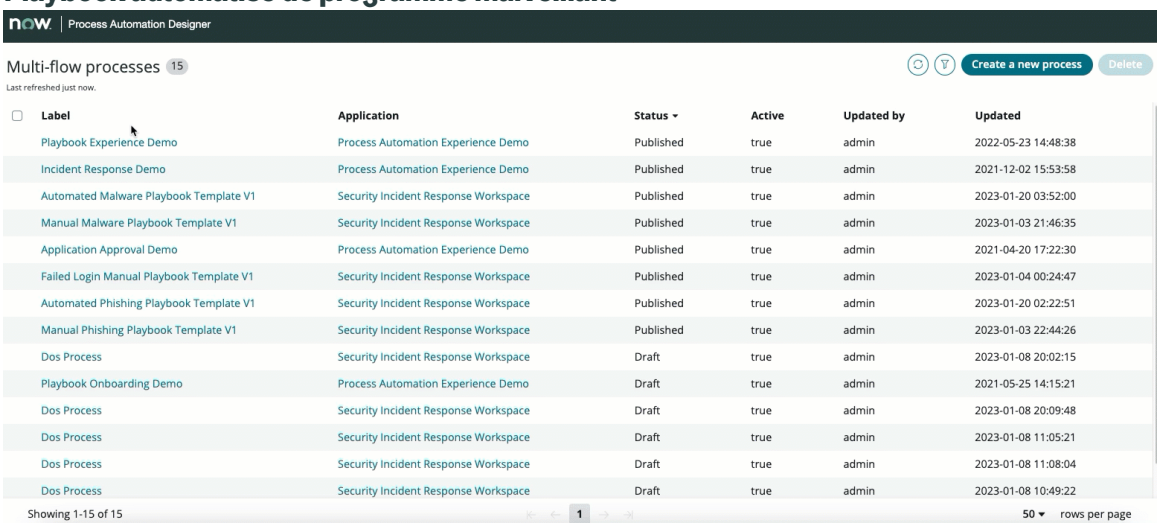
   Par exemple, Playbook de programme malveillant automatisé : modèle V1.

2. Saisissez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour le moment où votre processus s'exécute**, puis sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions pour définir quand votre processus doit s'exécuter en sélectionnant une table et en remplissant les conditions.
   Par exemple, la condition de déclenchement est lorsqu'un incident de sécurité de catégorie Hameçonnage est créé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook automatisé de programme malveillant

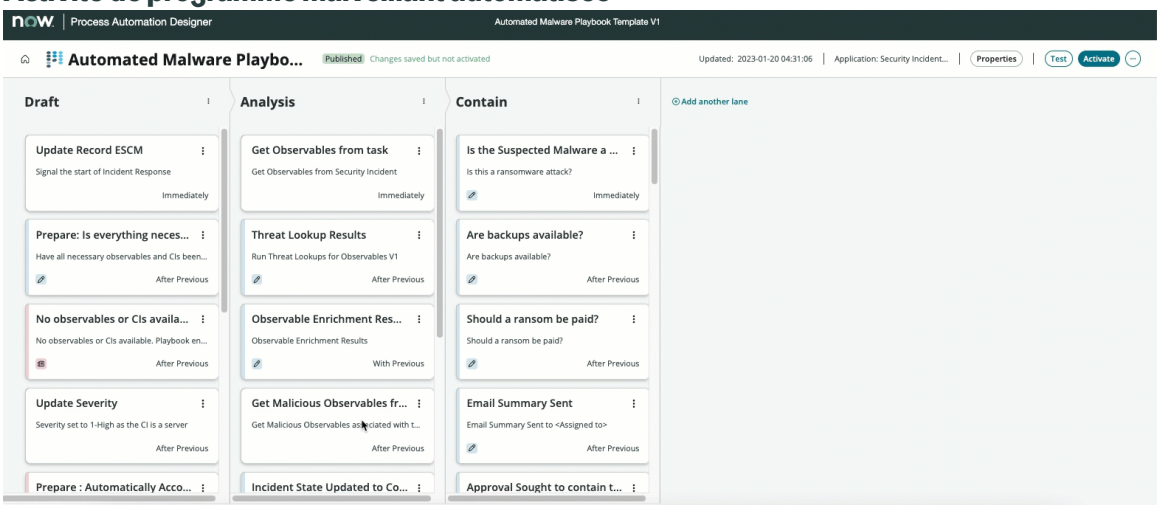


7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet des propriétés de l'étape, saisissez les détails suivants : **Nom**, **Description**, **Condition d'exécution** et **Indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer indiquent quand l'étape** doit s'exécuter.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour Analyser, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a pas de condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité de processus** à une étape particulière (par exemple, l'étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus pour chaque étape.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activité de programme malveillant automatisée



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité de processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité de la définition d'activité.

Utilisation du playbook de programme malveillant automatisé

Suivez ces étapes pour apprendre à utiliser le playbook de programme malveillant automatisé dans l'espace de travail de l'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

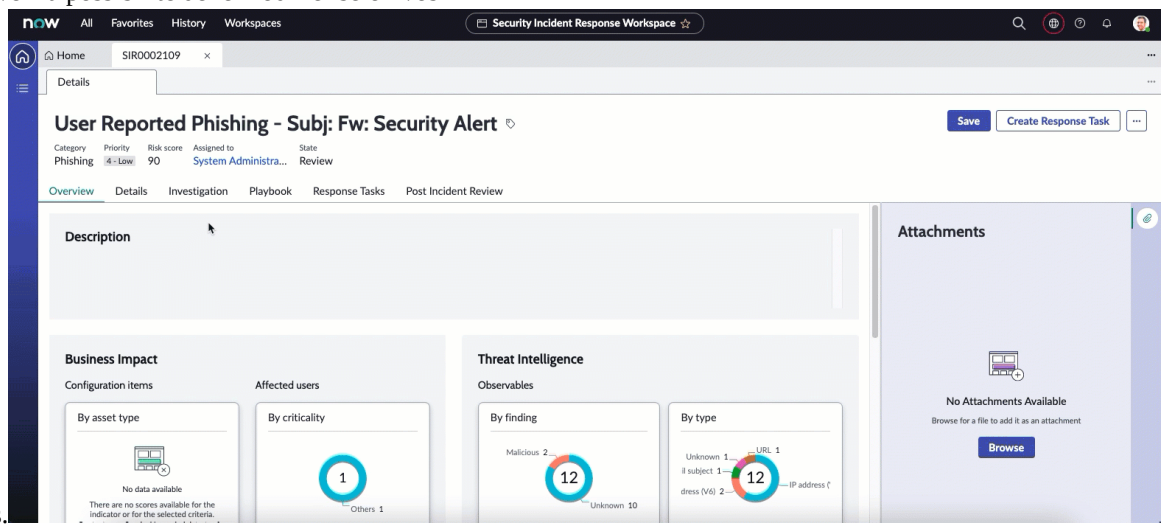
   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de l'afficher dans l'onglet **Playbook** .

3. Cliquez sur le **Playbook de programme malveillant automatisé**.
   Pour les programmes malveillants automatisés, les tâches sont automatiquement exécutées pour l'incident de sécurité.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Examiner pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action utilisateur à effectuer, elle s'affiche dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase respective et effectuez l'action pour terminer l'activité.

Playbook pour l'échec de la connexion manuelle

Le playbook Échec de la connexion manuelle fournit des conseils et aide à optimiser l'enquête sur les incidents de sécurité liés aux échecs de connexion.

Lorsqu'un utilisateur effectue certaines tentatives de connexion infructueuses (selon la configuration SIM), un incident de sécurité est créé. Ces tentatives de connexion infructueuses peuvent être soit des faux positifs, soit des tentatives effectuées par des attaquants pour obtenir l'accès aux comptes de messagerie des utilisateurs.

Vous pouvez utiliser les modèles de playbook pour Studio de workflow effectuer les étapes du playbook Échec de la connexion et résoudre efficacement les incidents de sécurité liés à l'échec de connexion. Ce playbook comprend des conditions de déclenchement, une séquence d'actions et des flux secondaires que vous pouvez annoter. Ce playbook contient une séquence d'actions réutilisables conçues pour répondre aux incidents de sécurité liés à l'échec de la connexion. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires pour l'annotation.

Ce playbook peut être utilisé si un incident de sécurité lié à l'échec de connexion est créé ou mis à jour. Vous devez activer le Playbook manuel d'échec de Studio de workflow connexion et créer toutes les tâches, telles qu'analyser, contenir, éradiquer et examiner.

Les étapes de la définition du processus sont les suivantes et correspondent à l'état de l'incident de sécurité :

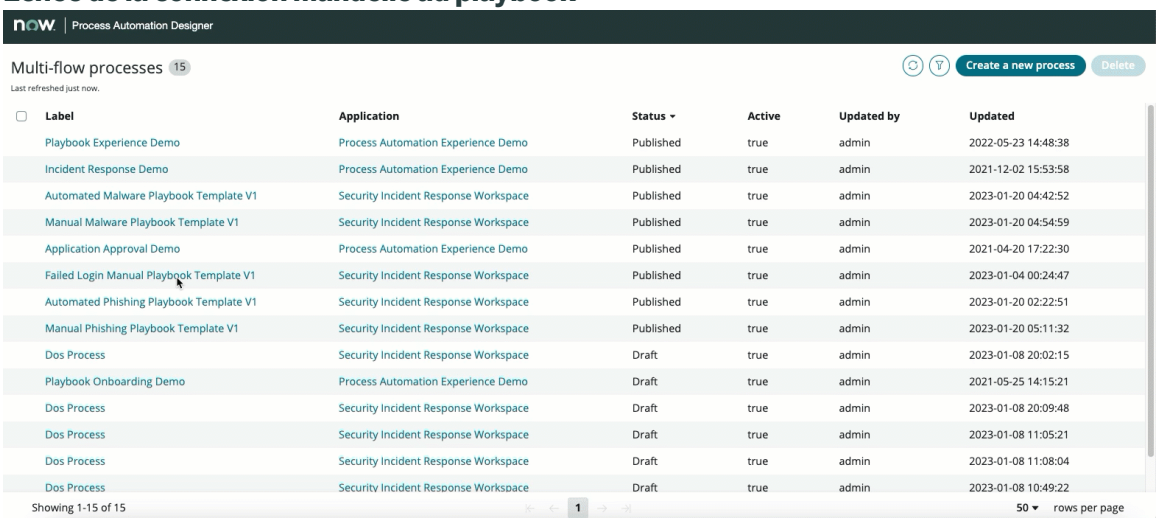
- Analyse
- Contenir
- Éradiquer
- Revue

Chaque étape comporte des activités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échec de la connexion manuelle au playbook



Une fois que vous marquez une tâche comme terminée dans une étape, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches d'une étape, vous pouvez passer à l'étape suivante. Le statut est reflété dans le panneau de gauche au fur et à mesure que vous terminez les tâches et les étapes. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les détails que vous avez saisis à toutes les étapes. Vous pouvez choisir de modifier n'importe quel champ ou cliquer sur Terminer pour terminer le processus de création de l'autorisation.

Créer des processus pour l'échec de la connexion manuelle dans PAD

Suivez ces étapes pour créer des processus pour l'échec de la connexion manuelle dans le Concepteur d'automatisation de processus (PAD).

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.manager

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

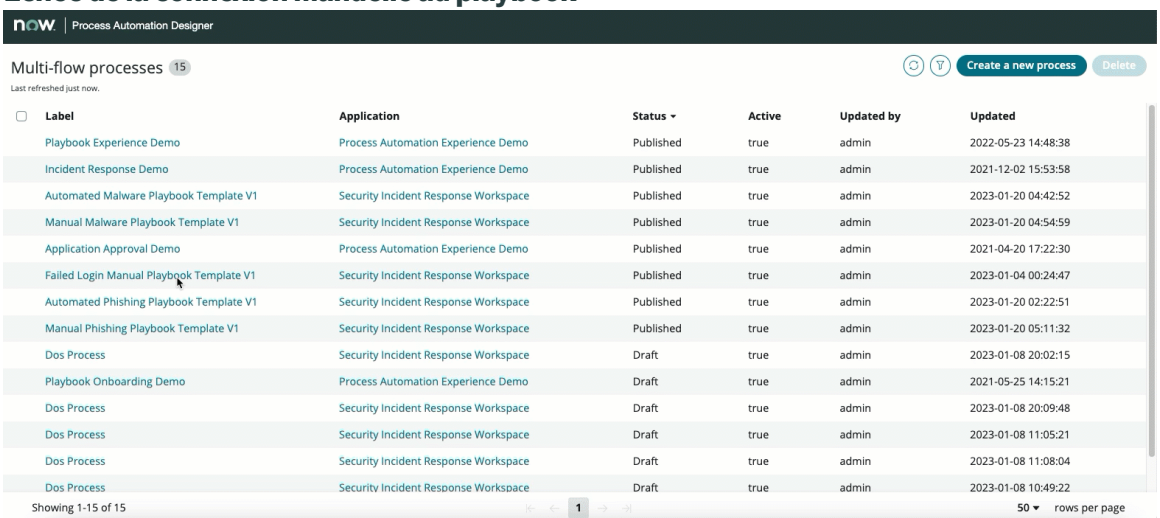
   Par exemple, Échec de la connexion manuelle au Playbook : modèle V1.

2. Saisissez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour le moment où votre processus s'exécute**, puis sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions pour définir quand votre processus doit s'exécuter en sélectionnant une table et en remplissant les conditions.
   Par exemple, la condition de déclenchement est lorsqu'un incident de sécurité de catégorie Hameçonnage est créé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

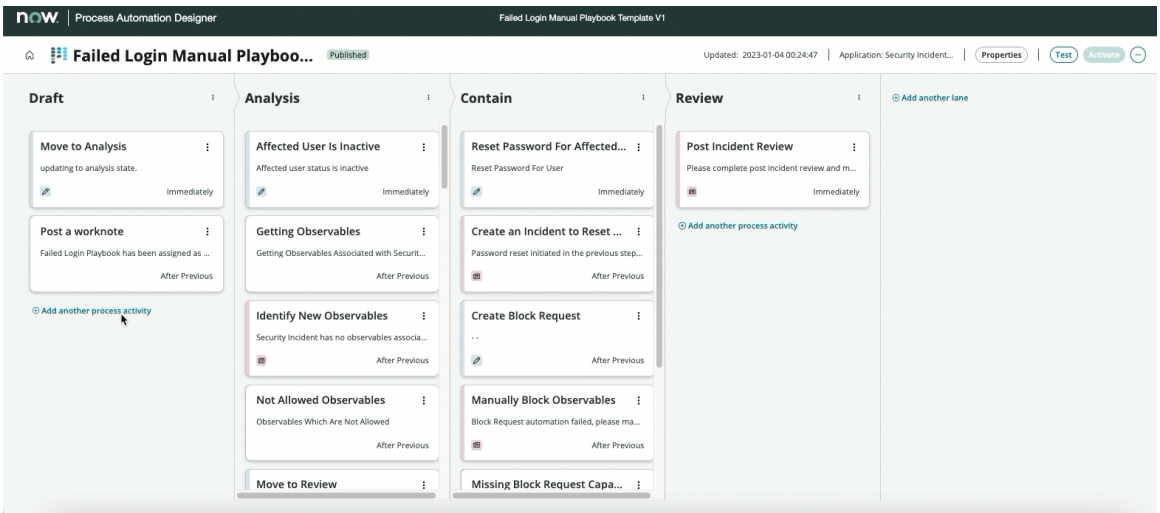
Échec de la connexion manuelle au playbook



7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle étape**.
   Le volet des propriétés de l'étape s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet des propriétés de l'étape, saisissez les détails suivants : **Nom**, **Description**, **Condition d'exécution** et **Indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer indiquent quand l'étape** doit s'exécuter.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre étape, cliquez sur **Ajouter une autre étape**.
    De même, vous pouvez créer autant d'étapes que vous le souhaitez. Dans cet exemple, vous pouvez créer une étape pour Analyser, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, l'étape **d'analyse** démarre immédiatement et n'a pas de condition d'exécution. **Contenir** le début de l'étape une fois l'étape précédente terminée et dont la condition d'exécution est basée sur le résultat d'une activité de l'étape précédente.
    Après avoir ajouté les étapes, vous devez ajouter des activités de processus pour chaque étape.
12. Cliquez sur **Ajouter une autre activité de processus** à une étape particulière (par exemple, l'étape d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les étapes. De même, vous pouvez créer d'autres activités de processus pour chaque étape.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité de processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité de la définition d'activité.

Utilisation du playbook Échec de la connexion manuelle

Suivez ces étapes pour apprendre à utiliser le playbook Échec de la connexion manuelle dans l'espace de travail de l'analyste SIR et ses options.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.manager ou sn_si.analyst

Procédure

1. Dans l'espace de travail SIR, ouvrez un incident de sécurité.
2. Cliquez sur l'onglet **Playbook** .

   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité. Vous pouvez également voir des détails tels que la catégorie de l'incident de sécurité et le score de risque.

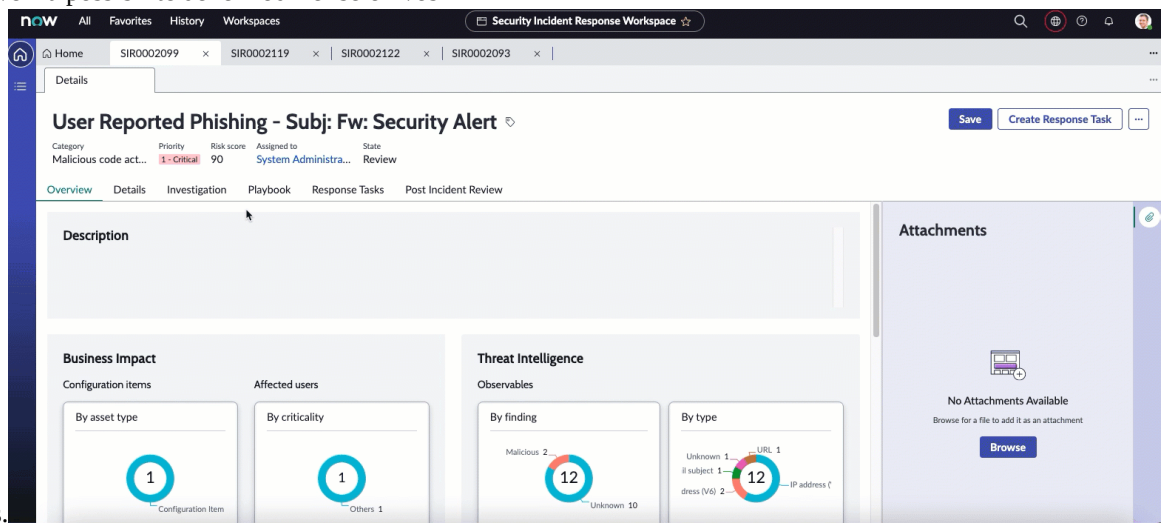
   Remarque : Si aucun playbook n'est répertorié, vous devez accéder à PAD et lui permettre de l'afficher dans l'onglet **Playbook** .

3. Cliquez sur le **playbook Échec de la connexion manuelle**.
   Pour l'échec de la connexion manuelle, les tâches sont automatiquement exécutées pour l'incident de sécurité.
4. Cliquez sur chaque étape pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous avez la possibilité de le modifier selon vos besoins.



6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Examiner pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action utilisateur à effectuer, elle s'affiche dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase respective et effectuez l'action pour terminer l'activité.

Playbooks basés sur le flux

Grâce à Flow Designer, les administrateurs de sécurité et les auteurs de conception de flux peuvent plus facilement passer de playbooks manuels ou non documentés à des playbooks automatisés et reproductibles. La fonction glisser-déposer offre une flexibilité dans le déplacement d'objets, les vérifications de conditions, les branches parallèles, les tables de décision, etc.

Réponse aux incidents de sécurité fournit les playbooks suivants avec le système de base.

En plus des playbooks répertoriés, il existe également des flux secondaires dans le spoke Security Operations qui peuvent être appelés à partir du playbook de flux. Les ransomwares sont l'un de ces flux secondaires.

Activez ces flux avant de les utiliser. Pour plus d'informations, consultez Activer un flux Security Incident Response.

Playbook pour l'hameçonnage automatisé

Le playbook d'hameçonnage automatisé vous aide à résoudre certains types de menaces de sécurité étape par étape. Les modèles de Concepteur de flux vous permettent d'automatiser les étapes du playbook de réponse d'hameçonnage et de résoudre les incidents rapidement et efficacement.

Vous pouvez utiliser des modèles créés avec Concepteur de flux pour automatiser les tâches dans le playbook de réponse d'hameçonnage afin d'analyser et de résoudre les attaques d'hameçonnage dans votre organisation.

Le playbook de réponse d'hameçonnage comprend les flux et flux secondaires suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Incident de sécurité - Modèle de réponse d'hameçonnage automatisé : ce modèle est conçu pour automatiser les tâches de réponse d'hameçonnage et contient une séquence d'actions, y compris un déclencheur.
- Incident de sécurité - Modèle manuel d'hameçonnage : ce modèle est le workflow de réponse manuelle par hameçonnage existant. Définissez la catégorie sur Hameçonnage pour activer le flux.

Ces modèles contiennent une séquence d'actions réutilisables conçues pour répondre aux attaques de phishing. Chaque flux dispose d'un déclencheur (condition), d'une séquence d'actions et de flux secondaires que vous pouvez annoter pour plus de lisibilité. Pour accéder à ces flux, vous devez installerle spoke Security Operations .

Remarque : Activez ces modèles avant de pouvoir les utiliser. Pour plus d'informations, consultez Activer un flux Security Incident Response .

- Exécuter des recherches de menace pour les observables : effectue des recherches de menace sur les observables sélectionnés.
- Enrichir les observables : vous permet d'enrichir les observables avec des informations supplémentaires provenant de diverses sources.
- Évaluer l'impact de l'e-mail d'hameçonnage : vous permet d'évaluer l'impact de l'e-mail d'hameçonnage. Lorsque vous recevez un e-mail à l'adresse e-mail d'hameçonnage, ce flux secondaire analyse le . Pièce jointe EML et compare les informations aux règles de correspondance d'e-mail.
- Éradiquer les e-mails d'hameçonnage : vous permet de supprimer ou d'éradiquer les e-mails d'hameçonnage afin de réduire l'exposition à une attaque spécifique.
- Exécuter une recherche de perception sur les observables : détermine la prévalence d'une menace dans le temps ou teste les efforts de rattrapage ou d'éradication.
- Créer des demandes de blocs : bloque la communication avec les observables associés à l'incident.

Ces flux secondaires représentent un ensemble d'opérations réutilisables que vous pouvez utiliser dans plusieurs playbooks. Vous pouvez utiliser ces flux secondaires pour définir des modèles personnalisés (flux) en fonction de vos besoins.

Pour créer des modèles personnalisés (flux), suivez les instructions de la section Flux .

Exécuter le flux du playbook de réponse d'hameçonnage automatisé

À l'aide du concepteur de flux, vous pouvez définir et automatiser les tâches dans le playbook pour analyser et résoudre les attaques de phishing contre votre organisation.

Avant de commencer

- Rôle requis : sn_si.admin, flow_designer et action_designer
- Installez et configurez les intégrations suivantes avec les bonnes informations d'identification :
  - Demande de bloc (Opérations de sécurité intégration NGFW Palo Alto Networks)
  - Enrichissement des éléments observables
  - Recherche de perception
  - Recherche de menace
  - Microsoft Office Exchange

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

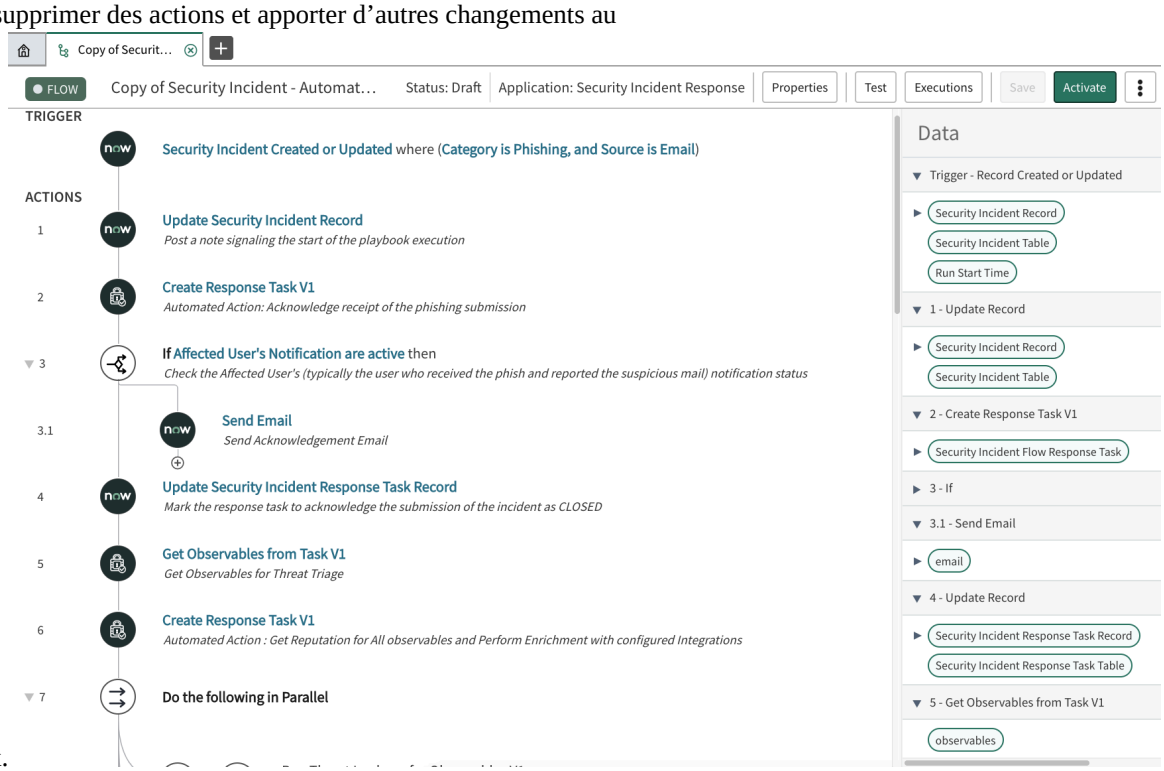
Lorsque les employés reçoivent un e-mail suspect contenant les signes courants d'une attaque de phishing (tels que définis par vos politiques de sécurité), ils peuvent l'envoyer sous forme de . Pièce jointe EML à l'adresse e-mail d'hameçonnage définie par votre organisation. À l'aide des tâches définies dans le flux du playbook d'hameçonnage automatisé, vous pouvez trier, analyser, contenir et éradiquer une menace d'hameçonnage. Ces tâches peuvent être invoquées dans le cadre de différents états d'incident (par exemple, Analyse, Contenir, etc.). Lorsqu'un incident de sécurité d'hameçonnage est créé, le flux d'hameçonnage automatisé peut être déclenché automatiquement. Le concepteur de flux vous permet d'afficher les détails des différentes actions de réponse aux incidents au fur et à mesure qu'elles sont invoquées.

Remarque : Le flux du playbook Incident de sécurité - Modèle de réponse d'hameçonnage automatisé V1 est en lecture seule. Vous pouvez effectuer une copie du flux et apporter les modifications nécessaires.

Les étapes suivantes décrivent comment faire une copie du modèle de playbook d'hameçonnage et vous guident à travers certaines des tâches du flux.

Procédure

1. Accédez à la **Tous** > **Concepteur de flux** > **Concepteur** pour afficher les flux disponibles avec le Opérations de sécurité spoke.
2. Cliquez sur le lien **Security Incident - Automated Phishing Response Template** VI.
3. Sur la page Flux, cliquez sur , faites une copie du flux et ouvrez-le pour votre utilisation. Vous pouvez modifier les conditions de déclenchement, ajouter ou supprimer des actions et apporter d'autres changements au flux.



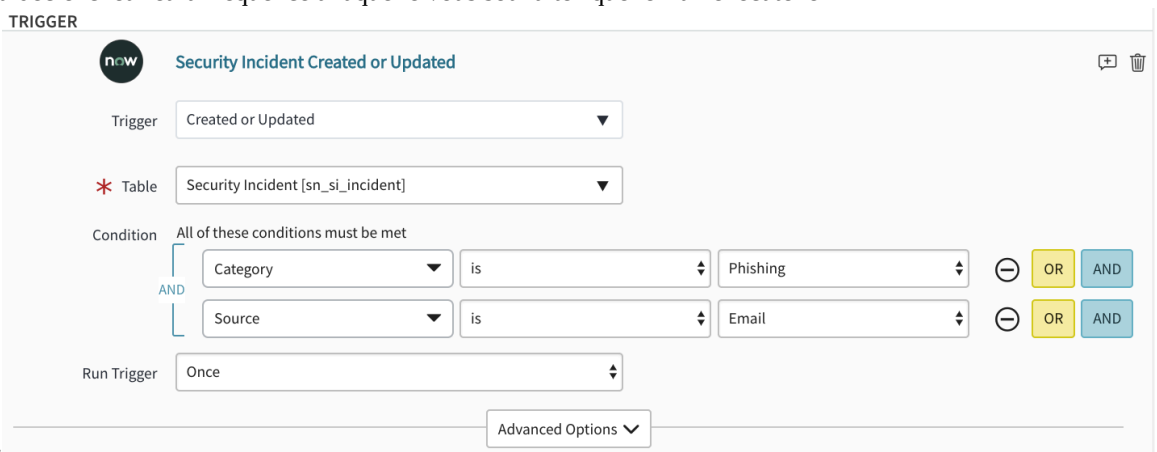
Cette image montre les conditions de déclenchement et les étapes exécutées par le flux. Le panneau de droite affiche le flux de données. Cliquez sur une icône pour développer l'étape et afficher les détails.

4. Cliquez sur l'icône **Déclencher** .

Traduction automatique

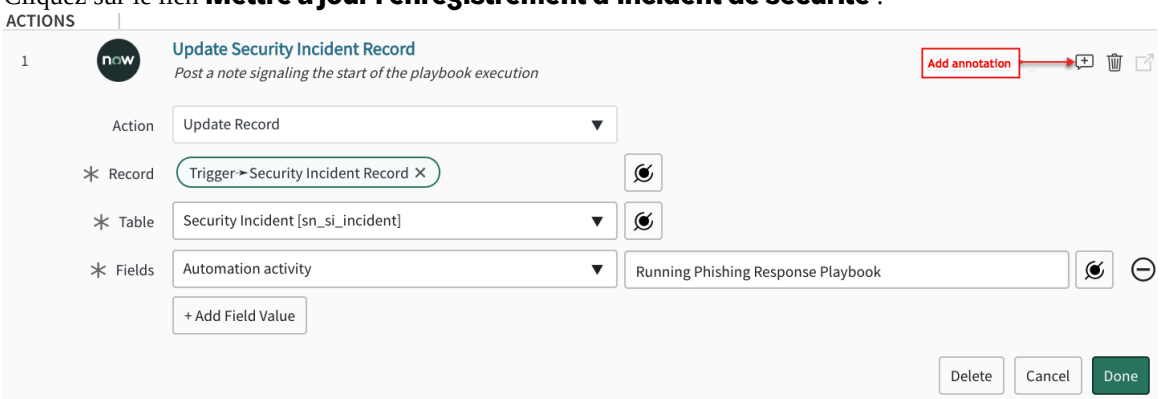
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans la première étape, vous définissez ou définissez le déclencheur du flux. Spécifiez les conditions du déclencheur et la fréquence à laquelle vous souhaitez que le flux exécute le déclencheur.



Lorsque les conditions définies dans le flux (catégorie est Hameçonnage et Source est E-mail) sont remplies dans l'enregistrement d'incident, les tâches du flux d'hameçonnage automatisé commencent à s'exécuter séquentiellement. Vous pouvez modifier le déclencheur, ajouter des annotations, ajouter ou supprimer des conditions, etc.

5. Cliquez sur le lien **Mettre à jour l'enregistrement d'incident de sécurité** .



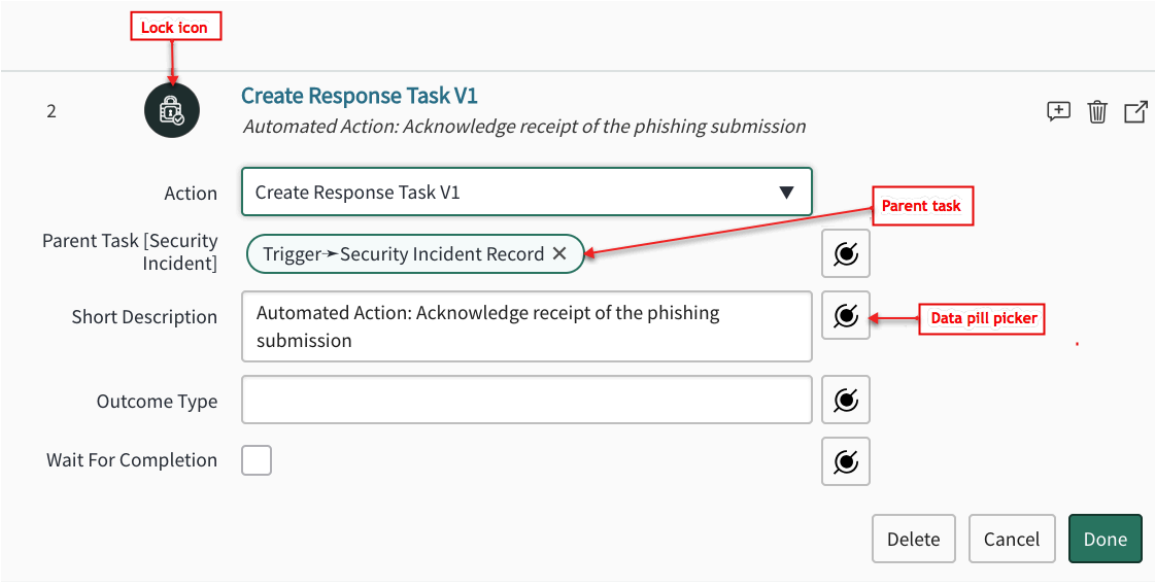
La mise à jour de l'enregistrement d'incident de sécurité constitue la première étape du flux. Cliquez sur l'icône pour ajouter une note à l'analyste de sécurité indiquant qu'un incident d'hameçonnage s'est produit et que le flux du playbook d'hameçonnage automatisé a commencé à s'exécuter.

6. Poursuivez avec l'étape 2 du flux, puis cliquez sur le lien **Créer une tâche de réponse** .

Dans cette étape, le flux crée une tâche de réponse automatisée pour en accuser réception à l'émetteur de l'incident ou à l'utilisateur affecté.

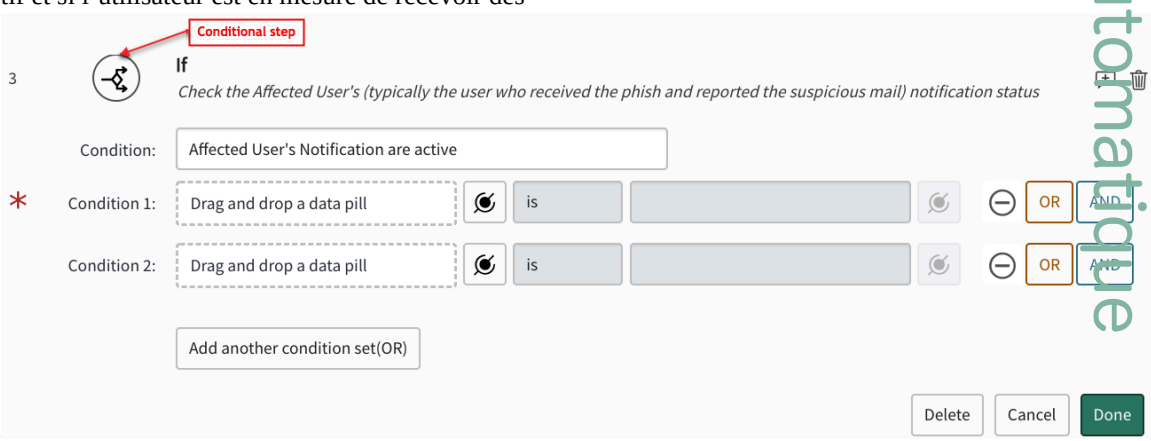
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Notez que le champ **Tâche parente [Incident de sécurité]** fait référence à l'enregistrement parent associé à cette étape. Vous pouvez choisir n'importe quel enregistrement de référence à l'aide de l'icône de sélection de pastilles de données, de ou faire glisser l'élément de référence pertinent depuis le panneau de droite. Remarquez l'icône de verrouillage . L'icône de verrou indique que cette étape ne nécessite aucune intervention de l'utilisateur.

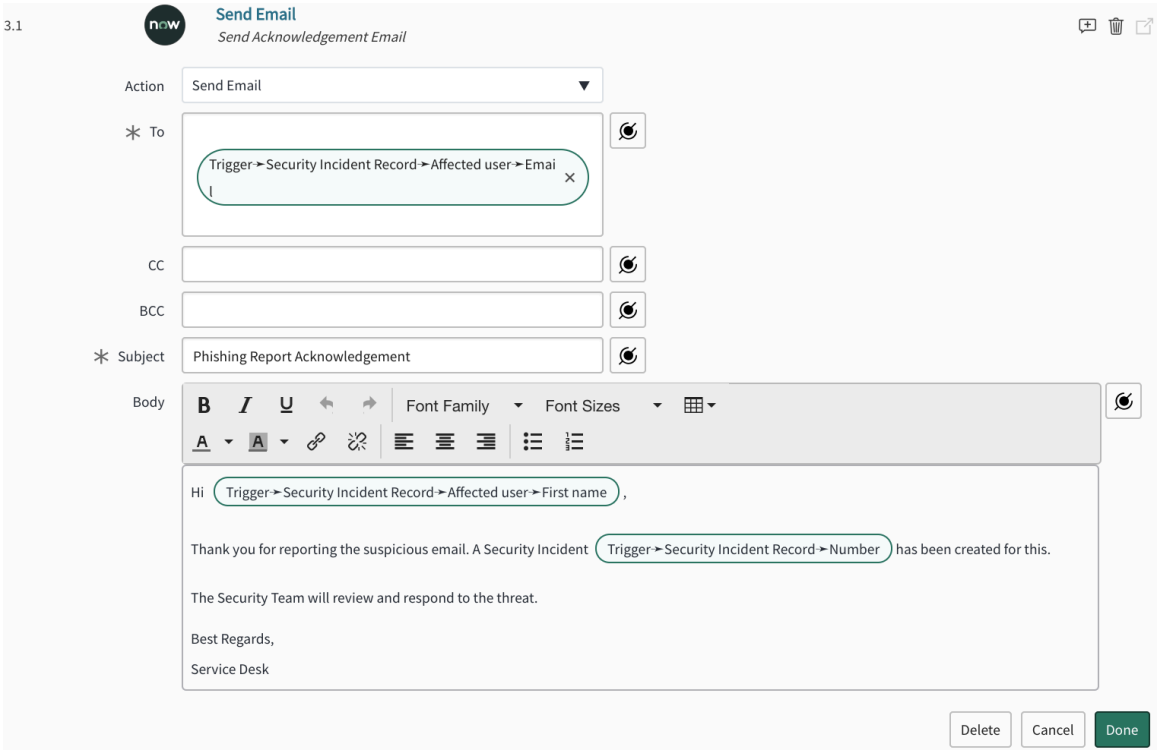
7. À l'étape 3, le flux collecte des détails supplémentaires sur l'utilisateur affecté (généralement l'utilisateur qui a soumis l'incident) pour s'assurer qu'il peut envoyer une notification avec succès.
Vous pouvez spécifier des conditions pour vérifier si l'état de l'utilisateur affecté est actif et si l'utilisateur est en mesure de recevoir des notifications.



Remarquez l'icône à l'étape 3. Le flux exécute l'étape suivante (3.1) uniquement si les conditions spécifiées sont remplies.

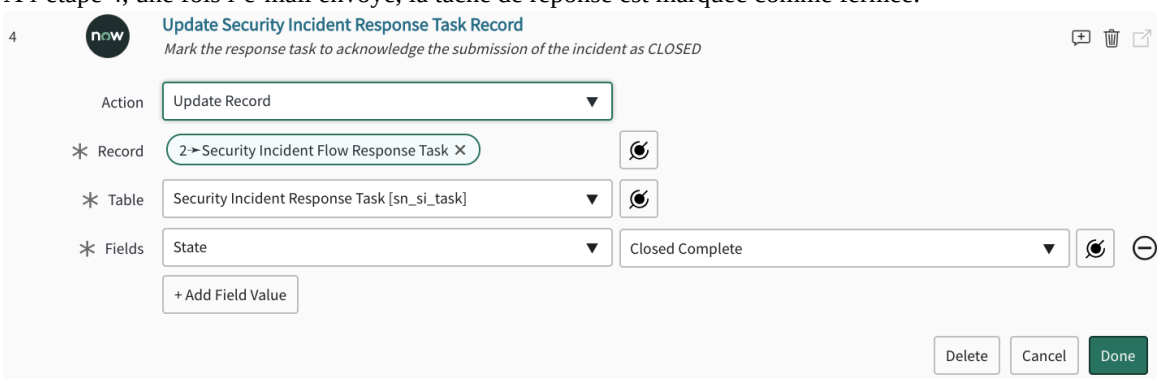
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Lorsque les conditions définies à l'étape 3 ont été remplies avec succès, l'e-mail est envoyé.

8. À l'étape 4, une fois l'e-mail envoyé, la tâche de réponse est marquée comme fermée.



9. À l'étape 5, tous les observables impliqués dans l'incident (tels que l'objet de l'e-mail, l'adresse e-mail à partir de laquelle l'e-mail d'hameçonnage a été envoyé, l'URL d'hameçonnage) ou les observables appartenant à une catégorie sélectionnée (hachage, fichier ou domaine) sont collectés pour effectuer des actions automatisées supplémentaires dans les étapes suivantes du playbook.



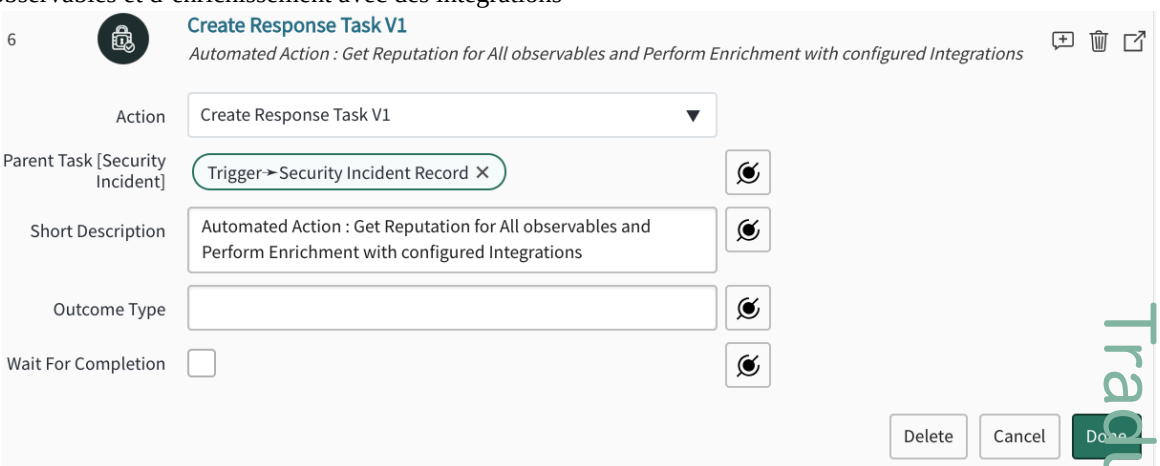
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

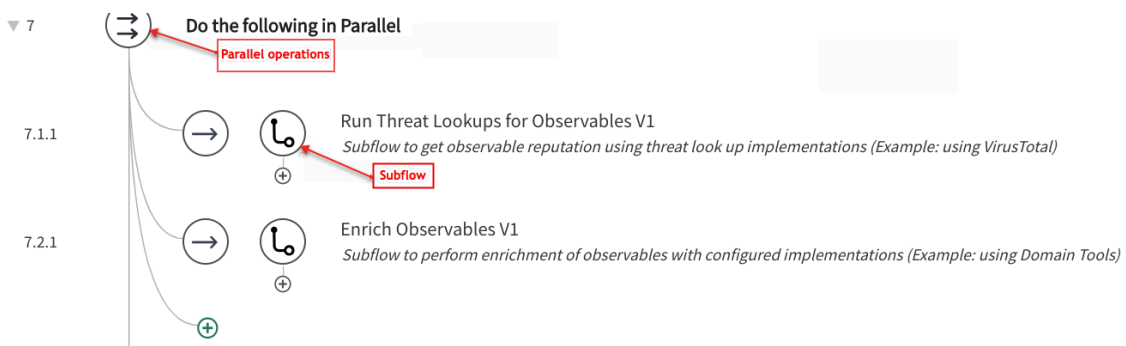
Cliquez sur l'icône du concepteur pour afficher une vue détaillée de l'action.

Pour afficher la page Concepteur d'action , développez une étape dans le flux et cliquez sur l'icône Concepteur d'action.

10. À l'étape 6, une tâche de réponse automatisée est créée.
Cette tâche capture le début du processus d'obtention de la réputation de tous les observables et d'enrichissement avec des intégrations configurées.



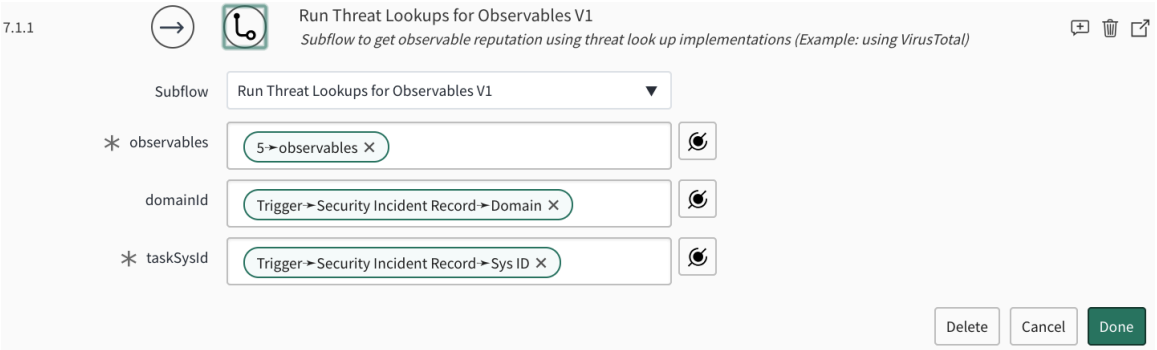
11. À l'étape 7, deux flux secondaires sont appelés :
    - Exécuter des recherches de menace pour les observables : ce flux secondaire est utilisé pour obtenir la réputation de tous les observables à l'aide d'implémentations de la recherche de menace.
    - Enrichir les observables : ce flux secondaire permet d'enrichir les observables avec des implémentations configurées.



Notez les icônes de cette tâche. L'icône Opérations parallèles indique que les deux tâches seront exécutées en parallèle et l'icône de flux secondaire indique que la tâche effectuée est un flux secondaire, comme indiqué ci-dessous :

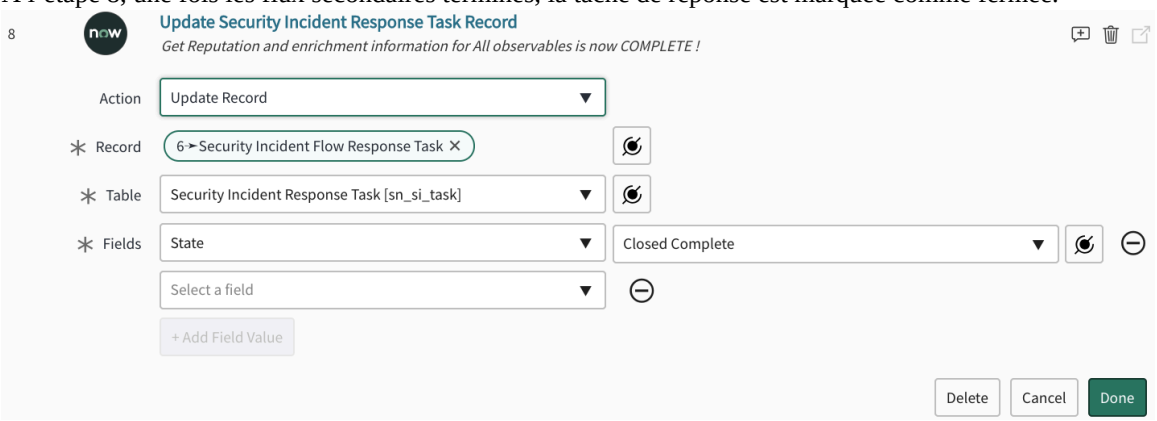
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

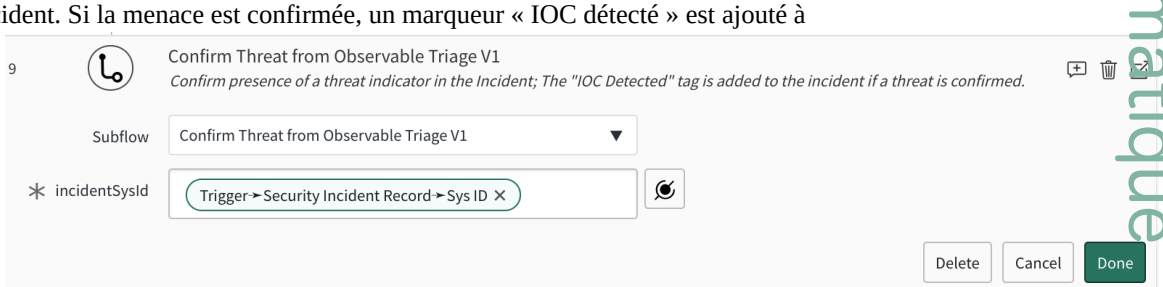


Notez le nombre 5 dans le champ Observables. Cela indique que la recherche de menace sera exécutée sur les observables récupérés à l'étape 5. Ce flux secondaire appelle à son tour des workflows et des actions existants, comme indiqué dans le concepteur de flux secondaires.

12. À l'étape 8, une fois les flux secondaires terminés, la tâche de réponse est marquée comme fermée.



13. À l'étape 9, le flux secondaire Confirmer la menace à partir du triage de l'observable est appelé. Ce flux secondaire est utilisé pour confirmer la présence d'un indicateur de menace dans l'incident. Si la menace est confirmée, un marqueur « IOC détecté » est ajouté à l'incident.



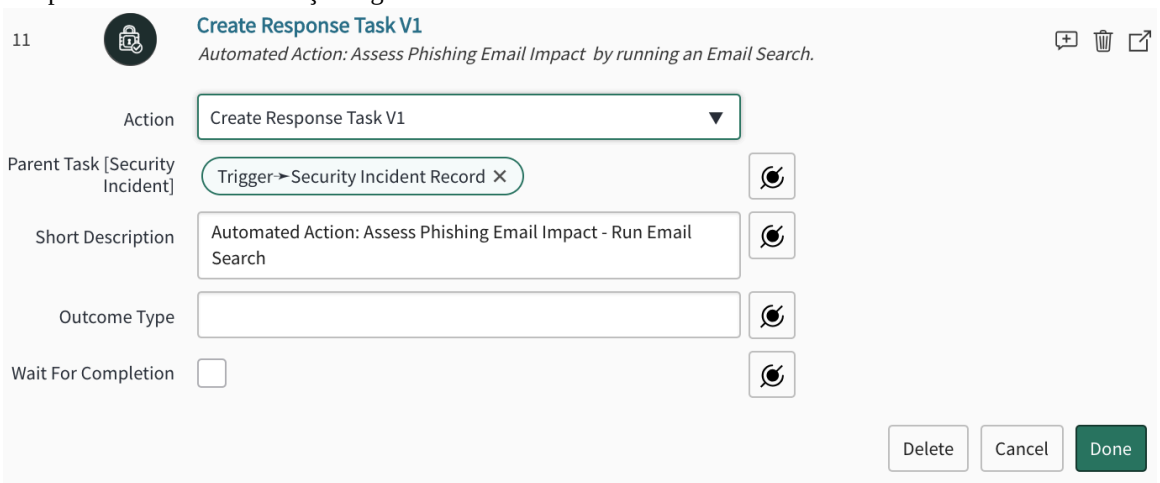
14. Lorsque la menace est confirmée, à l'étape 10, vous mettez à jour l'incident de sécurité et ajoutez une note indiquant que des tâches de maîtrise de la menace seront lancées.



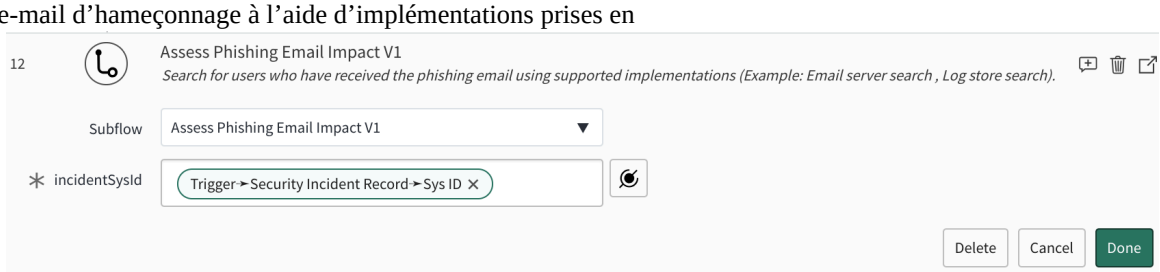
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

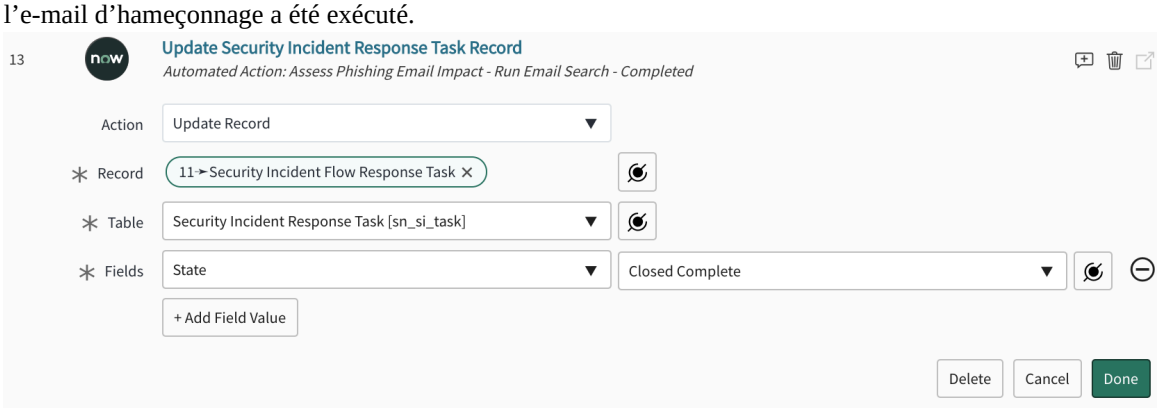
15. L'étape 11 est une tâche de réponse automatisée qui capture le début et la fin de la tâche utilisée pour évaluer l'impact des e-mails d'hameçonnage.



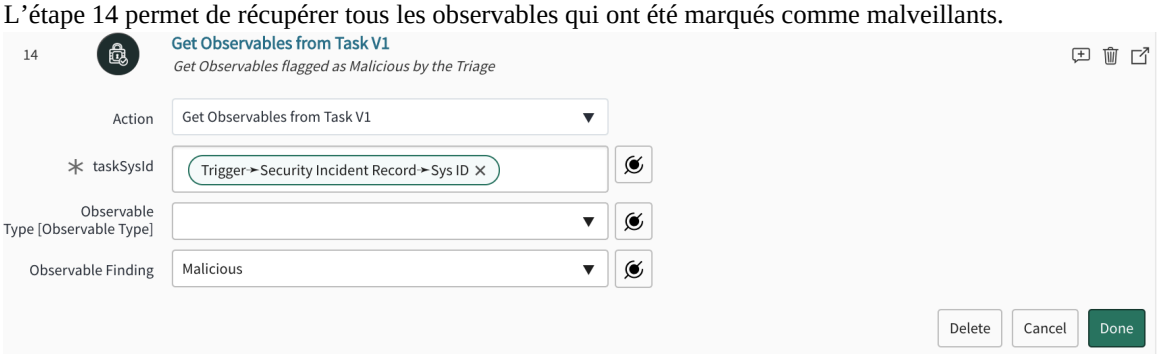
16. À l'étape 12, le flux secondaire Évaluer l'impact des e-mails d'hameçonnage est appelé. Ce flux secondaire est utilisé pour rechercher les utilisateurs qui ont reçu l'e-mail d'hameçonnage à l'aide d'implémentations prises en charge.



17. À l'étape 13, la tâche est marquée comme fermée pour indiquer que le flux secondaire Évaluer l'impact de l'e-mail d'hameçonnage a été exécuté.



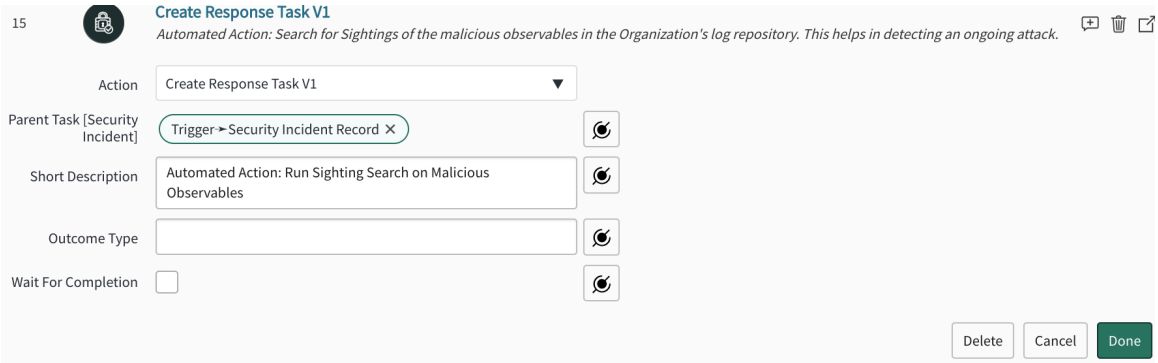
18. L'étape 14 permet de récupérer tous les observables qui ont été marqués comme malveillants.



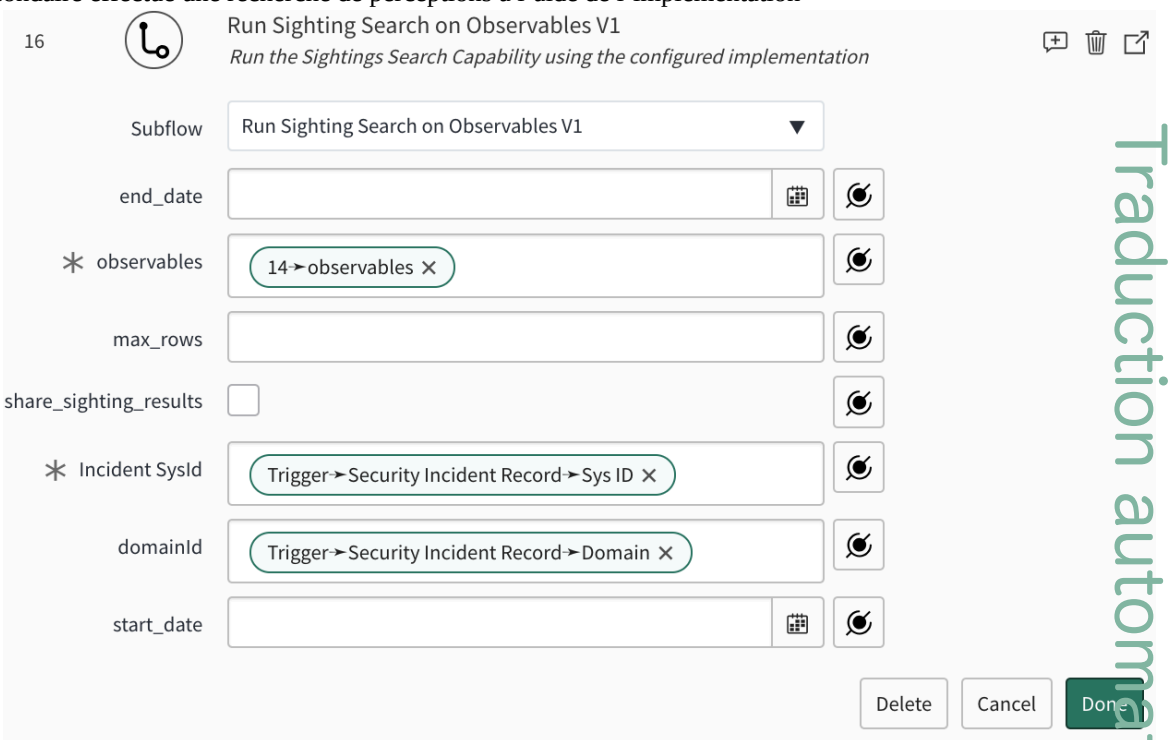
19. L'étape 15 est une tâche de réponse automatisée qui capture le début et la fin de la tâche Recherche d'observation des observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

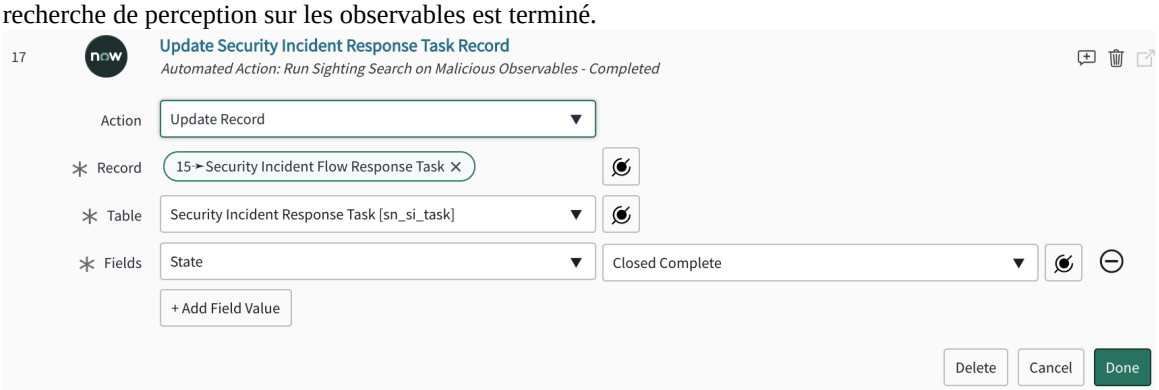


20. À l'étape 16, le flux secondaire Exécuter une recherche de perception sur les observables est appelé. Ce flux secondaire effectue une recherche de perceptions à l'aide de l'implémentation



configurée.

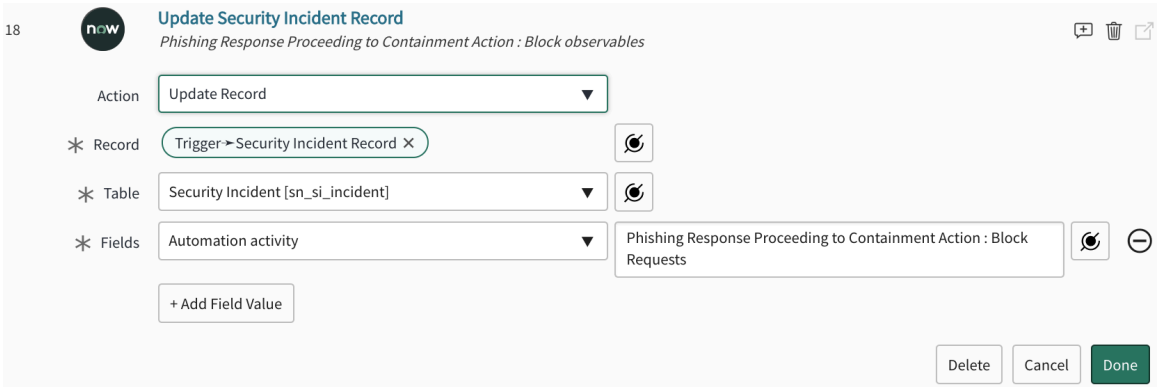
21. À l'étape 17, la tâche est marquée comme fermée pour indiquer que le flux secondaire Exécuter une recherche de perception sur les observables est terminé.



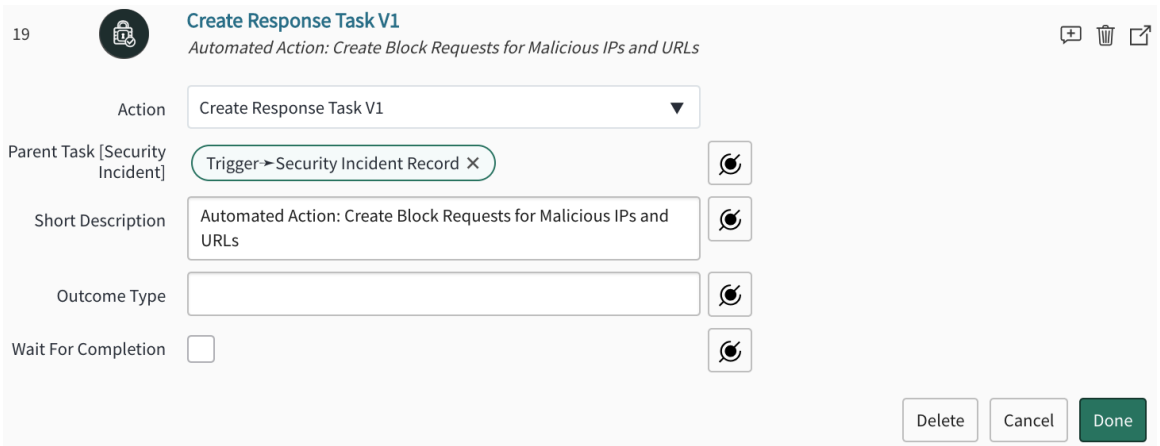
22. Une fois que vous avez identifié les observables malveillants, à l'étape 18, vous mettez à jour l'enregistrement d'incident de sécurité pour indiquer que les actions de confinement vont maintenant commencer.

Traduction automatique

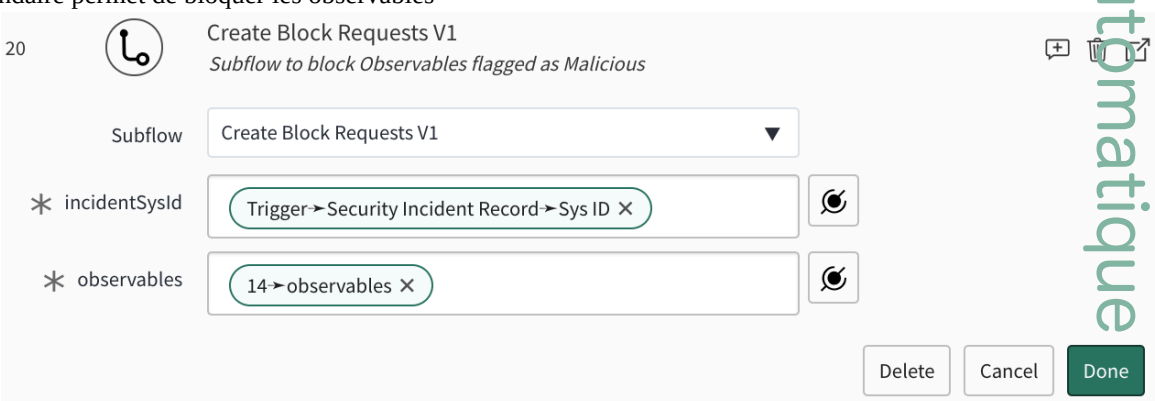
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



23. L'étape 19 est une tâche de réponse automatisée qui capture le début et l'achèvement de la tâche de demandes de bloc.

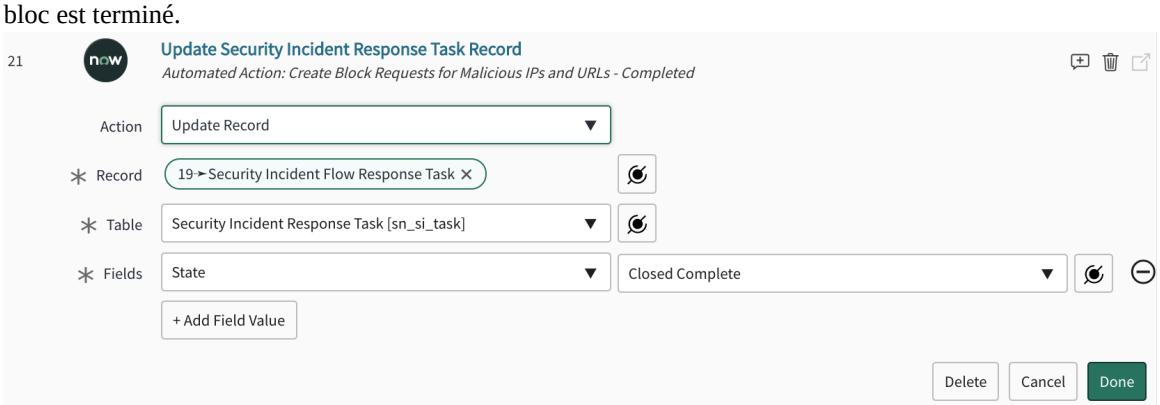


24. À l'étape 20, le flux secondaire Créer des demandes de bloc est appelé.
Ce flux secondaire permet de bloquer les observables



malveillants.

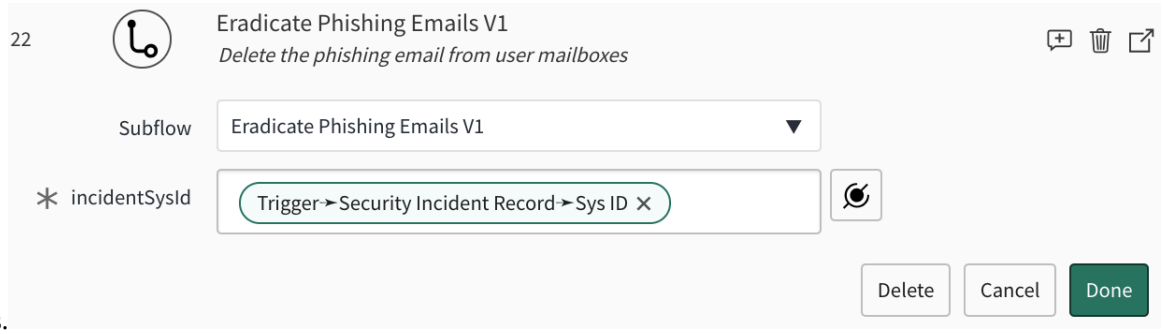
25. À l'étape 21, la tâche est marquée comme fermée pour indiquer que le flux secondaire Créer des demandes de bloc est terminé.



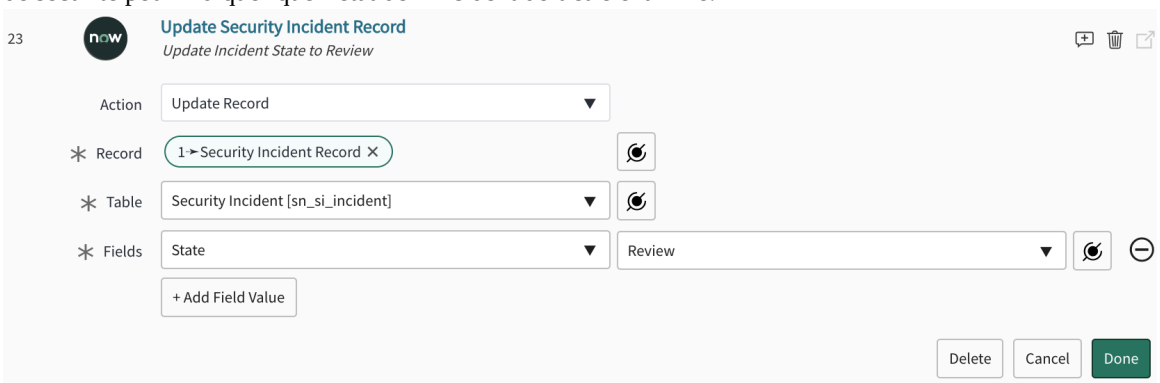
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

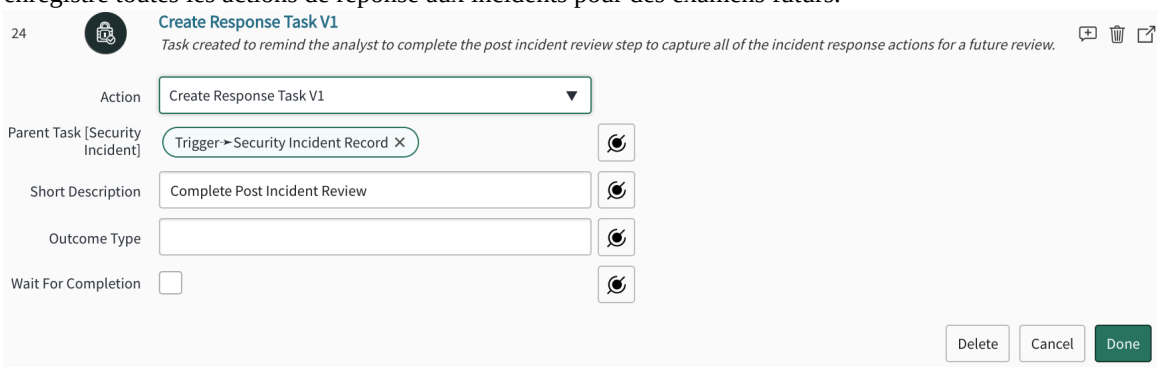
26. À l'étape 22, le flux secondaire Éradiquer les e-mails d'hameçonnage est appelé.
Ce flux secondaire est utilisé pour supprimer les e-mails d'hameçonnage des boîtes aux lettres des utilisateurs.



27. Une fois les e-mails d'hameçonnage supprimés, à l'étape 23, vous mettez à jour l'enregistrement d'incident de sécurité pour indiquer que l'état de l'incident doit être examiné.



28. Dans la dernière étape, le flux crée une tâche de réponse automatisée.
Cette tâche est utilisée pour envoyer un rappel à l'analyste de sécurité afin qu'il enregistre toutes les actions de réponse aux incidents pour des examens futurs.



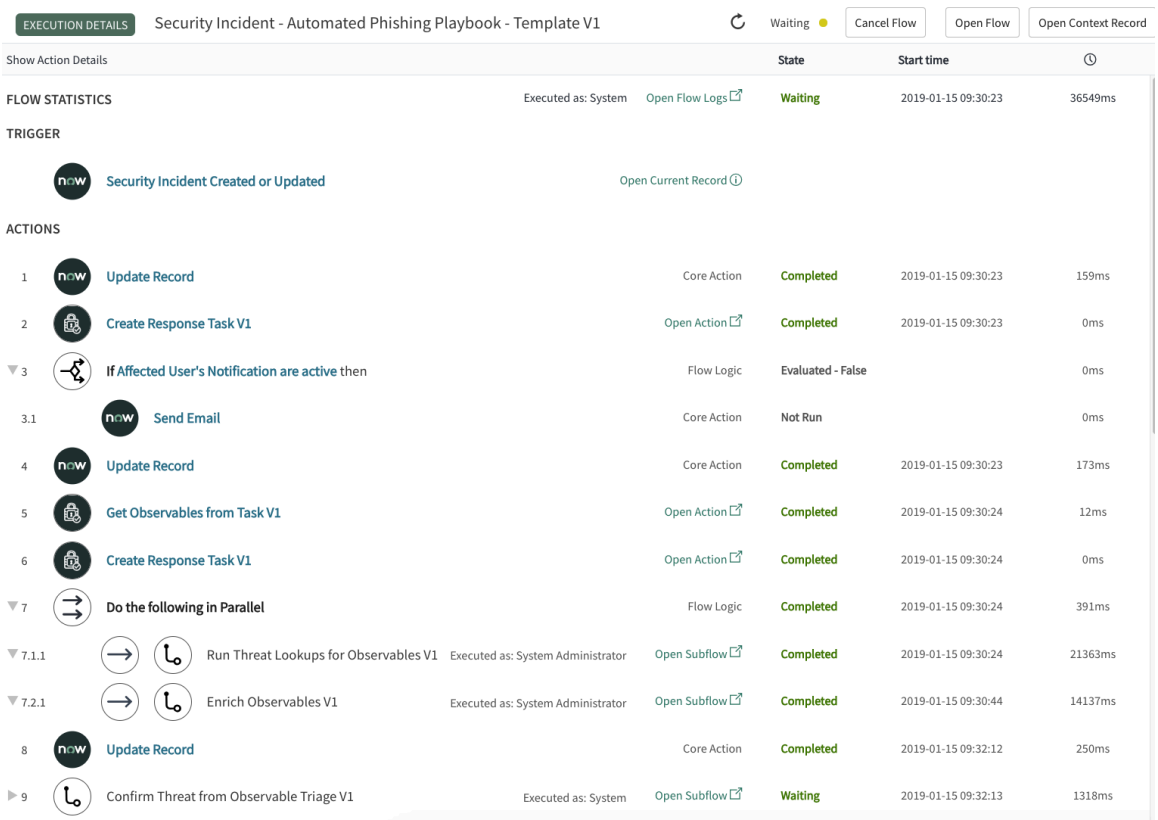
Que faire ensuite

Vous pouvez cliquer sur **Tester** pour simuler les actions dans le flux avant de le publier. Après avoir testé le flux, cliquez sur **Activer** pour activer le flux et l'exécuter.

Cliquez sur **Exécutions** pour afficher les détails d'exécution du flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



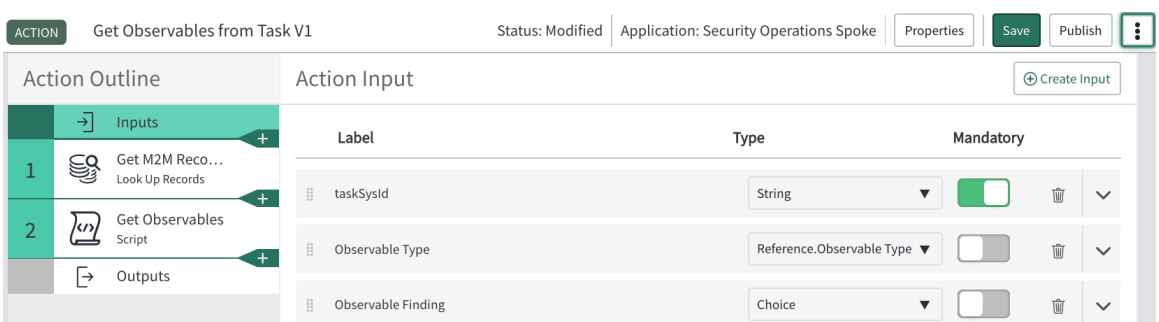
Afficher la réponse d'hameçonnage automatisée Concepteur d'action de flux de playbook

Vous pouvez explorer le concepteur d'action pour afficher des informations détaillées sur les actions effectuées pour une étape spécifique dans le flux de réponse d'hameçonnage automatisé.

Cette page décrit la page Concepteur d'action pour l'étape Obtenir des observables à partir de la tâche. Sélectionnez une tâche dans le panneau Plan d'action pour en afficher les détails.

Entrées d'action

Cette section affiche les détails de la création de l'action, y compris l'ID de l'incident, le type d'observable (hachage ou IP) et la recherche observable (e-mails malveillants uniquement).

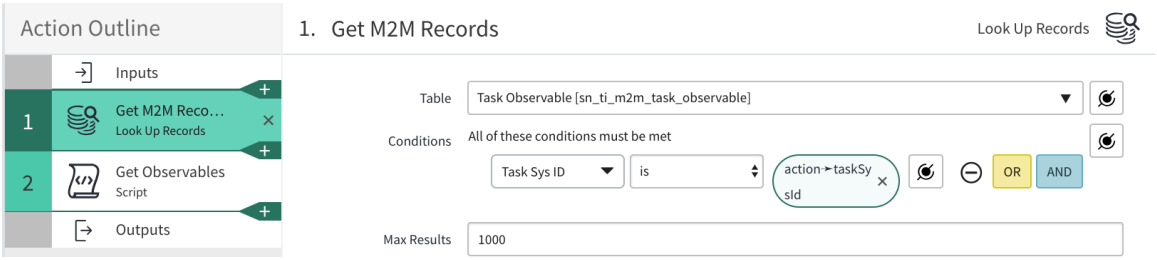


Obtenir les enregistrements N-N

Cette section affiche les conditions qui ont été définies pour rechercher des observables dans une table spécifiée.

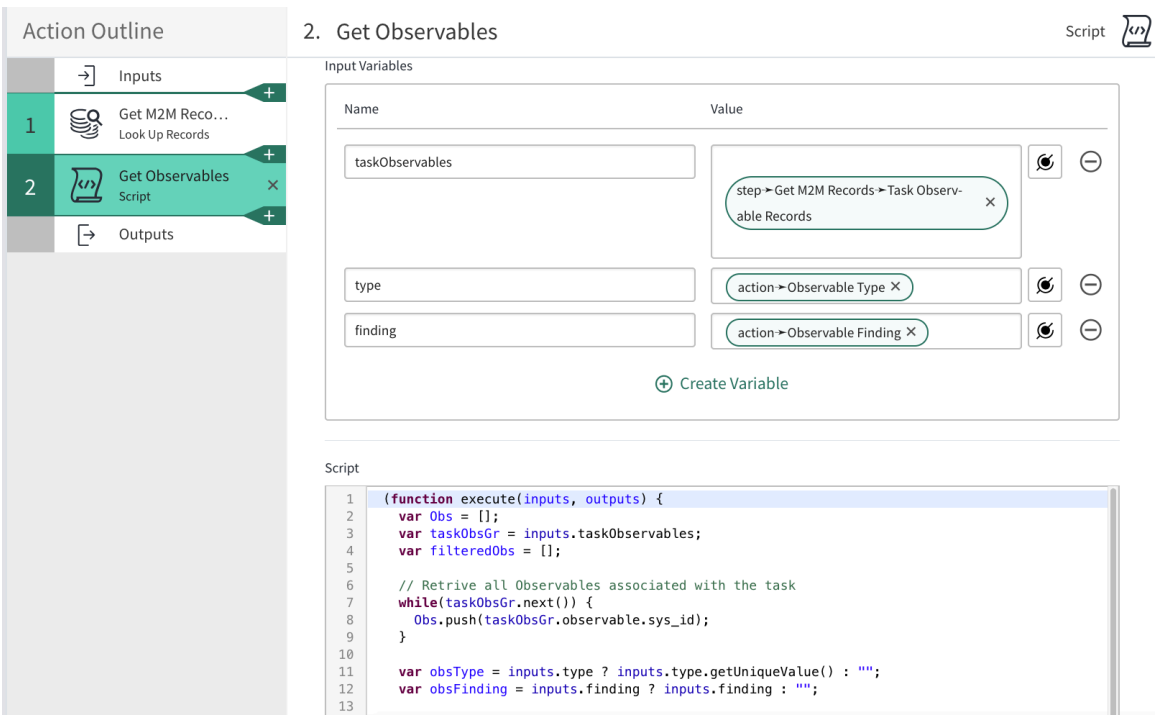
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Obtenir des observables

Cette section présente le script utilisé pour récupérer les observables en fonction des conditions de filtre spécifiées. Enfin, les observables répondant à ce critère et le nombre sont affichés.



Remarque : Toutes les actions définies dans ce flux sont réutilisables et modifiables en fonction de vos besoins.

Afficher le playbook de réponse d'hameçonnage automatisé Concepteur de flux secondaires

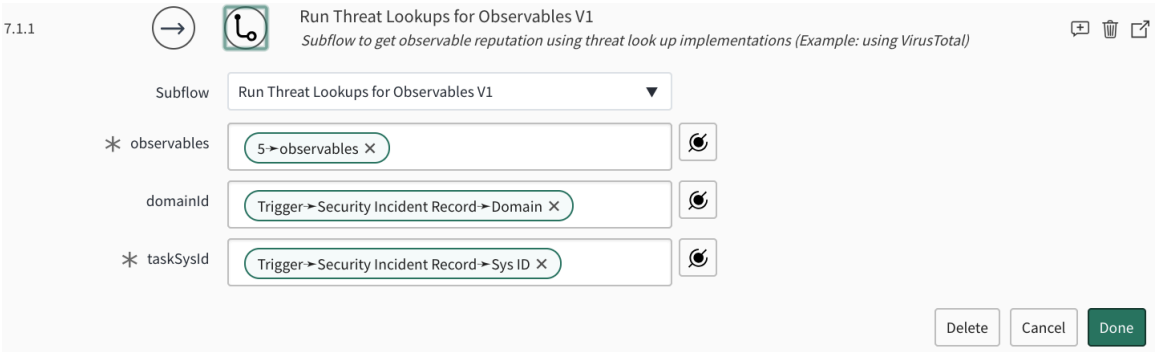
Vous pouvez explorer le concepteur de flux secondaire pour afficher des informations détaillées sur le flux secondaire exécuté dans le cadre du flux de réponse d'hameçonnage automatisé.

Vous pouvez lancer le concepteur de flux secondaires pour afficher les détails supplémentaires d'un flux secondaire. La page Concepteur de flux secondaire pour le flux secondaire Exécuter des recherches de menace pour les observables s'affiche ici.

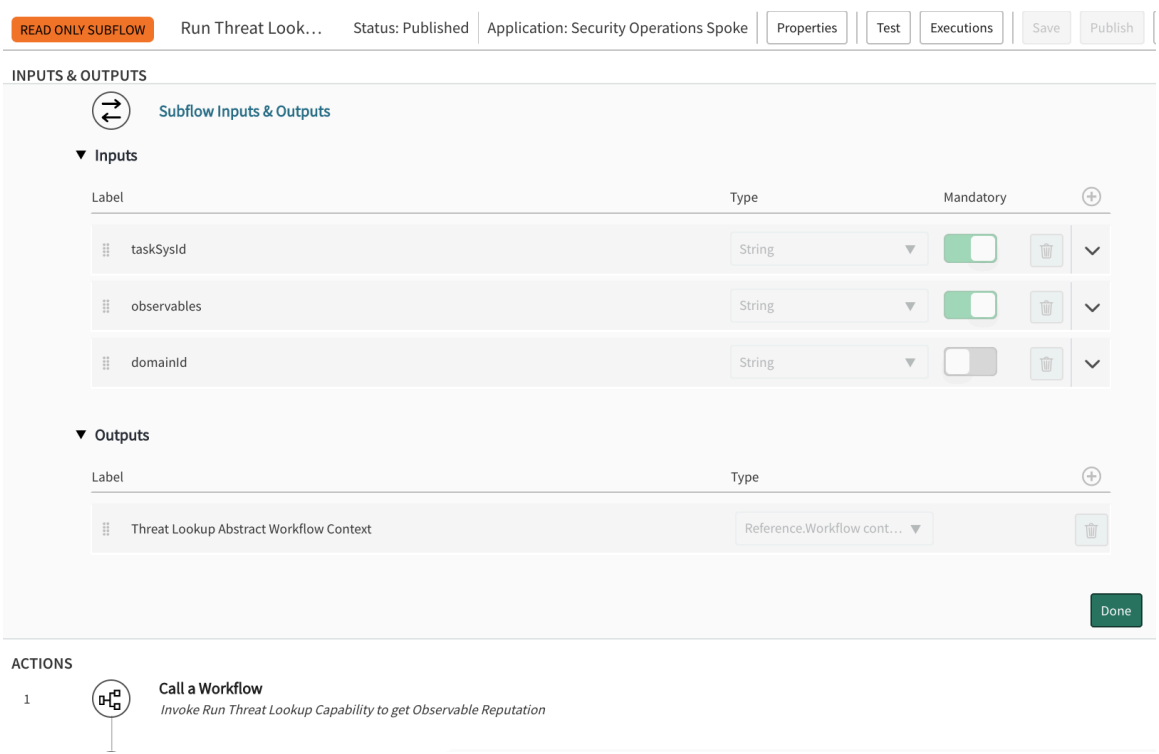
Sélectionnez l'icône du dans l'image ci-dessous pour afficher le concepteur de flux secondaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Sur la page Concepteur de flux secondaires, vous pouvez voir les entrées et sorties de ce flux secondaire, ainsi que les actions de workflow sous-jacentes en cours d'exécution.



Remarque : Ce flux secondaire est en lecture seule et ne peut pas être modifié. Vous pouvez ajouter ou supprimer des flux secondaires à l'étape, mais vous ne pouvez pas modifier les flux secondaires.

Playbook pour les programmes malveillants automatisés

Le playbook de programme malveillant automatisé fournit une séquence d'étapes automatisées qui vous aide à résoudre les alertes de programme malveillant rapidement et efficacement.

Utilisez le flux du playbook de programme malveillant pour automatiser les étapes de gestion des alertes de programme malveillant provenant du point de terminaison ou du réseau. Le modèle de flux comprend des conditions de déclenchement, une séquence d'actions et des flux secondaires annotés pour plus de lisibilité.

Ces modèles contiennent une séquence d'actions réutilisables conçues pour répondre aux attaques de phishing. Chaque flux possède un déclencheur (condition), une séquence d'actions et de flux secondaires annotés pour plus de lisibilité. Pour accéder à ces flux, vous devez installer lespoke Security Operations et l'application Security Operations Palo Alto Networks - WildFire à partir du ServiceNow Store.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous devez activer ces modèles avant de pouvoir les utiliser.

Les flux et flux secondaires suivants sont inclus :

- Modèle de playbook automatisé d'incidents de sécurité - programme malveillant : ce modèle est conçu pour automatiser les réponses aux alertes de programme malveillant et contient une séquence d'actions, y compris un déclencheur.
- Modèle manuel Incident de sécurité - Programme malveillant : ce modèle est le workflow de réponse manuelle aux programmes malveillants existant qui est activé lorsque la catégorie est définie sur Activité de code malveillant.

Flux secondaires

- Confirmer la menace à partir de l'observable : vérifie si les observables sont malveillants et doivent être traités.
- Définir la gravité de l'incident : définit un statut de gravité pour l'incident.
- Playbook de rançongiciel : détermine s'il s'agit d'une attaque de rançongiciel.

Ces flux secondaires représentent un ensemble d'opérations réutilisables qui peuvent être utilisées dans plusieurs playbooks. Vous pouvez utiliser ces flux secondaires pour définir des modèles personnalisés (flux) en fonction de vos besoins.

Pour créer des modèles personnalisés (flux), suivez les instructions de la section Flux .

Exécuter le flux du playbook de programme malveillant automatisé

Utilisez ce flux pour automatiser les tâches dans le playbook afin d'analyser et de résoudre les attaques de programmes malveillants contre votre organisation.

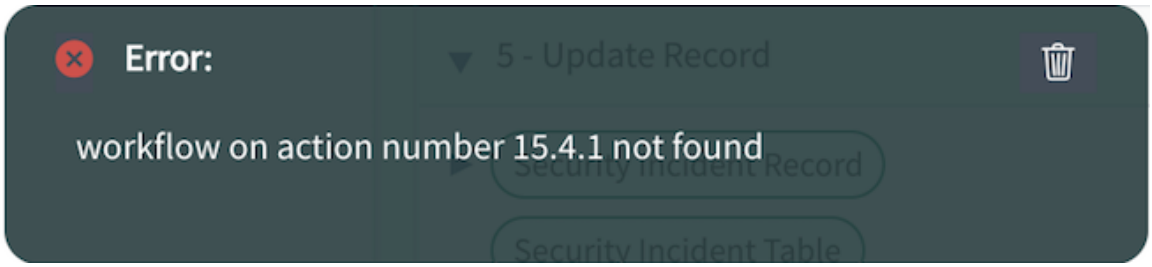
Avant de commencer

- Rôle requis : sn_si.admin, flow_designer et action_designer
- Installez et configurez les intégrations suivantes avec les informations d'identification correctes :
  - Palo Alto Networks WildFire pour les opérations de sécurité
  - Recherche de perception (Splunk)
  - Demandes de blocs
  - Recherche de menace
  - Enrichir les observables

  Vérifiez que ces intégrations fonctionnent correctement avant d'activer le modèle de Playbook Incident de sécurité - Programme malveillant automatisé.
- Application Security Operations Palo Alto Networks Wildfire : pour accéder au flux automatisé du Playbook de programme malveillant, vous devez installer le spoke Security Operations et l'application Security Operations Palo Alto Networks - WildFire à partir du ServiceNow Store. Si l'application Security Operations Palo Alto Networks Wildfire n'est pas installée, vous verrez une erreur « workflow sur l'action numéro 15.4.1 introuvable » comme indiqué ci-dessous :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Si vous ne souhaitez pas installer cette application, supprimez les étapes **15.2, 15.3 et 15.4** du flux du playbook automatisé de programme malveillant.

- Assurez-vous que les conditions suivantes sont remplies :
  - L'incident de sécurité a été affecté à un analyste de sécurité qui appartient au groupe d'approbation approprié.
  - L'analyste de sécurité qui gère l'incident doit avoir une adresse e-mail valide.
  - Les éléments de configuration et les observables nécessaires ont été ajoutés à l'incident de sécurité.
- Pour **l'étape 21 (Demander l'approbation),** remplacez le groupe **d'Affectation d'incident de sécurité** par votre groupe préféré.
- L'étape 21 du flux est une étape d'approbation de tâche obligatoire où une demande d'approbation est envoyée à l'administrateur. Pour approuver la demande, l'administrateur doit accéder à la page Approbations des tâches et définir le champ État sur **Approuvé**. Si la tâche n'est pas approuvée, le concepteur de flux ne peut pas poursuivre et le processus se termine.

Pourquoi et quand exécuter cette tâche

Lorsqu'une activité de code malveillant est détectée dans le réseau, un incident de sécurité est créé et le flux automatisé du playbook de programme malveillant est lancé. Vous pouvez utiliser les tâches définies dans le flux du playbook automatisé de programme malveillant pour trier, analyser, contenir et éradiquer la menace.

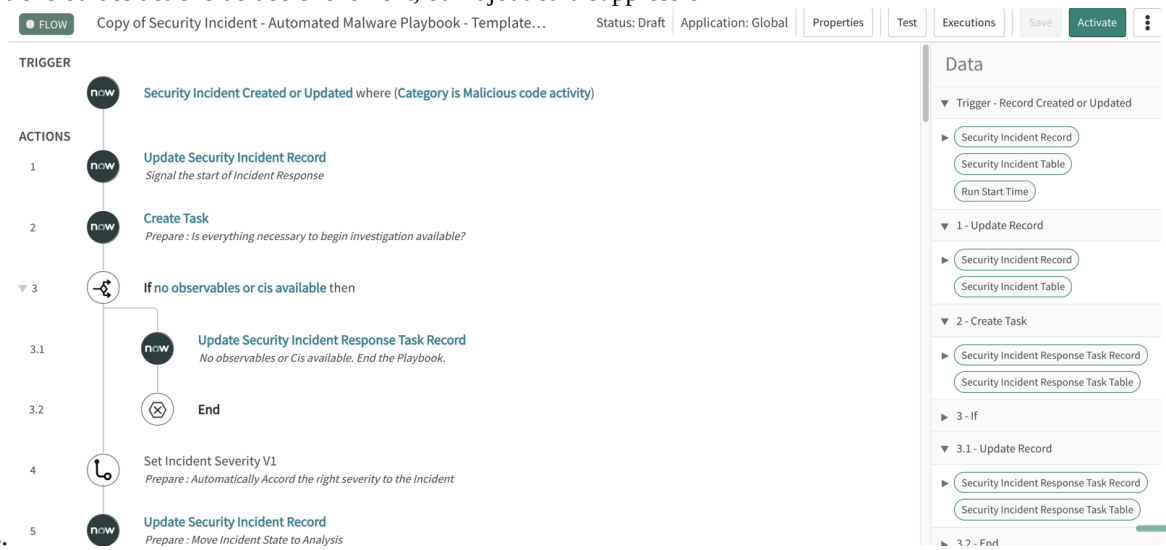
Procédure

1. Accédez à la **Tous** > **Concepteur de flux** > **Concepteur** pour afficher les flux disponibles avec le spoke Security Operations.
2. Cliquez sur le lien **Incident de sécurité - Playbook de programme malveillant automatisé - Modèle VI** .
3. Sur la page Flux, cliquez sur , faites une copie du flux et ouvrez-le pour votre utilisation.

Traduction automatique

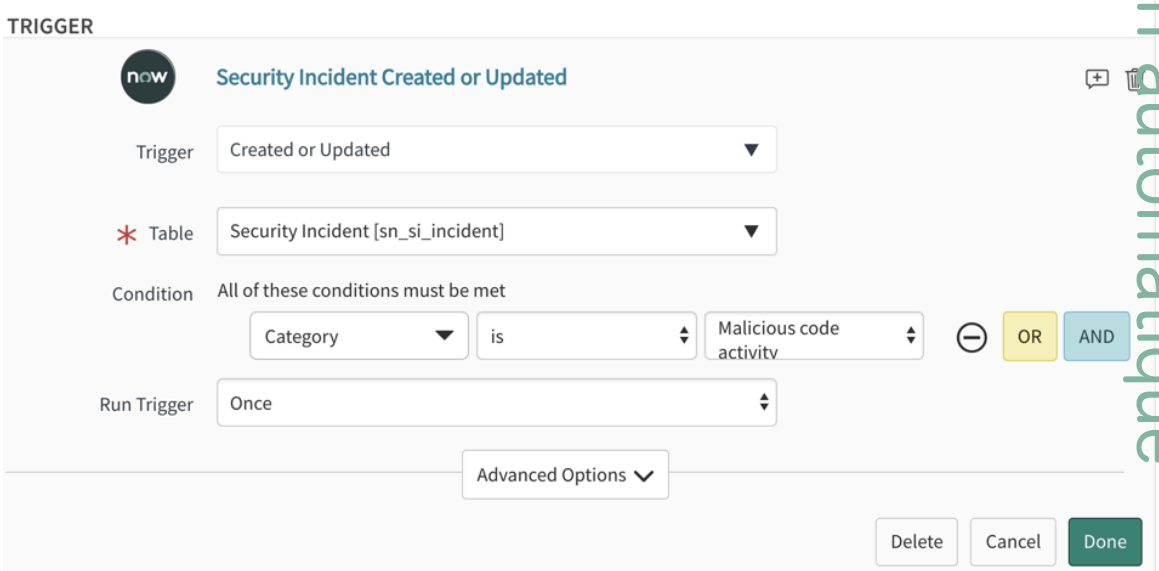
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez maintenant apporter des changements à votre flux, tels que la modification des conditions ou des actions de déclenchement, ou l'ajout et la suppression d'actions.



Le déclencheur et les étapes qui seront exécutées avec le flux s'affichent. Le panneau de droite affiche le flux de données. Cliquez sur une icône pour développer l'étape et afficher les détails.

4. Cliquez sur l'icône **Déclencher** .
   Dans la première étape, vous définissez ou définissez le déclencheur du flux. Spécifiez les conditions pour le déclencheur et la tâche à effectuer lorsque les conditions sont remplies.

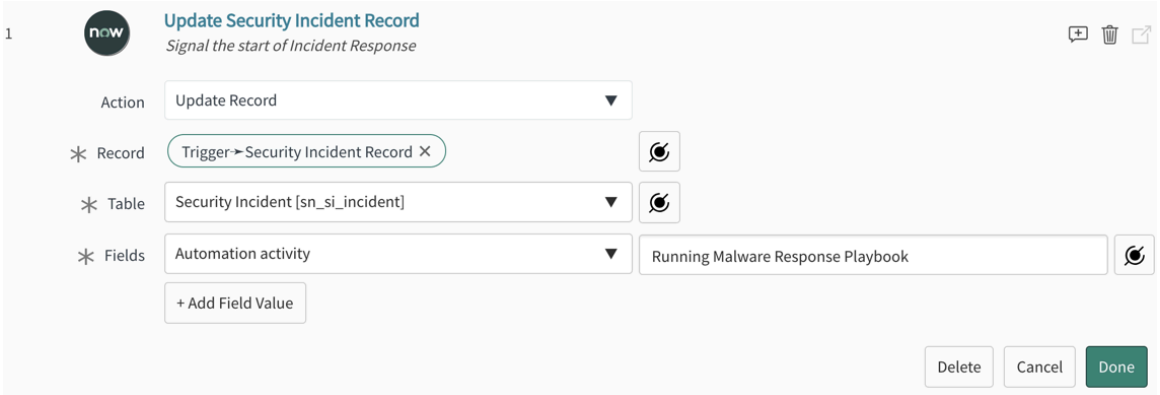


Lorsque la condition définie dans le flux (la catégorie est Activité de code malveillant) est remplie dans l'enregistrement d'incident, les tâches du flux d'hameçonnage automatisé commencent à s'exécuter séquentiellement. Vous pouvez modifier le déclencheur, ajouter des annotations, ajouter ou supprimer des conditions, etc.

5. La première étape du flux consiste à **mettre à jour l'enregistrement d'incident de sécurité**.

Traduction automatique

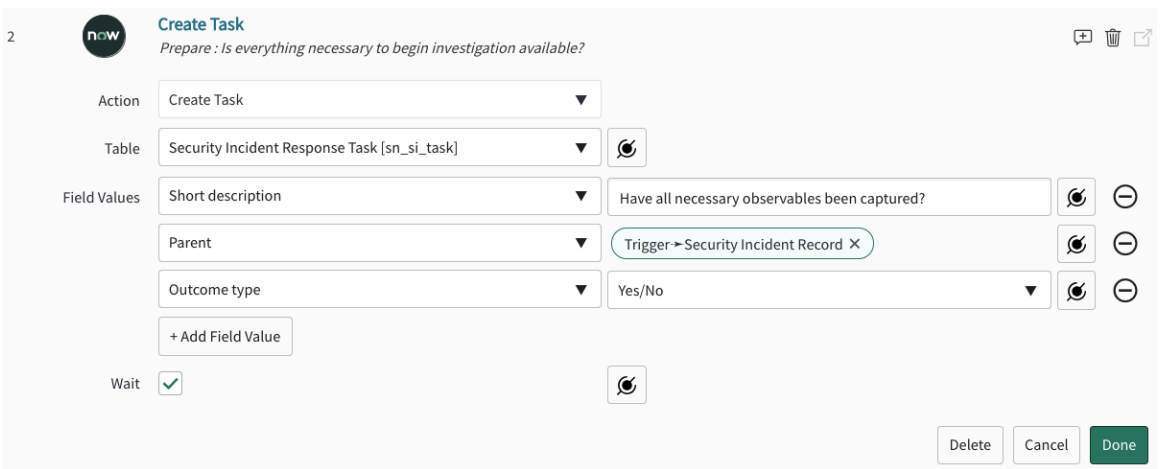
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cliquez sur le lien, puis sur l'icône d'annotation pour ajouter une note à l'analyste de sécurité indiquant qu'il y a eu une activité de code malveillant et que le flux automatisé du playbook de réponse aux programmes malveillants a commencé à s'exécuter.

6. Poursuivez avec l'étape 2 du flux et cliquez sur le lien **Créer une tâche** .

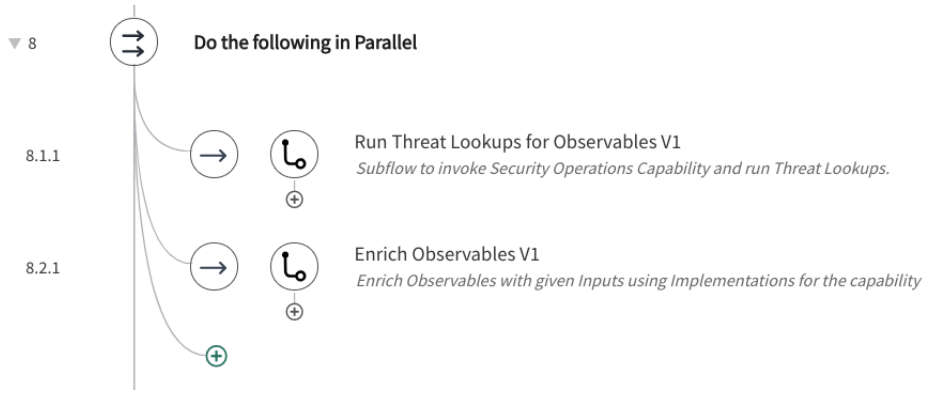
   Dans cette étape, une tâche de réponse automatisée est créée pour vérifier si tous les observables nécessaires ont été capturés et si l'enquête peut commencer.



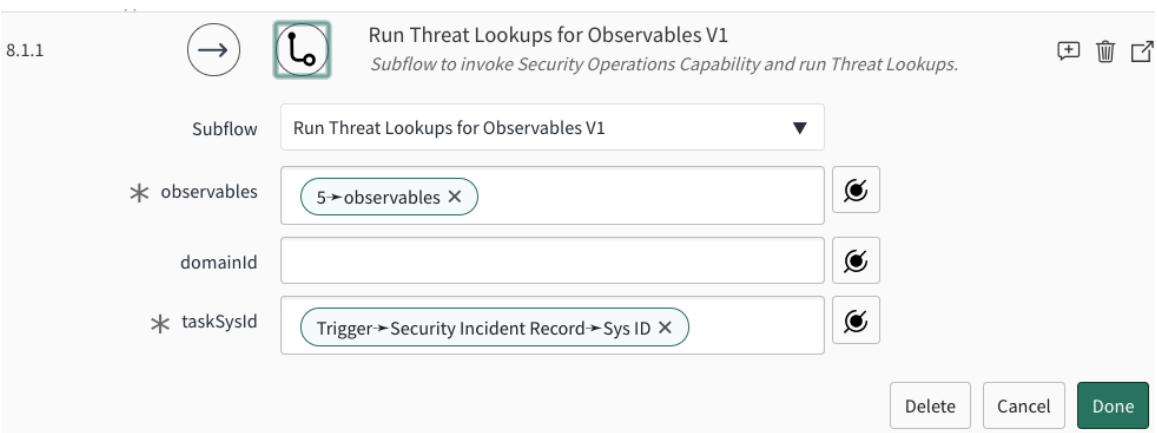
7. Si le type de résultat est **Non**, cela indique qu'aucun observable ou CI n'est disponible pour initier l'enquête. Mettez à jour l'enregistrement d'incident de sécurité pour indiquer que le playbook ne peut pas aller plus loin.
8. Si le type de résultat est **Oui**, le flux secondaire Définir la gravité de l'incident affecte automatiquement la gravité correcte à l'incident de sécurité.
9. À l'étape suivante, l'enregistrement d'incident de sécurité est mis à jour.
10. À l'étape suivante, tous les observables impliqués dans l'incident ou une catégorie sélectionnée sont collectés pour effectuer des actions automatisées supplémentaires dans les étapes suivantes du playbook.
11. À l'étape suivante, une tâche de réponse automatisée est créée.
    Cette tâche capture le début du processus d'obtention de la réputation de tous les observables et d'enrichissement avec des intégrations configurées.
12. À l'étape 8, deux flux secondaires sont appelés :
    - Exécuter des recherches de menace pour les observables : ce flux secondaire est utilisé pour obtenir la réputation de tous les observables à l'aide d'implémentations de la recherche de menace.
    - Enrichir les observables : ce flux secondaire permet d'enrichir les observables avec des implémentations configurées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Notez les icônes de cette tâche. L'icône Opérations parallèles indique que les deux tâches seront exécutées en parallèle et l'icône de flux secondaire indique que la tâche effectuée est un flux secondaire, comme indiqué ci-dessous :



Notez le nombre 5 dans le champ Observables. Cela indique que la recherche de menace sera exécutée sur les observables récupérés à l'étape 5. Ce flux secondaire appelle à son tour les workflows et actions existants.

13. L'étape suivante consiste à exécuter l'action Exécuter la recherche d'enregistrements.
Cette action est utilisée pour rechercher des enregistrements de contexte de workflow dans lesquels les workflows parents peuvent être l'un des suivants.

- Contexte de workflow abstrait de la recherche de menace
- Contexte de workflow abstrait d'enrichissement d'observable

14. À l'étape suivante, les résultats de réputation et d'enrichissement sont examinés tous les 8 enregistrements.

15. Passez en revue les étapes suivantes :

a. Mettre à jour l'enregistrement d'incident de sécurité : met à jour l'enregistrement d'incident de sécurité pour indiquer que les activités de recherche et d'enrichissement de la réputation ont été terminées.

b. Obtenir les observables à partir de la tâche : récupère tous les observables malveillants associés à l'incident de sécurité.

c. Créer une tâche : vérifie et confirme si les exécutions de triage automatisées ont réussi.

16. S'il existe des observables qui ont été marqués comme malveillants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Mettre à jour l'enregistrement d'incident de sécurité : publiez une note de travail indiquant qu'une menace a été détectée.

b. Créer une requête d'entrée à partir d'observables : si plus de dix observables ont été marqués comme malveillants, le flux secondaire Recherche de perception sur les observables (sur Splunk ou Carbon Black) est exécuté.

17. Si les observables ne sont pas marqués comme malveillants, le flux continue avec les étapes suivantes :

a. Mettre à jour l'enregistrement d'incident de sécurité : publier une note de travail indiquant qu'aucune menace n'a été détectée

b. Obtenir les observables à partir de la tâche : identifie tous les ID de hachage SHA256 de l'incident.

c. Rechercher des enregistrements d'observables : recherche des enregistrements qui répondent à ce critère.

18. Passez en revue les étapes suivantes :

a. Pour chaque observable malveillant, le workflow **Security Operations Palo Alto Networks - Get Wildfire Data Enrichment** est exécuté.

b. Examine les résultats de l'enquête pour voir s'ils sont satisfaisants.
Une tâche de réponse est créée pour vérifier si le programme malveillant suspecté est une attaque de rançongiciel. Si oui, le flux secondaire du Playbook de rançongiciel est exécuté.

c. À l'étape suivante, un e-mail est envoyé avec un résumé de l'analyse et une demande d'approbation pour lancer les procédures de confinement.

d. Une tâche est créée pour capturer les détails de l'approbation demandée.

e. L'étape suivante consiste à mettre à jour l'enregistrement d'incident de sécurité.
Publiez une note de travail informant l'analyste de sécurité que la demande d'approbation a été effectuée.

f. Demande l'approbation de maîtrise des attaques de programmes malveillants à votre gestionnaire SOC.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsqu'une demande d'approbation est générée par le flux, la note de travail est mise à jour avec le message suivant :

Une demande d'approbation a été faite pour <ID de tâche> la poursuite de l'imbrication. Pour approuver cette tâche, en tant que gestionnaire SOC, procédez manuellement comme suit :

- Accédez à la page Approbations des tâches.
- Vous verrez la liste des approbations. Cliquez sur l'<ID de la tâche> à approuver.
- Changez l'état sur **Approuver** et enregistrer l'<ID de tâche> mis à jour.

g. À l'étape suivante, l'enregistrement d'incident de sécurité est mis à jour pour suivre le statut d'approbation.

h. Ensuite, une tâche est créée pour lancer les procédures de confinement.

i. Le flux secondaire Exécuter la création de demandes de bloc pour les observables malveillants est exécuté et un enregistrement d'incident est créé avec une demande de reconstruction de l'appareil infecté et de ses actifs.

j. Ensuite, une tâche est créée pour exécuter la recherche de perceptions afin de confirmer si l'environnement est sécurisé.
La recherche d'observations est répétée jusqu'à ce qu'aucune observation ne soit trouvée.

k. Ensuite, une tâche est créée pour indiquer que l'enregistrement d'incident de sécurité est prêt à être examiné.

l. Enfin, l'enregistrement est mis à jour et déplacé vers l'étape Examen.

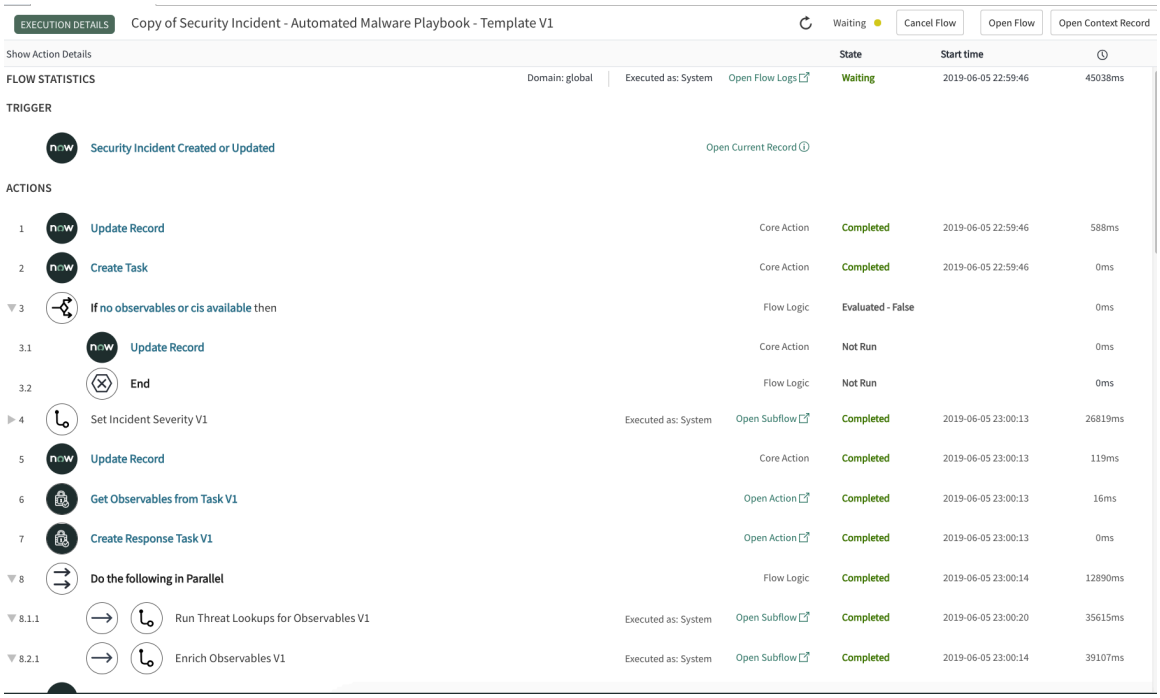
Que faire ensuite

Vous pouvez cliquer sur **Tester** pour simuler les actions dans le flux avant sa publication. Après avoir testé le flux, cliquez sur **Activer** pour activer le flux afin qu'il puisse être exécuté.

Cliquez sur **Exécutions** pour afficher les détails d'exécution du flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Playbook pour l'échec de la connexion manuelle

Lorsqu'un utilisateur effectue certaines tentatives de connexion infructueuses (en fonction de la configuration SIM), un incident de sécurité est créé.

Ces tentatives de connexion infructueuses peuvent être soit des faux positifs, soit des tentatives effectuées par des attaquants pour obtenir l'accès aux comptes de messagerie des utilisateurs. Dans de tels scénarios, le playbook manuel d'échec de connexion peut fournir des conseils et aider à optimiser l'enquête sur les incidents de sécurité liés aux échecs de connexion.

Prérequis

Rôle requis :

- sn_si.admin
- flow_designer

Spoke : installer le spoke Security Operations (sn_sec_spoke)

Principales options

Le playbook d'échec de connexion couvre les options suivantes pour enquêter sur les incidents de sécurité :

1. Vérifie si l'utilisateur affecté est un utilisateur actif/inactif
2. Filtres des éléments observables sur liste d'autorisation
3. Enrichit les observables
4. Effectue une recherche automatisée de menaces.
5. Envoie un e-mail automatisé à l'utilisateur pour confirmer l'échec de la tentative de connexion.
6. Affecte des tâches à l'analyste pour examiner l'accès des utilisateurs
7. Identifie les observables malveillants et bloque les adresses IP et URL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Réinitialise le mot de passe utilisateur.
9. Met à jour l'état de l'incident de sécurité
10. Affecte des tâches à un analyste de sécurité pour gérer l'examen post-incident.

Options requises

- Recherche de menace (total de virus, analyse hybride)
- Enrichissement des observables (Whois, ReverseWhois)
- Recherche de perception (Splunk, QRadar)
- Blocage des observables (CheckPoint, Palo Alto)

Pour plus d'informations, consultez le ServiceNow Store .

Expérience de l'analyste de sécurité

Pour comprendre comment résoudre les menaces de sécurité étape par étape, reportez-vous à la section Résoudre les menaces de sécurité avec le playbook.

Utilisation du playbook d'échec de connexion avec les options de Concepteur de flux

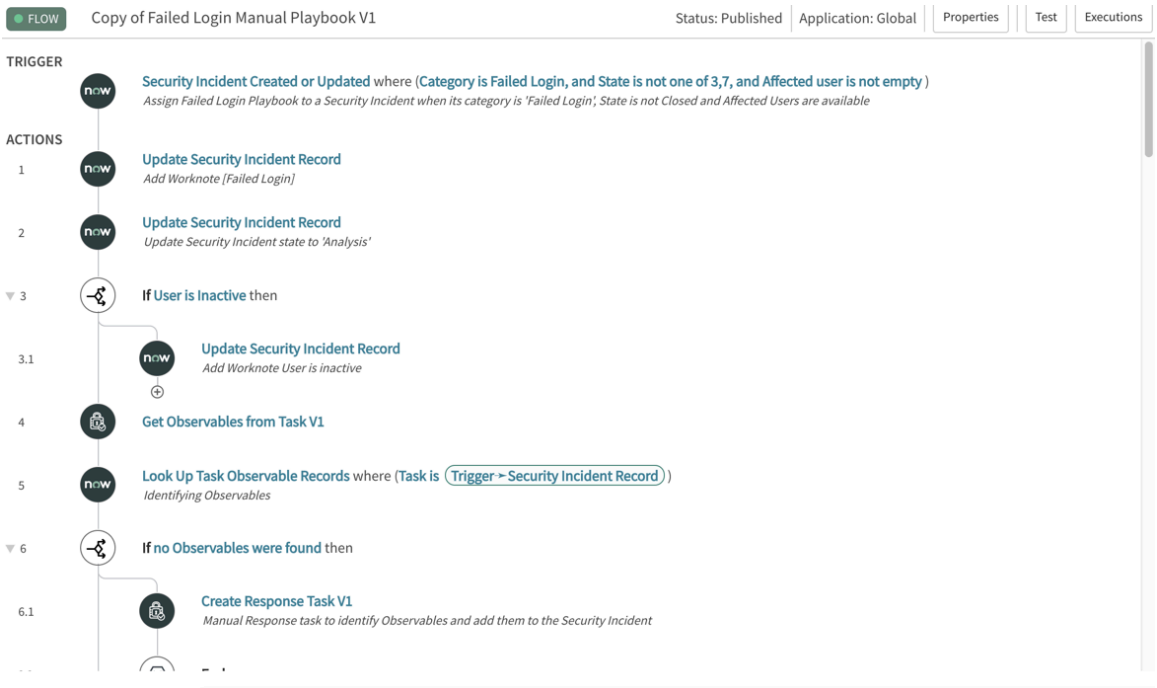
Commencer

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Concepteur de flux** > **Concepteur** et cliquez sur le playbook **Échec de la connexion** .
3. Faites une copie des flux suivants pour copier le Playbook d'échec de connexion et apporter les modifications nécessaires. (Il s'agit d'une étape facultative. Suivez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.
   - Échec de la connexion manuelle au Playbook V1
   - Échec de la connexion : analyser la réponse de l'utilisateur et mettre à jour la tâche de réponse V1
4. Apportez les modifications nécessaires en fonction de vos besoins. (Il s'agit d'une étape facultative. Suivez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.
5. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible avec le système de base.
   - Activez les flux copiés après avoir apporté des modifications en fonction de vos besoins.

L'image suivante montre une copie du playbook Échec de la connexion manuelle. Passez en revue les étapes ci-dessous pour mieux comprendre les différentes actions du playbook.

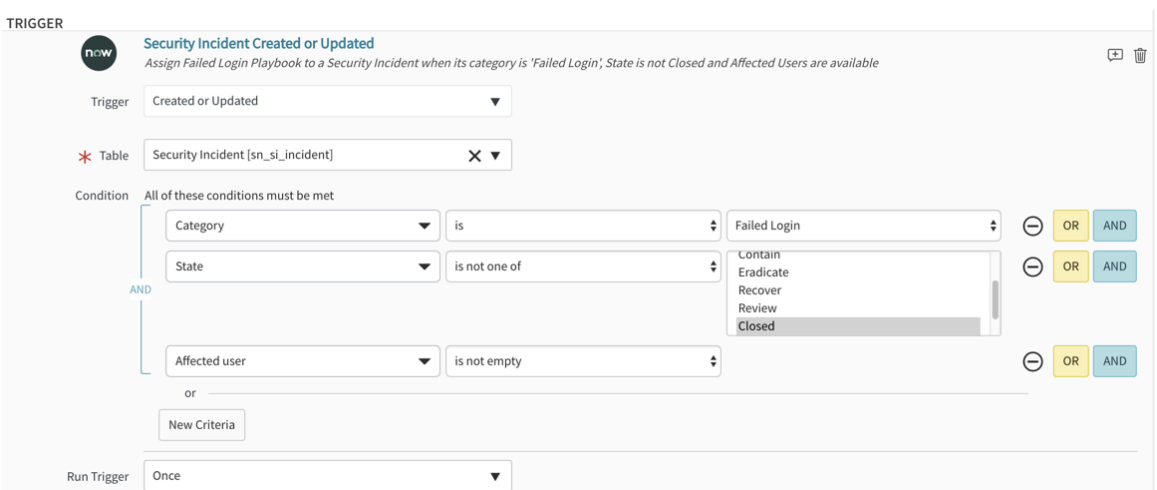
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :

- La catégorie est Échec de connexion
- A un ou plusieurs utilisateurs affectés
- L'incident de sécurité n'est ni fermé ni annulé

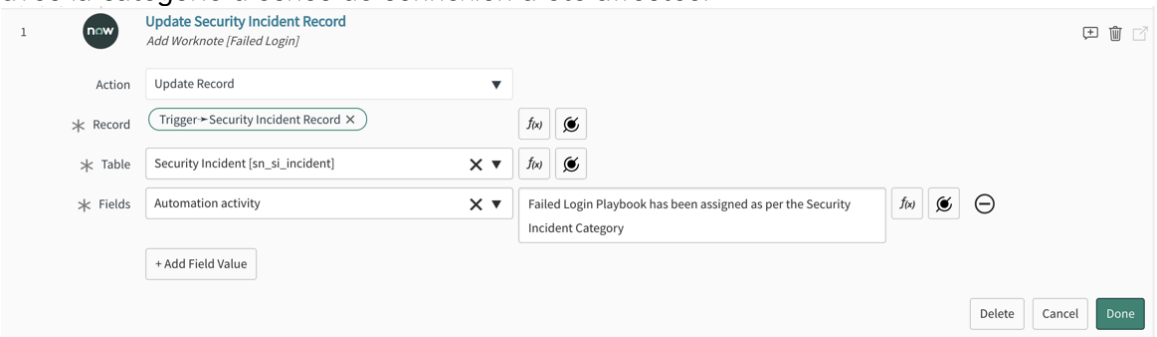


Les étapes suivantes vous guident à travers les actions, les tâches et les flux secondaires disponibles dans le playbook Échec de la connexion manuelle.

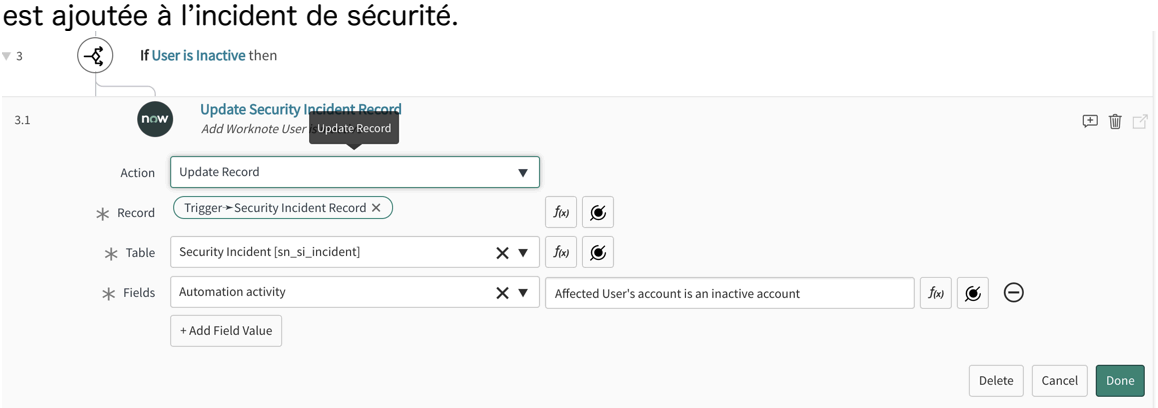
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Lorsque le playbook commence à s'exécuter, à l'étape 1, le playbook est automatiquement mis à jour avec une note de travail indiquant que l'incident de sécurité avec la catégorie d'échec de connexion a été affectée.



2. À l'étape 2, le playbook est mis à jour et passe à l'état Analyse.
3. À l'étape 3, le playbook vérifie si l'utilisateur affecté est un utilisateur actif ou inactif. Si l'utilisateur est inactif, une note de travail indiquant que le compte d'utilisateur est inactif est ajoutée à l'incident de sécurité.



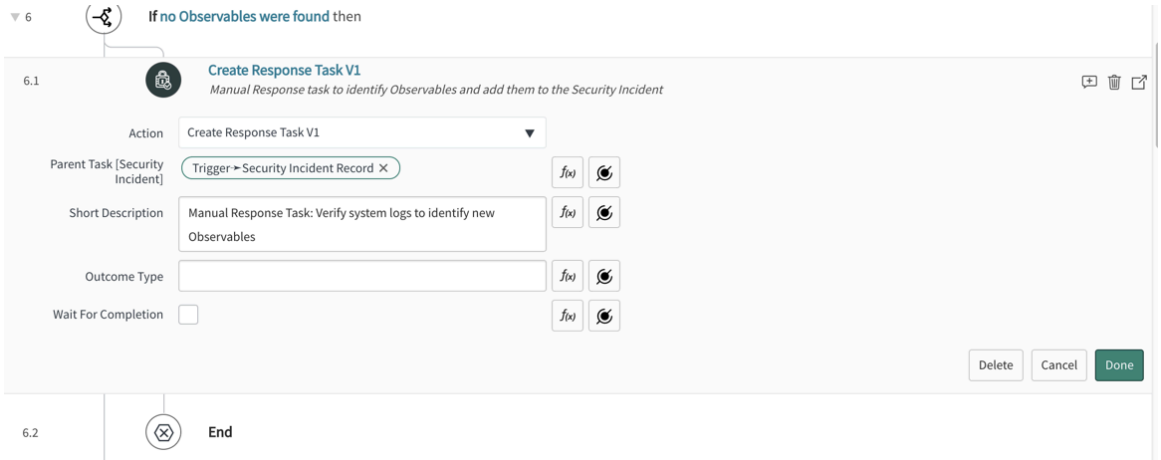
Remarque : À l'étape 3 du flux, le flux vérifie les utilisateurs inactifs dans la table `sn_si_incident` disponible dans ServiceNow. Cette étape est fournie à titre indicatif et doit être modifiée en fonction de votre environnement spécifique. Si vous souhaitez utiliser cette fonctionnalité, nous vous recommandons de configurer une intégration Active Directory dans votre environnement. Vous pouvez vérifier auprès de votre intégration Active Directory l'état de l'utilisateur et, en fonction de la réponse, vous pouvez concevoir les prochaines étapes de votre playbook.

Si vous n'avez pas d'intégration Active Directory, remplacez cette étape par une tâche manuelle pour que l'analyste de sécurité travaille avec l'équipe informatique pour bloquer l'utilisateur et poursuivre avec le reste des étapes du playbook.

4. À l'étape 4, les observables de l'incident de sécurité sont récupérés.
5. À l'étape 5, les observables sont identifiés.
6. Si aucun observable n'est trouvé, une tâche de réponse manuelle est créée à l'étape 6 et le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Si des observables sont trouvés à l'étape 7, les observables qui ne sont pas sur la liste d'autorisation sont identifiés.
8. Si au moins un des observables n'est pas sur liste d'autorisation, les étapes suivantes sont exécutées :
   a. Les étapes 8.1 et 8.2 sont exécutées. Les observables sont récupérés et une tâche de réponse automatisée est lancée.



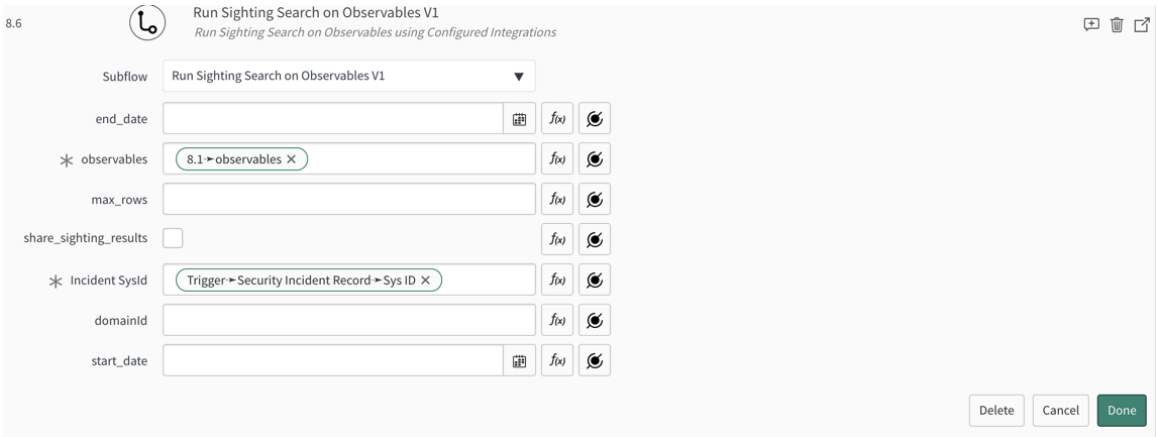
   b. Une fois la tâche automatisée créée, l'étape 8.3 (8.3.1.1 et 8.3.2.1) est exécutée et les intégrations Enrichir les observables et Recherche de menace sont exécutées. Notez qu'il s'agit de flux secondaires qui ont été inclus dans le playbook.



   c. À l'étape 8.4, une fois les intégrations terminées, l'enregistrement d'incident de sécurité est mis à jour.
   d. À l'étape 8.5, une nouvelle tâche de réponse est créée pour indiquer la prochaine tâche automatisée qui aura lieu.
   e. À l'étape 8.6, l'intégration de la recherche de perception sera exécutée sur les observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



f. Une fois le flux secondaire de recherche de perception terminé, à l'étape 8.7, l'incident de sécurité est mis à jour.

g. À l'étape 8.8, les observables sont vérifiés pour voir s'ils sont malveillants.

h. Si les observables ne sont pas malveillants et si le compte utilisateur est actif, un e-mail automatisé est envoyé à l'utilisateur pour confirmer à nouveau les tentatives de connexion infructueuses. Une tâche de réponse manuelle est créée pour identifier les observables et les ajouter à l'incident de sécurité. Le playbook se termine alors à cette étape.

i. Si les observables sont malveillants, trois tâches de réponse sont créées :

  i. Un e-mail automatisé est envoyé à l'utilisateur pour confirmer **(Oui ou Non)** les tentatives de connexion infructueuses. Si l'utilisateur répond Oui :

    1. L'état de l'incident de sécurité est mis à jour et prend la valeur **Maîtriser**.

    2. Un e-mail automatisé est envoyé à l'utilisateur pour réinitialiser le mot de passe.

    3. Le flux secondaire Réinitialiser le mot de passe est lancé et un e-mail est envoyé à l'utilisateur lorsque la tâche est terminée.

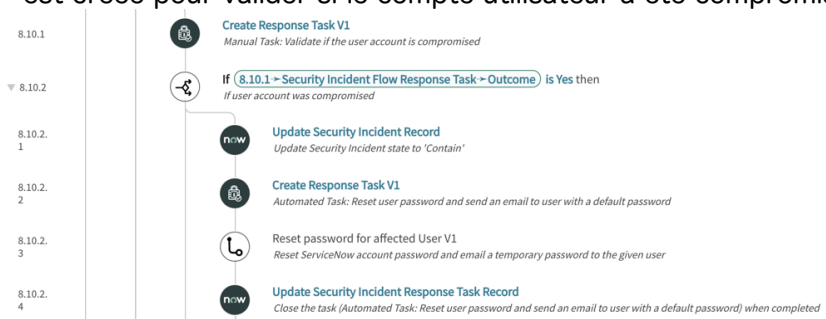
> **Remarque :** L'étape Réinitialiser le mot de passe est fournie à titre indicatif. Les étapes du flux réinitialisent le mot de passe du compte de l'utilisateur dans le système ServiceNow. Mais le processus de réinitialisation du mot de passe peut être différent selon votre environnement. Vous pouvez vérifier auprès de votre intégration Active Directory pour réinitialiser automatiquement le mot de passe des utilisateurs. Si vous n'avez pas d'intégration Active Directory, remplacez cette étape par une tâche manuelle pour que l'analyste de sécurité travaille avec l'équipe informatique respective pour réinitialiser le mot de passe des utilisateurs et poursuivre avec le reste des étapes du playbook, une fois la tâche respective terminée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ii. Si l'utilisateur répond Non, un e-mail automatisé lui est envoyé pour confirmer à nouveau sa réponse. L'analyste de sécurité doit prendre manuellement les mesures appropriées.

iii. Si l'utilisateur ne répond pas à l'e-mail automatisé, l'analyste de sécurité doit mettre à jour manuellement l'incident de sécurité et fournir une réponse. Une tâche manuelle est créée pour valider si le compte utilisateur a été compromis.



9. À l'étape 8.10.3, l'état de l'incident de sécurité est mis à jour.
10. À l'étape 8.10.4, une tâche automatisée est créée pour vérifier si l'implémentation de l'aptitude Créer des demandes de bloc pour les adresses IP et URL malveillantes est disponible. Si l'implémentation de l'aptitude est disponible, le flux secondaire Créer des demandes de bloc est exécuté. Si cette option n'est pas disponible, l'incident de sécurité est mis à jour et une note de travail est publiée pour indiquer que l'implémentation de l'aptitude n'est pas disponible.
11. À l'étape 9, l'incident de sécurité est mis à jour et l'état est défini sur **Examen**.
12. À l'étape 10, une tâche de réponse est créée pour que l'utilisateur termine l'examen post-incident avant de fermer la tâche.

Playbook pour l'automatisation des incidents de sécurité enfants

Les incidents de sécurité en double sont classés comme des incidents de sécurité enfants et sont déployés sur les incidents de sécurité parents.

Le playbook d'automatisation des incidents de sécurité enfants permet de réduire le temps nécessaire pour examiner et fermer les incidents de sécurité en double. Ce playbook déploie automatiquement des artefacts uniques spécifiques de l'incident de sécurité enfant (observables, utilisateurs affectés, CI) sur l'incident de sécurité parent.

Prérequis

Rôle requis :

- sn_si.admin
- flow_designer

Spoke : installer le spoke Security Operations (sn_sec_spoke)

Principales options

Le playbook d'automatisation enfant couvre les options suivantes :

1. Déplace l'incident de sécurité vers l'étape **d'analyse** .
2. Élimine les doublons et ajoute (déploie) les utilisateurs et CI affectés à l'incident de sécurité parent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Ajoute des observables de l'incident enfant à l'incident de sécurité parent.
4. Ferme ou annule l'incident de sécurité enfant lorsque l'incident de sécurité parent est fermé.

Options requises

Pour plus d'informations, consultez le ServiceNow Store .

Expérience de l'analyste de sécurité

Pour comprendre comment résoudre les menaces de sécurité étape par étape, reportez-vous à la section Résoudre les menaces de sécurité avec le playbook.

Meilleure compréhension du playbook d'automatisation des incidents de sécurité enfants avec les options de Concepteur de flux

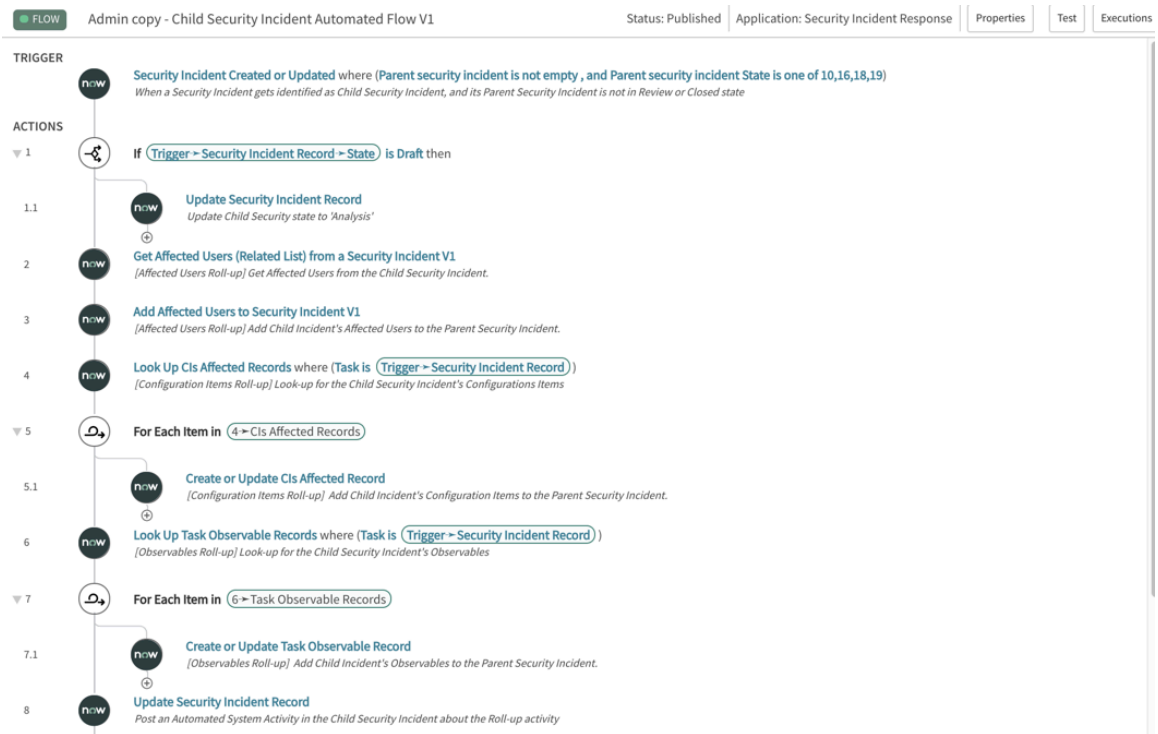
Commencer

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Concepteur de flux** > **Concepteur** et cliquez sur le playbook Échec de la connexion.
3. Faites une copie du playbook d'automatisation des incidents de sécurité enfants et apportez les modifications nécessaires. (Il s'agit d'une étape facultative. Suivez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.
4. Apportez les modifications nécessaires en fonction de vos besoins. (Il s'agit d'une étape facultative. Suivez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.
5. Activez le playbook.
   - Activez le flux principal pour utiliser le playbook disponible avec le système de base.
   - Activez le flux copié après avoir apporté des modifications en fonction de vos besoins.

L'image suivante montre une copie du playbook d'automatisation des incidents de sécurité enfants. Passez en revue les étapes ci-dessous pour mieux comprendre les différentes actions du playbook.

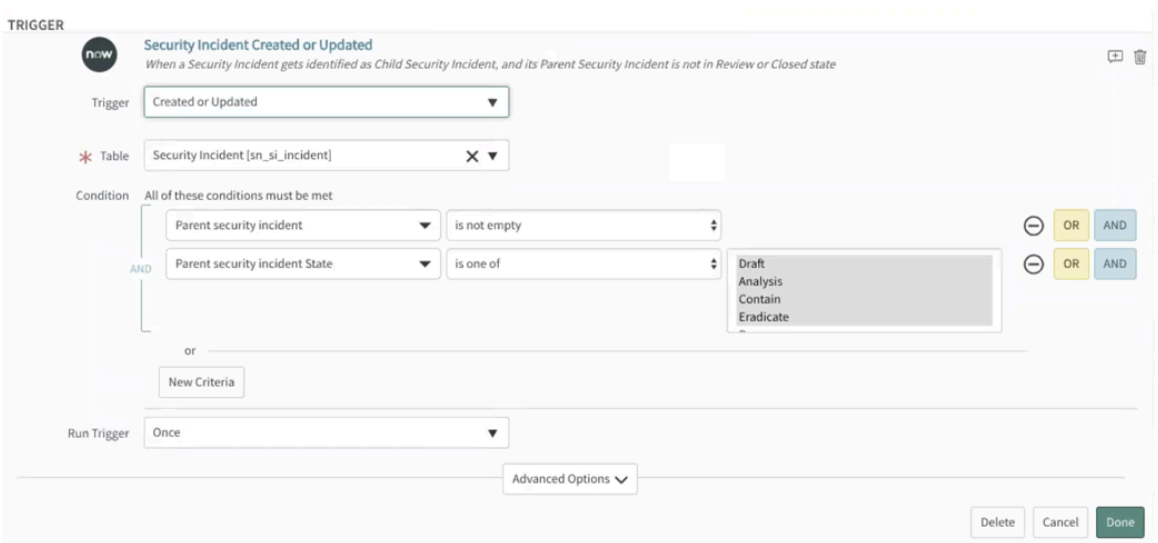
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Ce playbook est déclenché lorsque :

- Le champ d'incident de sécurité parent n'est pas vide.
- L'incident de sécurité parent est à l'état Brouillon, Analyse, Contenir ou Éradiquer.

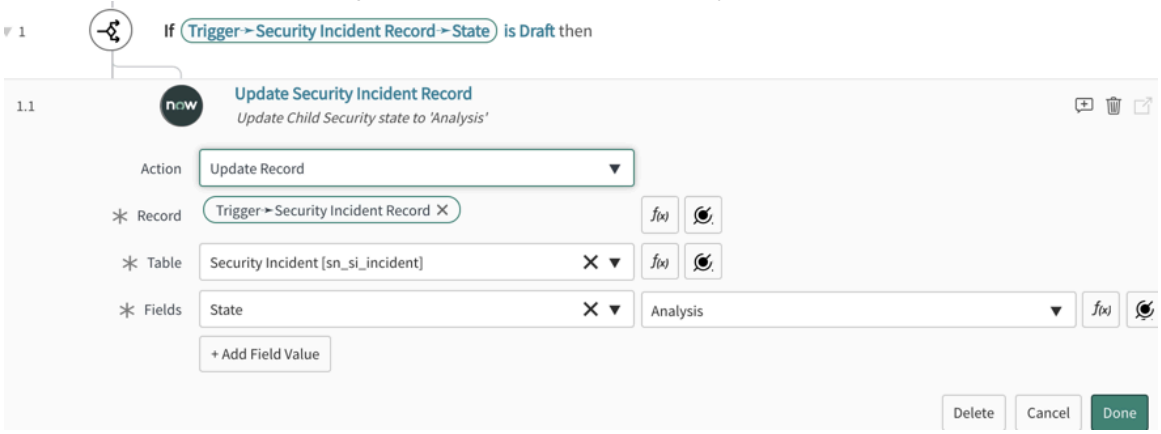


Les étapes suivantes vous guident à travers les actions et les tâches disponibles dans le playbook d'automatisation des incidents de sécurité enfants.

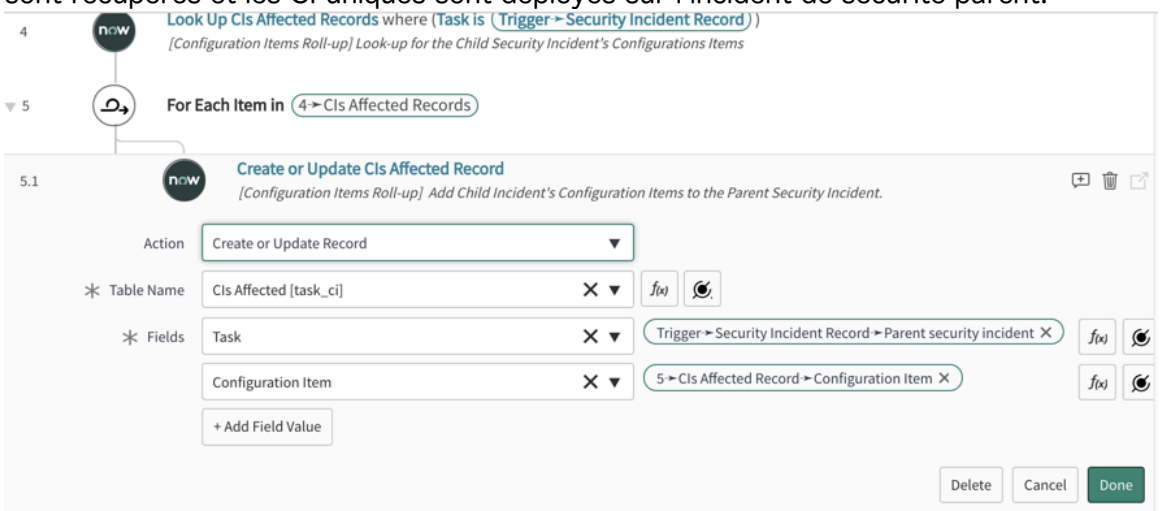
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

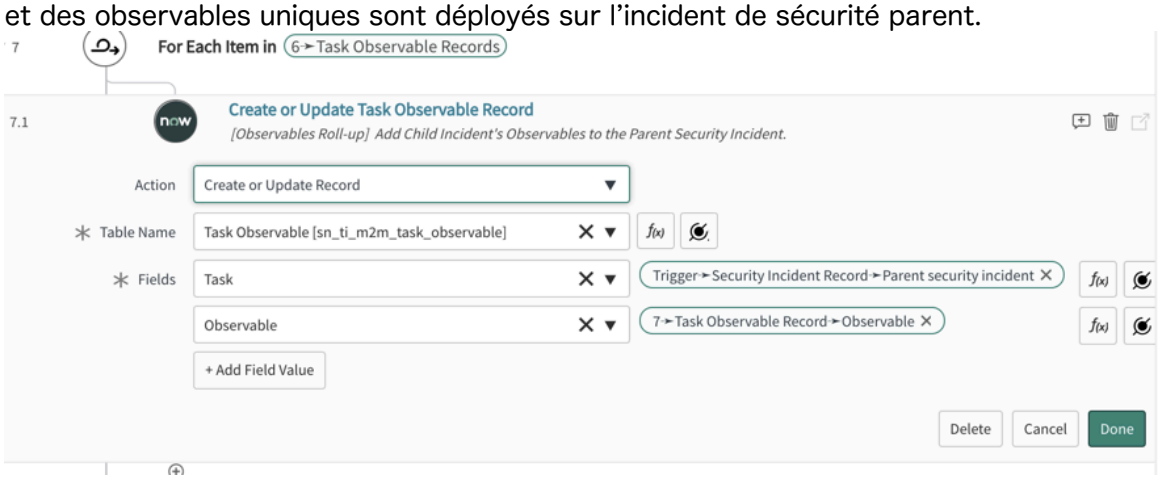
1. Lorsque le playbook commence à s'exécuter, à l'étape 1, si l'incident de sécurité est à l'état Brouillon, il est mis à jour et défini sur l'état Analyse.



2. Aux étapes 2 et 3, les utilisateurs affectés par l'incident de sécurité sont récupérés et déployés sur l'incident de sécurité parent. Tous les utilisateurs en double sont éliminés.
3. Aux étapes 4 et 5, les éléments de configuration associés à l'incident de sécurité enfant sont récupérés et les CI uniques sont déployés sur l'incident de sécurité parent.



4. Aux étapes 6 et 7, les observables associés à l'incident de sécurité enfant sont récupérés et des observables uniques sont déployés sur l'incident de sécurité parent.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Aux étapes 8 et 9, des notes de travail automatisées sont publiées pour les incidents de sécurité parent et enfant, indiquant que les utilisateurs, les éléments de configuration et les observables affectés ont été déployés de l'incident de sécurité enfant vers l'incident de sécurité parent.

Playbook pour Office 365 : fichier malveillant détecté

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les fichiers malveillants détectés dans Office 365.

Lorsque des fichiers malveillants sont détectés dans Office 365, vous pouvez utiliser le playbook 365 : fichier malveillant détecté dans Concepteur de flux pour obtenir des conseils et optimiser l'examen de ces fichiers malveillants.

Configurer le playbook Office Fichier malveillant détecté

Suivez les étapes suivantes pour configurer le playbook Office Malicous File Detected (Fichier malicous détecté).

Avant de commencer

Rôle requis :

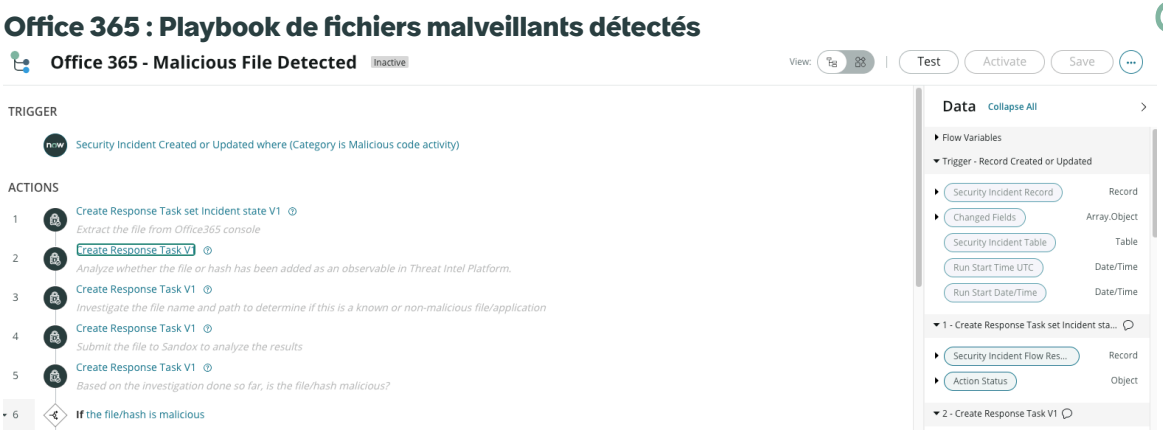
- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **Office 365 - Fichier malveillant détecté** .
3. **Facultatif :** Vous pouvez créer une copie du flux de playbook Office 365 - Fichier malveillant détecté et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.



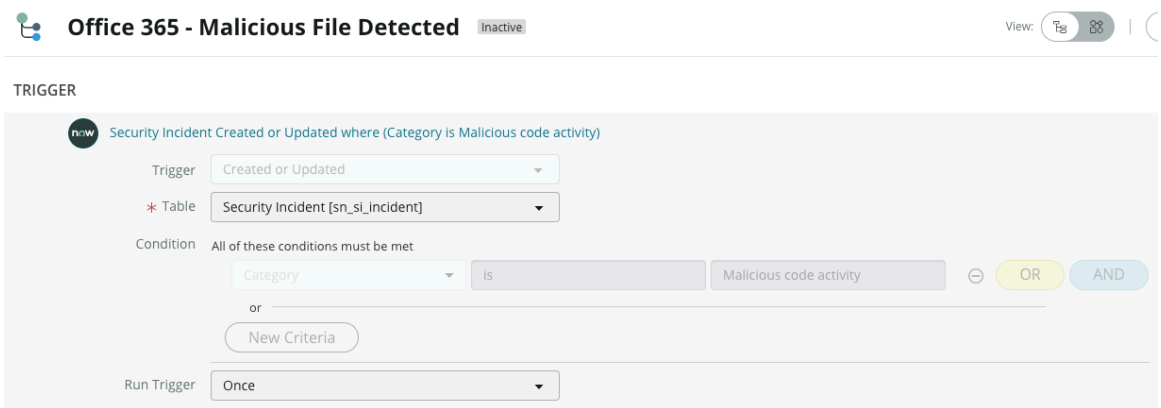
4. Activez les playbooks.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez le flux principal pour utiliser le playbook disponible dans le système de base.
- Activez les flux copiés après avoir apporté les changements requis.

5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Activité de code malveillant**.



Utiliser le playbook Fichier malveillant détecté Office 365

Utilisez ce playbook pour enquêter sur les fichiers malveillants détectés dans Office 365. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Fichier malveillant détecté Office 365.

Avant de commencer

Rôle requis :

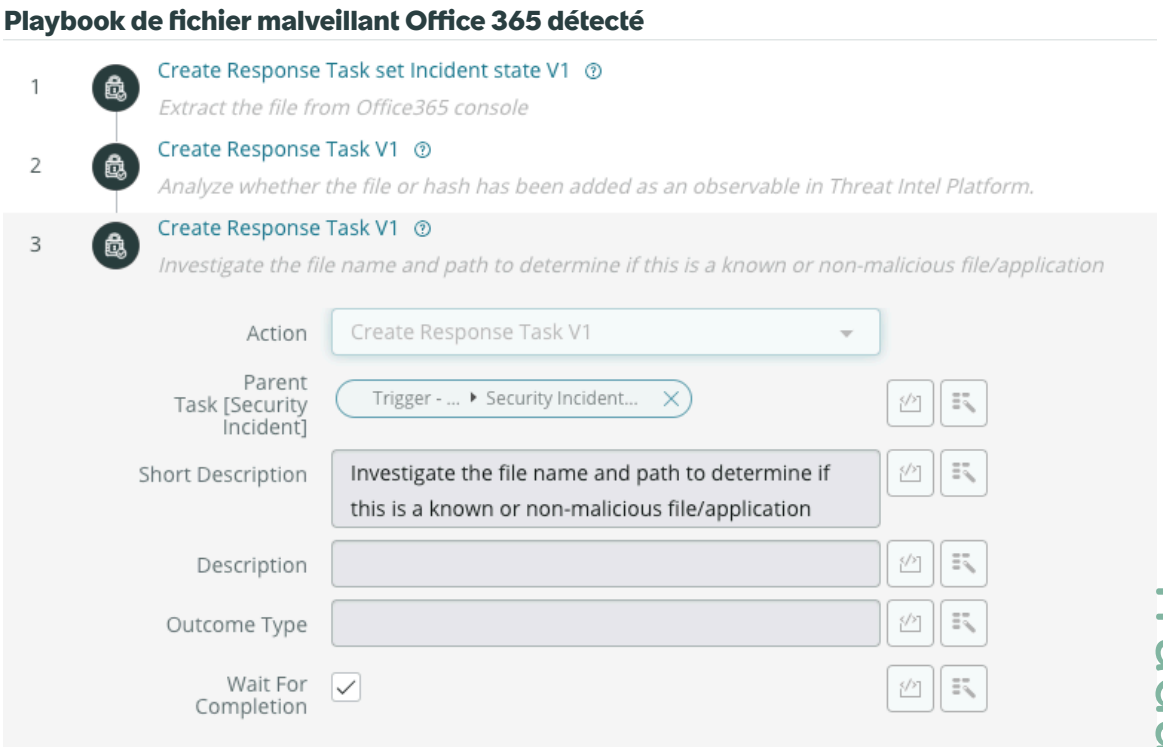
- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez extraire le fichier malveillant de la console Office 365.
2. Dans l'action 2, vous devez analyser si le fichier ou le hachage a été ajouté en tant qu'observable dans la plateforme Threat Intel.
3. Dans l'action 3, vous devez examiner le nom et le chemin d'accès du fichier pour déterminer s'il s'agit d'un fichier/d'une application connue ou non malveillante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans l'action 4, vous devez soumettre le fichier à Sandbox pour analyser les résultats.
5. Dans l'action 5, sur la base de l'enquête effectuée jusqu'à présent, vous devez vérifier si le fichier ou le hachage est malveillant ou non.
   Si le fichier ou le hachage n'est pas malveillant, une tâche de réponse manuelle est créée dans l'action 5 et le flux s'arrête.
6. Dans l'action 6, si le fichier ou le hachage est malveillant, les actions 7 et 8 sont exécutées.
7. Dans l'action 7, vous devez contacter l'utilisateur final pour obtenir une justification commerciale valable expliquant pourquoi il a un fichier malveillant sur l'appareil.
   Si le fichier ou le hachage est malveillant, vous pouvez utiliser le modèle d'e-mail préexistant dans le playbook pour envoyer un e-mail à l'utilisateur final demandant des clarifications.
8. Dans l'action 8, vous devez vérifier si l'utilisateur final a fourni une justification commerciale valable ou non.
   Si l'utilisateur final a fourni une justification commerciale valide, une tâche de réponse manuelle est créée dans l'action 5 et le flux s'arrête.
9. Dans l'action 9, si l'utilisateur n'a pas fourni de justification commerciale valide, les actions 10, 11 et 12 sont exécutées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Dans l'action 10, étant donné qu'il n'y a pas de justification commerciale valable, vous pouvez transmettre le fichier ou le hachage malveillant à l'équipe Threat Intelligence pour examen.
11. Dans l'action 11, vous devez exécuter le script Malware bytes scanner pour vérifier si le fichier ou le hachage est malveillant.
12. Dans l'action 12, vous devez effectuer une analyse médico-légale pour vérifier si le fichier ou le hachage est malveillant.
13. Dans l'action 13, une tâche de réponse est créée pour que l'utilisateur termine l'examen post-incident avant de fermer la tâche.

Playbook pour la détection de répétition

Ce playbook vous aide à déterminer si la réponse à un incident a été fournie sur un rapport d'hameçonnage exact ou similaire dans le passé et fonctionne automatiquement sur le nouveau rapport de la même manière.

Le playbook de répétition de détection vérifie si l'incident d'hameçonnage nouvellement signalé ressemble à un incident passé. Lorsque la détection répétée est identifiée, l'incident de sécurité correspondant et les détails de résolution sont fournis à l'analyste, qui peut les utiliser sur l'incident nouvellement signalé, ce qui entraîne une correction rapide de l'incident de sécurité.

Configurer le playbook de détection de répétition

Procédez comme suit pour configurer le playbook de détection de répétition.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*). Vous pouvez modifier les propriétés système suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *sn_sec_spoke.similarphish.earlyterminationscore*
- *sn_sec_spoke.similarphish.lookbackdays*
- *sn_sec_spoke.similarphish.maxComparisonSize*
- *sn_sec_spoke.similarphish.minmatchscore*

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook de **détection des répétitions** .
3. **Facultatif :** Vous pouvez créer une copie du flux du playbook de détection de répétition et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

   Playbook de détection de répétition

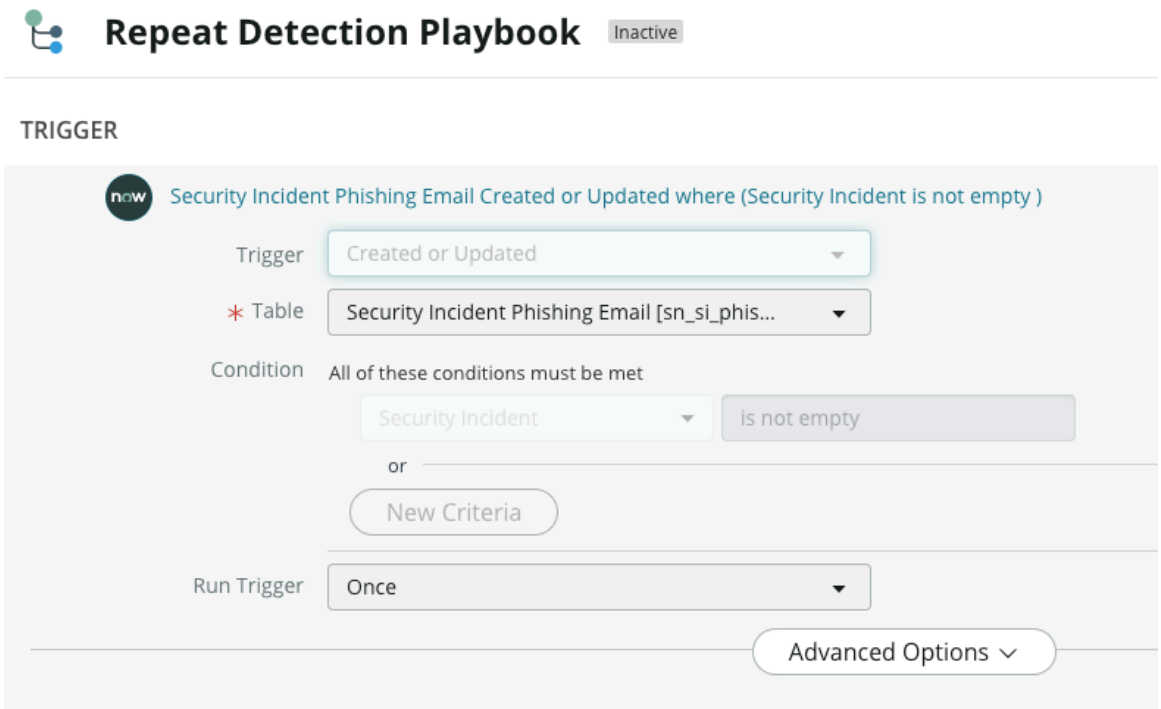
   

4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché lorsque **l'incident de sécurité n'est pas vide**.



Utiliser le playbook de détection de répétition

Utilisez ce playbook pour vérifier si la réponse à un incident a été fournie sur un rapport d'hameçonnage exact ou similaire dans le passé et fonctionne automatiquement sur le nouveau rapport de la même manière. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook de détection des répétitions.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

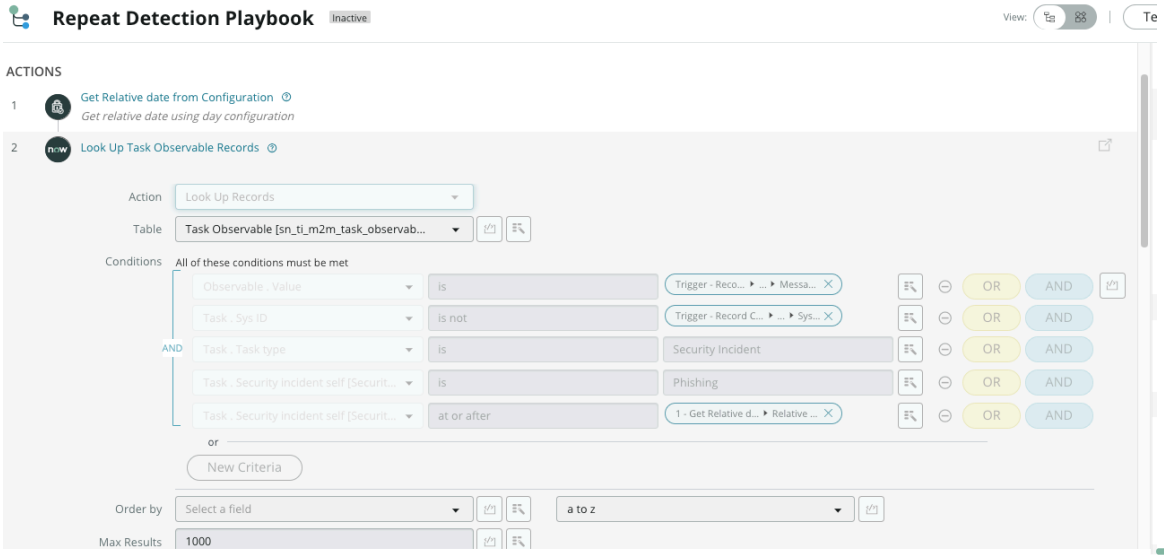
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, le playbook récupère la date relative de l'incident de sécurité à l'aide de la configuration du jour.
2. Dans l'action 2, le playbook recherche les enregistrements d'observables de tâche sur la table `sn_ti_m2m_task_observable` qui correspondent à l'incident en fonction de l'ID du message.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

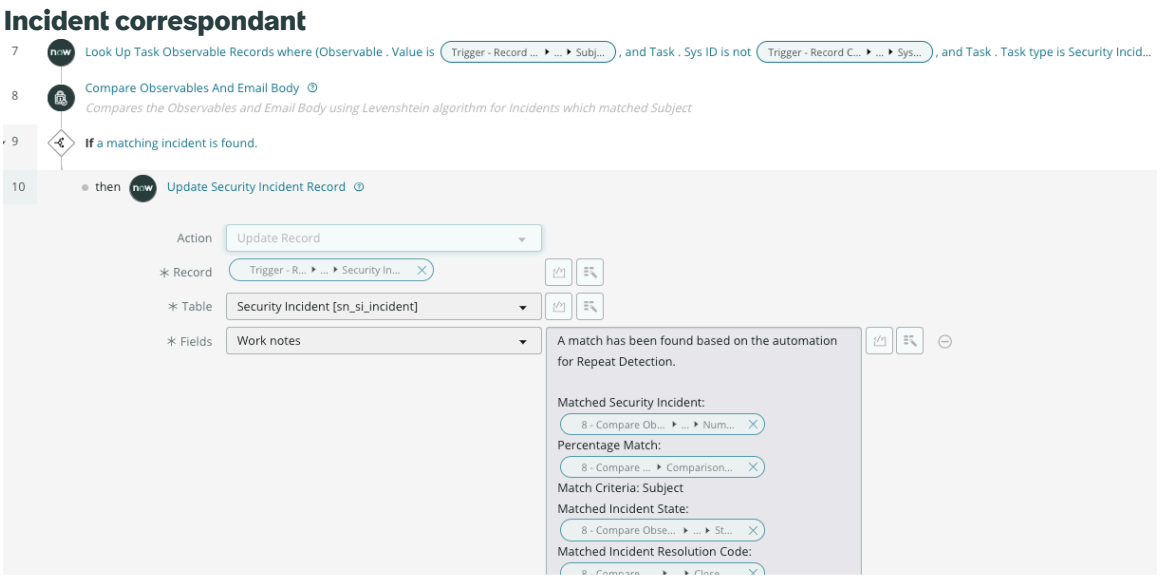
Playbook de détection de répétition



3. Dans l’action 3, le playbook compare les observables de tâche et le corps de l’e-mail à l’aide de l’algorithme de Levenshtein pour les incidents qui correspondaient à l’ID du message.
4. Dans l’action 4, sur la base de l’enquête effectuée jusqu’à présent, le playbook vérifie si l’incident correspondant est trouvé en fonction de l’ID du message ou non.
   Dans l’action 5, si l’incident correspondant est trouvé, le playbook met automatiquement à jour la note de travail indiquant qu’une correspondance a été trouvée en fonction de l’automatisation de la détection de répétition. Dans l’action 6, le flux s’arrête.
5. Si l’incident correspondant est introuvable, dans l’action 7, le playbook recherche les enregistrements d’observables de tâche sur la table `sn_ti_m2m_task_observable` qui correspondent à l’incident en fonction de l’objet.
6. Dans l’action 8, le playbook compare les observables de tâche et le corps de l’e-mail à l’aide de l’algorithme de Levenshtein pour les incidents qui correspondaient à l’objet.
7. Dans l’action 9, le playbook vérifie si l’incident correspondant est trouvé ou non.
   Dans l’action 10, si l’incident correspondant est trouvé, le playbook met automatiquement à jour la note de travail indiquant qu’une correspondance a été trouvée en fonction de l’automatisation de la détection de répétition. Dans l’action 11, le flux s’arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Dans l'action 12, le playbook recherche les enregistrements d'observables de tâche dans les *sn_ti_m2m_task_observable* de table qui correspondent à l'incident en fonction de l'adresse.
9. Dans l'action 13, le playbook compare les observables de tâche et le corps de l'e-mail à l'aide de l'algorithme de Levenshtein pour les incidents qui correspondaient à l'adresse.
10. Dans l'action 14, le playbook vérifie si l'incident correspondant est trouvé en fonction de l'adresse ou non. Dans l'action 15, si l'incident correspondant est trouvé, le playbook met automatiquement à jour la note de travail indiquant qu'une correspondance a été trouvée en fonction de l'automatisation de la détection de répétition. Dans l'action 16, le flux s'arrête.

Playbook pour les e-mails falsifiés (utilisant le même nom d'affichage)

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les e-mails falsifiés, qui se déclenchent lorsque des noms usurpés d'e-mails sont envoyés aux employés de l'organisation.

Configurer le playbook d'e-mails falsifiés

Suivez les étapes suivantes pour configurer le playbook des e-mails usurpés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

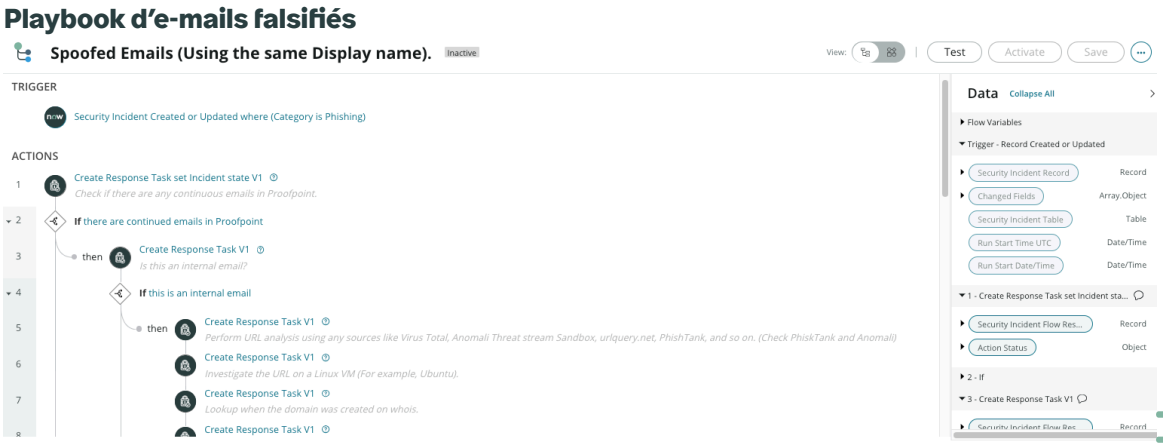
Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **E-mails falsifiés (utilisant le même nom d'affichage).**
3. **Facultatif :** Vous pouvez créer une copie du flux du playbook de détection de répétition et apporter les modifications nécessaires.

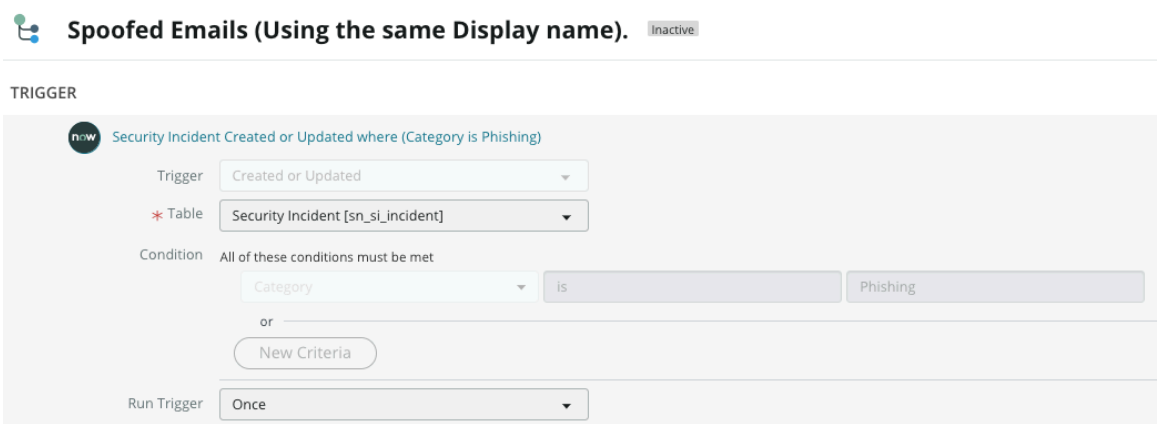
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour créer une copie du flux du playbook, cliquez sur l'icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Hameçonnage**.



Utiliser le playbook E-mails falsifiés (utilisant le même nom d'affichage)

Utilisez ce manuel pour enquêter sur les e-mails falsifiés, qui se déclenchent lorsque des noms usurpés pour des e-mails sont envoyés aux employés de l'organisation. Les étapes suivantes vous donnent un aperçu des actions, des tâches et des flux secondaires disponibles dans le playbook Adresses e-mails falsifiées (utilisant le même nom d'affichage).

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

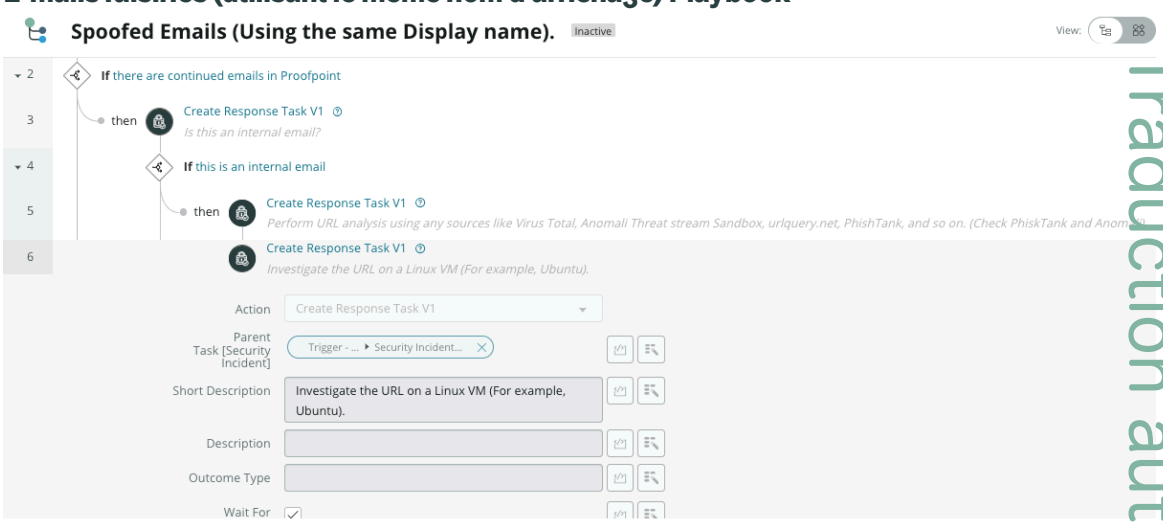
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez vérifier s'il existe des e-mails usurpés continus dans Proofpoint.
2. Dans l'action 2, s'il y a des e-mails continus dans Proofpoint, vérifiez s'il s'agit d'un e-mail usurpé interne ou non.
3. Dans l'action 3, s'il s'agit d'un e-mail usurpé en interne, effectuez les actions suivantes :

   a. Dans l'action 5, vous devez effectuer une analyse d'URL à l'aide de sources telles que Virus Total, Anomali Threat stream Sandbox, urlquery.net, PhishTank (par exemple, vérifiez PhiskTank et Anomali).

   b. Dans l'action 6, vous devez examiner l'URL sur une machine virtuelle Linux (par exemple, Ubuntu).

E-mails falsifiés (utilisant le même nom d'affichage) Playbook



   c. Dans l'action 7, vous devez rechercher la date de création du domaine sur WHOIS.
   Recherchez les domaines récemment enregistrés (au cours de la semaine dernière) qui sont suspects et présentent une forte probabilité d'attaques de phishing.

   d. Dans l'action 8, sur la base de l'enquête effectuée jusqu'à présent, vous devez vérifier si cet e-mail contient une pièce jointe ou un lien malveillant.
   Si cet e-mail ne contient pas de pièce jointe ou de lien malveillant, le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Dans l'action 9, si l'e-mail contient des liens ou des pièces jointes malveillants, effectuez les actions suivantes.

i. Dans l'action 10, vous devez contacter l'utilisateur concerné pour vérifier si les informations d'identification sont compromises. Vous pouvez utiliser le modèle d'e-mail fourni pour contacter l'utilisateur concerné.

ii. Dans l'action 11, vous devez vérifier si les informations d'identification sont compromises en fonction de la réponse par e-mail. Si les informations d'identification n'ont pas été compromises, le flux s'arrête.

1. Dans l'action 12, si les informations d'identification sont compromises, dans l'action 13, vous devez vérifier si des utilisateurs supplémentaires sont impactés. Si aucun utilisateur supplémentaire n'est impacté, le flux s'arrête.

2. Dans l'action 14, si des utilisateurs supplémentaires sont impactés, effectuez les actions suivantes :

a. Dans l'action 15, vous devez rechercher et supprimer des e-mails à l'aide de Microsoft Exchange Online.

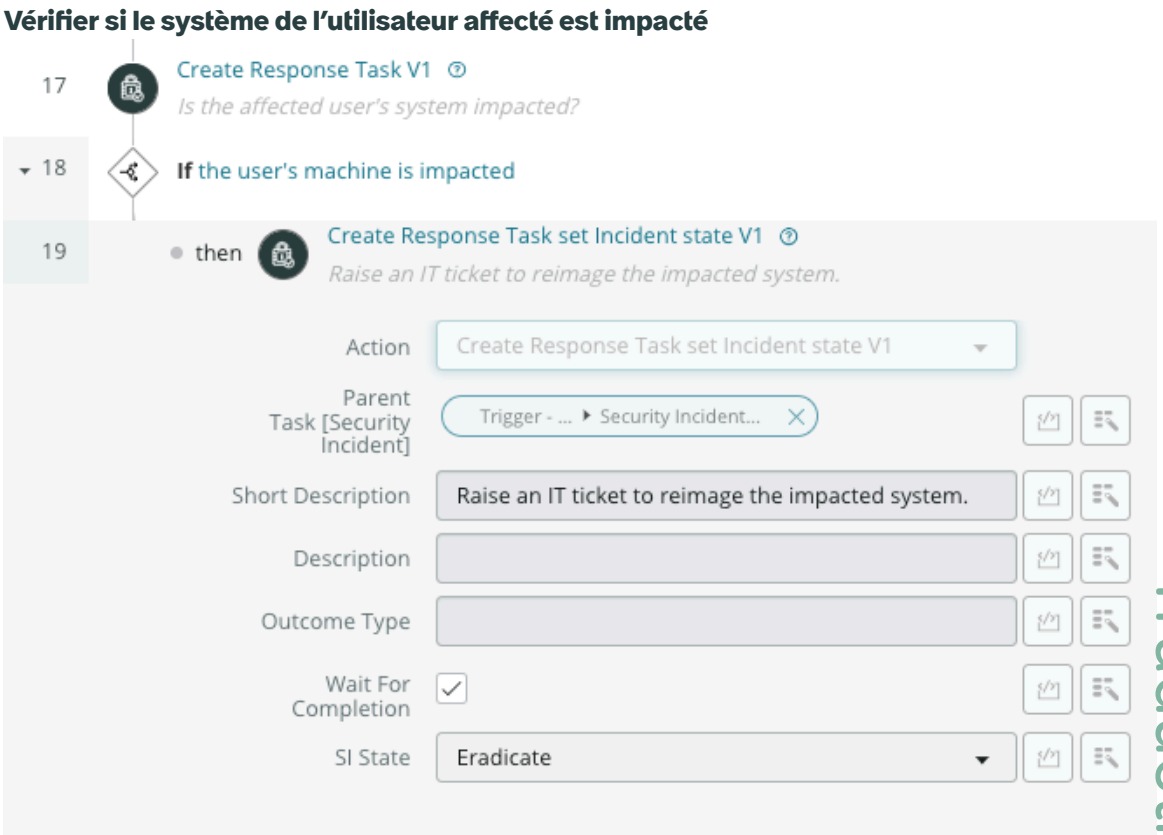
b. Dans l'action 16, vous devez bloquer l'expéditeur et les fichiers ou pièces jointes malveillants sur Office 365 et Proofpoint.

4. Dans l'action 17, s'il ne s'agit pas d'un e-mail interne falsifié, vous devez vérifier si le système de l'utilisateur concerné est impacté.

5. Dans l'action 18, si le système de l'utilisateur est impacté, dans l'action 19, émettez un ticket informatique pour recréer l'image du système impacté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Dans l'action 20, une tâche de réponse est créée pour vous permettre de terminer la revue post-incident avant de fermer la tâche.

Playbook pour la détection des points de terminaison

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les alertes de programme malveillant déclenchées sur un hôte ou un point de terminaison (par exemple, la détection d'un fichier malveillant).

Lorsque des alertes CrowdStrike sont déclenchées sur un hôte ou un point de terminaison, vous pouvez utiliser le playbook de détection des points de terminaison dans Flow Designer pour obtenir des conseils et optimiser l'examen de ces fichiers malveillants.

Configurer le playbook de détection des points de terminaison

Procédez comme suit pour configurer le playbook de détection des points de terminaison.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **de détection des points de terminaison** .

Traduction automatique

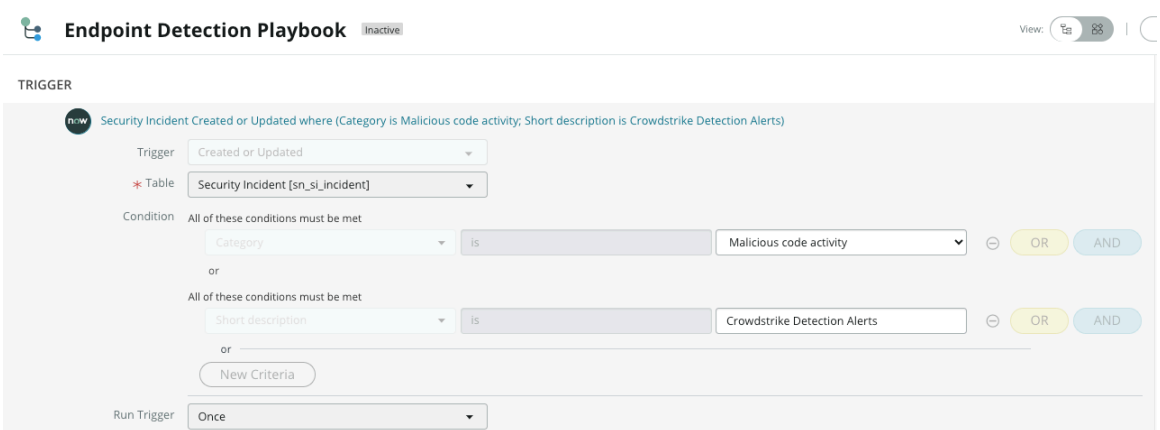
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. **Facultatif :** Vous pouvez créer une copie du flux du playbook de détection des points de terminaison et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :
   - **La catégorie** est **Activité de code malveillant**.
   - **La description brève** est **Alertes de détection CrowdStrike**.



Utiliser le playbook de détection des points de terminaison

Utilisez ce playbook pour enquêter sur les alertes de programme malveillant déclenchées sur un hôte ou un point de terminaison. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook de détection des points de terminaison.

Avant de commencer

Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez vérifier si le fichier ou le hachage est malveillant en analysant les résultats de la recherche de menaces dans SIR et en recueillant des informations à partir de VirusTotal, WildFire, ThreatCrowd, etc.
2. Dans l'action 2, vous devez vérifier si le fichier ou le hachage est malveillant ou non.
3. Dans l'action 3, si le fichier ou le hachage est malveillant, effectuez les actions suivantes :

   a. Dans l'action 4, vous devez identifier l'application ou le processus détecté comme une menace et recueillir des informations sur le raisonnement de détection pour continuer vers la liste sûre.

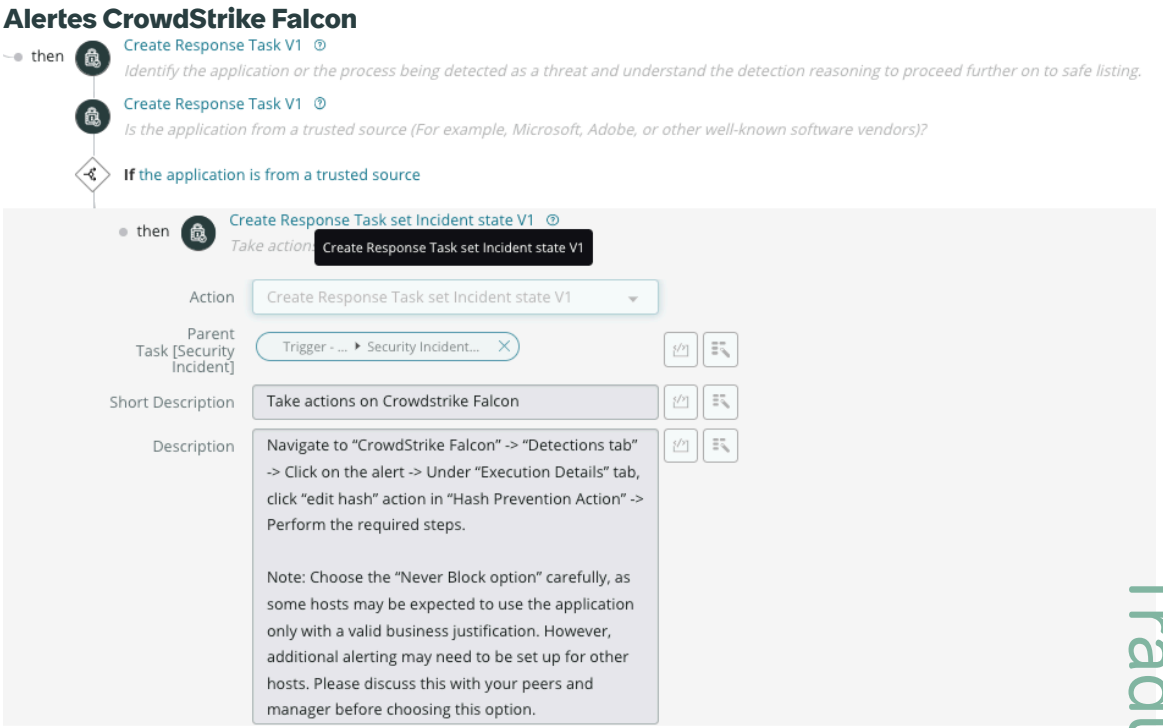


   b. Dans l'action 5, vous devez vérifier si l'application provient d'une source fiable (par exemple, Microsoft, Adobe ou d'autres fournisseurs de logiciels bien connus).

   c. Dans l'action 6, si l'application provient d'une source fiable, vous devez prendre des mesures sur les alertes CrowdStrike Falcon.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Dans l'action 7, effectuez les actions suivantes :

i. Accédez à la **CrowdStrike Falcon** > **Détections** onglet.

ii. Cliquez sur l'alerte CrowdStrike Falcon.

iii. Sous l'onglet Détails de l'exécution, cliquez sur Modifier l'action de **hachage** dans Action de prévention du hachage.

iv. Effectuez les étapes requises.

> **Remarque :** Choisissez l'option **Ne jamais bloquer** avec soin, car seuls certains hôtes peuvent être autorisés à utiliser l'application avec une justification commerciale valable. Toutefois, des alertes supplémentaires peuvent devoir être configurées pour d'autres hôtes.

e. Dans l'action 8, si l'application ne provient pas d'une source fiable, vous devez choisir si vous souhaitez supprimer le fichier ou l'application de l'appareil localement.
Dans l'action 10, si vous souhaitez supprimer le fichier ou l'application du périphérique localement, effectuez les actions suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Dans l'action 11, accédez à l'onglet **Fichiers en quarantaine** et filtrez le point de terminaison en recherchant le nom de l'appareil.

ii. Sélectionnez le fichier qui doit être supprimé localement, puis cliquez sur **Libérer**.

Remarque :

- Le fichier s'exécute toujours sur ce point de terminaison spécifique. Cependant, la détection et la quarantaine continuent de se produire sur tous les autres hôtes.
- Pour libérer en bloc le fichier de quarantaine sur plusieurs hôtes, sélectionnez le nom et l'état de fichier appropriés. Cliquez sur **Sélectionner**, puis sélectionnez **Mettre en production**.

Dans l'action 12, si vous ne souhaitez pas supprimer le fichier ou l'application de l'appareil localement, vous pouvez rediriger l'utilisateur vers le support informatique pour demander l'installation des applications approuvées.

4. Dans l'action 14, si le fichier ou le hachage n'est pas malveillant, effectuez les actions suivantes :

a. Dans l'action 15, vous devez déterminer si le fichier/hachage présente un risque élevé ou faible en fonction du rôle de l'utilisateur (département ou poste qui gère des informations sensibles), du type d'application (rançongiciel, rootkit...) et de l'impact de l'application (combien d'utilisateurs ont été touchés).

b. Dans l'action 16, s'il s'agit d'un fichier à haut risque, effectuez les actions suivantes :

i. Dans l'action 17, examinez les résultats avec l'équipe Threat Intelligence.

ii. Dans l'action 18, exécutez l'analyse des octets de programme malveillant sur le fichier.

iii. Dans l'action 19, lancez une analyse médico-légale.

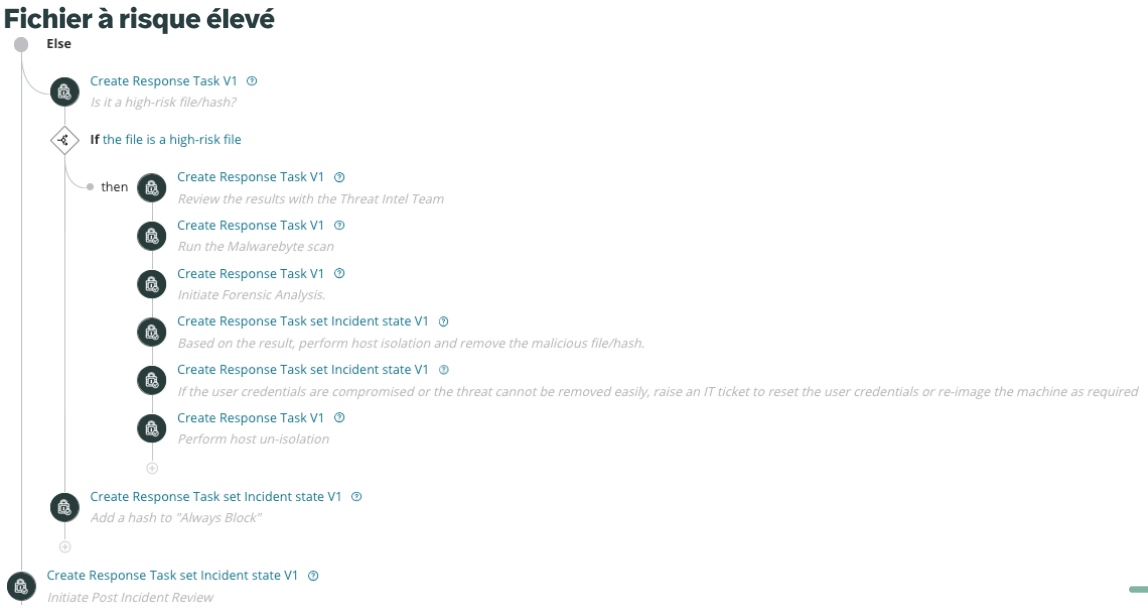
iv. Dans l'action 20, en fonction du résultat de l'analyse médico-légale, isolez l'hôte et supprimez le fichier/hachage malveillant.

v. Dans l'action 21, si les informations d'identification de l'utilisateur sont compromises ou si la menace ne peut pas être supprimée facilement, créez un ticket informatique pour réinitialiser les informations d'identification de l'utilisateur ou recréer l'image de l'ordinateur selon les besoins.

vi. Dans l'action 22, procédez à la désisolation de l'hôte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Dans l'action 23, si le fichier n'est pas un fichier à haut risque, effectuez les actions suivantes :

i. Accédez à la **CrowdStrike Falcon** > **Configurations** onglet.

ii. Depuis l'onglet Configurations, accédez à **Hachages de prévention** > > **Hachage de chargement** > **Ajouter le hachage**.

iii. Choisissez le système d'exploitation requis, puis sélectionnez **Toujours bloquer**.

5. Dans l'action 24, une tâche de réponse est créée pour que l'utilisateur termine l'examen post-incident avant de fermer la tâche.

Playbook pour un éventuel spray de mot de passe

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les alertes de pulvérisation de mots de passe déclenchées par plusieurs échecs de connexion (trop d'échecs d'authentification à partir de plusieurs adresses IP pour le même utilisateur).

Configurer le Playbook de pulvérisation de mot de passe possible

Suivez les étapes suivantes pour configurer le playbook de pulvérisation de mot de passe possible.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.

2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **Pulvérisation de mot de passe possible** .

Traduction automatique

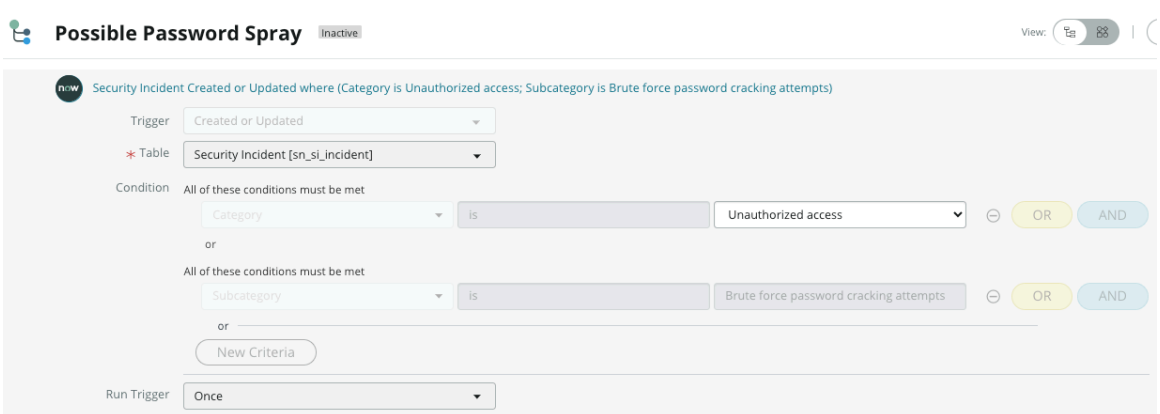
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. **Facultatif :** Vous pouvez créer une copie du flux de playbook Pulvérisation du mot de passe possible et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :
   - **La catégorie** est **Accès non autorisé**.
   - **La sous-catégorie** est **Tentatives de décodage de mot de passe en force brute**.



Utiliser le playbook de pulvérisation de mot de passe possible

Utilisez ce playbook pour examiner les alertes de pulvérisation de mots de passe déclenchées par plusieurs échecs de connexion (trop d'échecs d'authentification à partir de plusieurs adresses IP pour le même utilisateur). Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Pulvérisation de mot de passe possible.

Avant de commencer

Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

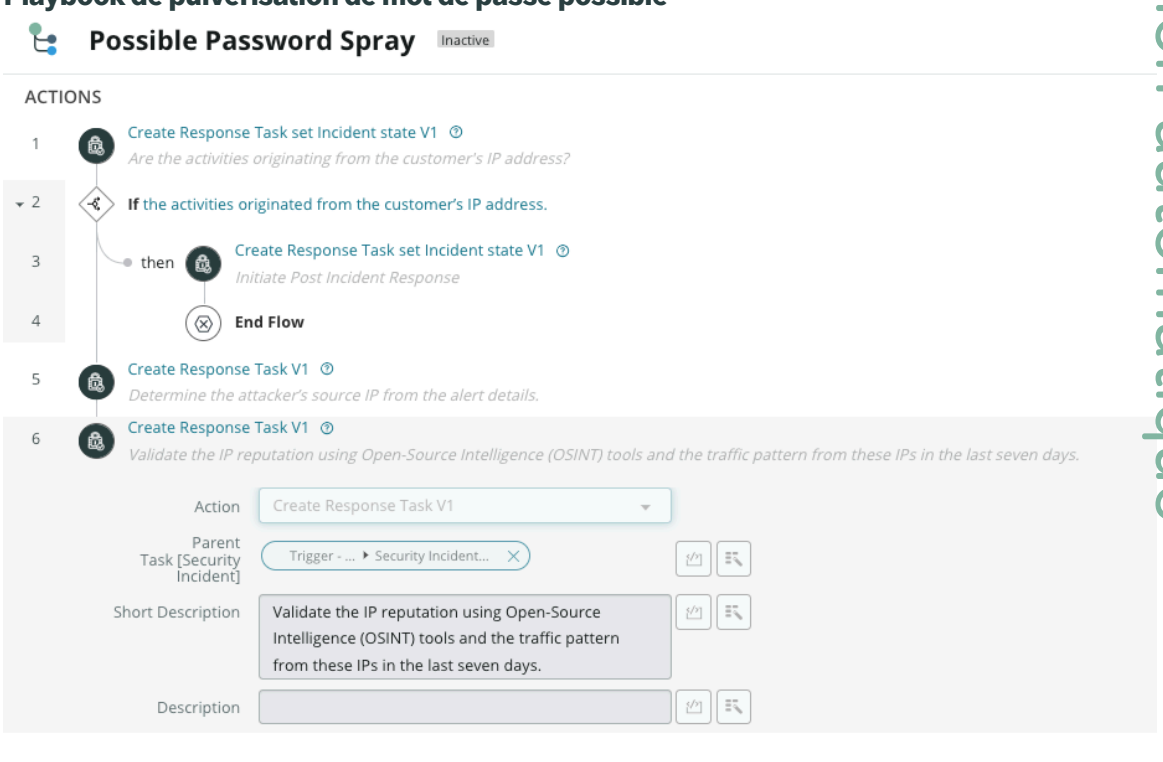
- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez vérifier si les activités proviennent de l'adresse IP du client.
   Identifiez les adresses IP effectuant l'attaque par pulvérisation de mot de passe. Par exemple, utilisez les TXID (ID de transaction) de l'alerte et recherchez-les par rapport aux journaux F5.
2. Dans l'action 2, si les activités proviennent de l'adresse IP du client, effectuez les actions suivantes :
   a. Dans l'action 3, vous devez lancer un examen post-incident de l'attaque possible par pulvérisation de mot de passe.
   b. Dans l'action 4, le flux s'arrête.
3. Dans l'action 5, si les activités ne proviennent pas de l'adresse IP du client, déterminez l'adresse IP source de l'attaquant à partir des détails de l'alerte.
4. Dans l'action 6, vous devez valider la réputation de l'adresse IP à l'aide d'outils d'intelligence open source (OSINT) et le modèle de trafic de ces adresses IP au cours des sept derniers jours.

Playbook de pulvérisation de mot de passe possible



5. Dans l'action 7, vous devez identifier les noms d'utilisateur qui se sont connectés avec succès à l'aide de l'attaque par pulvérisation de mot de passe.
6. Dans l'action 8, vous devez identifier le nombre d'échecs de connexion et de schémas.
7. Dans l'action 9, vous devez identifier les indicateurs de vrai positif.

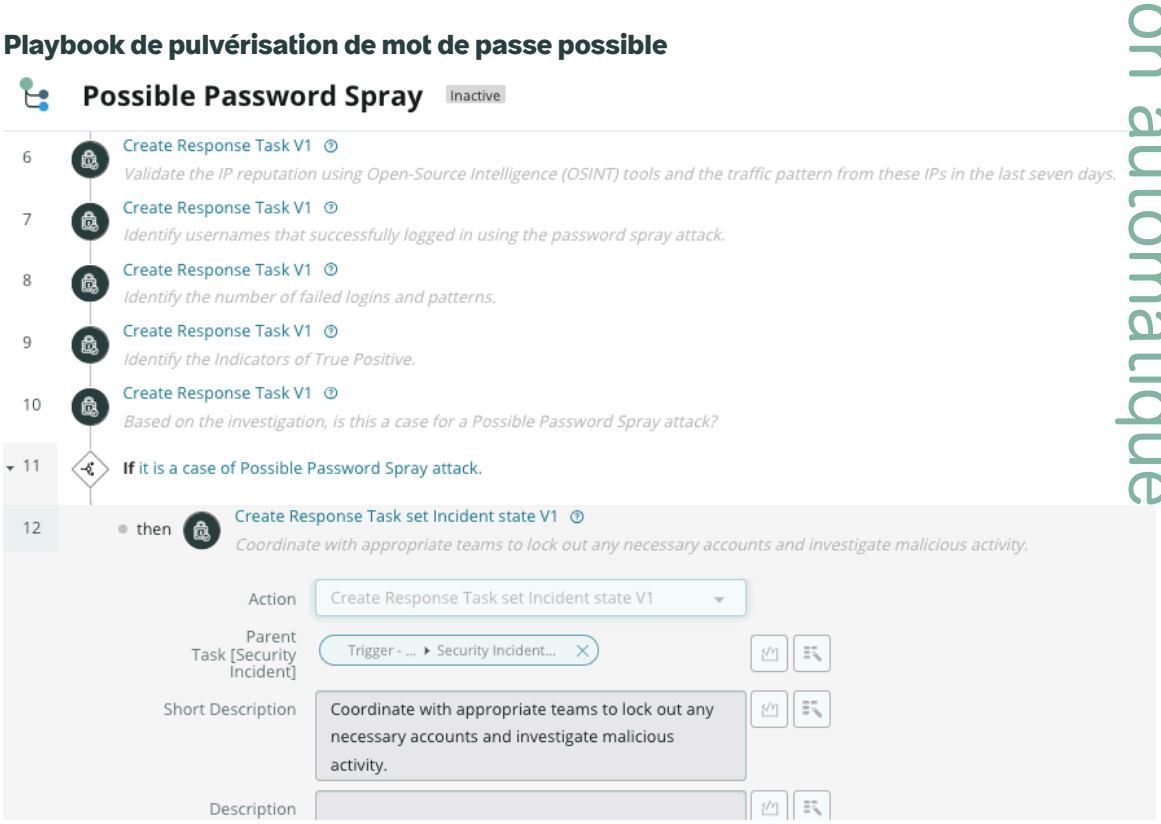
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifiez le trafic à partir des adresses IP sources au cours des 60 derniers jours. Aucun trafic historique ne peut être une indication d'un vrai positif.
- Vérifiez les schémas de nom d'utilisateur ayant des échecs d'authentification et leur nombre. Plus le nombre est élevé, plus la probabilité qu'il s'agisse d'un vrai positif est élevée.
- Le nom d'utilisateur ressemble à une base de dictionnaire (de A à Z) et peut avoir des noms d'administrateur communs comme administrateur, sysadmin, root, etc
- Le même nom d'utilisateur peut avoir des modèles différents dans l'attaque par pulvérisation, comme la même alerte peut avoir des défaillances pour john.doe, johnd, jdoe, john_doe, jdoe7, etc., indiquant que les attaquants devinent le modèle de nom d'utilisateur en fonction des cas d'utilisation courants.
- Remarquez l'agent utilisateur et les URI des journaux F5 dans l'étape ci-dessus, et voyez si les IOC sont liés aux alertes Red Condor. S'ils correspondent, alors c'est un véritable événement positif.

8. Dans l'action 10, sur la base de l'enquête effectuée jusqu'à présent, vous devez vérifier s'il s'agit d'un cas d'attaque possible par pulvérisation de mot de passe ou non.
9. Dans l'action 11, s'il s'agit d'une attaque possible par pulvérisation de mot de passe, effectuez les actions suivantes :

   a. Dans l'action 12, vous devez vous coordonner avec les équipes appropriées pour verrouiller tous les comptes nécessaires et enquêter sur les activités malveillantes.



   b. Dans l'action 13, vous devez lancer un examen post-incident de l'attaque possible par pulvérisation de mot de passe.

   c. Dans l'action 14, le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Dans l’action 15, vous devez vérifier s’il ne s’agit pas d’un cas d’attaque possible par pulvérisation de mot de passe.
11. Dans l’action 16, s’il ne s’agit pas d’un cas d’attaque possible par pulvérisation de mot de passe, effectuez les actions suivantes :
    a. Dans l’action 17, vous devez documenter les résultats obtenus jusqu’à présent.
    b. Dans l’action 18, vous devez lancer un examen post-incident de l’attaque possible par pulvérisation de mot de passe.
    c. Dans l’action 19, le flux s’arrête.
12. Dans l’action 20, vous devez consulter les pairs et le gestionnaire GIR pour obtenir des conseils.
13. Dans l’action 21, une tâche de réponse est créée pour terminer la revue post-incident avant de fermer la tâche.

Playbook pour T1003 - Outils de détection de dumping d’informations d’identification

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur un incident impliquant des activités de dumping d’informations d’identification.

Configurer le Playbook T1003 - Outils de détection des informations d’identification

Suivez les étapes suivantes pour configurer le playbook T1003 - Outils de détection de dumping d’informations d’identification.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d’avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu’utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **T1003 - Outils de détection du dumping d’informations d’identification** .
3. **Facultatif :** Vous pouvez créer une copie du flux de playbook T1003 - Détecter les outils de dumping d’informations d’identification et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l’icône de  et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d’apporter des changements spécifiques au flux.

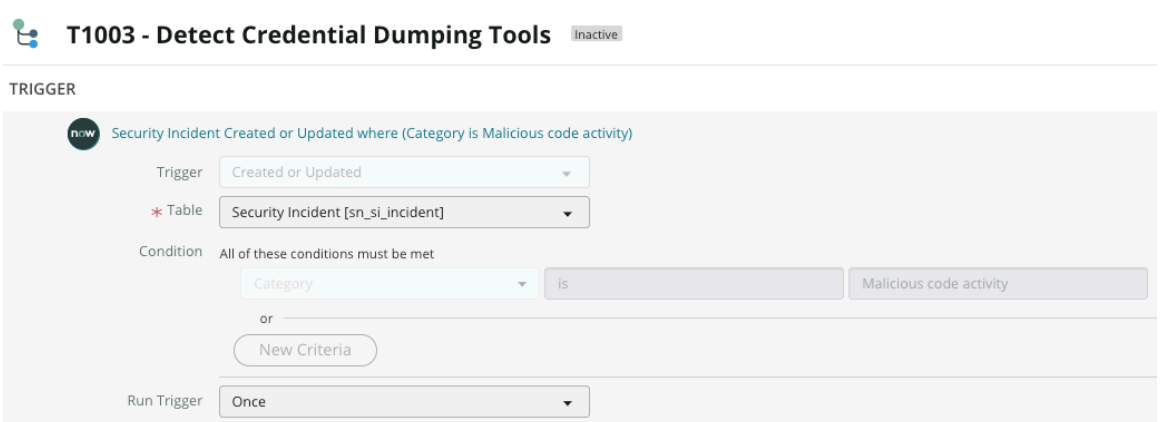
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Activité de code malveillant**.



Utiliser le playbook T1003 - Outils de détection de dumping d'informations d'identification

Utilisez ce manuel pour enquêter sur un incident impliquant des activités de dumping d'informations d'identification. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook T1003 - Détecter les outils de dumping d'informations d'identification.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

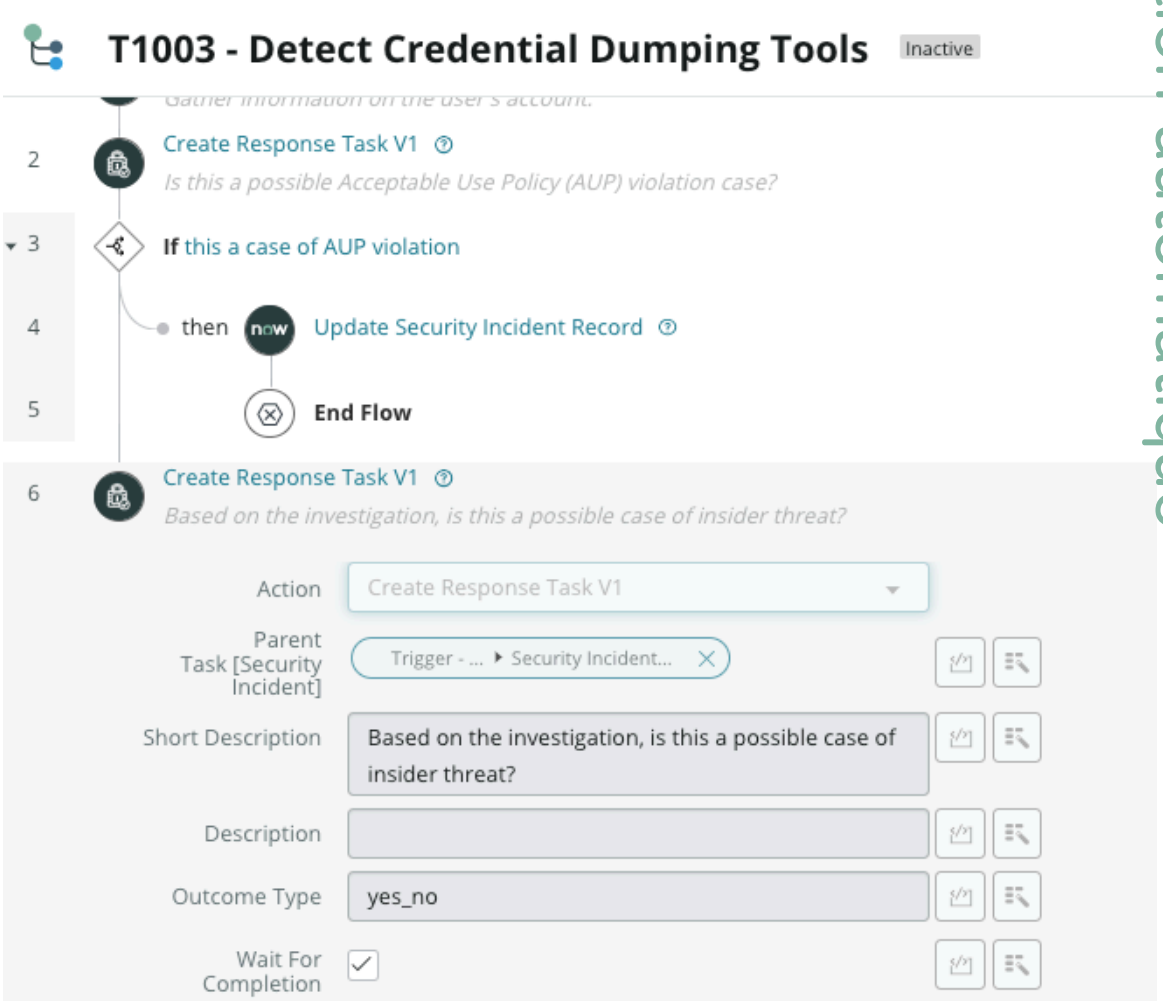
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez collecter des informations sur le compte de l'utilisateur.
   - Vous devez vérifier l'activité de l'hôte pour détecter toute activité suspecte.
   - Vous devez identifier le propriétaire du serveur/point de terminaison/VM et capturer les données corrélées à l'outil.
   - Vous devez recueillir des informations sur les autres comptes de l'utilisateur.
2. Dans l'action 2, vous devez vérifier s'il s'agit d'un cas possible de violation de la politique d'utilisation acceptable (AUP).
   Vous pouvez effectuer un examen par les pairs avec les preuves recueillies et consulter votre gestionnaire d'incidents régional pour savoir si vous souhaitez contacter l'utilisateur.
3. Dans l'action 3, s'il s'agit d'un cas de violation de la politique d'utilisation acceptable (AUP), effectuez les actions suivantes :
   a. Dans l'action 4, vous devez informer l'incident de sécurité qu'il s'agit d'un cas de violation d'AUP
   b. Dans l'action 5, le flux s'arrête.
4. Dans l'action 6, sur la base de l'enquête effectuée jusqu'à présent, vous devez vérifier s'il s'agit d'un cas possible de menace interne ou non.

T1003 - Playbook des outils de détection des informations d'identification



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans l’action 7, s’il s’agit d’un cas de menace interne, effectuez les actions suivantes :

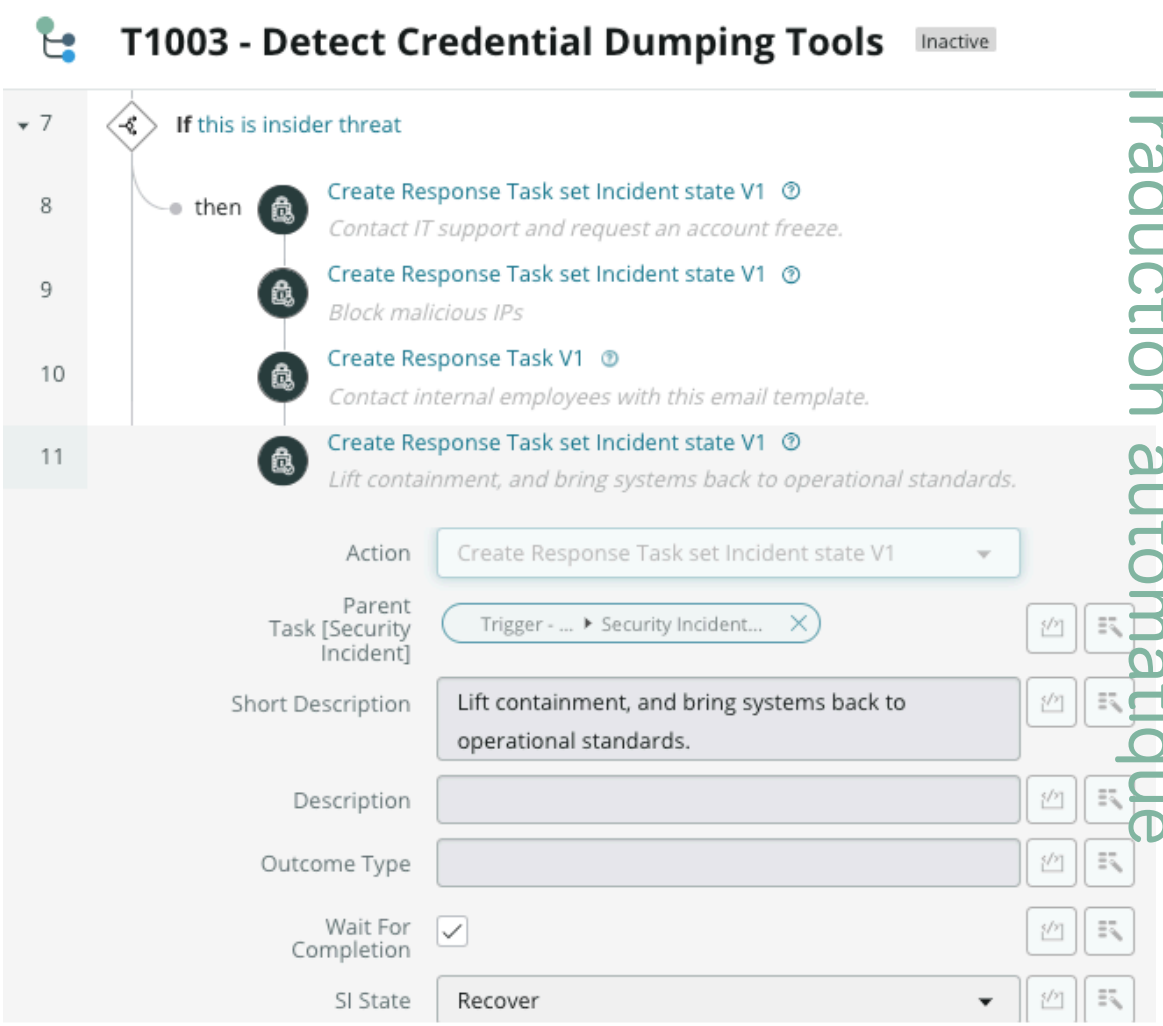
   a. Dans l’action 8, vous devez contacter le support informatique et demander un gel de compte.

   b. Dans l’action 9, vous devez bloquer les IP malveillantes.

   c. Dans l’action 10, vous devez contacter les employés internes par e-mail.
   Vous pouvez utiliser le modèle d’e-mail fourni pour contacter vos employés internes.

   d. Dans l’action 11, vous devez lever le confinement et ramener les systèmes aux normes opérationnelles.
   Le flux s’arrête.

Tâches de réponse pour lever le confinement



6. Dans l’action 12, s’il ne s’agit pas d’un cas de menace interne, dans l’action 13, vous devez effectuer un examen par les pairs pour déterminer si cela doit être ajouté à la liste d’exclusion.
   Le flux s’arrête.

7. Dans l’action 14, une tâche de réponse est créée pour terminer la revue post-incident avant de fermer la tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook pour la détection d'usurpation de domaine de messagerie

Ce playbook facilite le triage précoce des soumissions d'hameçonnage signalées par les utilisateurs en alertant l'analyste de la possibilité d'un domaine similaire dans l'adresse e-mail de l'hameçonneur.

Le playbook de détection d'usurpation de domaine d'e-mail cherche à trouver une correspondance de similitude entre le domaine de messagerie de l'expéditeur d'hameçonnage et un nom de domaine approuvé existe dans le référentiel observable. Lorsqu'une correspondance de domaine de messagerie d'expéditeur usurpé a été identifiée par le playbook, les analystes sont alertés par une balise.

Le workflow est créé en fonction d'un playbook existant, ce qui fournit une approche cohérente et efficace pour les enquêtes sur les incidents. Chaque point de décision du playbook a été converti en une tâche pilotée par les résultats et le flux change de direction en fonction du résultat de ces tâches.

Configurer le playbook de détection d'usurpation d'e-mail

Procédez comme suit pour configurer le playbook de détection d'usurpation d'adresse e-mail.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

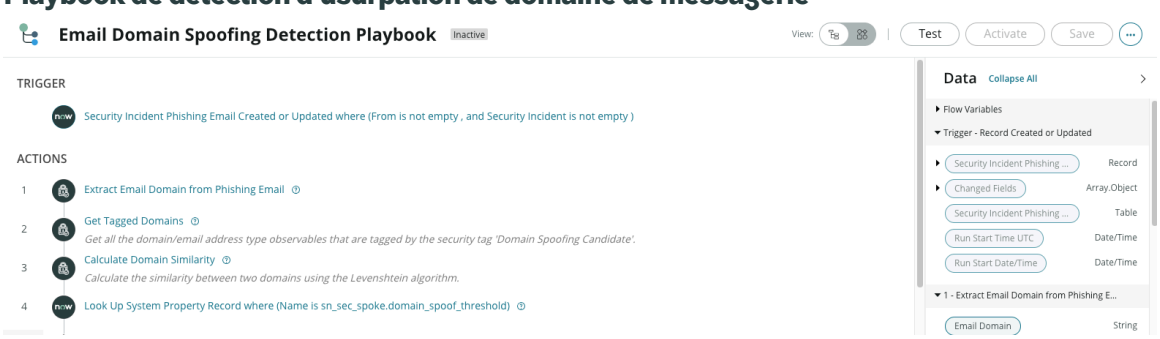
Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le **playbook de détection d'usurpation de domaine de messagerie** .
3. **Facultatif :** Vous pouvez créer une copie du flux de playbook Détection d'usurpation de domaine d'e-mail et apporter les modifications nécessaires.

   Pour créer une copie du flux du playbook, cliquez sur l'icône de ••• et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

Playbook de détection d'usurpation de domaine de messagerie



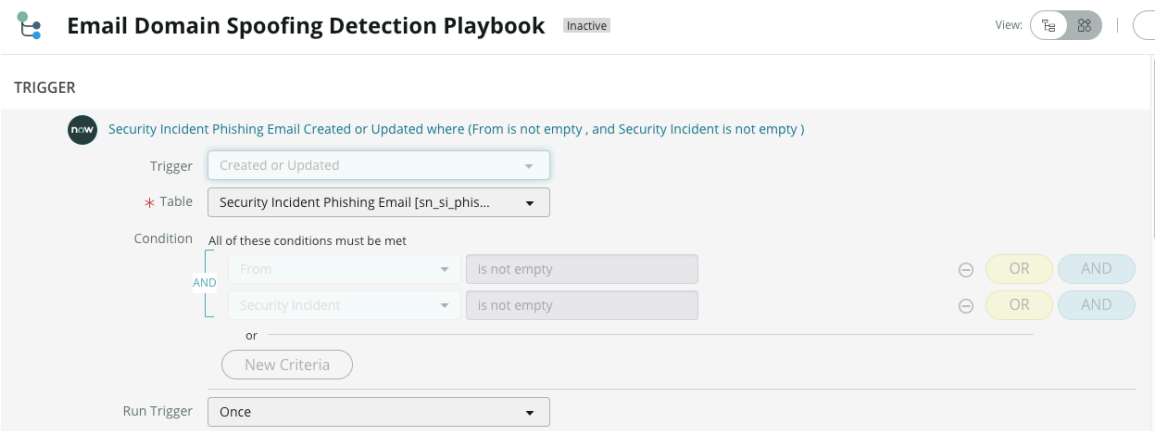
4. Activez les playbooks.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez le flux principal pour utiliser le playbook disponible dans le système de base.
- Activez les flux copiés après avoir apporté les changements requis.

5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :
   - **De n'est** pas **vide**.
   - **L'incident de sécurité n'est** pas **vide**.



Utiliser le playbook de détection d'usurpation de domaine de messagerie

Utilisez ce playbook pour trouver une correspondance de similarité entre le domaine de messagerie de l'expéditeur de l'hameçonneur et un nom de domaine approuvé existe dans le référentiel de l'observable. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook de détection d'usurpation de domaine de messagerie.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

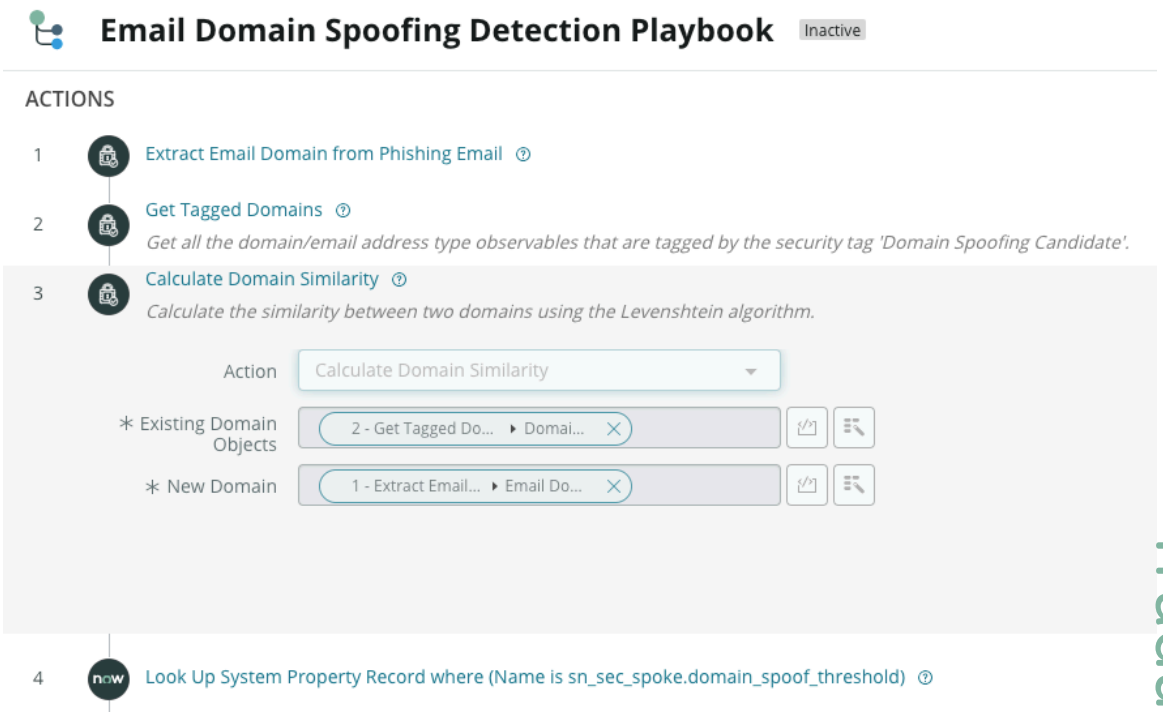
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, le playbook extrait le domaine de l'e-mail de l'e-mail d'hameçonnage.
2. Dans l'action 2, le playbook récupère tous les observables de type domaine/adresse e-mail marqués par la balise de sécurité « Candidat d'usurpation de domaine ».
3. Dans l'action 3, le playbook calcule la similarité entre le domaine Get Tagged et le domaine Email à l'aide de l'algorithme de Levenshtein.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de détection d'usurpation de domaine de messagerie

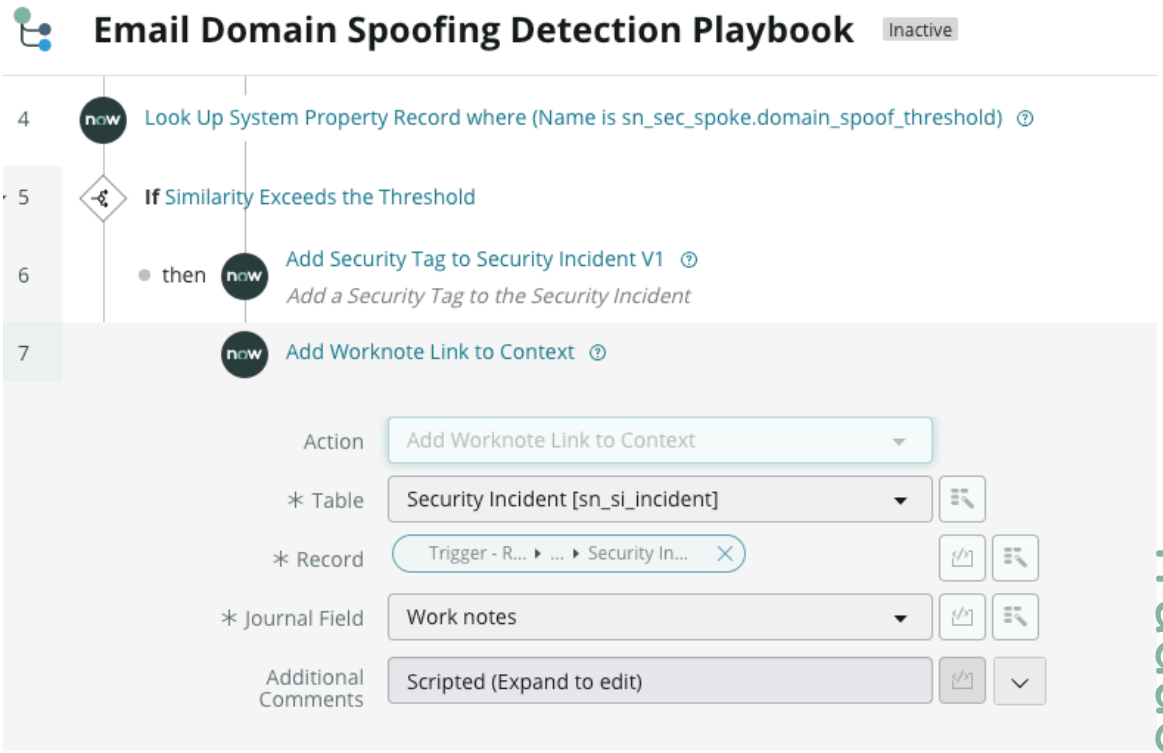


4. Dans l'action 4, le playbook recherche l'enregistrement de propriété système en fonction des conditions suivantes :
   - Le nom est sn_sec_spoke.domain_spoof_threshold, (OU)
   - Le nom est compris entre a et z. Si plusieurs enregistrements sont trouvés, renvoie uniquement le premier enregistrement.
5. Dans l'action 5, sur la base de l'enquête effectuée jusqu'à présent, le playbook vérifie si la similarité des deux domaines dépasse le seuil ou non.
   Si la similarité des deux domaines ne dépasse pas le seuil, une tâche de réponse manuelle est créée dans l'action 5 et le flux s'arrête. Si la similarité des deux domaines dépasse le seuil, les actions 6 et 7 sont exécutées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La similarité dépasse le seuil



6. Dans l'action 6, le playbook ajoute la balise de sécurité Usurpation de domaine de messagerie à l'incident de sécurité.
7. Dans l'action 7, le playbook ajoute un lien de note de travail au contexte à l'aide de l'option de script.
8. Dans l'action 8, le flux s'arrête.

Playbook pour les erreurs de frappe dans le domaine squatté

Ce playbook fournit des procédures systématiques pour enquêter sur les domaines mal orthographiés et collaborer avec le service juridique de l'organisation pour les retraits. Les domaines squattés sont des noms de domaine intentionnellement mal orthographiés qui ressemblent beaucoup à des noms légitimes. Les attaquants profitent des fautes d'orthographe pour les diriger vers un site Web mal intentionné à des fins d'exploitation financière ou d'autres activités malveillantes.

Les domaines squattés par faute de frappe sont signalés à l'équipe des opérations de sécurité à partir de différentes sources, telles que les solutions de protection contre les risques numériques (Digital Shadows) et les plateformes de renseignement sur les menaces (Anomali Threatstream). Après la création d'un incident de sécurité, cette solution permet d'identifier si le domaine est effectivement un domaine squatté par faute de frappe. S'il s'agit d'un domaine squatté par faute de frappe, l'analyste peut le signaler à l'équipe juridique afin que d'autres mesures puissent être prises.

Le workflow est créé en fonction d'un playbook existant, ce qui fournit une approche cohérente et efficace pour les enquêtes sur les incidents. Chaque point de décision du playbook a été converti en une tâche axée sur les résultats et le flux change de direction en fonction du résultat de ces tâches.

Configurer le playbook de domaine squatté par typo

Procédez comme suit pour configurer le playbook de domaine squatté par typo.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **Faute de frappe du domaine squatté** .
3. **Facultatif :** Vous pouvez créer une copie du flux de playbook Domaine squatté par typo et apporter les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, cliquez sur l'icône de ••• et sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.



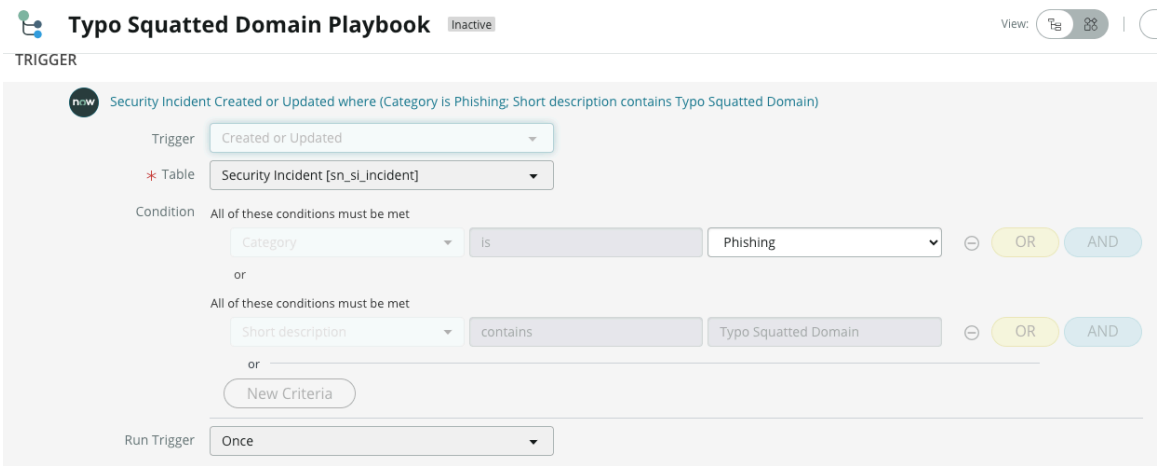
4. Activez les playbooks.
   - Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   - Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **La catégorie** est **Hameçonnage**.
- **La brève description** contient **un domaine squatté par faute de frappe**.



Utiliser le playbook de domaine squatté par typo

Utilisez ce manuel pour enquêter sur les domaines mal orthographiés et collaborer avec le service juridique de l'organisation pour les retraits. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook de domaine squatté de fautes de frappe.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

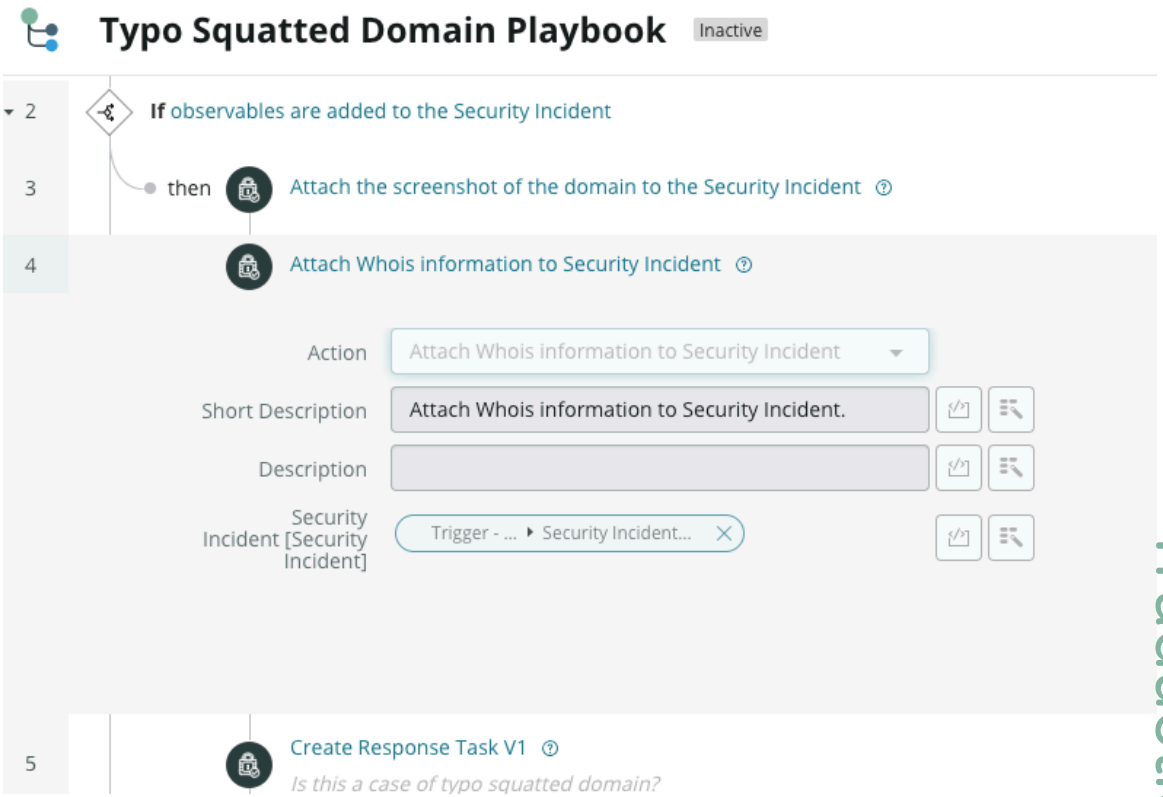
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vous devez vérifier si les observables sont ajoutés à Security Incident Response (SIR).
   Si les observables ne sont pas ajoutés à SIR, veuillez les ajouter avant de poursuivre. Si les observables ne sont pas disponibles, l'action 10 est exécutée et l'incident de sécurité est fermé.
2. Dans l'action 2, si les observables sont ajoutés à l'incident de sécurité, les actions suivantes sont exécutées.
3. Dans l'action 3, vous devez joindre la capture d'écran du domaine Typo Squatted à l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de domaine squatté pour une faute de frappe

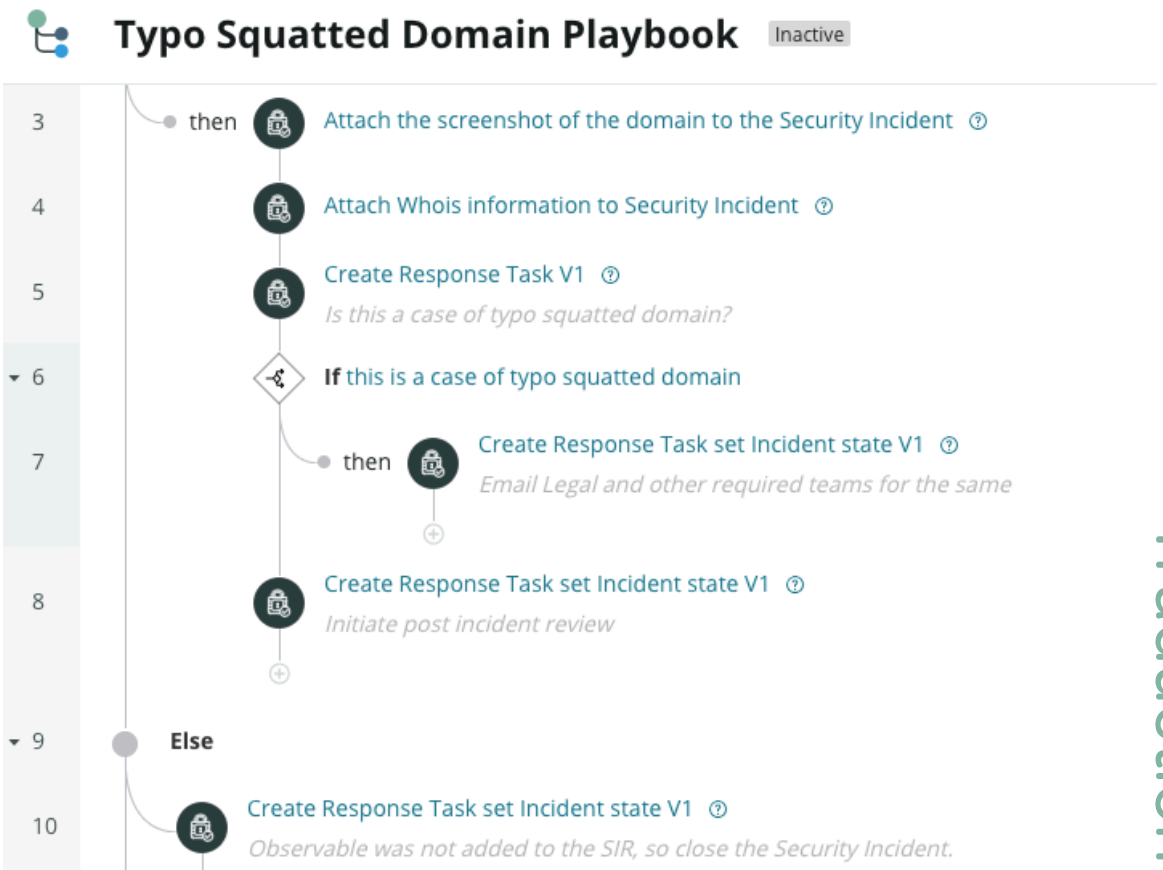


4. Dans l’action 4, vous devez joindre les informations Whois à l’incident de sécurité.
5. Dans l’action 5, sur la base de l’enquête effectuée jusqu’à présent, le playbook vérifie s’il s’agit d’un cas de domaine Typo Squatted ou non.
   S’il ne s’agit pas d’un cas de domaine Typo squatté, une tâche de réponse manuelle est créée dans l’action 5 et le flux s’arrête.
6. Dans l’action 6, s’il s’agit d’un cas de domaine Typo squatté, alors l’action 7 est exécutée.
7. Dans l’action 7, vous devez envoyer un e-mail et informer les équipes juridiques et autres équipes requises qu’il s’agit d’un cas de domaine Typo Squatted et prendre les mesures nécessaires pour l’éradiquer.
   S’il ne s’agit pas d’un cas de domaine Typo squatté, une tâche de réponse manuelle est créée dans l’action 5 et le flux s’arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas de faute de frappe : domaine squatté



8. Dans l'action 9, une tâche de réponse est créée pour vous permettre de terminer l'examen post-incident avant de fermer la tâche.

Playbook pour le reniflage des informations d'identification

Ce playbook fournit des étapes de rattrapage du système pour enquêter sur un incident impliquant des activités de reniflage d'informations d'identification effectuées via la `sys_installation_exit` table dans une instance ServiceNow.

Le playbook de reniflage des informations d'identification fournit un champ de script pour traiter les connexions à la base de données (DB), l'authentification unique (SSO) et le LDAP (Lightweight Directory Access Protocol) à l'aide des enregistrements de la `sys_installation_exit` table. Ces champs de script privilégiés permettent d'écouter les demandes et les paramètres de l'utilisateur sur les instances pendant la connexion, y compris les informations d'identification de l'utilisateur telles que le nom d'utilisateur et le mot de passe.

Un utilisateur malveillant peut créer un script pour écouter les demandes de l'utilisateur et enregistrer ces demandes sur l'instance. La `sys_installation_exit` table d'une instance définit les règles de traitement des activités de connexion et de déconnexion de tous les utilisateurs de cette instance.

Configurer le playbook de reniflage d'informations d'identification

Procédez comme suit pour configurer le playbook de détection des informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

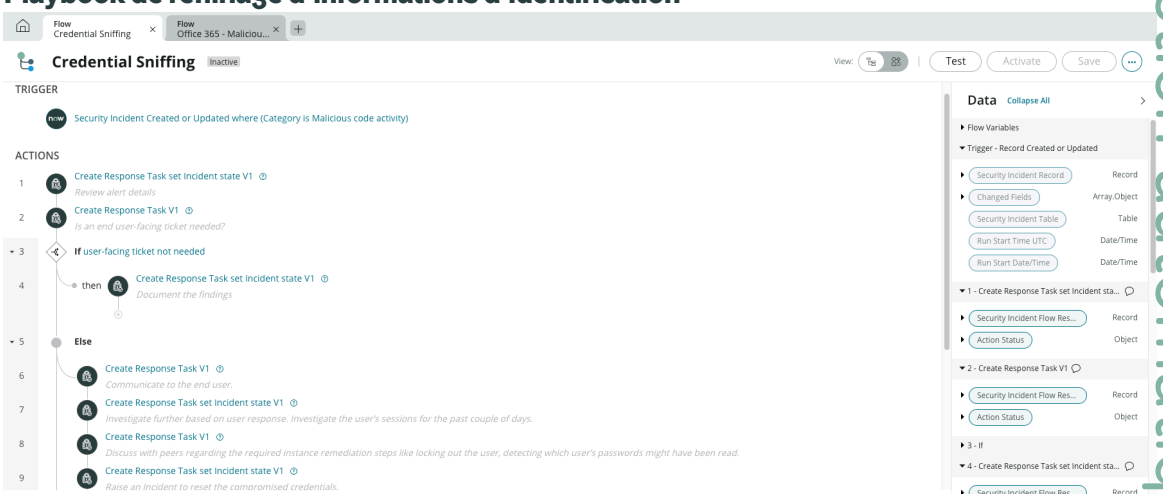
Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **de reniflage d'informations d'identification** .
3. **Facultatif :** Créer une copie du flux du playbook Renifler les informations d'identification et apporter les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de ••• , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

   Playbook de reniflage d'informations d'identification

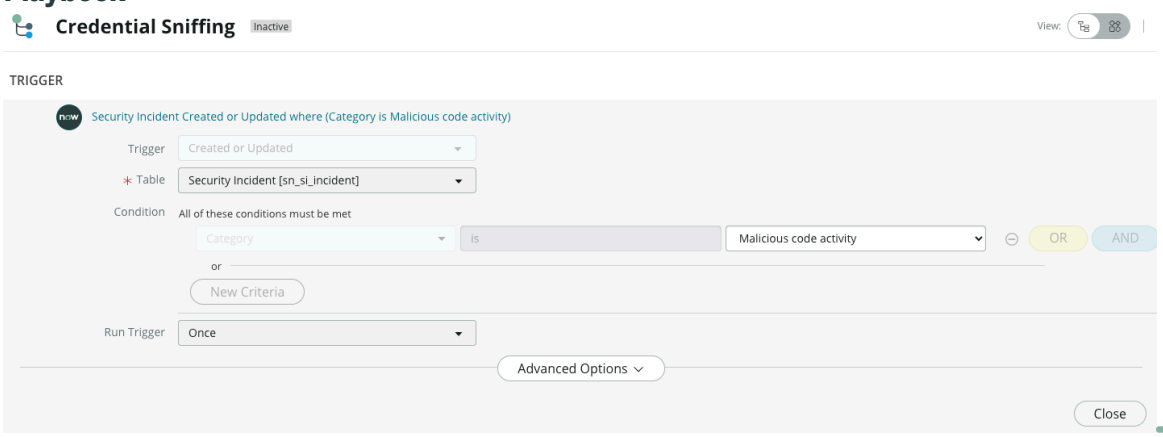
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Activité de code malveillant**.

Renifleur d'informations d'identification Condition de déclenchement du Playbook



Utiliser le playbook de reniflage d'informations d'identification

Utilisez ce manuel pour enquêter sur un incident impliquant des activités de reniflage d'informations d'identification effectuées via la `sys_installation_exit` table dans une instance ServiceNow. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook de reniflage des informations d'identification.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, examinez les détails d'alerte suivants.
   - Instance
   - ID de session
   - ID de transaction
   - _raw : fournit le script complet.

   Exemple de script :

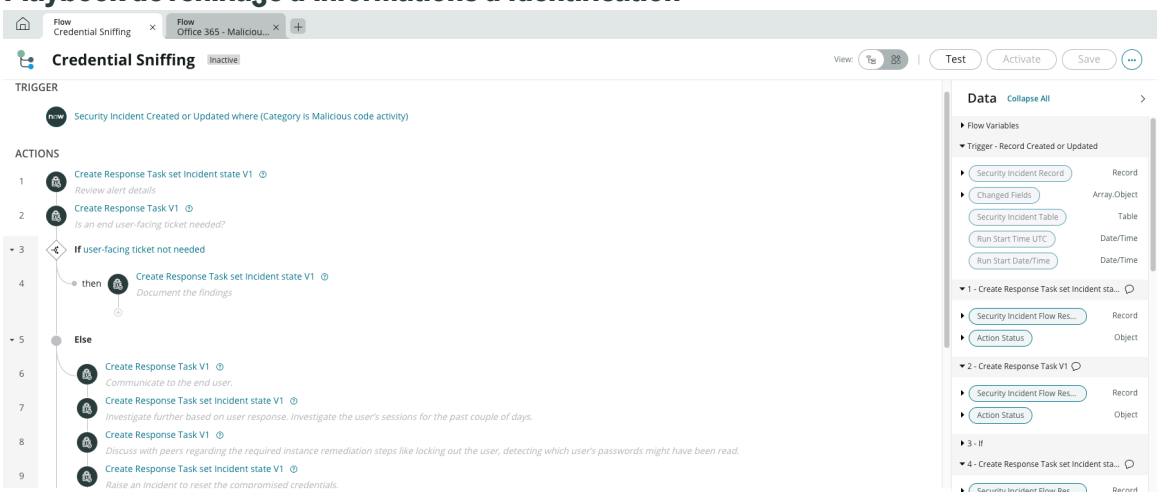
   ```
   Var pass= request.getParameter("user_password");
   Gs.log(pass);
   ```

2. Dans l'action 2, sur la base des données collectées jusqu'à présent, vérifiez si un ticket d'utilisateur final est requis pour cette alerte ou non.
3. Dans l'action 3, si l'alerte ne nécessite pas de ticket de l'utilisateur final, dans l'action 4, documentez les résultats obtenus jusqu'à présent.
   Le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook de reniflage d'informations d'identification



4. Dans l'action 5, si l'alerte nécessite un ticket d'utilisateur final, procédez comme suit :

   a. Dans l'action 6, informez l'utilisateur final que l'alerte nécessite un ticket d'utilisateur final.

   b. Dans l'action 7, examinez plus en détail en fonction de la réponse de l'utilisateur et des sessions de l'utilisateur au cours des deux derniers jours.

   c. Dans l'action 8, discutez avec vos pairs des étapes de rattrapage pour l'instance, comme le verrouillage de l'utilisateur et la détection des mots de passe d'utilisateur qui ont pu être lus.

   d. Dans l'action 9, soumettez un incident ou un ticket pour réinitialiser les informations d'identification de l'utilisateur compromis.

   e. Dans l'action 10, lever le confinement et ramener les systèmes aux normes opérationnelles
   Le flux s'arrête.

5. Dans l'action 11, effectuez l'examen post-incident avant de fermer la tâche.

Playbook pour T1070 : journaux des événements Windows effacés

Ce playbook fournit des étapes de rattrapage pour enquêter sur les incidents qui suivent les types d'événements où l'utilisateur supprime les journaux de sécurité. Chaque fois que le journal de sécurité est effacé, les événements 517 et 1102 sont journalisés, quel que soit l'état de la politique d'événement du système d'audit.

Cette alerte peut suivre les types d'événements suivants :

- **Événement 517** : Les champs Nom d'utilisateur principal et Nom d'utilisateur client identifient l'utilisateur qui a effacé le journal. Le nom d'utilisateur principal correspond au système et le nom d'utilisateur client indique l'utilisateur qui a effacé le journal.
- **Événement 1102** : Les champs Nom du compte et Nom du domaine identifient l'utilisateur qui a effacé le journal. L'ID de connexion vous permet d'établir une corrélation rétroactive avec l'événement de connexion et d'autres événements enregistrés au cours de la même session de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer le playbook T1070 - Journaux des événements Windows effacé

Suivez les étapes suivantes pour configurer le playbook T1070 - Journaux des événements Windows effacés.

Avant de commencer

Rôle requis :

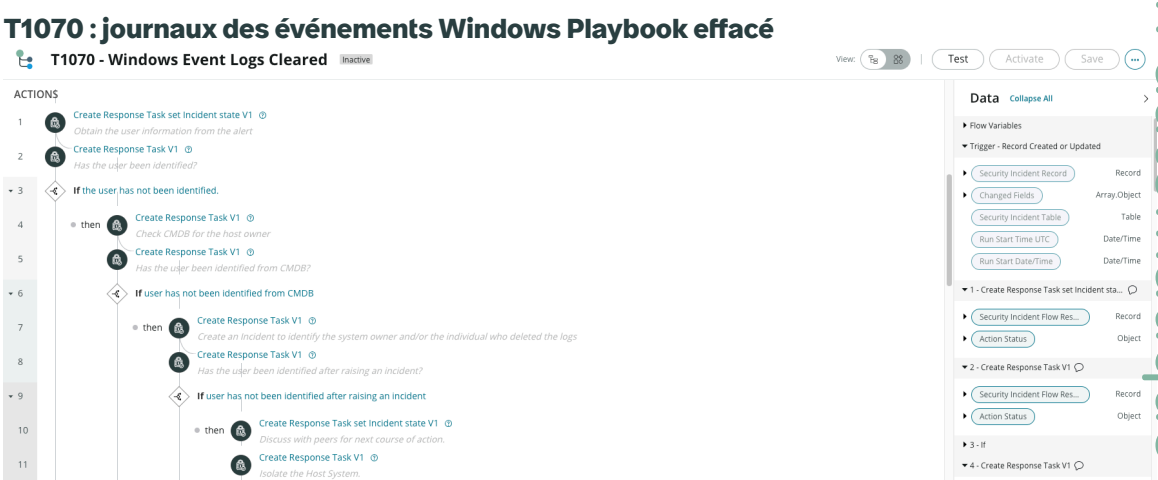
- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **T1070 - Windows Events Logs Cleared** .
3. **Facultatif :** Créez une copie du flux de playbook T1070 - Journaux des événements Windows effacés et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.



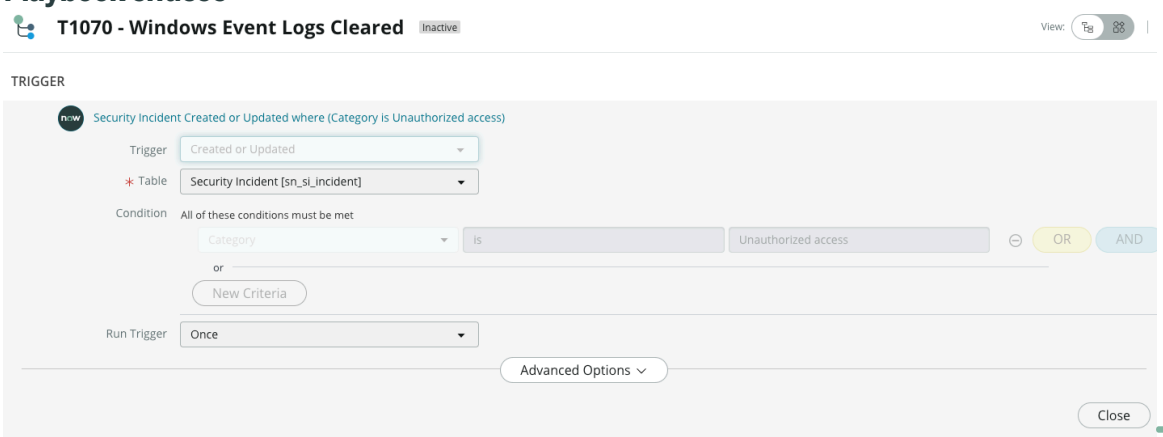
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Accès non autorisé**.

T1070 : journaux des événements Windows Condition de déclenchement du Playbook effacée



Utiliser le playbook T1070 - Journaux des événements Windows effacé

Utilisez ce playbook pour enquêter sur les incidents qui suivent les types d'événements où l'utilisateur supprime des journaux de sécurité. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook T1070 - Journaux des événements Windows effacés.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, obtenez les détails de l'utilisateur à partir de l'alerte.
2. Dans l'action 2, vérifiez si l'utilisateur a été identifié ou non.
3. Dans l'action 3, si l'utilisateur n'a pas été identifié, procédez comme suit :

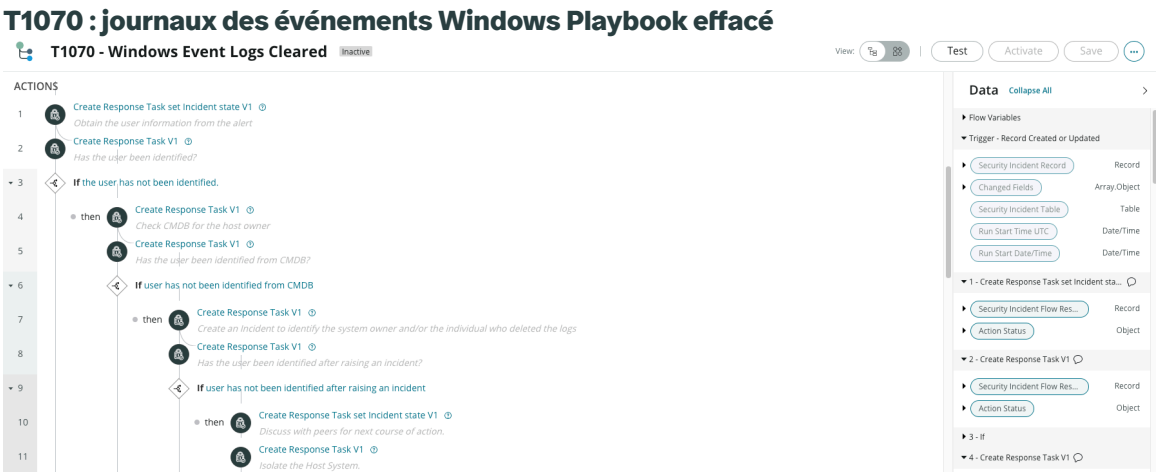
   a. Dans l'action 4, vérifiez la CMDB (Configuration Management Database) pour connaître les détails du propriétaire de l'hôte.

   b. Dans l'action 5, vérifiez si l'utilisateur a été identifié à partir de la CMDB ou non.

      Si l'utilisateur a été identifié à partir de la CMDB, une tâche de réponse manuelle est créée dans l'action 5 et le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Dans l'action 6, si l'utilisateur n'a pas été identifié à partir de la CMDB, procédez comme suit :

i. Dans l'action 7, créez un incident pour identifier le propriétaire du système et la personne qui a supprimé les journaux.

ii. Dans l'action 8, vérifiez si l'utilisateur a été identifié après avoir signalé un incident ou non.

Si l'utilisateur a été identifié après avoir soumis un incident, une tâche de réponse manuelle est créée dans l'action 8 et le flux s'arrête.

iii. Dans l'action 9, si l'utilisateur n'a pas été identifié après avoir signalé un incident, procédez comme suit :

1. Dans l'action 10, discutez de la prochaine ligne de conduite avec vos pairs.

2. Dans l'action 11, isolez le système hôte.

3. Dans l'action 12, supprimez tous les fichiers indésirables qui ont pu être créés et supprimez les comptes malveillants.

4. Dans l'action 13, levez le confinement et ramenez les systèmes aux normes opérationnelles.

5. Dans l'action 14, effectuez l'examen post-incident avant de fermer la tâche.

Dans l'action 15, le flux s'arrête.

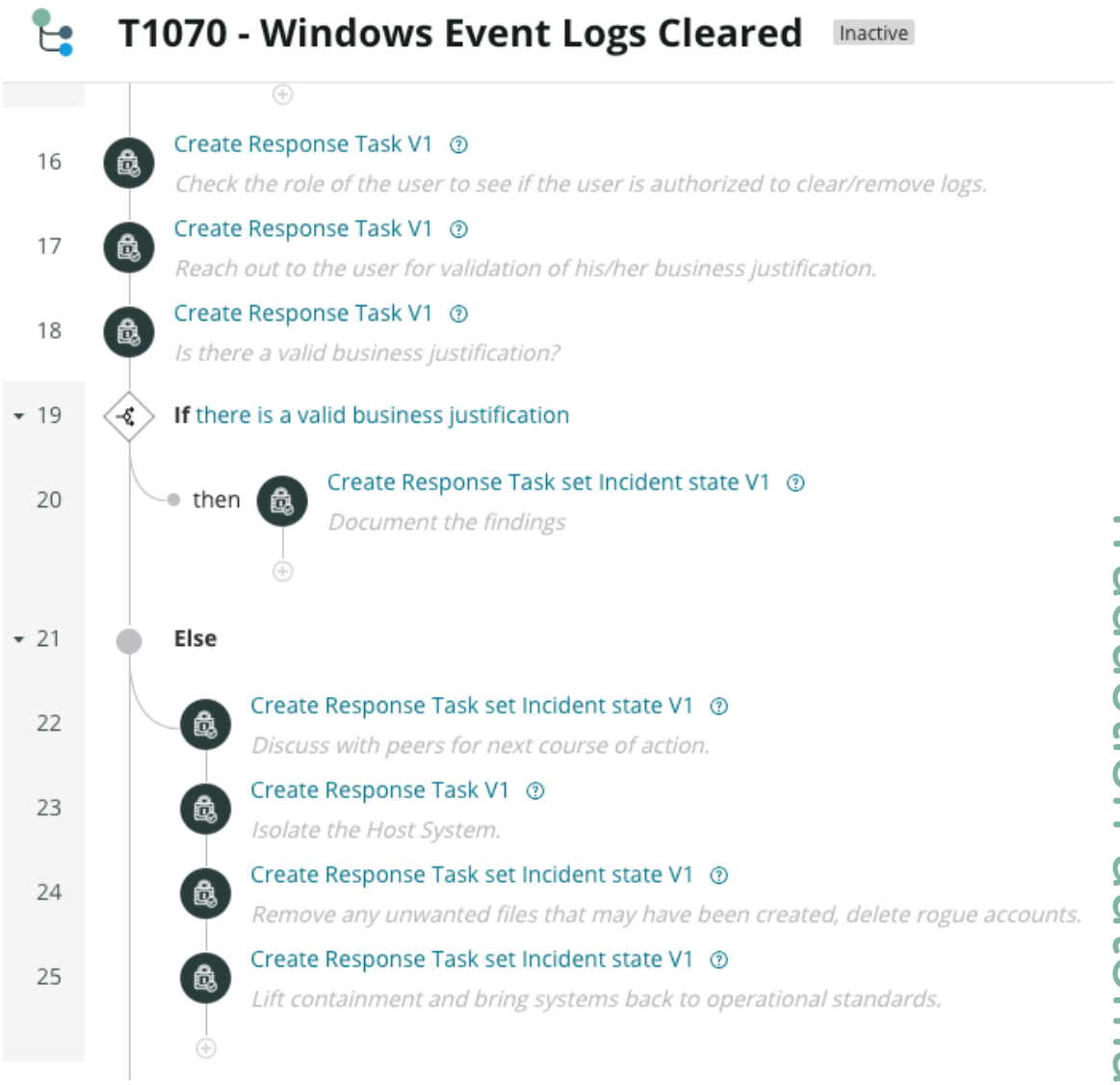
4. Dans l'action 16, si l'utilisateur a été identifié, vérifiez son rôle pour voir si l'utilisateur est autorisé à effacer ou à supprimer des journaux.

5. Dans l'action 17, contactez l'utilisateur pour valider sa justification commerciale.
Vous pouvez utiliser le modèle d'e-mail fourni pour contacter l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook T1070 - Journaux des événements Windows effacé



6. Dans l’action 18, vérifiez si une justification commerciale valide est fournie ou non.
7. Dans l’action 19, si une justification commerciale valide a été fournie, alors dans l’action 20, documentez les constatations jusqu’à présent.
   Le flux s’arrête.
8. Dans l’action 21, si aucune justification commerciale valable n’a été fournie, procédez comme suit :
   a. Dans l’action 22, discutez de la prochaine ligne de conduite avec vos pairs.
   b. Dans l’action 23, isolez le système hôte.
   c. Dans l’action 24, supprimez tous les fichiers indésirables qui ont pu être créés et supprimez les comptes non autorisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Dans l'action 25, levez le confinement et ramenez les systèmes aux normes opérationnelles.
Le flux s'arrête.

9. Dans l'action 26, effectuez l'examen post-incident avant de fermer la tâche.

Playbook pour OSrequête de l'adresse externe dans le fichier /etc/hosts

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents qui indiquent qu'un nom d'hôte ou un domaine interne a été affecté à une adresse IP externe sur le DNS local (/etc/hosts) d'un serveur Linux.

Configurer la requête de système d'exploitation de l'adresse externe dans le playbook de fichier /etc/hosts

Suivez les étapes suivantes pour configurer le OSquery de l'adresse externe dans le playbook de fichier /etc/hosts.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

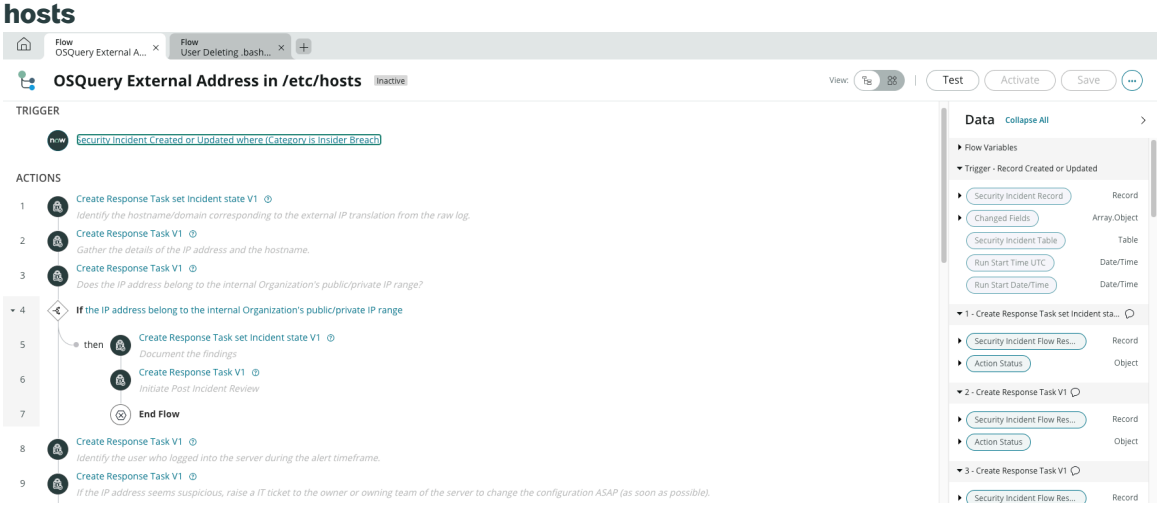
1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.

2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez **l'adresse externe OSquery dans le playbook /etc/hosts** .

3. Facultatif : Créez une copie de l'adresse externe OSquery dans le flux de playbook /etc/hosts et apportez les modifications nécessaires.

(Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de  , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

Requête du système d'exploitation de l'adresse externe dans le playbook /etc/hosts



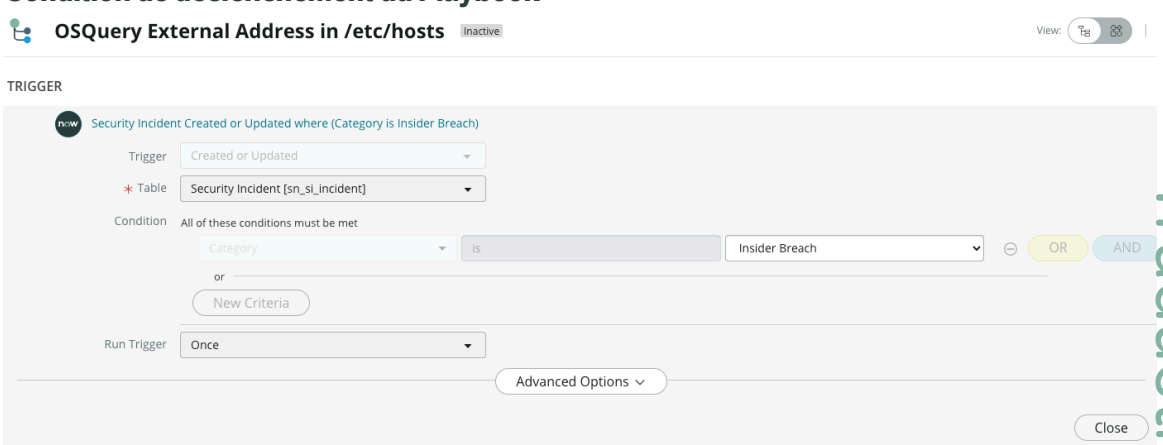
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Violation interne**.

Requête du système d'exploitation de l'adresse externe dans /etc/hosts Condition de déclenchement du Playbook



Utiliser la requête OS de l'adresse externe dans le playbook de fichier /etc/hosts

Utilisez ce playbook pour enquêter sur les incidents qui indiquent qu'un nom d'hôte ou un domaine interne a été affecté à une adresse IP externe sur le DNS (/etc/hosts) local d'un serveur Linux. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le OSquery de l'adresse externe dans le playbook de fichier /etc/hosts.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

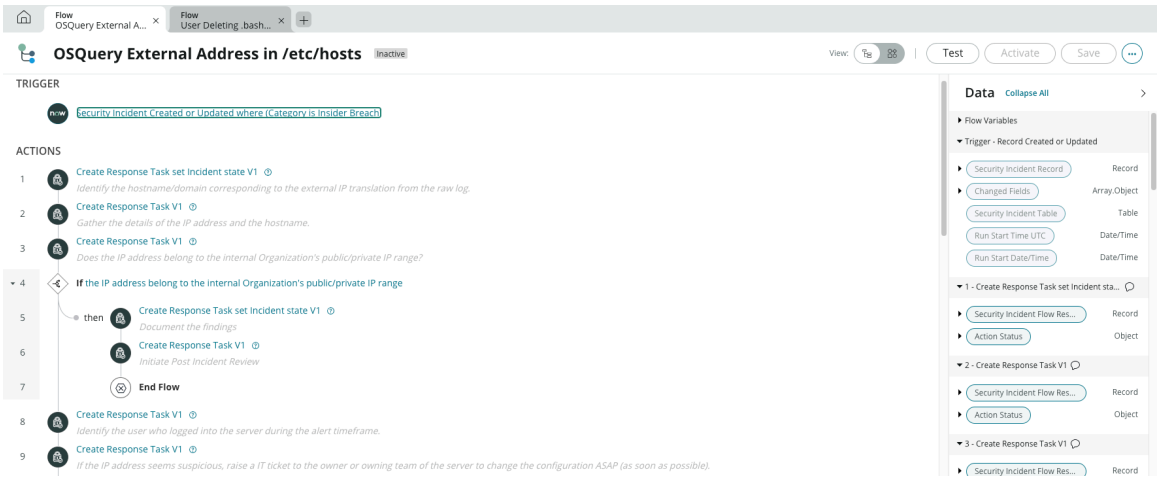
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, identifiez le nom d'hôte ou le nom de domaine correspondant à la traduction IP externe à partir du journal brut.
2. Dans l'action 2, rassemblez les détails de l'adresse IP et du nom d'hôte.
3. Dans l'action 3, vérifiez si cette adresse IP appartient ou non à la plage d'adresses IP publique/privée de l'organisation interne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Requête du système d'exploitation de l'adresse externe dans le playbook de fichier /etc/hosts



4. Dans l'action 4, si l'adresse IP appartient à la plage d'adresses IP publique/privée de l'organisation interne, procédez comme suit :

   a. Dans l'action 5, documentez les résultats obtenus jusqu'à présent.

   b. Dans l'action 6, lancez une revue post-incident.
   Dans l'action 7, après la revue post-incident, le flux s'arrête.

5. Si l'adresse IP n'appartient pas à la plage IP publique/privée de l'organisation interne, dans l'action 8, identifiez l'utilisateur qui s'est connecté au serveur pendant la période d'alerte.
6. Dans l'action 9, si l'adresse IP semble suspecte, soulevez un ticket informatique auprès du propriétaire ou de l'équipe du serveur pour modifier la configuration au plus vite.
7. Dans l'action 10, vérifiez s'il y a eu une activité malveillante sur le serveur avant et après l'ajout de l'entrée DNS.
8. Dans l'action 11, vérifiez toute connexion à l'adresse IP externe à partir du serveur.
9. Dans l'action 12, documentez les résultats obtenus jusqu'à présent.
10. Dans l'action 13, vérifiez si les informations du propriétaire ou de l'équipe sont disponibles ou non.
11. Dans l'action 14, si les informations du propriétaire ou de l'équipe sont disponibles, procédez comme suit :

    a. Dans l'action 15, contactez le propriétaire ou l'équipe du serveur pour voir s'ils reconnaissent l'activité.
    Vous pouvez utiliser le modèle d'e-mail fourni pour contacter le propriétaire ou l'équipe du serveur.

    b. Dans l'action 16, vérifiez si le propriétaire ou l'équipe a fourni une justification commerciale valide ou non.

    c. Dans l'action 17, si le propriétaire ou l'équipe fourni n'a pas fourni de justification commerciale valide, le flux s'arrête.
    Toutefois, si le propriétaire ou l'équipe a fourni une justification commerciale valide, procédez comme suit :

Traduction automatique

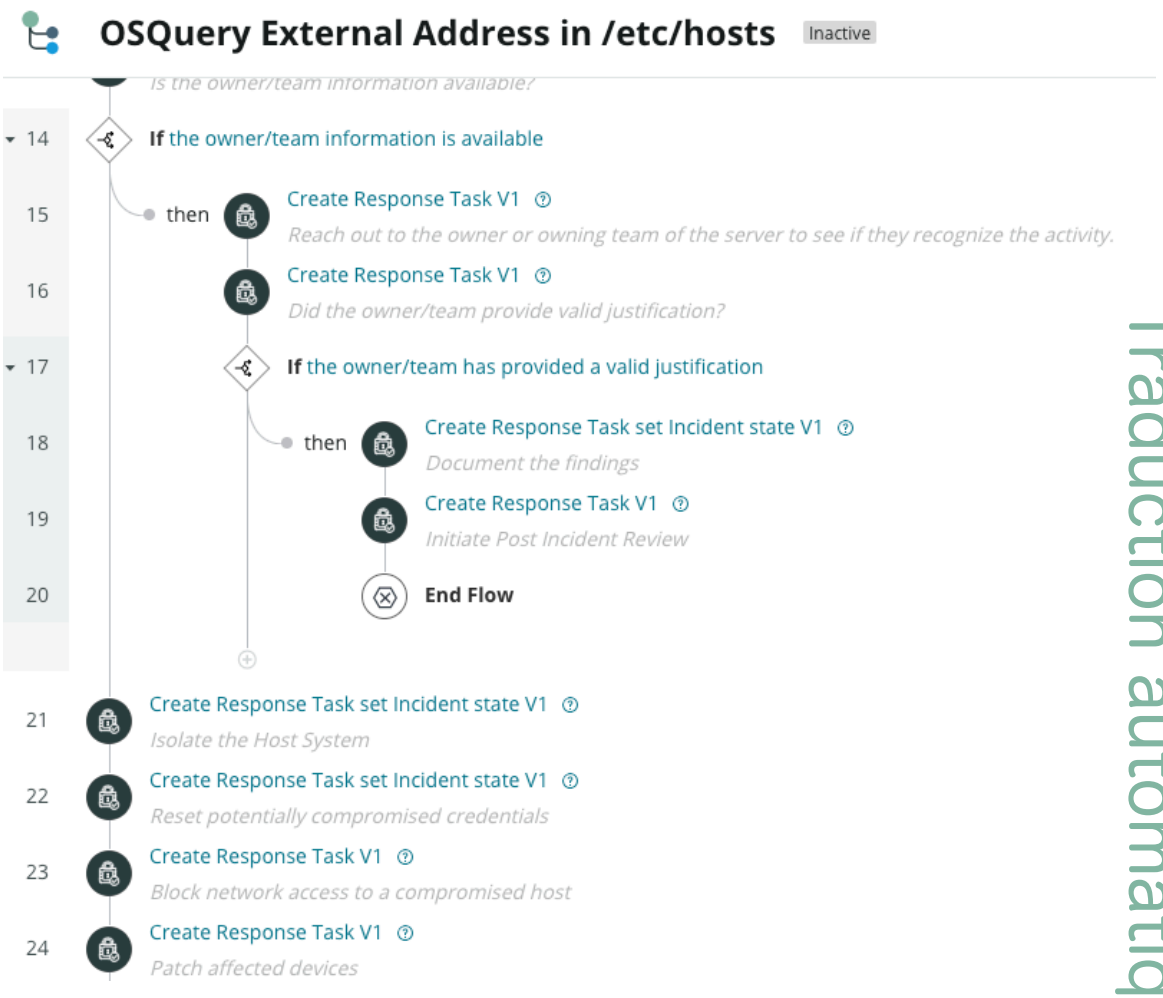
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Dans l'action 18, documentez les résultats obtenus jusqu'à présent.

ii. Dans l'action 19, lancez une revue post-incident.

Dans l'action 20, après la revue post-incident, le flux s'arrête.

Utilisation du OSquery de l'adresse externe dans le playbook de fichier /etc/hosts



12. Dans l'action 21, si les informations du propriétaire ou de l'équipe ne sont pas disponibles, isolez le système hôte.
13. Dans l'action 22, réinitialisez les informations d'identification potentiellement compromises.
14. Dans l'action 23, bloquez l'accès réseau à l'hôte compromis.
15. Dans l'action 24, corrigez les appareils affectés.
16. Dans l'action 25, lever le confinement et ramener les systèmes aux normes opérationnelles.
17. Dans l'action 26, effectuez l'examen post-incident avant de fermer la tâche.

Playbook pour la suppression de l'historique Bash par l'utilisateur : cloud

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents qui indiquent si quelqu'un a essayé de supprimer le fichier d'historique bash (`.bash_history`) d'un serveur Linux.

Remarque : Vous devez atténuer cette alerte avec prudence, car elle est rarement déclenchée et indique potentiellement une menace interne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la suppression du playbook d'historique Bash par l'utilisateur

Suivez les étapes suivantes pour configurer le playbook Utilisateur supprimant l'historique Bash.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

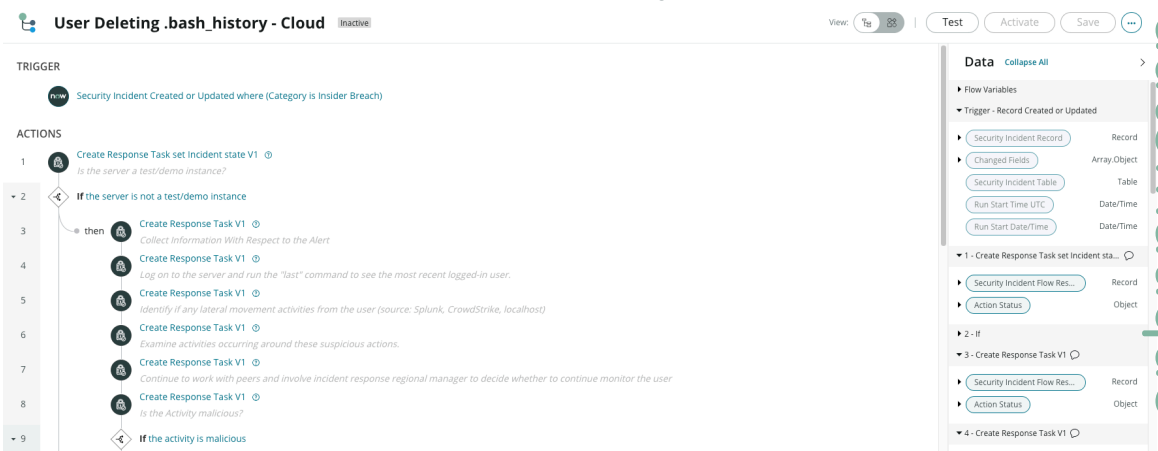
Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **Suppression de l'.bash_history utilisateur - Cloud** .
3. **Facultatif :** Créer une copie du flux Playbook Suppression de l'utilisateur .bash_history - Cloud et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

Utilisateur supprimant l'historique Bash : Cloud Playbook



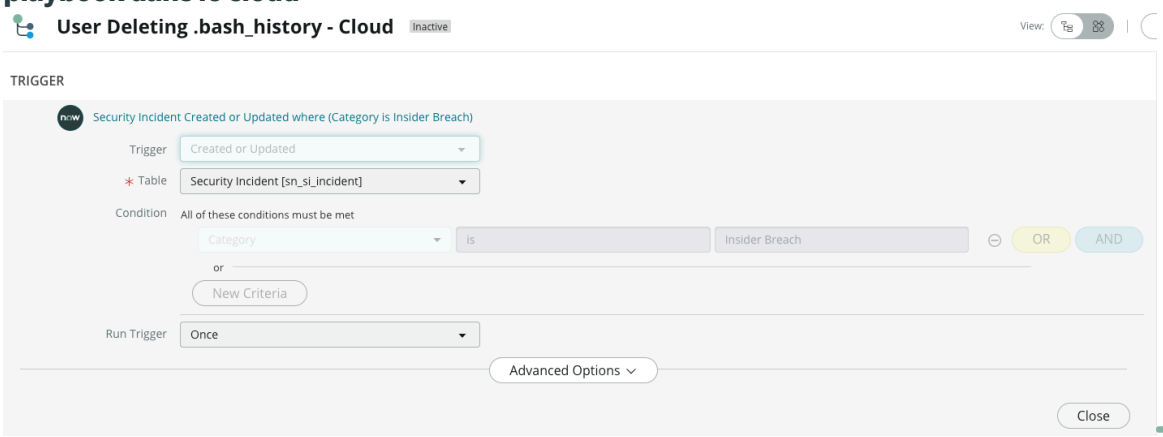
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Violation interne**.

Utilisateur supprimant l'historique Bash : condition de déclenchement du playbook dans le cloud



Utiliser le playbook de suppression de l'historique Bash par l'utilisateur

Utilisez ce playbook pour enquêter sur les incidents qui indiquent si quelqu'un a essayé de supprimer le fichier d'historique bash d'un serveur Linux. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Utilisateur supprimant l'historique Bash (`.bash_history`).

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vérifiez si le serveur est une instance de test ou de démonstration.
2. Dans l'action 2, si le serveur n'est pas une instance de test ou de démonstration, procédez comme suit :

   a. Dans l'action 3, collectez les informations suivantes pour l'alerte :
      - Nom d'utilisateur
      - Adresse IP
      - Commandes malveillantes tentant de supprimer l'historique bash
      - Toutes les commandes exécutées par l'utilisateur, si elles sont disponibles dans les journaux CrowdStrike.

   b. Dans l'action 4, connectez-vous au serveur et exécutez la `dernière` commande pour afficher l'utilisateur connecté le plus récemment.

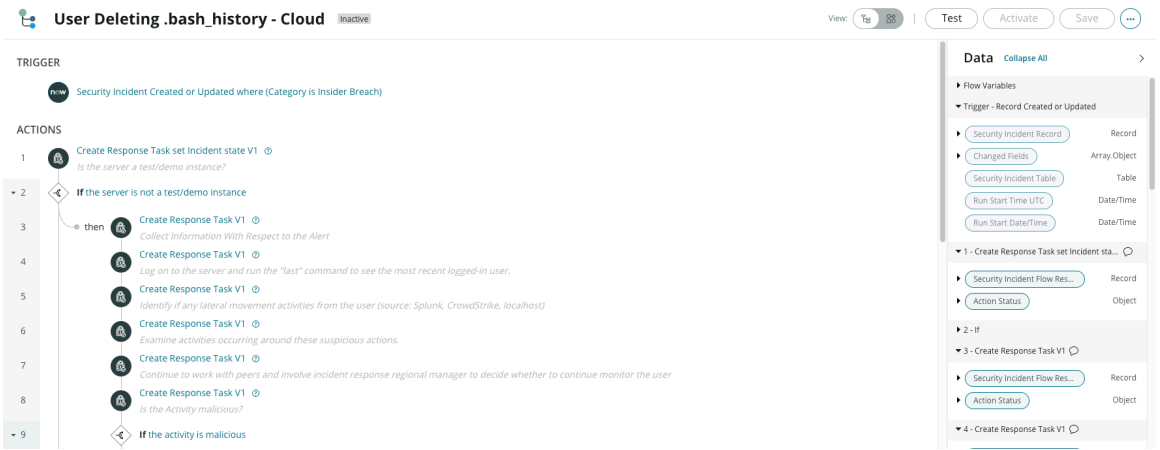
   c. Dans l'action 5, identifiez s'il y a eu des activités de mouvement latéral de la part de l'utilisateur (source : Splunk, CrowdStrike, localhost).

   d. Dans l'action 6, examinez les activités qui se produisent autour de ces actions suspectes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur supprimant le playbook d'historique de Bash



e. Dans l'action 7, continuez à travailler avec vos pairs et impliquez le responsable régional de la réponse aux incidents dans la décision de continuer à surveiller l'utilisateur.

f. Dans l'action 8, déterminez si l'activité est malveillante ou non.

g. Dans l'action 9, si l'activité est malveillante, effectuez les étapes suivantes :

i. Dans l'action 10, au cours de l'enquête, contactez le support informatique et demandez un gel de compte.

ii. Dans l'action 11, assurez-vous que l'instance est restaurée à un état normal exempt d'activité malveillante.

iii. Dans l'action 12, lever le confinement et ramener les systèmes aux normes opérationnelles.

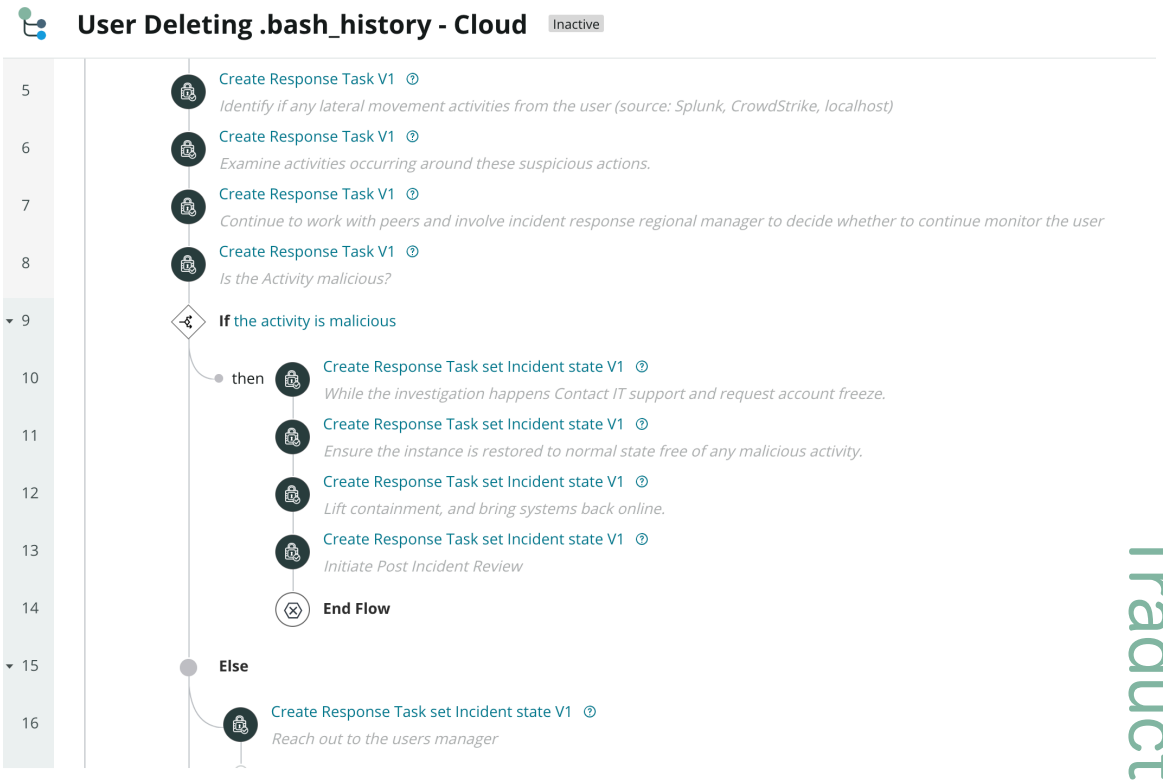
iv. Dans l'action 13, lancez une revue post-incident.

Dans l'action 14, après la revue post-incident, le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook de suppression de l'historique Bash par l'utilisateur



h. Dans l'action 15, si l'activité n'est pas malveillante, dans l'action 16, contactez le responsable de l'utilisateur.
Vous pouvez utiliser le modèle d'e-mail fourni pour contacter le responsable de l'utilisateur et l'informer de l'approche recommandée.

3. Dans l'action 17, documentez les résultats obtenus jusqu'à présent.

4. Dans l'action 18, effectuez l'examen post-incident avant de fermer la tâche.

Playbook pour les tentatives VPN réussies à partir des comptes de service - Entreprise/Cloud

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents qui suivent les tentatives de connexion réussies à partir de comptes de service via VPN. Les comptes de services ne sont pas censés avoir des événements de connexion à partir d'un VPN, et de tels événements peuvent être des indicateurs de force brute ou d'exposition possible des informations d'identification du compte.

Configurer le playbook Tentatives VPN réussies à partir du playbook Comptes de services

Suivez les étapes suivantes pour configurer les tentatives VPN réussies à partir du playbook Comptes de services.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Traduction automatique

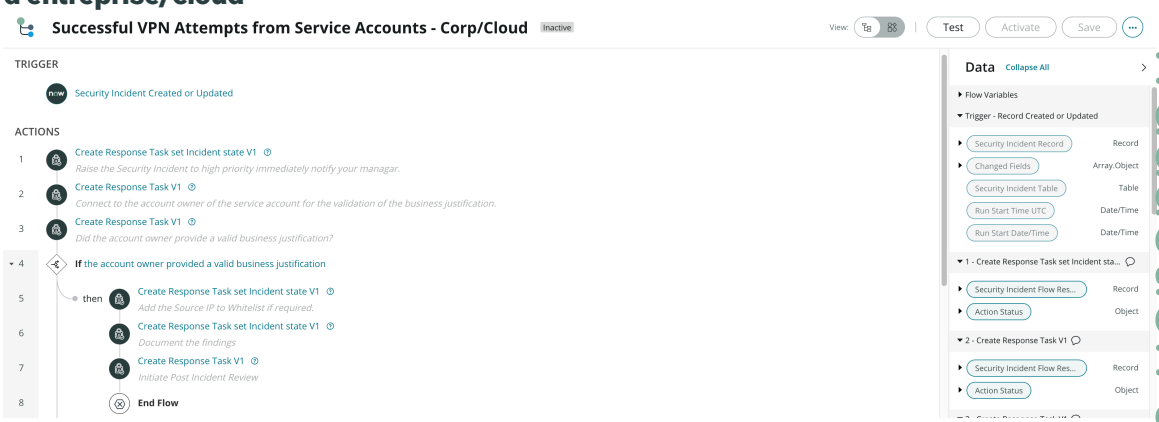
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez **Tentatives VPN réussies dans le playbook Comptes de service** .
3. **Facultatif :** Créez une copie du flux de playbook Tentatives VPN réussies à partir des comptes de service et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de ••• , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

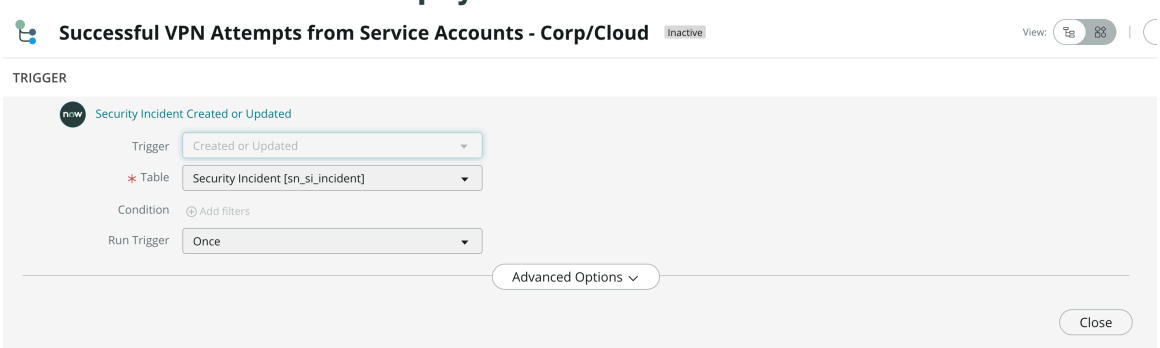
Tentatives VPN réussies à partir des comptes de services - Playbook d'entreprise/cloud



4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

   Ce playbook est déclenché et associé à l'incident de sécurité lorsque l'incident de sécurité est créé ou mis à jour en fonction de vos conditions requises. Par exemple, lorsque **la catégorie** est **Violation interne**.

Tentatives VPN réussies à partir des comptes de services : entreprise/cloud Condition de déclenchement du playbook



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser le playbook Tentatives VPN réussies à partir du playbook Comptes de services

Utilisez ce playbook pour enquêter sur les incidents qui suivent les tentatives de connexion réussies à partir de comptes de service via VPN. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Tentatives VPN réussies à partir du playbook Comptes de services.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, passez l'incident de sécurité en priorité élevée et informez immédiatement votre gestionnaire.
2. Dans l'action 2, contactez le propriétaire du compte de service pour valider la justification commerciale. Vous pouvez utiliser le modèle d'e-mail fourni pour contacter le propriétaire du compte de service afin de valider la justification commerciale.
3. Dans l'action 3, vérifiez si le propriétaire du compte de service a fourni une justification commerciale valide.



4. Dans l'action 4, si le propriétaire du compte de service a fourni une justification commerciale valide, procédez comme suit :

   a. Dans l'action 5, ajoutez l'adresse IP source à la liste d'autorisation si nécessaire.

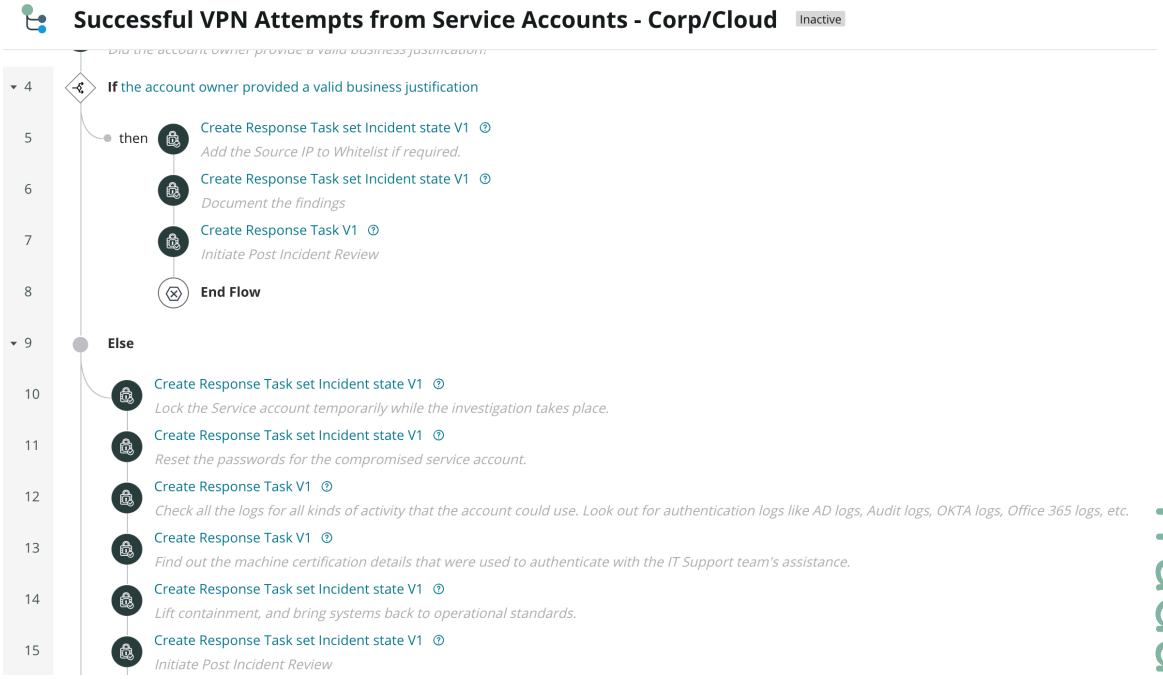
   b. Dans l'action 6, documentez les résultats obtenus jusqu'à présent.

   c. Dans l'action 7, lancez une revue post-incident.
   Dans l'action 8, après la revue post-incident, le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation des tentatives VPN réussies à partir du playbook Comptes de services - Entreprise/Cloud



5. Dans l'action 9, si le propriétaire du compte de service n'a pas fourni de justification commerciale valide, procédez comme suit :

a. Dans l'action 10, verrouillez temporairement le compte de service pendant l'enquête.

b. Dans l'action 11, réinitialisez les mots de passe du compte de service compromis.

c. Dans l'action 12, vérifiez les journaux pour toutes sortes d'activités que le compte pourrait utiliser. Recherchez les journaux d'authentification tels que les journaux Active Directory, les journaux d'audit, les journaux Okta, les journaux Office 365, entre autres.

d. Dans l'action 13, recherchez les détails de certification de l'ordinateur utilisés pour vous authentifier avec l'aide de l'équipe d'assistance informatique.

e. Dans l'action 14, lever le confinement et ramener les systèmes aux normes opérationnelles.

f. Dans l'action 15, effectuez la revue post-incident avant de fermer la tâche.

Playbook pour les tentatives d'accès aux comptes désactivés

Ce playbook se déclenche lorsqu'un employé dont le compte est résilié, désactivé ou séparé tente de se connecter avec ses informations d'identification. L'état d'identité de l'utilisateur dans le point de voile est généralement mis à jour sur désactivé à sa date de résiliation.

30 jours est le délai idéal à partir de la date d'arrêt pour qu'il soit mis à jour vers un état distinct. Vous pouvez utiliser la logique métier dans Point de navigation pour supprimer les comptes RSA et supprimer les adhésions au groupe Active Directory (AD) après 30 jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer le playbook de tentative d'accès au compte désactivé

Procédez comme suit pour configurer le playbook de tentative d'accès au compte désactivé.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **Compte désactivé de tentative d'accès** .
3. **Facultatif :** Créer une copie du flux de playbook Compte désactivé de tentative d'accès et apporter les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.



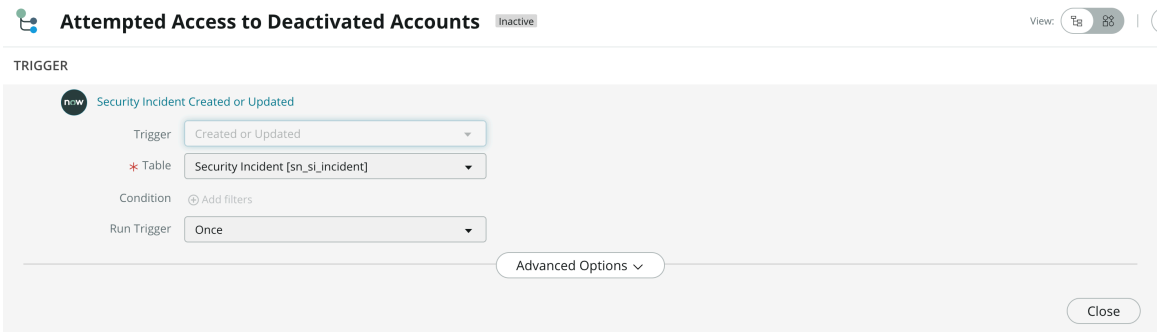
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché lorsque l'incident de sécurité est créé ou mis à jour en fonction des conditions requises. Par exemple, lorsque **la catégorie** est **Violation d'initié**

Tentative d'accès aux comptes désactivés Condition de déclenchement du Playbook



Utiliser le playbook de tentative d'accès aux comptes désactivés

Utilisez ce playbook lorsqu'un employé dont le compte est résilié, désactivé ou séparé tente de se connecter avec ses informations d'identification. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Tentative d'accès aux comptes désactivés.

Avant de commencer

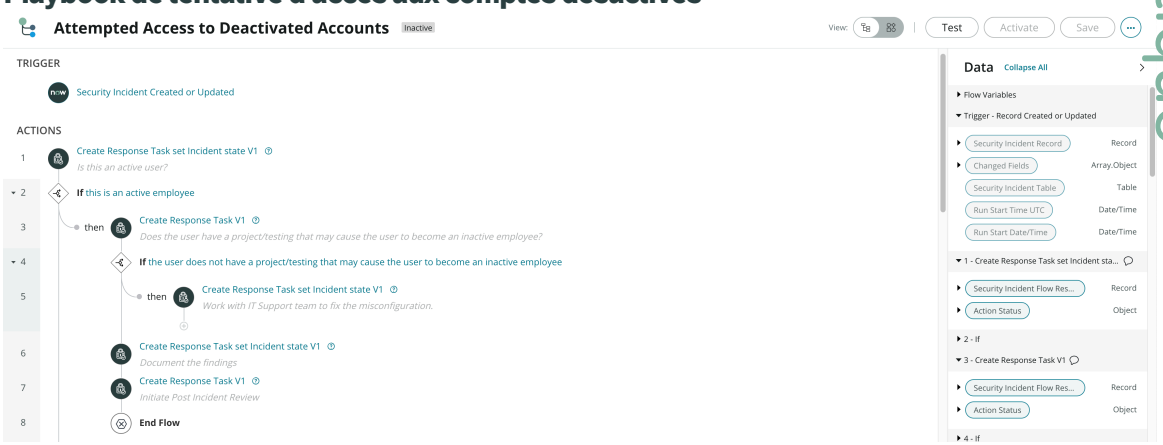
Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vérifiez si la tentative d'accès aux comptes désactivés a été effectuée par un utilisateur actif.
2. Dans l'action 2, vérifiez si la tentative d'accès aux comptes désactivés a été effectuée par un employé actif.

Playbook de tentative d'accès aux comptes désactivés



3. Si la tentative d'accès aux comptes désactivés a été faite par un employé actif, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans l'action 3, vérifiez si l'utilisateur avait un projet ou un scénario de test qui a entraîné l'inactivité de l'employé.

b. Dans l'action 4, si l'utilisateur n'avait pas de projet ou de scénario de test qui l'a amené à devenir un employé inactif, travaillez avec l'équipe d'assistance informatique pour corriger la mauvaise configuration. Le flux s'arrête.

c. Dans l'action 5, si l'utilisateur avait un projet ou un scénario de test qui l'a amené à devenir un employé inactif, procédez comme suit :

i. Dans l'action 6, documentez les résultats obtenus jusqu'à présent.

ii. Dans l'action 7, lancez une revue post-incident.

Dans l'action 8, après la revue post-incident, le flux s'arrête.

4. Dans l'action 9, si la tentative d'accès au compte désactivé n'a pas été faite par un employé actif, effectuez les étapes suivantes :

a. Dans l'action 10, vérifiez si l'utilisateur s'est connecté avec succès.

b. Dans l'action 11, vérifiez quand l'employé a été licencié.

c. Dans l'action 12, examinez les événements sur Splunk pour examiner les activités de l'utilisateur au cours de la période.

d. Dans l'action 13, sur la base de l'enquête menée jusqu'à présent, déterminez si l'utilisateur a exfiltré des données.

e. Dans l'action 14, si l'utilisateur n'a exfiltré aucune donnée, procédez comme suit :

i. Dans l'action 15, collaborez avec l'équipe d'assistance informatique pour mettre fin à toutes les sessions actives et désactiver les comptes.

ii. Dans l'action 16, documentez les résultats obtenus jusqu'à présent.

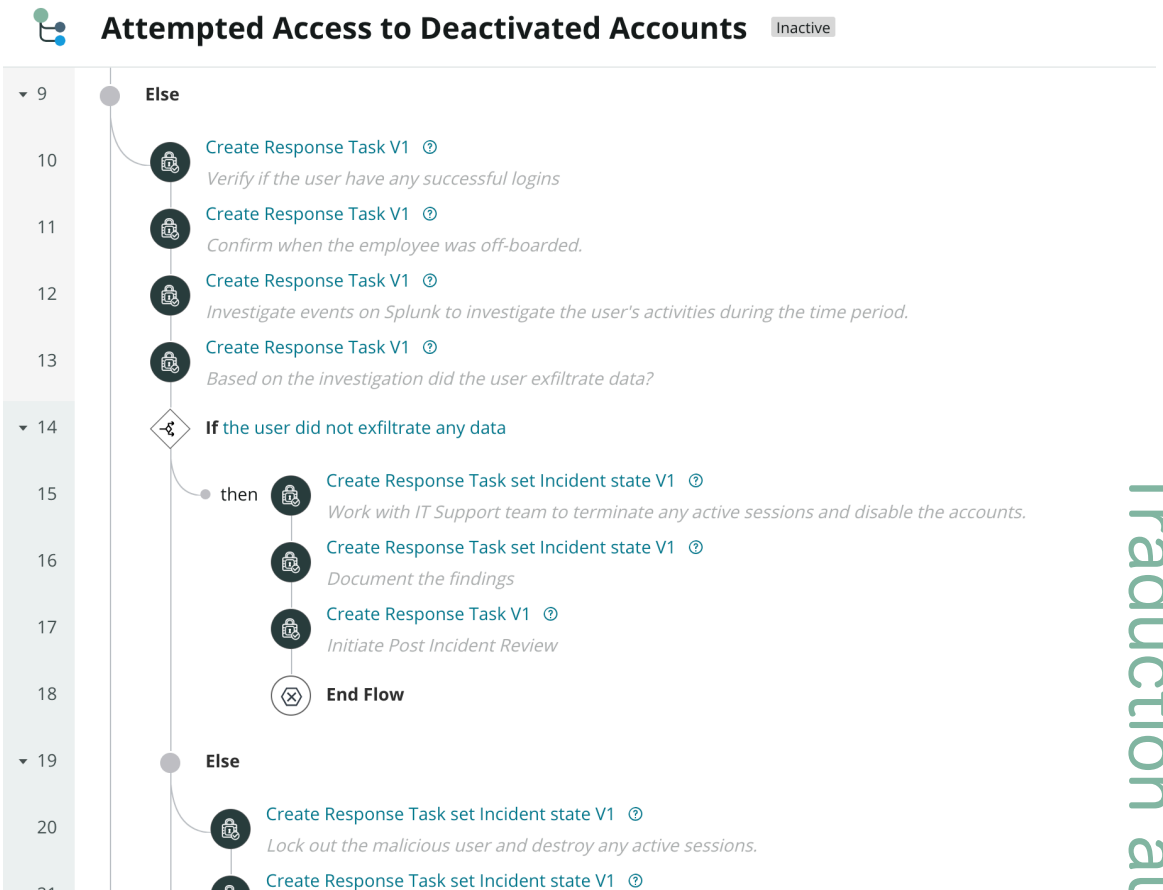
iii. Dans l'action 17, lancez une revue post-incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l’action 18, après la revue post-incident, le flux s’arrête.

Utilisation du playbook de tentative d’accès aux comptes désactivés



5. Dans l’action 19, si l’utilisateur a exfiltré des données, procédez comme suit :

a. Dans l’action 20, verrouillez l’utilisateur malveillant et détruisez toutes les sessions actives.

b. Dans l’action 21, travaillez avec l’équipe d’assistance informatique pour désactiver tous les comptes.

c. Dans l’action 22, assurez-vous que les ressources sont restaurées à l’état normal et exemptes de toute activité malveillante.
Vous pouvez recréer l’image des ressources si nécessaire.

d. Dans l’action 23, lever le confinement et ramener les systèmes aux normes opérationnelles.

e. Dans l’action 24, effectuez l’examen post-incident avant de fermer la tâche.

Playbook pour T1003 - Évasion de défense - Mimikatz DCShadow

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents soupçonnés d’être causés par Mimikatz DCShadow. DCShadow est une fonctionnalité de Mimikatz qui simule le comportement d’un contrôleur de domaine (un serveur contrôlant Active Directory) pour injecter ses propres données, contournant ainsi la plupart des contrôles de sécurité standard (y compris les SIEM).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mimikatz DCShadow aide l'attaquant à établir un contrôleur de domaine (DC) malveillant qui devient une partie d'Active Directory (AD). Une fois enregistré, il peut agir comme un DC légitime et causer des dommages.

Configurer le playbook T1003 - Defense Evasion - Mimikatz DCShadow

Procédez comme suit pour configurer le playbook T1003 - Defense Evasion - Mimikatz DCShadow.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

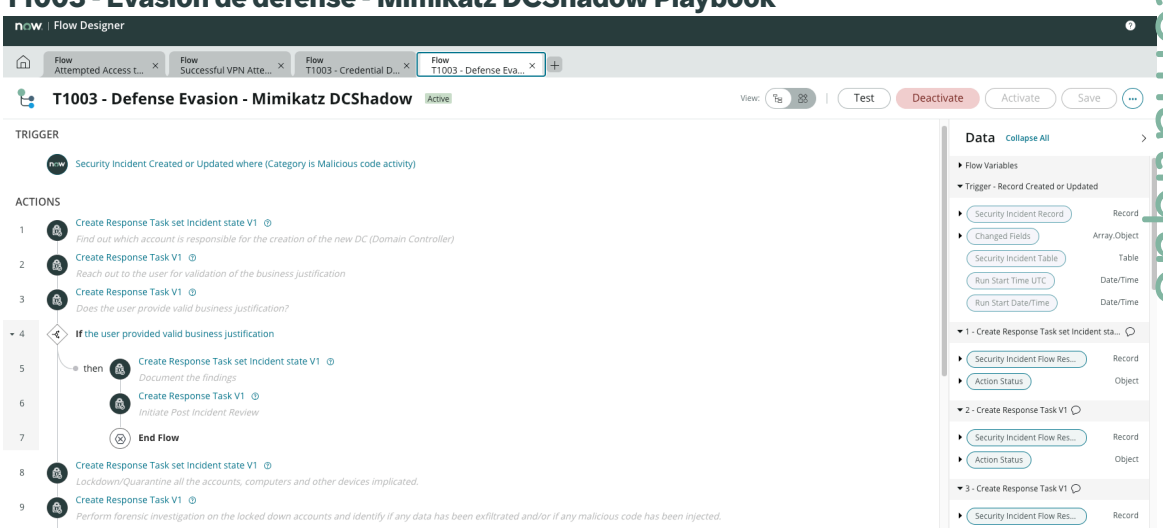
Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **T1003 - Defense Evasion - Mimikatz DCShadow** .
3. **Facultatif :** Créez une copie du flux de playbook T1003 - Defense Evasion - Mimikatz DCShadow et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

   T1003 - Évasion de défense - Mimikatz DCShadow Playbook

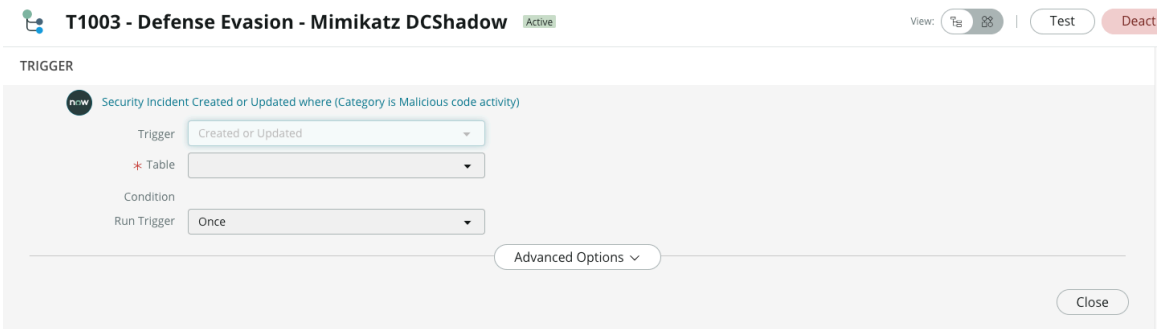
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Activité de code malveillant**.

T1003 : évasion de défense : Mimikatz DCShadow Condition de déclenchement du Playbook



Utiliser le playbook T1003 - Defense Evasion - Mimikatz DCShadow

Utilisez ce manuel pour enquêter sur les incidents de sécurité soupçonnés d'être causés par Mimikatz DCShadow. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook T1003 - Defense Evasion - Mimikatz DCShadow.

Avant de commencer

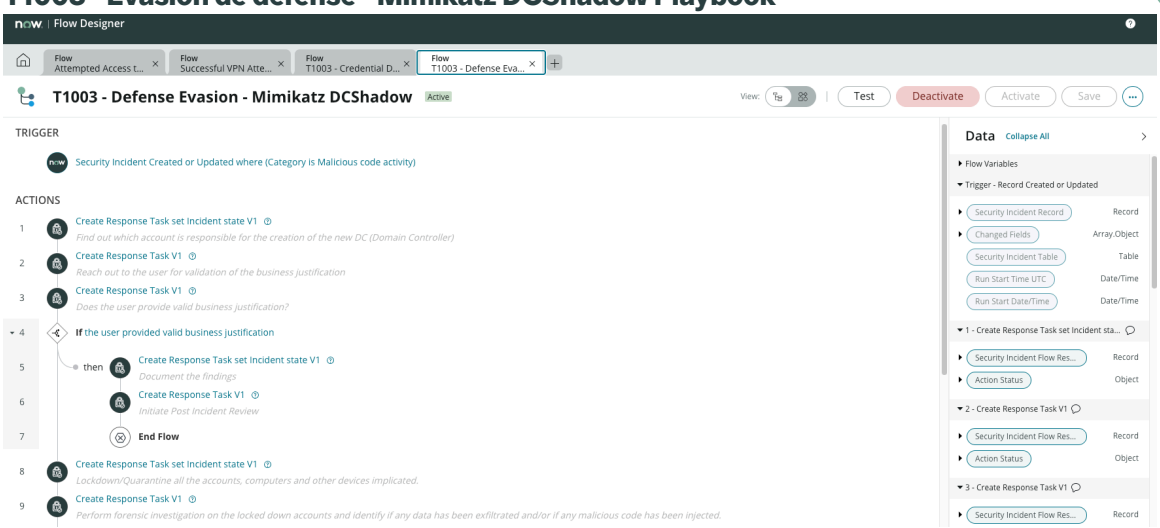
Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, découvrez quel compte est responsable de la création du nouveau DC (contrôleur de domaine).
2. Dans l'action 2, contactez l'utilisateur pour valider la justification commerciale.
   Vous pouvez utiliser le modèle d'e-mail fourni pour contacter l'utilisateur.
3. Dans l'action 3, vérifiez si l'utilisateur a fourni une justification commerciale valide.
4. Dans l'action 4, si l'utilisateur a fourni une justification commerciale valide, procédez comme suit :

T1003 - Évasion de défense - Mimikatz DCShadow Playbook



Traduction automatique

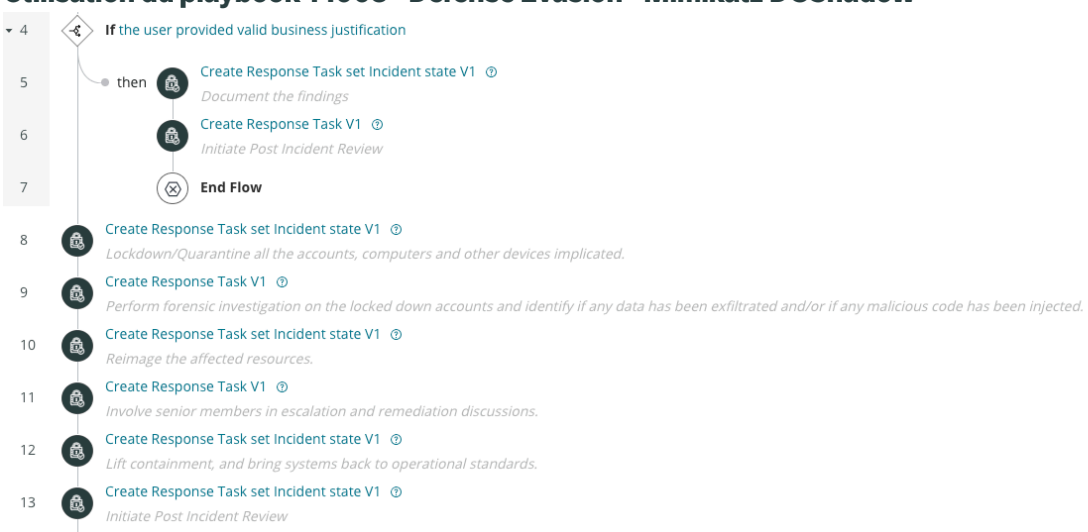
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans l'action 5, documentez les résultats obtenus jusqu'à présent.

b. Dans l'action 6, lancez une revue post-incident.
Dans l'action 7, après la revue post-incident, le flux s'arrête.

5. Dans l'action 8, si l'utilisateur n'a pas fourni de justification commerciale valide, procédez comme suit :

Utilisation du playbook T1003 - Defense Evasion - Mimikatz DCShadow



a. Dans Action 9, verrouillez ou mettez en quarantaine tous les comptes, ordinateurs et autres appareils impliqués.

b. Dans l'action 10, effectuez une enquête médico-légale sur les comptes verrouillés et identifiez si des données ont été exfiltrées ou si un code malveillant a été injecté.

c. Dans l'action 11, réimagez les ressources affectées.

d. Dans l'action 12, lever le confinement et ramener les systèmes aux normes opérationnelles.

e. Dans l'action 13, effectuez l'examen post-incident avant de fermer la tâche.

Playbook pour T1003 - Dumping d'informations d'identification - Mimikatz DCSync

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents soupçonnés d'être causés par Mimikatz DCSync. Ce playbook se déclenche lorsqu'une des fonctions Mimikatz (`lsadump ::d csync`) est utilisée. La fonction est généralement utilisée sur les contrôleurs de domaine (DC) attaqués.

Mimikatz est un outil de piratage populaire qui permet aux utilisateurs d'émettre des commandes qui aident à récupérer les données confidentielles du système attaqué. Les données confidentielles comprennent les mots de passe, leurs hachages et autres.

Remarque : Il s'agit d'une alerte haute fidélité, qui est supposée être rarement déclenchée. Lorsqu'il se déclenche, vous devez en informer immédiatement un membre senior de l'équipe ou un responsable.

Configurer le playbook T1003 - Dumping d'informations d'identification - Mimikatz DCsync

Suivez les étapes suivantes pour configurer le playbook T1003 - Credential Dumping - Mimikatz DCsync.

Avant de commencer
Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_si.admin
- flow_designer

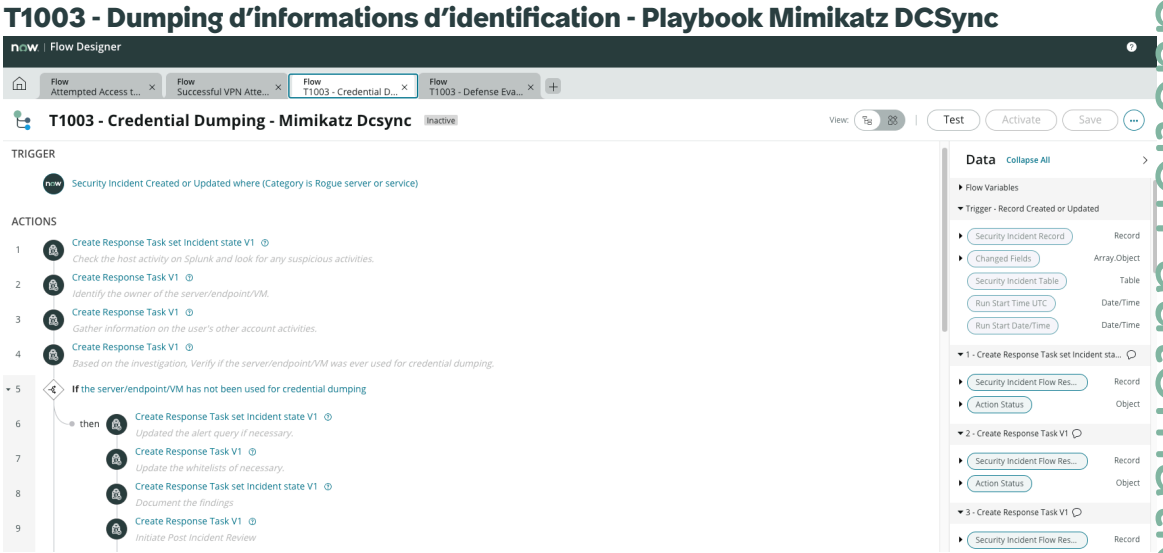
Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **T1003 - Credential Dumping - Mimikatz DCsync** .
3. **Facultatif :** Créez une copie du flux de playbook T1003 - Credential Dumping - Mimikatz DCsync et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

T1003 - Dumping d'informations d'identification - Playbook Mimikatz DCSync



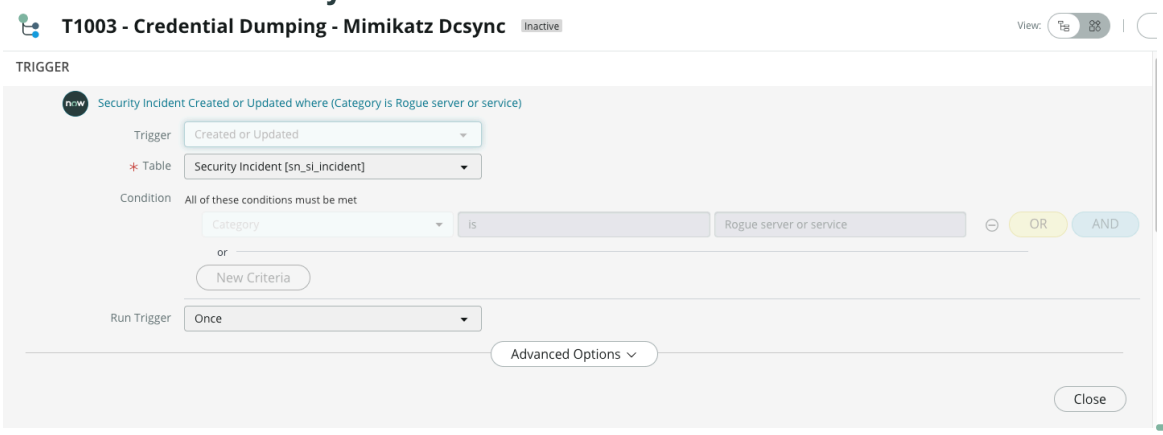
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Serveur ou service non autorisé**.

T1003 - Dumping d'informations d'identification - Mimikatz DCSync Condition de déclenchement du Playbook



Utiliser le playbook T1003 - Dumping d'informations d'identification - Mimikatz DCsync

Utilisez ce playbook pour enquêter sur les incidents soupçonnés d'être causés par Mimikatz DCSync. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook T1003 - Credential Dumping - Mimikatz DCsync.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

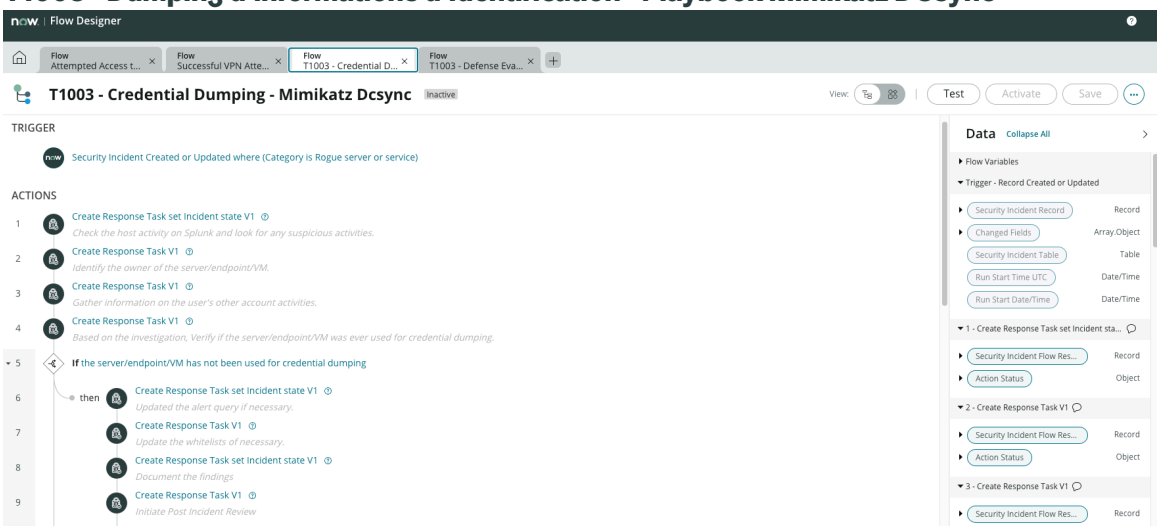
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vérifiez l'activité de l'hôte sur Splunk et recherchez toute activité suspecte.
2. Dans l'action 2, identifiez le propriétaire du serveur/point de terminaison/VM.
   Si l'utilisateur est en ligne, exécutez l'EDR CrowdStrike pour obtenir une meilleure portée des activités du système.
3. Dans l'action 3, rassemblez des informations sur les autres activités du compte de l'utilisateur.
4. Dans l'action 4, sur la base de l'enquête, vérifiez si le serveur/point de terminaison/ordinateur virtuel a déjà été utilisé pour le dumping d'informations d'identification.
5. Dans l'action 5, si le serveur/point de terminaison/VM n'a pas été utilisé pour le dumping des informations d'identification, effectuez les actions suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

T1003 - Dumping d'informations d'identification - Playbook Mimikatz DCsync



a. Dans l'action 6, mettez à jour la requête d'alerte si nécessaire.

b. Dans l'action 7, mettez à jour la liste d'autorisation si nécessaire.

c. Dans l'action 8, documentez les résultats obtenus jusqu'à présent.

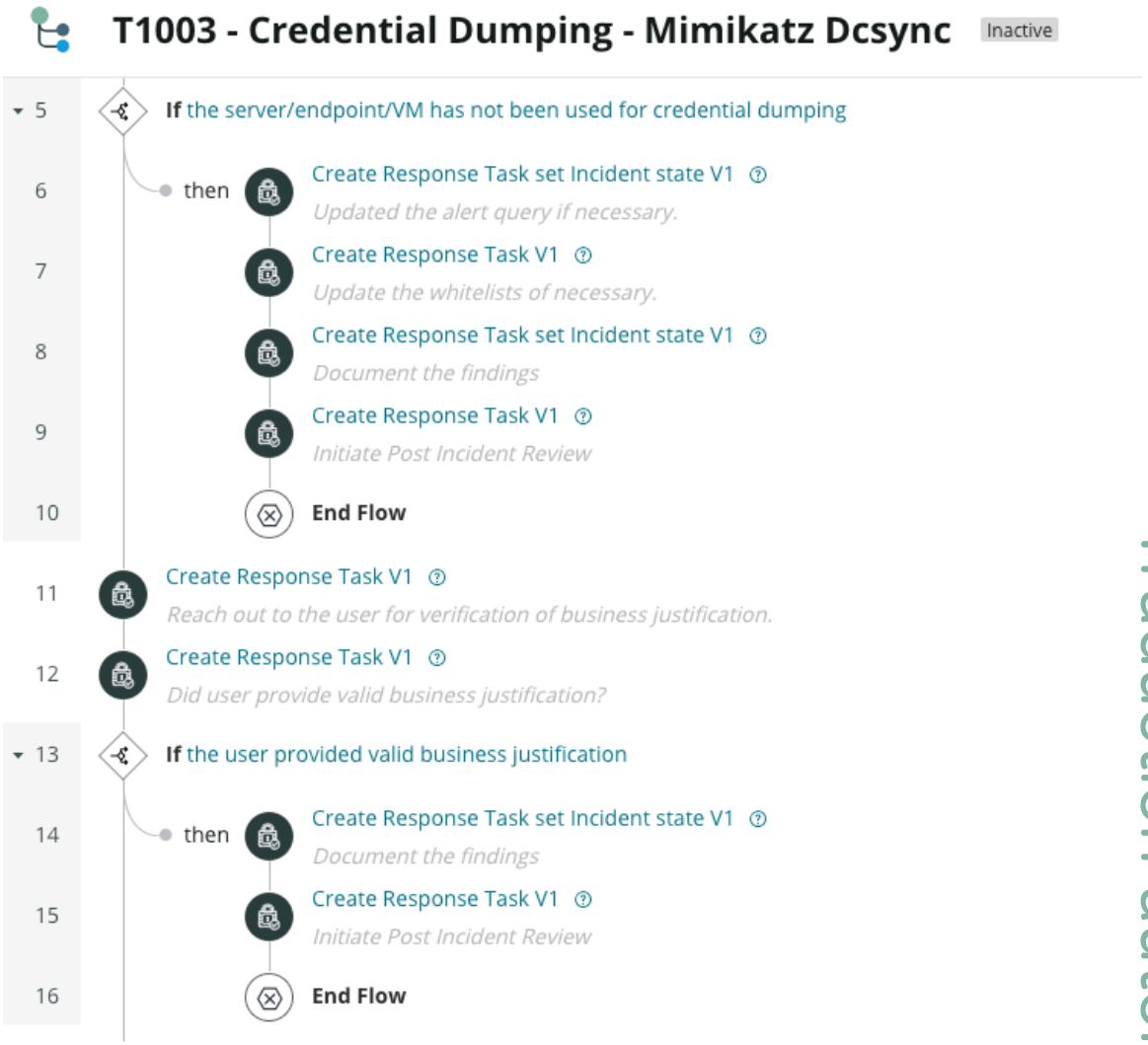
d. Dans l'action 9, lancez une revue post-incident.
Dans l'action 10, le flux s'arrête.

6. Si le serveur/point de terminaison/VM a été utilisé pour le dumping des informations d'identification, lors de l'action 11, contactez l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook T1003 - Credential Dumping - Mimikatz DCsync



7. Dans l'action 12, contactez l'utilisateur pour valider la justification commerciale.
8. Dans l'action 13, si l'utilisateur a fourni une justification commerciale valide, effectuez les actions suivantes :
   a. Dans l'action 14, documentez les résultats obtenus jusqu'à présent.
   b. Dans l'action 15, lancez une revue post-incident.
      Dans l'action 16, le flux s'arrête.
9. Si l'utilisateur n'a pas fourni de justification commerciale valide, lors de l'action 17, mettez le système en quarantaine.
10. Dans Action 18, supprimez tous les fichiers indésirables qui ont pu être créés ou supprimés par les comptes malveillants.
11. Dans l'action 19, lever le confinement et ramener les systèmes aux normes opérationnelles.
12. Dans l'action 20, effectuez la revue post-incident avant de fermer la tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Playbook pour les utilisateurs Okta Échecs de connexion à partir de plusieurs adresses IP

Ce playbook fournit des étapes de remédiation systématiques pour enquêter sur les incidents liés aux échecs de connexion des utilisateurs sur Okta.

Le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP fournit des instructions sur l'analyse de l'alerte lorsque des défaillances de compte ServiceNow sont observées sur Okta à partir de plusieurs adresses IP non ServiceNow. L'alerte associée à ce playbook vérifie les journaux Okta. Il déclenche une alerte en cas d'échec de connexion pour les ID d'utilisateurs ServiceNow de plus de trois plages d'adresses IP non-ServiceNow sur une durée d'une heure.

Configurer le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP

Suivez les étapes suivantes pour configurer le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

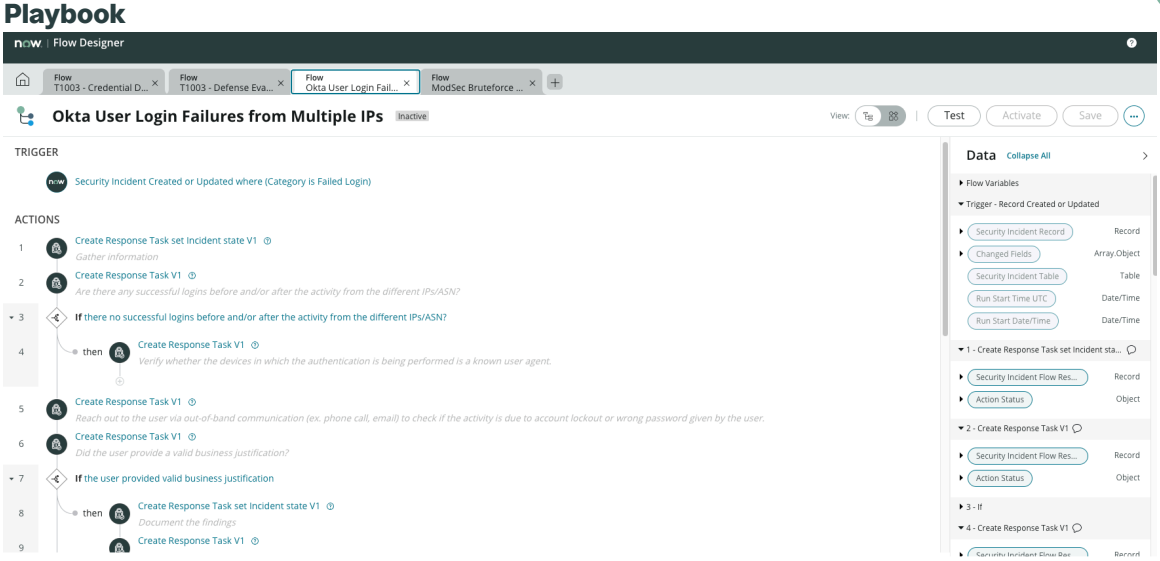
Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **Échecs de connexion des utilisateurs Okta à partir de plusieurs adresses IP** .
3. **Facultatif :** Créez une copie du flux de playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône de ••• , puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.

Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP Playbook

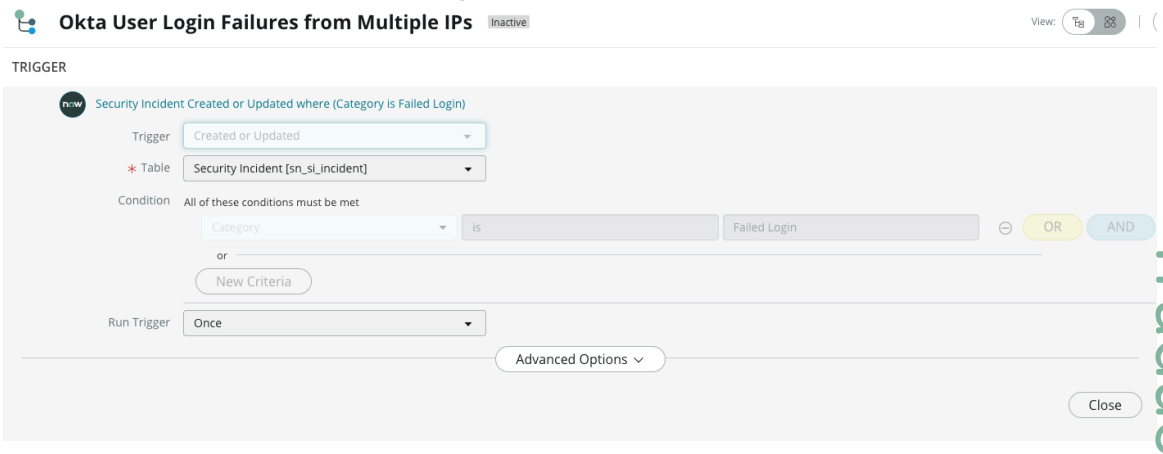


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque la **catégorie** est **Échec de** connexion.

Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP
Condition de déclenchement du Playbook



Utiliser le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP

Utilisez ce playbook pour enquêter sur les incidents de sécurité liés aux échecs de connexion des utilisateurs sur Okta. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

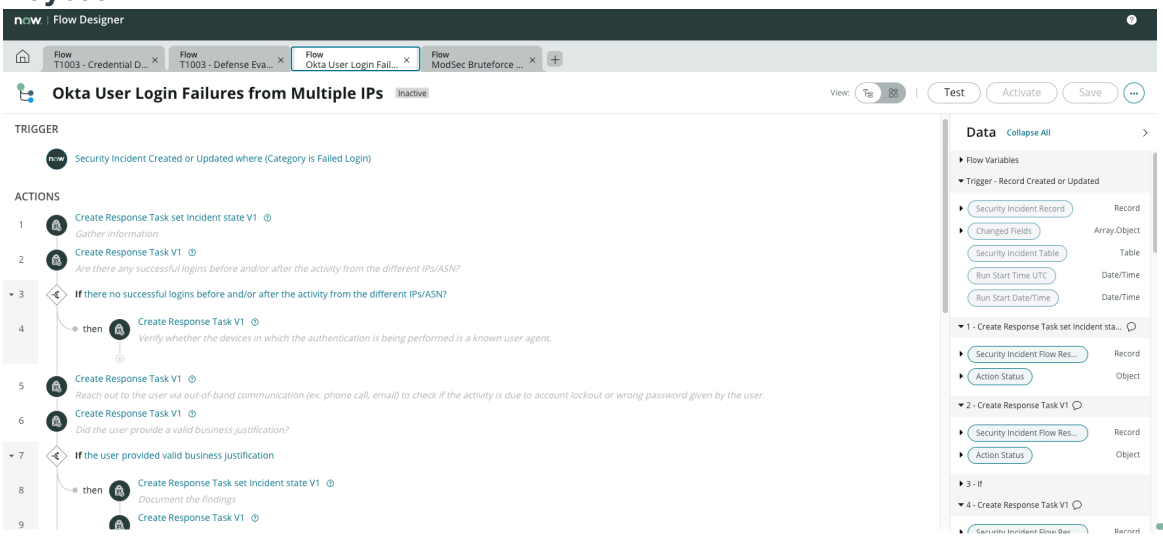
Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, effectuez les tâches suivantes :
   - Identifiez le compte d'utilisateur ciblé.
   - Vérifiez le sous-réseau IP et vérifiez s'ils appartiennent tous au même propriétaire du numéro de système autonome (ASN).
2. Dans l'action 2, vérifiez s'il y a eu des connexions réussies avant ou après l'activité à partir des différentes adresses IP/ASN.
3. Dans l'action 3, s'il n'y a pas eu de connexions réussies avant ou après l'activité à partir des différentes adresses IP/ASN, dans l'action 4, vérifiez si les appareils dans lesquels l'authentification est effectuée sont des agents utilisateur connus.
   Si les appareils sont authentifiés par des agents utilisateur connus, le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échecs de connexion de l’utilisateur Okta à partir de plusieurs adresses IP Playbook

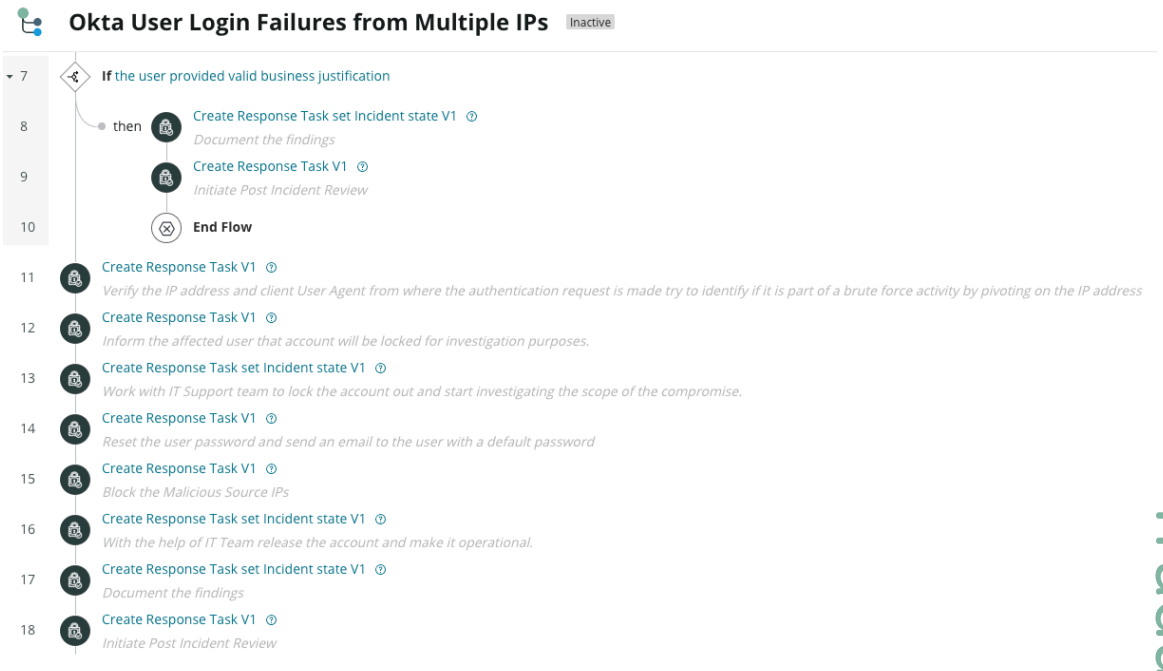


4. Dans l’action 5, en fonction de l’enquête, contactez l’utilisateur par le biais d’une communication hors bande (par exemple, appel téléphonique ou e-mail) pour vérifier si l’activité est due à un verrouillage du compte ou à un mot de passe incorrect fourni par l’utilisateur.
5. Dans l’action 6, vérifiez si l’utilisateur a fourni une justification commerciale valable.
6. Dans l’action 7, si l’utilisateur a fourni une justification commerciale valide, effectuez les tâches suivantes.
   a. Dans l’action 8, créez une tâche de réponse pour documenter les résultats obtenus jusqu’à présent.
   b. Dans l’action 9, créez une réponse pour lancer une revue post-incident.
      Dans l’action 10, le flux s’arrête.
7. Dans l’action 11, vérifiez l’adresse IP et l’agent utilisateur client à partir duquel la demande d’authentification est effectuée et essayez d’identifier s’il fait partie d’une activité de force brute en pivotant sur l’adresse IP.
8. Dans l’action 12, informez l’utilisateur affecté que le compte sera verrouillé à des fins d’enquête.
   Vous pouvez utiliser le modèle d’e-mail fourni pour informer l’utilisateur concerné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook Échecs de connexion de l'utilisateur Okta à partir de plusieurs adresses IP



9. Dans l'action 13, travaillez avec l'équipe d'assistance informatique pour verrouiller le compte et commencer à enquêter sur l'étendue de la compromission.
10. Dans l'action 14, réinitialisez le mot de passe utilisateur et envoyez un e-mail à l'utilisateur avec le mot de passe par défaut.
11. Dans l'action 15, bloquez les adresses IP sources malveillantes.
12. Dans l'action 16, demandez l'aide de l'équipe d'assistance informatique pour libérer le compte et le ramener aux normes opérationnelles.
13. Dans l'action 17, documentez les résultats obtenus jusqu'à présent.
14. Dans l'action 18, effectuez l'examen post-incident avant de fermer la tâche.

Playbook pour ModSec Brute force par IP Burst

Ce playbook fournit des étapes de rattrapage systématiques pour enquêter sur les incidents de tentatives de force brute sur les pages de connexion à partir de plusieurs adresses IP détectées par ModSec. Les conditions d'événement peuvent être définies au niveau de la politique ModSec elle-même et déclencheront une alerte chez Splunk lorsque l'événement est créé au niveau de ModSec.

Ce playbook permet de détecter les nombres de trafic anormaux sur la page de connexion. Dans cet exemple, deux rafales successives de plus de 50 occurrences/minute devraient provenir d'une adresse IP vers la page de connexion, ce qui indique une tentative de connexion par force brute.

Configurer le playbook ModSec Brute force by IP Burst

Suivez les étapes suivantes pour configurer le playbook ModSec Brute force by IP Burst.

Avant de commencer

Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_si.admin
- flow_designer

Assurez-vous d'avoir installé Security Operations Spoke (*sn_sec_spoke*).

Procédure

1. Connectez-vous en tant qu'utilisateur avec les rôles sn_si.user et flow_designer.
2. Accédez à la **Tous** > **Concepteur de flux** et sélectionnez le playbook **ModSec Bruteforce by IP Burst** .
3. **Facultatif :** Créez une copie du flux de playbook ModSec Bruteforce par IP Burst et apportez les modifications nécessaires.

   (Optional) Pour créer une copie du flux du playbook, sélectionnez l'icône du menu Actions supplémentaires (menu), puis sélectionnez **Copier le flux**. Effectuez cette étape uniquement si vous prévoyez de personnaliser ou d'apporter des changements spécifiques au flux.



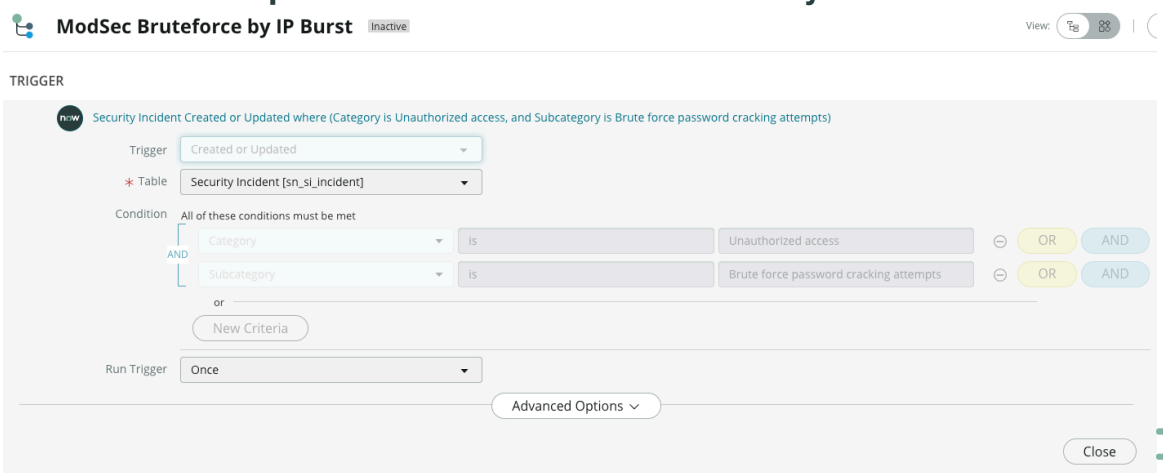
4. Activez les playbooks.
   a. Activez le flux principal pour utiliser le playbook disponible dans le système de base.
   b. Activez les flux copiés après avoir apporté les changements requis.
5. Définissez une **condition de déclenchement** pour le playbook.
   Ce playbook est déclenché et associé à l'incident de sécurité lorsque les conditions suivantes sont remplies :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **La catégorie** est **Accès non autorisé**.
- **La sous-catégorie** est les **tentatives de décodage de mot de passe en force brute**.

ModSec Force brute par IP Condition de déclenchement du Playbook en rafale



Utiliser le playbook ModSec Brute force by IP Burst

Utilisez ce playbook pour enquêter sur les incidents de tentatives de force brute sur les pages de connexion à partir de plusieurs adresses IP détectées par ModSec. Les étapes suivantes vous donnent une procédure pas à pas des actions, des tâches et des flux secondaires disponibles dans le playbook ModSec Brute force by IP Burst.

Avant de commencer

Rôle requis :

- sn_si.admin
- flow_designer

Procédure

1. Lorsque le playbook est déclenché et commence à s'exécuter, dans l'action 1, vérifiez si l'adresse IP source appartient à un client ou à l'adresse IP interne de l'organisation.
2. Dans l'action 2, si l'adresse IP source appartient à un client ou à l'adresse IP interne de l'organisation, procédez comme suit :

ModSec Brute force par IP Playbook de rafale



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans l'action 3, vérifiez s'il y a eu des activités suspectes.

- Vérifiez l'activité à partir de l'adresse IP source au cours des derniers jours. Si l'adresse IP avait un trafic négligeable, cela indique une attaque réelle.
- Vérifiez les noms d'utilisateur de pulvérisation. Par exemple, vérifiez si les noms d'utilisateur sont classés par ordre alphabétique.
- Recherchez les noms de compte génériques impliqués. Par exemple, admin, sysadmin, root, administrateur et autres noms de compte d'application.

S'il n'y a pas d'activités suspectes, le flux s'arrête.

b. Dans l'action 4, s'il y a eu des activités suspectes, dans l'action 5, vérifiez si l'historique d'accès à l'instance et le nom d'utilisateur semblent authentiques.

Vérifiez les *Appnode* journaux pour voir s'il y a des signes de défaillance. Il peut y avoir des événements d'échec SAML, SSO ou LDAP, qui peuvent être dus à un problème opérationnel.

Si l'historique d'accès à l'instance et le nom d'utilisateur ne semblent pas authentiques, le flux s'arrête.

c. Dans l'action 6, si l'historique d'accès à l'instance et le nom d'utilisateur semblent authentiques, procédez comme suit :

i. Dans l'action 7, communiquez avec l'équipe appropriée pour résoudre le problème.

ii. Dans l'action 8, documentez les résultats obtenus jusqu'à présent.

iii. Dans l'action 9, effectuez l'examen post-incident avant de fermer la tâche.

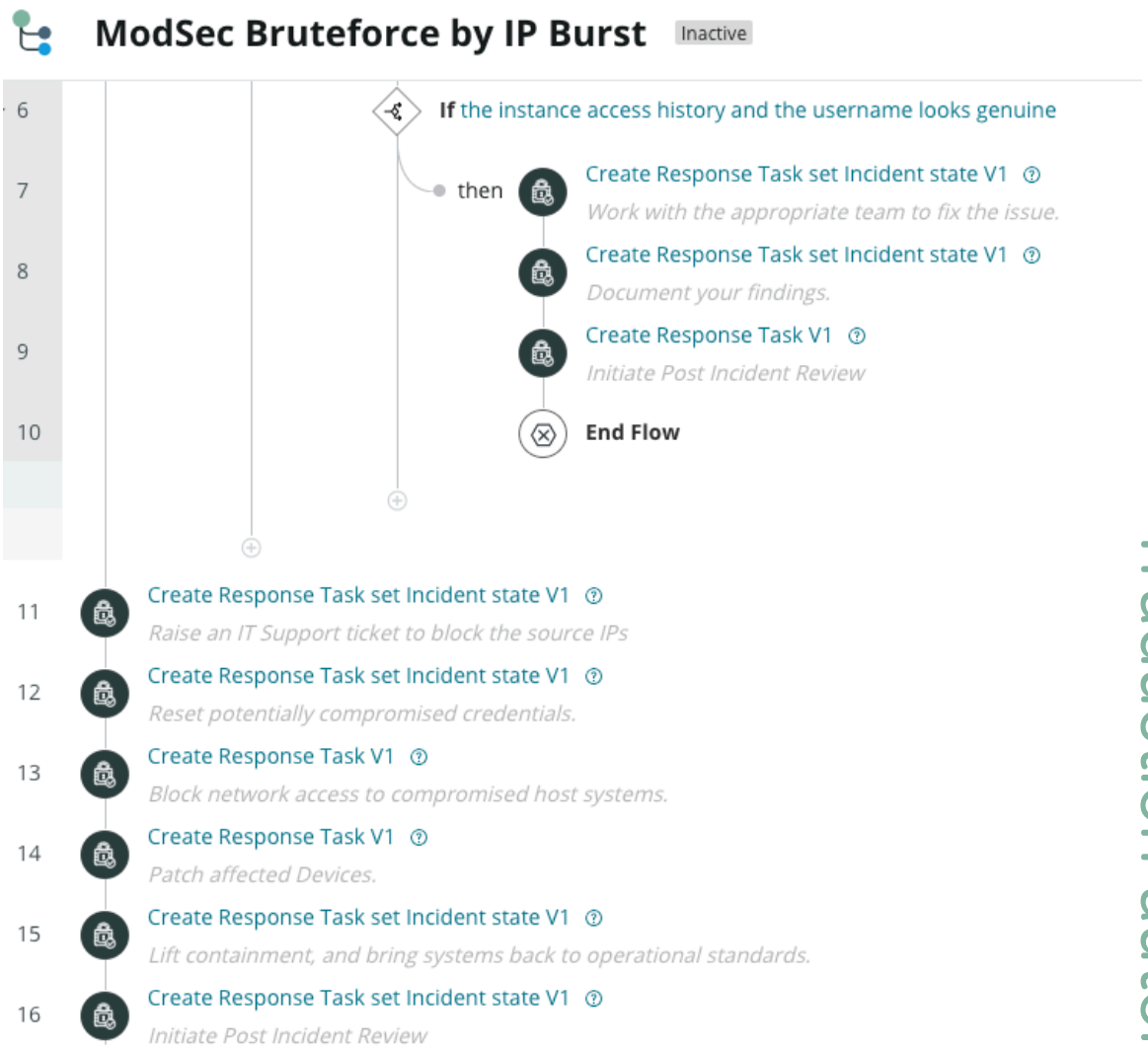
Dans l'action 10, le flux s'arrête.

3. Si l'adresse IP source n'appartient pas à un client ou à l'adresse IP interne de l'organisation, lors de l'action 11, créez un ticket d'assistance informatique pour bloquer les adresses IP sources.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation du playbook ModSec Brute force by IP Burst



Traduction automatique

4. Dans l’action 12, réinitialisez les informations d’identification potentiellement compromises.
5. Dans l’action 13, bloquez l’accès réseau aux systèmes hôtes compromis.
6. Dans l’action 14, corrigez les appareils affectés.
7. Dans l’action 15, levez le confinement et ramenez les systèmes aux normes opérationnelles.
8. Dans l’action 16, effectuez la revue post-incident avant de fermer la tâche.

Actions du playbook de Réponse aux incidents de sécurité

Cette section décrit les actions fournies dans la bibliothèque d’actions de Concepteur de flux.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
Ajouter une balise de sécurité à l'incident de sécurité	Utilisez cette action pour ajouter automatiquement une balise de sécurité à l'aide de la logique du Concepteur de flux.	Si le flux détecte un IOC, la balise **IOC détectée** peut être automatiquement ajoutée à l'aide de cette action. **Flux** :	• Entrée : incident de sécurité, balise de sécurité • Sortie : non applicable
Ajouter des observables à l'incident de sécurité	Utilisez cette action pour ajouter des observables à un incident de sécurité sélectionné. • Par défaut, la liste des observables est séparée par un séparateur de virgules (,), mais ce paramètre peut être modifié. Vous pouvez spécifier un autre caractère spécial unique comme délimiteur. Lors de l'ajout d'observables, le type (URL, adresse IP, hachage) est automatiquement défini. • Lorsque les observables sont ajoutés à l'incident de sécurité, le type (URL, adresse IP, hachage) est automatiquement défini. • Lorsque les observables sont ajoutés, l'option Filtrer les observables sur liste d'autorisation identifie les observables de la liste d'autorisation et ne les ajoute pas à la liste connexe Observables de l'incident de sécurité. Une activité système		• Entrée : ◦ incident de sécurité ◦ observables ◦ délimiteur ◦ Filtrer les éléments observables sur la liste d'autorisation et publier la note d'activité • Sortie : non applicable

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
	automatisée (réponse) est ajoutée pour indiquer que ces observables ont été supprimés.		
Obtenir les utilisateurs affectés (listes connexes) par plusieurs incidents de sécurité V1	Récupère tous les utilisateurs affectés répertoriés dans la liste connexe Utilisateurs affectés pour les incidents de sécurité spécifiés.	Vous pouvez avoir des incidents de sécurité parents avec plusieurs incidents de sécurité enfants. Utilisez cette action pour déployer les utilisateurs affectés de tous les incidents de sécurité enfants vers les incidents de sécurité parents correspondants. Seuls les utilisateurs affectés uniques sont déployés et tous les doublons sont éliminés.	• Entrée : incidents de sécurité • Sortie : ◦ Utilisateur affecté ◦ compter
Obtenir les utilisateurs affectés par plusieurs incidents de sécurité	Récupère l'utilisateur affecté principal pour l'incident de sécurité spécifié. Cela n'inclut pas les utilisateurs affectés de la liste connexe Utilisateurs affectés.	• Pendant l'enquête sur un incident de sécurité lié au hameçonnage, envoyez un e-mail aux principaux utilisateurs affectés (qui ont signalé l'incident de hameçonnage) pour confirmer si l'un des utilisateurs a cliqué sur les liens malveillants contenus dans l'e-mail de hameçonnage. • Mettez à jour la gravité de l'incident de sécurité parent ou le score de risque en fonction du nombre d'utilisateurs principaux affectés.	• Entrée : incidents de sécurité • Sortie : ◦ Utilisateurs affectés ◦ compter

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
Obtenir les utilisateurs affectés (liste connexe) à partir d'un incident de sécurité	Récupère tous les utilisateurs affectés répertoriés dans la liste connexe Utilisateurs affectés pour un incident de sécurité spécifié.		• Entrée : incidents de sécurité • Sortie : ◦ Utilisateurs affectés ◦ compter
Ajouter des utilisateurs affectés à un incident de sécurité	Ajoute tous les utilisateurs affectés à un incident de sécurité.	Supposons que vous ayez un incident de sécurité parent avec plusieurs incidents de sécurité enfants. Vous pouvez utiliser cette action pour déployer les utilisateurs affectés de tous les incidents de sécurité enfants vers l'incident de sécurité parent correspondant. Seuls les utilisateurs affectés uniques sont déployés et tous les doublons sont éliminés.	• Entrée : ◦ incident de sécurité ◦ utilisateur • Sortie : non applicable
Obtenir les éléments de configuration des utilisateurs affectés	Récupère les éléments de configuration (CI) de tous les utilisateurs affectés.	Dans les scénarios d'hameçonnage ou de programme malveillant, vous pouvez utiliser cette action pour mettre à jour la liste connexe des éléments de configuration (CI) affectés et examiner les CI. Vous pouvez ensuite mettre à jour la gravité ou le score de risque de l'incident de sécurité en fonction du nombre de CI identifiés.	• Entrée : utilisateurs • Sortie : ◦ Éléments de configuration ◦ compter
Obtenir tous les incidents de sécurité enfants pour un incident de sécurité	Récupère tous les incidents de sécurité enfants liés à un incident de sécurité parent spécifique.	Exemple de scénario : Utilisez cette action pour : • Mettez à jour l'état des incidents de sécurité enfants lorsque leur état d'incident de sécurité parent correspondant est mis à jour. • Mettez à jour automatiquement	• Entrée : ◦ incident de sécurité ◦ État de l'incident • Sortie : ◦ incident de sécurité enfant ◦ compter

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
		la gravité ou le score de risque de l'incident de sécurité en fonction du nombre d'incidents de sécurité enfants.	
Obtenir les éléments de configuration pour les observables (adresse IP de type)	Récupère tous les éléments de configuration (CI) des observables de type adresse IP.	Un observable d'adresse IP peut être associé à un élément de configuration. Par exemple, l'adresse IP d'un serveur. Si vous utilisez cette action, vous pouvez récupérer des informations pour le serveur.	• Entrée : adresse IP de l'observable • Sortie : ◦ Éléments de configuration ◦ compter
Est observable malveillant	Confirme la présence d'un ou de plusieurs observables malveillants dans un ensemble d'observables.	Une fois la recherche de menaces terminée et que vous avez identifié la présence d'observables malveillants, vous pouvez augmenter la gravité ou le score de risque d'un incident de sécurité.	• Entrée : incident de sécurité • Sortie : malveillante (vrai/faux)
Envoyer un e-mail pour confirmer l'interaction de l'utilisateur	Envoie un e-mail en réponse à une réponse d'un utilisateur.	Si un utilisateur tente plusieurs fois de se connecter à une application et échoue, il en résulte un scénario d'échec de la connexion. Dans ce cas, un e-mail est envoyé à l'utilisateur pour confirmer s'il a tenté de se connecter ou non. En fonction de la réponse de l'utilisateur (Oui ou Non), différentes actions peuvent être entreprises. **Flux** : échec de la connexion manuelle Playbook	
Filtrer les éléments observables sur liste d'autorisation	Utilisez cette action pour autoriser la liste des observables à partir d'un ensemble donné d'observables.	Vous pouvez identifier certains observables qui peuvent être ignorés à partir d'un ensemble d'observables. Ces observables ne seront pas pris en compte lors de la	• Entrée : incident de sécurité • Sortie :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de l'action	Description	Exemple de scénario	
		résolution de l'incident de sécurité.	◦ Observables de liste d'autorisation ◦ compter
Réinitialiser le mot de passe pour les utilisateurs affectés	Utilisez cette action pour réinitialiser le mot de passe pour les utilisateurs concernés.	Si un compte utilisateur a été piraté ou si un utilisateur demande la réinitialisation d'un mot de passe, un e-mail est envoyé à l'utilisateur pour réinitialiser le mot de passe. **Flux** : échec de la connexion manuelle au playbook.	
Obtenir le groupe d'utilisateurs pour l'utilisateur affecté	Récupère les détails du groupe d'utilisateurs des utilisateurs affectés.	Dans une organisation, si deux utilisateurs ou plus signalent des e-mails d'hameçonnage, vous pouvez identifier le groupe auquel ils appartiennent et identifier si d'autres utilisateurs ont été affectés	• Entrée : utilisateur • Sortie : ◦ Groupes d'utilisateurs ◦ compter

Représentation visuelle de la génération de rapports de Security Incident Response

Les responsables de la sécurité peuvent utiliser les interfaces graphiques de haut niveau telles que les cartes, les treemaps pour identifier les zones de préoccupation.

Pour afficher Réponse aux incidents de sécurité le tableau de bord de l'explorateur en détail, reportez-vous à Espace de travail de la Réponse aux incidents de sécurité la section Affichage des tableaux de bord de l'espace de travail SIR.

Tableau de bord de vue d'ensemble Réponse aux incidents de sécurité

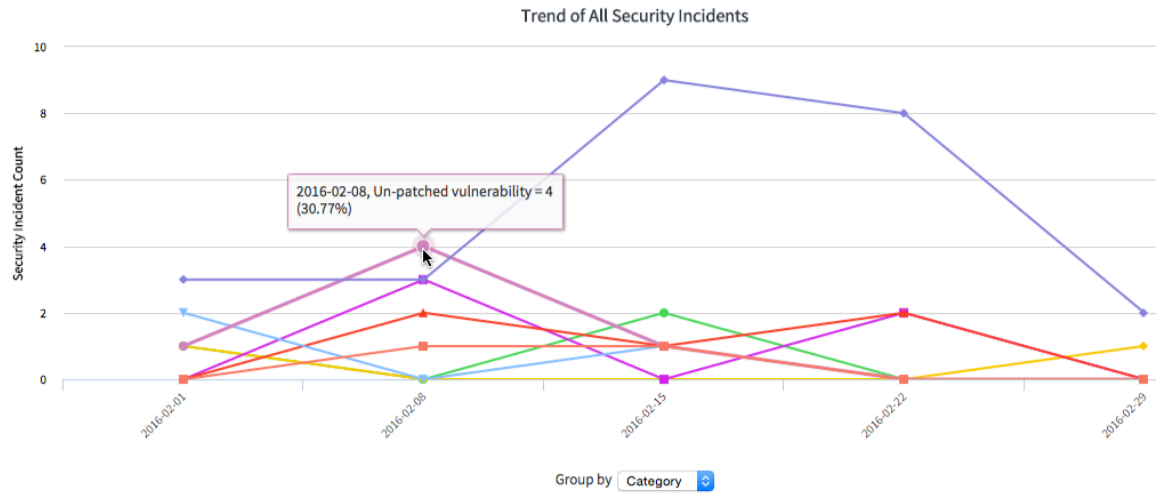
Le Réponse aux incidents de sécurité tableau de bord Vue d'ensemble fournit une vue exécutive de l'activité des incidents de sécurité, fournissant des tendances et des rapports, ainsi que des détails sur des données spécifiques.

Le module de vue d'ensemble affiche des informations sur les incidents de sécurité adaptées au rôle de l'utilisateur. Vous pouvez pointer sur n'importe quelle partie d'un graphique (barre, secteur, point de données, carte thermique, etc.) pour afficher des données générales spécifiques à cette partie. Voir l'image suivante. Si vous cliquez sur une partie d'un rapport, une liste s'ouvre pour fournir des informations détaillées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tendance de tous les incidents de sécurité



Présentation du gestionnaire d'incidents de sécurité

Les utilisateurs disposant des rôles d'administrateur d'incident de sécurité et de gestionnaire d'incident de sécurité consultent la vue d'ensemble du gestionnaire d'incident de sécurité. Il contient les rapports suivants dans le système de base.

Rapports Vue d'ensemble du gestionnaire d'incidents de sécurité

Nom	Visuel	Description
Équipe Incidents de sécurité critique	Score unique	Nombre d'incidents de sécurité critique affectés à l'équipe.
Équipe Incidents de sécurité élevée	Score unique	Nombre d'incidents de sécurité élevée affectés à l'équipe.
SLA arrivant à expiration dans les 24 heures	Score unique	Nombre de SLA qui expirent dans les prochaines 24 heures.
Risque par rapport à la gravité	Carte thermique	Répartition des incidents de sécurité affectés à l'équipe par risque et gravité.
Incidents de sécurité par classe CI, 3 derniers mois	Histogramme	Nombre d'incidents de sécurité affectés à l'équipe par classe d'élément de configuration.
Tendance de tous les incidents de sécurité	Graphique de tendance	Trace le nombre d'incidents de sécurité reçus par catégorie ou priorité.
Accès non autorisé Incidents de sécurité	Histogramme	Affiche les types de catégories d'incidents de sécurité reçus au fil du temps.
Délai moyen pour contenir	Score unique	Temps moyen nécessaire pour contenir tous les incidents de sécurité.
Délai moyen pour contenir critique	Score unique	Temps moyen nécessaire pour contenir tous les incidents de sécurité critiques.
Délai moyen jusqu'à l'identité	Score unique	Temps moyen nécessaire pour identifier tous les incidents de sécurité.

Vue d'ensemble des analyses de sécurité

Les utilisateurs disposant du rôle d'analyste des incidents de sécurité consultent la vue d'ensemble de l'analyste de sécurité. Il contient les rapports suivants dans le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble des analystes de la sécurité

Nom	Visuel	Description
Mes tâches de priorité critique	Score unique	Nombre d'incidents de sécurité critique qui me sont affectés.
Mes tâches de priorité élevée	Score unique	Nombre d'incidents de sécurité élevée qui me sont affectés.
Mes SLA arrivant à expiration dans les 24 heures	Score unique	Nombre de SLA qui me sont affectés et qui expirent dans les prochaines 24 heures.
Incidents de sécurité qui me sont affectés	Histogramme	Incidents de sécurité qui me sont affectés par état ou catégorie d'incident.
Tâches qui me sont affectées par type	Histogramme	Tâches de sécurité (incidents, tâches ou demandes) qui me sont affectées par type ou par priorité.
Incidents de sécurité, demandes et tâches qui me sont affectées	Liste	Une liste de tous les incidents de sécurité, demandes de sécurité et tâches qui me sont affectées.
Emplacement de l'incident de sécurité	Carte	Emplacement régional des incidents de sécurité.
Nombre	Carte	Nombre d'incidents de sécurité par région.
Nombre min./max.	Barre du spectre de couleurs	Nombre minimal et maximal d'incidents de sécurité par région, représentés par une barre de spectre de couleurs.
Pourcentage de décompte	Carte	Pourcentage du nombre total d'incidents par région.

Vue d'ensemble du CISO d'incidents de sécurité avec l'analyse des incidents de sécurité activée

Lorsque le module d'extension Analyse des incidents de sécurité est activé, les utilisateurs ayant les rôles de CISO d'incident de sécurité et d'administrateur système consultent la vue d'ensemble du CISO d'incident de sécurité. Les rapports CISO suivants sont fournis dans le système de base.

Rapports Vue d'ensemble du CISO des incidents de sécurité (avec l'analyse des incidents de sécurité activée)

Nom	Visuel	Description
Nouveaux incidents de sécurité de cette semaine	Score unique	Nombre de nouveaux incidents de sécurité reçus au cours de la semaine en cours.
Incidents de sécurité fermés cette semaine	Score unique	Nombre d'incidents de sécurité fermés au cours de la semaine actuelle.
Nouveaux incidents de sécurité (sur 7 jours)	Score unique	Nombre d'incidents de sécurité ouverts au cours des 7 derniers jours.
Incidents de sécurité clôturés (sur 7 jours)	Score unique	Nombre d'incidents de sécurité fermés au cours des 7 derniers jours.
Nouveaux incidents de sécurité quotidiens par rapport aux incidents de sécurité fermés	Graphique de tendance	Nombres d'incidents de sécurité nouveaux et fermés au fil du temps et par jour.
Nouveaux incidents de sécurité hebdomadaires par rapport aux incidents de sécurité fermés	Graphique de tendance	Incidents de sécurité nouveaux et fermés au fil du temps par semaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble du CISO des incidents de sécurité (avec l'analyse des incidents de sécurité activée) (suite)

Nom	Visuel	Description
Code de fermeture de l'incident de sécurité	Graphique de tendance	Nombre complet de codes de fermeture au fil du temps.
Impact opérationnel d'un incident de sécurité	Arborescence	Services aux entreprises comportant des incidents de sécurité regroupés par criticité opérationnelle disponibles.
Durée moyenne pour contenir (hebdomadaire)	Graphique de tendance	Le temps moyen de 7 jours qu'il faut pour contenir un incident de sécurité au fil du temps.
Durée moyenne pour l'élimination (hebdomadaire)	Graphique de tendance	Délai moyen de 7 jours nécessaires pour éradiquer un incident de sécurité au fil du temps.
Délai moyen d'obtention de l'identité (hebdomadaire)	Graphique de tendance	Délai moyen de 7 jours nécessaires pour identifier un incident de sécurité au fil du temps.
Emplacement de l'incident de sécurité	Carte	Emplacement régional des incidents de sécurité.
Nombre	Carte	Nombre d'incidents de sécurité par région.
Nombre min./max.	Barre du spectre de couleurs	Nombre minimal et maximal d'incidents de sécurité par région, représentés par une barre de spectre de couleurs.
Pourcentage de décompte	Carte	Pourcentage du nombre total d'incidents par région.

Vue d'ensemble du CISO des incidents de sécurité sans l'analyse des incidents de sécurité activée

Lorsque le module d'extension n'est Analyse des incidents de sécurité pas activé, les utilisateurs ayant les rôles de CISO d'incident de sécurité et d'administrateur système consultent la vue d'ensemble de la génération de rapports de CISO d'incident de sécurité. Les rapports CISO suivants sont fournis dans le système de base.

Rapports Vue d'ensemble du CISO des incidents de sécurité (sans l'analyse des incidents de sécurité activée)

Nom	Visuel	Description
Nouveaux incidents de sécurité de cette semaine	Score unique	Nombre de nouveaux incidents de sécurité ouverts au cours de la semaine actuelle.
Incidents de sécurité fermés cette semaine	Score unique	Nombre d'incidents de sécurité fermés au cours de la semaine actuelle.
Nouveaux incidents de sécurité (sur 7 jours)	Score unique	Nombre d'incidents de sécurité ouverts au cours des 7 derniers jours.
Incidents de sécurité clôturés (sur 7 jours)	Score unique	Nombre d'incidents de sécurité fermés au cours des 7 derniers jours.
Nouveaux incidents de sécurité chaque semaine	Graphique de tendance	Les nouveaux incidents de sécurité s'ouvrent chaque semaine.
Incidents de sécurité fermés chaque semaine	Graphique de tendance	Les incidents de sécurité se fermaient chaque semaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapports Vue d'ensemble du CISO des incidents de sécurité (sans l'analyse des incidents de sécurité activée) (suite)

Nom	Visuel	Description
Codes de fermeture des incidents de sécurité	Graphique de tendance	Codes de fermeture des incidents de sécurité au fil du temps.
Services d'entreprise avec incidents de sécurité : impact sur l'entreprise	Arborescence	Services aux entreprises comportant des incidents de sécurité regroupés par criticité opérationnelle disponibles.
Délai moyen pour contenir	Score unique	Temps moyen nécessaire pour contenir tous les incidents de sécurité.
Délai moyen pour contenir critique	Score unique	Temps moyen nécessaire pour contenir tous les incidents de sécurité critiques.
Délai moyen jusqu'à l'identité	Score unique	Temps moyen nécessaire pour identifier tous les incidents de sécurité.

Remarque : Le Réponse aux incidents de sécurité système de base inclut des solutions Analyse des performances pour afficher des tableaux de bord de bonnes pratiques préconfigurés. Les tableaux de bord présentent des mesures importantes pour analyser votre processus Security Incident Response, tels que les nouveaux incidents de sécurité ou l'âge moyen des incidents de sécurité ouverts. Pour plus d'informations et d'instructions d'installation, consultez Réponse aux incidents de sécurité Platform Analytics et Reporting.

Accéder à l'explorateur de Réponse aux incidents de sécurité

Vous pouvez accéder au tableau de bord de l'explorateur pour visualiser l'activité Réponse aux incidents de sécurité des incidents de sécurité afin d'identifier instantanément les zones de préoccupation et de résoudre rapidement les problèmes.

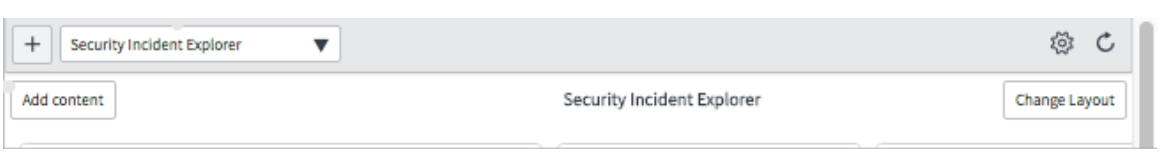
Avant de commencer

Rôles requis :

- sn_si.admin (pour écrire)
- sn_si_basic (en lecture)

Procédure

1. Accédez à la **Tous** > **Libre-service** > **Page d'accueil** ou accédez à **Libre-service** > **Tableaux de bord**.
2. Choisissez l'Explorateur des incidents de sécurité dans la liste des rapports.



Résultats

Le tableau de bord de l'explorateur Réponse aux incidents de sécurité s'affiche.

Que faire ensuite

Pour afficher Réponse aux incidents de sécurité le tableau de bord de l'explorateur en détail, reportez-vous à Espace de travail de la Réponse aux incidents de sécurité la section Affichage des tableaux de bord de l'espace de travail SIR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Carte des incidents de sécurité

La carte des incidents de sécurité fournit des données par emplacement géographique. La carte du monde est mise en évidence dans chaque zone où un incident se produit. Lorsque le module d'extension Analyse des incidents de sécurité est activé, vous pouvez ajouter la carte des incidents de sécurité à la vue d'ensemble Réponse aux incidents de sécurité . Une fois qu'elle a été ajoutée, vous pouvez configurer la carte en modifiant les filtres de carte.

Ajouter la carte à la vue d'ensemble Réponse aux incidents de sécurité

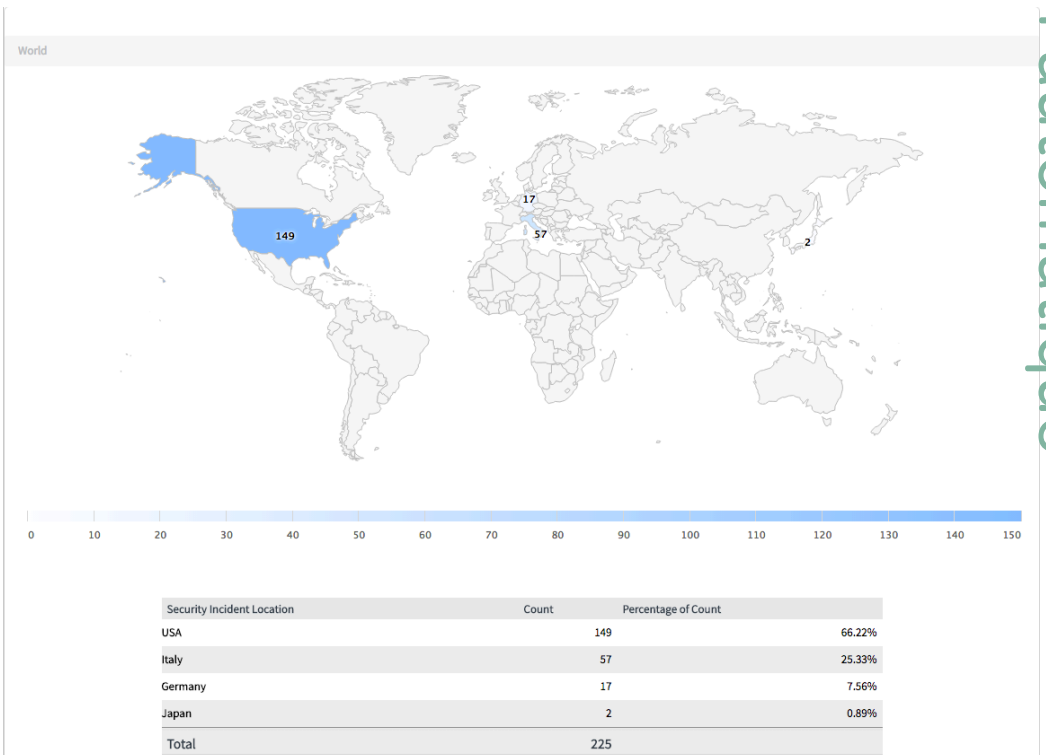
Vous pouvez ajouter la carte à la vue d'ensemble pour afficher les données d'incident Réponse aux incidents de sécurité de sécurité par emplacement géographique. Une carte vous permet d'explorer les informations sur les incidents de sécurité par emplacement.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Vue d'ensemble**.
2. Cliquez sur **Ajouter du contenu** dans le coin supérieur gauche de la page pour ouvrir le contrôle de sélection des widgets.
3. Dans la première zone de sélection, cliquez sur **Rapports**.
4. Dans la deuxième zone de sélection, cliquez sur **Incident de sécurité**.
5. Dans la troisième zone de sélection, cliquez sur **Carte des incidents de sécurité**.



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. En bas de l'écran, cliquez sur l'emplacement de l'écran que vous souhaitez ajouter au rapport.
7. Fermez la zone **Ajouter du contenu** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

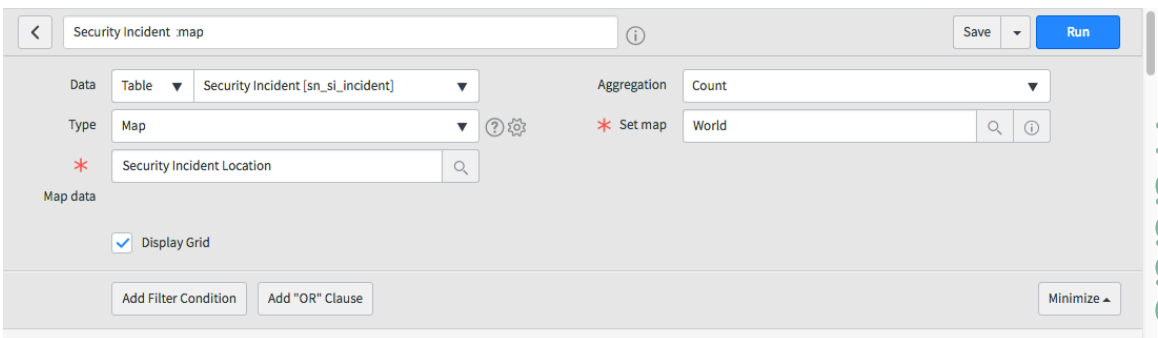
Modifier la carte des incidents de sécurité

Les administrateurs dans le domaine global peuvent modifier la façon dont la carte des incidents de sécurité gère les incidents de sécurité à l'aide de filtres.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Rapports** > **Administration** > **Tous**.
2. **Recherchez la carte des incidents de sécurité**.
3. Cliquez sur **Modifier le rapport**.



4. Cliquez sur **Ajouter une condition de filtre** pour ajouter ou modifier des filtres.
5. Cliquez sur **Exécuter** pour voir les changements appliqués.
6. Cliquez sur **Enregistrer**.

Arborescences d'incidents de sécurité

Lorsque le module d'extension Analyse des incidents de sécurité est activé, vous pouvez ajouter les arborescences incident de sécurité - impact sur le service et incident de sécurité - temps réel à la Réponse aux incidents de sécurité vue d'ensemble. Une fois qu'ils ont été ajoutés, vous pouvez configurer les arborescences en modifiant les catégories et les indicateurs des arborescences.

Ajouter des treemaps à la vue d'ensemble de Security Incident Response

Les treemaps affichent des données hiérarchiques (arborescentes) sous la forme d'un ensemble de rectangles imbriqués. Chaque branche de l'arbre reçoit un rectangle, qui est ensuite recouvert de rectangles plus petits représentant des sous-branches. Les treemaps vous permettent d'afficher les informations sur les incidents de sécurité de manière dynamique et attrayante.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Vue d'ensemble**.
2. Cliquez sur **Ajouter du contenu** dans le coin supérieur gauche de la page pour ouvrir le contrôle de sélection des widgets.
3. Dans la première zone de sélection, cliquez sur **Arborescence**.

Traduction automatique

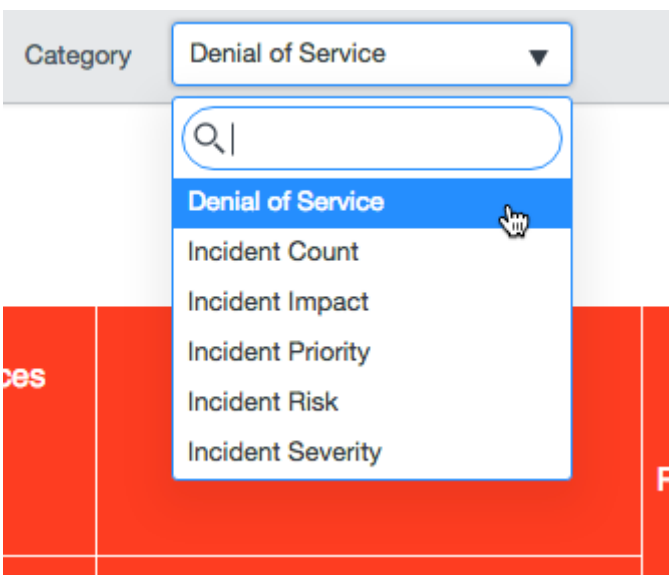
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la deuxième zone de sélection, sélectionnez l'arborescence que vous souhaitez insérer dans la liste suivante :
   - Incident de sécurité - Impact sur le service
   - Incident de sécurité - Temps réel
   - Incident de sécurité - Impact sur l'entreprise
   - Importance de la vulnérabilité

   Remarque : L'arborescence de l'impact sur l'entreprise s'affiche par défaut sur la page d'accueil Réponse aux incidents de sécurité . L'impact sur le service et les arborescences en temps réel nécessitent l'activation du module d'extension Analyse des incidents de sécurité.

5. Dans la troisième zone de sélection, sélectionnez le niveau de granularité des informations que vous souhaitez récupérer pour l'arborescence sélectionnée.

   Remarque : Pour l'arborescence Incident de sécurité - Impact du service, sélectionnez **Incident de sécurité** dans la troisième zone de sélection. Cette sélection fournit une liste déroulante avec plusieurs catégories de données.



6. En bas de l'écran, cliquez sur l'emplacement de l'écran où vous souhaitez ajouter la jauge.
7. Fermez la zone **Ajouter du contenu** .

Créer ou mettre à jour une catégorie d'arborescence

Vous pouvez modifier les catégories prédéfinies pour les arborescences d'incidents de sécurité ou créer des catégories selon vos besoins.

Avant de commencer
Rôle requis : sn_si.admin

Les treemaps utilisent l'analyse des performances comme source de données. Le module Analyse des performances nécessite un module d'extension distinct.

Pourquoi et quand exécuter cette tâche
Dans le système de base, les catégories d'arborescence telles que Risque d'incident, Déni de service et Gravité de l'incident sont incluses. Vous pouvez modifier ces catégories ou en définir d'autres selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Administration**et ouvrez l'arborescence pour laquelle vous souhaitez configurer des catégories :
   - **Définition de reporting sur la criticité des services**
   - **Définition en temps réel**
2. **Facultatif :** Changez le nom de la définition de l'arborescence.
   Dans le système de base, le nom par défaut pour la définition de l'arborescence d'impact de service est **Incident de sécurité**. Le nom par défaut de la définition de l'arborescence en temps réel est **Incident de sécurité - Temps réel**.
3. À moins d'utiliser une arborescence personnalisée, ne modifiez pas la valeur **du groupe d'indicateurs PA** .
4. Pour désactiver la définition de l'arborescence, décochez la case **Actif** .
   Si, par exemple, vous désactivez la catégorie Déni de service du tableau de bord d'impact sur le système, cette catégorie d'arborescence n'est pas disponible.
5. Dans la liste connexe **des catégories d'arborescence** , sélectionnez une catégorie à modifier ou cliquez sur **Nouveau** pour en créer une nouvelle.
6. Renseignez les champs.

Formulaire de catégorie d'arborescence

Champ	Description
Nom	Nom affiché pour la catégorie dans la liste **Catégories** au-dessus de l'arborescence.
Ordre	Ordre dans lequel la catégorie apparaît dans la liste **Catégories** au-dessus de l'arborescence.
Arborescence	Nom de l'arborescence qui utilise cette catégorie.
Couleur	Couleur affichée pour cette catégorie dans l'arborescence.
Actif	Sélectionnez cette option pour activer cette catégorie.
Description	Description de la catégorie.
Visible par tous les rôles	Sélectionnez cette option pour rendre cette catégorie visible à tous les utilisateurs, quel que soit leur rôle.
Rôles	Si vous n'avez pas coché la case **Visible par tous les rôles** , sélectionnez les rôles pouvant afficher cette catégorie.

7. Cliquez sur **Envoyer** ou **Mettre à jour**.

Créer ou mettre à jour un indicateur d'arborescence

Vous pouvez modifier les indicateurs prédéfinis pour une catégorie d'arborescence ou créer de nouveaux indicateurs. Pour chaque indicateur, vous pouvez configurer sa source de données et spécifier comment les listes d'incidents de sécurité sont ouvertes à partir des arborescences affichées avec l'indicateur.

Avant de commencer

Rôle requis : sn_si.admin

Les treemaps utilisent l'analyse des performances comme source de données. Le module Analyse des performances nécessite un module d'extension distinct.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez l’arborescence pour laquelle vous souhaitez configurer des indicateurs.

Définition de l’arborescence	Action
Arborescence de l’impact du service	Accédez à la **Incident de sécurité** > **Administration** > **Définition de l'impact sur le service**.
Arborescence en temps réel	Accédez à la **Incident de sécurité** > **Administration** > **Définition en temps réel**.

2. Dans la liste connexe **Catégories de l’arborescence** , sélectionnez la catégorie pour laquelle vous souhaitez configurer les indicateurs.
3. Dans la liste connexe **des indicateurs d’arborescence** , sélectionnez un indicateur à modifier ou cliquez sur **Nouveau** pour créer un indicateur.
4. Renseignez les champs.

Formulaire Indicateur d’arborescence

Champ	Description
Nom	Nom affiché pour l’indicateur dans la liste **Indicateurs** sur le tableau de bord d’impact du service.
Description brève	Description affichée pour l’indicateur dans la liste **Indicateurs** au-dessus de l’arborescence.
Limite du résultat	Nombre maximal de résultats autorisés. La limite supérieure est 100.
Précision du résultat	Nombre de chiffres à afficher après la décimale. ce champ est affiché uniquement pour la définition de l’arborescence en temps réel.
Actif	Case à cocher pour activer cet indicateur.
Catégorie	Nom de la catégorie saisi sur l’écran précédent.
Direction	Indique si la tuile de l’arborescence est réduite ou agrandie. ce champ est affiché uniquement pour la définition de l’arborescence en temps réel.
Unité	Unité de mesure à utiliser pour la mesure. ce champ est affiché uniquement pour la définition en temps réel.
Intervalle d’actualisation automatique	Fréquence d’actualisation de l’arborescence.
Ordre	Ordre dans lequel l’indicateur apparaît dans la liste **Indicateurs** au-dessus de l’arborescence.

5. Cliquez sur l’onglet Configuration de la **source de données** et configurez l’une des options de source de données suivantes pour l’indicateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Action
Analyse des performances	Sélectionnez **Analyse des performances** dans le champ **Source de données** , puis effectuez les entrées suivantes : ○ **Indicateur:** Indicateur utilisé pour regrouper les données PA. ○ **Répartition par défaut :** Répartition par défaut utilisée pour diviser l'indicateur PA sélectionné en plusieurs parties.
Script personnalisé	Sélectionnez **Script personnalisé** dans le champ **Source de données** . Utilisez ensuite l'éditeur HTML pour personnaliser le script selon vos besoins. Le résultat de l'exécution du script doit être un tableau pour que les informations s'affichent dans l'arborescence.
Conditions de la requête	Sélectionnez **Condition de requête** dans le champ **Source de données** , puis effectuez les entrées suivantes : ○ **Table de requêtes :** Table de base à interroger. ○ **Type d'agrégat :** Type d'agrégat (SUM, COUNT, AVG, MIN, MAX) à utiliser. ○ **Champ d'agrégat :** Champ que la requête doit utiliser. ○ **Grouper par :** Champ pour trier les données interrogées. **Remarque :** Pour améliorer la requête, cliquez sur **Ajouter une condition de filtre** et **Ajouter une clause « OU ».**

6. Cliquez sur l'onglet **Clic de renvoi** et spécifiez comment les listes d'incidents de sécurité sont ouvertes à partir de l'arborescence.
   a. Dans le champ Type de navigation dans les **URL par clic** , indiquez si vous souhaitez que la liste des incidents de sécurité s'ouvre dans une nouvelle fenêtre, dans la même fenêtre ou dans une boîte de dialogue.
   b. **Facultatif :** Dans le champ **de script URL par clic** , modifiez l'exemple de script si nécessaire.
7. Cliquez sur **Envoyer** ou **Mettre à jour**.

Ajouter des graphiques d'importance de vulnérabilité à une vue d'ensemble

Si le module d'extension Réponse aux vulnérabilités est activé, vous pouvez ajouter des graphiques de définition de la signification de la vulnérabilité et d'autres visualisations à la vue d'ensemble.

Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la page Vue d'ensemble à laquelle vous souhaitez ajouter la jauge de l'importance de la vulnérabilité.
2. Cliquez sur **Ajouter du contenu** dans le coin supérieur gauche de la page pour ouvrir le contrôle de sélection des widgets.
3. Dans les trois zones de sélection, effectuez les sélections en fonction de la jauge (arborescence ou rapport de score) que vous souhaitez ajouter :
   - Pour ajouter l'arborescence d'importance de la vulnérabilité, effectuez les sélections suivantes :
     - Arborescence
     - Importance de la vulnérabilité
     - Importance de la vulnérabilité
   - Pour ajouter le rapport de score d'importance de la vulnérabilité, effectuez ces sélections :
     - Analyse des performances
     - Score
     - Services avec une importance de vulnérabilité
4. Cliquez sur l'emplacement de l'écran pour lequel vous souhaitez ajouter la jauge.
5. Fermez la zone **Ajouter du contenu** .

Gestion des incidents de sécurité majeurs

L'application ServiceNow® Gestion des incidents de sécurité majeurs suit la progression de (MSI) depuis la découverte jusqu'à l'analyse, en passant par la proposition, la promotion et la liaison des Incident de sécurité majeur incidents de sécurité, ainsi que la fermeture.

Gestion des incidents de sécurité majeurs

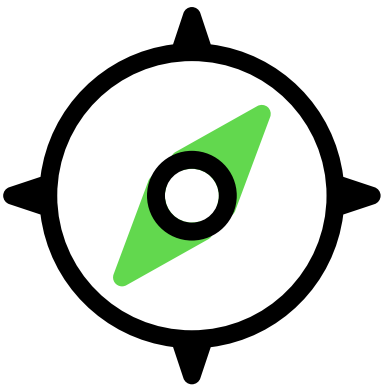
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

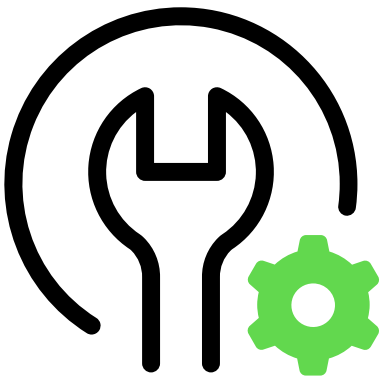
Traduction automatique

Explorer



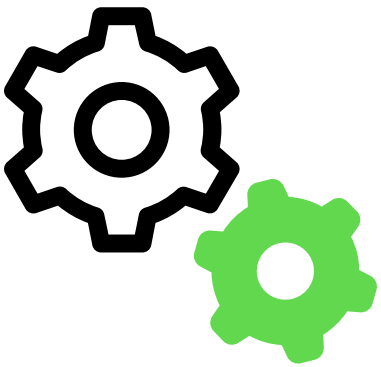
Découvrez comment les analystes, les administrateurs et les gestionnaires utilisent Major Security Incident Management (MSIM)

Configurer



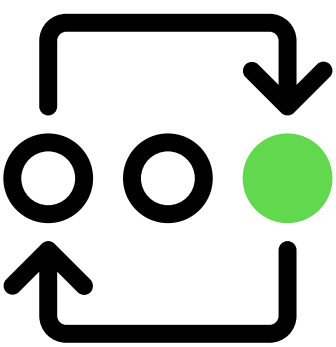
Planifier et configurer votre implémentation

Intégrer



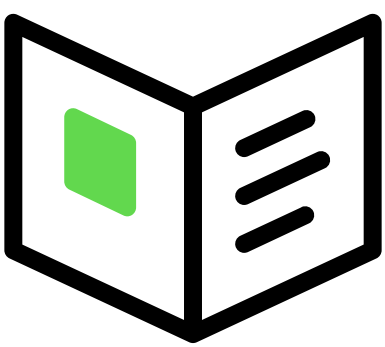
Étendre les options MSIM en les intégrant à d'autres Microsoft applications

Administrer



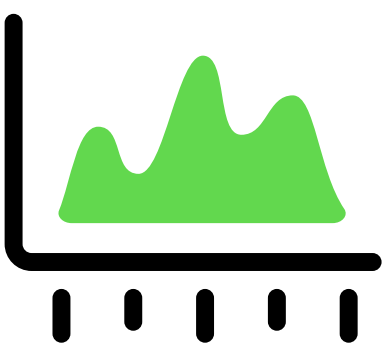
Tâches d'administration sur la façon de baliser les enregistrements d'incidents et de configurer les étiquettes

Utiliser



Proposer, promouvoir, lier et rejeter des enregistrements d'incidents de sécurité majeurs via la gestion de l'espace de travail

Rapports d'état



Surveillez les tâches liées aux incidents et améliorez les processus grâce à des mesures, des graphiques de tendances et des rapports

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Options supplémentaires



Configurer les informations pour déployer des enregistrements

Demander des applications dans l’App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Demander une application Opérations de sécurité dans l'App Store

Si vous êtes un nouveau Opérations de sécurité client le Rome ou une date ultérieure, consultez le ServiceNow Store pour afficher les applications disponibles et les informations sur la façon de soumettre des demandes à la boutique.

Dépannage et demande d'aide

- Gestion des incidents de sécurité majeurs forum sur le ServiceNow Community.
- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Explorer la gestion des incidents de sécurité majeurs

Explorez Gestion des incidents de sécurité majeurs pour comprendre le fonctionnement de l’application en termes de suivi des incidents de sécurité critiques de priorité élevée, qui sont identifiés comme une menace pour l’organisation.

Utilisez cette section pour découvrir les fonctionnalités clés et les différents rôles impliqués dans l’utilisation des enregistrements d’incidents de sécurité majeurs. Cette section vous aide également à comprendre la prise en main de l’application, les conditions préalables et les modules d’extension requis pour travailler avec l’application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des incidents de sécurité majeurs

Suivez et gérez diverses activités qui font généralement partie de la résolution d'un incident de sécurité majeur via Gestion des incidents de sécurité majeurs. Grâce à un espace de travail intuitif, les gestionnaires d'incidents et les personnes travaillant sur un incident peuvent proposer et promouvoir des incidents en incidents majeurs, suivre les activités liées aux incidents de sécurité majeurs et collaborer facilement avec leurs collègues.

Vue d'ensemble

Les principales options de gestion des incidents de sécurité fonctionnent conjointement avec les fonctionnalités existantes du produit Security Incident Response. Cela inclut la possibilité pour un analyste de sécurité d'escalader un incident de sécurité standard en un incident de sécurité majeur, afin que les nouvelles fonctionnalités du produit soient disponibles pour prendre en charge le processus de correction.

Après l'installation sur votre ServiceNow instance, un analyste d'incidents de sécurité peut :

- Proposer un incident de sécurité au candidat à un incident de sécurité majeur afin de lancer un processus d'examen sur la nécessité de créer un incident de sécurité majeur.
- Transformez directement un incident de sécurité en un incident de sécurité majeur sans avoir besoin d'un processus d'examen supplémentaire.
- Rejetez un incident de sécurité proposé en tant qu'incident de sécurité majeur (MSI).
- Liez un incident de sécurité en tant qu'incident enfant à l'incident de sécurité majeur (MSI) afin que tous les incidents de sécurité puissent être traités.

Fonctionnalités principales

La gestion des incidents de sécurité majeurs (MSIM) améliore le processus de correction des incidents de sécurité majeurs grâce aux fonctionnalités suivantes :

- Espace de travail dédié à la gestion des incidents de sécurité majeurs conçu pour le rôle d'utilisateur responsable des incidents de sécurité majeurs.
- Organisez les tâches de réponse pour plusieurs incidents de sécurité « enfants ».
- Automatisez la création de dossiers de collaboration et de canaux de communication par messagerie instantanée après la création d'un incident de sécurité majeur, ainsi que l'archivage dans le cadre de la clôture de l'incident.
- Composant d'explorateur de fichiers permettant d'organiser et de suivre la collecte d'artefacts (fichiers) liés à l'incident de sécurité majeur via une Microsoft SharePoint intégration.
- Gestionnaire de canal de messagerie instantanée et composants de flux d'activité pour gérer les communications entre plusieurs groupes de sécurité, informatiques et fonctionnels via une Microsoft Teams intégration.

Composants de l'espace de travail

Le Gestion des incidents de sécurité majeurs produit contient plusieurs nouveaux composants d'espace de travail et pages d'interface utilisateur qui offrent les fonctionnalités principales :

- Espace de travail dédié à la gestion des incidents de sécurité majeurs, spécialement conçu pour le rôle d'utilisateur principal de gestionnaire d'incidents de sécurité.
- Organisez les tâches de réponse pour plusieurs incidents de sécurité enfants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Automatisez la création de dossiers de collaboration et de canaux de communication par messagerie instantanée après la création d'un incident de sécurité majeur, ainsi que l'archivage dans le cadre de la clôture de l'incident.
- Composant d'explorateur de fichiers permettant d'organiser et de suivre la collecte d'artefacts (fichiers) liés à l'incident de sécurité majeur via une Microsoft SharePoint intégration.
- Gestionnaire de canal de messagerie instantanée et composants de flux d'activité pour gérer les communications entre plusieurs groupes de sécurité, informatiques et fonctionnels via une Microsoft Teams intégration.

Versions de Major Security Incident Management prises en charge

Gestion des incidents de sécurité majeurs (MSIM) nécessite ServiceNow AI Platform® Version Rome.

Cette fonctionnalité prend en charge Microsoft Teams, qui est un espace de travail centré sur la messagerie instantanée dans la Microsoft Office 365 suite. Auparavant, Microsoft Teams il y avait une installation séparée des Microsoft Office 365 applications.

Versions prises en charge ServiceNow AI Platform

Cette fonctionnalité est prise en charge dans les Rome versions ultérieures.

Les applications suivantes Opérations de sécurité sont les modules d'extension standard Réponse aux incidents de sécurité qui seront probablement installés pour la plupart des utilisateurs s'ils utilisent déjà Réponse aux incidents de sécurité (SIR). Si elle n'est pas installée, vous devez l'installer et l'activer à partir de ServiceNow Store. Installez puis activez une application à la fois dans l'ordre mentionné pour assurer une installation fluide :

1. Réponse aux incidents de sécurité: com.snc.si_dep est le module d'extension dépendant. L'installation de ce module d'extension active les autres applications Security Operations.
2. Cadre de travail d'intégration de sécurité
3. Security Support Common
4. Security Support Common Orchestration

Introduction à MSIM

Examinez les informations suivantes avant de commencer à utiliser .Gestion des incidents de sécurité majeurs

Rôle requis : sn_msi.workspace_admin.

Pour faciliter l'installation et la configuration de l'application Gestion des incidents de sécurité majeurs , vous devrez peut-être vérifier si les modules d'extension suivants sont activés.

Important : Un ensemble de mises à jour (KB1289784) est disponible dans le Guide de démarrage rapide de Major Security Incident Management. Pour aider les utilisateurs à configurer facilement, vous devez importer l'ensemble de mises à jour une fois l'installation terminée. Suivez la procédure décrite dans le Guide de démarrage rapide (étape 2) sous la section Pièces justificatives de l'application MSIM, qui se trouve sur ServiceNow Store.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prérequis

Tâche	Description
Avant de commencer avec l'application, assurez-vous que vous disposez des modules d'extension dépendants requis.	Dans un premier temps, installez : • Programme d'installation du Centre d'intégration ServiceNow (com.glide.hub.integrations) • ServiceNow® Centre d'intégration Exécution (com.glide.hub.integration.runtime). • ServiceNow® Centre d'intégration Action Step - REST (com.glide.hub.action_step.rest) • ServiceNow® Centre d'intégration Modèle d'action : flux de données (com.glide.hub.action_type.datastream) • ServiceNow® Centre d'intégration Flow Designer : entrées dynamiques (com.glide.hub.dynamic_inputs) **Remarque :** Si vous ne disposez pas des privilèges nécessaires pour l'un des modules d'extension répertoriés ServiceNow® Centre d'intégration , soumettez un ticket de support pour installer ces applications prérequises.
Vérifiez que vous disposez de l'accès requis pour installer Microsoft SharePoint le spoke et Microsoft Teams Graph le spoke. **Remarque :** La liste ci-dessus correspond aux principales applications dépendantes pour commencer Gestion des incidents de sécurité majeurs.	Avant d'installer Microsoft SharePoint Spoke et Microsoft Teams Graph Spoke, assurez-vous d'avoir l'accès requis aux ServiceNow Centre d'intégration applications. **Remarque :** Microsoft SharePoint Spoke et Microsoft Teams Graph Spoke sont des applications dépendantes des ServiceNow® Centre d'intégration applications.

Liste de vérification pour MSIM la configuration

Avant d'utiliser l'application (MSIM), téléchargez l'application ServiceNow® Gestion des incidents de sécurité majeurs à partir du ServiceNow® Store.

Suivez votre progression avec l'installation, l'installation et la configuration à partir de la table suivante.

Remarque : Les rôles affectés à Gestion des incidents de sécurité majeurs l'application sont répertoriés dans les sections suivantes. Pour plus d'informations, reportez-vous à la section Gestion des incidents de sécurité majeurs rôles.

Utilisez la liste de vérification suivante pour vous guider dans les étapes de bout en bout de l'installation et de la configuration Gestion des incidents de sécurité majeurs de l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification

Tâche de configuration	Description
Vérifiez que l'application Gestion des incidents de sécurité majeurs est installée et activée à partir du ServiceNow® Store.	Gestion des incidents de sécurité majeurs v1.1.1 est disponible sur ServiceNow® Store. Suivez ces instructions : Télécharger une application à partir de ServiceNow Store.
Vérifiez que les applications suivantes sont installées dans l'ordre donné.	Les applications suivantes seront installées par défaut après l'installation Gestion des incidents de sécurité majeurs de l'application dans la version actuelle de l'application : • File Explorer Core pour Security Operations v1.1.1 • Microsoft SharePoint File Explorer Connecteur pour Opérations de sécurité v1.1.1 • File Explorer Composant pour Opérations de sécurité v1.0.0 • Microsoft Teams Connecteur de messagerie instantanée pour Security Operations v1.0.0 • Cœur de la messagerie instantanée pour Opérations de sécurité la version 1.0.0 • Incident de sécurité majeur Réponse v1.1.1 • Carte EVAM de la messagerie instantanée de collaboration pour MSIM l'espace de travail v1.0.0 (cette application est configurée uniquement pour les visualisations d'interface utilisateur en arrière-plan de l'application pour Gestion des incidents de sécurité majeurs l'espace de travail) • Composant de l'interface utilisateur de l'organisateur de tâche pour Gestion des incidents de sécurité majeurs l'espace de travail 1.0.0 • Réponse aux incidents de sécurité v12.8.1
Vérifiez que les rôles d'utilisateur sont affectés comme Incident de sécurité majeur il convient.	Les rôles suivants sont impliqués tout au long du cycle de vie des incidents du processus de Incident de sécurité majeur rattrapage :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	• Administrateur MSI [sn_msi.workspace_admin] • Gestionnaire MSI [sn_msi.workspace_manager] • Répondeur MSI [sn_msi.workspace_responder Pour en savoir plus sur chaque rôle, reportez-vous à la section Gestion des incidents de sécurité majeurs rôles.
Vérifiez que vous avez correctement configuré Microsoft SharePoint la version 1.0.0.	Microsoft SharePoint gère les sites, les dossiers, les fichiers, les groupes et les utilisateurs dans Microsoft SharePoint. Ajoutez Microsoft SharePoint des données à votre ServiceNow® instance. Pour ce faire, vous devez configurer des connexions Graph et Rest. Pour plus d'informations, consultez la documentationdu spoke Microsoft SharePoint v1.1.2 sur la configuration de la configuration des connexions REST et Graph. Établissez une connexion Graph et REST pour vous connecter à votre ServiceNow® instance à partir de Microsoft SharePoint.
Vérifiez que vous avez créé un Microsoft SharePoint site pour créer une bibliothèque de documents.	Créez un Microsoft SharePoint site, si nécessaire, ou vous pouvez utiliser un site existant pour créer notre bibliothèque de documents.
Vérifiez que vous avez créé une bibliothèque de documents sous le Microsoft SharePoint site.	Créez une bibliothèque de documents dédiée sous un site nouveau ou existant Microsoft SharePoint .
Vérifiez que les autorisations requises sont fournies aux utilisateurs et affectées aux groupes d'utilisateurs requis dans le Microsoft SharePoint.	Gérez l'accès du site à différents utilisateurs et groupes d'utilisateurs Microsoft SharePoint .
Vérifiez que vous avez créé et configuré Microsoft SharePoint Drive et les paramètres de configuration nécessaires.	Pour vérifier les configurations de lecteur, configurez le connecteur de l'explorateur de fichiers, les Microsoft SharePoint actions de dossier et de fichier et les modèles de dossier :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	• Configurer le lecteur de référentiel de l'explorateur de fichiers: créer une connexion à partir de Microsoft SharePoint l'instance ServiceNow® . • Configurer les paramètres d'action de fichier et de dossier: configurez et contrôlez les actions de dossier et de fichier individuelles affichées sur le composant Explorateur de fichiers. • Créer des modèles de dossier: à configurer pour créer des dossiers uniques pour différents types d'incidents de sécurité majeurs.
Vérifiez que vous avez établi une connexion à l'application Connecteur de messagerie instantanée Microsoft Teams.	Pour établir la connexion de l'application Connecteur de messagerie instantanée Microsoft Teams avec ServiceNow® l'instance, suivez la procédure expliquée ici : Établir une connexion au graphique MS Teams sur ServiceNow AI Platform.
Vérifiez que vous avez configuré Microsoft Teams avec ServiceNow AI Platform® instance et créé des configurations de connexions et d'informations d'identification.	Pour vérifier Microsoft Teams la configuration avec ServiceNow® l'instance, suivez la procédure expliquée ici : • Établir une connexion au graphique MS Teams sur ServiceNow AI Platform • Créer un modèle de canal de messagerie instantanée
Vérifiez que les paramètres de configuration de Major Security Incident Administration (Administration des incidents de sécurité majeurs) sont corrects.	En tant qu'administrateur MSI, vous devez être en mesure de : • Déterminer si les analystes de sécurité peuvent proposer et promouvoir l'incident et lier d'autres incidents de sécurité. • Activez ou désactivez les notifications lorsqu'un incident est proposé ou promu. Possibilité de modifier les messages du modèle par défaut. • Configurez les balises de sécurité qui apparaissent sur l'interface d'analyste de la sécurité pour différencier les incidents qui ont été proposés en tant que candidats à l'incident de sécurité majeur ou promus en incident de sécurité majeur.
Vérifiez que les paramètres Administration des incidents de sécurité majeurs - Notifications sont corrects.	En tant qu'administrateur MSI, déclenchez des notifications par e-mail lorsqu'un incident de sécurité est proposé et envoyez-les à tous les utilisateurs et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	groupes configurés dans la liste de notifications. Pour plus d'informations, consultez Définir les préférences de notification pour MSIM.

Gestion des incidents de sécurité majeurs rôles

Affectez des rôles pour vous assurer que les utilisateurs peuvent effectuer toutes les actions nécessaires dans l'application MSIM.

Rôles pour Gestion des incidents majeurs

Type de rôle	Rôle	Description
Administrateur MSI	sn_msi.workspace_admin	Puis-je installer, configurer Gestion des incidents majeurs et configurer les applications dépendantes telles que File Explorer (FE), la configuration de Microsoft Teams et du canal de messagerie instantanée, la configuration de l'espace de travail et l'administration MSI : configuration des configurations et des notifications. Comment configurer : • Composant de l'explorateur de fichiers (FE) : ◦ Configurer le référentiel de fichiers. ◦ Configurez les actions de fichier et de dossier fournies dans le composant Explorateur de fichiers de l'onglet Collaboration de l'espace de travail Major Security Incident Management. ◦ Créez les dossiers racine et sous-dossier, puis fournissez un accès aux sous-dossiers. • Gestion des canaux de messagerie instantanée ◦ Activez et configurez Microsoft Teams en validant la Microsoft Teams connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles pour Gestion des incidents majeurs (suite)

Type de rôle	Rôle	Description
		◦ Créez des équipes et des canaux de messagerie instantanée, puis ajoutez des utilisateurs et affectez-les aux différents groupes d'utilisateurs. • Administration MSI : ◦ Configurations : configurez les actions des analystes de sécurité, les notifications envoyées lorsque des incidents sont proposés et promus, et affichez les balises pour les incidents de sécurité. ◦ Notifications : automatisez le processus de notification par e-mail et les notifications de l'utilisateur lorsqu'un incident de sécurité est proposé ou promu comme incident de sécurité majeur.
Gestionnaire MSI	sn_msi.workspace_manager	• Affichez l'accès à la page des paramètres de configuration de la gestion des incidents de sécurité majeurs. Il est interdit de modifier les paramètres de configuration. • Affichez et modifiez les données d'enregistrement d'incident dans les onglets **Détails**, **Collaboration** et **Organisateur de tâche** de l'espace Gestion des incidents majeurs de travail. • Promouvoir l'incident de sécurité en incident de sécurité majeur. • Configurez les actions de fichiers et de dossiers disponibles dans le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles pour Gestion des incidents majeurs (suite)

Type de rôle	Rôle	Description
		composant **Explorateur** de fichiers de l'onglet Collaboration de l'espace Gestion des incidents majeurs de travail. • Liaison et dissociation des enregistrements supplémentaires aux incidents de sécurité majeurs de l'espace de travail.
Répondeur MSI	sn_msi.workspace_responder	• Rôle facultatif permettant d'afficher, de modifier et de répondre aux incidents de sécurité majeurs dans **Détails** et **Tâches** Onglets de l'espace Gestion des incidents majeurs de travail. • Liaison et dissociation des enregistrements supplémentaires aux incidents de sécurité majeurs de l'espace de travail.

Intégrant Gestion des incidents de sécurité majeurs

Étendre les options de l'instance Gestion des incidents de sécurité majeurs et s'y connecter en ServiceNow AI Platform intégrant des Microsoft applications.

Important : Un ensemble de mises à jour (KB1289784) est disponible dans le Guide de démarrage rapide de Major Security Incident Management. Pour aider les utilisateurs à configurer facilement, vous devez importer l'ensemble de mises à jour une fois l'installation terminée. Suivez la procédure décrite dans le Guide de démarrage rapide (étape 2) sous la section Pièces justificatives de l'application MSIM, qui se trouve sur ServiceNow Store.

Intégrer Gestion des incidents de sécurité majeurs à Microsoft SharePoint

Intégrez votre Microsoft SharePoint à Gestion des incidents de sécurité majeurs.

Enregistrer une nouvelle application sur le portail Azure pour les connexions SharePoint

Enregistrez une nouvelle application sur le portail Azure pour Microsoft SharePoint l'intégration.

Avant de commencer

Rôle requis : admin, administrateur Azure

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Se connecter à Microsoft Azure à l'aide de votre compte Microsoft en tant qu'administrateur Azure.
2. Accédez à la **Azure Services** > **Inscription de l'application** > **Nouvelle inscription**.

   Remarque : Si vous ne trouvez pas, accédez aux **services Azure** et recherchez **Inscription de l'application**.

3. Entrez le nom de l'application.
   Par exemple, Microsoft SharePoint graphique.
4. Sélectionnez **les types de comptes pris en charge : comptes dans ce répertoire organisationnel uniquement (ServiceNow uniquement : locataire unique**).
5. Sélectionnez Type **Web** dans la liste déroulante sous le champ URI de redirection (facultatif).
6. Entrez ServiceNow AI Platform® l'URL de redirection d'instance dans le champ URL de redirection autorisée.
   Par exemple, https://<InstanceName>.service-now.com/oauth_redirect.do.
7. Cliquez sur **S'inscrire** et assurez-vous que la page est affichée avec la section **Vue d'ensemble** .
8. Notez l'ID client et l'ID de locataire de la section **Éléments principaux** de la page Vue d'ensemble.
9. Sous **Autorisations API**, ajoutez l'autorisation Microsoft Graph :
   a. Cliquez sur **Ajouter une autorisation**.
   b. Sélectionnez **Microsoft Graph**.
   c. **Sélectionnez les autorisations d'application**.
   d. Dans la liste **Sites** , sélectionnez **Sites.Autorisation sélectionnée** .
   e. Cliquez sur **Ajouter des autorisations**.
10. Sous **Autorisations API**, ajoutez l'autorisation SharePoint :
    a. Cliquez sur **Ajouter une autorisation**.
    b. Sélectionnez **SharePoint**.
    c. **Sélectionnez les autorisations d'application**.
    d. Dans la liste **Sites** , sélectionnez l'autorisation **Sites.Selected** .
    e. Cliquez sur **Ajouter des autorisations**.
11. Après avoir ajouté les autorisations, cliquez sur **Accorder le consentement de l'administrateur**.
    Toutes les autorisations sont maintenant acceptées par l'administrateur.

Utiliser des certificats pour l'authentification

Demandez un jeton d'accès avec des informations d'identification de certificat.

Avant de commencer

1. Vous pouvez utiliser un certificat autosigné ou un certificat émis par l'autorité de certification. Vous pouvez créer un certificat auto-signé en exécutant le script PowerShell comme indiqué dans Configuration d'une application Azure AD pour un accès à l'application uniquement . Le script génère deux fichiers : . PFX et . Fichier CER.

   Remarque : Assurez-vous de connaître le mot de passe utilisé pour chiffrer la clé privée afin de générer le . PFX et . Fichier CER.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Utilisez le fichier . PFX pour créer un fichier Java Key Store (JKS).

> **Remarque :** Assurez-vous de connaître le mot de passe utilisé pour générer le fichier JKS à partir du fichier . PFX.

Rôle requis : admin

Procédure

1. Accédez aux **inscriptions d'applications sur le** portail Azure AD.
2. Cliquez sur **Certificats et secrets** dans la section **Gérer** .
3. Dans l'onglet **Certificats** , cliquez sur **Charger le certificat**.
4. Renseignez ces valeurs sur le formulaire.

Champ	Description
Chargez un certificat (clé publique) avec l'un des types de fichiers suivants : .cer, .pem, .crt	. Fichier CER que vous avez généré à l'aide du script PowerShell.
Description	Description du certificat.

5. Cliquez sur **Ajouter**.
   Le certificat est téléchargé et ses détails s'affichent sous l'onglet **Certificats** .
6. Copiez la valeur **d'empreinte** digitale du certificat chargé.

> **Remarque :** La valeur **de l'empreinte** est une valeur hexadécimale.

7. Codez la valeur **Empreinte** en une valeur Base64 et enregistrez la valeur pour une utilisation ultérieure.

> **Remarque :** Vous pouvez utiliser un outil de conversion hexadécimal en base64 (hexadécimal en base64) pour coder la valeur **d'empreinte digitale** en une valeur base64.

Configurer Microsoft SharePoint avec Gestion des incidents de sécurité majeurs

Configurer Gestion des incidents de sécurité majeurs avec Microsoft SharePoint connexion.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Administration**.
2. Sélectionnez **Collaboration documentaire**, puis **Configuration de Microsoft SharePoint**.
3. Sélectionnez **Accorder l'accès de l'application Azure au site SharePoint** dans le menu contextuel.
4. Accordez l'accès à votre application enregistrée à l'aide de l'une des méthodes suivantes : commandes Curl, Azure CLI ou PowerShell.

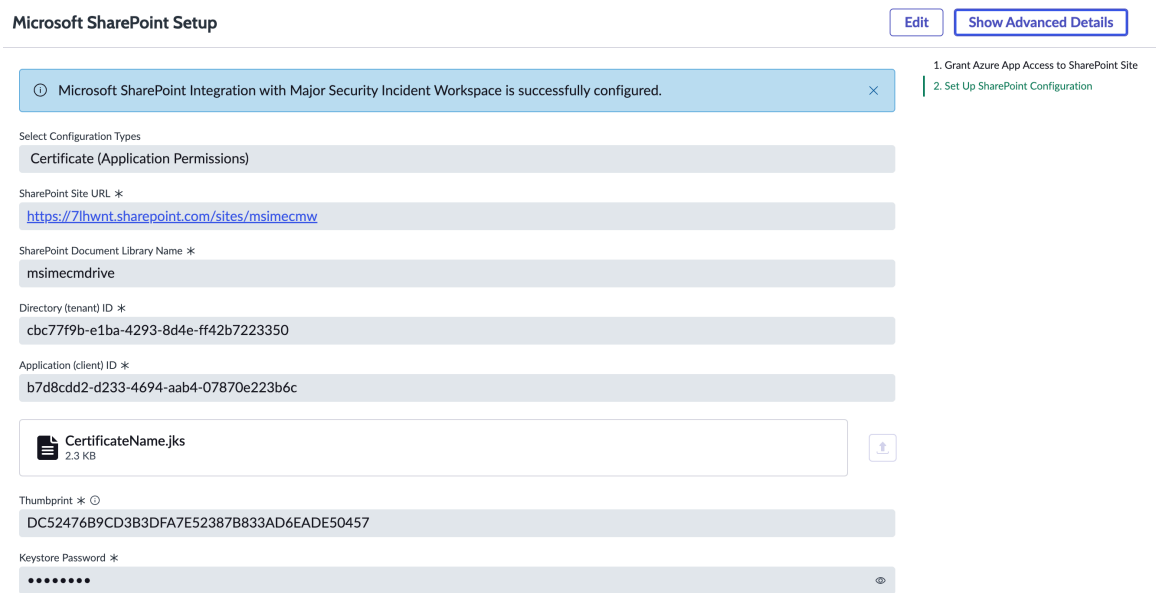
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- L’administrateur Azure doit fournir la configuration de l’accès.
- Accordez l’autorisation Sites.FullControl.All à l’application enregistrée.
- Supprimez l’autorisation Sites.FullControl.All lorsque l’accès est accordé avec succès.

5. Sélectionnez **Configurer la configuration SharePoint** dans le menu contextuel.
6. Sélectionnez un type de configuration dans **Sélectionner des types de configuration**, puis configurez les éléments suivants.
   - Certificat (autorisations des applications)



Paramètres SharePoint pour le certificat

Champ	Description
URL du site SharePoint	L’URL Microsoft SharePoint du site.
Nom de la bibliothèque de documents SharePoint	Nom de la Microsoft SharePoint bibliothèque de documents.
ID (locataire) du répertoire	L’identificateur unique de votre instance Azure Active Directory.
ID (client) de l'application	L’identificateur unique de votre application enregistrée dans Azure.
Charger le certificat	Fichier de certificat pour l’authentification.
Empreinte digitale	L’empreinte du certificat.
Mot de passe du keystore	Mot de passe du magasin de clés permettant d’accéder à l’empreinte du certificat.

   - Secret client (autorisations des applications)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Paramètres SharePoint pour le secret client

Champ	Description
URL du site SharePoint	L'URL Microsoft SharePoint du site.
Nom de la bibliothèque de documents SharePoint	Nom de la Microsoft SharePoint bibliothèque de documents.
ID (locataire) du répertoire	L'identificateur unique de votre instance Azure Active Directory.
ID (client) de l'application	L'identificateur unique de votre application enregistrée dans Azure.
Secret client	La chaîne secrète de l'application utilisée pour demander un jeton.

7. Sélectionnez **Configurer et obtenir le jeton OAuth**.
   Une invite de connexion apparaît pour fournir les détails de votre compte Microsoft.
8. Fournissez les détails de votre compte Microsoft et identifiez-vous.
   Un message concordant s'affiche et la connexion est établie.

Intégrer Gestion des incidents de sécurité majeurs à Microsoft Teams

Intégrez votre Microsoft Teams à Gestion des incidents de sécurité majeurs.

- Inscrire une nouvelle application sur le portail Azure pour Microsoft Teams les connexions
- Configurer la Microsoft Teams connexion avec Gestion des incidents de sécurité majeurs

Inscrire une nouvelle application sur le portail Azure pour Microsoft Teams les connexions

Enregistrez une nouvelle application sur le portail Azure pour Microsoft Teams l'intégration et accordez l'accès à l'application Azure.

Avant de commencer

Remarque : Si vous le souhaitez, vous pouvez utiliser la même application que celle que vous avez créée pour SharePoint pour établir la connexion Microsoft Teams Graph.

Rôle requis : admin, administrateur Azure

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Connectez-vous au portail Azure à l'aide de votre compte Microsoft.
2. Accédez à la **Azure Services** > **Inscription de l'application** > **Nouvelle inscription**.
3. Saisissez le nom de l'application.
   Par exemple, Microsoft Teams Graph.
4. Sélectionnez le **type de compte pris en charge : comptes dans ce répertoire organisationnel uniquement (ServiceNow uniquement : locataire unique).**
5. **Sélectionnez Type** Web dans la liste déroulante sous l'URL de redirection.
6. Entrez ServiceNow AI Platform® l'URL de redirection d'instance dans le champ URL de redirection autorisée.
   Par exemple, https://<<InstanceName>>.service-now.com/oauth_redirect.do
7. Cliquez sur **S'inscrire** et assurez-vous que la page est affichée avec la section **Vue d'ensemble** .
8. Notez l'ID client et l'ID de locataire dans la section **Éléments principaux** de la page **Vue d'ensemble** .
9. Vous pouvez suivre l'étape 6.1 ou l'étape 6.2 pour terminer la procédure d'établissement d'une connexion sur votre ServiceNow instance.

Configurer la Microsoft Teams connexion avec Gestion des incidents de sécurité majeurs

Configurer Gestion des incidents de sécurité majeurs avec Microsoft Teams connexion.

Avant de commencer

Prérequis : assurez-vous d'avoir enregistré une application dans Azure Active Directory avec les autorisations de délégué requises.

Rôle requis : admin

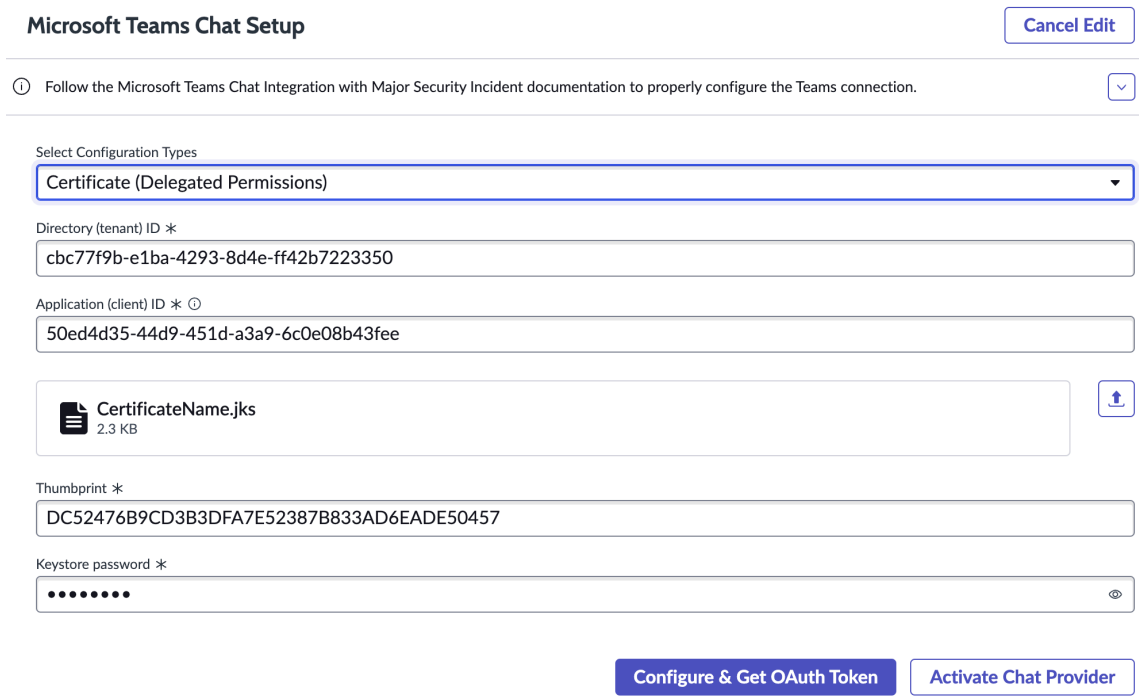
Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Administration**.
2. Sélectionnez **Collaboration de messagerie instantanée**, puis **Installation de Microsoft Teams**.
3. Sélectionnez un type de configuration dans le champ **Sélectionner les types de configuration** et configurez les éléments suivants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Certificat (autorisations déléguées)



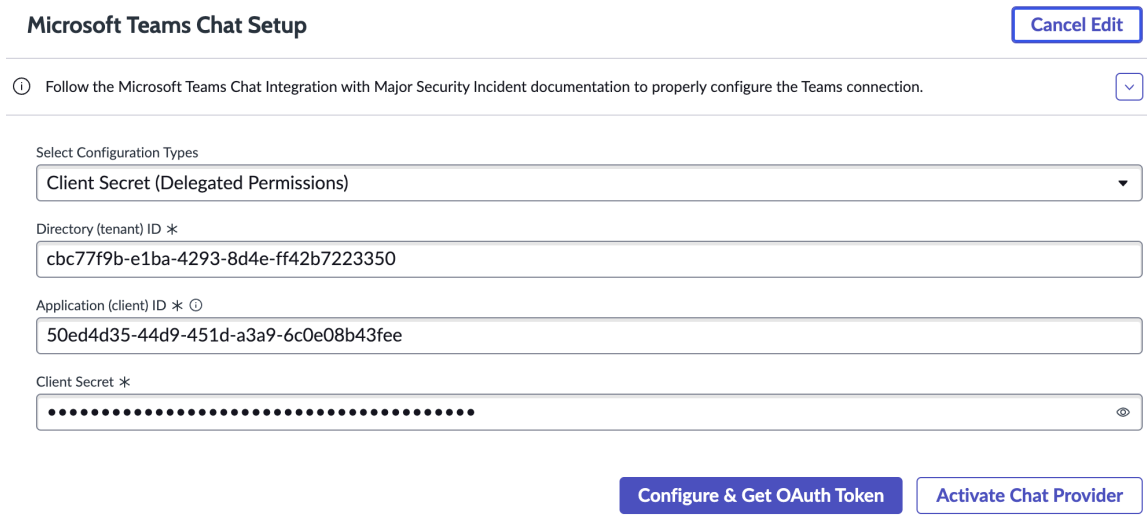
Paramètres Microsoft Teams pour la certification

Champ	Description
ID (locataire) du répertoire	L’identificateur unique de votre instance Azure Active Directory.
ID (client) de l'application	L’identificateur unique de votre application enregistrée dans Azure.
Charger le certificat	Fichier de certificat pour l’authentification.
Empreinte digitale	L’empreinte du certificat.
Mot de passe du keystore	Mot de passe du magasin de clés permettant d’accéder à l’empreinte du certificat.

- Secret client (autorisations déléguées)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Paramètres Microsoft Teams pour le secret client

Champ	Description
ID (locataire) du répertoire	L'identificateur unique de votre instance Azure Active Directory.
ID (client) de l'application	L'identificateur unique de votre application enregistrée dans Azure.
Secret client	La chaîne secrète de l'application utilisée pour demander un jeton.

4. Sélectionnez **Configurer et obtenir le jeton OAuth**.
   Une invite de connexion apparaît pour fournir les détails de votre compte Microsoft.
5. Fournissez les détails de votre compte Microsoft et identifiez-vous.
   Un message concordant s'affiche et la connexion est établie.
6. Sélectionnez **Activer le fournisseur de messagerie instantanée** pour activer Microsoft Teams la connexion.
7. **Facultatif :** Sélectionnez **Afficher les détails avancés** pour afficher les détails de la configuration.

Établir une connexion au graphique MS Teams sur ServiceNow AI Platform

Intégrez ServiceNow AI Platform l'instance et Microsoft Teams le compte en établissant une Microsoft Teams Graph connexion.

Avant de commencer

Si vous le souhaitez, vous pouvez utiliser la même application que celle que vous avez créée pour SharePoint pour établir la connexion Microsoft Teams Graph.

Rôle requis : admin, administrateur Azure

Inscrire une nouvelle application sur Azure pour Microsoft Teams Graph Connexion

Procédure

1. Connectez-vous au portail Azure à l'aide de votre Microsoft compte.
2. Accédez à la **Azure Services** > **Inscription de l'application** > **Nouvelle inscription**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Saisissez le nom de l'application.
   Par exemple, Microsoft Teams Graph.
4. Sélectionnez l'option **Modèles de comptes pris en charge** respective, celle qui convient à votre organisation.
   Par exemple, sélectionnez **l'option Comptes dans ce répertoire organisationnel uniquement (ServiceNow uniquement : locataire unique**).

   Remarque : Pour plus d'informations sur les types de comptes pris en charge, voir Enregistrer une application auprès de la plateforme d'identité Microsoft .

5. **Sélectionnez Type** Web dans la liste déroulante sous l'URL de redirection.
6. Entrez ServiceNow AI Platform l'URL de redirection d'instance dans le champ URL de redirection autorisée.
   Par exemple, https://<<InstanceName>>.service-now.com/oauth_redirect.do
7. Cliquez sur **Enregistrer** pour enregistrer votre nouvelle application et assurez-vous que la page est affichée avec la section **Vue d'ensemble** .

Utilisation de certificats pour l'authentification

Demandez un jeton d'accès avec des informations d'identification de certificat.

Avant de commencer

1. Vous pouvez utiliser un certificat autosigné ou un certificat émis par l'autorité de certification. Vous pouvez créer un certificat auto-signé en exécutant le script PowerShell comme indiqué dansConfiguration d'une application Azure AD pour un accès à l'application uniquement . Le script génère deux fichiers : . PFX et . Fichier CER.

   Remarque : Assurez-vous de connaître le mot de passe utilisé pour chiffrer la clé privée afin de générer le . PFX et . Fichier CER.

2. Utilisez le fichier . PFX pour créer un fichier Java Key Store (JKS).

   Remarque : Assurez-vous de connaître le mot de passe utilisé pour générer le fichier JKS à partir du fichier . PFX.

Rôle requis : admin

Procédure

1. Accédez aux **inscriptions d'applications sur le** portail Azure AD.
2. Cliquez sur **Certificats et secrets** dans la section **Gérer** .
3. Dans l'onglet **Certificats** , cliquez sur **Charger le certificat**.
4. Renseignez ces valeurs sur le formulaire.

Champ	Description
Chargez un certificat (clé publique) avec l'un des types de fichiers suivants : .cer, .pem, .crt	. Fichier CER que vous avez généré à l'aide du script PowerShell.
Description	Description du certificat.

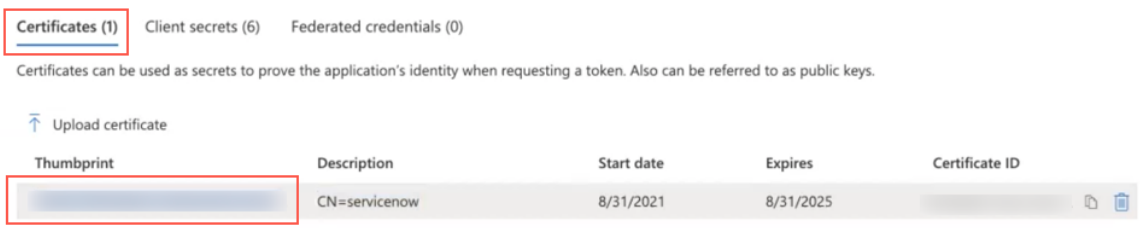
5. Cliquez sur **Ajouter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le certificat est téléchargé et ses détails s'affichent sous l'onglet **Certificats** .

6. Copiez la valeur **d'empreinte** digitale du certificat chargé.
   La valeur **de l'empreinte** est une valeur hexadécimale.



7. Codez la valeur **Empreinte** en une valeur Base64 et enregistrez la valeur pour une utilisation ultérieure.

> **Remarque :** Vous pouvez utiliser un outil de conversion hexadécimal en base64 (hexadécimal en base64) pour coder la valeur **d'empreinte digitale** en une valeur base64.

Joindre un certificat de magasin de clés Java pour MS Teams

Activez l'authentification par jeton JWT Bearer Grant en joignant un certificat Java Key Store (JKS) valide.

Avant de commencer

Connectez-vous à votre instance ServiceNow pour effectuer la procédure suivante.

- Certificat de stockage de clé Java valide
- Rôle requis : admin

Procédure

1. Accédez à la **Définition du système** > **Certificats**.
2. Ouvrez l'enregistrement **Certificat du connecteur Microsoft Teams**.
   Assurez-vous d'utiliser uniquement l'enregistrement par défaut **Certificat de connecteur Microsoft Teams** .
3. Entrez le mot de passe associé au fichier JKS dans **Mot de passe du magasin de clés**.
4. Cliquez sur l'icône) et joignez le certificat JKS que vous avez généré.
   Pour plus d'informations, consultez .
5. Cliquez sur **Valider les banques/certificats**.
6. Cliquez sur **Mettre à jour**.

Configurer la clé de signature JWT pour MS Teams

Créez une clé de signature JSON Web Token (JWT) à affecter à votre certificat Java Key Store.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **OAuth système** > **Clés JWT**.
2. Ouvrez l'enregistrement **Connecteur Microsoft Teams JWT**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Entrez le mot de passe utilisé pour chiffrer la clé privée pour générer le fichier . PFX et . CER dans le **mot de passe de clé de signature**.
4. Cliquez sur **Mettre à jour**.

Configurer le fournisseur JWT pour MS Teams

Ajoutez un fournisseur de jeton Web JSON (JWT) à votre instance ServiceNow.

Avant de commencer

- Copiez et enregistrez la valeur de **l'ID d'application (client)** et de l'ID de **répertoire (locataire)** de l'application que vous aviez inscrite dans le portail Azure.



- Rôle requis : admin

Procédure

1. Accédez à la **OAuth système** > **Fournisseurs JWT**.
2. Ouvrez l'enregistrement **Connecteur MS Teams Fournisseur JWT**.
3. Saisissez les **valeurs iss,sub** et **aud** dans la liste connexe Réclamations standard.

Champ	Valeur
Aud	URL de Microsoft Online au format suivant : https://login.microsoftonline.com/<tenant-id>/oauth2/token. Remplacez <tenant-id> par **ID de répertoire (locataire)** que la valeur de votre application avait enregistrée dans le portail Azure.
Iss	**ID (client)** de l'application que vous aviez inscrite sur le portail Azure.
sub	**ID (client)** de l'application que vous aviez inscrite sur le portail Azure.

4. Cliquez sur **Mettre à jour**.

Établir une connexion à l'aide de certificats

Établissez une connexion entre les applications Microsoft Teams Graph nouvellement créées à l'aide de certificats.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.
2. Ouvrez **le spoke Microsoft Teams**.
3. Modifiez la valeur du champ **Modèle de configuration : modèle de code d'autorisation du connecteur MSIM Microsoft Teams** et enregistrez le formulaire.

   Remarque : Ce modèle contient l'autorisation API déléguée requise pour l'intégration MSTeams.

4. Dans la section Liens connexes, cliquez sur Créer **une nouvelle connexion et informations d'identification**.

Nom	N'importe quel nom unique.
URL de connexion	URL de connexion. Par exemple, https://graph.microsoft.com
Version de l'API	Version de l'API. Par exemple, v1.0
URL d'autorisation	https://login.microsoftonline.com/<<ID de locataire>/oauth2/v2.0/authorize
URL de jeton	https://login.microsoftonline.com/<<ID de locataire>/oauth2/v2.0/jeton
URL de révocation du jeton	https://login.microsoftonline.com/<<ID de locataire>/oauth2/v2.0/revoke
ID client OAuth	ID client.
Secret client OAuth	Vous pouvez entrer n'importe quelle valeur. **Remarque :** Cela n'a pas d'importance car vous utiliserez l'authentification basée sur certificat.

5. Cliquez sur **« Créer et obtenir un jeton OAuth** ».
   Un message d'erreur s'affiche et vous invite à 401- non autorisé.
6. Rechargez le formulaire et ouvrez l'enregistrement dans la liste connexe Connexions.
7. Saisissez la valeur **Empreinte** codée Base64 dans l'attribut **Empreinte du certificat codé** de la section **Attributs** .

   Remarque : La valeur de l'empreinte est une valeur hexadécimale. Vous pouvez utiliser un outil de conversion hexadécimal en base64 (hexadécimal en base64) pour coder la valeur d'empreinte digitale en une valeur base64.

8. Accédez à la **OAuth système** > **Registre d'application**
9. Ouvrez **l'enregistrement du code d'autorisation du connecteur MSIM Microsoft Teams** .
10. Modifiez le script de l'API OAuth : **OAuthUtilJWTMSTeamsConnector**.
11. Accédez à la **Connexions et informations d'identification** > **Informations d'identification**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

12. Ouvrez l'enregistrement **Informations d'identification du connecteur MSIM Microsoft Teams**.
13. Dans Liens connexes, cliquez sur **Obtenir un jeton OAuth**.
    En cas de réussite, les autorisations d'API suivantes sont ajoutées à l'application Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Utilisation de la valeur du secret client

Utilisez la valeur du secret client pour configurer l'enregistrement du registre d'application Graph.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez aux **inscriptions d'applications sur le** portail Azure AD.
2. Cliquez sur **Certificats et secrets** dans la section **Gérer** .
3. Cliquez sur **Nouveau secret client**.
4. Copiez et notez le secret client créé dans le champ **Valeur** .

Établir une connexion à l'aide du secret client

Établissez une connexion entre l'application Microsoft Teams Graph nouvellement créée avec ServiceNow AI Platform l'instance.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.
2. Ouvrez **le spoke Microsoft Teams**.
3. Modifiez la valeur du champ **Modèle de configuration : modèle de code d'autorisation du connecteur MSIM Microsoft Teams** et enregistrez le formulaire.

Remarque : Ce modèle contient l'autorisation API déléguée requise pour l'intégration MSTeams.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la section Liens connexes, cliquez sur Créer **une nouvelle connexion et informations d'identification**.

Nom	N'importe quel nom unique.
URL de connexion	URL de connexion. Par exemple, https://graph.microsoft.com
Version de l'API	Version de l'API. Par exemple, v1.0
URL d'autorisation	https://login.microsoftonline.com/<<ID de locataire>/oauth2/v2.0/authorize
URL de jeton	https://login.microsoftonline.com/<<ID de locataire>/oauth2/v2.0/jeton
URL de révocation du jeton	https://login.microsoftonline.com/<<ID de locataire>/oauth2/v2.0/revoke
ID client OAuth	ID client.
Secret client OAuth	Secret client.

5. Cliquez sur **« Créer et obtenir un jeton OAuth »**.
En cas de réussite, les autorisations d'API suivantes sont ajoutées à l'application Azure.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Activer le connecteur de messagerie instantanée MS Teams pour l'utilisateur de spoke graphique MS Teams

Si vous êtes un utilisateur existant, suivez la procédure décrite dans cette section pour activer le connecteur de messagerie instantanée Microsoft Teams pour l'utilisateur de spoke graphique MS Teams.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Si vous êtes un utilisateur existant du spoke Microsoft Teams Graph, procédez comme suit :

- Accédez à votre application inscrite sur le portail Azure, qui est utilisée par Microsoft Teams Graph Spoke.
- Accédez à la section **Autorisations d'API** pour configurer les autorisations d'API requises.
- Cliquez sur **Ajouter une autorisation**.
- Sélectionnez **Microsoft Graph**.
- Pour utiliser l'application Microsoft Teams Connector, vous devez ajouter deux autres autorisations déléguées à votre application à partir du portail Azure : « ChannelMember.ReadWrite.All » et « TeamMember.ReadWrite.All ».
- Après avoir ajouté les autorisations requises ci-dessus, cliquez sur **Accorder le consentement de l'administrateur**.

Configurez MS Teams sur *ServiceNow AI Platform* **l'instance pour un utilisateur existant :**

- Accédez aux **alias de connexion et d'informations d'identification**.
- Sélectionnez un enregistrement **Microsoft Teams Spoke** .
- Sélectionnez l'enregistrement d'informations d'identification associé au spoke Microsoft Teams.
- Cliquez sur **Obtenir un jeton OAuth**. Un message de confirmation indique que le jeton d'actualisation OAuth est disponible.

En tant qu'utilisateur existant, vous avez maintenant terminé l'intégration de l'application de connecteur de messagerie instantanée Microsoft Teams à l'API Microsoft Teams Graph.

Gestion des incidents de sécurité majeurs Intégration de téléconférence

Avec Gestion des incidents de sécurité majeurs l'intégration des téléconférences, vous pouvez collaborer avec vos clients et vos pairs agents pour résoudre les problèmes des clients à l'aide des options de partage de vidéo et d'écran dans Microsoft Teams ou Cisco WebexZoom à partir de l'application MSIM.

L'intégration Gestion des incidents de sécurité majeurs de la téléconférence vous permet d'intégrer le canal de communication de conférence au Notification canal de communication en gérant et en initiant une réunion Cisco Webex ou Zoom une Microsoft Teams réunion directement à partir de l'applicationGestion des incidents de sécurité majeurs.

En tant que gestionnaire MSI, vous pouvez utiliser l'intégration de téléconférence MSIM pour lancer Microsoft Teams des Cisco WebexZoom réunions. Intégrez la Gestion des incidents de sécurité majeurs téléconférence avec les fournisseurs de services tiers comme canal de communication pour rencontrer les personnes concernées afin de résoudre les incidents de sécurité majeurs.

Fonctionnalités principales

L'intégration Incident de sécurité majeur de la téléconférence de gestion fournit les fonctionnalités clés suivantes :

- Les gestionnaires MSI peuvent lancer une , Cisco Webex ou Zoom une Microsoft Teams téléconférence directement à partir de l'incident de sécurité majeur.
- Invitez d'autres participants à l'appel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Afficher les enregistrements d'appels et les détails de la messagerie instantanée.
- Envoie des invitations aux participants par e-mail et Microsoft Teams par messagerie instantanée.

Commencer une téléconférence

Démarrez une téléconférence à partir d'une tâche ou d'un titre majeur en invitant un ou plusieurs utilisateurs à participer à une téléconférence. La téléconférence ne commencera que lorsqu'au moins deux participants se joindront.

Avant de commencer
Rôle requis : sn_msi.workspace_manager

Assurez-vous d'avoir effectué les opérations suivantes sur l'instance ServiceNow® :

- Installé et activé le module d'extension Notification (com.snc.notify).
- Composants d'interface utilisateur installés pour l'application Notification Espaces de travail configurables.
- Installé et activé le module d'extension Tableau de tâches visuel (com.devsnc.snb_vtb).

Pour plus d'informations, consultez Demander Centre d'intégration .

Pourquoi et quand exécuter cette tâche
Les participants à l'appel peuvent inclure les éléments suivants :

- Utilisateurs auxquels des responsabilités spécifiques ont été affectées.
- Contacts ad hoc ou à la demande
- Autres contacts de tiers

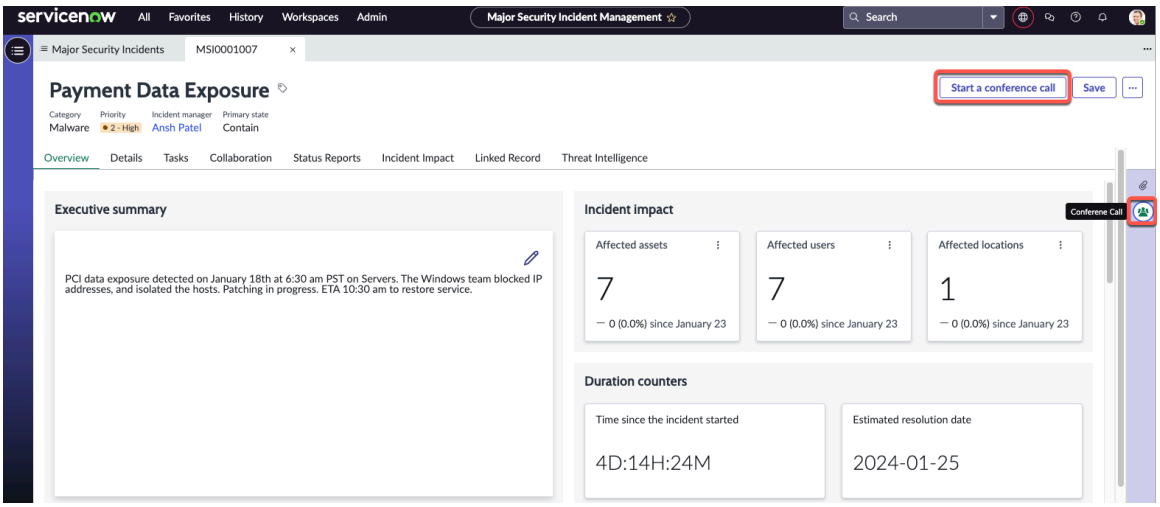
Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez un incident de sécurité majeur.
3. Sélectionnez l'action **Démarrer une téléconférence** .
4. Vous pouvez également démarrer une téléconférence en sélectionnant l'icône  dans le menu contextuel de droite et en sélectionnant l'icône +.
   La fenêtre contextuelle Démarrer la téléconférence s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Téléconférence MSIM

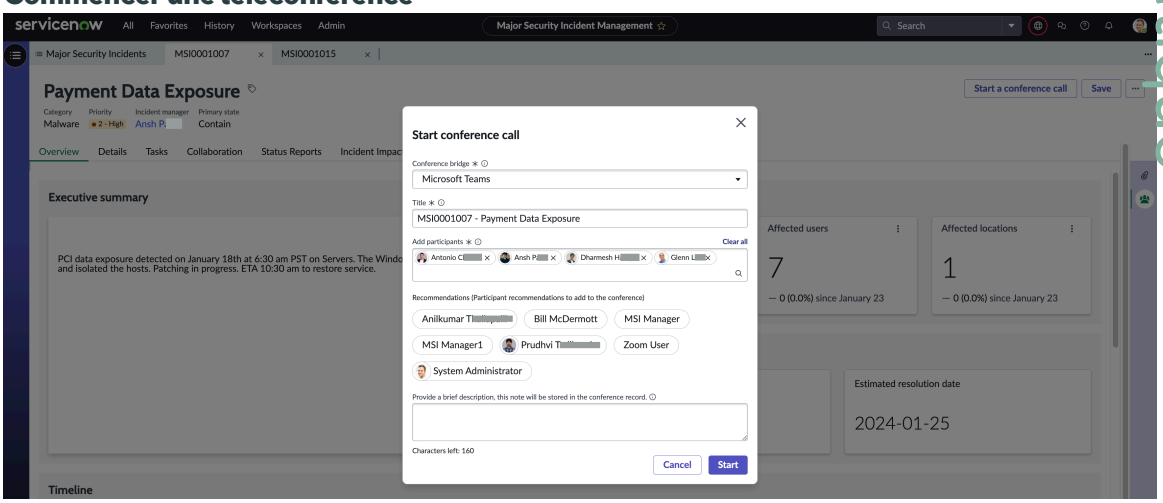


5. Dans le champ Pont de conférence, choisissez un **pont de conférence** à partir duquel vous souhaitez vous connecter.
   Par exemple, Microsoft Team, Zoom ou Cisco Webex.
6. Dans le champ Titre, indiquez un titre décrivant le motif de la téléconférence.
7. Dans le champ Ajouter des participants, sélectionnez les participants à la téléconférence.
   Vous pouvez utiliser l'option de recherche pour rechercher et ajouter les participants requis, ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations aux participants à ajouter à la téléconférence.

   L'utilisateur (hôte) à l'origine de la téléconférence est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste **Recommandations** .

   Remarque : Assurez-vous que les participants que vous sélectionnez ont une adresse e-mail valide.

Commencer une téléconférence



8. Après avoir sélectionné les participants, décrivez brièvement la raison du démarrage de la téléconférence dans le champ Description.
   La description que vous fournissez sera ajoutée à l'enregistrement de la conférence.
9. Une fois la liste des participants finalisée, sélectionnez **Démarrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La téléconférence commence sur le pont de conférence sélectionné. Tous les participants sont avertis par e-mail, et ils le sont également via le pont de conférence respectif qui a été sélectionné.

10. Sélectionnez l'option **Cliquer ici** en plus de l'incident de sécurité majeur pour rejoindre la téléconférence. Les participants peuvent utiliser le lien de la notification par e-mail ou la notification du pont de conférence sélectionné pour rejoindre l'appel.
11. Ouvrez l'incident de sécurité majeur associé pour afficher les détails de la téléconférence. Lorsque le dernier participant quitte la conférence, la téléconférence se termine ou sélectionnez **Mettre fin à l'appel** pour mettre fin à la téléconférence.

Ajouter des participants à une téléconférence

Ajoutez des participants à une téléconférence à l'aide de l'option de recherche de la fenêtre contextuelle **Démarrer la téléconférence** pour rechercher et ajouter les participants requis. Vous pouvez également ajouter des participants en sélectionnant les participants dans la liste Recommandations, qui fournit des recommandations aux participants à ajouter à la téléconférence.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche

L'utilisateur (hôte) à l'origine de la téléconférence est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste Recommandations.

Les participants à l'appel peuvent inclure les éléments suivants :

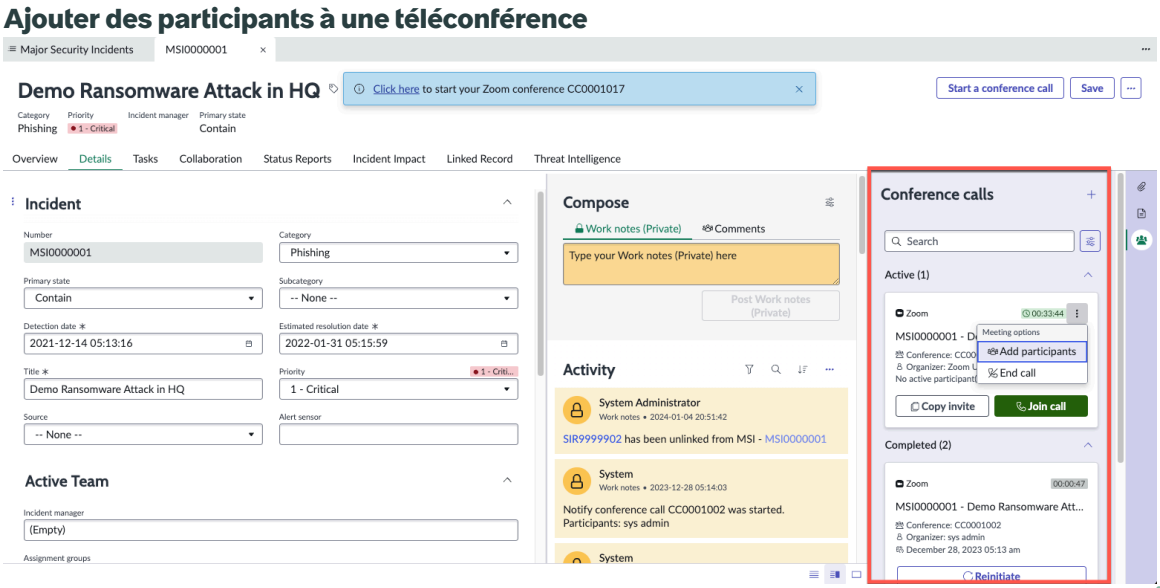
- Utilisateurs auxquels des responsabilités spécifiques ont été affectées.
- Contacts ad hoc ou à la demande
- Autres contacts de tiers

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez l'incident de sécurité majeur que vous essayez de résoudre lors de la téléconférence.
3. Sélectionnez l'icône  dans le menu contextuel de droite pour afficher les détails des téléconférences. Cela inclut des détails tels que le nom du pont de conférence, le nom de l'organisateur, la date, l'heure, la durée de l'appel, les participants actifs et inactifs.
4. Sélectionnez en regard de la téléconférence active, puis sélectionnez l'option **Ajouter des participants** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Vous pouvez utiliser l'option de recherche pour rechercher et ajouter les participants requis, ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations aux participants à ajouter à la téléconférence.
6. Après avoir sélectionné les participants, décrivez brièvement la raison du démarrage de la téléconférence dans le champ Description.
   Tous les participants sont avertis par e-mail, et ils le sont également via le pont de conférence respectif qui a été sélectionné. Les participants peuvent utiliser le lien de la notification par e-mail ou la notification du pont de conférence sélectionné pour rejoindre l'appel.
7. Vous pouvez également ajouter des participants en sélectionnant l'option **Copier l'invitation** dans la section Téléconférences du menu contextuel droit, et vous pouvez partager avec les participants requis.

Désactiver le micro des participants à une téléconférence active

En tant que gestionnaire MSI ou hôte de téléconférence, vous avez la possibilité de désactiver le micro d'un participant particulier ou de tous les participants à la téléconférence.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Avant de commencer cette procédure, vérifiez qu'il y a une téléconférence active avec un ou plusieurs participants.

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez l'incident de sécurité majeur que vous essayez de résoudre lors de la téléconférence.
3. Sélectionnez l'icône  dans le menu contextuel de droite pour afficher les détails des téléconférences.
4. Sélectionnez **Rejoindre l'appel** sur le pont de conférence actif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Après avoir rejoint la téléconférence, sélectionnez un participant dont vous souhaitez mettre le micro et sélectionnez **Désactiver le micro** sur le pont de conférence.
6. Pour désactiver le micro de tous les participants à la téléconférence, sélectionnez **Participants** dans les contrôles de réunion, puis sélectionnez **Désactiver tous les micros**.

Afficher les détails de la téléconférence

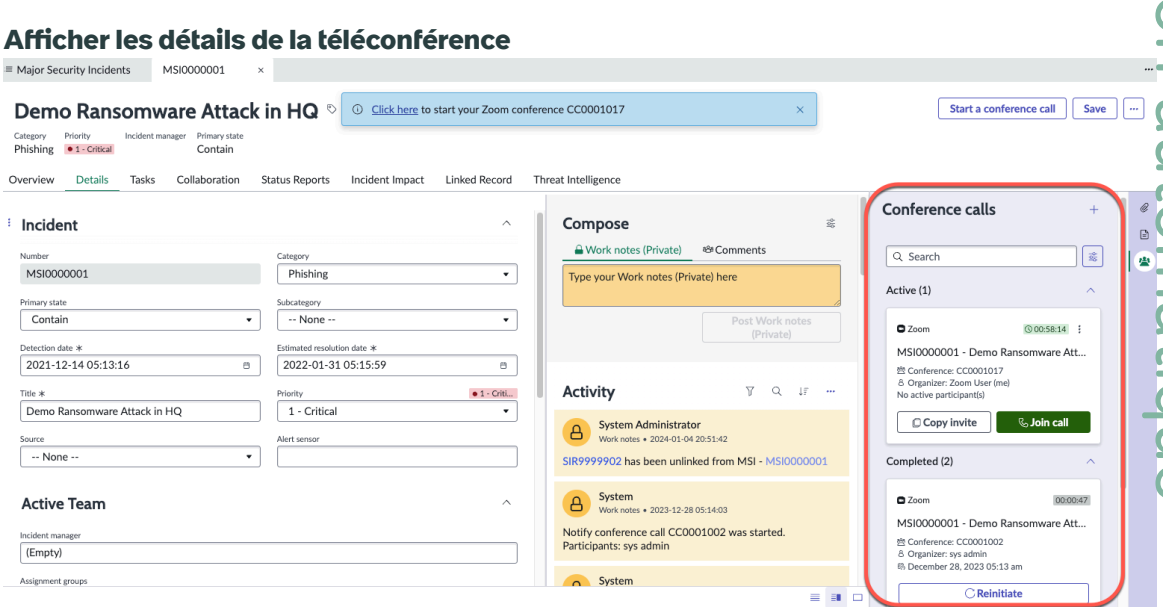
Les téléconférences sont répertoriées en tant qu'activités système dans la section Activité de l'incident de sécurité majeur et dans la liste connexe des téléconférences. Vous pouvez afficher des détails tels que le nom du pont de conférence, le nom de l'organisateur, la date, l'heure, la durée de l'appel, les participants actifs et inactifs.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez l'incident de sécurité majeur que vous essayez de résoudre lors de la téléconférence.
3. Sélectionnez l'icône  dans le menu contextuel de droite pour afficher les détails des téléconférences. Cela inclut des détails tels que le nom du pont de conférence, le nom de l'organisateur, la date, l'heure, la durée de l'appel, les participants actifs et inactifs.



4. Vous pouvez utiliser l'option de recherche pour rechercher une téléconférence particulière. Il peut y avoir plusieurs appels pour le même incident de sécurité majeur.
5. Pour ajouter des participants à une téléconférence, sélectionnez Options ⋮ en regard de la téléconférence téléphonique active, puis sélectionnez l'option **Ajouter des participants** .
6. Vous pouvez également ajouter des participants en utilisant l'option **Copier l'invitation** et en partageant le lien avec les participants requis.
7. Pour rejoindre une téléconférence, accédez à la section Actif et sélectionnez l'option **Rejoindre l'appel** de la téléconférence requise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Pour terminer une téléconférence, sélectionnez Options en regard de la téléconférence active, puis sélectionnez l'option **Mettre fin à l'appel** .
9. Pour redémarrer une téléconférence, accédez à la section Terminé et sélectionnez l'option **Réinitier** de la téléconférence requise.

Intégrer les téléconférences MSIM à Microsoft Teams

L'intégration de la téléconférence Microsoft Teams vous permet de gérer et de lancer une Microsoft Teams téléconférence directement à partir d'un incident de sécurité majeur.

Fonctionnalités principales

- Démarrez et terminez Microsoft Teams les téléconférences directement à partir d'incidents de sécurité majeurs ou d'une tâche de la console de sécurité majeure.
- Gérez une téléconférence en ajoutant ou en supprimant des Microsoft Teams participants.

Prérequis

Vérifiez que vous avez installé les modules d'extension suivants Centre d'intégration sur votre ServiceNow instance.

- Notification Module d'extension (com.snc.notify)
- Microsoft Teams Module d'extension Communications Spoke (sn_msteams_com_spk).
- Module d'extension Mappage de l'utilisateur Azure Active Directory (sn_now_azure).
- Notification Composants d'interface utilisateur pour les espaces de travail configurables

Pour plus d'informations, consultez Demander Centre d'intégration .

Configuration

- Pour configurer l'intégration de la téléconférence Microsoft Teams MSIM à l'aide de l'application préconfigurée, reportez-vous à la section Intégrer l'application prépubliée du connecteur Notification à Microsoft Teams .
- Pour configurer l'intégration de la téléconférence Microsoft Teams MSIM à l'aide de l'application autoconfigurée, reportez-vous à la section Intégrationde l'application autoconfigurée du connecteur Notification avec Microsoft Teams .

Utiliser l'intégration de la téléconférence Microsoft Teams MSIM

Les étapes suivantes vous expliquent comment gérer et lancer une Microsoft Teams téléconférence directement à partir d'un incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

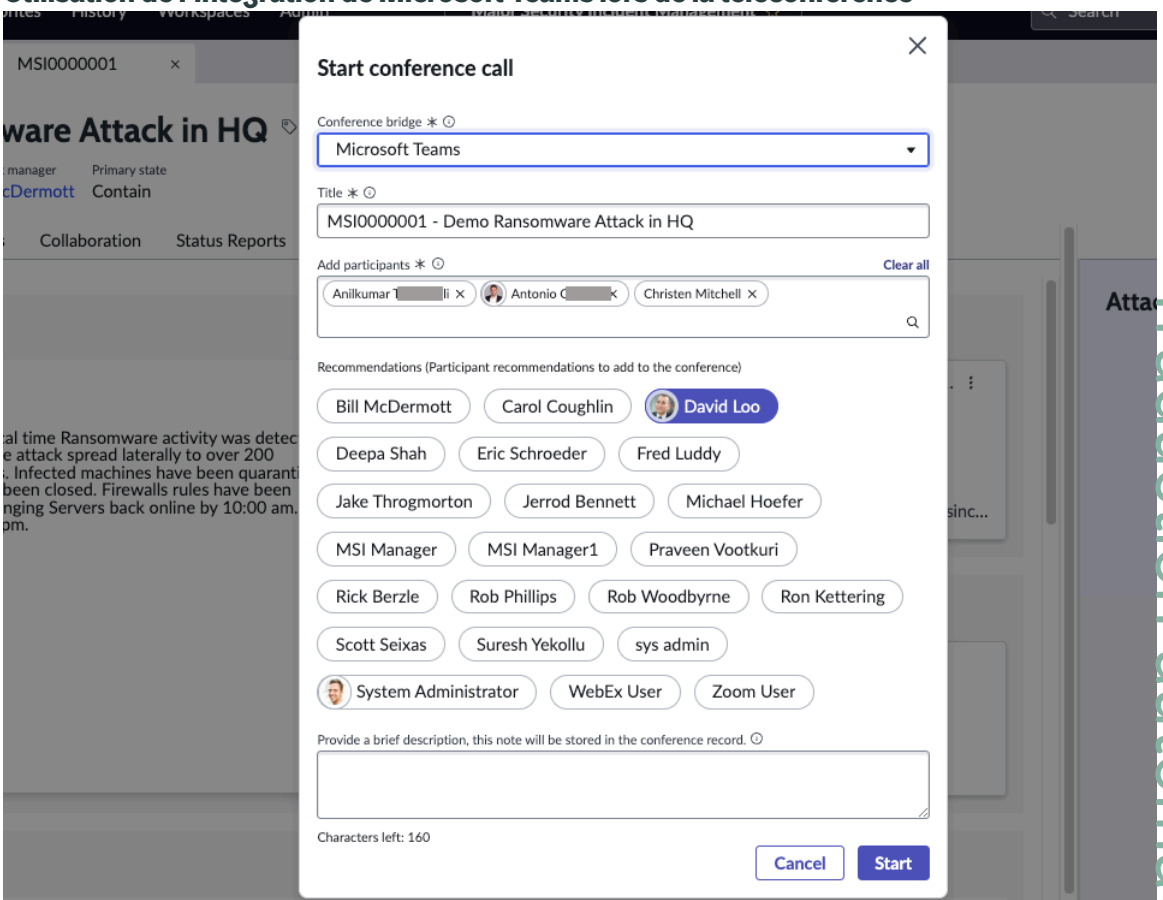
1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez un incident de sécurité majeur.
3. Sélectionnez l'action **Démarrer une téléconférence** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Vous pouvez également démarrer une téléconférence en sélectionnant l'icône dans le menu contextuel de droite et en sélectionnant l'icône +.
   La fenêtre contextuelle Démarrer la téléconférence s'affiche.
5. Choisissez **Microsoft Teams** comme pont de conférence à partir duquel vous souhaitez vous connecter.
6. Dans le champ Titre, fournissez un titre qui décrit le motif de la téléconférence Microsoft Teams.

Utilisation de l'intégration de Microsoft Teams lors de la téléconférence



7. Dans le champ Ajouter des participants, sélectionnez les participants à la téléconférence Microsoft Teams. Vous pouvez utiliser l'option de recherche pour trouver et ajouter les participants requis ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations de participants à ajouter à la téléconférence Microsoft Teams.

   L'utilisateur (hôte) qui lance la téléconférence Microsoft Teams est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste **Recommandations** .

   Remarque : Assurez-vous que les participants que vous sélectionnez ont une adresse e-mail valide.

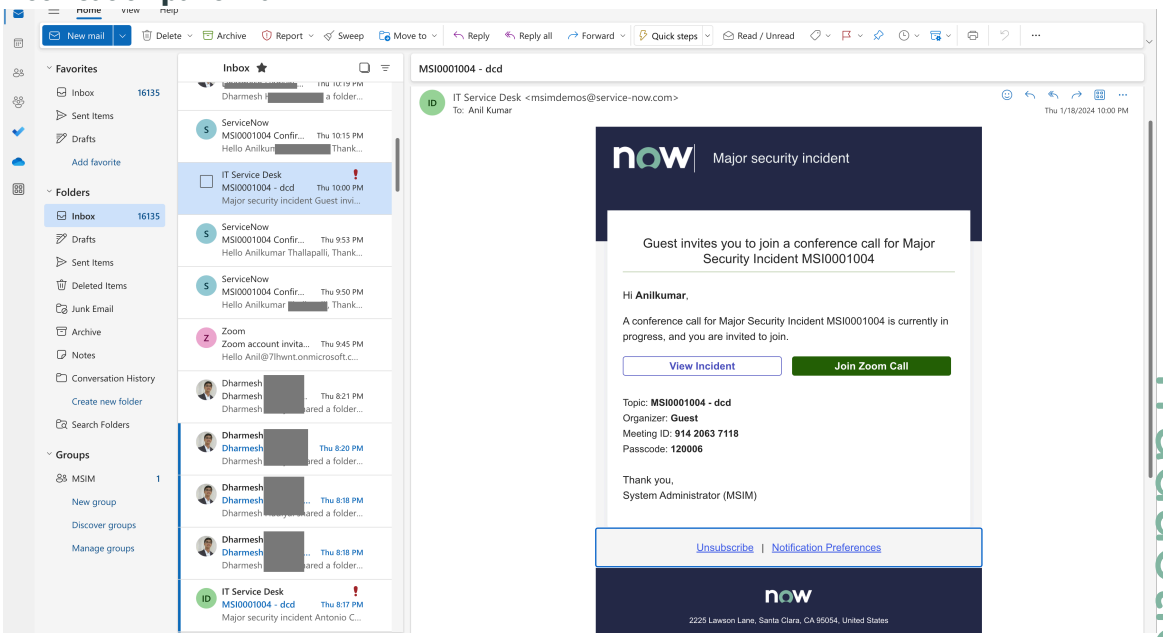
8. Après avoir sélectionné les participants, décrivez brièvement la raison du démarrage de la téléconférence dans le champ Description.
   La description que vous fournissez sera ajoutée à l'enregistrement de la conférence.
9. Une fois la liste des participants finalisée, sélectionnez **Démarrer**.
   La téléconférence commence dans l'application Microsoft Teams. Tous les participants sont avertis par e-mail depuis l'application MSIM et l'autre notification est envoyée via un bot sur l'application Microsoft Teams.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Sélectionnez l'option **Cliquer ici** en haut de l'incident de sécurité majeur pour rejoindre la téléconférence sur l'application Microsoft Teams.
    Les participants peuvent utiliser le lien de la notification par e-mail MSIM ou de l'application Microsoft Teams pour rejoindre l'appel.

Notification par e-mail



11. Ouvrez l'incident de sécurité majeur associé dans l'espace de travail MSIM pour afficher les détails de la téléconférence.

    Lorsque le dernier participant quitte l'appel, la téléconférence se termine ou sélectionnez **Mettre fin à l'appel** dans la section Téléconférence pour terminer la téléconférence.

Intégrer les téléconférences MSIM à Zoom

L'intégration de la téléconférence Zoom vous permet de gérer et de lancer une Zoom téléconférence directement à partir d'un incident de sécurité majeur.

Fonctionnalités principales

- Démarrez et terminez Zoom les réunions directement à partir de n'importe quel enregistrement de tâche tel qu'un incident de sécurité majeur ou un changement ou même à partir de la console d'incident majeur.
- Gérer les Zoom réunions en ajoutant ou en supprimant des participants.
- Suivez et rapportez les détails de la réunion, tels que la durée de la réunion et les participants, pour une analyse plus approfondie.

Prérequis

Vérifiez que vous avez installé les modules d'extension suivants Centre d'intégration sur votre ServiceNow instance.

- Notification Module d'extension (com.snc.notify)
- Zoom Spoke (sn_zoom_spoke)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Notification Zoom (sn_notify_zoom)
- Notification Composants d'interface utilisateur pour les espaces de travail configurables

Pour plus d'informations, consultez Demander Centre d'intégration .

Configuration

Pour configurer l'intégration de la téléconférence Zoom MSIM à l'aide du canal de communication, reportez-vous à la Notification section Configurer le connecteur Zoom de Notification dans Notification .

Utiliser l'intégration de la téléconférence Zoom MSIM

Les étapes suivantes vous expliquent comment gérer et lancer une Zoom téléconférence directement à partir d'un incident de sécurité majeur.

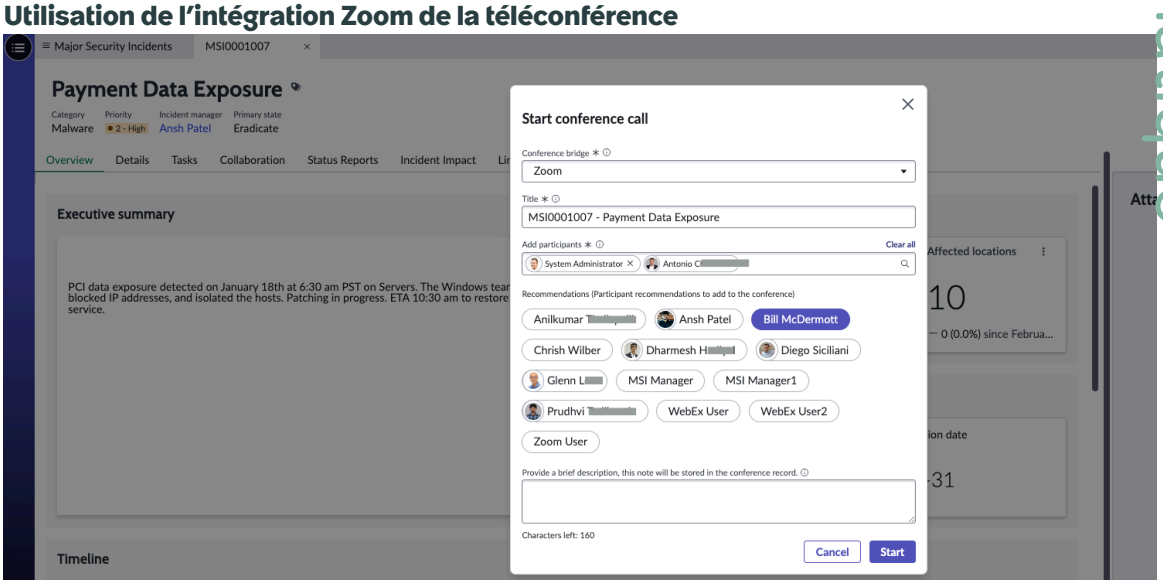
Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez un incident de sécurité majeur.
3. Cliquez sur l'action **Démarrer une téléconférence** .
4. Vous pouvez également démarrer une téléconférence en cliquant sur l'icône dans le menu contextuel de droite et en sélectionnant l'icône +.
   La fenêtre contextuelle Démarrer la téléconférence s'affiche.
5. Choisissez **Zoom** comme pont de conférence à partir duquel vous souhaitez vous connecter.
6. Dans le champ Titre, indiquez un titre qui décrit la raison de la téléconférence Zoom.

Utilisation de l'intégration Zoom de la téléconférence



7. Dans le champ Ajouter des participants, sélectionnez les participants à la téléconférence Zoom.
   Vous pouvez utiliser l'option de recherche pour trouver et ajouter les participants requis ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations de participants à ajouter à la téléconférence Zoom.

Traduction automatique

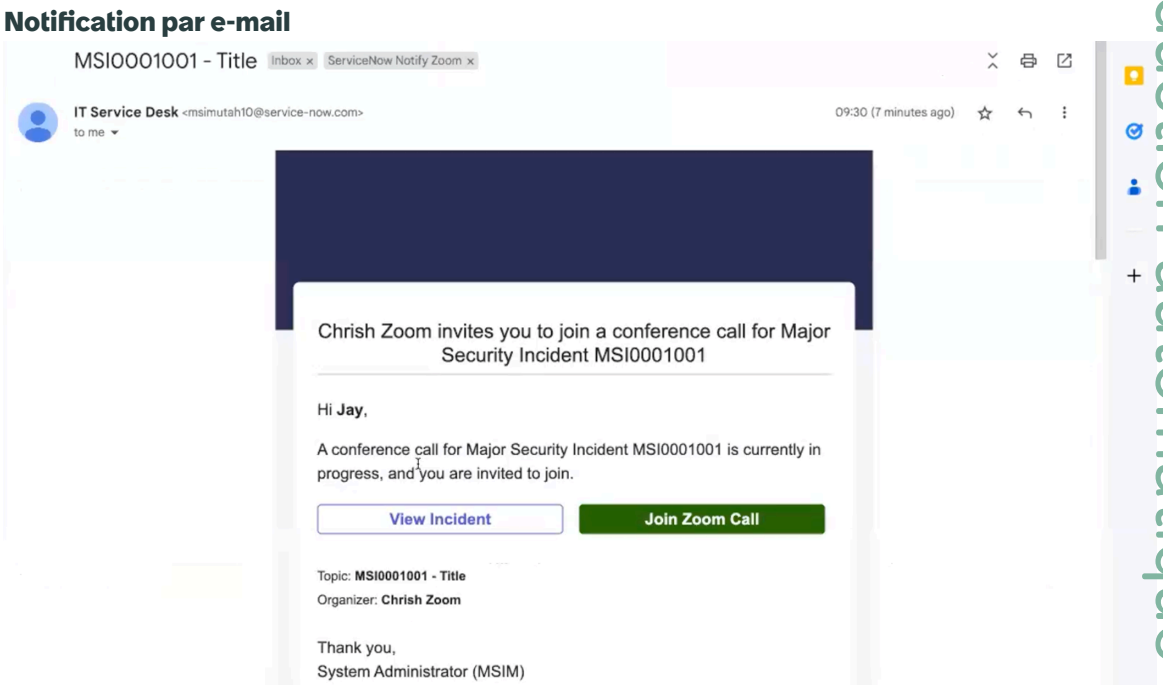
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'utilisateur (hôte) qui lance la téléconférence Zoom est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste **Recommandations** .

Remarque : Assurez-vous que les participants que vous sélectionnez ont une adresse e-mail valide.

8. Après avoir sélectionné les participants, décrivez brièvement la raison du démarrage de la téléconférence dans le champ Description.
   La description que vous fournissez sera ajoutée à l'enregistrement de la conférence.
9. Une fois la liste des participants finalisée, cliquez sur **Démarrer**.
   La conférence téléphonique commence dans l'application Zoom. Tous les participants sont informés par le biais de deux e-mails, l'un est envoyé aux participants depuis l'application MSIM et l'autre est envoyé depuis le pont de conférence Zoom.
10. Sélectionnez l'option **Cliquer ici** en haut de l'incident de sécurité majeur pour rejoindre la téléconférence sur l'application Zoom.
    Les participants peuvent utiliser le lien de la notification par e-mail MSIM ou de l'application Zoom pour rejoindre l'appel.

Notification par e-mail



11. Ouvrez l'incident de sécurité majeur associé dans l'espace de travail MSIM pour afficher les détails de la téléconférence.

Lorsque le dernier participant quitte l'appel, la téléconférence se termine ou sélectionnez **Mettre fin à l'appel** dans la section Téléconférence pour terminer la téléconférence.

Si la téléconférence a été enregistrée, l'enregistrement sera disponible dans la section Téléconférence de l'incident de sécurité majeur associé après un certain temps.

Intégrer les téléconférences MSIM à Cisco Webex

L'intégration MSIM Conference Call Cisco Webex vous permet de gérer et d'initier une Cisco Webex téléconférence directement à partir d'un incident de sécurité majeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalités principales

- Démarrez et terminez les Cisco Webex réunions directement à partir d'incidents de sécurité majeurs.
- Gérez une réunion en ajoutant ou en supprimant des Cisco Webex participants.

Prérequis

Vérifiez que vous avez installé les modules d'extension suivants Centre d'intégration sur votre ServiceNow instance.

- Notification Module d'extension (com.snc.notify)
- Notification Cisco Webex Connecteur (sn_notify_webex)
- Cisco Webex Spoke Teams (sn_cisco_teams_spk)
- Notification Composants d'interface utilisateur pour les espaces de travail configurables

Pour plus d'informations, consultez Demander Centre d'intégration .

Configuration

Pour configurer l'intégration de la téléconférence Cisco Webex MSIM à l'aide du canal de communication, reportez-vous à la Notification section Configurer Notification Cisco le connecteur Webex .

Utiliser l'intégration des téléconférences Cisco Webex

Les étapes suivantes vous expliquent comment gérer et lancer une Cisco Webex téléconférence directement à partir d'un incident de sécurité majeur.

Avant de commencer
Rôle requis : sn_msi.workspace_manager

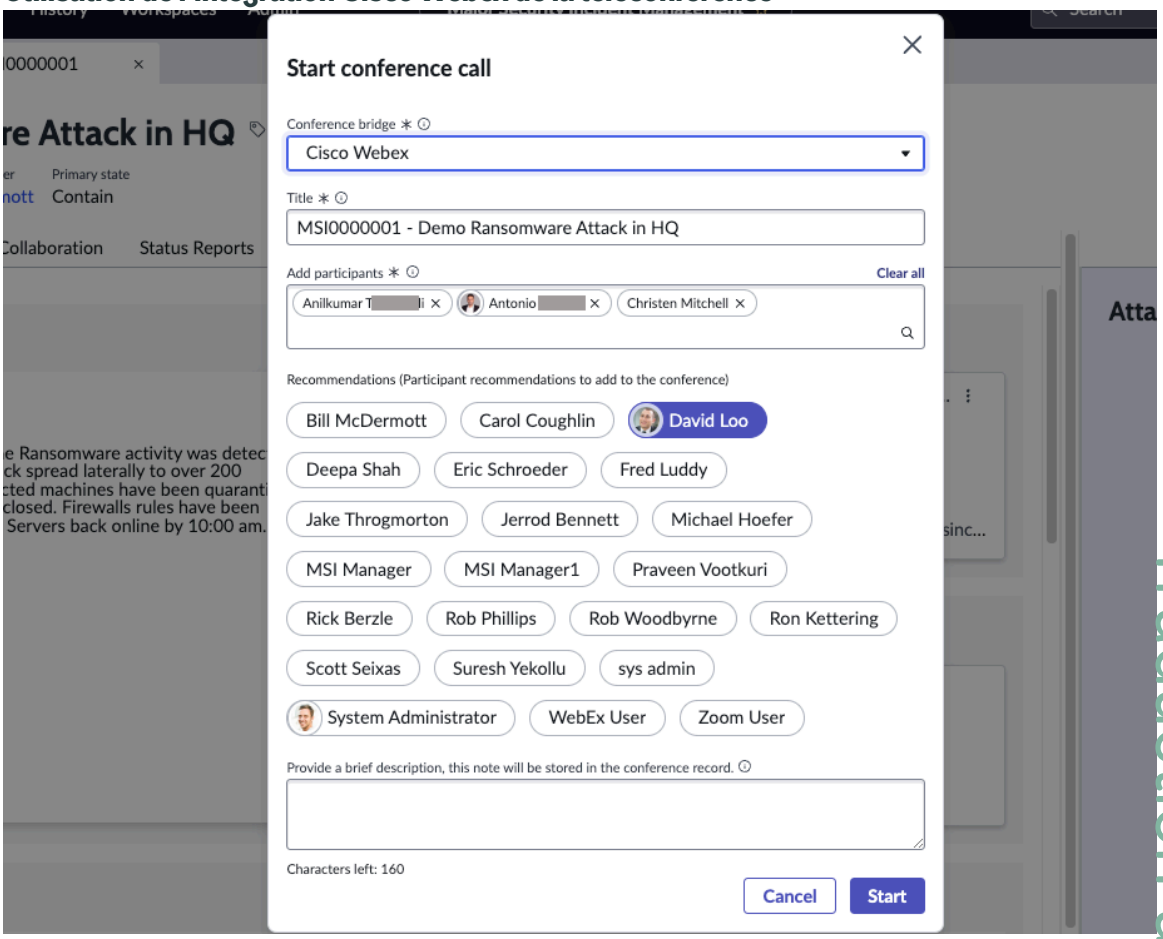
Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs**.
2. Dans la liste des incidents de sécurité majeurs, sélectionnez un incident de sécurité majeur.
3. Sélectionnez l'action **Démarrer une téléconférence** .
4. Vous pouvez également démarrer une téléconférence en sélectionnant l'icône  dans le menu contextuel de droite et en sélectionnant l'icône +.
   La fenêtre contextuelle Démarrer la téléconférence s'affiche.
5. Choisissez **Cisco Webex** comme pont de conférence à partir duquel vous souhaitez vous connecter.
6. Dans le champ Titre, fournissez un titre qui décrit la raison de la téléconférence Cisco Webex.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation de l'intégration Cisco Webex de la téléconférence



7. Dans le champ Ajouter des participants, sélectionnez les participants à la téléconférence Cisco Webex. Vous pouvez utiliser l'option de recherche pour trouver et ajouter les participants requis ou sélectionner les participants dans la liste **Recommandations** , qui fournit des recommandations de participants à ajouter à la téléconférence Cisco Webex.

   L'utilisateur (hôte) qui lance la téléconférence Cisco Webex est automatiquement ajouté à la liste des participants sélectionnés. Tous les utilisateurs associés à l'incident de sécurité majeur sont disponibles par défaut dans la liste **Recommandations** .

   Remarque : Assurez-vous que les participants que vous sélectionnez ont une adresse e-mail valide.

8. Après avoir sélectionné les participants, décrivez brièvement la raison du démarrage de la téléconférence dans le champ Description.
   La description que vous fournissez sera ajoutée à l'enregistrement de la conférence.

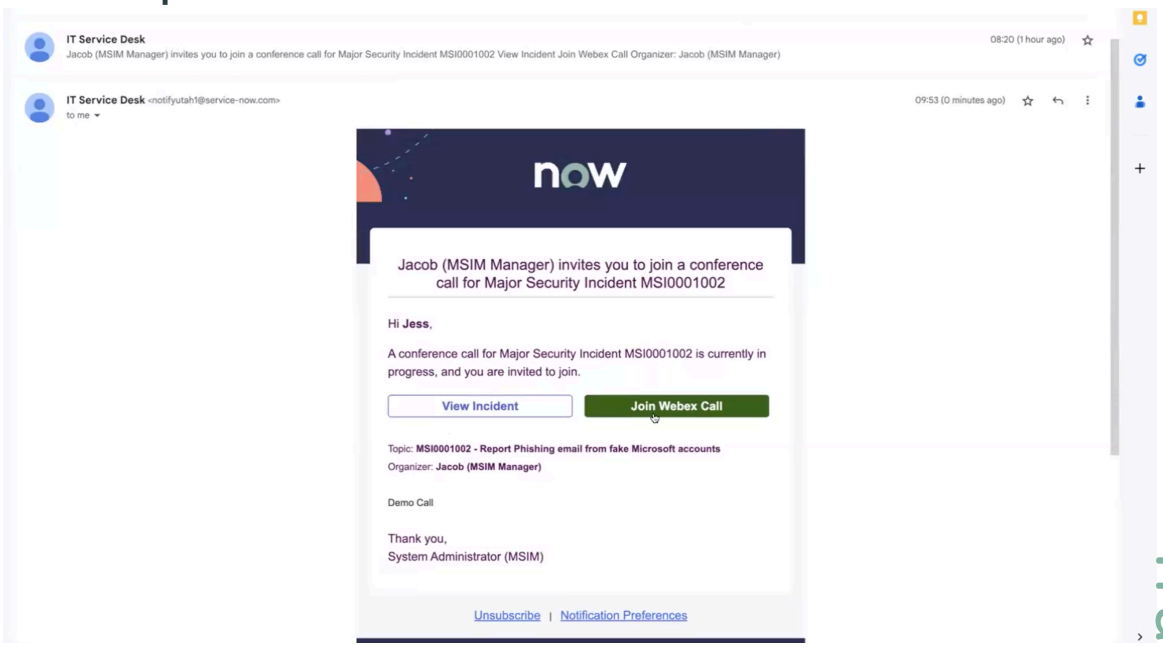
9. Une fois la liste des participants finalisée, sélectionnez **Démarrer**.
   La téléconférence commence dans l'application Cisco Webex. Tous les participants sont informés par le biais de deux e-mails, l'un est envoyé aux participants à partir de l'application MSIM et l'autre est envoyé à partir du pont de conférence Cisco Webex.

10. Sélectionnez l'option **Cliquez ici** en haut de l'incident de sécurité majeur pour rejoindre la téléconférence sur l'application Cisco Webex.
    Les participants peuvent utiliser le lien de la notification par e-mail MSIM ou de l'application Cisco Webex pour rejoindre l'appel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notification par e-mail



11. Ouvrez l'incident de sécurité majeur associé dans l'espace de travail MSIM pour afficher les détails de la téléconférence.

    Lorsque le dernier participant quitte l'appel, la téléconférence se termine ou sélectionnez **Mettre fin à l'appel** dans la section Téléconférence pour terminer la téléconférence.

    Si la téléconférence a été enregistrée, l'enregistrement sera disponible dans la section Téléconférence de l'incident de sécurité majeur associé après un certain temps.

Configurer Gestion des incidents de sécurité majeurs

Installez et configurez Gestion des incidents de sécurité majeurs l'application.

Important :

- Pour démarrer rapidement la Gestion des incidents de sécurité majeurs configuration, vous pouvez consulter le Guide de démarrage rapide de Major Security Incident Management (MSIM) sur le ServiceNow Store.
- Après avoir installé l'application Gestion des incidents de sécurité majeurs , assurez-vous d'importer l'ensemble de mises à jour dans KB1289784 pour charger les fichiers partiellement préconfigurés.

Utilisez cette section pour apprendre à configurer les configurations nécessaires pour travailler avec Incident de sécurité majeur les enregistrements en les intégrant à d'autres applications externes Microsoft afin d'établir des connexions avec ServiceNow l'instance.

Configurer le composant de l'explorateur de fichiers

Le composant de l'espace de travail Explorateur de fichiers organise et suit la collecte d'artefacts (fichiers) liés à un incident de sécurité majeur. Il est conçu pour prendre en charge l'intégration avec n'importe quel fournisseur d'hébergement de fichiers tiers, par exemple Microsoft SharePoint dans l'espace de Gestion des incidents de sécurité majeurs travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- File Explorer Composant : fournit une interface utilisateur graphique pour afficher le système de fichiers et permet aux utilisateurs d'effectuer des opérations sur les fichiers.
- File Explorer Core : fournit une couche d'abstraction qui permet au composant de l'explorateur de fichiers d'afficher le système de fichiers et d'effectuer diverses opérations de fichier sans rien savoir du connecteur sous-jacent utilisé pour communiquer avec les référentiels externes.
- File Explorer Microsoft SharePoint Application Connecteur : fournit les modules d'implémentation nécessaires pour suivre et extraire les métadonnées des fichiers/dossiers d'une bibliothèque de documents et effectuer des Microsoft SharePoint opérations sur les fichiers.

Le File Explorer composant Core fournit une infrastructure de base requise pour les différentes applications de connecteur de partage de fichiers afin de définir ses propriétés de connexion.

Vous devez installer et configurer le lecteur de référentiel de fichiers et le fournisseur de référentiel de fichiers en ajoutant les propriétés de connexion pour extraire les métadonnées des fichiers à partir d'un emplacement de fournisseur d'hébergement de fichiers.

Pour cette version actuelle de , File Explorer ces instructions incluent la configuration et l'abonnement à un fichier de récupération des métadonnées telles que Microsoft SharePoint les mises à jour de fichiers et de dossiers, les opérations de fichiers et l'activité de journalisation des fichiers. Une bibliothèque de documents désignée Microsoft SharePoint et une configuration de lecteur connexe seront nécessaires pour créer des dossiers individuels spécifiques à un incident de sécurité majeur.

File Explorer permet également des applications de connecteur telles que Microsoft SharePoint. Vous pouvez utiliser cet exemple pour configurer ses implémentations d'opération de fichier, telles que **Télécharger** ou **Renommer** Les actions de dossier et de fichier seront activées dans le composant de l'espace de travail de l'explorateur de fichiers. Ces actions sont activées et exécutées à l'aide des sous-flux intégrés du concepteur de flux. Pour plus d'informations, voir Paramètres d'action de dossier et de fichier.

File Explorer La configuration comprend la configuration suivante :

- Configurer le lecteur de référentiel de l'explorateur de fichiers
- Configurer les paramètres d'action de fichier et de dossier
- Créer des modèles de dossier

Mise en route de l'Explorateur de fichiers

Examinez les informations suivantes avant de commencer à utiliser File Explorer le composant.

Examinez les informations suivantes avant de commencer à établir la connexion avec Microsoft SharePoint, à créer des actions de dossier et de fichier et à créer des modèles de dossier pour le composant d'explorateur de fichiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prérequis

Nom	Description
Microsoft SharePoint spoke, version 2.0.2 pour ServiceNow® Centre d'intégration.	Utilisez **sn_sp_spoke** ID de module d'extension pour rechercher et installer Microsoft SharePoint le spoke. L'installation de ce module d'extension fournit des flux et des actions pour automatiser la collaboration, la gestion des documents et les droits d'accès des utilisateurs dans Microsoft SharePoint.
Composant de l'explorateur de fichiers v1.1.0	Utilisez **sn_file_explorer** ID de module d'extension pour rechercher et installer le composant de l'explorateur de fichiers v1.1.0 L'installation de ce module d'extension fournit une interface utilisateur graphique pour parcourir le système de fichiers, qui est disponible dans le noyau de l'explorateur de fichiers.
Cœur de l'explorateur de fichiers pour Opérations de sécurité v1.1.1	Utilisez **sn_fe** ID de module d'extension pour rechercher et installer File Explorer Core. L'installation de ce module d'extension fournit une infrastructure de base à intégrer à n'importe quel fournisseur d'hébergement de fichiers tiers.
Microsoft SharePoint Connecteur de l'explorateur de fichiers pour Security Operations v1.1.1	Utilisez **sn_fe_sharepoint** ID de module d'extension pour rechercher et installer Microsoft SharePoint le connecteur de l'explorateur de fichiers. L'installation de ce module d'extension gérera les fichiers/dossiers à l'aide de l'explorateur Microsoft SharePoint de fichiers.

Configurer le lecteur de référentiel de l'explorateur de fichiers

Le Microsoft SharePoint connecteur fournit diverses fonctionnalités à implémenter dans Microsoft SharePoint les fonctionnalités de l'explorateur de fichiers en gérant et en suivant les métadonnées des fichiers.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tous** > **Incident de sécurité majeur** > **Explorateur de fichiers** > **Configuration du référentiel de fichier**.
2. Renseignez les champs suivants comme décrit dans le tableau suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description de champ
Nom	Nom de l'enregistrement du référentiel de fichiers qui identifie l'utilisation. Par exemple, MSIM.
Fournisseur	Nom du fournisseur qui est le fournisseur de référentiel d'hébergement de fichiers tiers. Par exemple,Microsoft SharePoint.
Propriétés	
Chemin d'accès à l'URL du site	Entrez une Microsoft SharePoint URL avec un chemin d'accès au site spécifique. Fournir uniquement le chemin relatif vers le site et une URL complète du site peut ne pas être requise. Par exemple, Sites/MSIM.
Nom de la bibliothèque de documents	Créez une bibliothèque de documents sous le Microsoft SharePoint site et fournissez le même nom de bibliothèque de documents ici. Il s'agit de la même bibliothèque de documents que celle que vous avez créée dans la configuration du Microsoft SharePoint lecteur de connecteur.
Connexion graphique	Sélectionnez l'enregistrement du locataire du graphe de l'explorateur de fichiers. Pour plus d'informations sur la configuration de la connexion du locataire, voir Spoke Microsoft SharePoint.
Connexion REST	Sélectionnez l'enregistrement de locataire REST de l'explorateur de fichiers. Pour plus d'informations sur la configuration de la connexion du locataire, voir Spoke Microsoft SharePoint.

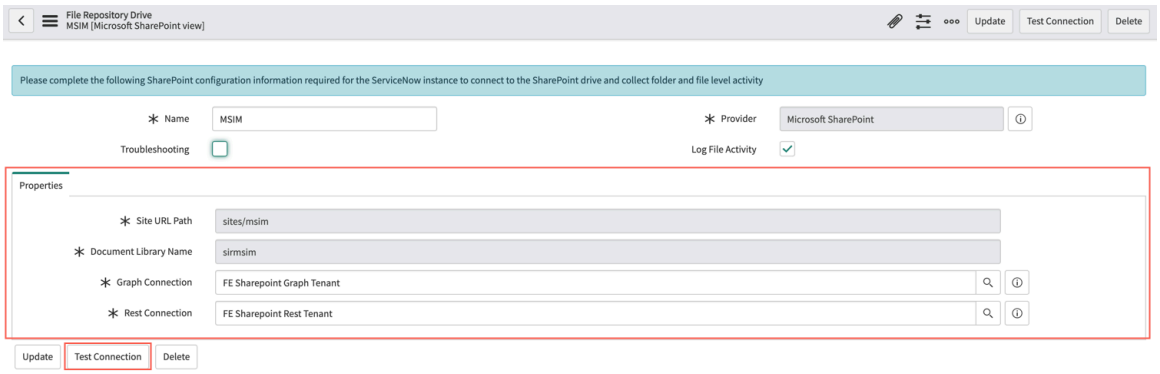
3. Sélectionnez **Enregistrer**.
4. Cliquer sur **Test de la connexion** Onglet permettant de tester la connexion et de valider les propriétés de configuration du lecteur de référentiel de fichiers.

   Remarque : Avant **d'activer** le référentiel de fichiers, assurez-vous que la bibliothèque Microsoft SharePoint de documents correspondante ne contient pas de données de dossier ou de fichier.

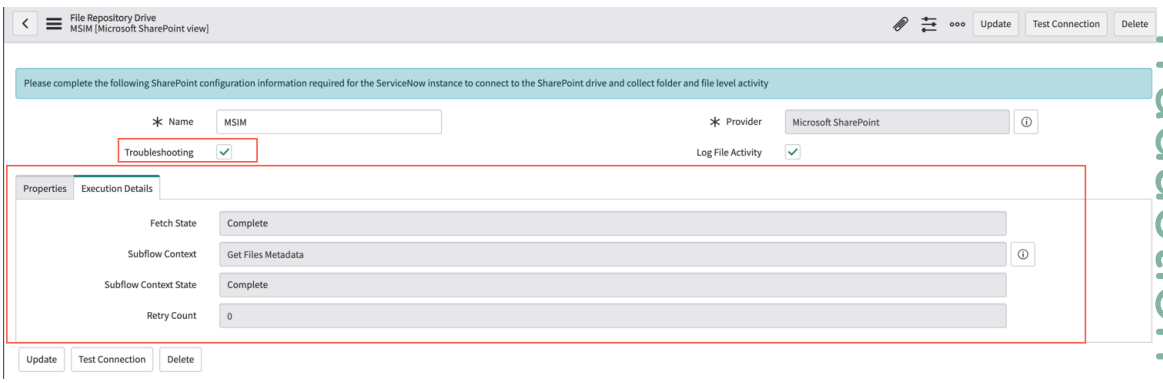
5. Cliquez sur **Activer** pour activer le référentiel de fichiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cochez la case **Dépannage** pour vérifier les **détails de l'exécution** du référentiel de fichiers et vérifier le **État d'extraction** est terminé et assurez-vous que le formulaire Abonnements au lecteur est créé et que l'état Microsoft SharePoint est terminé.



Remarque : À l'aide du bouton **Test de la connexion** , l'administrateur ou le gestionnaire MSI peut uniquement valider la configuration du référentiel de fichiers.

Configurer les paramètres d'action de fichier et de dossier

Sélectionnezles actions de dossier et de fichier que vous souhaitez activer à partir du composant Explorateur de fichiers de l'espace de travail Major Security Incident Management, à l'aide de la page de configuration Paramètres d'action de dossier et de fichier. En tant qu'administrateur MSI, vous pouvez contrôler les actions de dossier et de fichier individuelles affichées sur le composant de l'explorateur de fichiers.

Avant de commencer

Voici les options d'opérations de fichier implémentées dans le composant de l'explorateur de fichiers à l'aide du concepteur de ServiceNow® flux :

Options d'opérations de fichiers

Opération de fichier	Description
Ouvrir dans Microsoft SharePoint	Ouvre un nouvel onglet de navigateur pour afficher Microsoft SharePoint la vue des fichiers de la bibliothèque de documents
Créer un dossier	Possibilité de créer des dossiers ad hoc supplémentaires après la création de l'incident de sécurité majeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Options d'opérations de fichiers (suite)

Opération de fichier	Description
Renommer un dossier	Possibilité de renommer les dossiers créés.
Déplacer le fichier	Vous permet de déplacer des fichiers entre des dossiers dans le composant Explorateur de fichiers de l'espace de travail, ce qui entraîne le déplacement des fichiers dans Microsoft SharePoint
Localiser le fichier	Affiche l'emplacement du dossier lors de l'utilisation de **Récents** de l'explorateur de fichiers.
Supprimer le fichier	Supprimez le fichier.
Supprimer un dossier	Supprimez le dossier.
Télécharger le fichier	Télécharge le fichier dans l'onglet de navigateur existant de MSIM Workspace pour un affichage rapide.
Renommer un fichier	Renomme le fichier.

Remarque :

1. Toutes les actions répertoriées sont actuellement activées par défaut. Vous devrez modifier le **Paramètres de l'action de fichier** Si vous ne souhaitez pas que certaines actions apparaissent. Tous les paramètres sont actuellement globaux pour tous les utilisateurs, ce qui signifie qu'il n'est pas possible d'activer des actions pour un sous-ensemble d'utilisateurs ayant un rôle spécifique.
2. **Révoquer l'accès de l'utilisateur** et **Ajoutez des autorisations** Les actions sont des actions liées au système. Il est recommandé de ne pas modifier ces actions de fichier.

L'exemple de procédure suivant décrit l'une des fonctionnalités d'opération de fichier permettant de désactiver toute action spécifique sur un dossier et un fichier lors de la configuration du référentiel de l'explorateur de fichiers. Cette procédure s'applique à toutes les autres actions qui peuvent avoir besoin d'être modifiées :

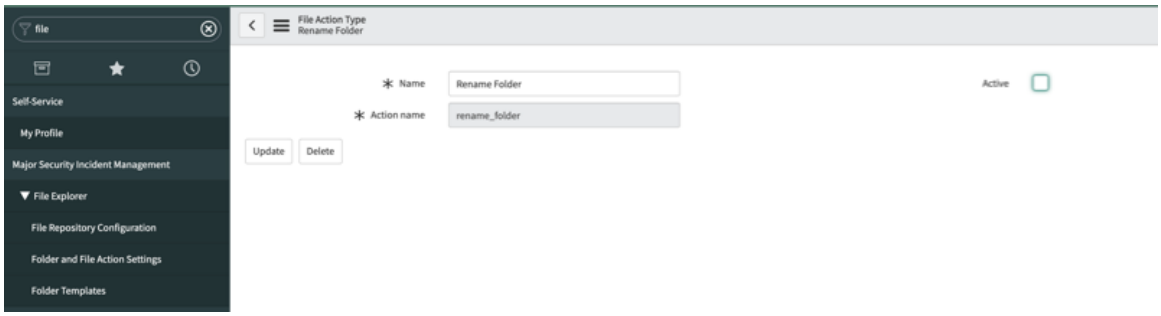
Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Explorateur de fichiers** > **Options pour l'action de fichier et de dossier**.
2. Sélectionnez l'enregistrement souhaité pour activer ou désactiver l'action du dossier ou du fichier respectivement.
3. Désélectionner **Actif** Cochez la case pour désactiver l'action Dossier et fichier.

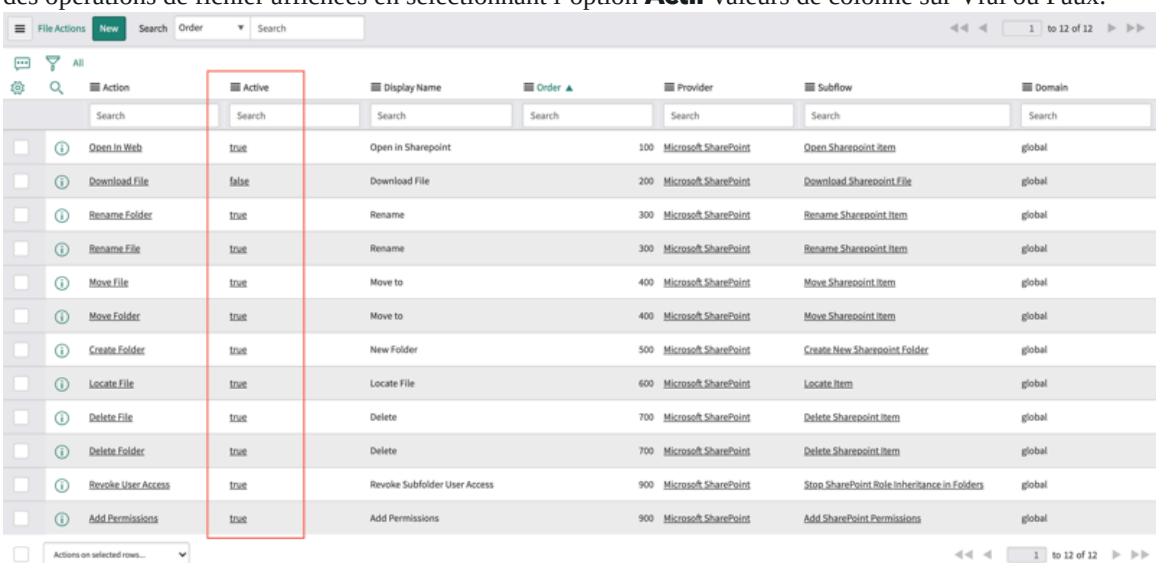
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

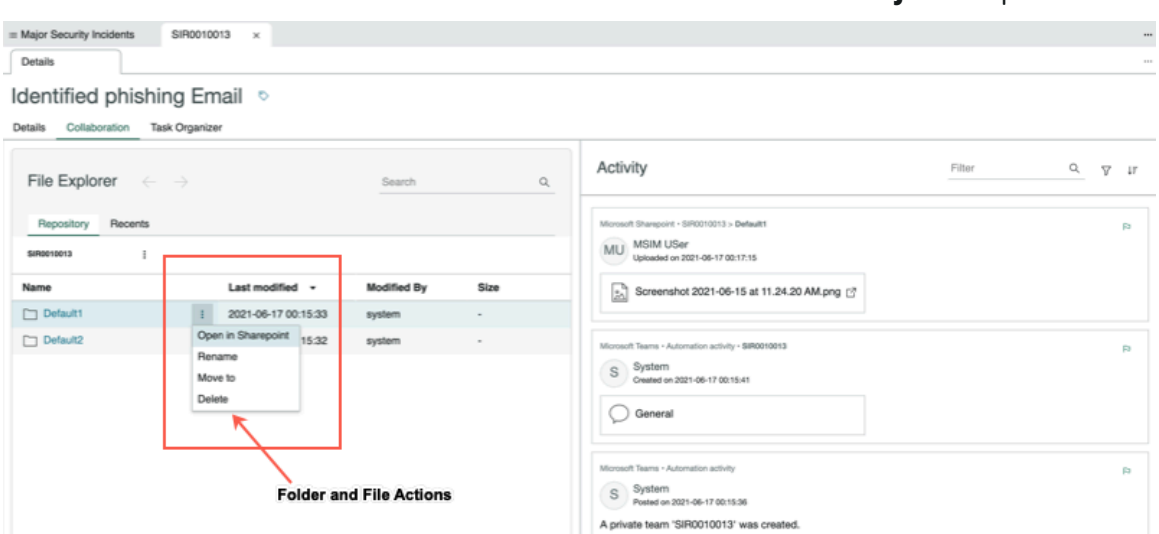


4. **Mettez à jour** l'enregistrement du lecteur.

Remarque : Vous pouvez également effectuer l'action de fichier directement à partir de la liste des opérations de fichier affichées en sélectionnant l'option **Actif** valeurs de colonne sur Vrai ou Faux.



Si l'action de fichier effectuée est désactivée, l'action ne sera pas affichée sur le **Collaborations** de la commande **Gestion des incidents de sécurité majeurs** Espace.



Créer des modèles de dossier

Utilisez des modèles de dossiers pour créer automatiquement des dossiers uniques pour différents types d'incidents de sécurité majeurs. Les modèles de dossiers du composant Explorateur de fichiers sont utilisés pour créer une structure de dossiers de base pour l'incident de sécurité dans le Microsoft SharePoint.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

En tant qu'administrateur MSI, vous définissez la structure de dossiers initiale nécessaire pour permettre la collaboration entre différents groupes d'intervenants en cas d'incident et attribuez les privilèges d'accès appropriés au niveau d'un sous-dossier. Plusieurs configurations peuvent être créées pour différents Incident de sécurité majeur types à l'aide d'un générateur de conditions pour des valeurs de champ spécifiques Incident de sécurité majeur , ce qui inclut l'autorisation d'accès à différents utilisateurs et groupes d'utilisateurs à chaque niveau de sous-dossier.

Remarque : Ces modèles de dossiers sont utilisés par tous les incidents de sécurité majeurs qui répondent aux conditions spécifiées dans le générateur de conditions. Il est recommandé d'utiliser des variables de champ d'incident, telles que le numéro ou la catégorie d'incident, pour créer des noms de dossier racine uniques qui distinguent un ensemble de sous-dossiers avec des noms de dossier communs pour un incident de sécurité majeur des dossiers similaires portant ces noms qui font partie d'un autre incident de sécurité majeur.

La configuration définie des modèles de dossier n'est appliquée à l'incident de sécurité majeur que lorsque la condition est remplie.

Remarque : Une configuration système de base (sans aucun sous-dossier) est appliquée à tous les incidents de sécurité. Vous pouvez modifier cette configuration par défaut pour inclure des sous-dossiers spécifiques ou créer une nouvelle configuration basée sur un ensemble spécifié de valeurs de champs d'incident de sécurité majeur. Par exemple, catégorie = activité du code malveillant.

Rôle requis : sn_msi.workspace_admin

Procédure

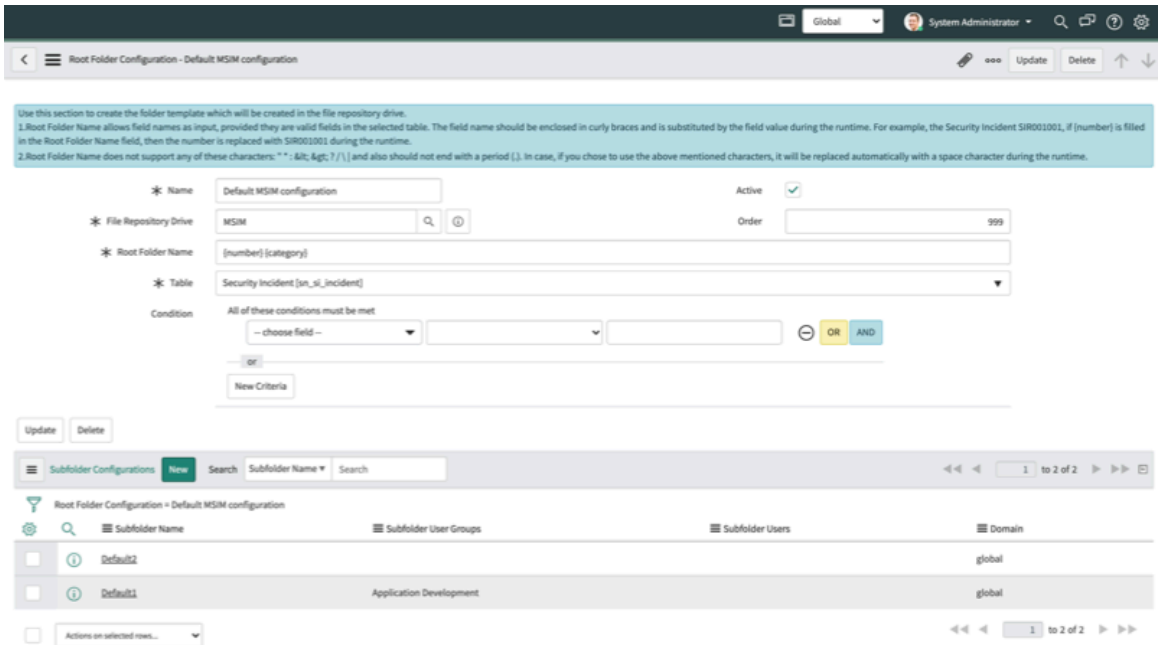
1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Explorateur de fichiers** > **Modèles de dossier**.
2. Cliquer sur **Nouveau** pour la configuration du dossier racine.
3. Renseignez les champs du formulaire.

Nom de champ	Description
Nom	Nom du modèle de dossier.
Lecteur de référentiel de fichiers	
Nom du dossier racine	Nom du dossier racine qui apparaîtra ainsi Microsoft SharePoint que dans l'explorateur de fichiers et devrait probablement inclure des variables de champ d'incident telles que le numéro et la catégorie de l'incident de sécurité majeur afin de pouvoir distinguer un incident de sécurité majeur d'un autre.
Table	

4. Définir l'incident de sécurité **Condition** Valeurs.

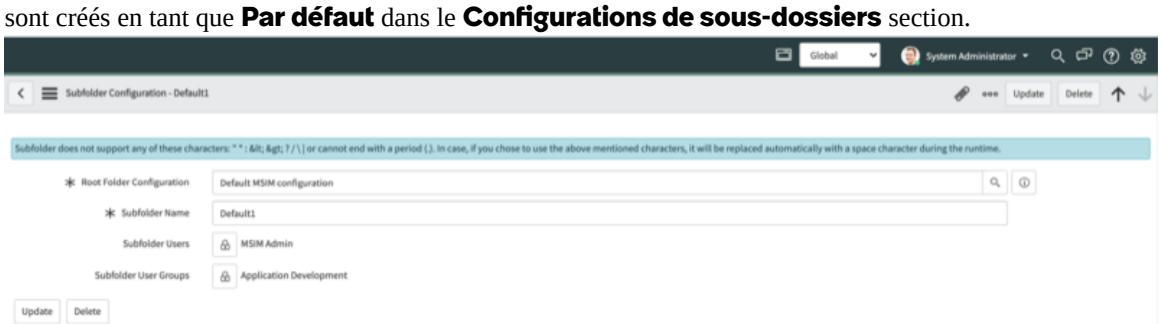
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. **Mettre à jour** le record.
   Les sous-dossiers sont créés avec les valeurs définies.

6. Cliquez sur le **sous-dossier** souhaité.
   Si vous ne créez pas de sous-dossier avec un nom approprié, les noms de sous-dossiers sont créés en tant que **Par défaut** dans le **Configurations de sous-dossiers** section.



La même structure de dossiers sera créée automatiquement à l'aide des Microsoft SharePoint mêmes privilèges d'accès qui sont configurés sur le **Modèles de dossier** la page.

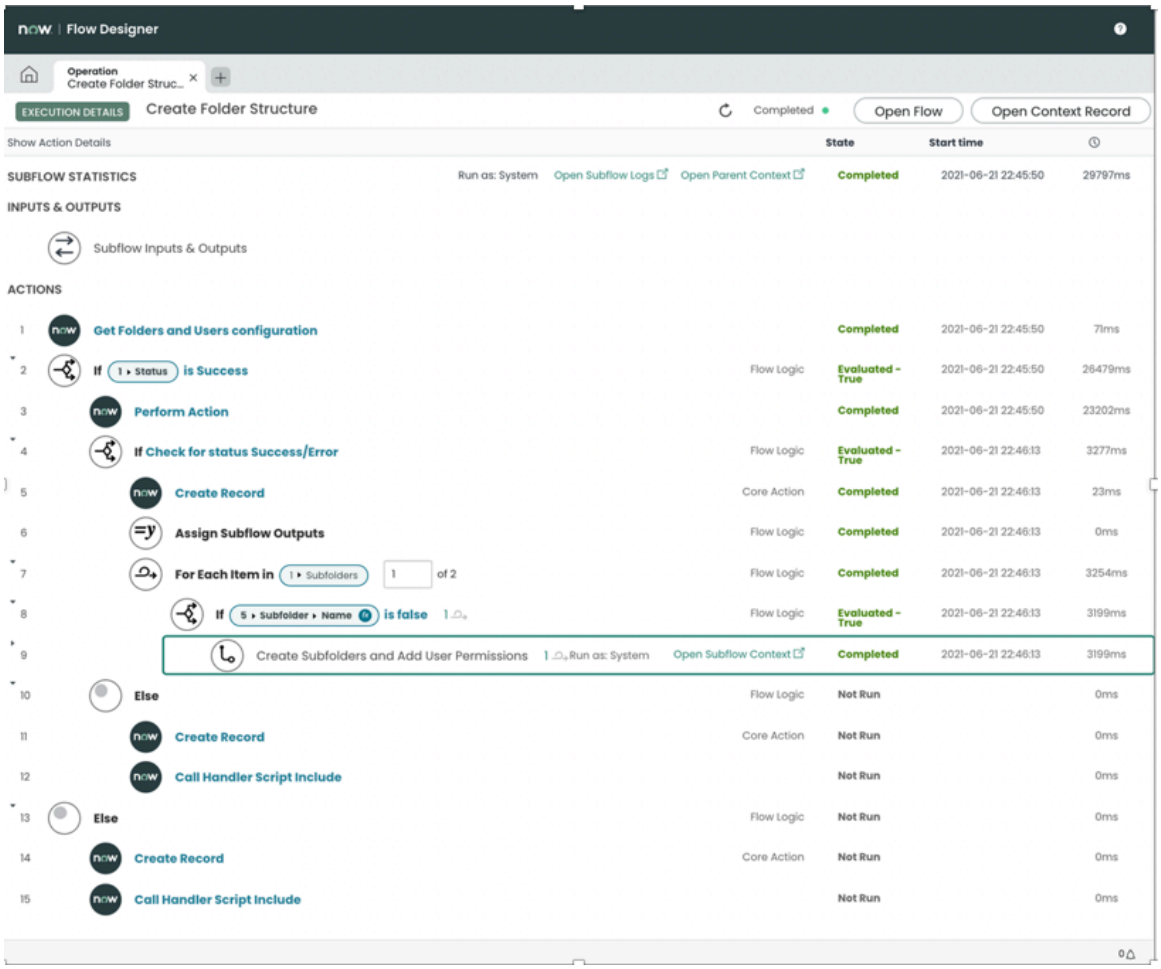
Remarque :

- **Le nom du dossier racine** autorise les noms de variables de champs comme entrée, à condition qu'il s'agisse de champs valides dans la table sélectionnée. Le nom du champ doit être entouré d'accolades et est remplacé par la valeur du champ pendant l'exécution du flux. Par exemple, pour le SIR001001 d'incident de sécurité, si la variable {number} est configurée dans le champ **Nom du dossier racine** , le numéro est remplacé par SIR001001 pendant l'exécution.
- **Nom du dossier racine** ne prend en charge aucun de ces caractères : " * : < > ? / \ | et aussi, ne doit pas se terminer par un point (.). Si vous utilisez les caractères mentionnés ci-dessus, ils seront automatiquement remplacés par un caractère d'espace pendant l'exécution.
- Si le nom du **dossier racine** et du **sous-dossier** dépasse la limite définie (256 caractères), le nom de dossier est tronqué.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voici l'exécution au moment de l'exécution du flux secondaire Créer une structure de dossiers :



File Explorer Flux d'activité dans l'espace de travail

Utilisez la section Explorateur de fichiers de l'espace Gestion des incidents de sécurité majeurs de travail pour afficher les dossiers et les fichiers, la séquence dans laquelle ils ont été créés dans Microsoft SharePoint la bibliothèque de documents.

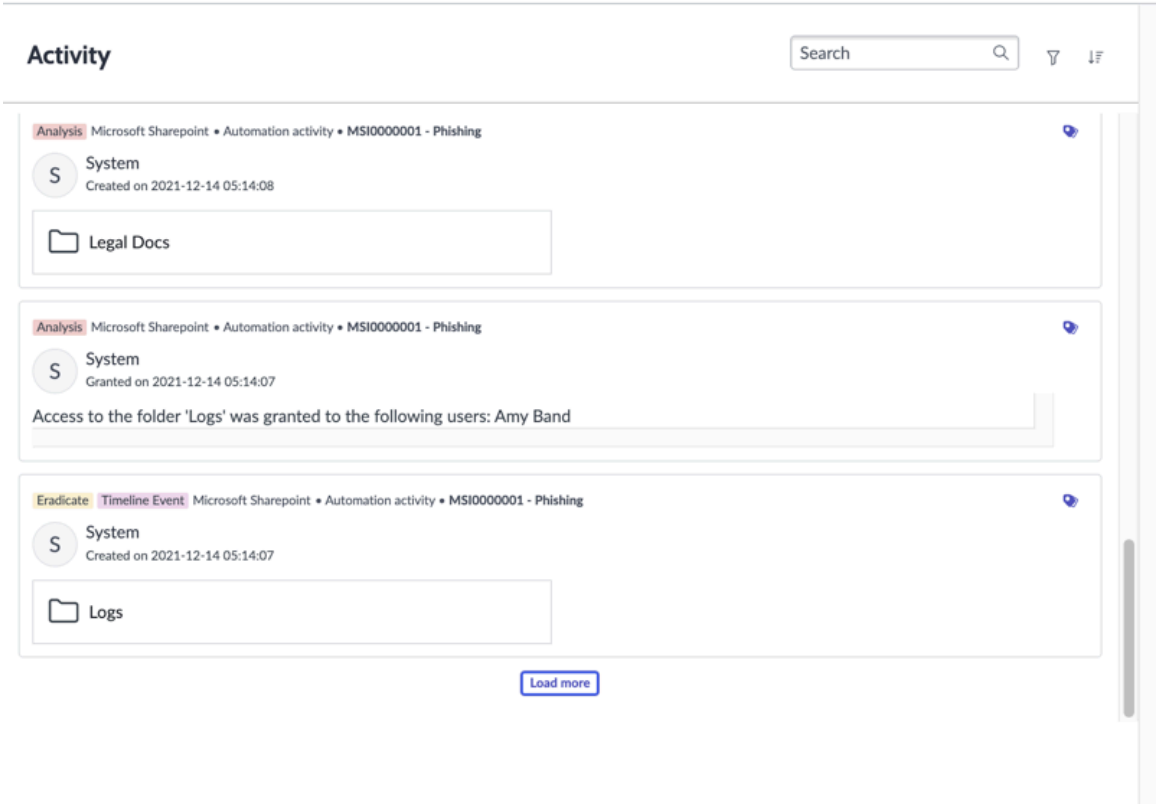
Le flux d'activité répertorie toutes les publications d'activités d'automatisation chaque fois qu'une activité de dossier et de fichier, ou des journaux se produisent pendant la Incident de sécurité majeur résolution. La structure du flux d'activités est alignée dans le même format que la Microsoft SharePoint bibliothèque, qui affiche les dossiers qui ont été créés et les utilisateurs ou groupes d'utilisateurs qui ont été affectés à ces dossiers.

Flux d'activité permet aux gestionnaires de l'espace de travail et à d'autres utilisateurs ou groupes d'utilisateurs de communiquer et de collaborer efficacement, de répertorier les activités qui ont été effectuées sur Microsoft SharePoint les dossiers et les fichiers, de surveiller l'état de l'incident, de publier les notes ou d'ajouter des commentaires supplémentaires qu'ils ont sur l'enregistrement d'incident. Les gestionnaires de l'espace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de travail peuvent reprendre et travailler en fonction de la dernière activité mise à



jour.

Dépannage de File Explorer

La section de dépannage peut vous aider à résoudre certains des problèmes techniques que vous pouvez rencontrer lors de la configuration File Explorer du composant.

Consultez en détail la section suivante sur les travaux planifiés, les propriétés système et File Explorer les flux secondaires du concepteur de flux.

Travaux planifiés pour File Explorer

Les travaux planifiés sont des travaux automatisés exécutés pour traiter les notifications provenant de, ingérer les métadonnées des fichiers dans ServiceNow l'instance et renouveler les abonnements au référentiel de Microsoft SharePoint fichiers selon un calendrier récurrent.

Les travaux planifiés sont des travaux automatisés qui sont exécutés en arrière-plan pour :

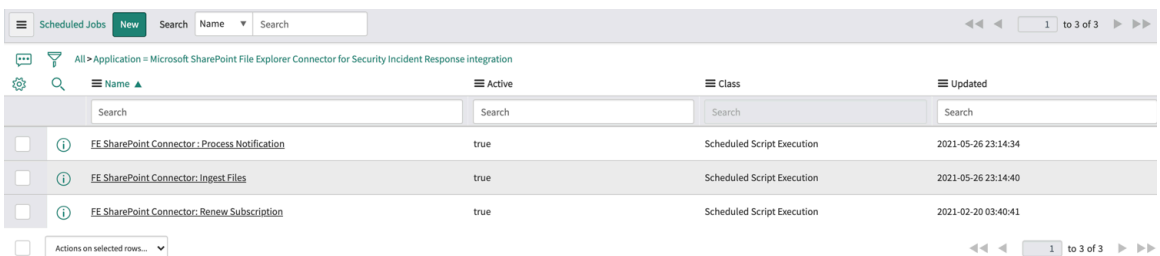
- traiter les notifications de Microsoft Microsoft SharePoint.
- Ingérer les métadonnées des fichiers dans ServiceNow AI Platform l'instance.
- Renouvelez l'abonnement avec Microsoft SharePoint la bibliothèque de documents pour recevoir des notifications.

Tâche	Description
Microsoft SharePoint File Explorer Connecteur : traiter la notification	S'exécute toutes les 30 secondes et est responsable de la lecture des notifications indiquant qu'un changement s'est produit sur la bibliothèque de documents abonnée et marque l'état des lecteurs (sn_fe_file_repo_drive) comme en attente.
Microsoft SharePoint File Explorer Connecteur : ingérer des fichiers	S'exécute toutes les 30 secondes et est principalement responsable du traitement des lecteurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	(sn_fe_file_repo_drive) qui sont dans l'état En attente et extrait les changements de fichier delta de la bibliothèque de documents configurés Microsoft SharePoint depuis la dernière extraction.
Microsoft SharePoint File Explorer: renouveler l'abonnement	S'exécute toutes les 10 minutes et est responsable du renouvellement de l'abonnement à la Microsoft SharePoint bibliothèque de documents un jour avant sa date d'expiration. Habituellement, ces abonnements expirent dans 30 jours.



Propriétés système de l'explorateur de fichiers disponibles

Les propriétés système disponibles du connecteur de l'explorateur de fichiers sont les Microsoft SharePoint suivantes.

Propriétés système

Nom de la propriété	Description
sn_fe_sharepoint.max_retry_count	Contrôle la fréquence des tentatives de l'application Microsoft SharePoint du connecteur pour extraire le lecteur défaillant ou renouveler l'abonnement ayant échoué. La valeur de fréquence par défaut est définie sur 50.
sn_fe_sharepoint.retry_after_seconds	Intervalle de temps entre chaque tentative d'extraction du lecteur défaillant ou de renouvellement de l'abonnement. La valeur par défaut est définie sur 900 s ou 15 minutes.
sn_fe_sharepoint.max_subscription_expiration_time	Période maximale d'expiration de l'abonnement en nombre de jours pour Microsoft SharePoint. La période d'expiration par défaut est fixée à 30 jours.

File Explorer Flux secondaires du concepteur de flux

Voici les flux secondaires du concepteur de flux qui sont installés avec Microsoft SharePoint File Explorer le connecteur.

Flux secondaires

Nom	Description
Ajoutez Microsoft SharePoint des autorisations	Accorde une autorisation de modification pour un dossier spécifique à des utilisateurs spécifiques.
Créer un abonnement au lecteur	Abonne avec une bibliothèque de documents configurée Microsoft SharePoint pour recevoir

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux secondaires (suite)

Nom	Description
	des notifications sur les mises à jour apportées à la bibliothèque de documents.
Créer un dossier Microsoft SharePoint	Crée un nouveau Microsoft SharePoint dossier sous un dossier parent donné.
Supprimer Microsoft SharePoint l'élément	Supprime les fichiers et les Microsoft SharePoint dossiers.
Télécharger le Microsoft SharePoint fichier	Renvoie l'URL de téléchargement des Microsoft SharePoint fichiers
Obtenir les métadonnées des fichiers	S'abonne aux modifications de la bibliothèque de documents et les extrait de celle-ci Microsoft SharePoint .
Déplacer Microsoft SharePoint l'élément	Déplace les Microsoft SharePoint fichiers/dossiers vers le dossier de destination
Ouvrir l'élément Microsoft SharePoint	Renvoie l'URL Web du Microsoft SharePoint fichier/dossier à ouvrir dans un navigateur.
Renouveler l'abonnement au lecteur	Renouvelle l'abonnement avec Microsoft SharePoint la bibliothèque de documents.
Créer une structure de dossier	Suit les configurations du modèle de dossier et crée la structure des dossiers sur Microsoft SharePoint la bibliothèque de documents.

Configurer Microsoft Teams

Configurer Gestion des incidents de sécurité majeurs avec Microsoft Teams qui aide la communication sur la messagerie instantanée à résoudre Incident de sécurité majeur.

La configuration et l'abonnement à un environnement de Microsoft Teams messagerie instantanée, la récupération des conversations instantanées à partir des canaux spécifiés et l'archivage de l'équipe et des canaux associés sont inclus dans le processus de clôture de l'incident. Un environnement désigné Microsoft Teams et une configuration d'API connexe Microsoft Teams Graph sont nécessaires pour créer des canaux individuels spécifiques à un Incident de sécurité majeur.

Pour configurer Microsoft Teams, activez Teams en tant que fournisseur de messagerie instantanée. Vous pouvez ensuite créer des canaux de messagerie instantanée pour les différentes personnes concernées et groupes qui communiquent sur les activités et suivre les conversations de messagerie instantanée pour résoudre le Incident de sécurité majeur problème. La configuration de Microsoft Teams et de l'API Microsoft Graph comprend :

- Établir une connexion au graphique MS Teams sur ServiceNow AI Platform
- Activer MS Teams en tant que fournisseur de messagerie instantanée
- Créer un modèle de canal de messagerie instantanée
- Afficher l'activité du message de la messagerie instantanée

Introduction à Microsoft Teams

Examinez les informations suivantes avant de commencer à utiliser l'application Microsoft Teams en tant que connecteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Assurez-vous que les modules d'extension suivants sont installés avant de commencer à établir, activer et valider Microsoft Teams les connexions de configuration.

Modules d'extension requis

Nom	Description
Intégration de la messagerie instantanée à Gestion des incidents de sécurité	Utilisez **sn_chat_collab_core** ID de module d'extension pour rechercher et installer Microsoft Teams la messagerie instantanée. L'installation de ce module d'extension vous permet de suivre l'activité de messagerie instantanée pour des applications tierces telles que Microsoft Teams (ou Slack et d'autres applications de messagerie instantanée tierces).
Connecteur de messagerie instantanée Microsoft Teams pour Gestion des incidents de sécurité	Utilisez **sn_ms_teams_connector** ID de module d'extension pour rechercher et installer Microsoft Teams Chat Connector for Major Security Incident Management. L'installation de ce module d'extension vous permet de suivre les activités de messagerie instantanée à l'aide du composant de collaboration spécifique à Microsoft Teams.
Microsoft Teams Spoke graphique	L'installation de ce module d'extension établit une connexion de spoke Graph avec Microsoft Teams. Pour plus d'informations, voir Spoke Microsoft Teams Graph

Activer MS Teams en tant que fournisseur de messagerie instantanée

Activez Microsoft Teams en validant la Microsoft Teams connexion.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Une fois la connexion activée et validée, un message d'information s'affiche indiquant que la connexion du fournisseur est validée avec succès. Vous pouvez modifier la configuration du canal en ajoutant et en supprimant des utilisateurs, et éventuellement en ajoutant d'autres canaux ou en renommant les canaux existants.

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Configuration du fournisseur de messagerie instantanée**.
2. Sélectionnez **l'enregistrement Microsoft Teams**.
3. Cliquez sur **Valider la connexion**.
   Un message de confirmation s'affiche indiquant que la connexion du fournisseur est validée avec succès.
4. Cochez **la case Actif** pour activer l'enregistrement de fournisseur.
   Un message de confirmation indique que la connexion du fournisseur a été validée avec succès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Enregistrez** le formulaire après avoir activé la configuration du fournisseur de messagerie instantanée. Grâce à cela, la connexion entre Microsoft Teams et ServiceNow AI Platform l'instance est établie avec succès.

Créer un modèle de canal de messagerie instantanée

Configurez les équipes de messagerie instantanée et les modèles de canaux pour créer des équipes et des canaux de messagerie instantanée pour collaborer, suivre les conversations de messagerie instantanée et ajouter des utilisateurs et des groupes d'utilisateurs à ces canaux de messagerie instantanée. Ces modèles de canal sont créés dans Microsoft Teams lorsqu'un incident de sécurité majeur est promu.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

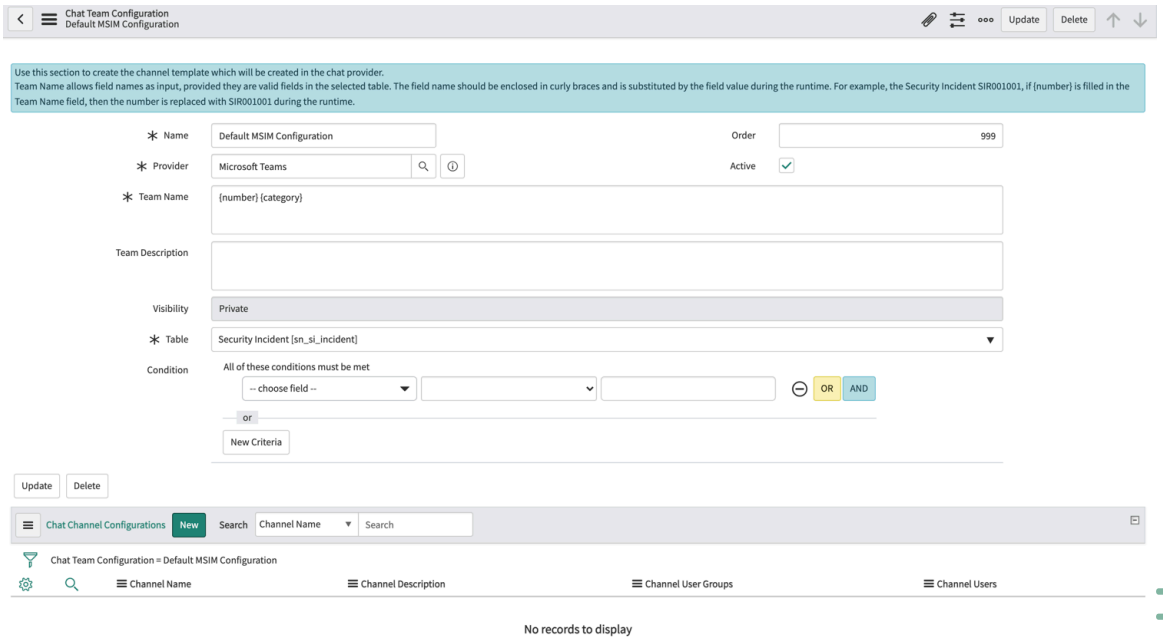
1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Canal de messagerie instantanée** > **Modèles de canaux**.
2. Dans le formulaire Configuration du canal de messagerie instantanée, cliquez sur **Nouveau** dans l'en-tête du formulaire.
3. Remplissez les champs du formulaire.

Formulaire de configuration d'équipe de messagerie instantanée

Champ	Description
Nom	Nom du dossier.
Fournisseur	Équipes Microsoft.
Nom de l'équipe	Nom de l'équipe, par exemple, au format {numéro}-{catégorie}. **Remarque :** Le nom d'équipe fourni ici sera utilisé dans tous les enregistrements d'incidents de sécurité majeurs. Pour vous assurer que le nom réel de l'équipe Microsoft est affiché dans l'application MS Teams et qu'il a une valeur de nom unique pour différents incidents de sécurité majeurs, il est recommandé d'utiliser une valeur de champ d'incident unique, telle que le numéro d'incident : {number}. Comme le montre l'exemple de capture d'écran, le {numéro} suivi d'un séparateur « - » et de la variable de champ {category} fournirait un numéro unique et une description de l'incident de sécurité majeur pour lequel Microsoft Teams est créé, par exemple {number} - {category}.
Description de l'équipe	Description facultative de l'équipe.
Table	Incident de sécurité majeur (sn_msi_incident).

Traduction automatique

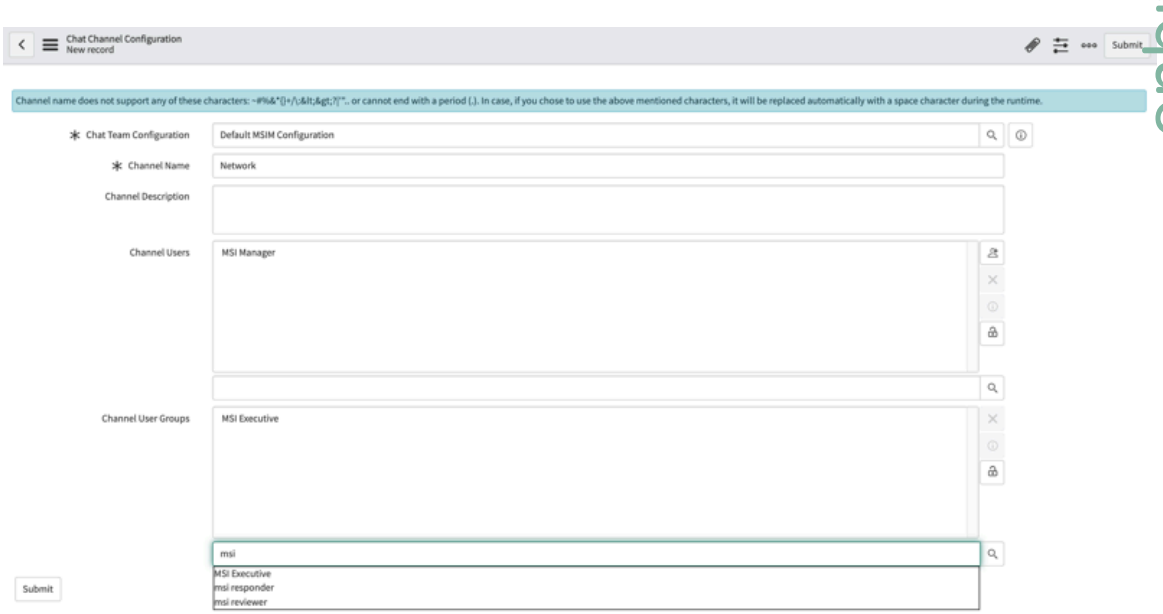
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Envoyer**.
5. Accédez à la section Configuration du canal de messagerie instantanée.
6. Cliquer sur **Nouveau** pour créer une nouvelle configuration de canal de messagerie instantanée.
7. Entrez le **Configuration d'équipe de messagerie instantanée** et **Nom du canal**.

> **Remarque :** Le nouveau canal que vous avez créé ici sera également votre nom de canal dans Microsoft Teams. Vous pouvez rechercher le même canal et ajouter vos conversations.

8. Ajouter le **Utilisateur de canal** et **Groupes d'utilisateurs de canaux** à partir de la liste de recherche.
9. **Envoyer** Le nouvel enregistrement de configuration du canal de messagerie instantanée.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Le canal de messagerie instantanée est maintenant créé et les utilisateurs sont affectés à ces groupes de canaux de messagerie instantanée. Vous pouvez afficher les activités Collaboration Chat à la fois dans Microsoft Teams et dans le flux d'activité Collaboration de l'espace de travail MSIM avec la structure hiérarchique des canaux de messagerie instantanée organisée telle que configurée dans la configuration du fournisseur de canal de messagerie instantanée.

Afficher l'activité du message de la messagerie instantanée

L'activité des messages de la messagerie instantanée est enregistrée et affichée dans l'onglet Collaboration de l'espace de travail Major Security Incident Management.

L'activité Message de la messagerie instantanée inclut toutes les conversations instantanées qui ont eu lieu entre les participants et différents groupes d'utilisateurs.

Dépannage du connecteur de messagerie instantanée MS Teams pour MSIM

Reportez-vous à la section de dépannage du connecteur de messagerie instantanée Microsoft Teams sur les travaux planifiés, les propriétés système et les flux secondaires du concepteur de flux Microsoft Teams.

Vérifiez que le connecteur de messagerie instantanée traite les travaux planifiés dans tous les cas si vous ne voyez pas les messages de Collaboration Chat sont publiés sur Microsoft Team et sur le flux d'activité de collaboration externe de l'espace de travail MSIM.

Travaux planifiés pour Microsoft Teams

Les travaux planifiés sont des travaux automatisés qui sont exécutés pour traiter les notifications à partir du connecteur de Microsoft Teams messagerie instantanée et renouveler les abonnements Microsoft Teams selon un calendrier récurrent.

Rôle requis : admin.

- **Connecteur de messagerie instantanée MS Teams : traiter la notification**

  Pour chaque événement de message de messagerie instantanée, une notification contenant l'ID de ressource et la notification sont stockés dans une table. Une tâche planifiée est exécutée toutes les 30 secondes pour choisir les notifications non traitées et interroger l'API Microsoft Teams pour obtenir le contenu réel du message, qui est ensuite stocké dans une autre table.

- **Connecteur de messagerie instantanée MS Teams : renouveler les abonnements**

  Pour chaque canal au sein de l'équipe, des abonnements sont créés pour être informés des événements créés, mis à jour et supprimés. Cet abonnement n'est actif que pendant 60 minutes. Les abonnements sont renouvelés toutes les 25 minutes via le travail de planification Connecteur Microsoft Teams : renouveler la notification.

Microsoft Teams Flux fonctionnel du connecteur de messagerie instantanée

Affichez cette section pour comprendre les Microsoft Teams flux secondaires du concepteur de flux connexes utilisés pour gérer la création du ou des canaux de messagerie instantanée et l'accès des utilisateurs à partir d'un incident de sécurité majeur.

Avant de commencer

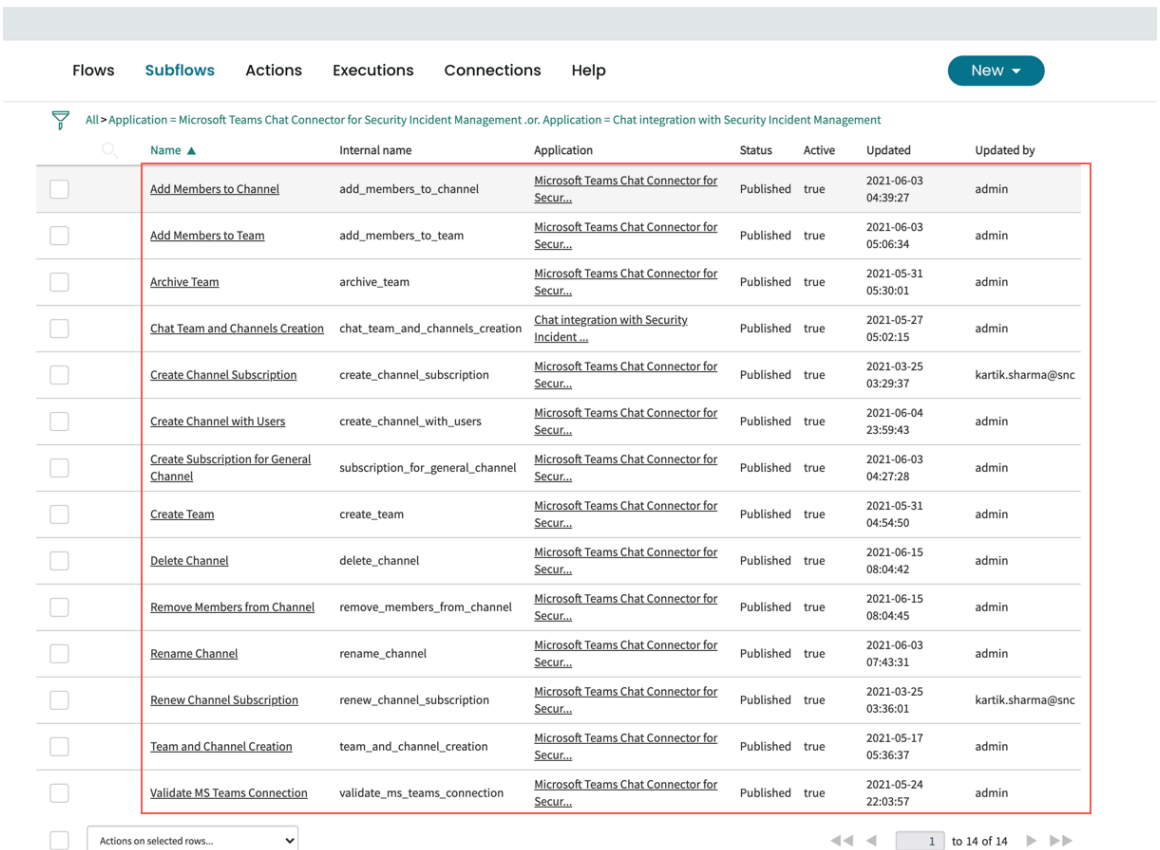
Rôle requis : sn_msi.workspace_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Concepteur de flux**.
2. Ajouter des membres au canal
3. Ajouter des membres à l’équipe
4. Équipe d'archivage
5. Création de canaux et d’équipes de messagerie instantanée
6. Créer un abonnement à un canal
7. Créer un canal avec des utilisateurs
8. Créer l’abonnement pour le canal général
9. Créer une équipe
10. Supprimer un canal
11. Supprimer des membres du canal
12. Renommer le canal
13. Renouveler l’abonnement au canal
14. Création d’équipes et de canaux
15. Valider la connexion MS Teams



Configurer le connecteur de messagerie instantanée Slack pour les incidents de sécurité majeurs

Intégrez et collaborez avec Slack pour résoudre un incident de sécurité majeur afin d’afficher et de filtrer les activités de Collaboration Chat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La configuration et l'abonnement à un Slack environnement de messagerie instantanée, la récupération des conversations instantanées à partir des canaux spécifiés et l'archivage de Slack et des canaux associés sont inclus dans le cadre du processus de clôture de l'incident. Un environnement désigné Slack et une configuration d'API connexe Slack sont nécessaires pour créer des canaux individuels spécifiques à un Incident de sécurité majeur.

Pour configurer Slack, activez Slack en tant que fournisseur de messagerie instantanée. Vous pouvez ensuite créer des canaux de messagerie instantanée pour les différentes personnes concernées et groupes qui communiquent sur les activités et suivre les conversations de messagerie instantanée pour résoudre le Incident de sécurité majeur problème. La configuration de l'API Slack and Slack comprend :

- Introduction à la configuration du connecteur de messagerie instantanée Slack
- Activer Slack en tant que fournisseur de canal
- Créer un modèle de canal de messagerie instantanée pour Slack
- Afficher les activités des messages de messagerie instantanée dans Slack

Introduction à la configuration du connecteur de messagerie instantanée Slack

Examinez les informations suivantes avant de commencer à utiliser l'application Slack en tant que connecteur.

Assurez-vous que les modules d'extension suivants sont installés avant de commencer à établir, activer et valider Slack les connexions de configuration.

Modules d'extension requis

Nom	Description
Slack Connecteur de messagerie instantanée pour Gestion des incidents de sécurité	Utilisez **sn_slack_connector** ID de module d'extension pour rechercher et installer Slack le connecteur pour la gestion des incidents de sécurité majeurs. L'installation de ce module d'extension vous permet de suivre les activités de messagerie instantanée à l'aide du composant de collaboration spécifique à Slack.
Spoke Slack	L'installation de ce module d'extension établit une connexion de spoke avec Slack. Pour plus d'informations, voir Slack Rayon

Créer un modèle de canal de messagerie instantanée pour Slack

Configurez les équipes de messagerie instantanée et les modèles de canaux pour créer des équipes et des canaux de messagerie instantanée pour collaborer, suivre les conversations de messagerie instantanée et ajouter des utilisateurs et des groupes d'utilisateurs à ces canaux de messagerie instantanée. Ces modèles de canal sont créés lorsqu'un Slack incident de sécurité majeur est promu.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Pourquoi et quand exécuter cette tâche

Le nouveau canal que vous créez sera également votre nom de Slack canal. Vous pouvez rechercher le même canal et ajouter vos conversations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Canal de messagerie instantanée** > **Modèles de canaux**.
2. Sélectionnez **la configuration du canal Slack** pour afficher les détails de la configuration de Slack.
3. Cochez la case **Actif** pour activer la configuration du canal de messagerie instantanée Slack.
4. Dans le champ Nom de l'équipe, fournissez le numéro MSI et le nom de code.

   Par défaut, tous les canaux Slack sont précédés du numéro d'incident. Par exemple, `MSI000000 - {nom du canal}`. Vous pouvez modifier le préfixe de n'importe quel champ de votre choix au format suivant : `{field_name}`.

   Remarque : Le nom d'équipe fourni ici sera utilisé dans tous les enregistrements d'incidents de sécurité majeurs. Pour vérifier que la valeur réelle Slack est affichée dans Slack l'application et qu'elle a une valeur de nom unique pour différents incidents de sécurité majeurs, il est recommandé d'utiliser une valeur de champ d'incident unique, telle que le `MSI000000 - {nom du canal}`.

5. Cliquez avec le bouton droit sur la configuration et sélectionnez **Enregistrer**.
6. Accédez à la section Configuration du canal de messagerie instantanée.
7. Sélectionner **Nouveau** pour créer une nouvelle configuration de canal de messagerie instantanée.
8. Renseignez les champs du formulaire.

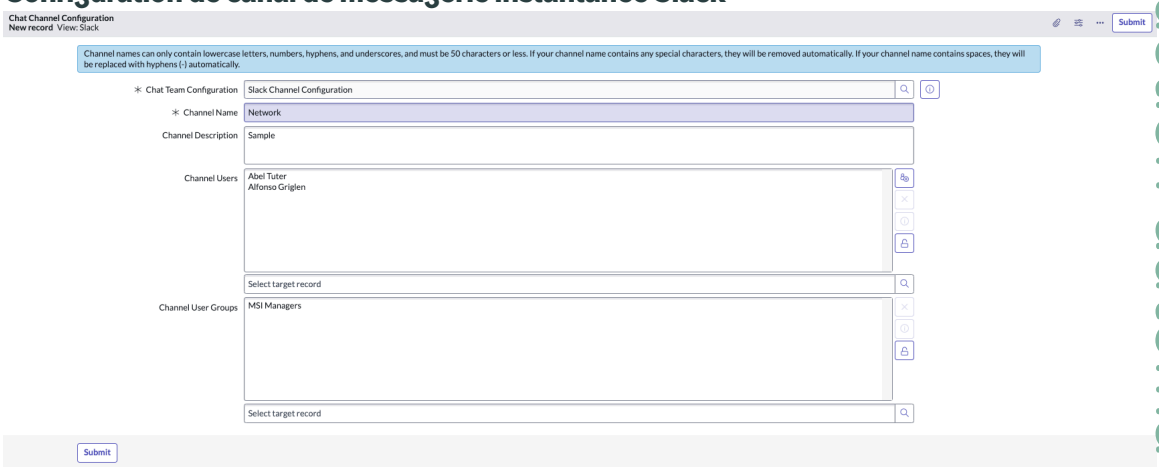
Champ	Description
Configuration d'équipe de messagerie ins tantanée	Nom de la configuration de l'équipe de messagerie instantanée. Par exemple, la configuration du canal Slack.
Nom du canal	Nom du canal. Par exemple, juridique. **Remarque :** ○ Les noms de canaux ne peuvent contenir que des lettres minuscules, des chiffres, des tirets et des traits de soulignement et doivent com–porter au maximum 50 caractères. Si le nom de votre chaîne contient des caractères spéciaux, ils sont automatiquement supprimés. Si le nom de votre canal contient des es–paces, ils sont automatiquement remplacés par des traits d'union (-). ○ Le nouveau canal que vous créez ici sera également votre nom de Slack canal. Vous pouvez rechercher le même canal et ajouter vos conver–sations.
Description du canal	Description unique pour le canal.
Utilisateur de canal	Sélectionnez l'icône **Déverrouiller les utilisa teurs du canal** et ajoutez les utilisateurs qui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	peuvent accéder à ce canal à partir de la liste de recherche. Sélectionnez l'icône **Verrouiller les utilisateurs du canal** pour verrouiller la liste sélectionnée d'utilisateurs du canal.
Groupes d'utilisateurs de canaux	Sélectionnez l'icône **Déverrouiller les groupes d'utilisateurs du canal** , puis ajoutez les groupes d'utilisateurs qui peuvent accéder à ce canal à partir de la liste de recherche. Vous pouvez également utiliser l'icône **Add me (Ajouter à moi**) pour vous ajouter. Sélectionnez l'icône **Verrouiller les groupes d'utilisateurs du canal** pour verrouiller la liste sélectionnée des groupes d'utilisateurs du canal.

Configuration de canal de messagerie instantanée Slack



9. Sélectionnez **Soumettre**.

Résultats

Le canal de messagerie instantanée est maintenant créé et les utilisateurs sont affectés à ces groupes de canaux de messagerie instantanée. Vous pouvez afficher les activités Collaboration Chat à la fois dans Slack et dans le flux d'activité Collaboration de l'espace de travail MSIM avec la structure hiérarchique des canaux de messagerie instantanée organisée telle que configurée dans la configuration du fournisseur de canal de messagerie instantanée.

Activer Slack en tant que fournisseur de canal

Activez Slack en validant la Slack connexion.

Avant de commencer

Rôle requis :

- sn_msi.workspace_admin : écriture
- sn_msi.chat_collab_provider : en lecture

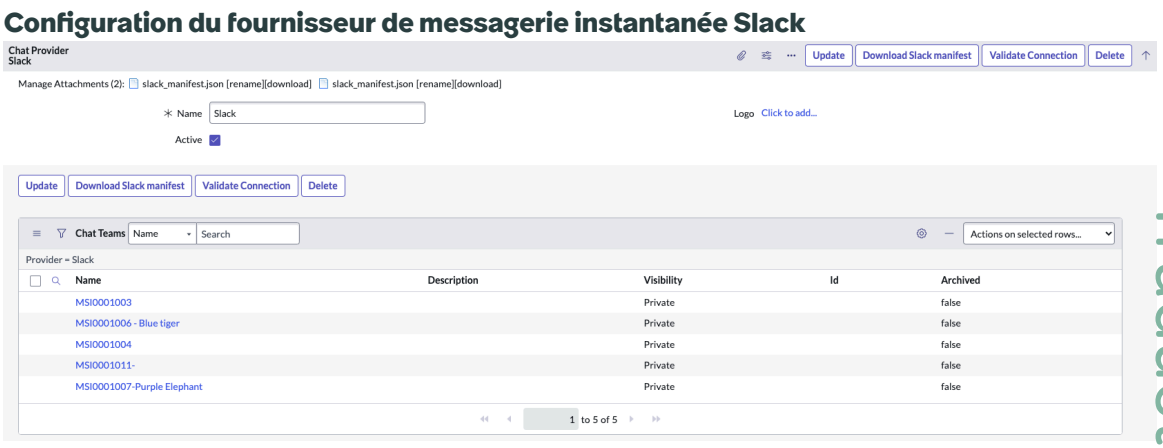
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois la connexion activée et validée, un message d'information s'affiche indiquant que la connexion du fournisseur est validée avec succès. Vous pouvez modifier la configuration du canal en ajoutant et en supprimant des utilisateurs, et éventuellement en ajoutant d'autres canaux ou en renommant les canaux existants.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Canal de messagerie instantanée** > **Configuration du fournisseur de messagerie instantanée**.
2. Sélectionnez **Slack** pour ouvrir la configuration du fournisseur de messagerie instantanée Slack.



3. Sélectionnez **Télécharger le manifeste Slack** pour télécharger le fichier `slack_manifest.json` .
   Le fichier `slack_manifest.json` contient la configuration complète de la configuration de Slack et vous permet de configurer Slack automatiquement. Vous devez charger ce fichier JSON dans la configuration de Slack.
4. Ouvrez le fichier `slack_manifest.json` et procédez comme suit :
   a. Accédez à l'URL `api.slack.com/apps` sur votre navigateur Web.
   b. Sélectionnez **l'action Créer une application** .
   c. Dans la fenêtre contextuelle Créer une application, choisissez l'option **À partir d'un manifeste d'application** .
   d. Dans la fenêtre contextuelle Choisir un espace de travail pour développer votre application, choisissez un espace de travail dans la liste et sélectionnez **Suivant**.
   Par exemple, Espace de travail Marge MSIM.
   e. Dans la fenêtre contextuelle du manifeste de l'application Enter ci-dessous, sélectionnez l'onglet **JSON** et copiez-collez le code du fichier `slack_manifest.json` .
   f. Sélectionnez **Suivant**.
   g. Dans la fenêtre contextuelle Examiner le résumé et créer votre application, sélectionnez **Créer**.
   Votre application a maintenant été créée.
   h. Dans la page Informations de base, sélectionnez **Installer dans l'espace de travail**.
   Le bot d'intégration de Slack vous demande l'autorisation d'accéder à l'espace de travail Slack MSIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Sélectionner **Autoriser**.

j. Dans la section Informations d'identification de l'application, renseignez les détails en revenant à l'instance ServiceNow.

k. Sélectionner **Tous** > **Configurations de Slack**.
Vous avez besoin du rôle sn_msi.workspace_admin pour cette action.

l. Sélectionnez une propriété **Secret de signature** .

m. Copiez le secret de signature et collez-le dans la section Informations d'identification de l'application de Slack.

n. Dans l'instance ServiceNow, accédez à **Tous** > **Concepteur de flux**.

o. Accédez à la **Connexions** > **Slack** > **Afficher les détails** > **Configurer**.

p. Renseignez les champs du formulaire.

Champ	Description
Nom de la connexion	Nom de cette connexion. Par exemple, Slack.
URL de connexion	URL de cette connexion. Par exemple, https://slack.com
Nom des informations d'identification	Nom des informations d'identification. Par exemple, les informations d'identification Slack.
Nom OAuth	Nom de l'OAuth. Par exemple, Slack OAuth.
ID client OAuth	L'ID client qui a été généré pour le compte que vous avez créé dans Slack.
Secret client OAuth	Clé secrète du client pour le compte que vous avez créé dans Slack.
URL de redirection OAuth	Nom de l'instance de redirection OAuth. Par exemple, msimslack.service-now.com/oauth_redirect.do

q. Sélectionnez **Configurer et obtenir le jeton OAuth**.
Le bot d'intégration de Slack vous demande l'autorisation d'accéder à l'espace de travail Slack MSIM.

r. Sélectionner **Autoriser**.
Le jeton d'accès OAuth est disponible et expirera le <AAAA-MM-JJ> <HH :MM :SS>.

5. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Canal de messagerie instantanée** > **Configuration du fournisseur de messagerie instantanée**.
6. Cochez la case **Actif** pour activer l'enregistrement du fournisseur de messagerie instantanée.
7. Sélectionnez **Valider la connexion** pour tester la connexion.
Un message de confirmation indique que la connexion du fournisseur a été validée avec succès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Cliquez avec le bouton droit sur l'enregistrement et sélectionnez **Enregistrer**.
   Ensuite, la connexion entre Slack et ServiceNow AI Platform l'instance est établie avec succès.
9. Accédez à la **api.slack.com/apps** > **Fonctionnalités** > **OAuth et autorisations**.

   a. Vérifiez si tous les champs d'application sont corrects.

   b. Accédez à la **Fonctionnalités** > **Abonnements d'événement**.

   c. Dans le champ URL de la demande, sélectionnez **Réessayer**.
      Vous pouvez voir un message vérifié.

   d. Sélectionnez **Enregistrer**.

Afficher les activités des messages de messagerie instantanée dans Slack

L'activité des messages de la messagerie instantanée est enregistrée et affichée dans l'onglet Collaboration de l'espace de travail Major Security Incident Management.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Pourquoi et quand exécuter cette tâche
L'activité Message de la messagerie instantanée inclut toutes les conversations instantanées qui ont eu lieu entre les participants et différents groupes d'utilisateurs. Pour plus d'informations, consultez Gérer les communications des canaux de messagerie instantanée à l'aide de Slack.

Administration Gestion des incidents de sécurité majeurs

Planifiez et configurez votre implémentation Gestion des incidents de sécurité majeurs.

Vous pouvez configurer les aspects d'administration Gestion des incidents de sécurité majeurs suivants :

Activer la proposition, la promotion et le lien des incidents de sécurité majeurs

Permettez aux utilisateurs de décider de proposer ou de promouvoir des incidents en tant qu'incidents de sécurité majeurs. Suivez facilement tous les incidents liés à un incident de sécurité majeur en permettant de lier les incidents de sécurité à l'incident parent ou enfant.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configurations**.
2. Permettez aux utilisateurs de proposer un incident de sécurité à un incident de sécurité majeur en cochant la case **Proposer un incident de sécurité majeur** dans la section Actions de l'espace de travail SIR/VR.
3. Permettez aux utilisateurs de promouvoir un incident de sécurité en un incident de sécurité majeur en cochant la case **Promouvoir en incident de sécurité majeur** .
4. Activez la liaison d'un incident de sécurité à un incident de sécurité majeur afin qu'ils puissent être suivis ensemble en cochant la case **Lier à un incident de sécurité majeur** .
5. Sélectionnez **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Marquer les incidents de sécurité comme incidents de sécurité majeurs

Balisez ou étiquetez les incidents de sécurité ou les enregistrements vulnérables d'un incident de sécurité majeur lorsque l'incident est proposé ou promu. Si un incident de sécurité est proposé, l'enregistrement d'incident est considéré comme un candidat à l'incident de sécurité majeur. Lorsqu'un titre est promu, l'enregistrement d'incident est alors appelé Incident de sécurité majeur avec l'état Accepté.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configurations**.
2. Cochez la case Activer les **étiquettes d'affichage** pour étiqueter le candidat à l'incident proposé comme incident de sécurité majeur en sélectionnant le champ de recherche Nom de l'étiquette **- Proposer en tant que candidat** et sélectionnez Candidat à l'incident de sécurité majeur dans la section **Étiquettes de l'espace de travail SIR/VR** .
3. Cochez la case Activer les **étiquettes d'affichage** pour étiqueter le candidat à l'incident promu comme incident de sécurité majeur en sélectionnant le champ **de recherche Nom d'étiquette - Promotion en incident de sécurité majeur** et sélectionnez Incident de sécurité majeur dans la section **Étiquettes de l'espace de travail SIR/VR** .
4. Sélectionnez **Mettre à jour**.

Configurer des étiquettes pour les incidents de sécurité majeurs

Configurez les étiquettes dans la gestion des incidents de sécurité majeurs pour créer des étiquettes personnalisées et filtrer les activités et les tâches de collaboration externes dans le flux d'activité. Les différents types d'étiquettes implémentées sont les étiquettes d'état et les étiquettes de chronologie.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configurations**.
2. Case à cocher Activer **les étiquettes d'affichage** pour activer l'étiquetage des différents états d'incident tels que Analyse, Contenir, Éradiquer, Récupérer, Examiner, Événement de chronologie dans la section **Étiquettes de l'espace de travail MSIM (affichage sur les activités et tâches de collaboration).**
3. Sélectionnez **Mettre à jour**.

Configurer des étiquettes pour les incidents de sécurité majeurs

Configurez différents types d'étiquettes pour mieux filtrer et indiquer les états des incidents. Les étiquettes d'incident de sécurité majeur offrent la flexibilité d'étiqueter les activités et les tâches de collaboration des enregistrements d'incidents.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez sélectionner ou désélectionner les étiquettes à l'aide de l'icône d'étiquettes disponible dans la section Flux d'activité de la section Collaboration et organisateur de tâches de l'espace de travail MSIM.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Étiquettes MSI**.
2. Cliquez sur **Nouveau** pour créer une étiquette.
3. Remplissez le formulaire avec le **nom de l'étiquette** et la **couleur de l'étiquette**.
4. Cliquez sur **Créer une étiquette**.
5. Dans le cadre du système de base, les étiquettes configurées sont les suivantes pour chaque état d'incident et vous ne pouvez pas modifier le nom ou la couleur de l'étiquette :
   - Analyse
   - Contenir
   - Éradiquer
   - Revue
   - Récupérer
   - Événement de chronologie

Remarque : Vous pouvez modifier les étiquettes personnalisées et leurs propriétés.

Configurer des catégories de chronologie pour les incidents de sécurité majeurs

Configurez et affectez des catégories de chronologie telles que Menace, Réponse ou Personnalisé à vos incidents de sécurité majeurs à l'aide de la section Chronologie de l'onglet Vue d'ensemble.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Catégories de chronologie**.
   Les catégories de chronologie suivantes sont fournies dans le cadre du système de base :
   - **Personnalisé**.
   - **Réponse**.
   - **Menace**.
2. Pour modifier une catégorie d'événement de chronologie existante, procédez comme suit :
   a. Sélectionnez une catégorie d'événement de chronologie dans la liste.
   b. Vous pouvez modifier le nom de la catégorie d'événement de chronologie.
   c. Vous pouvez modifier la couleur de l'événement et sélectionner une autre couleur pour votre catégorie d'événement de chronologie.
   d. Sélectionnez **Mettre à jour**.
3. Pour créer une nouvelle catégorie d'événement de chronologie, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sélectionnez **Nouveau**.

b. Dans le champ Nom, saisissez un nom pour la catégorie d'événement de chronologie.

c. Dans le champ Couleur de l'événement, choisissez une couleur pour la catégorie de chronologie de l'événement à l'aide de la liste déroulante.

d. Sélectionnez **Soumettre**.

Définir les préférences de notification pour MSIM

Automatisez le processus de notification par e-mail et notifiez les utilisateurs lorsqu'un incident de sécurité est proposé ou promu en candidat à un incident de sécurité majeur.

Rôle requis : sn_msi.workspace_admin.

Les notifications ne sont déclenchées que lorsqu'un incident de sécurité est proposé et envoyé à tous les utilisateurs et groupes configurés dans la liste de notifications. Par défaut, la notification par e-mail est reçue par l'utilisateur qui a proposé l'incident de sécurité en tant que candidat à l'incident de sécurité majeur.

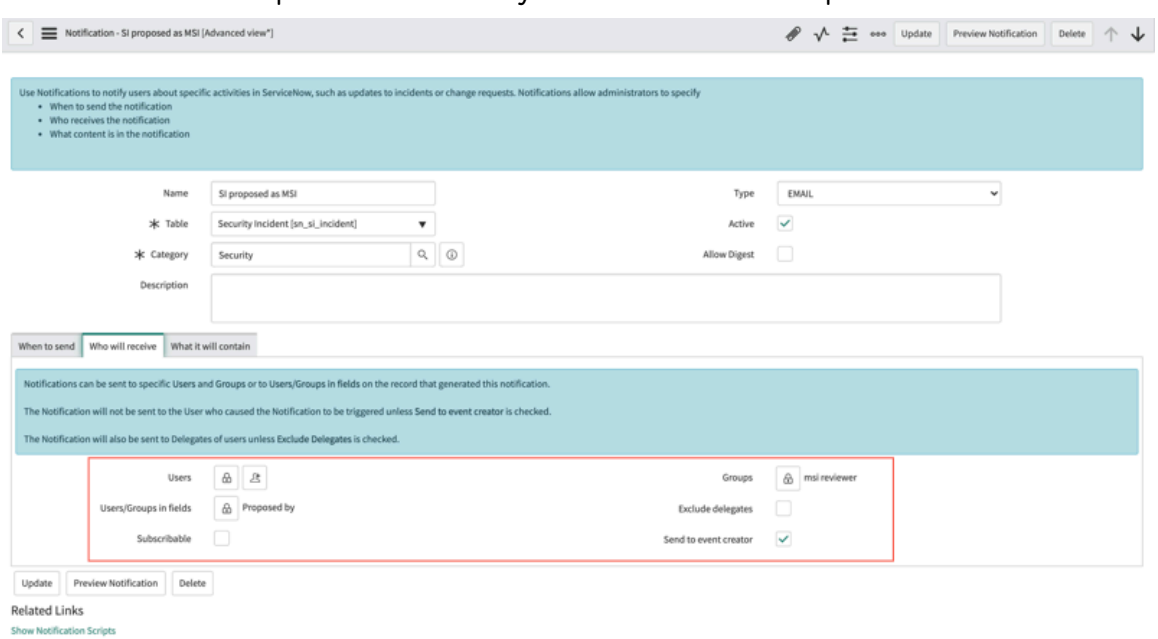
Notification : incident de sécurité proposé (SI) en tant qu'incident de sécurité majeur (MSI)

Qui recevra :

- Par défaut **Réviseurs MSI** Le nom de groupe est créé et tout utilisateur ajouté à ce groupe aura le privilège d'être un **Gestionnaire MSIM** et les utilisateurs qui font partie de ce groupe recevront les e-mails de notification.
- Tout utilisateur spécifique ajouté au **Utilisateurs** recevra également les e-mails de notification.

Que contiendra-t-il :

Si vous souhaitez modifier le contenu de l'e-mail, tel que le corps de l'e-mail qui inclut l'objet ou le message HTML, vous devez disposer du rôle d'administrateur système ou vous être affecté en tant qu'administrateur système et non en tant qu'administrateur MSI.



Notification : incident de sécurité promu (SI) en tant qu'incident de sécurité majeur (MSI)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

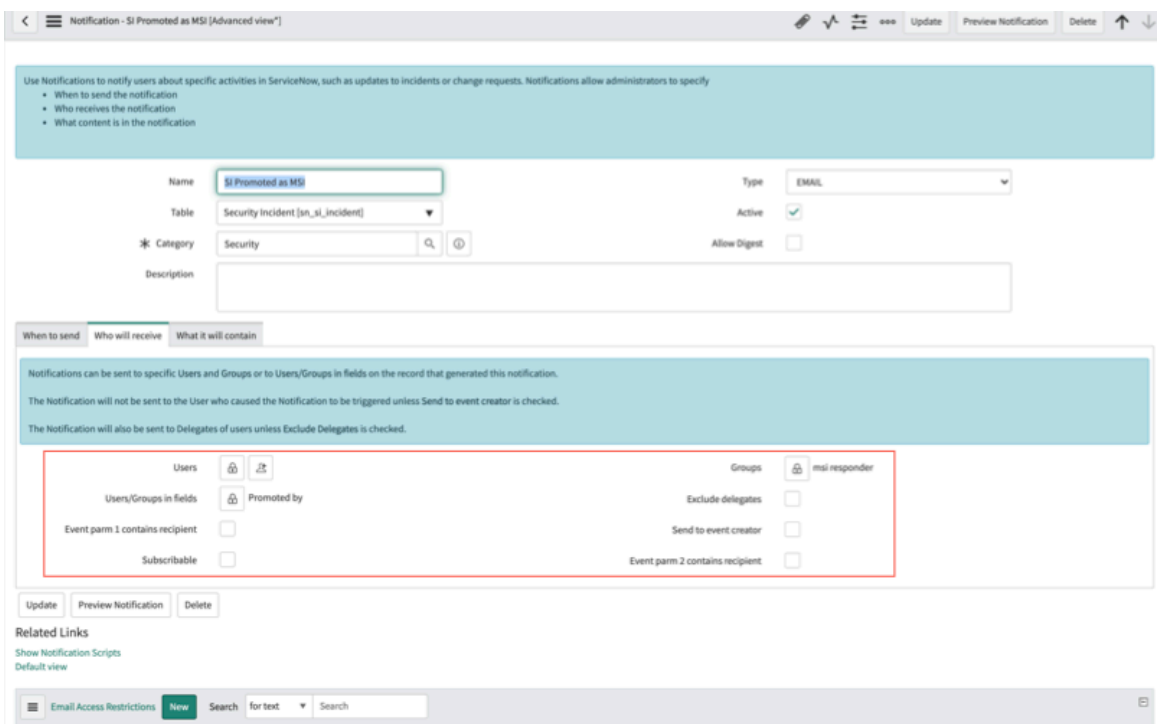
Cette notification est déclenchée lorsqu'un incident de sécurité est promu et lorsque l'explorateur de fichiers et Microsoft Teams la structure de base sont créés. Par défaut, cette notification est reçue par l'utilisateur qui a promu l'incident de sécurité en incident de sécurité majeur.

Destinataire

- Par défaut, un **Groupe** par nom **Répondeur MSI** est créée et tout utilisateur ajouté à ce groupe aura le privilège d'avoir **Répondeur MSIM** et tous les utilisateurs qui font partie de ce groupe recevront l'e-mail de notification.
- Tout utilisateur spécifique ajouté au **Utilisateurs** recevra également les e-mails de notification.

Que contiendra-t-il ?

Si vous souhaitez modifier le contenu de l'e-mail, notamment le corps de l'e-mail, qui inclut le code HTML de l'objet ou du message, vous devez disposer de l'accès au rôle d'administrateur système ou lui affecter le rôle d'administrateur système et non celui d'administrateur MSI.



Configurer les activités de fermeture de MSI

Établissez des actions qui se produiront automatiquement lors de la fermeture d'un incident de sécurité majeur. Augmentez la sécurité en archivant automatiquement et en supprimant l'accès aux dossiers contenant des informations de résolution.

Avant de commencer
Rôle requis : sn_msi.workspace_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configurations**.
2. Archivez les communications de messagerie instantanée liées à la résolution de l'incident en cochant la case **Archiver les canaux de collaboration** dans la section Actions de fermeture automatisées.
3. Supprimez les dossiers contenant des documents liés à la résolution de l'incident en cochant la case **Supprimer les dossiers de collaboration** .
4. Sélectionnez **Mettre à jour**.

Gestion des incidents de sécurité majeurs Workspace

Gestion des incidents de sécurité majeurs fournit un espace de travail dédié à la gestion des incidents de sécurité majeurs, spécialement conçu pour le Incident de sécurité majeur gestionnaire.

Collaborez facilement sur des activités qui aident à résoudre les incidents de sécurité majeurs en partageant et en visualisant des fichiers et des dossiers, en visualisant et en mettant à jour les tâches d'incident et en communiquant avec les personnes travaillant sur l'incident via des canaux de chat dédiés.

Gestion des incidents de sécurité majeurs (MSIM) fournit un mécanisme pour suivre et résoudre les incidents de sécurité majeurs. MSIM fonctionne conjointement avec les fonctionnalités existantes des produits Security Incident et Vulnerability Response et améliore le processus de correction des incidents de sécurité majeurs avec les fonctionnalités suivantes :

- Espace de travail dédié à la gestion des incidents de sécurité majeurs, spécialement conçu pour le rôle d'utilisateur responsable des incidents de sécurité majeurs.
- Organiser les tâches de réponse aux incidents de sécurité majeurs, y compris les tâches suivies sur les incidents de sécurité et les groupes de vulnérabilité liés.
- Automatisez la création de dossiers de collaboration et de canaux de communication par messagerie instantanée lorsqu'un incident de sécurité majeur est créé, ainsi que l'archivage dans le cadre de la clôture de l'incident.
- Composant d'explorateur de fichiers permettant d'organiser et de suivre la collecte d'artefacts (fichiers) liés à l'incident de sécurité majeur via une Microsoft SharePoint intégration.
- Gestionnaire de canal de messagerie instantanée et composants de flux d'activité pour gérer les communications entre plusieurs groupes de sécurité, informatiques et fonctionnels via une Microsoft Teams intégration.
- Rapports de synthèse de l'impact de l'incident de sécurité majeur et des mesures de progression, y compris le déploiement des actifs, des utilisateurs, des emplacements et des ressources d'équipe affectés, ainsi que la chronologie des jalons importants de l'incident.

Utilisez l'espace de travail MSIM pour suivre et résoudre les incidents de sécurité majeurs :

1. Affichez les graphiques de tendance et la progression de l'incident de sécurité majeur.
2. Suivez et organisez l'activité des fichiers Microsoft SharePoint via l'espace de travail MSIM.
3. Suivez et organisez l'activité de messagerie instantanée Microsoft Teams via l'espace de travail MSIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Affichez et mettez à jour les détails de l'incident via l'espace de travail MSIM.
5. Filtrer les activités de collaboration dans le flux d'activité de l'espace de travail MSIM.

Utiliser Gestion des incidents de sécurité majeurs

Les gestionnaires peuvent utiliser Gestion des incidents de sécurité majeurs l'espace de travail pour afficher les enregistrements d'incidents proposés, promus, liés et rejetés et suivre leurs activités connexes.

Proposez, promouvez et liez des enregistrements d'incidents

Proposez ou promouvez les incidents de sécurité en tant qu'incidents de sécurité majeurs lorsque les incidents sont identifiés comme une menace critique pour l'organisation.

Une fois Major Security Incident Management installé sur votre ServiceNow instance, vous pouvez gérer la transition des incidents de sécurité vers les incidents majeurs comme suit :

- Proposez un incident de sécurité au candidat à un incident de sécurité majeur afin de lancer un processus d'examen.
- Faites directement la promotion d'un incident de sécurité en un incident de sécurité majeur sans processus de révision.
- Rejeter un incident de sécurité proposé en tant qu'incident de sécurité majeur.

Vous pouvez également lier un incident de sécurité en tant qu'incident enfant à l'incident de sécurité majeur afin que tous les incidents de sécurité associés puissent être suivis ensemble.

Proposer en tant que Incident de sécurité majeur

Proposer un incident de sécurité à un incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Listes**.
2. Sélectionnez l'incident de sécurité dans la catégorie connexe que vous souhaitez proposer comme incident de sécurité majeur.
3. Sélectionnez l'icône Actions **supplémentaires** , puis **Proposer comme incident de sécurité majeur**.
4. Renseignez les champs de la boîte de dialogue Proposer comme incident de sécurité majeur.
   a. **Date de détection** : date à laquelle l'incident de sécurité majeur a été créé ou proposé pour la première fois.
   b. **Justification** : fournissez la justification de la proposition d'incident.
   c. **Impact potentiel** : indiquez l'impact de l'incident.
5. Sélectionnez **Proposer**.

Résultats

L'incident est proposé et les actions suivantes se produisent :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dans l'enregistrement d'incident de sécurité, un message de bannière de vérification s'affiche et la balise d'incident de sécurité majeur définie apparaît.
- L'enregistrement figure dans la liste connexe des incidents de sécurité majeurs de l'enregistrement d'incident, avec l'état Proposé, et dans la liste des candidats à l'espace de travail MSIM.
- La section Activité de l'espace de travail MSIM montre que l'incident de sécurité a été proposé pour être promu comme incident de sécurité majeur.
- Un message contenant un lien vers l'enregistrement d'incident et l'onglet Détails de l'incident est envoyé aux personnes figurant dans la liste de notification définie.

Promouvoir à Incident de sécurité majeur

Promouvoir un incident de sécurité en un incident de sécurité majeur ou rejeter les propositions promues via l'espace de Gestion des incidents de sécurité majeurs travail (MSIM).

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité** > **Incidents de sécurité** > **Listes**.
2. Sélectionnez l'incident de sécurité dans la catégorie connexe que vous souhaitez promouvoir comme incident de sécurité majeur.
   Passez en revue les détails de l'incident de sécurité dans la section Détails ou affichez les détails étendus de l'enregistrement d'incident dans un onglet distinct en cliquant sur **Afficher plus de détails**.
3. Sélectionnez l'icône Actions **supplémentaires** , puis **Promouvoir en incident de sécurité majeur**.
4. Renseignez les champs de la boîte de dialogue Promouvoir un incident de sécurité majeur.
   a. **Date de détection** : date à laquelle l'incident de sécurité majeur a été créé ou proposé pour la première fois.
   b. **Date de résolution estimée** : date de résolution estimée à laquelle la résolution de l'incident de sécurité majeur est estimée.
   c. **Nom** de code : sélectionnez le nom de code de l'incident de sécurité majeur.
   Par exemple, Blue Tiger.
   d. **Catégorie** : sélectionnez la catégorie de l'incident de sécurité majeur.
   Par exemple, Mauvaise configuration.
   e. **Justification** : fournissez la justification de la proposition d'incident.
   f. **Impact potentiel** : indiquez l'impact de l'incident.
5. Sélectionnez **Proposer**.
6. Faites la promotion de l'incident de sécurité ou rejetez la proposition de promotion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour promouvoir l'incident, cliquez sur **Promouvoir en incident de sécurité majeur**.
- Pour rejeter la proposition de promotion, cliquez sur **Rejeter en tant qu'incident de sécurité majeur**.

7. Sélectionnez **Enregistrer**.

Résultats

- Si vous avez rejeté la proposition de promotion, l'incident n'est pas promu et l'entrée de l'incident est déplacée vers l'onglet Rejeté.
- Si vous avez promu l'incident, l'entrée d'incident se déplace vers l'onglet Ouvrir et l'enregistrement de sécurité affiche une balise indiquant qu'il s'agit d'un incident de sécurité majeur.
- La décision est répertoriée dans la section Activité de l'espace de travail MSIM.

Une fois qu'un incident est promu, la configuration par défaut est appliquée.

- Une structure de dossiers est créée en fonction de la configuration du modèle de dossier.
- Les canaux de messagerie instantanée sont créés en fonction de leur configuration.
- Un message électronique est envoyé aux utilisateurs désignés. La notification par défaut contient un lien vers l'incident de sécurité majeur et les détails de l'incident. Les utilisateurs désignés ont également désormais accès aux ressources de collaboration, de sorte que la notification inclut également le nom de l'équipe Microsoft et un lien vers les dossiers Microsoft SharePoint liés à l'incident.

Lier à Incident de sécurité majeur

Liez les incidents de sécurité à un incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_msi.workspace_admin

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité dans la catégorie connexe que vous souhaitez lier à l'incident de sécurité majeur.
3. Sélectionnez l'icône **Actions supplémentaires** , puis **Lier à l'incident de sécurité majeur**.
4. Sélectionnez l'incident de sécurité majeur auquel vous souhaitez le lier.
   a. Dans la boîte de dialogue, sélectionnez l'icône Rechercher à l'aide d'une liste.
   b. Sélectionnez l'incident de sécurité majeur auquel vous souhaitez lier le lien.
   c. Sélectionnez **OK**.
5. Sélectionnez **Proposer**.

Résultats

La proposition est soumise et les actions suivantes sont effectuées :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Dans l'enregistrement d'incident de sécurité, un message de bannière de vérification s'affiche et la balise d'incident de sécurité majeur définie apparaît à côté du champ **Sélectionner une balise de sécurité** .

- Dans l'onglet **Détails** de l'incident de sécurité majeur dans Gestion des incidents de sécurité majeurs, la liste déroulante Numéro d'enregistrement inclut les deux incidents.

- L'enregistrement apparaît dans la liste connexe Incident de sécurité majeur de l'enregistrement d'incident, avec l'état Proposé.

- Un message contenant un lien vers l'enregistrement d'incident et l'onglet Détails de l'incident est envoyé aux personnes figurant dans la liste de notification définie.

- La section **Activité** de l'espace de travail MSIM montre que l'incident de sécurité a été ajouté en tant qu'incident de sécurité enfant à l'incident de sécurité majeur avec un lien.

Utilisation de la vue de liste MSI dans l'espace de travail MSIM

La vue de liste de l'espace de travail MSIM vous permet d'afficher les incidents de sécurité majeurs proposés, promus et rejetés.

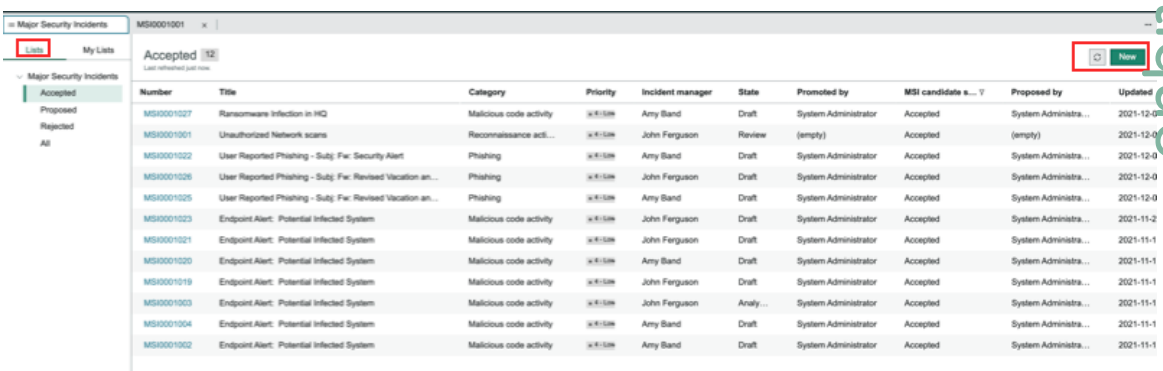
Avant de commencer

Rôle requis : sn_msi.workspace_manager

Vous pouvez également créer de nouveaux incidents à l'aide du bouton **Nouveau** disponible dans le coin supérieur droit de l'espace de travail.

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Espace de travail MSIM**.
2. Sélectionnez l'onglet Listes pour afficher la vue Listes.



3. Sélectionnez **Mes listes** pour créer votre propre liste d'incidents de sécurité majeurs.
4. Reportez-vous au tableau suivant pour savoir ce que vous pouvez faire à partir de la vue de liste :

Tâche	Description
Mes listes	Créez de nouvelles listes d'enregistrements MSI et affichez celles que vous avez créées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
Définir des filtres pour une colonne d'une liste	Sélectionnez une colonne et développez le menu de points verticaux pour afficher les options qui filtrent davantage les données de la colonne.
Filtrer les éléments ou faire correspondre les éléments d'une ligne dans une colonne	Sélectionnez une cellule dans une colonne et affinez les données affichées en choisissant l'une des options suivantes : ○ Afficher la correspondance : affiche uniquement les éléments qui correspondent à l'élément sélectionné dans la colonne. ○ Filtrer : filtrer les éléments de la colonne qui correspondent à l'élément sélectionné dans la colonne respective.
Actualiser la liste	Actualiser les listes et afficher les listes complètes qui ont été mises à jour.
Nouveau	Créez un nouvel enregistrement MSI.

Afficher les Incident de sécurité majeur mesures d'impact

Fournit des rapports de synthèse à jour sur l'impact et la progression des incidents de sécurité majeurs, ce qui est un aspect important de la gestion d'un incident de sécurité majeur à l'aide du nouvel espace de travail.

L'onglet **Vue d'ensemble** fournit les mesures pertinentes pour gérer à la fois le champ d'application et la progression de l'incident, y compris un déploiement des actifs, des utilisateurs, des emplacements et des ressources d'équipe affectés, ainsi que la chronologie des jalons importants de l'incident.

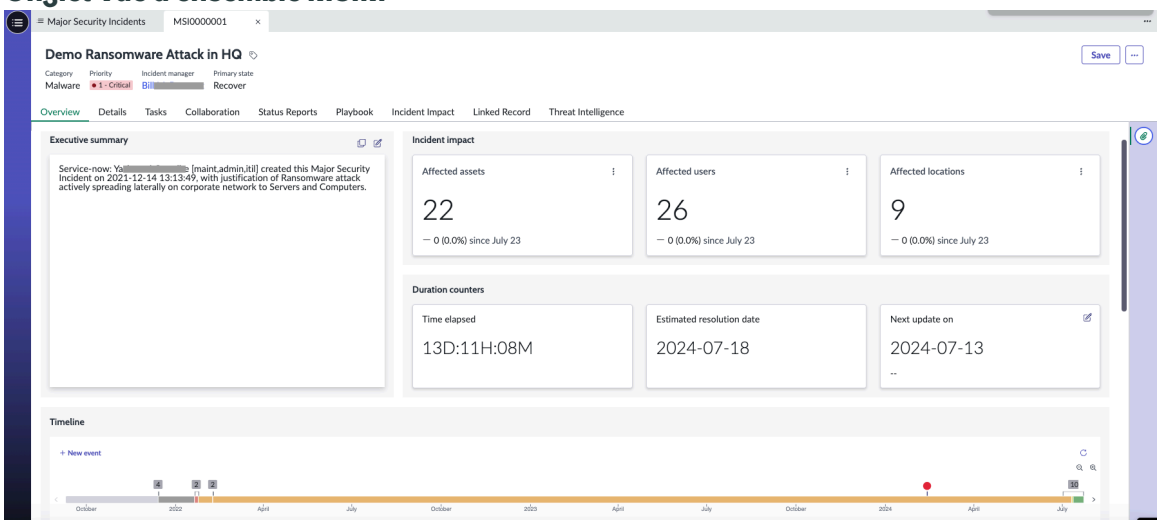
La chronologie fournit une vue horizontale des événements clés et des jalons qui se sont produits dans le cadre de la résolution de l'incident de sécurité majeur spécifique. Le composant de chronologie s'affiche au-dessus de tous les onglets de l'espace de travail de Major Security Incident Management, avec la possibilité de se réduire et de s'étendre pour une visualisation selon les besoins. Les données d'événements représentées seront mises à jour et actualisées chaque fois que des événements jalons ou des jalons désignés seront ajoutés ou mis à jour.

Chaque événement ou jalon est indiqué par une option de type d'événement de chronologie différente pour identifier le nombre et le type d'événements ou de jalons. Par exemple, mises à jour d'enregistrements NOW, activités de collaboration. En outre, la période pour les différents états d'incident de sécurité majeur est suivie automatiquement et affichée à l'aide de plages codées par couleur affichées avec la durée de chaque état d'incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d’ensemble MSIM



Résumé analytique et impact de l’incident

Tâche	Description
Résumé du cadre	Bref résumé de l’incident de sécurité majeur ainsi que le nom et le rôle de l’utilisateur et les détails de l’horodatage. • Vous pouvez modifier le résumé analytique en sélectionnant l’icône **Modifier** . Une fois que vous avez apporté les modifications requises, sélectionnez l’option **Mettre à jour** . • Pour copier le résumé et le coller dans un incident de sécurité majeur, sélectionnez l’icône **Copier** et collez le résumé dans l’incident de sécurité majeur requis.
Impact de l'incident	Ces composants affichent les ressources impactées en fonction d’un déploiement de toutes les tâches actives et des incidents liés avec des actifs, des utilisateurs, des emplacements et des membres d’équipe identifiés. Les ressources impactées sont : • **Actifs affectés** • **Utilisateurs affectés** • **Emplacements affectés** La sélection des valeurs numériques vous permet d’explorer et d’accéder aux détails des actifs, des utilisateurs et des emplacements impactés, et affiche les tâches connexes dans l’onglet **Impact de l’incident** de l’espace de travail. En fonction du lien du type d’impact d’incident que vous avez sélectionné, les détails de l’incident connexe, tels que le

Traduction automatique

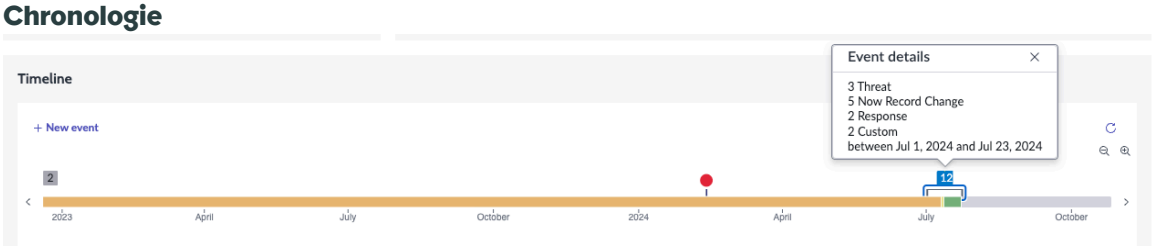
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résumé analytique et impact de l'incident (suite)

Tâche	Description
	type de tâche et sa description, le groupe d'affectation et l'état de l'incident, sont affichés dans le **Impact de l'incident** de l'espace de travail MSIM.
Compteurs de durée	Ces composants affichent la durée de l'incident de sécurité majeur. Les ressources impactées sont : • **Temps écoulé** : affiche le temps écoulé depuis le moment où l'incident de sécurité majeur est détecté. • **Date de résolution estimée** : affiche la date de résolution estimée à laquelle la résolution de l'incident de sécurité majeur est estimée. • **Prochaine mise à jour le** : date et heure de la prochaine mise à jour pour la résolution de l'incident de sécurité majeur. Par exemple, à 17h00 HNE le 25 mars 2024. Vous pouvez modifier la **prochaine mise à jour en** sélectionnant l'icône **Modifier** . Sélectionnez la nouvelle date et heure, puis sélectionnez **Mettre à jour**.

Vous pouvez activer ou désactiver l'affichage de certains types d'événements pour les indicateurs de chronologie et les plages de chronologie en conséquence à l'aide des boutons bascule de filtre.

Chronologie



Reportez-vous au tableau suivant pour connaître les options supplémentaires disponibles avec le composant de chronologie.

Options supplémentaires du composant de chronologie

Tâche	Description
Nouvel événement	Crée de nouveaux événements personnalisés et les associe à l'enregistrement MSI. Cela permet de créer des événements pour les dates passées et futures qui ne seraient peut-être pas capturées via une tâche étiquetée, un changement d'état d'enregistrement ou une activité de collaboration étiquetée, qui sont affichées par défaut sur la chronologie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Options supplémentaires du composant de chronologie (suite)

Tâche	Description
Actualiser	Actualise les événements de chronologie pour afficher les dernières mises à jour.
Indicateurs de chronologie	Répertorie les différents types d'événements tels que les modifications des champs Now Record, les activités de collaboration étiquetées et Autre (personnalisé), ainsi que les icônes et le nombre total d'événements qui se sont produits pour chaque indicateur de type d'événement. L'indicateur de diapositives vous permet d'activer ou de désactiver tous les événements pour un type d'événement spécifique.
Afficher la légende	Sélectionnez cette option pour afficher la légende déroulante avec différents types d'indicateurs de chronologie.
Barre de progression de la chronologie	Affiche la progression globale de l'incident via des événements ou des jalons de chronologie désignés qui se sont produits dans les différentes plages de chronologie affichées. Vous pouvez également lier un type d'événement à une catégorie d'événement. Une fois que vous l'avez lié, les détails de l'événement sont mis à jour aux deux endroits de la chronologie.
Plages de chronologie	Affiche les différents types d'états et durées des incidents à mesure que l'incident progresse tout au long du cycle de vie de l'incident de sécurité majeur. Activer ou désactiver un événement spécifique en fonction de l'état de l'incident.

Créer un événement de chronologie

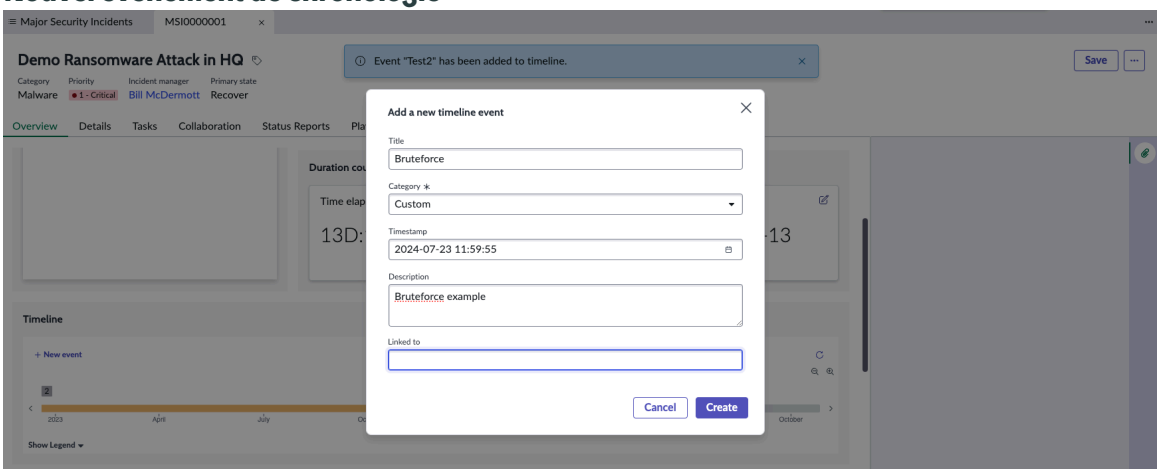
Pour créer un nouvel événement de chronologie, procédez comme suit :

1. Dans l'onglet Vue d'ensemble, accédez à la section **Chronologie** .
2. Sélectionner **+ Nouvel événement**.
3. Renseignez les champs de la fenêtre contextuelle Ajouter un nouvel événement de chronologie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nouvel événement de chronologie



Tâche	Description
Titre	Saisissez le titre de l'événement de chronologie.
Catégorie	Sélectionnez une catégorie pour l'événement de chronologie. Les catégories suivantes sont fournies dans le cadre du système de base et vous pouvez en choisir une en fonction de vos besoins. ○ **Personnalisé**. ○ **Réponse**. ○ **Menace**. Pour ajouter ou configurer une catégorie d'événement de chronologie, reportez-vous à la section Configurer des catégories de chronologie pour les incidents de sécurité majeurs.
Horodatage	Sélectionnez la date et l'heure de l'événement de chronologie à l'aide du calendrier Horodatage. Vous pouvez ajouter des événements à la chronologie avant et après la date de début.
Description	Fournissez une brève description de l'événement de chronologie.
Lié à	Option permettant de lier l'événement de chronologie à un enregistrement d'incident de sécurité majeur.

4. Sélectionner **Créer**.
5. Vous pouvez utiliser les icônes Zoom **avant** et **Zoom arrière** pour effectuer un zoom avant ou arrière sur la barre de progression de la chronologie, ce qui inclut l'affichage d'événements individuels lorsque des nombres sont affichés pour représenter plusieurs événements à proximité de l'heure de clôture.

   Vous pouvez également ajouter le niveau de zoom par défaut pour afficher tous les événements.
6. Sélectionnez l'icône **Actualiser** pour afficher les derniers événements de chronologie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

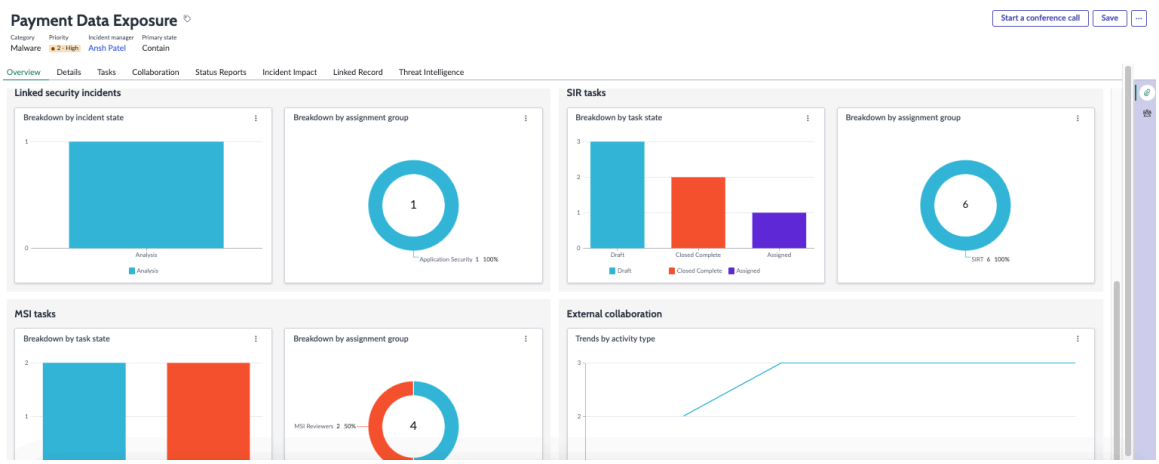
Afficher les Incident de sécurité majeur graphiques de tendance

Affichez les mesures de progression de l'impact de l'incident de sécurité majeur visualisées sous forme de graphiques à barres et de diagrammes.

En plus des visualisations de la chronologie des incidents et du graphique de tendance de progression, le **Vue d'ensemble** fournit des mesures d'impact pertinentes pour gérer l'évolution du champ d'application de l'incident, y compris le déploiement des actifs, des utilisateurs, des emplacements et des ressources d'équipe affectés.

Les nombres affichés dans les composants de visualisation sont basés sur les tâches actives sur les incidents de Réponse aux incidents de sécurité (SIR) liés. Au fur et à mesure que les tâches sont ouvertes et fermées, ces nombres changent en termes de nature et de volume d'activité restante planifiée pour l'incident de sécurité majeur afin de représenter les tendances affichées dans les composants de visualisation du graphique de tendances.

Mesures d'impact de l'onglet Vue d'ensemble MSIM



Reportez-vous au tableau suivant pour connaître les actions d'interface utilisateur que vous pouvez effectuer à partir du **Vue d'ensemble** section:

Sections de l'interface utilisateur Vue d'ensemble

Titre	Description
Heure	Affiche la période en nombre total de jours à partir du moment où l'incident de sécurité majeur est actif. Le temps est calculé en fonction de la **Date de détection** saisi dans le **Détails** de l'espace de travail. La date de détection est souvent capturée initialement lorsque l'incident de sécurité majeur a été créé ou proposé pour la première fois. Chaque fois que cette date est modifiée, l'heure est automatiquement calculée, actualisée et affichée au format jours : heures : minutes, par exemple 20D : 13H : 58M. **Date de résolution estimée**: date à laquelle la résolution de l'incident est estimée être résolue. Cette date est souvent

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sections de l'interface utilisateur Vue d'ensemble (suite)

Titre	Description
	capturée initialement lorsque l'incident de sécurité majeur a été créé ou promu pour la première fois. La date est mise à jour et actualisée en fonction de la date estimée fournie dans le **Détails** de l'espace de travail. Si la date estimée n'est pas fournie dans la section Détails, cette section affiche un « trait d'union » sans aucune valeur de date.
Équipe active	Affiche les différentes équipes de réponse et les membres de chaque équipe qui travaillent activement sur l'incident de sécurité majeur et ses tâches connexes. **Équipe active** tendance : affiche le graphique de tendance de chaque équipe et des membres de son équipe qui travaillent activement sur l'incident de sécurité majeur et les tâches connexes à intervalles réguliers. **Remarque :** Afficher les groupes actifs affectés à partir de **Détails** de l'espace de travail.
Incidents SIR liés	**Par état de l'incident**: affichez la répartition des incidents de sécurité liés en fonction d'un état d'incident tel que Analyser, Contenir, Éradiquer, Récupérer ou Examiner. **Tendances par l'état d'incident**: indique en outre la vue des tendances de la progression du nombre d'incidents liés en fonction de l'état de l'incident. La sélection de chaque lien d'état d'incident vous permet de parcourir et d'afficher les détails de l'incident de sécurité lié directement sur le **SI/VI lié** de l'espace de travail. Cette section est mise à jour et actualisée automatiquement chaque fois que des changements sont apportés aux incidents sous-jacents.
Tâches SIR	Affiche le total des tâches actives liées à l'enregistrement MSI via des incidents SIR. • **Par état de la tâche**: afficher les tâches de réponse aux incidents en fonction de l'état de l'incident, par exemple Brouillon,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sections de l'interface utilisateur Vue d'ensemble (suite)

Titre	Description
	Affecté, Travail en cours, Fermé terminé. Ce graphique de distribution permet une répartition plus détaillée de la distribution par groupes d'affectation. La sélection de chaque état de tâche vous permet d'afficher une liste filtrée par état de tâche d'incident sur le **Tâches** de l'espace de travail. La vue filtrée vous permet d'afficher et de mettre à jour les détails de chaque tâche. • **Tâches en cours par étiquette d'état d'incident**: affiche les tâches et les groupes actifs en fonction de l'étiquette d'état de l'incident qui doit être appliquée dans les composants de l'organisateur de tâche. Ces étiquettes par défaut ont des valeurs telles que Analyse, Contenir, Éradiquer, Récupérer ou Examiner pour indiquer la nature de la tâche impliquée. • **En retard**: affiche les tâches de réponse aux incidents de sécurité qui sont actives et qui ont dépassé la date d'échéance. Vous pouvez afficher les détails de toutes les tâches en retard en sélectionnant le nombre total de tâches en retard et en le faisant naviguer automatiquement vers l'onglet Tâches. • **Tendances par état de tâche**: afficher la tendance de progression des tâches de réponse en cours et fermées sur la durée de l'incident. **Remarque :** Le graphique de tendance récupère les données les plus récentes en fonction de la tâche planifiée. Vous pouvez configurer ou modifier l'intervalle de temps de récupération de données selon vos besoins.
Tâches MSI	Affiche l'ensemble des tâches actives qui ont été créées directement sur l'enregistrement MSI (et qui ne sont pas des tâches de réponse liées) : **Par état de la tâche :** Affichez les tâches créées pour l'incident de sécurité majeur, les tâches affectées et les informations connexes. La sélection de chaque état de tâche vous permet d'afficher une liste filtrée par

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sections de l'interface utilisateur Vue d'ensemble (suite)

Titre	Description
	état de tâche d'incident sur le **Tâches** de l'espace de travail. La vue filtrée permet d'afficher et de mettre à jour les détails des tâches individuelles.
Collaboration externe	Affiche le total des activités de collaboration pour toutes les activités de collaboration étiquetées du flux d'activité de collaboration : • **Par étiquette d'état d'incident :**Affichez les données des activités de collaboration liées aux incidents qui Microsoft TeamsMicrosoft SharePoint sont coordonnées, ainsi que les fichiers et les dossiers, et qui sont étiquetées à l'aide d'étiquettes d'état d'incident telles que Analyse, Contenir, Éradiquer ou Récupérer dans l'onglet **Collaboration** de l'espace de travail. • **Tendances par type d'activité**: consultez le graphique de tendance du nombre d'activités de Microsoft TeamsMicrosoft SharePoint fichiers et de dossiers sur la durée de l'incident.

Mettre à jour Incident de sécurité majeur les détails

Affichez et mettez à jour des détails spécifiques liés à l'incident de sécurité majeur, tels que les détails de l'enregistrement d'incident, les participants à l'équipe active et le journal d'activité correspondant.

Tous les détails relatifs à l'incident de sécurité majeur sont affichés dans différentes sections de formulaire sous l'onglet **Détails** de l'espace de travail. Affiche les détails tels que les détails de l'enregistrement d'incident, les participants à l'équipe active et le journal d'activité correspondant. Vous pouvez également afficher les incidents SIR liés, les détails des enregistrements du groupe de vulnérabilité et la possibilité de diffuser une publication d'activité dans tous les enregistrements d'incidents liés.

L'onglet Détails contient principalement :

1. Champs du formulaire d'incident de sécurité majeur et sections de l'interface utilisateur liées aux incidents.
2. Flux d'activité

La table suivante fournit les détails des champs du formulaire d'incident de sécurité majeur :

Sections du formulaire Incident de sécurité majeur

Champ	Description
Incident	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sections du formulaire Incident de sécurité majeur (suite)

Champ	Description
Numéro	Numéro d'enregistrement d'incident de sécurité majeur.
État primaire	État primaire de l'enregistrement d'incident de sécurité majeur.
Date de détection	Date à laquelle l'incident de sécurité majeur a été créé ou proposé pour la première fois. Chaque fois que vous modifiez la date de détection dans l'onglet Détails, la date et l'heure de l'incident de sécurité sont automatiquement calculées, actualisées et affichées sur le **Heure** > **Délai depuis le début de l'incident** dans la section **Vue d'ensemble** de l'espace de travail.
Titre	Titre de l'incident de sécurité majeur.
Nom de code	Nom de code de l'incident de sécurité majeur. Par exemple, Blue Tiger.
Prochaine mise à jour le	Date et heure de la prochaine mise à jour pour la résolution de l'incident de sécurité majeur. Par exemple, à 17h00 HNE le 25 mars 2024.
Catégorie	Catégorie de l'incident de sécurité majeur.
Sous-catégorie	Type de sous-catégorie de l'incident de sécurité majeur.
Date de résolution estimée	Date estimée à laquelle l'incident devrait être résolu. La valeur par défaut est de 7 jours à compter de la création de l'incident de sécurité majeur.
Priorité	Priorité de l'incident de sécurité majeur.
Capteur d'alerte	Capteur d'alerte de l'incident de sécurité majeur. Par exemple, Hameçonnage signalé par un utilisateur.
Source	Source de l'incident de sécurité majeur.
Équipe active	
Gestionnaire des incidents	Nom du gestionnaire d'incidents.
Groupes d'affectation	Indique les différentes équipes de réponse et les membres de chaque équipe qui travaillent activement sur l'incident de sécurité majeur.
Candidat	
État du candidat MSI	Indique l'état candidat à l'incident de sécurité majeur, comme proposé ou promu. Si l'incident est promu, l'état est affiché comme Accepté.
Promus par	Utilisateur ayant promu l'incident de sécurité majeur.
Promu(e)	Date à laquelle l'incident de sécurité majeur a été promu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sections du formulaire Incident de sécurité majeur (suite)

Champ	Description
Justification	Justification de l'incident de sécurité majeur. La justification doit inclure le numéro MSI et le nom de code.
Impact potentiel	L'impact et la gravité potentiels de l'incident de sécurité majeur. L'impact potentiel doit inclure le numéro MSI et le nom de code.
Restriction	
Appliquer la restriction	Sélectionnez cette option pour appliquer des restrictions sur certaines restrictions d'incident de sécurité majeur. Vous pouvez appliquer des restrictions pour limiter la vue ou modifier l'accès uniquement à certains utilisateurs ou groupes. Pour plus d'informations, consultez Restreindre l'accès à certains incidents de sécurité majeurs.
Membres autorisés	Liste des utilisateurs pouvant accéder à l'incident de sécurité majeur.
Groupes autorisés	Liste des groupes pouvant accéder à l'incident de sécurité majeur.
Autres actions	
Pièce jointe	Toute pièce jointe liée à l'incident de sécurité majeur. Sélectionnez l'option **Sélectionner** pour ajouter des pièces jointes à l'incident.
Téléconférence	Utilisez les téléconférences avec les fournisseurs de services tiers comme canal de communication pour rencontrer les personnes concernées en vue de résoudre les incidents de sécurité majeurs. Pour plus d'informations, voir Gestion des incidents de sécurité majeurs Intégration de téléconférence

Activité :

Utilisez la section Activité pour ajouter vos notes de travail et vos commentaires, et publiez votre activité en privé et ajoutez également des commentaires supplémentaires si nécessaire à l'aide de la section Composer. Enregistrez l'activité après avoir publié vos notes de travail et commentaires pour afficher l'activité ou les notes de travail ajoutées dans la section Activité.

Remarque : Sélectionnez le lien **Afficher plus** de détails pour afficher les détails d'un enregistrement d'incident de sécurité spécifique associé à cet incident de sécurité majeur.

Configurez vos préférences pour afficher les activités connexes, telles que :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. **Filtres** : sélectionnez l'icône **Ensembles de filtres** pour définir des filtres.

   Définissez des filtres pour afficher les conversations sur les activités, telles que les activités ajoutées dans les notes de travail, l'e-mail, la chronologie et tout commentaire supplémentaire.

2. **Marqué** : sélectionnez l'icône **Marqué** pour marquer les activités.

   Marquez toutes les conversations d'activité importantes pour les garder à portée de main.

Restreindre l'accès à certains incidents de sécurité majeurs

Gérez qui peut consulter ou modifier les incidents de sécurité majeurs qui contiennent des informations sensibles. Vous pouvez appliquer des restrictions d'incident de sécurité majeur pour déterminer qui a accès à l'affichage ou à la modification de certains enregistrements d'incidents de sécurité majeurs et des listes connexes, et limiter l'accès en lecture ou en écriture à certains utilisateurs ou groupes.

Avant de commencer
Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche
Les restrictions relatives aux incidents de sécurité majeurs vous permettent de masquer l'accès ou la modification des incidents de sécurité majeurs critiques par tous les utilisateurs ou groupes d'une organisation particulière. Ces restrictions vous permettent de fournir un moyen plus granulaire de contrôler les incidents de sécurité majeurs qu'un utilisateur ou un groupe peut afficher ou modifier. Vous pouvez appliquer une restriction d'incident de sécurité majeur en cochant la case **Appliquer la restriction** et en sélectionnant les utilisateurs ou les groupes autorisés à afficher ou à modifier l'incident de sécurité majeur particulier.

Une fois que vous avez appliqué la restriction sur les incidents de sécurité majeurs ou les listes connexes à certains utilisateurs ou groupes, tous les utilisateurs ou groupes restants de votre organisation ne seront pas en mesure d'afficher ou de modifier ces incidents de sécurité majeurs ou les listes connexes.

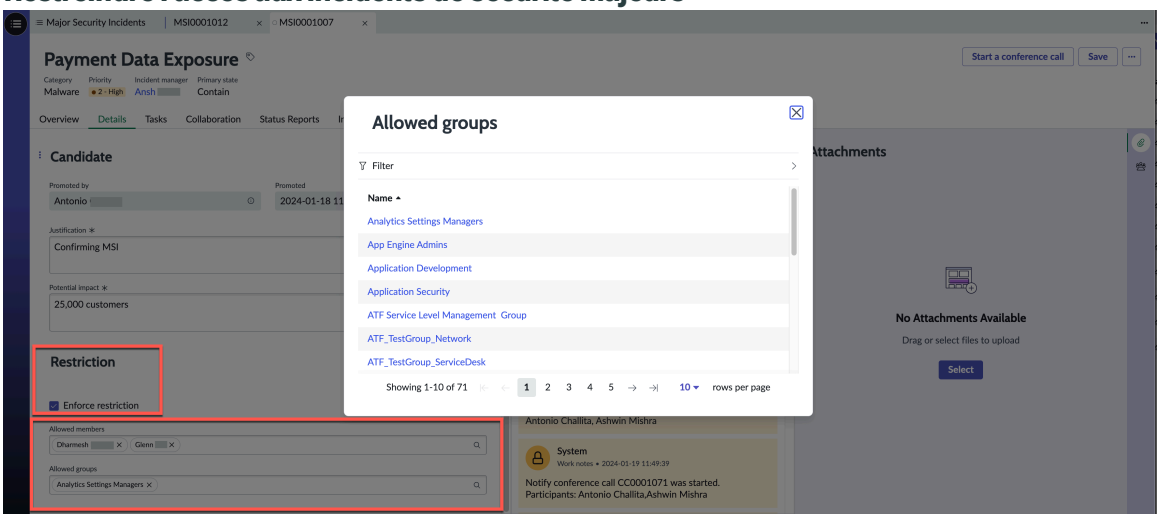
Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Détails**.
5. Faites défiler vers le bas et sélectionnez la section **Restriction** .
6. Cochez la case **Appliquer la restriction** pour activer la restriction de l'incident de sécurité majeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Restreindre l'accès aux incidents de sécurité majeurs



7. Dans le champ Membres autorisés, sélectionnez les utilisateurs qui peuvent afficher ou modifier l'incident de sécurité majeur à l'aide de l'option Rechercher.
8. Dans le champ Groupes autorisés, sélectionnez les groupes qui peuvent afficher ou modifier l'incident de sécurité majeur à l'aide de l'option Rechercher.

> **Remarque :** Une fois que la case **Appliquer la restriction** est cochée pour l'incident de sécurité majeur, seuls le sn_msi.workspace_manager et les membres ou groupes autorisés auront accès à l'affichage ou à la modification de l'incident de sécurité majeur.

9. Sélectionnez **Enregistrer**.

Lier des enregistrements supplémentaires à Incident de sécurité majeur

Dans l'espace de travail, utilisez la fonctionnalité de liaison des enregistrements pour lier tous les enregistrements d'incident de sécurité connexes et ses incidents de sécurité enfants, les tâches de rattrapage de Vulnerability Response et les tickets de sécurité de Threat Intelligence à un Incident de sécurité majeur enregistrement (MSI).

Avant de commencer

Rôles requis : sn_msi.workspace_manager et sn_msi.workspace_responder

Procédure

1. Accédez à la **Réponse aux incidents de sécurité majeurs** > **Espace de travail MSIM**.
2. Accédez à la vue **Listes** , qui s'affiche dans le volet gauche de l'espace de travail.
3. Cliquez sur **Accepté** pour sélectionner les enregistrements d'incidents de sécurité majeurs promus.
4. Sélectionnez l'enregistrement d'incident qui doit être lié et qui n'est pas à l'état Fermé dans la liste des enregistrements promus.
5. Cliquez sur l'onglet **Enregistrements liés** .
   Une liste déroulante est fournie pour sélectionner d'autres tables d'enregistrements liés.
   La section Enregistrements liés affiche les enregistrements liés et ses enregistrements connexes, qui étaient liés à l'incident de sécurité majeur.
6. Sélectionnez la vue de table souhaitée, par exemple Incidents de sécurité, Tâches de rattrapage (éléments vulnérables) ou Ticket de sécurité dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En fonction de votre vue de la table d'enregistrements de type de sélection, les enregistrements liés aux enregistrements d'incidents de sécurité majeurs s'affichent.

7. Liez un enregistrement qui n'est lié à aucun enregistrement MSI et qui est à l'état **Ouvert** en sélectionnant l'enregistrement et en cliquant sur **Lier l'enregistrement** en haut à droite de la page.

   Remarque : Vous ne pouvez pas lier un enregistrement d'incident à un enregistrement MSI si celui-ci est à l'état **Fermé** .

8. Sélectionnez l'enregistrement à lier, puis cliquez sur **Lien**.
   Un message de confirmation indique que l'enregistrement est lié avec succès et que le déploiement des enregistrements connexes est traité en arrière-plan.

   Remarque : Une fois qu'un enregistrement est lié, la vue de liste est automatiquement actualisée et répertorie la liste mise à jour des enregistrements d'incidents.

Information associée

Dissocier les enregistrements de Incident de sécurité majeur

Dissocier les enregistrements de Incident de sécurité majeur

À l'aide de l'espace de travail Gestion des incidents de sécurité majeurs, dissociez les enregistrements d'incidents de sécurité majeurs de la section Enregistrements liés.

Avant de commencer

Rôles requis : sn_msi.workspace_manager et sn_msi.workspace_responder

Remarque : Vous ne pouvez dissocier qu'un seul enregistrement à la fois. Une fois que vous avez dissocié un enregistrement, les informations cumulatives connexes sont supprimées des sections Impact de l'incident et Threat Intelligence de l'espace de travail et l'action ne peut pas être annulée.

Pour plus d'informations sur les enregistrements de déploiement, reportez-vous à la section Cadre de travail de déploiement pour MSIM.

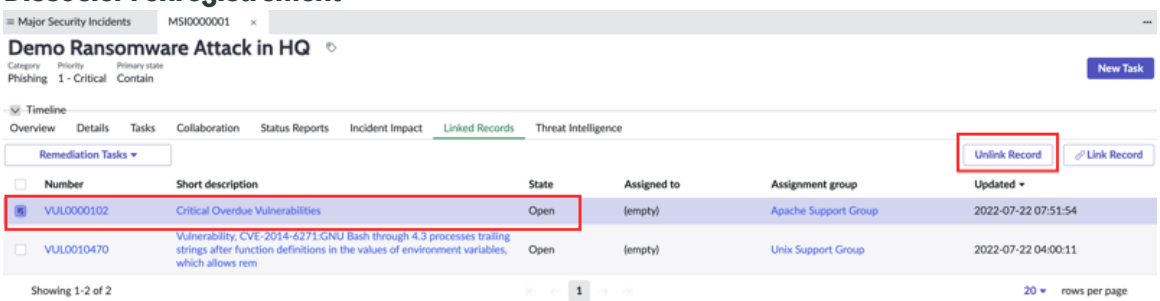
Procédure

1. Accédez à la **Réponse aux incidents de sécurité majeurs** > **Espace de travail MSIM**.
2. Accédez à la vue **Listes** , qui s'affiche dans le volet gauche de l'espace de travail.
3. Cliquez sur **Accepté** pour sélectionner les enregistrements d'incidents de sécurité majeurs promus.
4. Cliquez sur l'onglet **Enregistrements liés** .
   Cette section affiche les enregistrements liés et ses enregistrements connexes, qui sont liés à l'incident de sécurité majeur.
5. Sélectionnez la vue de table souhaitée, par exemple Incidents de sécurité, Tâches de rattrapage (éléments vulnérables) ou Ticket de sécurité.
6. Sélectionnez l'enregistrement à dissocier de la vue de liste des enregistrements.
7. Cliquez sur **Dissocier l'enregistrement**.

Traduction automatique

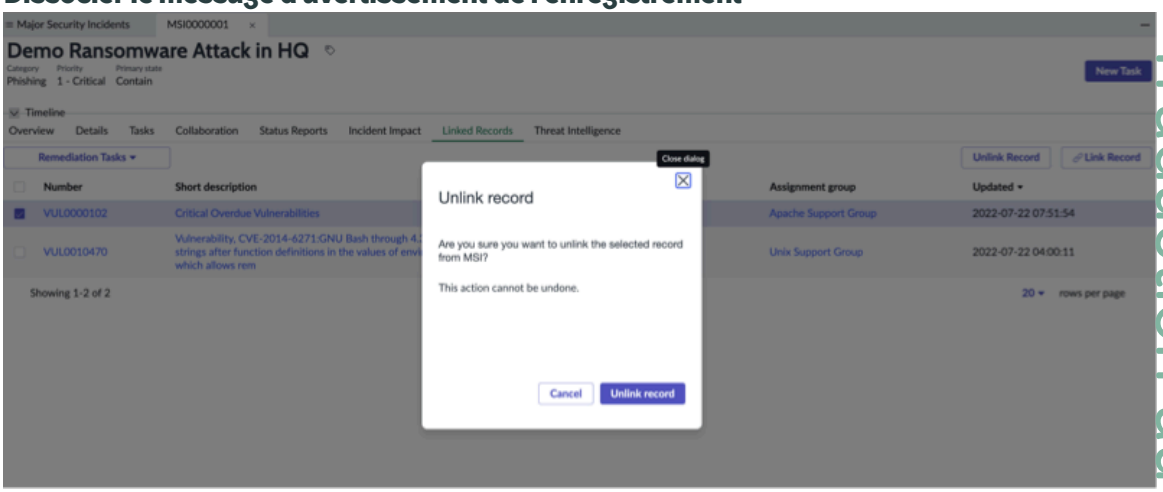
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dissocier l'enregistrement



8. Un message d'avertissement s'affiche pour vous demander si vous souhaitez dissocier l'enregistrement sélectionné de MSI.

Dissocier le message d'avertissement de l'enregistrement



9. Cliquez sur **Dissocier l'enregistrement**.
   Le lien de l'enregistrement est annulé et, une fois supprimé, les changements ne peuvent pas être annulés. La vue de liste des enregistrements liés sera actualisée après la suppression de la liaison.

Information associée

Configurer les enregistrements liés dans Gestion des incidents de sécurité majeurs

Configurer les enregistrements de déploiement dans Gestion des incidents de sécurité majeurs

Gérer les tâches dans un Incident de sécurité majeur

L'onglet Tâche vous permet de suivre et de gérer toutes les tâches associées à un incident de sécurité majeur à partir de l'espace de travail MSIM. Vous pouvez afficher les différentes tâches à l'aide du tableau visuel des tâches par défaut (vue Kanban) ou de la vue Listes.

Le sn_msi.workspace_manager peut effectuer les actions suivantes dans l'onglet Tâches :

- Créer une tâche
- Modifier les tâches
- Afficher et affecter des tâches à soi-même ou à d'autres personnes
- Supprimer des tâches

Traduction automatique

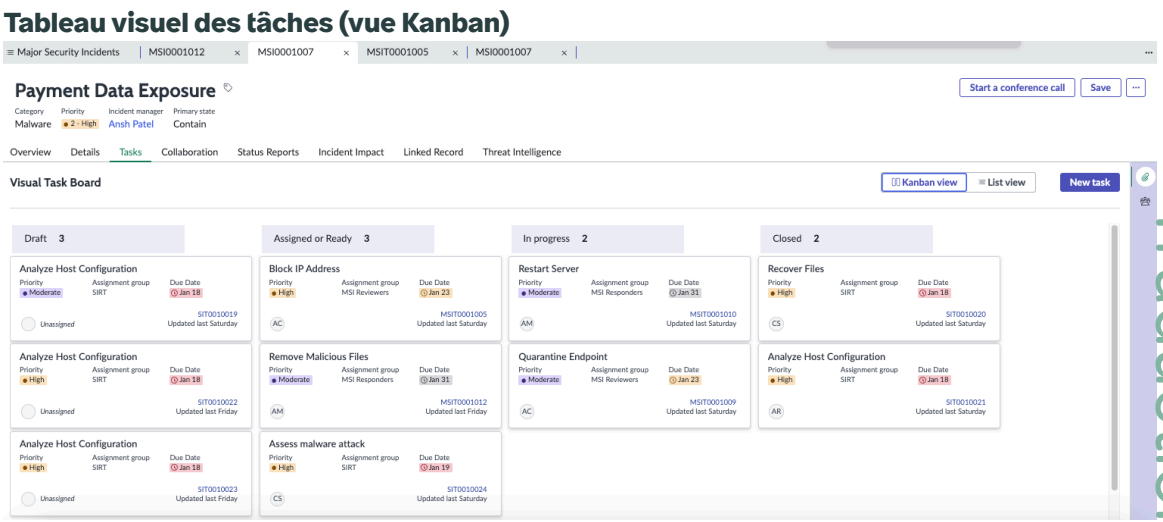
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Assurez-vous d'avoir installé **l'application Carte de tâche VTB MSIM : 1.0.1v** séparément après avoir installé l'application MSIM.

L'onglet Tâches affiche les détails de toutes les tâches associées à un incident de sécurité majeur. L'onglet Tâche prend en charge deux vues :

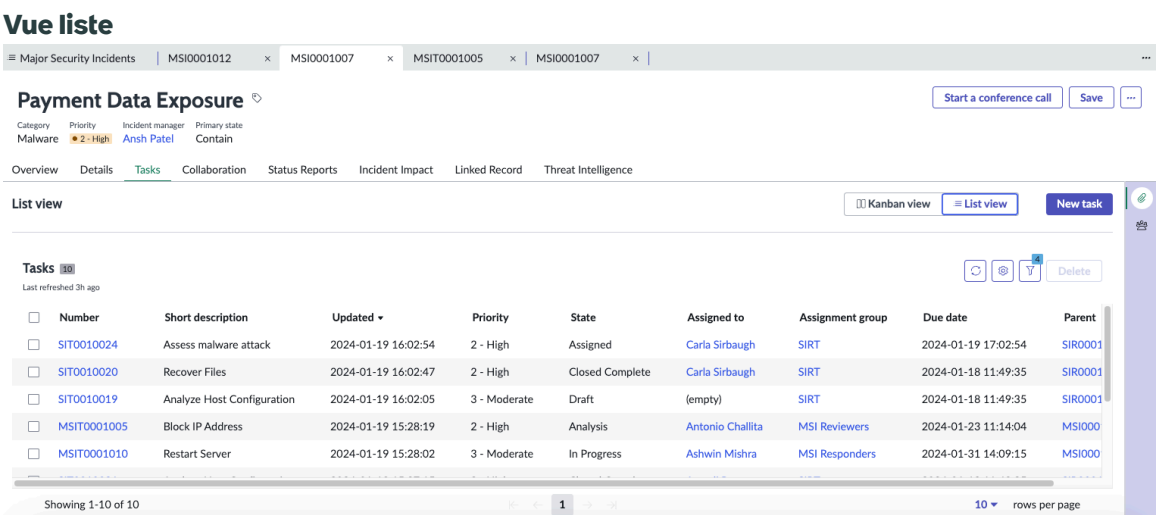
- **Tableau visuel des tâches (vue Kanban)** :

  Affichez et mettez à jour plusieurs enregistrements de tâches, qui apparaissent sous forme de cartes sur le tableau visuel des tâches qui peuvent être déplacées entre les voies en fonction de l'état des tâches dans l'incident de sécurité majeur.



- **Vue liste** :

  Affichez et mettez à jour plusieurs enregistrements de tâches sous forme de listes. À l'aide de ces catégories de liste et de ces filtres, vous pouvez rapidement trouver et suivre les tâches sur lesquelles vous devez travailler dans un incident de sécurité majeur.



Les activités étiquetées sont résumées et affichées dans la section Vue d'ensemble de l'incident de sécurité majeur. Un graphique de tendance est disponible dans la section Vue d'ensemble pour afficher l'état des activités de la tâche consolidée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer des tâches à l'aide du tableau visuel des tâches

Suivez et gérez toutes les tâches associées à un incident de sécurité majeur à l'aide du Tableau visuel des tâches (vue Kanban).

Vous pouvez utiliser le Tableau visuel des tâches pour déplacer les cartes étape par étape entre les voies telles que Brouillon, Affecté ou Prêt, En cours et Fermé en fonction de l'état des tâches. Un flux d'activité sur le tableau affiche l'activité récente pour suivre facilement les changements de tâches. Vous pouvez ajouter des cartes de tâches à partir de n'importe quelle table qui étend la tâche pour suivre rapidement les mises à jour et modifier les incidents de sécurité majeurs directement à partir du tableau.

Créer une tâche à l'aide du Tableau visuel des tâches

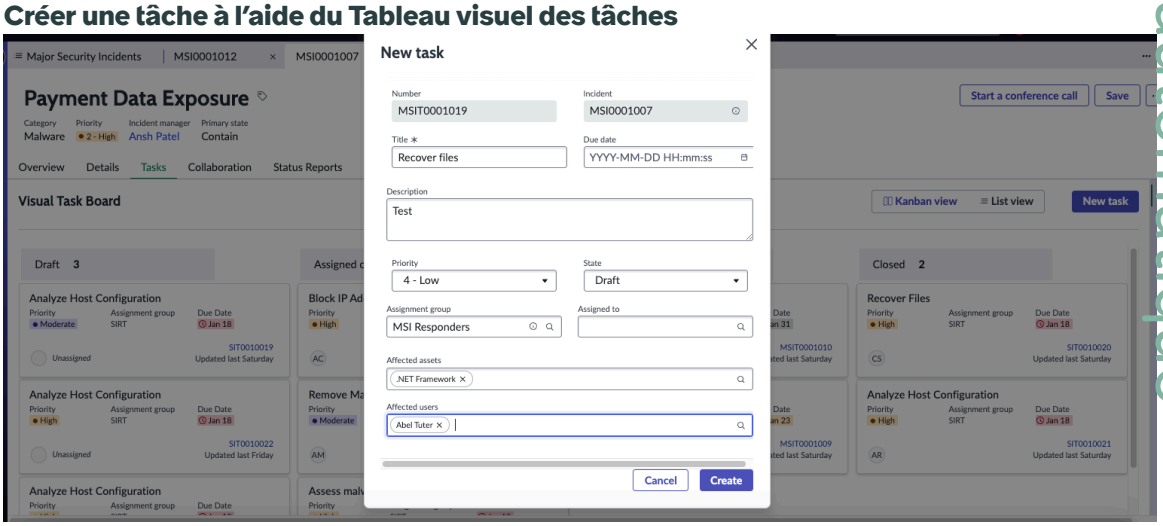
Rôle requis : sn_msi.workspace_manager.

Remarque : Assurez-vous d'avoir installé **l'application Carte de tâche VTB MSIM : 1.0.1v** séparément après avoir installé l'application MSIM.

Les gestionnaires MSI peuvent créer une tâche dans le Visual Task Board en procédant comme suit :

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** .

Créer une tâche à l'aide du Tableau visuel des tâches



5. Sélectionnez **la vue Kanban**, puis Nouvelle **tâche**.
6. Remplissez les champs du formulaire.

Champ	Description
Numéro	Un numéro unique qui est automatiquement généré pour la tâche sélectionnée. Ce champ n'est pas modifiable.
Incident	Numéro d'incident de sécurité majeur. Ce champ n'est pas modifiable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Titre	Nommez la tâche.
Date d'échéance	Sélectionnez une date et une heure d'échéance pour l'achèvement de la tâche. Sélectionnez une date à l'aide de l'option **Calendrier** et spécifiez l'heure dans la section **Sélectionner une heure** .
Description	Fournissez une description unique de la tâche.
Priorité	Sélectionnez la priorité de la tâche pour déterminer quand la tâche est exécutée. La priorité peut être l'une des valeurs suivantes : ○ **Aucun** ○ **1 - Critique** ○ **2 : Élevé** ○ **3 : Modéré** ○ **4 - Faible** ○ **5- En préparation**
État	Sélectionnez l'état actuel de la tâche. L'état peut être l'un des suivants : ○ **Brouillon** ○ **Analyse** ○ **En cours** ○ **Fermé** L'état par défaut est **Brouillon**.
Groupe d'affectation	Sélectionnez un groupe d'affectation de l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Affecté à	Sélectionnez l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Actifs affectés	Sélectionnez les actifs affectés par la tâche à l'aide de l'option de recherche.
Utilisateurs affectés	Sélectionnez les utilisateurs affectés par la tâche à l'aide de l'option de recherche.

Traduction automatique

7. Sélectionnez **Créer** pour créer la tâche.

Afficher et modifier une tâche à l'aide du Tableau visuel des tâches

Rôle requis : sn_msi.workspace_manager.

Remarque : Assurez-vous d'avoir installé **l'application Carte de tâche VTB MSIM : 1.0.1v** séparément après avoir installé l'application MSIM.

Les gestionnaires MSI peuvent afficher les détails d'une tâche et les informations d'activité à partir des répondeurs MSI et modifier une tâche dans le tableau visuel des tâches en procédant comme suit :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** , puis choisissez **la vue Kanban**.
5. Choisissez la carte de tâche souhaitée dans l'une des voies pour afficher les détails de la tâche.

   La carte de tâche peut se trouver dans l'une des voies suivantes : Brouillon, Affecté ou Prêt, En cours ou Fermé.
6. Dans la section Informations sur la tâche, vous pouvez modifier les détails suivants :

Champ	Description
Numéro	Un numéro unique qui est automatiquement généré pour la tâche sélectionnée. Ce champ n'est pas modifiable.
Incident	Numéro d'incident de sécurité majeur. Ce champ n'est pas modifiable.
Titre	Nommez la tâche.
Date d'échéance	Sélectionnez une date et une heure d'échéance pour l'achèvement de la tâche. Sélectionnez une date à l'aide de l'option **Calendrier** et spécifiez l'heure dans la section **Sélectionner une heure** .
Description	Fournissez une description unique de la tâche.
Priorité	Sélectionnez la priorité de la tâche pour déterminer quand la tâche est exécutée. La priorité peut être l'une des valeurs suivantes : ○ **Aucun** ○ **1 - Critique** ○ **2 : Élevé** ○ **3 : Modéré** ○ **4 - Faible** ○ **5- En préparation**
État	Sélectionnez l'état actuel de la tâche. L'état peut être l'un des suivants : ○ **Brouillon** ○ **Analyse** ○ **En cours** ○ **Fermé** L'état par défaut est **Brouillon**.
Groupe d'affectation	Sélectionnez un groupe d'affectation de l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.

Traduction automatique

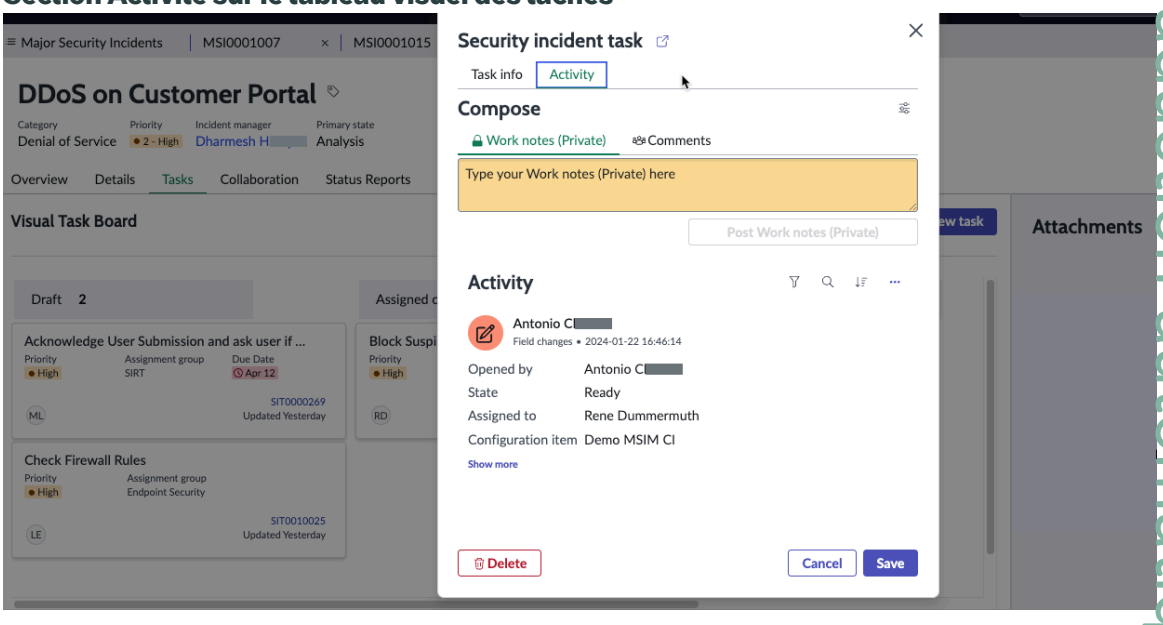
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Affecté à	Sélectionnez l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Actifs affectés	Sélectionnez les actifs affectés par la tâche à l'aide de l'option de recherche.
Utilisateurs affectés	Sélectionnez les utilisateurs affectés par la tâche à l'aide de l'option de recherche.

7. Sélectionnez la section **Activité** pour afficher les détails de l'activité des répondeurs MSI.

   Utilisez la section Activité pour ajouter vos notes de travail et vos commentaires, et publiez votre activité en privé et ajoutez également des commentaires supplémentaires si nécessaire à l'aide de la section Composer. Enregistrez l'activité après avoir publié vos notes de travail et commentaires pour afficher l'activité ou les notes de travail ajoutées dans la section Activité.

Section Activité sur le tableau visuel des tâches



Remarque : Sélectionnez le lien **Afficher plus** de détails pour afficher les détails d'un enregistrement d'incident de sécurité spécifique, associé à cet incident de sécurité majeur.

8. Sélectionnez **Enregistrer** pour mettre à jour les informations de la tâche.

   Les informations sur la tâche sont mises à jour instantanément.

Supprimer une tâche à l'aide du Tableau visuel des tâches

Rôle requis : sn_msi.workspace_manager.

Remarque : Assurez-vous d'avoir installé **l'application Carte de tâche VTB MSIM : 1.0.1v** séparément après avoir installé l'application MSIM.

MSI Manager peut supprimer une tâche dans le Visual Task Board en procédant comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** , puis choisissez la **vue Kanban**
5. Choisissez la carte de tâche que vous souhaitez supprimer.
6. Dans la fenêtre contextuelle de la tâche d'incident de sécurité majeur, sélectionnez l'option **Supprimer** .

   La fenêtre contextuelle Supprimer la tâche s'affiche et vous demande de confirmer la suppression de la tâche.

7. Sélectionnez **Supprimer**.

Gérer les tâches à l'aide de la vue de liste

Suivez et gérez toutes les tâches associées à un incident de sécurité majeur à l'aide de la vue de liste.

La vue de listes affiche les détails de toutes les tâches associées à l'incident de sécurité majeur, comme le numéro de tâche, la priorité, l'état actuel, l'affectation et le groupe affecté. À l'aide de ces catégories de liste et filtres, vous pouvez rapidement trouver et suivre les tâches requises sur lesquelles vous devez travailler en cas d'incident de sécurité majeur.

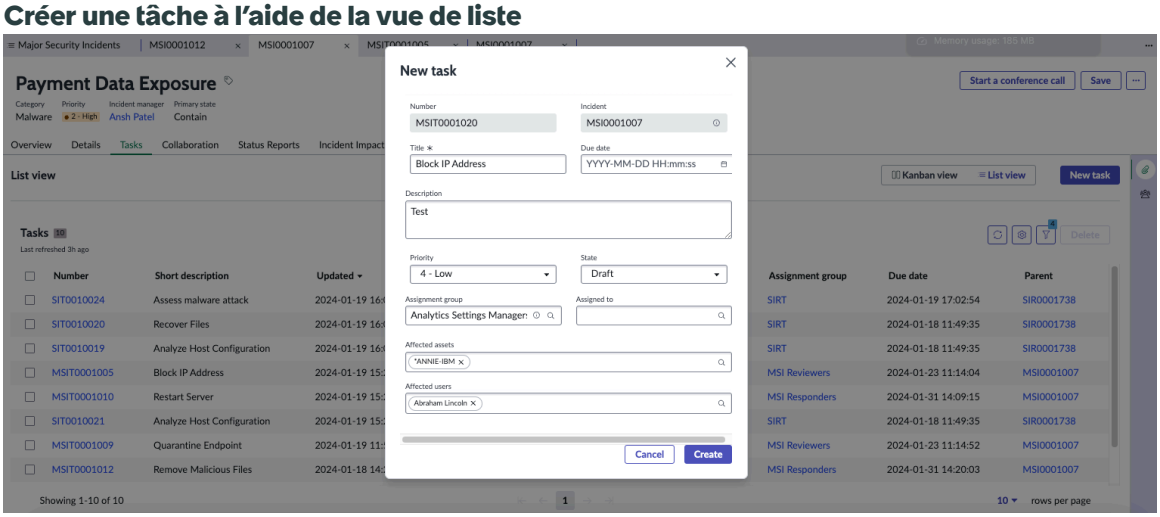
Créer une tâche à l'aide de la vue de liste

Rôle requis : sn_msi.workspace_manager.

Les gestionnaires MSI peuvent créer une tâche dans la vue de liste en procédant comme suit :

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** .

Créer une tâche à l'aide de la vue de liste



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez **la vue de liste**, puis choisissez **Nouvelle tâche**.
6. Remplissez les champs du formulaire.

Champ	Description
Numéro	Un numéro unique qui est automatiquement généré pour la tâche sélectionnée. Ce champ n'est pas modifiable.
Incident	Numéro d'incident de sécurité majeur. Ce champ n'est pas modifiable.
Titre	Nommez la tâche.
Date d'échéance	Sélectionnez une date et une heure d'échéance pour l'achèvement de la tâche. Sélectionnez une date à l'aide de l'option **Calendrier** et spécifiez l'heure dans la section **Sélectionner une heure** .
Description	Fournissez une description unique de la tâche.
Priorité	Sélectionnez la priorité de la tâche pour déterminer quand la tâche est exécutée. La priorité peut être l'une des valeurs suivantes : ○ **Aucun** ○ **1 - Critique** ○ **2 : Élevé** ○ **3 : Modéré** ○ **4 - Faible** ○ **5- En préparation**
État	Sélectionnez l'état actuel de la tâche. L'état peut être l'un des suivants : ○ **Brouillon** ○ **Analyse** ○ **En cours** ○ **Fermé** L'état par défaut est **Brouillon**.
Groupe d'affectation	Sélectionnez un groupe d'affectation de l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Affecté à	Sélectionnez l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Actifs affectés	Sélectionnez les actifs affectés par la tâche à l'aide de l'option de recherche.
Utilisateurs affectés	Sélectionnez les utilisateurs affectés par la tâche à l'aide de l'option de recherche.

7. Sélectionnez **Créer** pour créer la tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher et modifier une tâche à l'aide de la vue de liste

Rôle requis : sn_msi.workspace_manager.

Les gestionnaires MSI peuvent afficher les détails d'une tâche et les informations d'activité des intervenants MSI et modifier une tâche dans la vue de liste en procédant comme suit

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** , puis la **vue Liste**.
5. Choisissez la tâche souhaitée dans la vue de liste pour afficher les détails de la tâche.
6. Dans la section Informations sur la tâche, vous pouvez modifier les détails suivants :

Champ	Description
Numéro	Un numéro unique qui est automatiquement généré pour la tâche sélectionnée. Ce champ n'est pas modifiable.
Incident	Numéro d'incident de sécurité majeur. Ce champ n'est pas modifiable.
Titre	Nommez la tâche.
Date d'échéance	Sélectionnez une date et une heure d'échéance pour l'achèvement de la tâche. Sélectionnez une date à l'aide de l'option **Calendrier** et spécifiez l'heure dans la section **Sélectionner une heure** .
Description	Fournissez une description unique de la tâche.
Priorité	Sélectionnez la priorité de la tâche pour déterminer quand la tâche est exécutée. La priorité peut être l'une des valeurs suivantes : ○ **Aucun** ○ **1 - Critique** ○ **2 : Élevé** ○ **3 : Modéré** ○ **4 - Faible** ○ **5- En préparation**
État	Sélectionnez l'état actuel de la tâche. L'état peut être l'un des suivants : ○ **Brouillon** ○ **Analyse** ○ **En cours** ○ **Fermé** L'état par défaut est **Brouillon**.

Traduction automatique

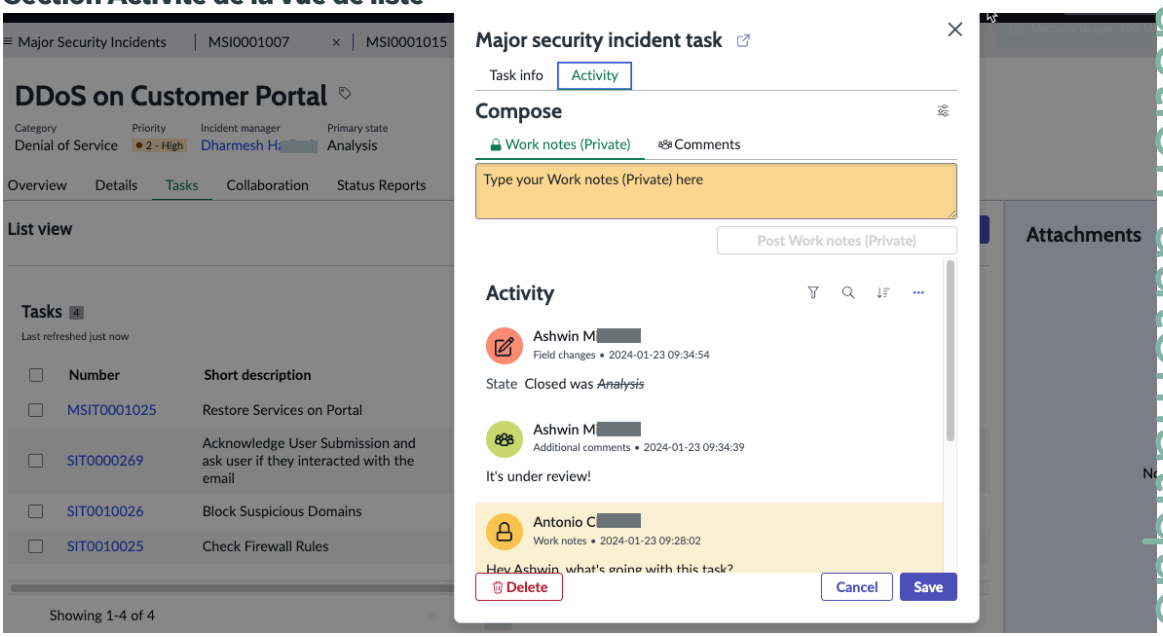
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Groupe d'affectation	Sélectionnez un groupe d'affectation de l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Affecté à	Sélectionnez l'utilisateur auquel affecter la tâche à l'aide de l'option de recherche.
Actifs affectés	Sélectionnez les actifs affectés par la tâche à l'aide de l'option de recherche.
Utilisateurs affectés	Sélectionnez les utilisateurs affectés par la tâche à l'aide de l'option de recherche.

7. Sélectionnez la section **Activité** pour afficher les détails de l'activité des répondeurs MSI.

   Utilisez la section Activité pour ajouter vos notes de travail et vos commentaires, et publiez votre activité en privé et ajoutez également des commentaires supplémentaires si nécessaire à l'aide de la section Composer. Enregistrez l'activité après avoir publié vos notes de travail et commentaires pour afficher l'activité ou les notes de travail ajoutées dans la section Activité.

Section Activité de la vue de liste



Remarque : Sélectionnez le lien **Afficher plus** de détails pour afficher les détails d'un enregistrement d'incident de sécurité spécifique, associé à cet incident de sécurité majeur.

8. Sélectionnez **Enregistrer** pour mettre à jour les informations de la tâche.

   Les informations sur la tâche sont mises à jour instantanément.

9. Vous pouvez également effectuer les actions suivantes dans la vue de liste :
   a. Sélectionnez l'icône **Actualiser** pour actualiser la liste des tâches de la vue de liste.
   b. Sélectionnez l'icône **Paramètres** , puis utilisez l'option **Modifier les colonnes** pour modifier la liste des colonnes qui apparaissent dans la vue de liste. Utilisez l'option **Rétablir les largeurs** pour réinitialiser les largeurs des colonnes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supprimer une tâche à l'aide de la vue de liste

Rôle requis : sn_msi.workspace_manager.

Le gestionnaire MSI peut supprimer une tâche de la vue de liste en procédant comme suit :

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Choisissez l'enregistrement d'incident de sécurité majeur requis.
4. Sélectionnez l'onglet **Tâches** .
5. Sélectionnez **la vue de liste**.
6. Choisissez une tâche que vous souhaitez supprimer de la liste.
7. Dans la fenêtre contextuelle de la tâche d'incident de sécurité majeur, sélectionnez l'option **Supprimer** .

   La fenêtre contextuelle Supprimer la tâche s'affiche et vous demande de confirmer la suppression de la tâche.
8. Sélectionnez **Supprimer**.

Suivre l'activité de collaboration via l'espace MSIM de travail

Suivez les activités de messagerie instantanée et de fichiers liées à la résolution des incidents de sécurité majeurs via l'espace de travail MSIM.

Les activités sont coordonnées à l'aide Microsoft Teams du chat, Microsoft SharePoint des fichiers et des dossiers, puis republiées via les Incident de sécurité majeur intégrations.

Une fois Microsoft Teams que Microsoft SharePoint sont intégrés Gestion des incidents de sécurité majeursà , vous pouvez utiliser l'espace de travail pour suivre la collaboration entre les MSIM utilisateurs de la réponse aux incidents et d'autres groupes qui contribuent à la résolution d'un incident de sécurité majeur. Toutes les mises à jour des dossiers et des fichiers de collaboration sont Microsoft SharePoint synchronisées avec l'espace de MSIM travail File Explorer et également reflétées dans les composants du flux d'activité.

Lorsqu'un incident de sécurité est promu en incident de sécurité majeur :

1. Une structure de dossiers sera créée en Microsoft SharePoint fonction de la configuration du modèle de dossier. La même structure de dossiers sera reflétée sur le composant de l'espace File Explorer de travail.
2. Une équipe avec plusieurs canaux est créée sous Microsoft Teams l'application et cela se reflète dans le composant Gestion de la messagerie instantanée de l'espace de travail.

Rôle requis : sn_msi.workspace_manager.

Interagissez avec des fichiers et des dossiers

L'explorateur de fichiers affiche le système de fichiers afin que vous puissiez afficher et interagir avec les fichiers et dossiers liés à la résolution de l'incident.

Affiche le fichier et les dossiers capturés dans Microsoft SharePoint pour un incident de sécurité spécifique. Ces dossiers seront automatiquement créés sur Microsoft SharePoint pour cet incident de sécurité majeur. Vous pouvez utiliser ces dossiers créés par défaut pour charger les fichiers de support, si nécessaire. Vous pouvez renommer, déplacer ou supprimer ces fichiers et dossiers selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En outre, chaque fois que vous chargez un fichier dans l'un des dossiers, l'activité correspondant à ces dossiers est automatiquement associée aux dossiers de l'explorateur de fichiers dans l'onglet Collaboration et l'activité est enregistrée et affichée dans la section Activité de l'espace de travail Major Security Incident Management.

Remarque : Dans l'onglet **Collaboration** , l'enregistrement d'incident est ajouté au fichier parent sur SharePoint avec un numéro d'incident et une catégorie d'incident uniques.

1. **Vue Référentiel** : répertorie les fichiers et dossiers répertoriés dans Microsoft SharePoint pour cet incident de sécurité spécifique. Pour chaque fichier ou dossier, la vue du référentiel affiche le nom, Modifié par, Dernière modification et la taille seront affichées.

Vue Référentiel

Champ	Description
Ouvrir dans SharePoint	Sélectionnez cette option disponible en regard de votre incident de sécurité majeur. Cliquez sur le lien pour sélectionner et afficher la structure des dossiers dans Microsoft SharePoint.
Nouveau dossier	Sélectionnez cette option pour créer un dossier selon vos besoins. Après avoir créé un nouveau dossier, le même nouveau dossier est créé et associé dans votre Microsoft SharePoint, par défaut.

2. **Récents** : affiche tous les journaux d'activité récents. Ces journaux incluent à la fois vos activités SharePoint et d'exploration de fichiers. Les activités récentes sont généralement vos fichiers de support qui incluent le dossier parent.

   Voici la procédure pour **localiser le fichier journal :**

   a. Sélectionnez le fichier respectif pour afficher les détails.

   b. Cliquez sur **Localiser le fichier**.

   Remarque : La navigation et les détails du fichier parent et des dossiers parents sont affichés dans la section Vue de liste **Récents** . Vous pouvez ouvrir le même fichier dans votre SharePoint. Chaque fois que vous chargez les fichiers journaux connexes ou des activités, tous ces fichiers et activités sont affichés à la fois dans SharePoint et dans l'explorateur de fichiers.

Gérer les communications des canaux de messagerie instantanée à l'aide de Microsoft Teams

Le gestionnaire de canaux de messagerie instantanée affiche Microsoft Teams avec plusieurs canaux créés dans l'application Microsoft Teams en fonction d'une configuration de modèle de configuration.

Ces canaux configurés sont reflétés dans le composant Gestion de la messagerie instantanée ainsi que les utilisateurs et les groupes d'utilisateurs qui leur sont affectés. Le gestionnaire de canal de messagerie instantanée vous permet d'effectuer les actions suivantes :

- **Gérer les canaux de messagerie instantanée**
- **Renommer l'équipe**
- **Gérer les membres de votre équipe**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’équipe et les canaux sont créés en fonction de la configuration du canal de messagerie instantanée dans Microsoft Teams.

Gérer les canaux de messagerie instantanée

Le gestionnaire de canaux de messagerie instantanée vous permet de créer, modifier ou supprimer des canaux de messagerie instantanée. Pour gérer un canal de messagerie instantanée dans Microsoft Teams, procédez comme suit :

1. Sélectionnez l’onglet **Collaboration** .
2. Accédez à la **Gestionnaire de canal de messagerie instantanée** > **Créer un canal**.
3. Ajoutez un nouveau **nom de canal**, une **nouvelle description** et sélectionnez les **membres** du canal.
4. Sélectionnez **Créer**.

   Remarque : Un nouvel enregistrement de canal est créé dans la section Canaux Microsoft Teams de l’application Microsoft Teams et le même enregistrement est reflété dans MSIM.

5. Pour modifier un canal de messagerie instantanée, sélectionnez-le dans la liste Gestionnaire de canaux de messagerie instantanée.
6. Vous pouvez modifier le nom du canal, la liste des membres ou la liste des membres du groupe en fonction de vos besoins.
7. Sélectionnez **Enregistrer**.
8. Pour supprimer un canal de messagerie instantanée, sélectionnez-le dans la liste des gestionnaires de canaux de messagerie.
9. Sélectionnez **Supprimer un canal**.

Renommer l'équipe

Pour renommer une équipe dans Microsoft Teams, procédez comme suit :

1. Sélectionnez l’onglet **Collaboration** .
2. Accédez à la **Gestionnaire de canal de messagerie instantanée** > **Renommer l'équipe**.
3. Dans le champ Nom de l’équipe, renommez l’équipe en fonction de vos besoins.
4. Sélectionnez **Enregistrer**.

   Remarque : Renommer le nom de l’équipe renomme également le nom de l’équipe dans Microsoft Teams.

Gérer les membres de votre équipe

Le gestionnaire de canal de messagerie instantanée vous permet d’ajouter ou de supprimer des membres de l’équipe dans Microsoft Teams. Vous pouvez également ajouter des membres par le biais de groupes. Pour gérer les membres de l’équipe dans Microsoft Teams, procédez comme suit :

1. Sélectionnez l’onglet **Collaboration** .
2. Accédez à la **Gestionnaire de canal de messagerie instantanée** > **Gérer les membres de votre équipe**.
3. Dans le champ Membres, ajoutez ou supprimez des membres de l’équipe en fonction de vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans le champ Ajouter des membres via des groupes, sélectionnez les groupes que vous souhaitez ajouter dans Microsoft Teams.

   Remarque : Si les membres du groupe font déjà partie de l'équipe, ils ne seront pas ajoutés.

5. Sélectionnez **Enregistrer**.

   Le gestionnaire de canal de messagerie instantanée affiche les détails du nombre total de membres de l'équipe et le nombre de nouveaux membres qui seront ajoutés.

Gérer les communications des canaux de messagerie instantanée à l'aide de Slack

Le gestionnaire de canaux de messagerie instantanée affiche Slack avec plusieurs canaux créés dans l'application Slack en fonction d'une configuration de modèle de configuration.

Ces canaux configurés sont reflétés dans le composant Gestion de la messagerie instantanée ainsi que les utilisateurs et les groupes d'utilisateurs qui leur sont affectés. Le gestionnaire de canaux de messagerie instantanée vous permet de **gérer les canaux de messagerie instantanée**. L'équipe et les canaux sont créés en fonction de la configuration du canal de messagerie instantanée dans Slack.

Gérer les canaux de messagerie instantanée

Le gestionnaire de canaux de messagerie instantanée vous permet de créer, modifier ou supprimer des canaux de messagerie instantanée dans Slack. Pour gérer un canal de messagerie instantanée, procédez comme suit :

1. Sélectionnez l'onglet **Collaboration** .
2. Accédez à la **Gestionnaire de canal de messagerie instantanée** > **Créer un canal**.
3. Ajoutez un nouveau **nom de canal**, une **nouvelle description** et sélectionnez les **membres** du canal.
4. Sélectionnez **Créer**.

   Remarque : Un nouvel enregistrement de canal est créé dans la section Canaux Slack de l'application Slack et le même enregistrement est reflété dans MSIM.

5. Pour modifier un canal de messagerie instantanée, sélectionnez-le dans la liste Gestionnaire de canaux de messagerie instantanée.
6. Vous pouvez modifier le nom du canal, la liste des membres ou la liste des membres du groupe en fonction de vos besoins.
7. Sélectionnez **Enregistrer**.
8. Pour supprimer un canal de messagerie instantanée, sélectionnez-le dans la liste des gestionnaires de canaux de messagerie.
9. Sélectionnez **Supprimer un canal**.

Gérer les conversations sur le flux d'activité

Affiche l'ensemble des activités, des journaux, des statuts qui ont été effectués le , l'explorateur Microsoft SharePoint de fichiers et Microsoft Teams.

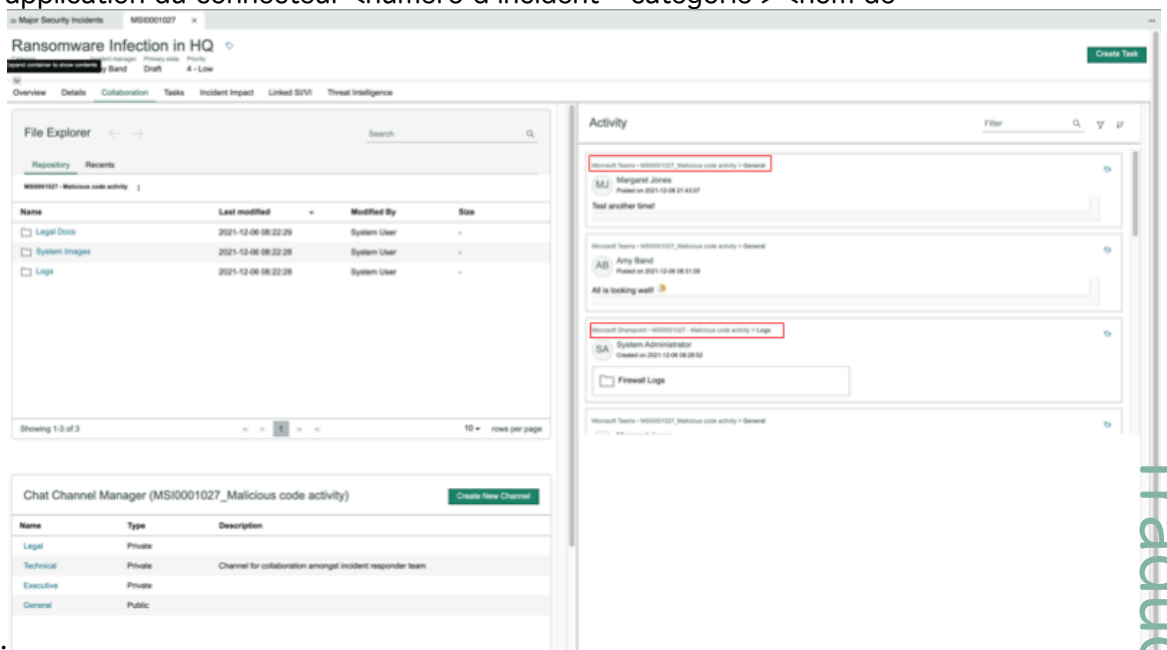
Si vous souhaitez afficher une activité spécifique ou rechercher les détails de l'activité de collaboration qui ont été interagies entre différents fichiers et dossiers, ainsi que sur Microsoft Teams, vous pouvez utiliser l'option de filtre qui s'affiche en haut à droite de la section Flux d'activité et localiser les détails de l'activité souhaitée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

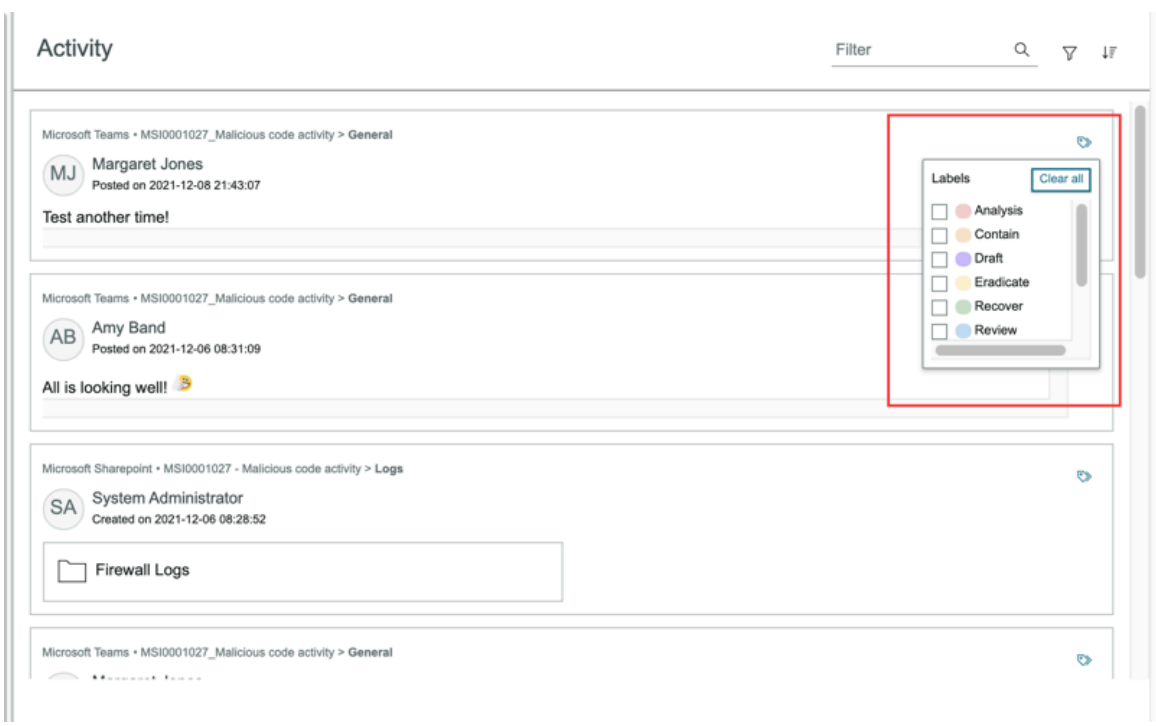
Les dossiers et les conversations de messagerie instantanée partagés avec Major Security Incident Management se reflètent sous forme de fils d'Ariane avec la structure :

Nom de l'application du connecteur <numéro d'incident – catégorie > <nom de dossier>).



Étiquetez les activités :

1. Cliquez sur l'icône **Étiquette** .
2. Cochez la case de l'étiquette d'activité d'incident correspondante, comme indiqué dans la capture d'écran ci-dessous.



3. Les activités étiquetées sont codées par couleurs et représentées sous forme de graphique de tendance de progression dans la section **Collaboration externe** de l'espace de travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer et distribuer des rapports d'état MSIM

Incident de sécurité majeur En tant que gestionnaire, vous pouvez créer et distribuer les différents rapports d'état à différentes personnes concernées à différents intervalles en fonction du modèle de rapport configuré ou d'un rapport d'état précédent tout au long de la résolution de l'incident de sécurité majeur.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Vous pouvez prévisualiser les éléments de données du rapport de synthèse précédemment configurés, ajouter du texte ou un résumé supplémentaire, supprimer des composants de rapport individuels si nécessaire et vérifier l'exactitude et l'exhaustivité du rapport avant de le distribuer à différentes personnes concernées.

Créez des rapports d'état en sélectionnant le modèle de rapport initialement configuré sur la page Configuration des modèles de rapport MSI.

Procédure

1. Accédez à la **Espaces de travail** > **Gestion des incidents de sécurité majeurs** > **Incidents de sécurité majeurs**.
2. Sélectionnez la vue **Listes** .
3. Sélectionnez l'enregistrement MSI promu respectif.
4. Sélectionnez l'onglet **Rapports d'état** .
   L'onglet Rapports d'état contient trois types différents de sous-sections, comme ci-dessous.

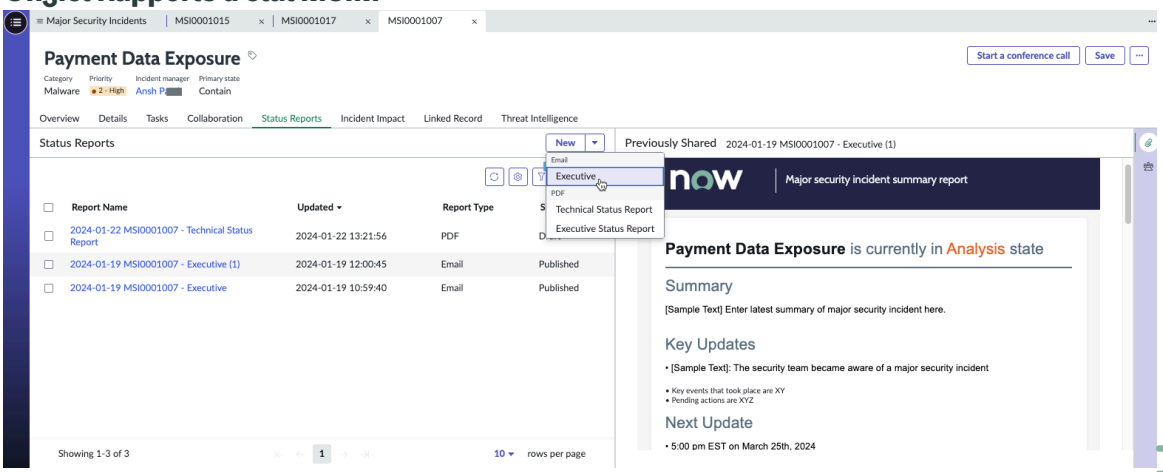
Champ	Description
Nom du rapport	Nom du modèle de rapport d'état. **Remarque :** La vue Rapports d'état répertorie les modèles de rapports prédéfinis existants qui sont disponibles dans le cadre du système de base pour le profil concerné. Par exemple, les rapports d'état de la direction par e-mail (adaptés aux mobiles), les rapports d'état technique et les rapports d'état de la direction au format PDF.
Mis à jour	Date à laquelle le modèle de rapport a été mis à jour pour la dernière fois.
Type de rapport	Type de rapport d'état. Le rapport d'état peut avoir l'un des types suivants : ○ PDF ○ E-mail
État	État des rapports d'état. Les rapports d'état peuvent être dans l'un des états suivants : ○ Brouillon ○ Mis en file d'attente ○ Publié

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez le type de rapport d'état que vous souhaitez afficher ou sélectionnez **Nouveau** pour créer un rapport d'état.

Onglet Rapports d'état MSIM



6. Choisissez l'un des types de rapports d'état suivants dans la liste.
   - **Exécutif** Envoyez des rapports d'état par e-mail adaptés aux mobiles.
   - **Rapport d'état technique** PDF
   - **Rapport d'état de la direction** PDF

   Remarque : Lorsque vous sélectionnez le modèle de rapport souhaité, l'aperçu du rapport sélectionné est immédiatement généré dans le volet droit. Vous pouvez afficher le rapport d'état sélectionné du MSI.

7. Dans le modèle de rapport d'état d'e-mail de la direction, remplissez les sections avec les détails du rapport d'état.

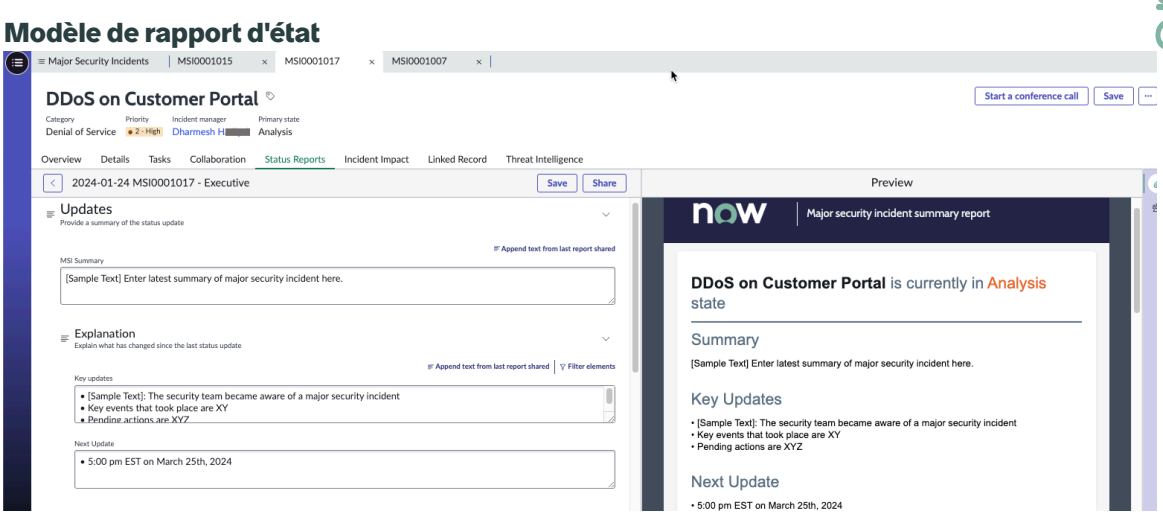
Section de rapport	Description
Mises à jour	Fournir un résumé de la mise à jour de l'état. Cette section contient les éléments suivants : ○ **Résumé MSI** : fournissez un bref résumé de l'incident de sécurité majeur. ○ **Ajouter le texte du dernier rapport partagé** : sélectionnez cette option pour ajouter le texte du dernier rapport partagé.
Explication	Ajoutez une explication sur ce qui a changé depuis la dernière mise à jour de statut. Cette section contient les éléments suivants : ○ **Mises à jour clés** : fournissez des mises à jour clés telles que ce que l'équipe de sécurité doit savoir sur l'incident de sécurité majeur, nommez les événements clés qui ont eu lieu et répertoriez toutes les actions en attente. ○ **Mise à jour suivante** : indiquez la date et l'heure de la prochaine mise à jour pour résoudre l'incident de sécurité majeur. Par exemple, à 17h00 HNE le 25 mars 2024.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Section de rapport	Description
	○ **Ajouter le texte du dernier rapport partagé** : sélectionnez cette option pour ajouter le texte du dernier rapport partagé. ○ **Éléments de filtre** : sélectionnez les éléments de rapport à inclure dans le rapport. Par exemple, Mises à jour clés ou Mises à jour suivantes.
Information supplémentaire	Fournissez des détails spécifiques pertinents pour la mise à jour de statut.
Visualisations	Sélectionnez les visualisations qui aident le mieux à communiquer la mise à jour de statut. ○ **Impact de l'incident** : sélectionnez les mesures d'impact de l'incident telles que les actifs affectés, l'emplacement affecté, les utilisateurs affectés qui sont liées à la mise à jour du statut. ○ **Éléments de filtre** : sélectionnez les éléments de rapport à inclure dans le rapport. Par exemple, Impact de l'incident.
Listes	Sélectionnez les listes d'enregistrements qui fournissent un contexte à la mise à jour du statut. ○ **Enregistrements liés** : sélectionnez les enregistrements liés à la mise à jour de l'état de l'incident de sécurité majeur. Par exemple, Incident de sécurité lié. ○ **Éléments de filtre** : sélectionnez les éléments de rapport à inclure dans le rapport. Par exemple, Enregistrements liés.

Remarque : Les options que vous avez sélectionnées dans la section Rapports d'état sont les mêmes que celles affichées dans l'aperçu du rapport.



8. Sélectionnez **Enregistrer** pour enregistrer les mises à jour que vous avez apportées au rapport d'état.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Sélectionnez **Partager** pour partager le rapport d'état avec des personnes concernées internes et externes.
   La boîte de dialogue Partager s'affiche.

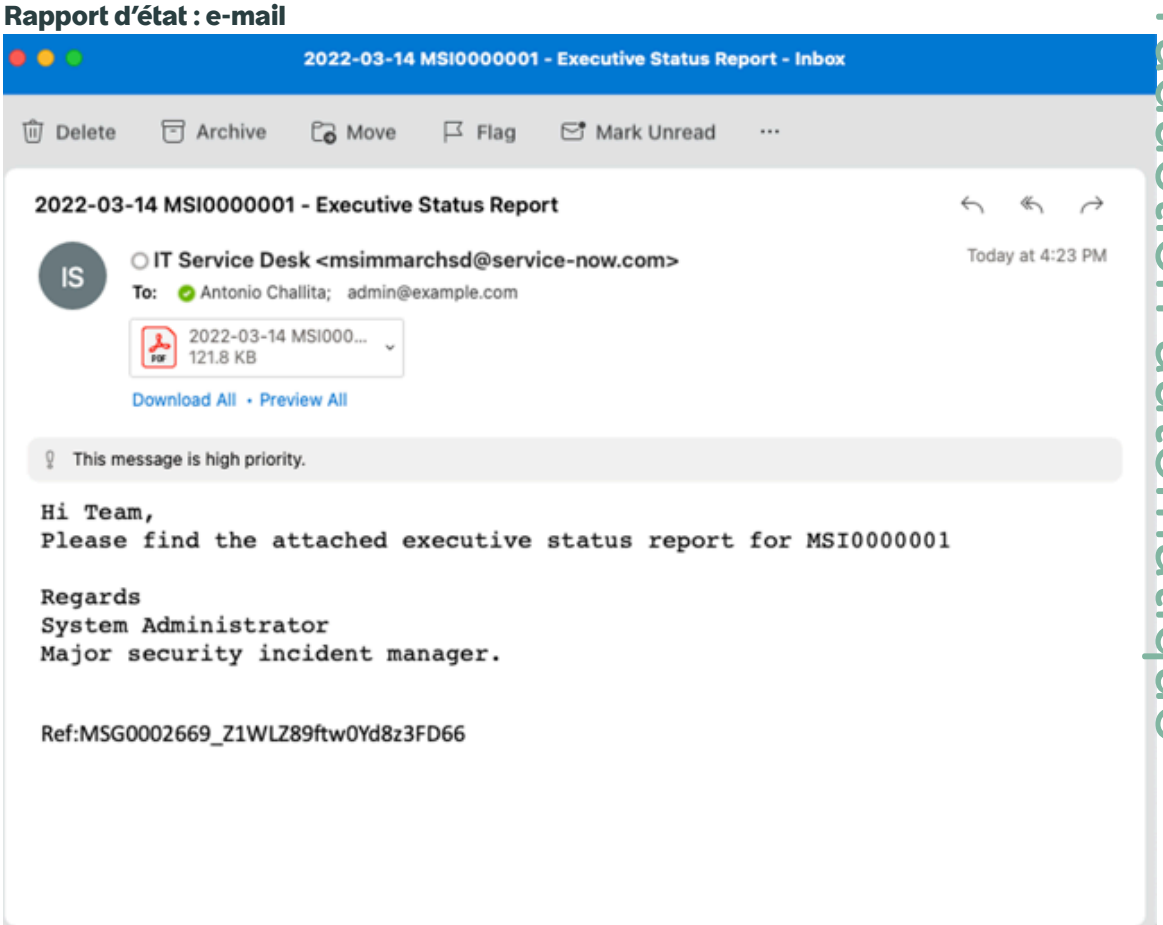
   a. Dans le champ Objet, saisissez l'objet du rapport d'e-mail.

   b. Dans le champ Ajouter des destinataires internes, saisissez et sélectionnez les destinataires du rapport d'e-mail.

   c. Dans le champ Ajouter des destinataires externes, saisissez l'e-mail ou la DL des destinataires pour le rapport d'e-mail.
   Vous pouvez ajouter plusieurs ID d'e-mail à l'aide d'une virgule ou d'un point-virgule.

10. Sélectionnez **Rapport d'e-mail**.
    Un e-mail avec le rapport d'état PDF joint est envoyé avec succès au destinataire concerné pour qu'il le vérifie.

Rapport d'état : e-mail



11. Vous pouvez également effectuer les actions suivantes dans l'onglet Rapports d'état :

    a. Utilisez l'action **Actualiser** de la vue Rapports d'état pour actualiser la liste des rapports d'état.

    b. Utilisez l'action Actions de la **liste** dans la vue Rapports d'état pour modifier des colonnes ou réinitialiser la largeur de la liste des rapports d'état.

    c. Utilisez l'action **Filtrer** de la vue Rapports d'état pour filtrer les rapports d'état en fonction de certaines conditions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Configurer les Incident de sécurité majeur rapports d'état

Gestion des rapports d'état MSIM

Les rapports d'état fournissent des graphiques de tendances préconfigurés avec des visualisations de données exploitables pour améliorer les processus des opérations de sécurité, mesurer et analyser la chronologie de résolution, le nombre de retards et l'état de chaque tâche affectée.

Configurer les Incident de sécurité majeur rapports d'état

Configurez les rapports d'incidents de sécurité majeurs pour configurer et télécharger les rapports en fonction de vos besoins professionnels tout au long du cycle de vie du processus de correction des enregistrements d'incidents de sécurité majeurs.

Vous pouvez créer des modèles de rapport avec un format et une mise en page spécifiques, et personnaliser ces rapports en fonction de vos besoins spécifiques à l'aide de la fonctionnalité Rapports d'état de l'espace Gestion des incidents de sécurité majeurs de travail.

Un utilisateur disposant du rôle sn_msi.workspace_manager peut créer et configurer les modèles de rapport qui décrivent le type d'informations de rapport pouvant être utilisées pour générer tous les rapports d'état. Ils peuvent être partagés avec des utilisateurs spécifiques tels que les personnes concernées de la direction et les services juridiques, et mapper ces modèles aux enregistrements d'incidents de sécurité majeurs.

Pour personnaliser vos rapports d'état MSI, vous devez d'abord configurer les modèles de rapport à l'aide de **modèles de rapport**. À l'aide des modèles de rapport, vous pouvez créer les types de modèles de rapport, définir les composants de rapport pour ces modèles de rapport, ajouter des informations supplémentaires, créer des données visualisées pour suivre le périmètre et les mesures de progression, ajouter des données de liste connexes et générer les rapports d'état.

La section suivante décrit les champs par défaut fournis dans tous les types de modèles de rapports. Vous pouvez configurer et formater le modèle de rapport en fonction de vos besoins à l'aide de sections, de sous-sections et de ses éléments :

Composants de rapport d'état

Type de composant	Description
Titre de rapport	Titre du type de rapport. Par exemple, le format par défaut du type de rapport est : {Numéro MSI} - {Rapport du membre de la direction} représenté par MSI0001001 : Rapport du membre de la direction.
Nom	Affiche le nom de l'utilisateur qui a généré le rapport à l'aide de la section Rapports d'état de l'espace de travail Major Security Incident Management.
Résumé	Affiche un bref résumé du rapport.
Date	Affiche la date à laquelle le rapport est partagé avec le destinataire concerné.
Progression	Affiche les mesures de progression et de champ d'application, telles que les incidents SIR liés, les tâches de réponse, les tâches supplémentaires, la collaboration externe, les composants de chronologie et les événements de chronologie récents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants de rapport d'état (suite)

Type de composant	Description
Défis	Cette section affiche une brève description des défis impliqués tout au long du processus de correction des incidents de sécurité majeurs.
Étapes suivantes	Cette section affiche une brève description des prochaines étapes de la résolution de l'incident de sécurité majeur. Par exemple, la sous-section Équipe active du rapport sur les personnes concernées par la direction vous fournit des informations sur l'étape suivante de l'affectation d'équipe qui est impliquée dans une analyse plus approfondie de l'enregistrement d'incident de sécurité majeur.
Autres personnalisations	Le modèle de rapport vous permet également de charger le logo et de personnaliser les en-têtes et pieds de page du rapport.

Voici les types de catégories de rapport qui peuvent être configurés et affichés :

- **Exécutif** Messagerie électronique
- **Rapport d'état technique** PDF
- **Rapport d'état de la direction** PDF

Les rapports ci-dessus sont configurés et disponibles pour que l'utilisateur puisse sélectionner, afficher et générer le rapport à partir de l'espace de travail Major Security Incident Management.

Adapté aux mobiles Rapports d'état de la direction : e-mail

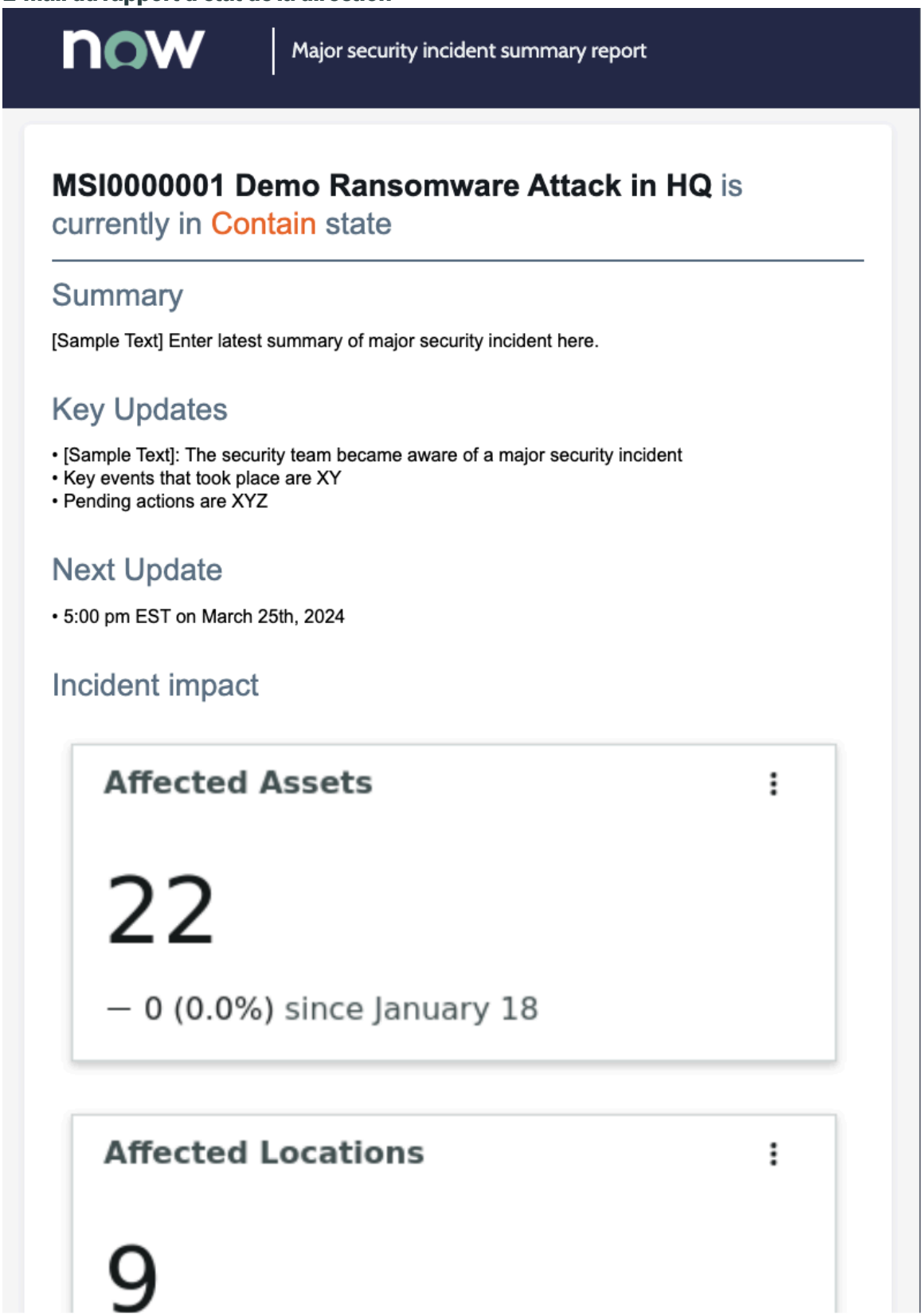
Les rapports d'état exécutifs - e-mail sont des rapports d'état adaptés aux appareils mobiles qui sont générés au format e-mail. La section Rapport comprend un résumé du rapport, la colonne Durée MSI, la portée/l'impact de l'incident, les mesures d'équipe active, les mesures de progression et les composants de chronologie tels que les événements de chronologie récents pour cet enregistrement d'incident de sécurité majeur spécifique.

Personnalisez et configurez les fonctionnalités de modèle de rapport suivantes pour ajouter des informations supplémentaires au rapport. Un exemple de rapport d'état d'e-mail de direction est affiché ci-dessous à titre de référence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

E-mail du rapport d'état de la direction



Traduction automatique

Rapports d'état de la direction - PDF

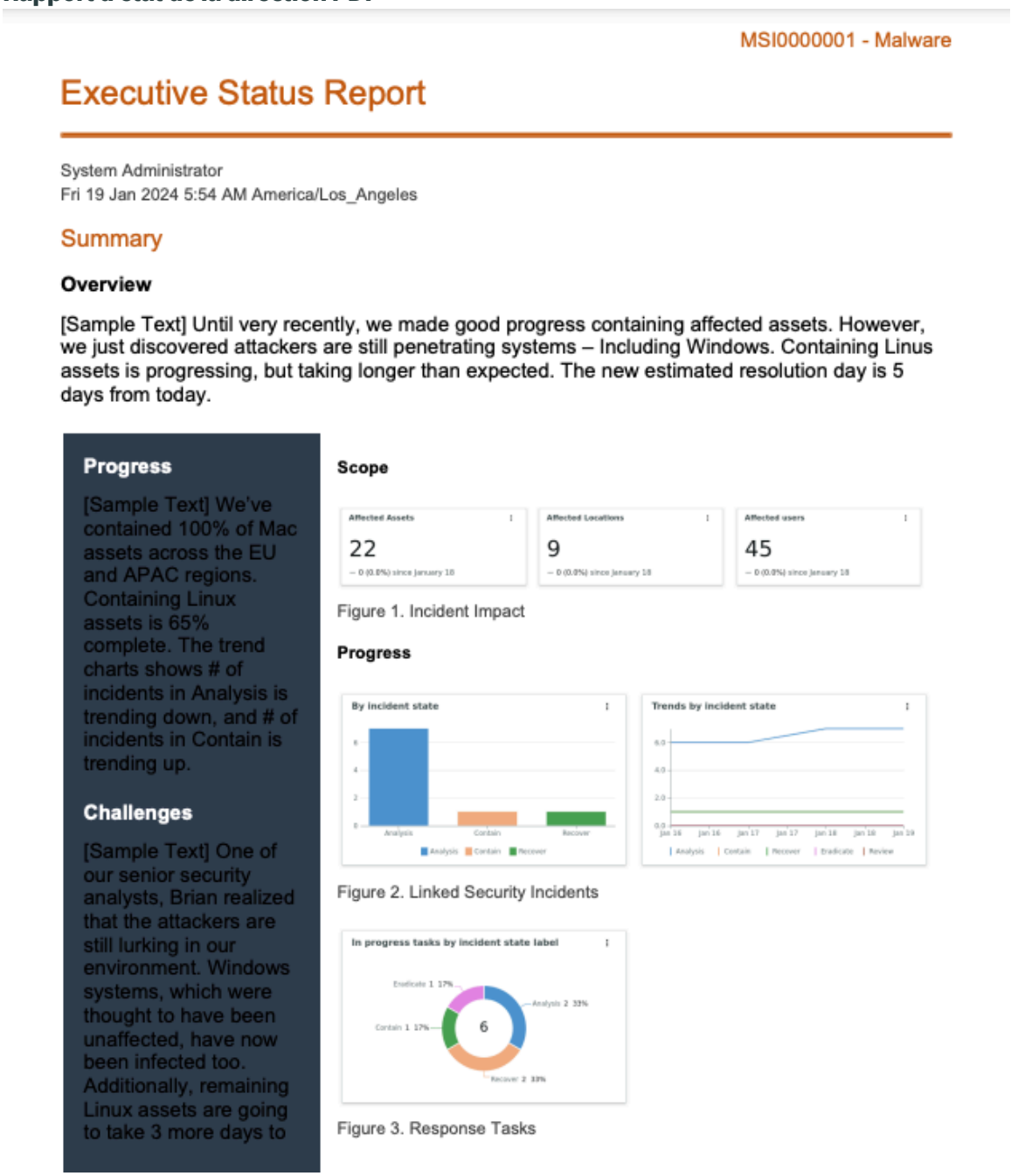
Les rapports d'état exécutifs - PDF sont des rapports d'état qui sont générés au format PDF. La section Rapport comprend un résumé du rapport, la colonne Durée MSI, la portée/ l'impact de l'incident, les mesures d'équipe active, les mesures de progression et les

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

composants de chronologie tels que les événements de chronologie récents pour cet enregistrement d'incident de sécurité majeur spécifique.

Personnalisez et configurez les fonctionnalités de modèle de rapport suivantes pour ajouter des informations supplémentaires au rapport. Un exemple de rapport exécutif est présenté ci-dessous à titre de référence.

Rapport d'état de la direction PDF



MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22 — 0 (0.0%) since January 18
Affected Locations 9 — 0 (0.0%) since January 18
Affected users 45 — 0 (0.0%) since January 18

Figure 1. Incident Impact

Progress

By incident state — Analysis, Contain, Recover
Trends by incident state — Analysis, Contain, Recover, Eradicate, Review

Figure 2. Linked Security Incidents

In progress tasks by incident state label — Eradicate 1 17%, Analysis 2 33%, Contain 1 17%, Recover 2 33%, 6

Figure 3. Response Tasks

Rapports d'état technique - PDF

Les rapports d'état technique - PDF sont des rapports d'état qui sont générés en format PDF. La section Rapport comprend un résumé du rapport, la colonne Durée MSI, le périmètre/l'impact de l'incident, les mesures d'équipe active, les mesures de progression et les composants de chronologie tels que les événements de chronologie récents pour cet enregistrement d'incident de sécurité majeur spécifique, les mises à jour de tâches étiquetées et les activités étiquetées, en fonction du groupe d'affectation et de l'étiquette

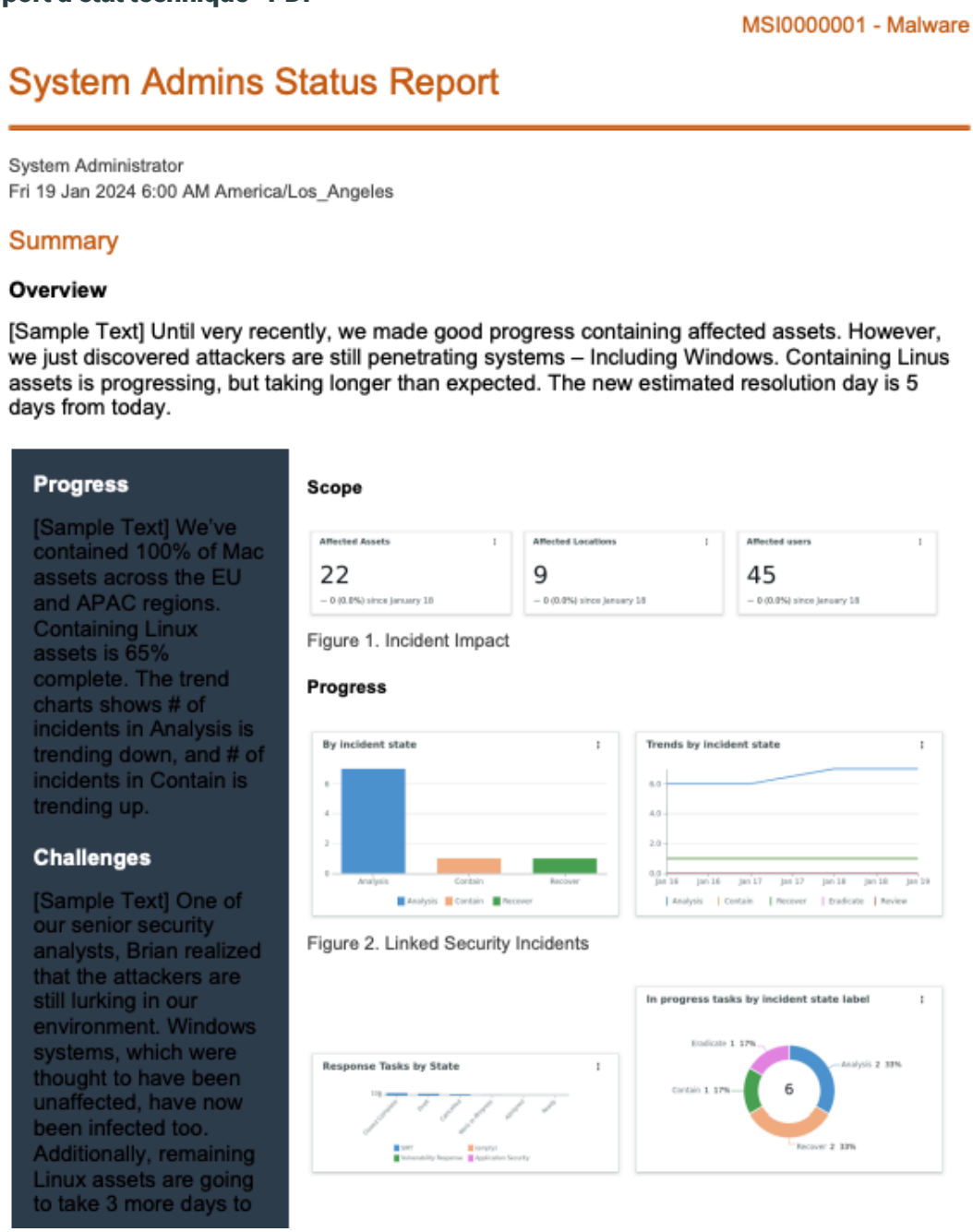
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de balise sélectionnée depuis lors de la génération du dernier rapport d'état, et des informations supplémentaires telles que l'impact de l'incident et les incidents liés.

Personnalisez et configurez le modèle de rapport pour ajouter des informations supplémentaires au rapport. Un exemple de rapport technique qui montre les informations supplémentaires, telles que l'impact de l'incident, est illustré ci-dessous à titre de référence, et la partie restante des informations du rapport est similaire aux rapports exécutifs.

Rapport d'état technique - PDF


MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

Response Tasks by State
In progress tasks by incident state label

Les sections de modèle de rapport contiennent différentes sous-sections qui décrivent comment vous pouvez construire les sous-sections de rapport et leurs éléments, notamment :

1. Marque: Ajouter des marques à vos modèles de rapports
2. Scripts de modèle : Utiliser des scripts de modèle dans vos modèles de rapport

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Utiliser des visualisations dans des modèles de rapport
4. Utiliser des listes de rapports dans des modèles de rapports

Créer un modèle de rapport

Créez différents modèles de rapport qui peuvent être appliqués aux incidents de sécurité majeurs et générez un rapport d'état. Vous pouvez ajouter au modèle de rapport des champs de formulaire standard et personnalisés de réponse aux incidents de sécurité majeurs qui peuvent être remontés pas à pas. En outre, vous pouvez formater et configurer le rapport en fonction de vos besoins à l'aide de sections, de sous-sections et de ses éléments.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche

Vous pouvez définir des composants de rapport à vos modèles de rapport et fournir des informations supplémentaires. Créez des données visualisées pour suivre le périmètre et les mesures de progression, ajouter des données de liste connexe, prévisualiser et générer ou partager les rapports d'état.

Procédure

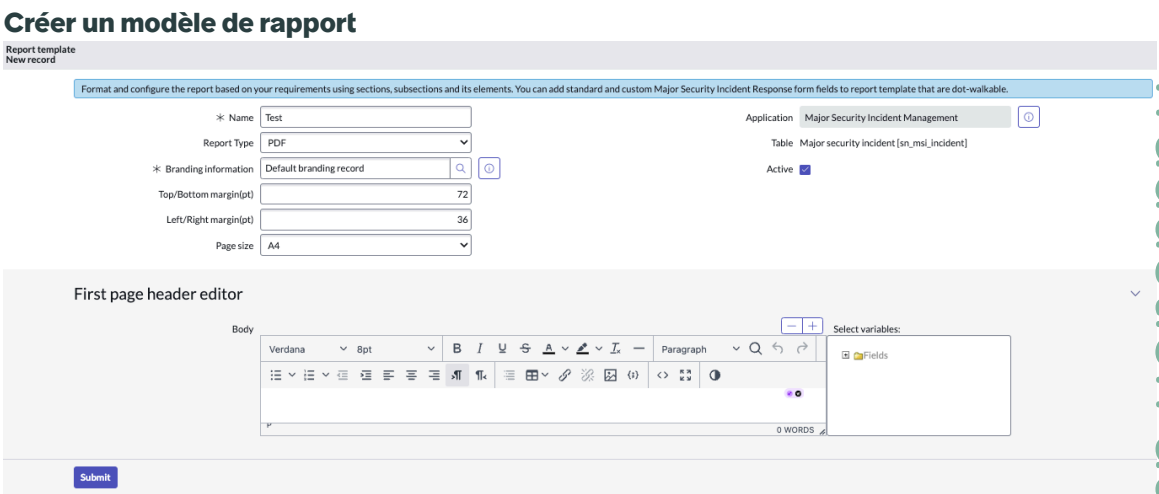
1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Sélectionnez **Nouveau** pour créer un modèle de rapport.
4. Renseignez les champs du formulaire Modèle de rapport.

Champ	Description
Nom	Nom du modèle de rapport.
Information sur la marque	Sélectionnez les informations de marque de votre modèle de rapport, telles que le logo, l'en-tête et le texte de pied de page. Par exemple, Enregistrement de marque par défaut.
Type de rapport	Type de rapport d'état. Le rapport d'état peut avoir l'un des types suivants : ○ PDF ○ E-mail
Table	Nom de la table de modèles de rapport.
Marge supérieure/inférieure	Définissez les indentations de marge supérieure et inférieure requises lors de la génération du rapport.
Marge gauche/droite	Définissez les indentations des marges gauche et droite requises lors de la génération du rapport.
Taille de page	La taille de la page de votre modèle de rapport. Par exemple, la taille par défaut est A4.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Cochez la case pour que le gestionnaire MSI génère un rapport à partir du modèle créé à partir de la section **Modèle de rapports** . **Remarque :** Si la case n'est pas cochée, le gestionnaire MSI ne peut pas créer de rapport pour ce type de modèle de rapport spécifique dans l'espace de travail MSIM.
Éditeur d'en-tête de la première page	Vous permet de définir le corps du modèle. Sélectionnez les variables requises à ajouter à la section de l'éditeur de modèles.



5. **Soumettez** le nouvel enregistrement de modèle de rapport.
   Un nouveau modèle de rapport est créé sous la page Modèles de rapports.

Information associée

Créer et distribuer des rapports d'état MSIM

Ajouter des marques à vos modèles de rapports

Ajoutez des marques à vos rapports. Vous pouvez ajouter une image d'en-tête et de pied de page, ainsi que du texte d'en-tête et de pied de page. Vous pouvez inclure ces informations de marque dans n'importe quel type de modèle de rapport que vous souhaitez créer autre que les deux rapports prédéfinis.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche

Les considérations clés lors de l'ajout de marques à vos modèles de rapports sont les suivantes :

- Chargez l'image d'en-tête et de pied de page et alignez la position de l'image.
- La taille maximale de l'image d'en-tête et de pied de page est de 5 Mo. Si la taille dépasse la limite spécifiée, un message d'erreur « Le format d'image ne peut pas être reconnu » s'affiche dans l'incident de sécurité majeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Ajustez la hauteur de l’image d’en-tête et de pied de page.
- La longueur du texte du pied de page est limitée à 100 caractères.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
2. Explorez jusqu’à **Modèle de rapport** > **Marques**.
3. Sélectionnez **Configurer**.
4. Sélectionnez **Nouveau** pour ajouter une marque à votre modèle de rapport.
5. Renseignez les champs du formulaire Modèle de marque.

Champ	Description
Nom	Nom du modèle de marque.
Image d'en-tête	Ajoutez une image d’en-tête pour le modèle de marques en procédant comme suit : **a.** Sélectionnez **Cliquer pour ajouter**. **b.** Sélectionnez **Choisir un fichier** **c.** Choisissez une image dans votre système et sélectionnez **OK.**
Image de pied de page	Ajoutez une image de pied de page pour le modèle de marques en procédant comme suit : **a.** Sélectionnez **Cliquer pour ajouter**. **b.** Sélectionnez **Choisir un fichier** **c.** Choisissez une image dans votre système et sélectionnez **OK.**
Position de l'image d'en-tête	Sélectionnez une position d’image d’en-tête pour le modèle de marque. Vous pouvez choisir **Gauche**, **Centre** ou **Droite**.
Position de l'image de pied de page	Sélectionnez une position d’image d’en-tête pour le modèle de marque. Vous pouvez choisir **En haut à gauche**, **En haut au centre**, **En haut à droite**, **En bas à gauche**, **En bas au centre** ou **En bas à droite**.
Hauteur de l'image d'en-tête	Fournissez une valeur de hauteur (en pt) pour l’image d’en-tête du modèle de marque.
Hauteur de l'image de pied de page	Fournissez une valeur de hauteur (en pt) pour l’image de pied de page du modèle de marque.
Texte de pied de page	Fournissez un texte de pied de page pour le modèle de marque. Vous pouvez inclure des informations de classification ou de confidentialité. Par exemple, cet e-mail est classifié comme confidentiel, interne uniquement ou protégé par le secret professionnel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Position du texte de pied de page	Sélectionnez une position de texte de pied de page pour le modèle de marque. Vous pouvez choisir **En haut à gauche**, **En haut au centre**, **En haut à droite**, **En bas à gauche**, **En bas au centre** ou **En bas à droite**.

6. Sélectionnez **Soumettre**.
   Un nouveau modèle de marques est créé sous la page Modèles de marques.

Utiliser des visualisations dans des modèles de rapport

Utilisez les widgets de rapports pour définir et inclure des éléments UIB (User Interface Builder) tels que des visualisations de données dans les rapports d'état MSIM.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Tous** > **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Explorez jusqu'à **Modèle de rapport** > **Visualisations**.
3. Sélectionnez **Configurer**.
   Voici les visualisations UIB prédéfinies dans le cadre du système de base, que vous pouvez utiliser pour configurer et modifier vos rapports d'état.

Nom du widget	Description
Équipe active	Affiche la liste des équipes actives impliquées dans la résolution du MSI.
Actifs affectés	Affiche la liste des actifs affectés.
Emplacements affectés	Affiche la liste des emplacements affectés.
Utilisateurs affectés	Affiche la liste des utilisateurs affectés.
Graphique à secteurs pour collaboration	Inclut les activités de collaboration dans le graphique à secteurs.
Graphique de tendance de collaboration	Affiche les activités de collaboration sous la forme d'un graphique de tendances.
Date de résolution estimée	Affiche la date de résolution estimée à laquelle la MSI est estimée résolue.
Graphique à barres pour les incidents liés	Affiche le graphique à barres des incidents liés.
Graphique de tendance des incidents liés	Affiche le graphique de tendance des incidents liés.
Graphique à barres pour tâches de réponse MSI	Affiche le graphique des tâches de réponse MSI.
Graphique à barres pour tâches de réponse	Affiche le graphique à barres des tâches de réponse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du widget	Description
Tâches de réponse en cours par étiquettes	Affiche les tâches de réponse en cours par étiquettes.
Tâches de réponse en retard	Affiche le nombre total de tâches de réponse dont la fermeture est en retard.
Graphique de tendance des tâches de réponse	Affiche le graphique de tendance des tâches de réponse.
Temps écoulé depuis la détection de l'incident	Affiche le temps écoulé depuis le moment où l'incident est détecté.
Chronologie	Affiche la chronologie des événements clés et des jalons qui se sont produits dans le cadre de l'incident de sécurité majeur.

Information associée

Créer un élément de type visualisation

Utiliser des listes de rapports dans des modèles de rapports

Utilisez les listes de rapports pour définir et inclure les artefacts de liste connexes afin de générer des listes au format PDF en fonction de vos enregistrements de liste MSI configurés.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Explorez jusqu'à **Modèle de rapport** > **Listes**.
3. Sélectionnez **Configurer**.
   La section Listes de rapports d'état MSI décrit la façon dont chaque liste connexe spécifique est affectée depuis la création de l'incident. Voici les listes de rapports MSI prédéfinies dans le cadre du système de base que vous pouvez utiliser pour configurer et modifier vos rapports d'état.

Listes de rapports MSI	Description
Actifs affectés	La liste connexe des actifs affectés affichée dans le rapport d'état.
Emplacements affectés	La liste connexe des emplacements affectés afficher dans le rapport d'état.
Utilisateurs affectés	La liste connexe des utilisateurs affectés s'affiche dans le rapport d'état.
Indicateurs	La liste connexe des indicateurs affichés dans le rapport d'état.
Incident de sécurité lié	La liste connexe des incidents de sécurité liés afficher dans le rapport d'état.
Observables	La liste connexe des observables vue dans le rapport d'état.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Créer un élément de type liste

Utiliser des scripts de modèle dans vos modèles de rapport

Créez un script pour inclure les données des listes connexes, les opérations de date et toutes les autres données qui ne sont pas directement accessibles par une remontée pas à pas.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser ce script de modèle prédéfini dans vos modèles de rapport pour inclure toutes les données connexes une fois les modèles de rapport configurés et personnalisés.

Construisez un script de modèle pour afficher les données de la liste connexe sur le modèle de rapport. Si vous souhaitez utiliser et remplir n'importe quel script de modèle, vous devez ajouter la balise de script de modèle de balise en tant que : `${template_script :nom du script}`.

Exemple : `${template_script :msi_collab_cards}`

Remarque : Vous ne pouvez pas supprimer les scripts de modèle prédéfinis. Un message d'erreur s'affiche si un utilisateur disposant d'un rôle administrateur tente de supprimer un enregistrement de script de modèle s'il est mappé à un modèle de rapport.

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Explorez jusqu'à **Modèle de rapport** > **Scripts de modèle**.
3. Sélectionnez **Configurer**.
   Voici les scripts de modèle prédéfinis dans le cadre du système de base que vous pouvez utiliser pour configurer et modifier vos rapports d'état.

Nom du script du modèle	Description
formatted_current_date	Renvoie la date et l'heure locales actuelles au format JJMMAAA, 00,00 AM ou p.m. Par exemple, 21 janv. 2021 15:51 PST.
msi_active_team	Générer du code HTML pour les cartes d'équipe actives.
msi_collab_cards	Générer du code HTML pour les cartes d'activité de collaboration.
msi_task_activities	Générer du code HTML pour les cartes de tâches.
msi_timeline_events	Générer du code HTML pour les cartes d'événements de chronologie.
si_affected_users	Renvoie les utilisateurs affectés de la liste connexe sous forme de tableau.
si_assessments	Renvoie les résultats de l'évaluation post-incident sous forme de tableau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du script du modèle	Description
si_associated_phish_emails	Renvoie les e-mails d'hameçonnage associés de la liste connexe sous forme de tableau.
si_associated_phish_headers	Renvoie les en-têtes d'hameçonnage associés de la liste connexe sous forme de tableau.
si_business_criticality	Renvoie une valeur de criticité opérationnelle codée par couleur.
si_malicious_observables	Renvoie les observables malveillants de la liste connexe sous forme de tableau.
si_observables	Renvoie les observables de la liste connexe sous forme de tableau.
si_priority	Renvoie une valeur de priorité codée par couleur.
si_response_tasks	Renvoie les tâches de réponse de la liste connexe sous forme de tableau.
si_time_to_identify	Renvoie la durée passée à l'état Brouillon et Analyse.
si_time_to_resolve	Renvoie le délai de résolution de l'incident.

Remarque : Vous pouvez également créer votre propre script de modèle pour inclure les données des listes connexes, les opérations de date et toutes les autres données qui ne sont pas directement accessibles par une remontée pas à pas, en plus des scripts de modèle répertoriés.

Afficher un aperçu du modèle de rapport

Utilisez la fonctionnalité Aperçu pour prévisualiser votre modèle de rapport au moment de la conception afin de générer et de partager le rapport avec d'autres personnes concernées pendant l'exécution à partir de l'espace de Gestion des incidents de sécurité majeurs travail.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Sélectionnez le modèle de rapport souhaité.
4. Sélectionnez le type de rapport **e-mail** ou **PDF** en fonction de vos besoins.
5. Sélectionnez l'action **Enregistrer et prévisualiser le rapport** .

   La boîte de dialogue Afficher un aperçu du rapport s'affiche.
6. Sélectionnez un incident de sécurité majeur à l'aide de l'option de recherche pour prévisualiser un rapport avec le modèle sélectionné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Sélectionnez **Afficher un aperçu du rapport**.
   Le rapport génère un aperçu en fonction de la configuration de modèle sélectionnée. Si vous avez sélectionné le type de rapport **E-mail**, l'aperçu est au format de modèle d'e-mail. Les rapports d'état au format e-mail sont adaptés aux mobiles.

Créer un modèle de section de rapport

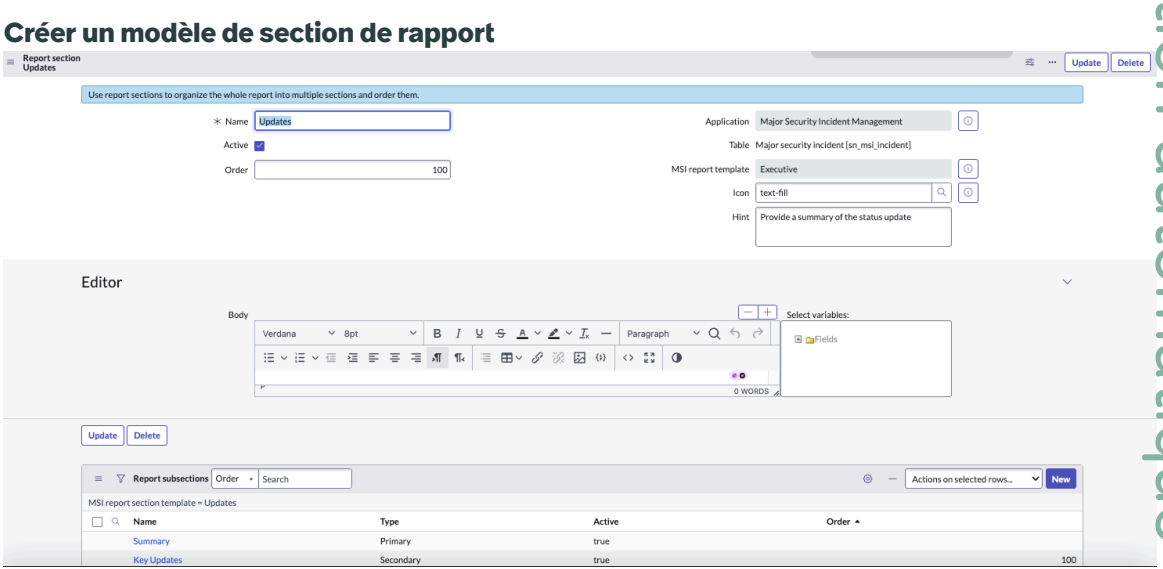
Un rapport peut ensuite être divisé en différentes sections. Utilisez la section Rapport pour décomposer le rapport en plusieurs sections et les réorganiser dans l'ordre.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant.
4. Accédez à la **Sections de rapport** > **Nouveau**.
   La nouvelle page de section de rapport s'affiche.



5. Renseignez les champs du formulaire Modèle de section de rapport.

Champ	Description
Nom	Nom de la section de modèle de rapport. Par exemple, Résumé.
Table	Nom de la table de modèles de rapport.
Actif	Cochez cette case pour créer une section de rapport pour le modèle sélectionné dans l'espace de travail MSIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si la case n'est pas cochée, le gestionnaire MSI ne peut pas créer de section de rapport pour ce modèle dans l'espace de travail MSIM.
Modèle de rapport MSI	Nom du modèle de rapport MSI pour lequel le rapport est divisé en sections.
Ordre	Ordre dans lequel les sections de rapport sont affichées.
Icône	Utilisez l'icône pour afficher les icônes système dans le rapport.
Conseil	Utilisez le texte de conseil pour guider la création du rapport. Dans le rapport, le texte de conseil s'affiche sous le titre de la section.
Éditeur : Body	Définissez le corps de la section du modèle. Vous pouvez définir le corps de la section en sélectionnant les jetons personnalisés ou les variables dans l'éditeur.

6. **Enregistrez et soumettez** la nouvelle section de modèle de rapport.

Créer un modèle de sous-section de rapport

Utilisez la sous-section Rapport pour organiser davantage la section en plusieurs sous-sections et configurer leur alignement et leur position à l'aide des types disponibles tels que Panneau latéral de texte, Primaire et Secondaire.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

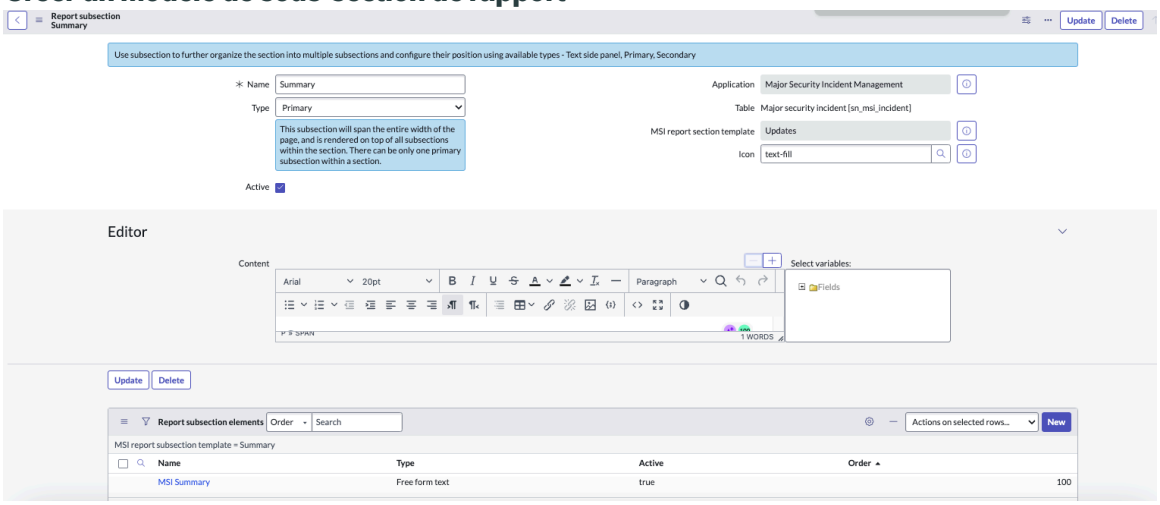
Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport respective.
4. Dans la liste des sections de rapport, ouvrez un modèle de section de rapport existant.
5. Accédez à la **Sous-sections de rapport** > **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un modèle de sous-section de rapport



6. Renseignez les champs du formulaire Sous-section de rapport.

Champ	Description
Nom	Nom de la sous-section de modèle de rapport. Par exemple, Périmètre. **Remarque :** Les sous-sections existantes pour les rapports prédéfinis sont : Vue d'ensemble, Portée, Progression, Explication. ○ **Vue d'ensemble** : affiche la vue d'ensemble sous forme de sous-section dans le rapport. ○ **Champ d'application** : affiche les éléments de visualisation dans le rapport, tels que les compteurs de durée, l'impact de l'incident, les équipes actives et la tendance des équipes actives. ○ **Progression** : affiche les éléments de visualisation du rapport, tels que les graphiques des incidents de sé–curité liés, le graphique des tâches de réponse et les graphiques de collaboration.
Type	Le type de sous-section de rapport. Les types dispo-nibles sont les suivants : ○ **Primaire** : cette sous-section couvre toute la largeur de la page et s'affiche en haut de toutes les sous-sections de la section. Il ne peut y avoir qu'une seule sous-section primaire dans une section. ○ **Secondaire** : cette sous-section couvre toute la largeur de la page, sauf si elle

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	est utilisée avec le panneau latéral de texte. ○ **Panneau latéral de texte** : cette sous-section accompagne le panneau secon–daire et ne prend en charge que le texte.
Table	Nom de la table de modèles de rapport.
Modèle de section de rapport MSI	Nom du modèle de rapport MSI pour lequel vous divisez le rapport en sections.
Ordre	Ordre dans lequel les sous-sections de rapport seront rendues.
Icône	Utilisez l'icône pour indiquer ou mettre en surbrillance le conteneur de sections sur le formulaire de configuration de l'exécution du rapport.
Actif	Cochez cette case pour créer une sous-section de rapport pour le modèle sélectionné dans l'espace de travail MSIM. **Remarque :** Si la case n'est pas cochée, le gestionnaire MSI ne peut pas créer de sous-section de rapport pour ce modèle dans l'espace de travail MSIM.
Éditeur : contenu	Définissez le contenu de la sous-section de modèle.

7. **Enregistrez et soumettez** la nouvelle section de modèle de rapport.

Créer un modèle d'élément de sous-section de rapport

Utilisez des éléments de sous-section pour organiser davantage une sous-section en plusieurs éléments. Les éléments de sous-section permettent de définir des visualisations, des listes et du texte de forme libre de manière plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

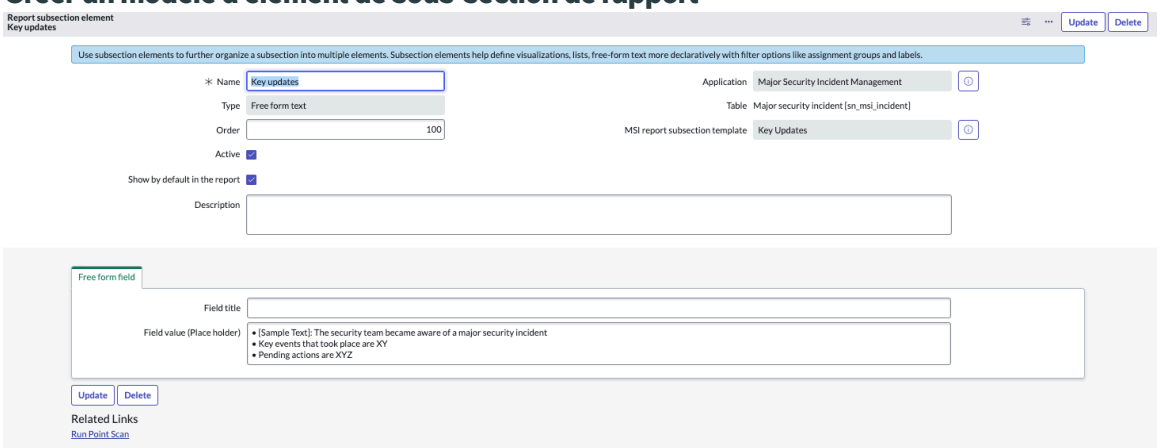
Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport respective.
4. Dans la liste des sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un modèle d'élément de sous-section de rapport



7. Renseignez les champs du formulaire Éléments de sous-section de rapport.

Champ	Description
Nom	Nom de l'élément de sous-section de modèle de rapport. Par exemple, Périmètre. **Remarque :** Les sous-sections existantes pour les rapports prédéfinis sont les suivantes : Compteurs de durée, Impact de l'incident, Équipe active, Tendance d'équipe active. ○ **Compteurs de durée** : affiche le compteur de durée sous la forme d'un élément de sous-section, tel que le temps estimé pour résoudre l'incident dans le rapport d'état. ○ **Impact de l'incident** : affiche les éléments de visualisation dans le rapport, tels que les actifs impactés, les emplacements impactés et les utilisateurs impactés. ○ **Équipe active** : affiche les éléments de visualisation dans le rapport, tels que le nombre d'équipes actives impliquées dans la fermeture de l'incident de sécurité majeur. ○ **Tendance de l'équipe active :** Représente la tendance des équipes actives dans une représentation graphique.
Type	Type d'élément de sous-section de rapport. Les types disponibles sont les suivants : ○ Texte de formulaire libre ○ Visualisation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Personnalisé ○ Liste
Table	Nom de la table de modèles de rapport.
Actif	Cochez cette case pour créer une section de rapport pour le modèle sélectionné dans l'espace de travail MSIM. **Remarque :** Si la case n'est pas cochée, le gestionnaire MSI ne peut pas créer de section de rapport pour ce modèle dans l'espace de travail MSIM.
Afficher par défaut dans le rapport	Cochez cette case si vous souhaitez inclure la section dans le rapport pour afficher rapidement les éléments.
Modèle de rapport MSI	Nom du modèle de rapport MSI pour lequel vous divisez le rapport en sections.
Ordre	Ordre dans lequel les sections de rapport sont affichées.
Description	Décrivez le type d'élément de sous-section.

8. **Enregistrez et mettez à jour** la section du nouveau modèle de rapport.

Créer un élément de type de formulaire libre

Créez un type d'élément de formulaire libre pour définir le texte du formulaire libre de manière plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport respective.
4. Dans la liste des sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.
7. Remplissez le formulaire Éléments de sous-section de rapport avec les détails requis, comme expliqué dans .Créer un modèle d'élément de sous-section de rapport
8. Accédez au champ Type d'élément de sous-section de rapport, puis sélectionnez l'option du **champ Formulaire libre** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La section **Champ de formulaire libre** s'affiche.

9. Renseignez les champs de l'onglet Formulaire libre.

Champ	Description
Titre de champ	Nom du titre du champ. Par exemple, Vue d'ensemble.
Valeur du champ (espace réservé)	Saisissez la description de la valeur du champ. Par exemple, voici un exemple de texte de présentation. Nous avons bien progressé dans la maîtrise des actifs affectés. Cependant, nous venons de découvrir que les attaquants continuent de pénétrer dans les systèmes, y compris Windows. Le conteneur des actifs Linus progresse, mais prend plus de temps que prévu. Le nouveau jour de résolution estimé est de 5 jours à compter d'aujourd'hui.

Créer un élément de type visualisation

Créez un type d'élément de visualisation pour définir les éléments de visualisation de manière plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport respective.
4. Dans la liste des sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.
7. Remplissez le formulaire Éléments de sous-section de rapport avec les détails requis, comme expliqué dans .Créer un modèle d'élément de sous-section de rapport
8. Accédez au champ Type d'élément de sous-section de rapport et sélectionnez l'option **de visualisation** .
   La section **Visualisation** s'affiche.
9. Renseignez les champs du formulaire Visualisation.

Champ	Description
Légende définie pour les visualisations	Saisissez le nom de la légende de l'ensemble de visualisations. Par exemple, les compteurs de durée.
Visualisations	Sélectionnez le type de visualisations. Par exemple, sélectionnez Temps écoulé depuis la détection de

Traduction automatique

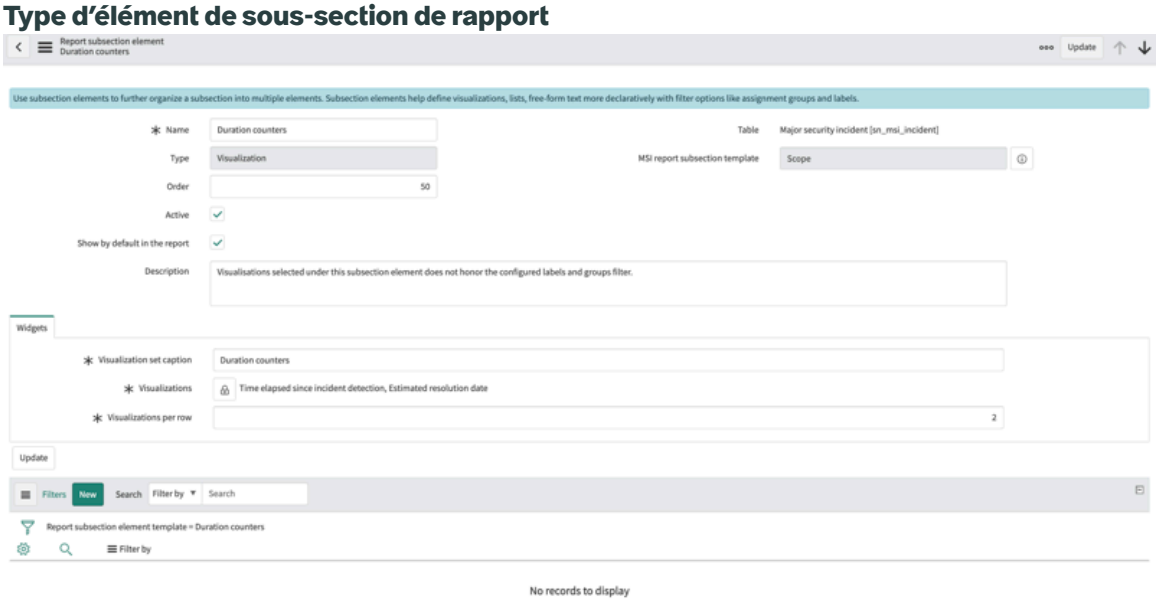
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	l’incident, Date de résolution estimée pour le type de sous-section : Compteurs de durée.
Visualisations par ligne	Sélectionnez le nombre de visualisations affichées en fonction de chaque ligne.

10. Sélectionnez **Soumettre**.

Example: Type d’élément de sous-section de modèle de rapport pour un rapport de statut technique

Type d’élément de sous-section de rapport



Créer un élément de type liste

Créez un élément de type liste, qui définit les éléments de liste connexes de façon plus déclarative avec des options de filtre telles que les groupes d’affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d’état MSI s’affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport respective.
4. Dans la liste des sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.
7. Remplissez le formulaire Éléments de sous-section de rapport avec les détails requis, comme expliqué dans .Créer un modèle d’élément de sous-section de rapport
8. Accédez au champ Type d’élément de sous-section de rapport, puis sélectionnez l’option **Liste** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La section **Listes** s'affiche.

9. Renseignez les champs du formulaire Liste.

Champ	Description
Listes	Nom des listes connexes associées au MSI. Par exemple, Observables, Indicateurs. Sélectionnez une liste à l'aide de l'option de recherche.

Créer un élément de type personnalisé

Créez un élément de type liste, qui définit les éléments de liste connexes de façon plus déclarative avec des options de filtre telles que les groupes d'affectation et les étiquettes.

Avant de commencer

Rôle requis : sn_msi.workspace_manager

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Administration MSI** > **Configuration du rapport d'état**.
   La page de configuration du rapport d'état MSI s'affiche.
2. Dans la section Modèle de rapport, sélectionnez **Configurer**.
3. Ouvrez un modèle de rapport existant et accédez à la liste des sections de rapport respective.
4. Dans la liste des sections de rapport, ouvrez un modèle de section de rapport existant.
5. Dans la liste des modèles de section de rapport, ouvrez un modèle de sous-section de rapport existant.
6. Accédez à la **Éléments de sous-section de rapport** > **Nouveau**.
7. Remplissez le formulaire Éléments de sous-section de rapport avec les détails requis, comme expliqué dans .Créer un modèle d'élément de sous-section de rapport
8. Accédez au champ Type d'élément de sous-section de rapport, puis sélectionnez l'option **Personnalisé** .
   La section **Contenu personnalisé** s'affiche.
9. Renseignez les champs du formulaire Contenu personnalisé.

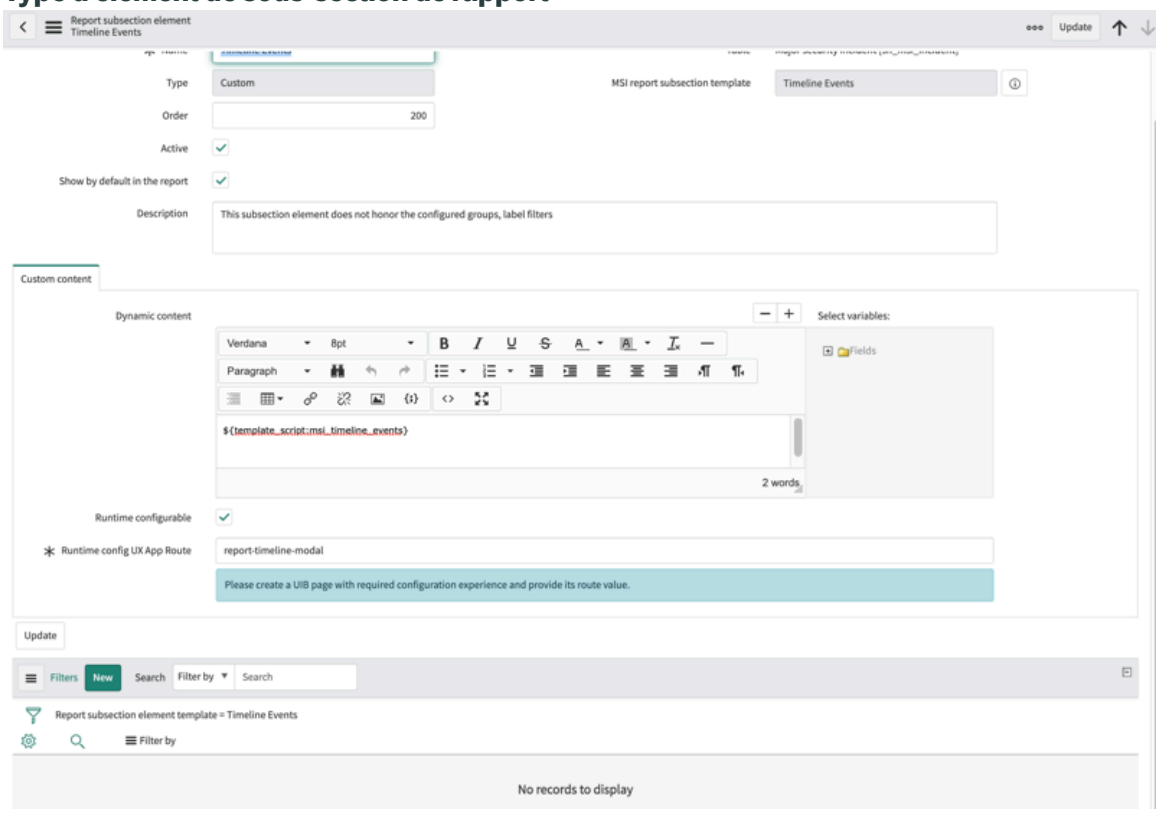
Champ	Description
Contenu dynamique	Saisissez le contenu dynamique tel que les scripts de modèle.
Temps d'exécution configurable	Cochez cette case si le type d'élément personnalisé est configurable au moment de l'exécution.
Configuration de l'exécution pour chemin de l'application UX	Saisissez la valeur Chemin de l'application UX de configuration d'exécution lorsqu'une page UIB est créée avec l'expérience de configuration requise. **Remarque :** Ce champ s'affiche uniquement lorsque l'option **Exécution configurable** est sélectionnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example: Voici un exemple de type d’élément de sous-section de modèle de rapport pour un rapport de statut technique

Type d’élément de sous-section de rapport



Ajouter des propriétés système

Ajoutez des propriétés système pour contrôler le comportement de l’application MSIM. Voici les propriétés système par défaut introduites dans le Gestion des incidents de sécurité majeurs cadre des rapports d’état.

Propriétés système

Nom de la propriété	Description
sn_msi.export_img	Utilisez cette propriété pour contrôler l’exportation d’images. La valeur par défaut est ACTIVÉ.
sn_msi.export_img_log	Utilisez cette propriété pour activer la connexion à la console du navigateur. La valeur par défaut est définie sur OFF.
sn_msi.export_img_parallel_threshold	Utilisez cette propriété pour contrôler le nombre maximum de demandes parallèles afin de générer les images à partir des configurations de widget de rapport. La valeur par défaut est définie sur 14.
sn_msi.img_export_log	Utilisez cette propriété pour activer les journaux de la console dans le navigateur.
sn_msi.img_export_poll_interval	Utilisez cette propriété pour contrôler l’écart de temps entre les interrogations qui vérifie si l’image est générée ou non. L’intervalle d’interrogation par défaut est défini sur 3 000 millisecondes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés système (suite)

Nom de la propriété	Description
sn_msi.export_poll_request_timeout	Utilisez cette propriété pour contrôler le temps maximal pendant lequel le système peut interroger l'image exportée. La valeur par défaut est de 120 000 millisecondes.
sn_msi.msi_report_uib_element_js_path	Utilisez cette propriété pour contrôler le chemin d'accès générique pour capturer l'image hors de la portion de page UIB.
sn_msi.report_default_style_objects	Utilisez cette propriété pour modifier le CSS des fichiers PDF générés, tel que la taille de la police, la couleur de police ou la valeur du champ. Par exemple, si sn_msi.workspace_manager préfère changer la couleur de la police du panneau gauche du rapport d'état PDF généré, le gestionnaire de l'espace de travail peut modifier la couleur de police de la propriété système et afficher le PDF dans la vue souhaitée.

Playbooks de gestion des incidents de sécurité majeurs

Vous pouvez invoquer le flux de playbook de Gestion des incidents de sécurité majeurs automatiquement ou manuellement.

Un Playbook n'est visible que si au moins un Playbook est associé à un incident de sécurité. Le composant de playbook n'est pris en charge que pour le concepteur d'automatisation de processus (PAD) créé. Major Security Incident Management fournit le playbook de demande juridique avec le système de base.

Playbook pour les demandes juridiques

Le playbook de demande juridique fournit des conseils étape par étape sur la façon dont vous pouvez informer le service juridique du dernier résumé d'un MSI afin qu'il puisse informer la SEC dans le délai de 4 jours requis pour les violations substantielles.

Vue d'ensemble

En tant que gestionnaire d'incidents, vous pouvez utiliser le Playbook de demande juridique pour informer l'équipe juridique du dernier résumé d'une MSI afin qu'elle puisse notifier la SEC en cas d'infractions importantes. Vous pouvez utiliser les modèles Concepteur d'automatisation de processus (PAD) pour effectuer les étapes du playbook de demande juridique et informer l'équipe juridique en conséquence.

Ce playbook peut être utilisé si un incident de sécurité majeur est créé ou mis à jour. Vous devez activer le playbook de demande juridique sur PAD, puis effectuer toutes les tâches, telles que l'analyse, contenir, éradiquer et examiner.

Les voies de la définition du processus sont les suivantes et correspondent à l'état de l'incident de sécurité majeur :

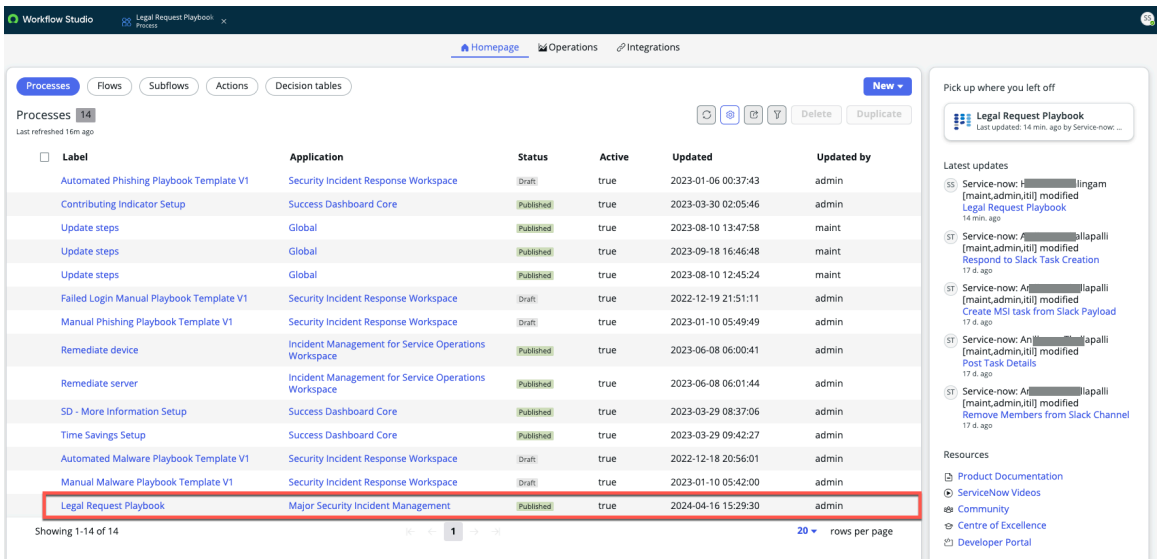
- Analyse
- Contenir
- Éradiquer
- Revue

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chaque voie comporte certaines activités.

Playbook pour les demandes juridiques



Une fois que vous marquez une tâche comme terminée dans une voie, vous pouvez passer à la tâche suivante. Vous pouvez enregistrer une tâche à tout moment et revenir au playbook à une date et une heure ultérieures. Une fois que vous avez terminé toutes les tâches dans une voie, vous pouvez passer à la voie suivante. Le statut est reflété dans le panneau de gauche lorsque vous continuez à accomplir des tâches et des voies. Un journal d'activité sur le côté droit du playbook affiche toutes les données que vous avez saisies pour chaque tâche.

Une fois que vous avez terminé toutes les tâches, vous êtes invité à examiner les détails que vous avez entrés dans toutes les voies. Vous pouvez choisir de modifier n'importe quel champ ou de sélectionner **Terminer** pour terminer le processus de création du droit.

Créer des processus pour le playbook de demande juridique

Suivez ces étapes pour créer des processus pour le playbook de demande juridique dans le Concepteur d'automatisation de processus (PAD).

Avant de commencer

Rôle requis : sn_msi.workspace_manager.

Procédure

1. Cliquer sur **TOUT** > **Concepteur d'automatisation de processus** > > **Créer un nouveau processus**.

   Par exemple, Playbook de demande juridique.

2. Saisissez un nom pour le processus, la description et l'application pour laquelle le processus est créé.
3. Cliquez sur **Sélectionner un déclencheur**.
4. Sélectionnez **Définir vos propres conditions pour le moment où votre processus s'exécute**, puis sélectionnez la condition de déclenchement pour le moment où votre processus doit s'exécuter.
5. Cliquez sur **Définir vos conditions de déclenchement**.
6. Choisissez les conditions pour définir quand votre processus doit s'exécuter en sélectionnant une table et en remplissant les conditions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Accéder à Designer**.
   La page Concepteur d'automatisation de processus s'ouvre.
8. Pour commencer à concevoir votre processus automatisé, cliquez sur **Ajouter une nouvelle voie**.
   Le volet des propriétés de la voie s'ouvre sur le côté droit de l'interface utilisateur.
9. Dans le volet Propriétés de la voie, saisissez les détails suivants : **Nom**, **Description**, **Condition d'exécution** et **Indiquer quand commencer**.
   Les champs **Condition d'exécution** et **Indiquer quand démarrer** impliquent quand la voie doit s'exécuter.
10. Cliquez sur **Enregistrer et fermer**.
11. Pour ajouter une autre voie, cliquez sur **Ajouter une autre voie**.
    De même, vous pouvez créer autant de voies que vous le souhaitez. Dans cet exemple, vous pouvez créer une voie pour Analyser, Contenir, Éradiquer et Examiner respectivement. Dans l'exemple suivant, la voie **d'analyse** démarre immédiatement et n'a aucune condition d'exécution. **Contenir** le début de la voie une fois la voie précédente terminée et a une condition d'exécution basée sur le résultat d'une activité dans la voie précédente.
    Après avoir ajouté les voies, vous devez ajouter des activités de processus pour chaque voie.
12. Cliquez sur **Ajouter une autre activité de processus** sous une voie particulière (par exemple, Voie d'analyse).
    La fenêtre contextuelle Ajouter une activité s'ouvre.
    a. Dans la fenêtre contextuelle Ajouter une activité, sélectionnez la définition d'activité requise.
13. Cliquez sur **Créer une activité**.
    Une fois qu'une définition d'activité est ajoutée, elle peut être configurée de la même manière que les voies. De même, vous pouvez créer d'autres activités de processus sous chaque voie.
14. Dans le volet Propriétés de l'activité, ajoutez une condition d'exécution et indiquez quand démarrer l'activité de processus.
15. Ajoutez une condition d'exécution et indiquez quand commencer.
    Toutes les entrées requises pour cette activité (y compris les entrées configurées dans le plan d'automatisation) seront affichées. Vous pouvez remplacer les valeurs ou utiliser les valeurs préconfigurées.
16. Cliquez sur **Afficher toutes les propriétés** et activez le bouton bascule **Propriétés avancées** pour afficher tous les champs d'expérience d'activité de la définition d'activité.

À l'aide du playbook de demande juridique

Suivez ces étapes pour découvrir comment utiliser le playbook Demande juridique dans l'espace de travail MSIM et ses options.

Avant de commencer

Rôle requis : sn_msi.workspace_manager.

Procédure

1. Dans l'espace de travail MSIM, ouvrez un incident de sécurité majeur.
2. Sélectionnez l'onglet **Playbook**.

   Vous pouvez afficher les playbooks qui ont été activés pour l'incident de sécurité majeur.

   Remarque : Si vous ne voyez pas les playbooks répertoriés, vous devez accéder à PAD et leur permettre de les voir dans l'onglet **Playbook** .

3. Sélectionnez le **Playbook de demande juridique**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur chaque voie pour savoir quelles tâches ont été effectuées par ce playbook.
5. Cliquez sur **Analyse** pour afficher la liste des activités effectuées dans la phase d'analyse.
   Vous avez la possibilité de le modifier selon vos besoins.
6. De même, vous pouvez cliquer sur Contenir, Éradiquer et Examiner pour afficher la liste des activités qui ont été effectuées dans la phase respective.
   Vous avez la possibilité de les modifier selon vos besoins. S'il reste une activité ou une action de l'utilisateur à effectuer, elle s'affiche dans la phase respective.
7. S'il reste une activité ou une action de l'utilisateur requise dans l'une des phases, cliquez sur la phase respective et effectuez l'action pour terminer l'activité.

Cadre de travail de déploiement pour MSIM

Étend la possibilité de lier les enregistrements sources à partir de l'espace de Gestion des incidents de sécurité majeurs travail.

Vue d'ensemble

Le cadre de travail de déploiement rend le flux de déploiement configurable et extensible. Utilisez ce modèle de cadre de travail pour configurer les informations, qui peuvent être déployées jusqu'à un incident de sécurité majeur.

Auparavant, sn_msi.workspace_manager était en mesure de lier les incidents de sécurité et les éléments vulnérables qui étaient proposés ou promus en tant que MSI. Après avoir lié l'incident de sécurité ou l'élément vulnérable, les informations ont ensuite été déployées dans un incident de sécurité majeur. Le type d'informations à déployer était codé en dur dans les scripts.

Vous pouvez utiliser le modèle de cadre de travail pour configurer le flux de déploiement, qui prend en charge les fonctionnalités suivantes et résout également les problèmes existants dans l'application :

Le modèle de cadre de travail de déploiement permet à sn_msi.workspace_manager avec les avantages suivants :

- Ajoutez ou supprimez les options de liaison, de proposition ou de promotion MSI d'enregistrement sur n'importe quelle table, ce qui étend la table de tâches.
- Contrôlez le type d'informations à déployer MSI lors de l'exécution d'actions telles que lier/proposer/promouvoir sur les enregistrements d'incidents.
- Prise en charge de la liaison, de la proposition ou de la promotion d'incidents de sécurité, de tâches de rattrapage et de tickets de sécurité prêts à l'emploi (OOTB) à partir de l'environnement classique et Gestion des incidents de sécurité majeurs de l'espace de travail.

Le cadre de travail de déploiement présente les configurations comme expliqué dans le tableau suivant.

Configurations de cadre de travail de déploiement

Nom	Description
Configuration d'enregistrement lié	Stocke les informations des tables de tâches qui peuvent être utilisées pour lier/promouvoir/proposer à Incident de sécurité majeur.
Configuration d'enregistrement de déploiement	Capture les informations qui peuvent être déployées à partir de la table de tâches lorsque des actions de liaison/promouvoir/proposer sont effectuées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurations de cadre de travail de déploiement (suite)

Nom	Description
Configuration de la mise en page de liste	Contrôle les étiquettes et la mise en page des listes de différentes tables, comme indiqué dans les onglets de l'espace de travail tels que Impact de l'incident Gestion des incidents de sécurité majeurs , Enregistrements liés et Renseignements sur les menaces.

Configurer les enregistrements liés dans Gestion des incidents de sécurité majeurs

Utilisez la configuration des enregistrements liés pour stocker les informations des tables de tâches qui peuvent être utilisées pour lier/promouvoir/proposer à Incident de sécurité majeur.

Rôle requis : admin et sn_msi.workspace_admin.

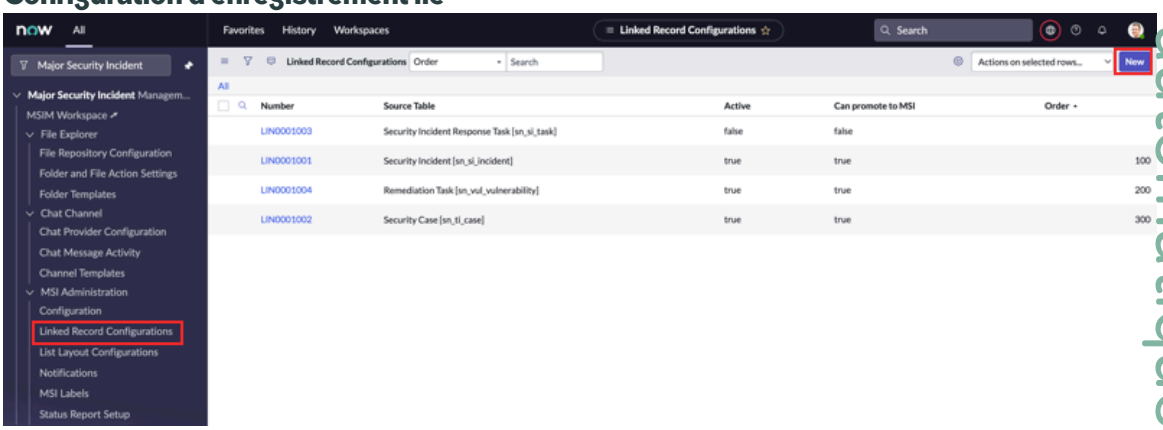
Remarque : L'administrateur peut créer l'enregistrement et MSIM l'administrateur de l'espace de travail peut le mettre à jour.

Procédure

1. Accédez à la **Gestion des incidents de sécurité majeurs** > **Configurations d'enregistrements liés**.

   La page Configuration d'enregistrement lié s'affiche.

Configuration d'enregistrement lié

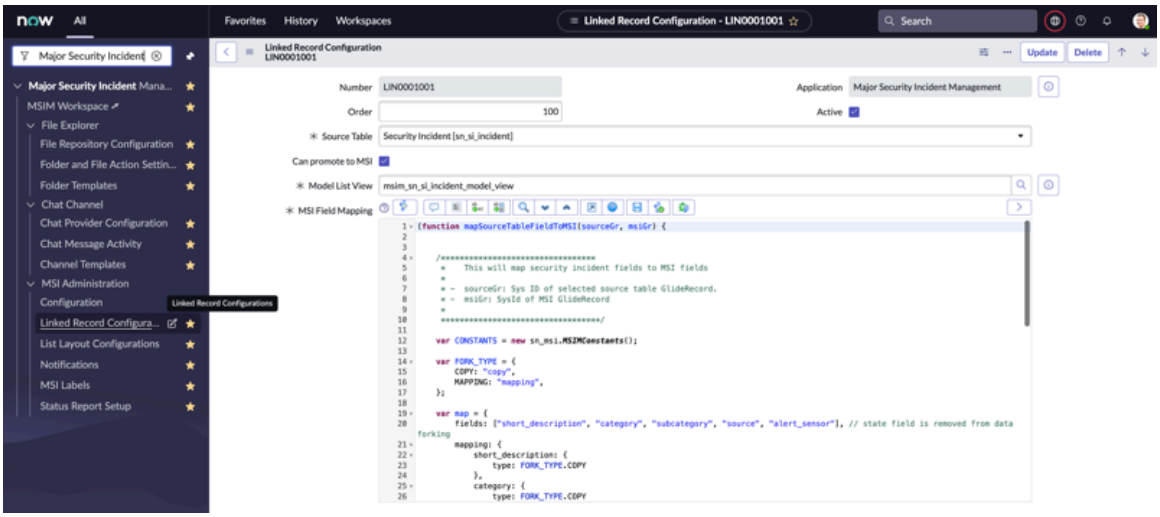


2. Sur la page Configuration d'enregistrement lié, cliquez sur **Nouveau**

Remarque : Assurez-vous que l'application figure dans Gestion des incidents de sécurité majeurs le périmètre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Renseignez les champs du formulaire de configuration de l'enregistrement.

Descriptions des champs d'enregistrements liés

Champ	Description
Table source	Indique la table de tâches qui doit être liée et déployée vers Incident de sécurité majeur.
Ordre	Vous permet de contrôler l'ordre de la table source actuelle dans la liste déroulante de l'espace de travail MSIM. Vous trouverez ci-dessous un exemple **d'ordre**. Reportez-vous à l'image 1 ci-dessous, qui est fournie après ce tableau.
ListView du modèle	Sélectionnez une vue qui peut contrôler la mise en page de la liste affichée dans la liste modale d'enregistrement lié.
Peut promouvoir à MSI	Cochez cette case pour confirmer s'il s'agit d'un enregistrement primaire. Vous trouverez ci-dessous un exemple de sélection **d'option Peut être promu en MSI** . Reportez-vous à l'image 2 suivante, qui est fournie après ce tableau. Si cette case est cochée et que la valeur est vraie, alors : ○ Vous pouvez directement proposer et promouvoir un enregistrement source à l'aide des actions d'environnement Incident de sécurité majeur classique avec des configurations supplémentaires. ○ Vous pouvez lier les enregistrements sources aux incidents de sécurité majeurs à partir de l'environnement classique et MSIM de l'espace de travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Gestion des incidents de sécurité majeurs La page d'enregistrement lié de l'espace de travail affiche les enregistrements de la table source liée. **Remarque :** Si un enregistrement peut être directement proposé/promu en tant que Incident de sécurité majeur, alors cet enregistrement est un enregistrement primaire. Par exemple, dans la configuration de la table Tâche Security Response, la valeur **Peut promouvoir en MSI est définie sur Faux** car vous ne pouvez pas promouvoir directement la tâche Security Response en Incident de sécurité majeur. Par conséquent, il ne s'affiche pas dans la liste déroulante de l'onglet d'enregistrement lié de l'espace MSIM de travail.
MSI Mappage de champs	Écrivez un script pour mapper les champs d'enregistrement source à un incident de sécurité majeur nouvellement créé lorsque l'enregistrement des tables sources est en cours de proposition ou de promotion. Ce script s'exécute uniquement lorsque la valeur **Peut convertir en MSI** est définie sur vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Image 1 : ordre de vue de liste des enregistrements liés

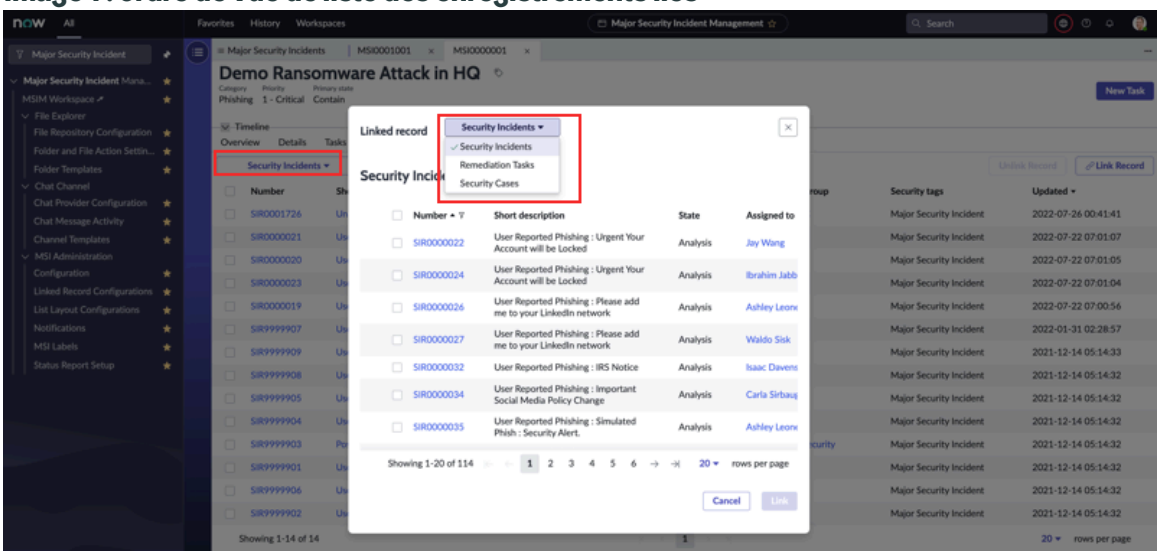
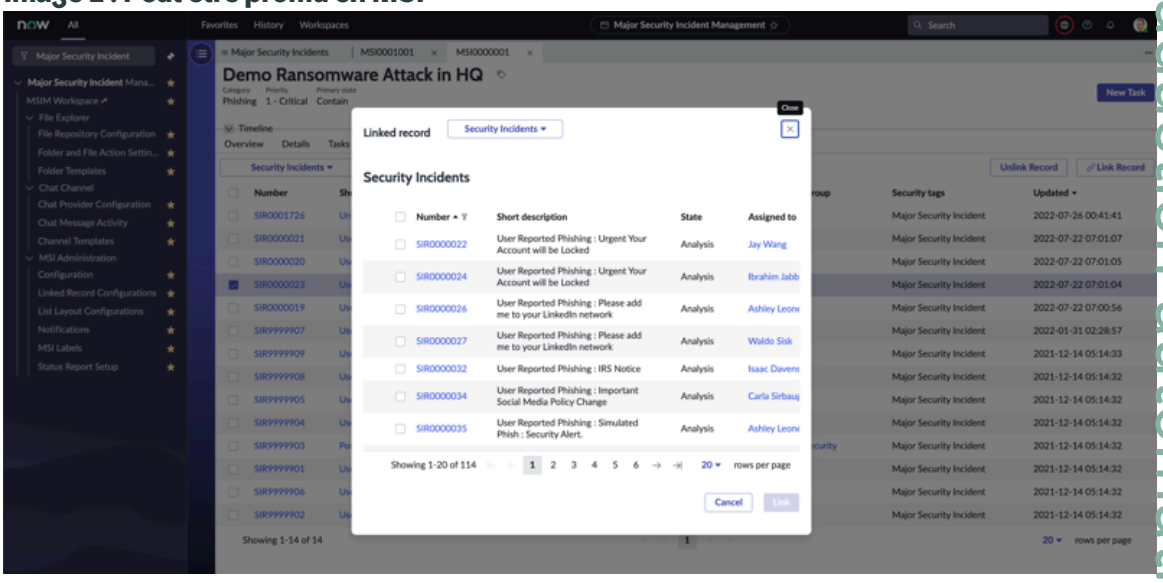


Image 2 : Peut être promu en MSI



Traduction automatique

Configurer les enregistrements de déploiement dans Gestion des incidents de sécurité majeurs

Configurez l'entrée pour reprendre les enregistrements afin Gestion des incidents de sécurité majeurs de contrôler les informations, qui sont déployées lorsque l'enregistrement source est lié/proposé/promu en tant qu'incidents de sécurité majeurs.

Rôle requis : admin et sn_msi.workspace_admin.

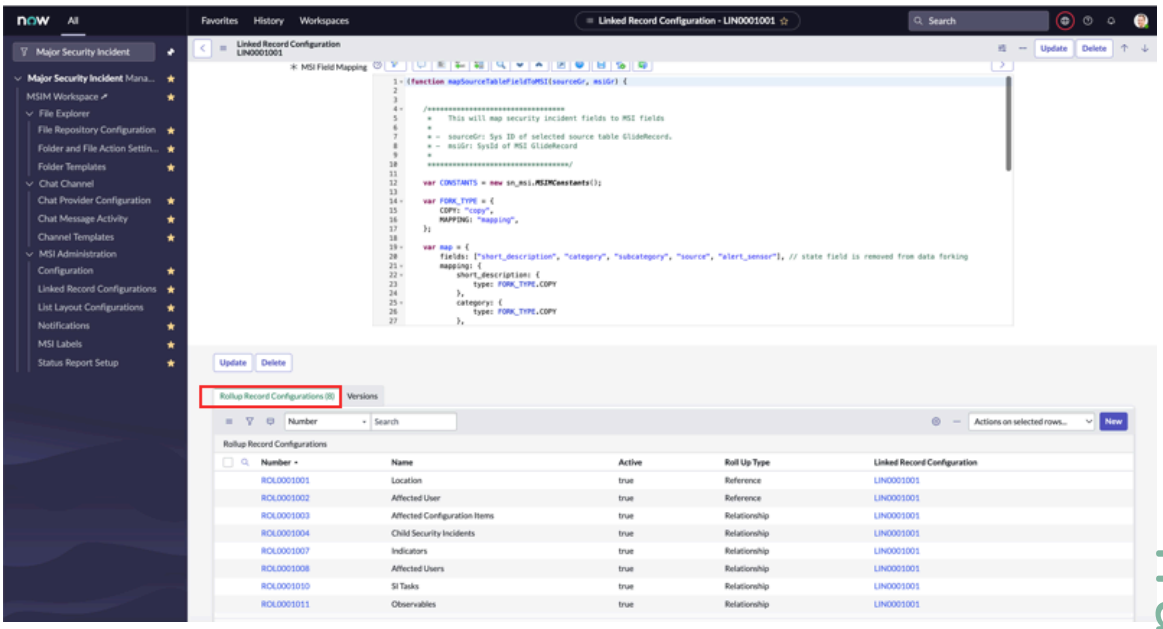
Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.

Procédure

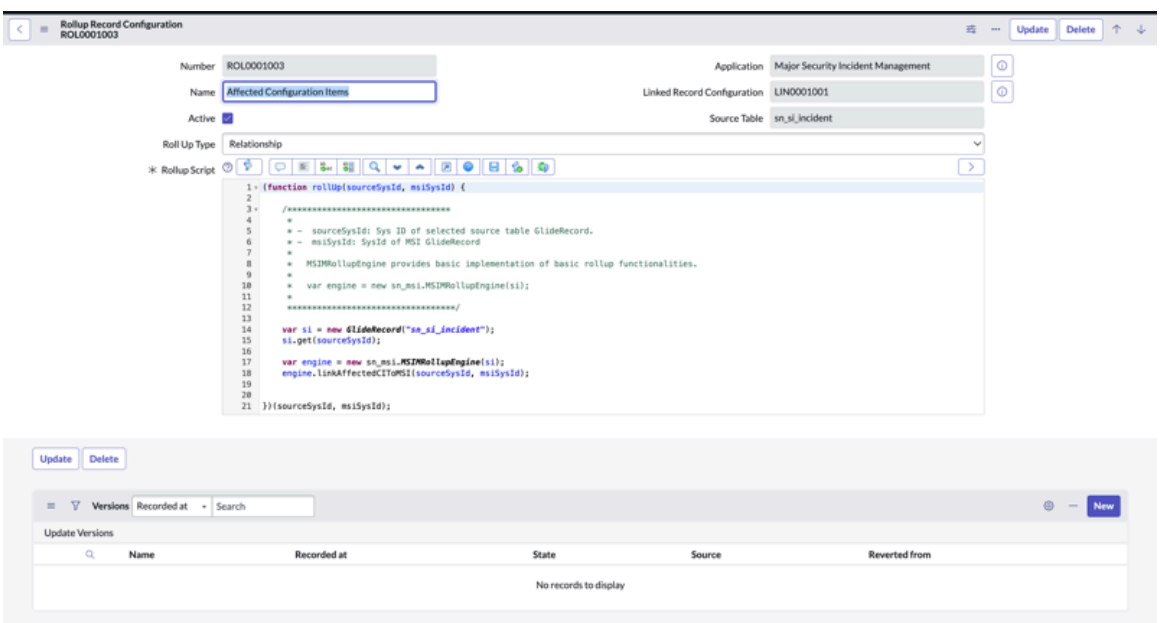
1. Accédez à la **Réponse aux incidents de sécurité majeurs** > **Configuration d'enregistrements liés**. La page Configurations d'enregistrements liés s'affiche.
2. Sélectionnez ou créez un nouvel enregistrement lié et accédez à la section **Configuration de déploiement d'enregistrement** à partir de la même page.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Section Configuration d'enregistrement de déploiement



3. Cliquez sur **Nouveau**.



4. Sur la page de configuration, renseignez les détails.

Configuration d'enregistrement de déploiement

Nom de champ	Description de champ
Nom	Indique le nom de l'enregistrement de déploiement.
Actif	Cochez cette case pour implémenter la configuration actuelle lors du déploiement de l'enregistrement source.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description de champ
Configuration d'enregistrement lié	Indique un numéro unique, qui fait référence à la configuration de vos enregistrements parents liés et en lecture seule.
Table source	Nom de la table source utilisée dans la configuration d'enregistrement lié, qui est en lecture seule.
Type de déploiement	Décrit le type d'informations qui doivent être déployées. ○ **Relation** : sélectionnez cette option si les données doivent être présentes en tant que liste connexe. ○ **Référence** : sélectionnez cette option si les données sont présentes en tant que champ de référence sur le formulaire de la table source.
Script de déploiement	Si le type de déploiement est : **Relation**, le champ **Script de déploiement** est activé, ce qui vous permet d'écrire un script et peut être utilisé pour déployer des informations. Ici, le script reçoit les entrées qui contiennent des informations sur l'enregistrement source et l'incident de sécurité majeur. Le script doit être en mesure de trouver les informations à partir des tables de relations et les déployer dans la table Enregistrement lié (sn_msi_m2m_child).
Champ source	Si le type de déploiement est : **Référence**, le **champ Source** est disponible. Cela vous permet de sélectionner le champ de référence Table source qui contient les informations à déployer.
Champ cible	Si le type de déploiement est : **Référence**, le **champ Cible** est disponible. Cela vous permet de référencer le champ à partir de la table Enregistrement(sn_msi_m2m_child) lié(s) et stockera les données présentes dans le champ source sélectionné et dans l'enregistrement de la table source.

Écriture d'un script pour le déploiement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

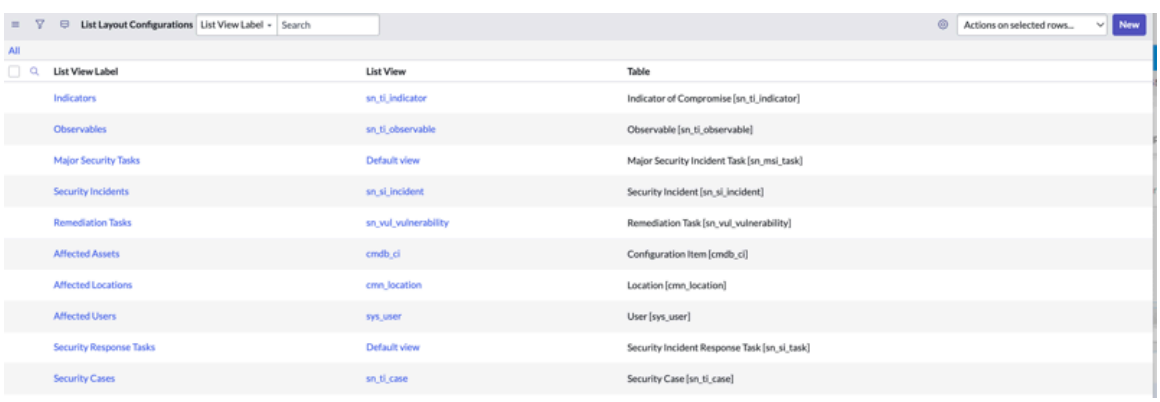
Nom	Description
Entrées	• sourceSysId : ID système de l'enregistrement de la table source en cours de liaison/proposé/promu. • msiSysId : ID système de l'incident de sécurité majeur auquel l'enregistrement source est lié/proposé/promu.
Sortie	Aucune valeur de retour de sortie.
Responsabilité	Le script doit déployer les informations dans la table Enregistrement(sn_msi_m2m_child) lié(e). • Utilisez sourceSysID pour interroger les données à partir des tables de ServiceNow relations. • Une fois les données extraites, déployez-les dans un enregistrement lié (sn_msi_m2m_child) à l'aide de l'utilitaire MSIRollupEngine pour les déployer.

Configurer la mise en page de la liste dans Gestion des incidents de sécurité majeurs

Configurez la mise en page des listes pour personnaliser la mise en page et les étiquettes utilisées dans Gestion des incidents de sécurité majeurs l'espace de travail, telles que les onglets Impact de l'incident, Enregistrements liés et Renseignements sur les menaces.

Rôle requis : admin et sn_msi.workspace_admin.

Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.



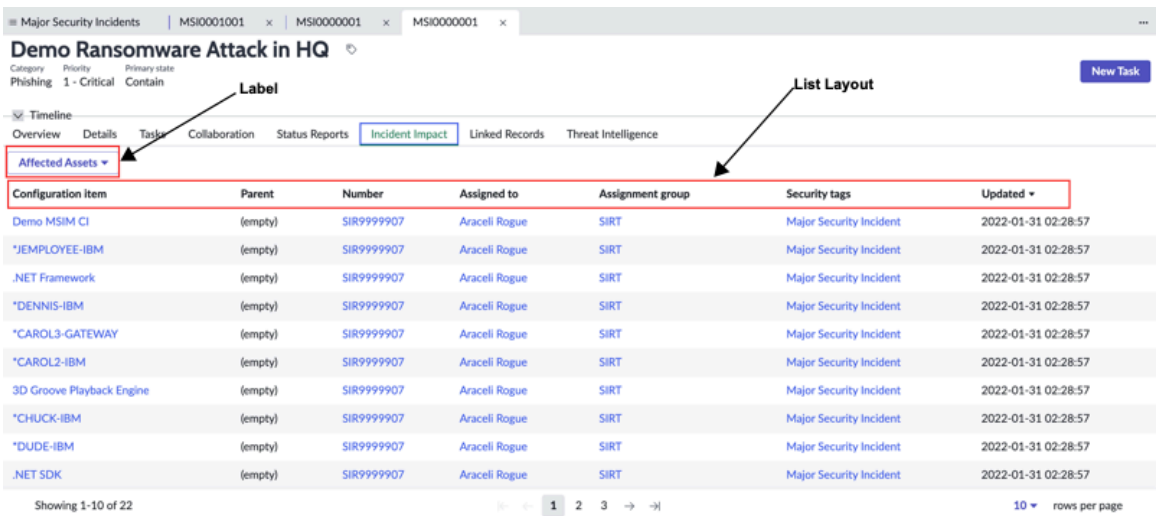
Les configurations de mise en page de liste ont déjà été expédiées pour les tables connues existantes affichées dans l'espace Gestion des incidents de sécurité majeurs de travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si vous souhaitez afficher la vue personnalisée pour les tables existantes, vous pouvez mettre à jour l'enregistrement de table respectif dans la configuration de la mise en page de liste avec la vue de liste personnalisée.
- Pour les nouvelles tables de tâches, vous pouvez créer une configuration de mise en page de liste pour afficher la vue de liste personnalisée et les étiquettes. Pour une procédure plus détaillée, voir comment Étape 4. Créer une vue pour un nouvel onglet d'enregistrement lié pour un ticket de sécurité



Exemple de déploiement d'implémentation de cas d'utilisation pour un ticket de sécurité

Les étapes suivantes expliquent un exemple de cas d'utilisation sur la façon d'ajouter une prise en charge pour lier/proposer/promouvoir en incident de sécurité majeur pour une table de ticket de sécurité.

- Étape 1. Créer une configuration d'enregistrement lié pour un ticket de sécurité
- Étape 2. Créer une vue pour la fenêtre modale d'un ticket de sécurité
- Étape 3. Créer des actions d'interface utilisateur pour la table source d'un ticket de sécurité
- Étape 4. Créer une vue pour un nouvel onglet d'enregistrement lié pour un ticket de sécurité
- Étape 5. Ajouter des listes de contrôle d'accès (ACL) pour Gestion des incidents de sécurité majeurs les utilisateurs de l'espace de travail
- Étape 6. Créer des règles métier pour un ticket de sécurité
- Étape 7. Créer des configurations d'enregistrement de déploiement

Étape 1. Créer une configuration d'enregistrement lié pour un ticket de sécurité

Créez une configuration d'enregistrement lié pour un ticket de sécurité.

Avant de commencer

Rôle requis : admin et sn_msi.workspace_admin

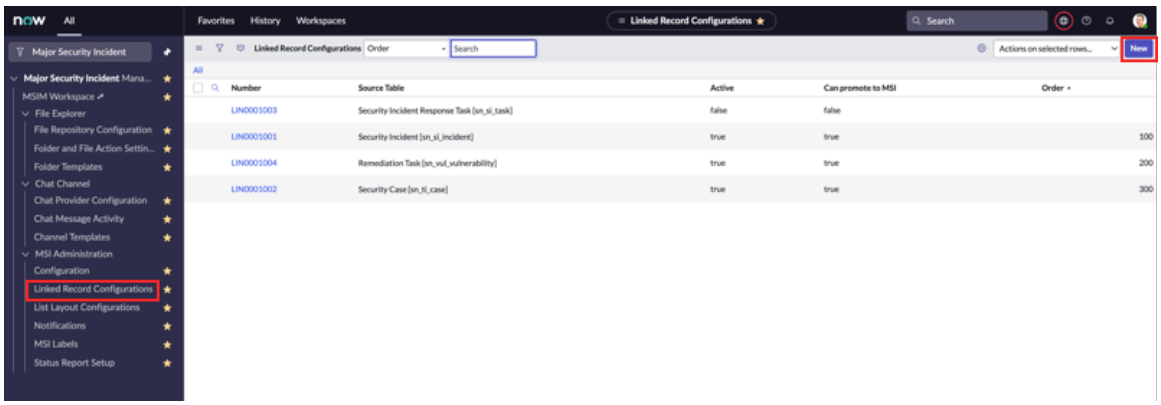
Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.

Traduction automatique

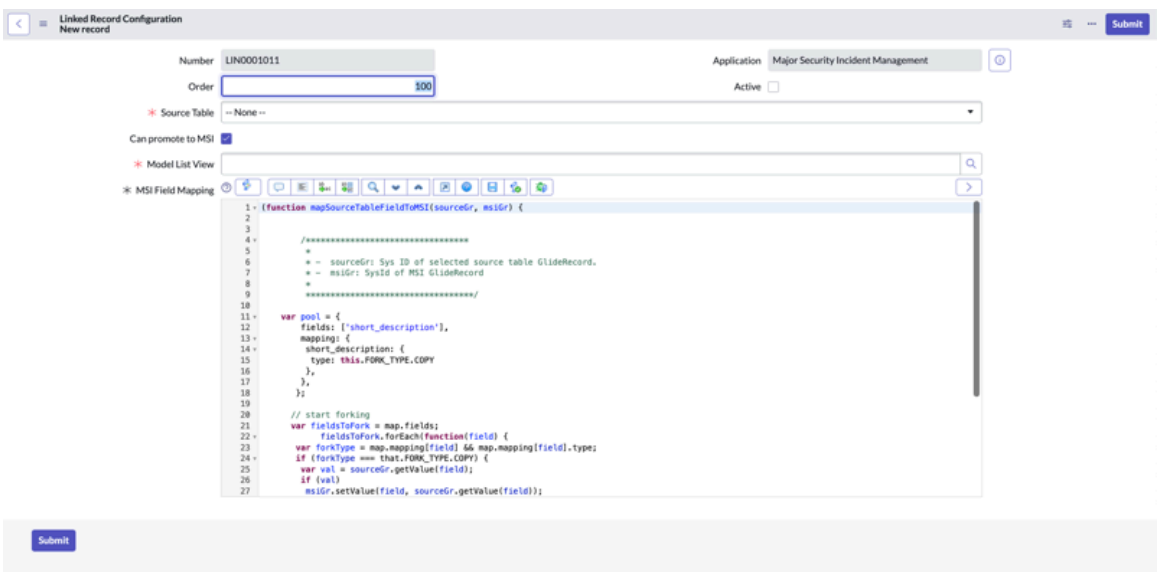
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Recherchez la configuration d’enregistrement lié dans le menu de navigation de gauche.
2. Cliquez sur **Nouveau**.



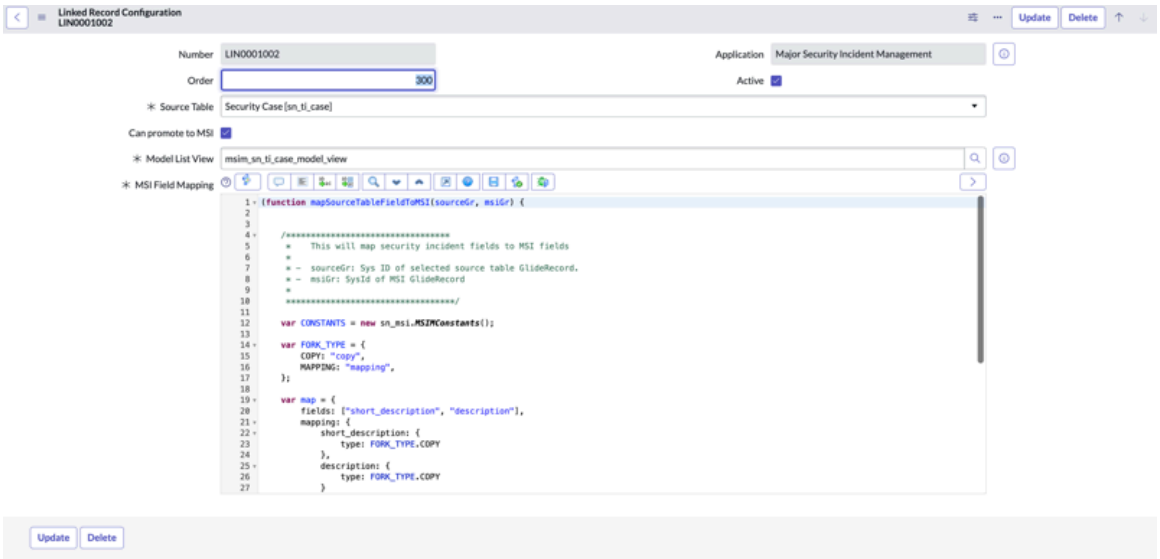
3. Remplissez le formulaire avec les colonnes requises et écrivez un script de mappage de champ.



4. Vous avez maintenant créé une configuration d’enregistrement lié pour le ticket de sécurité en ajoutant les valeurs comme décrit dans la table suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Nom	Description
Table source	Ticket de sécurité (sn_ti_case). Ici, dans cet exemple, liez/promouvez/proposez un ticket de sécurité en tant que MSI.
Ordre	Valeur d’entrée : 300 **Remarque :** L’ordre inférieur a priorité sur les ordres supérieurs. Comme un ticket de sécurité a un ordre supérieur à l’incident de sécurité et à la tâche de rattrapage, il apparaîtra dans la dernière séquence.
Peut convertir en MSI	Vrai, cochez cette case pour promouvoir le ticket de sécurité auprès de MSI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
	Remarque : ○ Lier et dissocier les enregistrements de tickets de sécurité des incidents de sécurité majeurs à partir de l'espace de Gestion des incidents de sécurité majeurs travail. En outre, la fonctionnalité Dissocier l'enregistrement n'est visible que pour les enregistrements liés. ▪ Cela permet de lier, de promouvoir et de proposer un ticket de sécurité à un incident de sécurité majeur à l'aide d'actions d'environnement classiques, mais ces actions d'interface utilisateur ne sont pas disponibles prêtes à l'emploi. Chaque action d'interface utilisateur doit être créée manuellement. Pour plus d'informations, consultez Étape 3. Créer des actions d'interface utilisateur pour la table source d'un ticket de sécurité. ▪ Lier/Promouvoir/Proposer des actions d'interface utilisateur sont disponibles pour l'incident de sécurité, la tâche de rattrapage et le ticket de sécurité prêts à l'emploi. ○ La page d'enregistrement lié de l'espace de travail MSIM affiche les enregistrements de tickets de sécurité liés. Reportez-vous à l'image ci-dessous 1 pour afficher les options disponibles après avoir coché cette case.
Vue de liste modale	msim_sn_ti_case_model_view **Remarque :** Cette vue contient des champs et l'ordre des champs affichés dans la vue de liste sur le modal de lien d'enregistrement dans l'espace de travail MSIM. Pour plus d'informations, voir Étape 2. Créer une vue pour la fenêtre modale d'un ticket de sécurité Reportez-vous à l'image ci-dessous 2 pour l'afficher à partir de la page **Enregistrements liés** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
Script de mappage de champs	Ce script décrit les champs de l’enregistrement des tables sources mappé à l’incident de sécurité majeur nouvellement créé lorsque l’enregistrement des tables sources est proposé ou promu. qui recevront les entrées : ○ sourceGr : objet d’enregistrement Glide de ticket de sécurité ○ msiGr : objet d’enregistrement Glide d’incident de sécurité majeur Le script lit la description brève du ticket de sécurité et la copie comme titre de l’incident de sécurité majeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Image 1 : Peut être promu en MSI

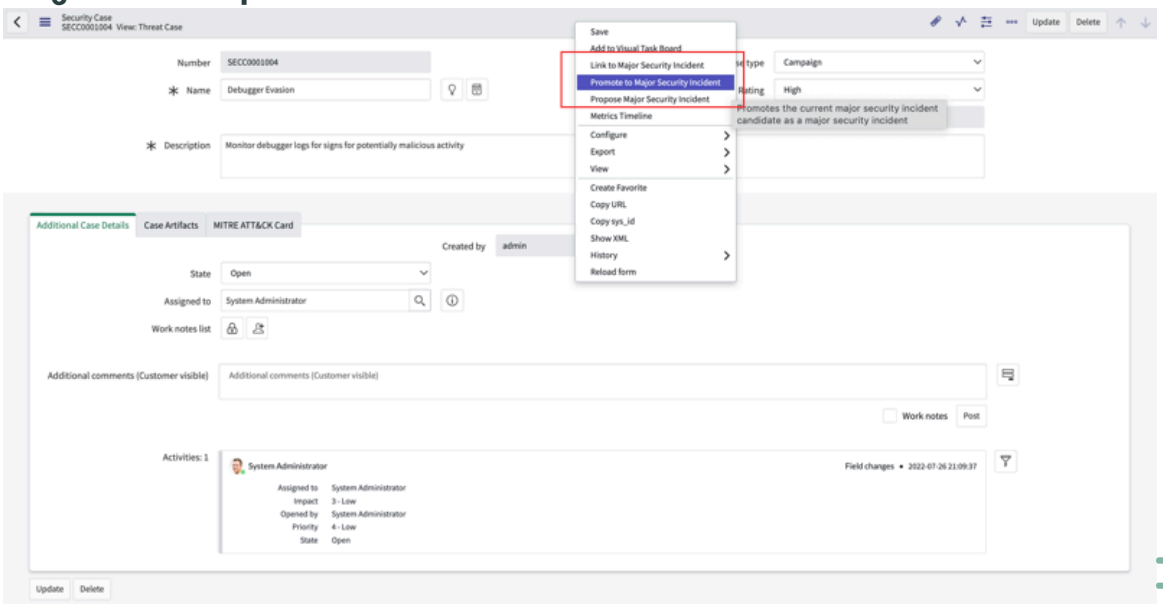
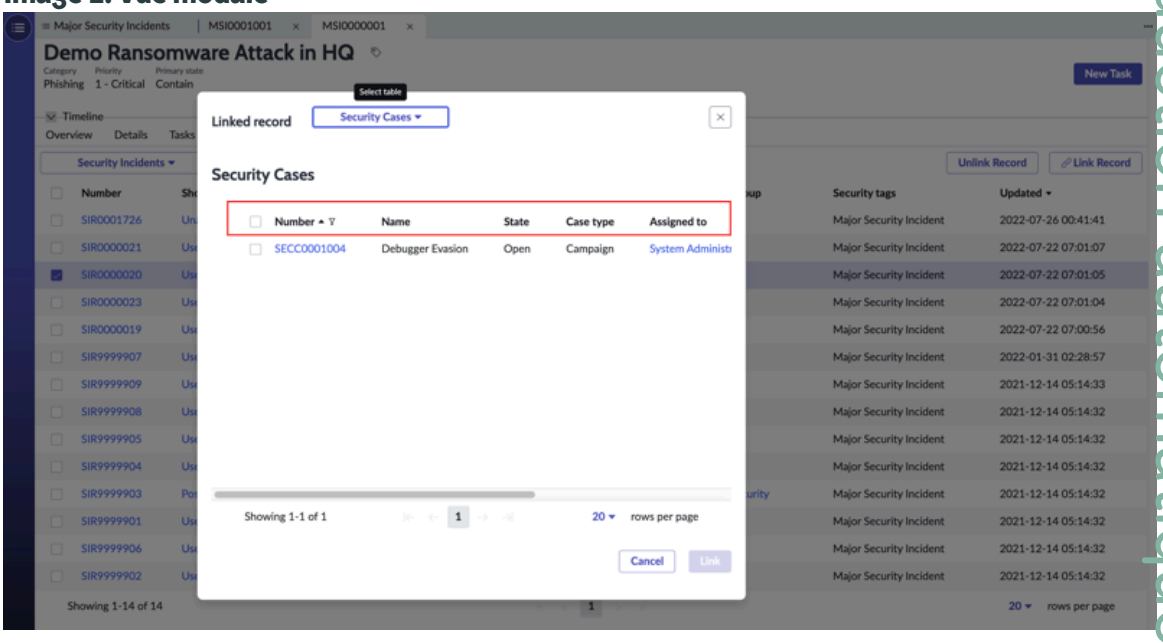


Image 2. Vue modale



Traduction automatique

Étape 2. Créer une vue pour la fenêtre modale d'un ticket de sécurité

Créer une vue pour la fenêtre modale d'un ticket de sécurité.

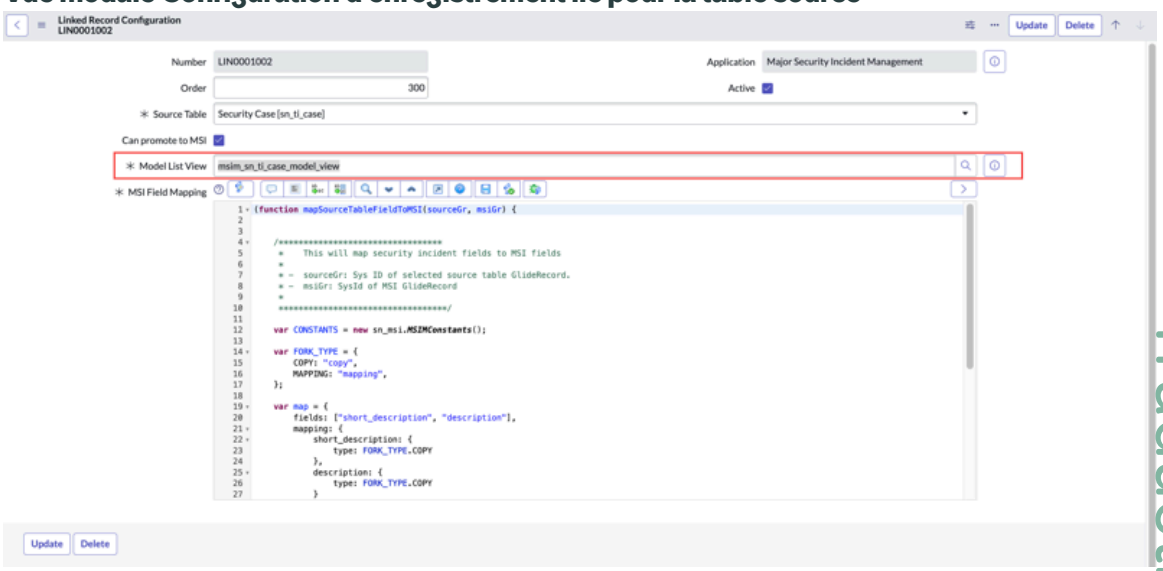
Avant de commencer

Considération clé :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Par défaut, la liste modale d'enregistrement lié affiche uniquement la mise en page de liste **par défaut** . Si vous souhaitez personnaliser la mise en page de la liste, vous pouvez utiliser **l'affichage personnalisé** sur la table source.
- Si vous souhaitez afficher la vue personnalisée, la vue personnalisée doit également être sélectionnée dans la configuration d'enregistrement lié pour la table source.

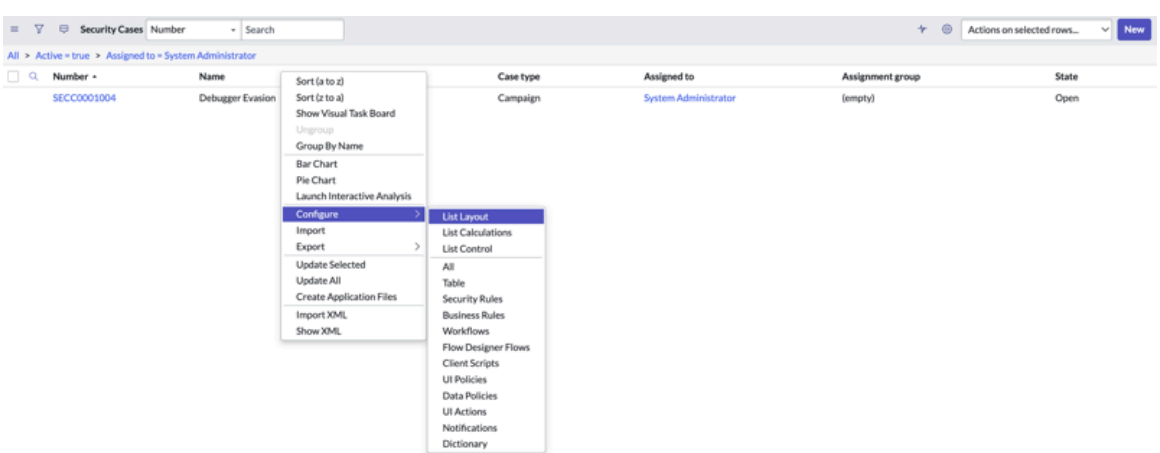
Vue modale Configuration d'enregistrement lié pour la table source



Rôle requis : admin

Procédure

1. Accédez à la table source et cliquez sur **Configurer** > **Mise en page de la liste**.



2. Accéder à **Vue liste** > **Nom de vue**.
3. Cliquez sur **Nouveau** dans la liste déroulante Nom de la vue et créez une nouvelle vue, par exemple, msim_sn_ti_case_modal_view.
4. Sélectionnez la vue nouvellement créée.
   Une fois cette option sélectionnée, vous pouvez choisir les champs requis dans la liste Disponibles.
5. Cliquez sur **Enregistrer**.
6. Accédez à la **Menu** > **Vues** pour vérifier si la vue s'est rendue correctement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étape 3. Créer des actions d'interface utilisateur pour la table source d'un ticket de sécurité

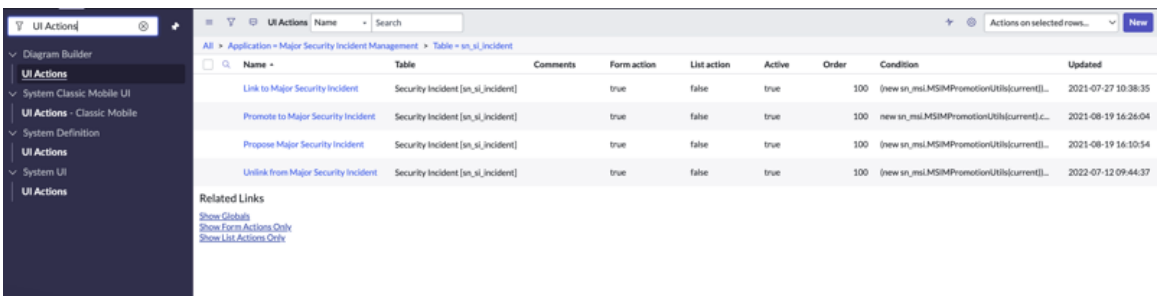
Créez des actions d'interface utilisateur pour la table source d'un ticket de sécurité.

Avant de commencer

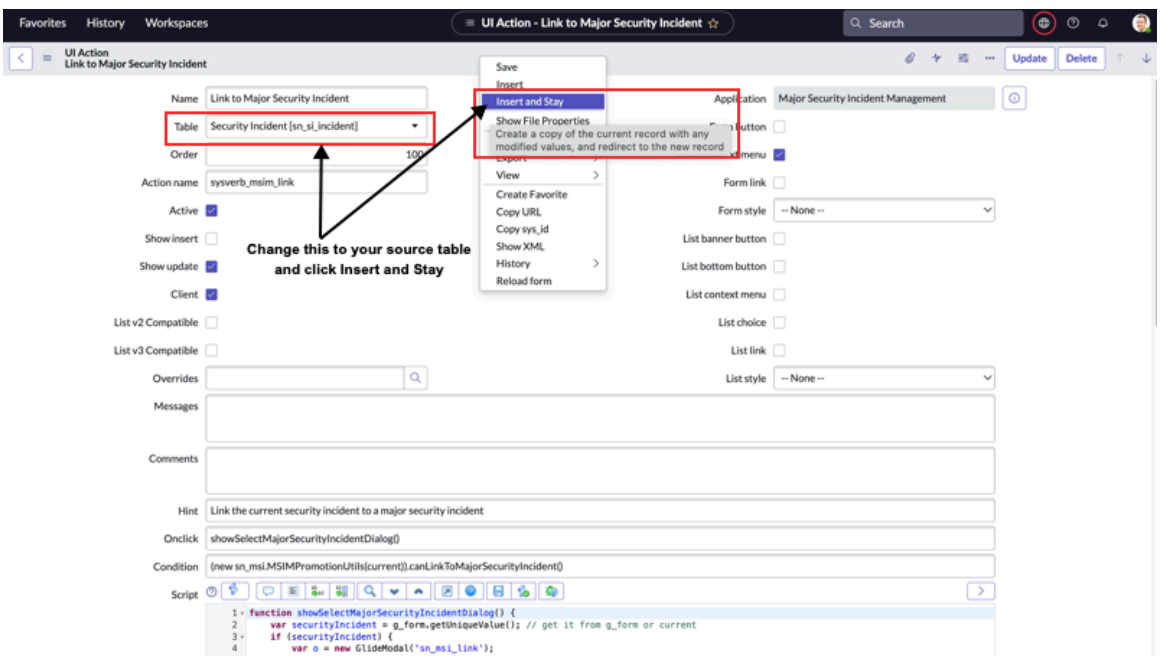
Rôle requis : admin

Procédure

1. Accédez à la **Définition du système** > **Actions d'interface utilisateur**.
2. Exécutez l'option Filtrer pour filtrer la liste par **Application** : Major Security Incident Management et **Table** : sn_si_incident.



3. Sélectionnez chaque action d'interface utilisateur une par une et enregistrez les détails dans la table source.



4. Répétez les mêmes étapes que ci-dessus pour les actions d'interface utilisateur suivantes :
   - Lier à l'incident de sécurité majeur
   - Incident de sécurité majeur proposé
   - Dissocier d'un incident de sécurité majeur
   - Promouvoir en incident de sécurité majeur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

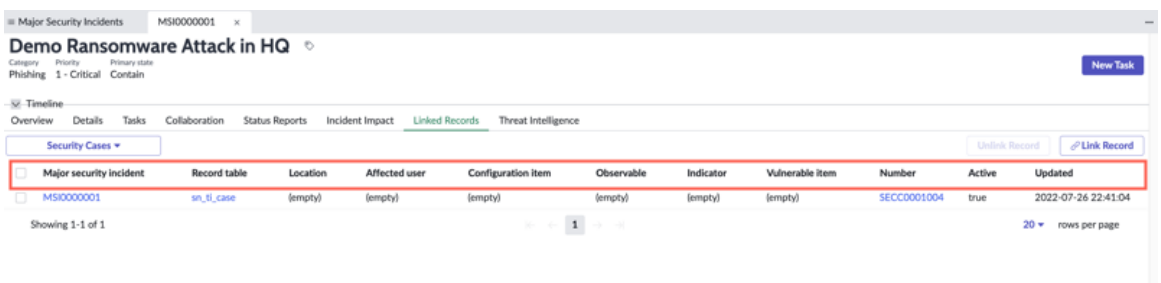
Étape 4. Créer une vue pour un nouvel onglet d'enregistrement lié pour un ticket de sécurité

Personnalisez la mise en page de la liste d'une table de tickets de sécurité lorsqu'elle s'affiche sur la page Lier les enregistrements avec l'espace de Gestion des incidents de sécurité majeurs travail.

Avant de commencer

Conditions préalables:

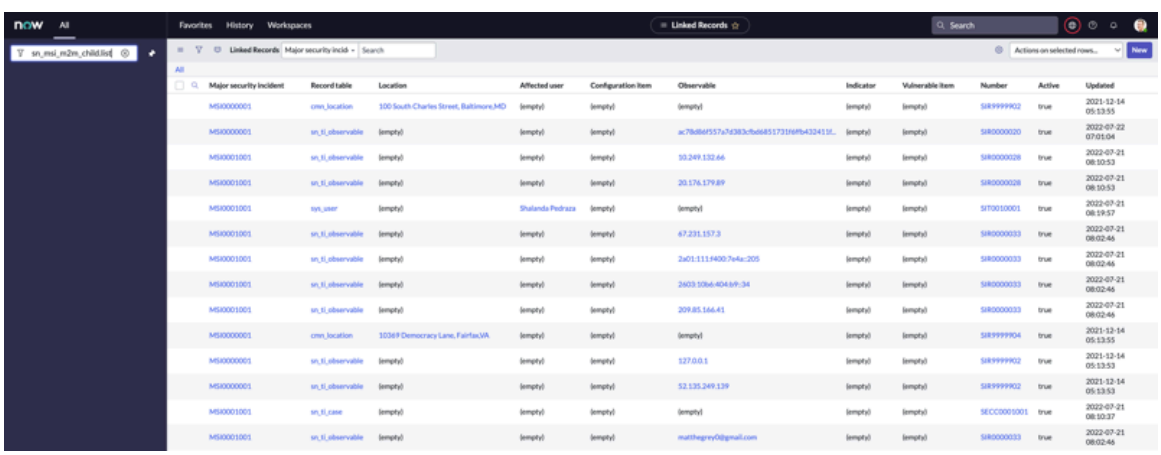
- Choisissez la colonne qui doit être visible lorsqu'une liste est affichée pour une table de ticket de sécurité.
- Choisissez l'ordre des champs à afficher dans la liste déroulante.



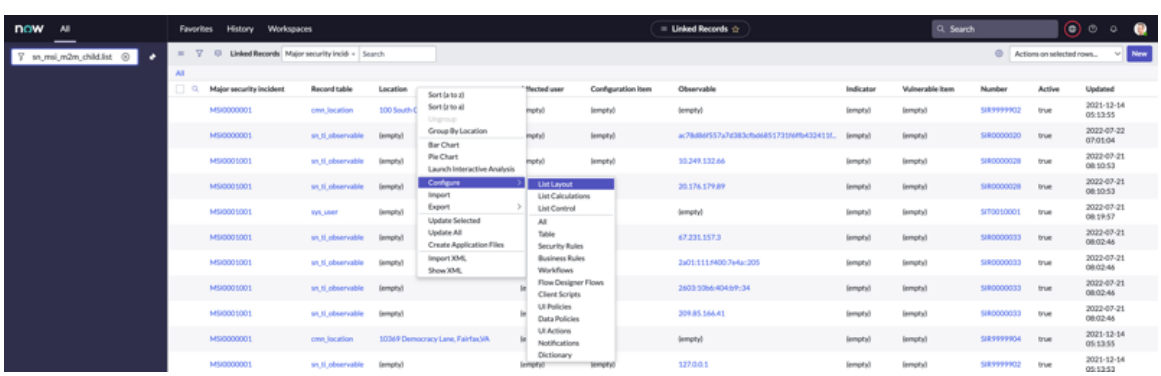
Rôle requis : admin

Procédure

1. Recherchez **sn_msi_m2m_child.list** à l'aide du volet de navigation de gauche.
   La table Enregistrements liés s'affiche.



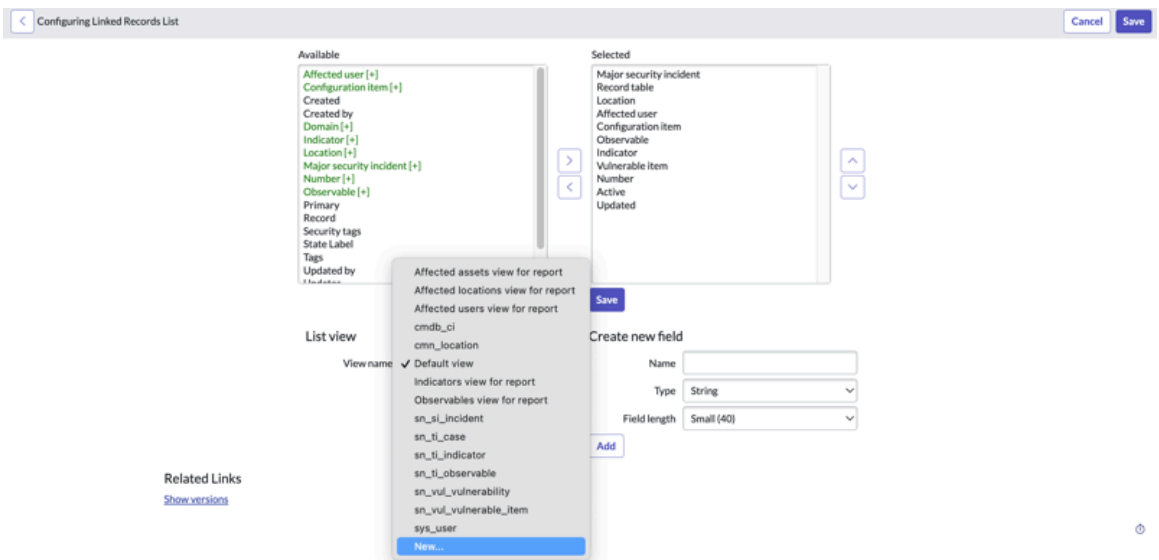
2. Cliquez avec le bouton droit sur l'en-tête, puis sélectionnez **Configurer** > **Mise en page de la liste**.
   La page Configuration de la liste des enregistrements liés s'affiche.



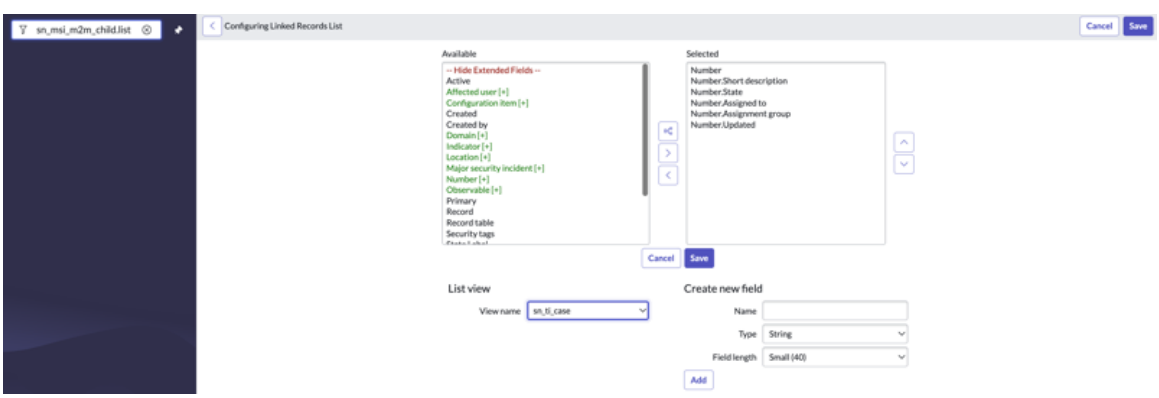
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

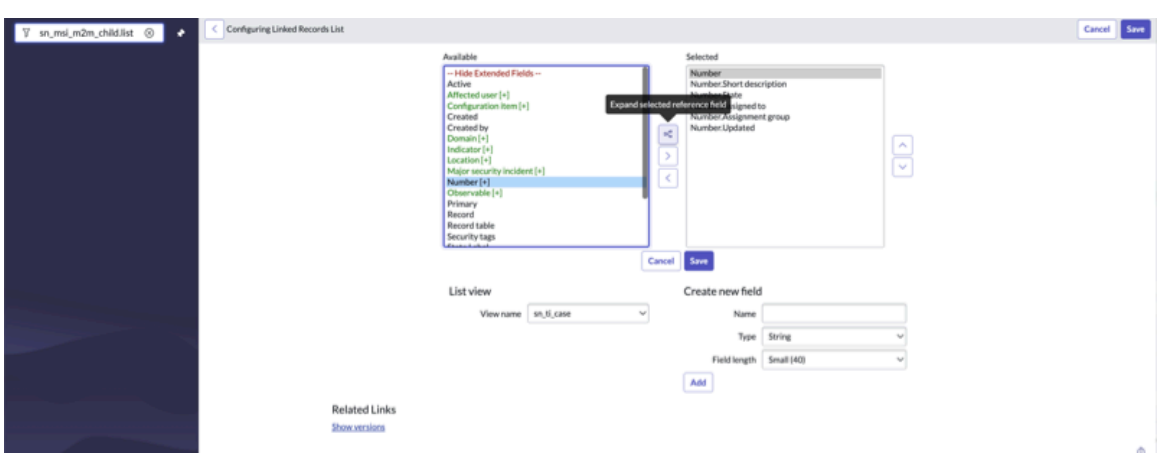
3. Accéder à **Vue liste** > **Nom de vue**.
4. Sélectionnez **Nouveau** dans la liste déroulante Nom de la vue.



5. Sélectionnez les colonnes qui s'afficheront dans la vue de liste de l'espace de travail.
   L'enregistrement du ticket de sécurité est stocké dans la colonne **Numéro** . Pour restituer les informations à partir d'un ticket de sécurité, vous devez effectuer une remontée pas à pas dans la colonne **Nombre** .



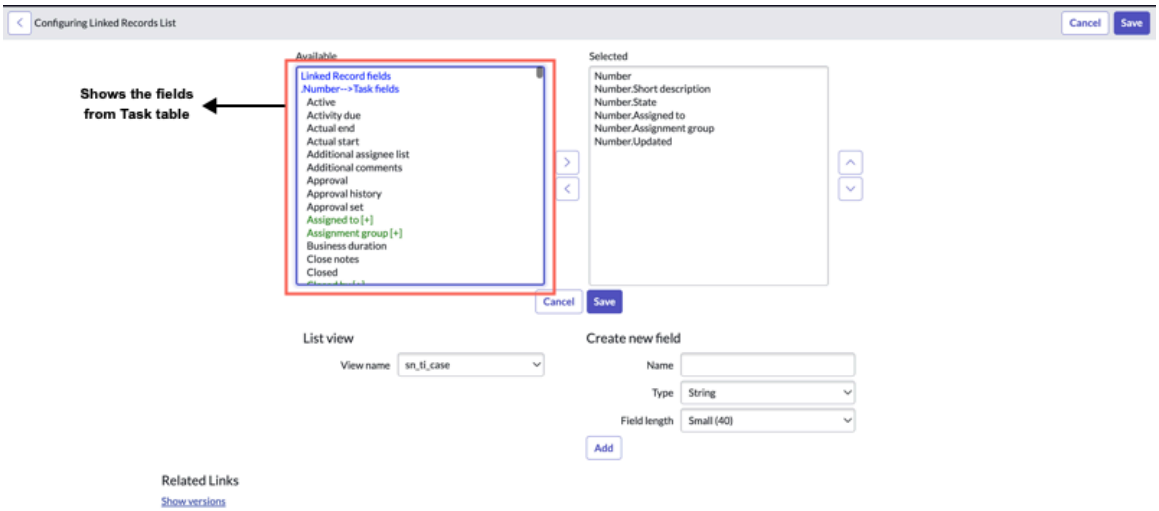
   a. Pour effectuer une remontée pas à pas, sélectionnez d'abord la colonne **Numéro** dans la liste Disponible, puis cliquez sur **Développer le champ de référence sélectionné**.



   b. Développez les colonnes à partir du **numéro** pour les sélectionner et déplacez-les vers la liste sélectionnée.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique



c. Cliquez sur **Enregistrer** pour enregistrer et créer une vue.

6. L'étape suivante consiste à afficher la vue créée dans l'espace de Gestion des incidents de sécurité majeurs travail, vous devez créer une **configuration de mise en page de liste**.

a. Recherchez la configuration de la **mise en page** de liste à l'aide du panneau de navigation de gauche.

b. Cliquer sur **Administration MSI** > **Configurations des mises en page de listes**.

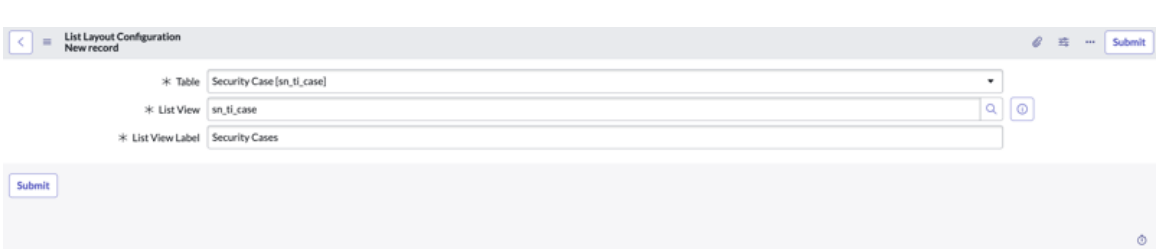
c. Cliquez sur **Nouveau** pour créer une nouvelle configuration.

d. Sélectionnez la table source dans la colonne Table et sélectionnez la vue nouvellement créée dans le champ Vue de liste.

e. L'étiquette **de vue de liste** vous permet de contrôler les étiquettes lorsque la même table source est affichée dans l'espace de Gestion des incidents de sécurité majeurs travail.

f. Enregistrez l'enregistrement.

Remarque : Une fois l'enregistrement sauvegardé, accédez à l'espace Gestion des incidents de sécurité majeurs de travail pour afficher la vue de liste et l'étiquette du rendu dans l'espace de travail.



Étape 5. Ajouter des listes de contrôle d'accès (ACL) pour Gestion des incidents de sécurité majeurs les utilisateurs de l'espace de travail

Ajoutez des listes de contrôle d'accès (ACL) pour Gestion des incidents de sécurité majeurs les utilisateurs de l'espace de travail.

Avant de commencer

Rôle requis : admin

Remarque : Les autorisations requises pour les options de liaison et de dissociation sont contrôlées par le rôle sn_msi.linkedsivi_read .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

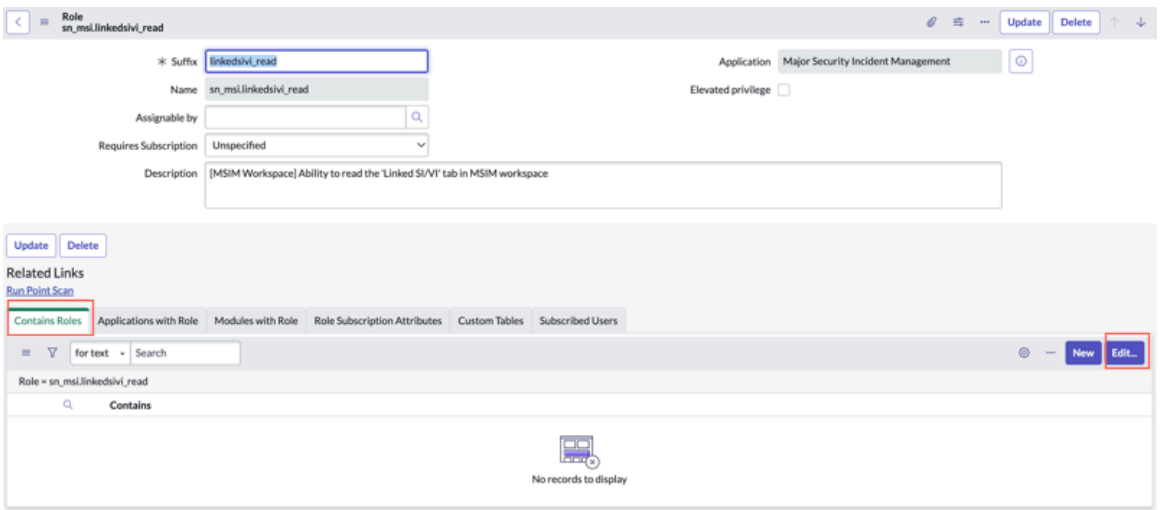
 Le profil contient le rôle sn_msi.linkedsivi_read.

1. sn_msi.workspace_admin (administrateur d'espace de travail MSIM)
2. sn_msi.workspace_manager (Gestionnaire de l'espace de travail MSIM)
3. sn_msi.workspace_responder (répondeur d'espace de travail MSIM)

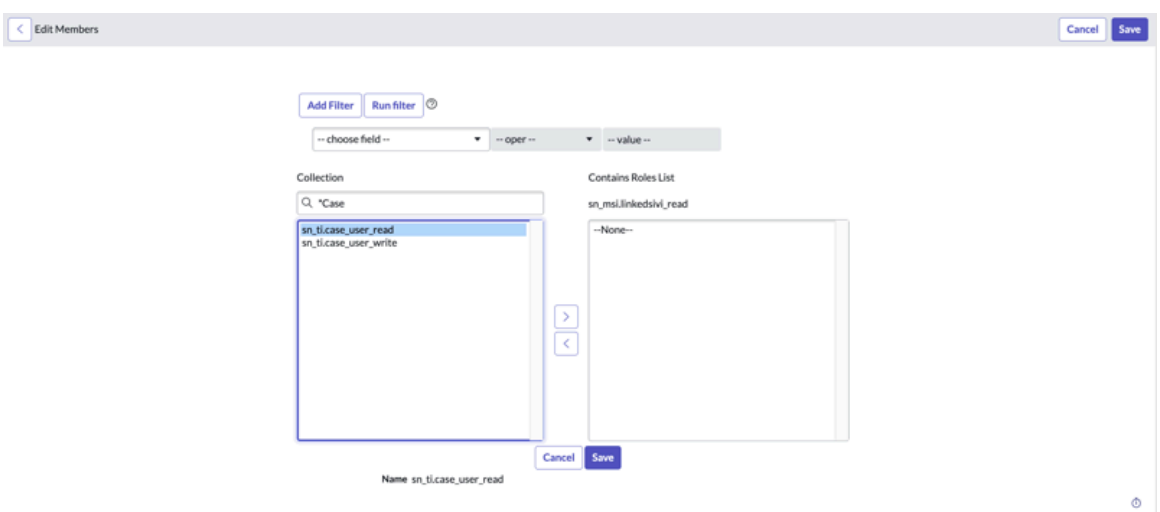
Remarque : Pour toute table source, vous devez vous assurer que les rôles requis sont ajoutés au rôle sn_msi.linkedsivi_read .

Procédure

1. Accédez à la **Administration utilisateurs** > **Rôles** et recherchez **le rôle sn_msi.linkedsivi_read** .
2. Cliquez sur **Modifier** dans la section de liste connexe Contient les rôles.



3. Assurez-vous que vos rôles de table source sont ajoutés dans la section Contient les rôles.
   La page Modifier les membres s'affiche pour configurer les rôles requis pour un ticket de sécurité.



4. Recherchez les rôles de la table source dans la section Collections.
   Sélectionnez les rôles requis qui autorisent l'accès en lecture et en écriture sur la table source pour un ticket de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Pour un ticket de sécurité, deux rôles distincts en lecture et en écriture sont nécessaires.
- Accès en écriture sur les tables pour pouvoir sélectionner un enregistrement source à partir du modal Enregistrement lié de l'espace de Gestion des incidents de sécurité majeurs travail.

5. Cliquez sur **Enregistrer** pour ajouter des rôles.
6. Vérifiez que les rôles sont ajoutés à la section de la liste connexe **Contient les rôles** .

Étape 6. Créer des règles métier pour un ticket de sécurité

Créez les règles métier requises pour un ticket de sécurité.

Avant de commencer
Rôle requis : admin

Créez les trois règles métier suivantes pour la nouvelle table source Ticket de sécurité (sn_ti_case). Ces règles métier sont nécessaires pour maintenir la cohérence du comportement avec la table source prête à l'emploi, telle que Incident de sécurité (sn_si_incident).

Règles métier pour la nouvelle table source :

1. **Désactiver le lien si inactif** : Une fois le ticket de sécurité fermé, les informations connexes ne seront plus affichées sur la Gestion des incidents de sécurité majeurs page de l'espace de travail.
2. **Synchroniser les informations de l'équipe lors de la mise à jour : l'onglet** de détails de l'incident de sécurité majeur affiche les informations sur toutes les équipes et tous les utilisateurs actifs travaillant sur différentes tâches. Une fois que nous avons mis à jour l'utilisateur affecté ou que le groupe d'affectation est modifié dans le ticket de sécurité, nous devons mettre à jour les informations de l'équipe de ticket de sécurité dans la section Équipe active d'incident de sécurité majeur. Ces règles métier mettent à jour les nouveaux utilisateurs affectés et groupes d'affectation dans la section Équipe active.
3. **Synchroniser les informations de l'équipe lors de la suppression : l'onglet** de détails de l'incident de sécurité majeur affiche les informations sur toutes les équipes et tous les utilisateurs actifs travaillant sur différentes tâches. Une fois le ticket de sécurité fermé, il n'est plus nécessaire d'afficher les informations de l'équipe du ticket de sécurité dans la section Équipe active de l'incident de sécurité majeur. Ces règles métier supprimeront l'utilisateur affecté et le groupe d'affectation de l'équipe active.

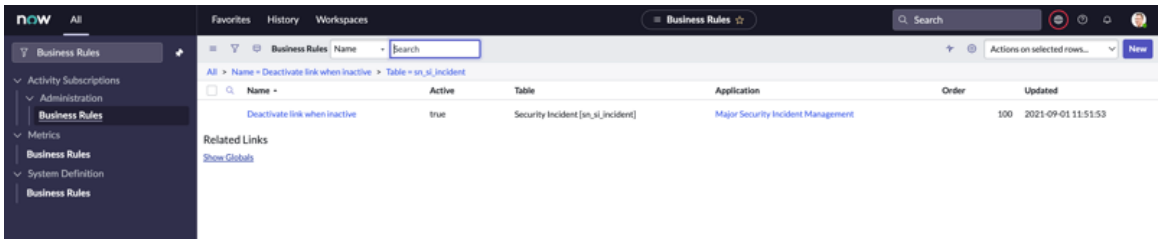
Créez des règles métier pour une nouvelle table source :

Procédure

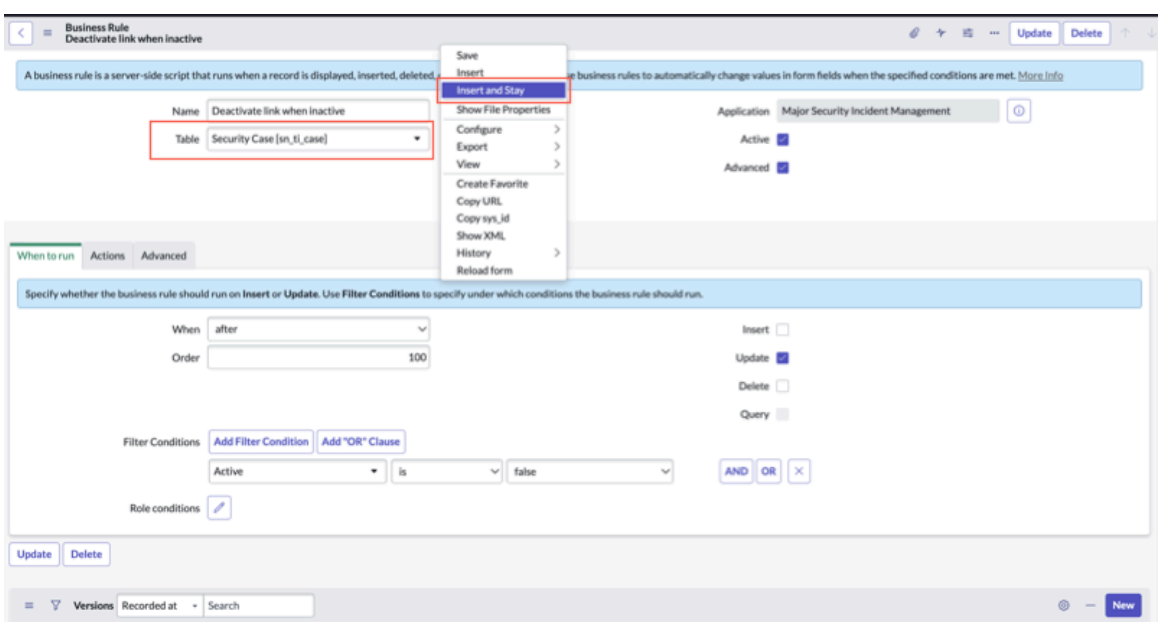
1. Accédez à la **Définition du système** > **Règles métier**.
2. Exécutez l'option de filtre pour filtrer les critères de règles métier avec les informations ci-dessous :
   - **Nom** : Désactiver le lien si inactif
   - **Tableau** : sn_si_incident

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Ouvrez l’enregistrement et remplacez le nom de la table par une nouvelle table source : sn_ti_case.
4. Cliquez avec le bouton droit sur le menu de la page, puis cliquez sur **Insérer et rester** pour créer l’enregistrement.



5. Répétez également la procédure pour deux autres règles métier.
   - Synchroniser les informations de l’équipe lors de la suppression
   - Synchroniser les informations sur l’équipe lors de la mise à jour

Étape 7. Créer des configurations d’enregistrement de déploiement

Créez une configuration d’enregistrement de déploiement pour lier et dissocier des enregistrements supplémentaires à MSI.

Avant de commencer

Rôle requis : admin et sn_msi.workspace_admin

Remarque : L’administrateur système peut créer l’enregistrement et l’administrateur de l’espace de travail MSI peut le mettre à jour.

Pour déployer des informations telles que des éléments de configuration, des observables et un indicateur de compromis lié à un ticket de sécurité, créez une configuration d’enregistrement de déploiement.

Procédure

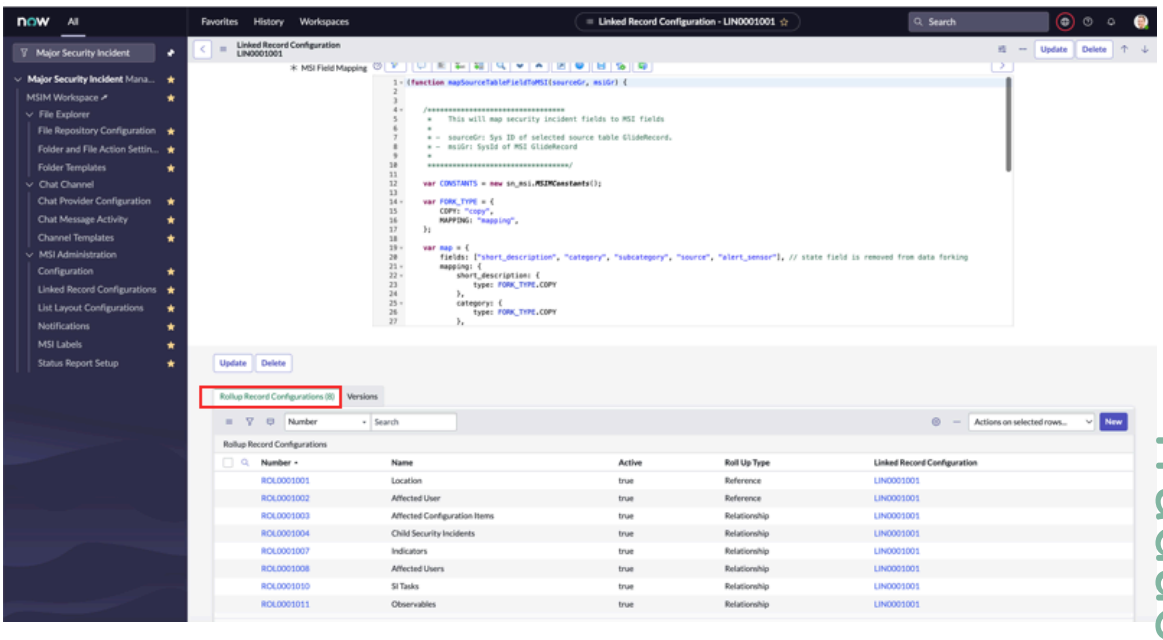
1. Accédez à la **Réponse aux incidents de sécurité majeurs** > **Configuration d’enregistrements liés**.
   La page Configurations d’enregistrements liés s’affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Sélectionnez ou créez un nouvel enregistrement lié et accédez à la section **Configuration de l'enregistrement de déploiement** à partir de la même page.

Section Configuration d'enregistrement de déploiement



Que faire ensuite

- Pour plus d'informations, voir Configurer les enregistrements de déploiement dans Gestion des incidents de sécurité majeurs
- Pour obtenir des exemples d'exemples de tickets de sécurité, consultezÉcriture d'un script pour un ticket de sécurité

Écriture d'un script pour un ticket de sécurité

Écriture d'un script pour un ticket de sécurité afin de déployer la configuration d'enregistrement.

Avant de commencer

Rôle requis : admin et sn_msi.workspace_admin

Remarque : L'administrateur système peut créer l'enregistrement et l'administrateur de l'espace de travail MSI peut le mettre à jour.

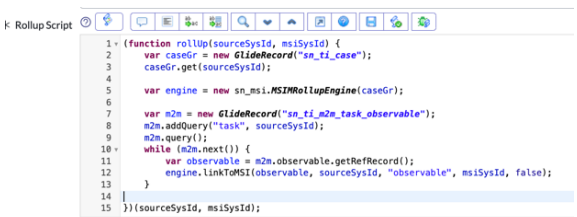
Procédure

1. Recherchez les configurations d'enregistrements liés à l'aide du volet de navigation de gauche.
2. Accédez à la **Administration MSI** > **Configuration d'enregistrement lié**.
3. Ouvrez l'enregistrement de configuration qui a été créé pour un ticket de sécurité.
4. La configuration de l'enregistrement de déploiement s'affiche dans la section Liste connexe.
5. Cliquez sur **Nouveau** pour créer une configuration d'enregistrement de déploiement.

   Vous trouverez ci-dessous un exemple d'enregistrement créé pour déployer les données des observables liées au ticket de sécurité que nous essayons de déployer avec les valeurs de champ suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description
Type de déploiement	Relation **Remarque :** Les informations sur l'observable sont disponibles sous forme de liste connexe.
Script de déploiement	L'entrée sourceSysId contient l'ID système du ticket de sécurité et le msiSysId contient l'ID système de l'incident de sécurité majeur.  ○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table. ○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case. ○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method: `MSIMRollupEngine.linkToMSI(« entityGr », « sourceSysId », « fieldNameInLinkedRecordTable », « msiSysId », « isPrimaryRecord »)`

Traduction automatique

Effectuer un déploiement atomique à la demande

Le cadre de travail de déploiement ne peut pas gérer les mises à jour des enregistrements liés existants. Dans de tels cas, un déploiement atomique à la demande doit être effectué pour les enregistrements liés, ce qui peut être réalisé via des règles métier.

Pour capturer les mises à jour des enregistrements liés, les règles métier doivent être créées sur la table source.

Ces règles métier fonctionnent sur les opérations d'insertion, de mise à jour et de suppression. Lorsque vous effectuez une opération d'insertion ou de mise à jour, vous devez ajouter ou mettre à jour des informations de déploiement vers MSI. Si vous effectuez une suppression, les informations cumulées seront supprimées de MSI.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, une fois qu'un incident de sécurité est lié à MSI, les informations connexes sont déployées automatiquement MSI. Mais ultérieurement, si vous ajoutez un nouvel observable à un MSI, l'observable nouvellement ajouté sera également déployé sur MSI. Ici, la règle métier **Synchroniser l'observable déployé** capture la mise à jour et déploie l'enregistrement mis à jour sur MSI. De même, la même règle métier gère également la suppression des observables cumulés existants, s'ils sont supprimés de l'incident de sécurité.

Règles métier prédéfinies

Voici quelques règles métier prédéfinies qui vous aident à comprendre comment gérer les déploiements atomiques

Règle	Description
Indicateur de déploiement de synchronisation (sn_ti_m2m_task_indicator)	Utilisez cette règle métier pour gérer le déploiement et la suppression de l'indicateur de compromis de l'incident de sécurité, du ticket de sécurité et de la tâche de rattrapage.
Synchroniser l'observable déployé (sn_ti_m2m_task_observable)	Utiliser cette règle métier gère le déploiement et la suppression des observables liés de l'incident de sécurité, du ticket de sécurité et de la tâche de rattrapage.
Utilisateur affecté déployé de synchronisation (sn_si_m2m_task_affected_user)	Utiliser cette règle métier gère le déploiement et la suppression des utilisateurs affectés liés de l'incident de sécurité, du ticket de sécurité et de la tâche de correction.
CI affecté déployé de synchronisation (task_ci)	Utiliser cette règle métier gère le déploiement et la suppression des éléments de configuration associés de l'incident de sécurité, du ticket de sécurité et de la tâche de rattrapage.

Intégrations de Réponse aux incidents de sécurité

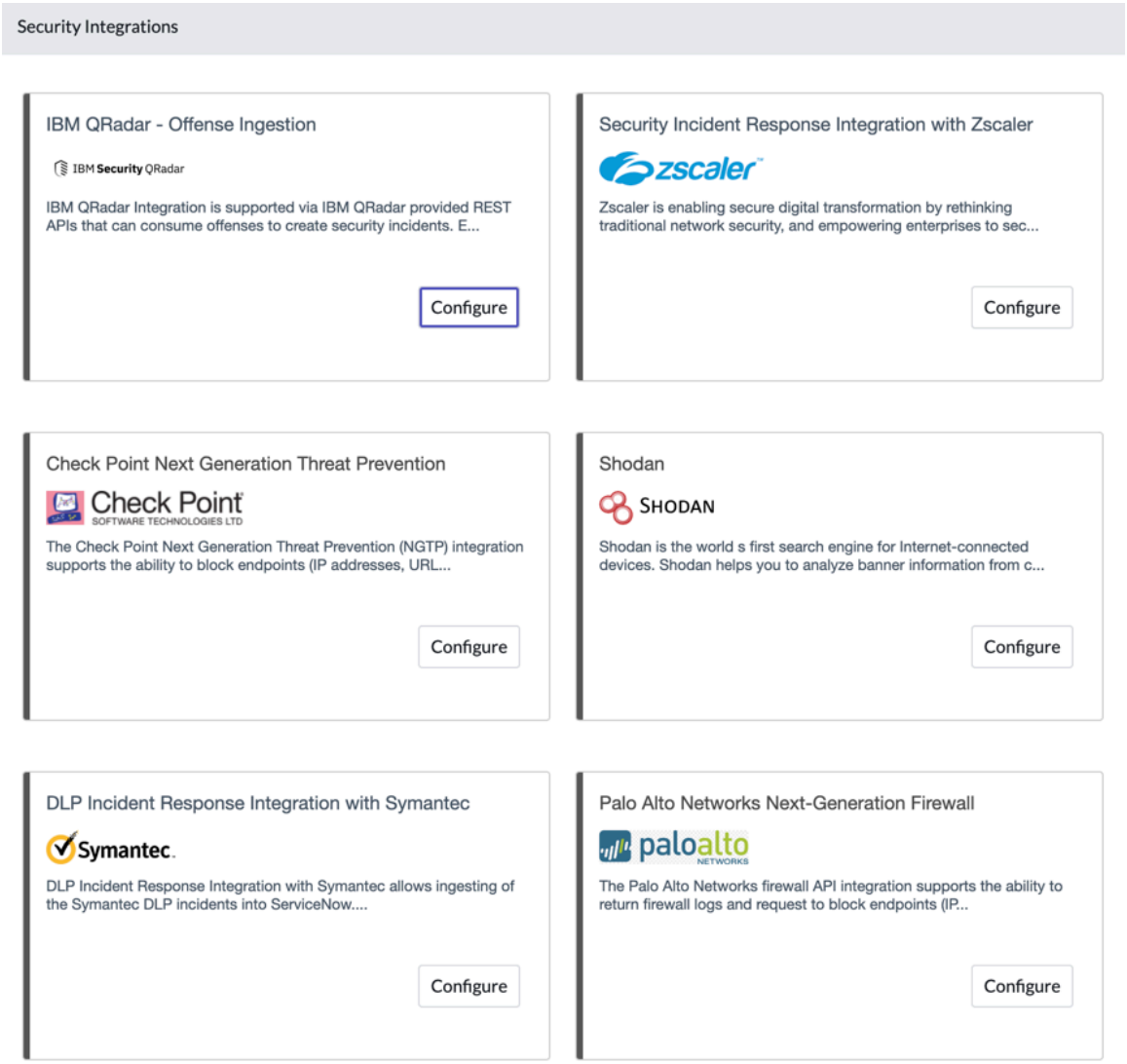
Toutes les Opérations de sécurité applications principales et les intégrations tierces non essentielles sont disponibles auprès du ServiceNow Store. Cette section fournit des instructions pour activer les intégrations et configurer les intégrations ServiceNow tierces. Vous y trouverez également des instructions de base pour développer vos propres intégrations, ainsi que des détails sur des intégrations spécifiques incluses dans le système de base.

Configurations d'intégration

Le système de base comprend une série de « cartes » pour chacune des implémentations d'intégration que vous pouvez activer et utiliser. En outre, des cartes sont affichées pour toutes les intégrations publiées sur le ServiceNow Store qui ont des dépendances à Opérations de sécurité des modules d'extension. Les cartes d'intégration peuvent être affichées en sélectionnant **Security Operations** > **Configurations d'intégration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez filtrer les intégrations visibles à l'aide du menu déroulant **Catégorie** . Le menu déroulant **Afficher les configurations** vous permet de voir plusieurs instances d'implémentations qui autorisent leur création.

Boutons sur les cartes d'intégration

Les cartes d'intégration affichent différents boutons en fonction de l'état actuel de l'intégration et de la source de la carte.

Bouton	Description
Installer le module d'extension	Cliquez sur ce bouton pour installer le module d'extension applicable afin d'activer l'intégration. Une fois le module d'extension installé, le bouton passe à **Configurer**.
Configurer	Cliquez sur ce bouton pour entrer des informations sur la configuration de l'intégration. Pour certaines intégrations, vous devrez peut-être saisir des clés API ou des URL acquises à partir du site web de l'intégration tierce.
Nouveau	Certaines intégrations, telles que Carbon Black et IBM QRadar, vous permettent de définir plusieurs implémentations d'une même intégration. Pour ces intégrations, cliquez sur **Nouveau**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bouton	Description
	une fois le module d'extension activé. Les cartes vous permettent d'installer des modules d'extension (le cas échéant) et de configurer les implémentations à utiliser.
Ouvrir la page	Dans le système de base, votre instance interroge le ServiceNow Store pour toutes les applications qui ont des dépendances sur Opérations de sécurité des modules d'extension. Lorsque ces applications sont trouvées et que les modules d'extension d'application associés sont activés, des cartes d'intégration s'affichent avec les autres cartes d'intégration de sécurité. Cliquez sur **Ouvrir la page** pour accéder au site web de l'application tierce pour configurer l'intégration. Une fois la configuration terminée, le bouton **Ouvrir la page** devient **Configurer**.

ArcSight ESM Intégration de l'ingestion d'événements

L'intégration ArcSight ESM de l'ingestion Réponse aux incidents de sécurité d'événements au produit permet aux analystes d'incidents de sécurité de collecter des événements corrélés et d'automatiser la création d'incidents de sécurité avec la ServiceNow plateforme. Les données sont ingérées en permanence en fonction d'un calendrier d'interrogation configuré, et elles sont utilisées par les analystes pour identifier et répondre aux menaces potentielles de cybersécurité.

Grâce à cette intégration, les événements corrélés candidats aux incidents de sécurité peuvent être ingérés périodiquement. Vous pouvez mapper les champs des événements corrélés aux champs d'incident de sécurité, prévisualiser la configuration d'un événement en tant qu'incident de sécurité et configurer l'ingestion programmée d'événements pour créer automatiquement des incidents de sécurité sur une base continue.

Vue d'ensemble de l'intégration de l'ingestion d'événements ArcSight ESM

Cette intégration fournit à un analyste du centre des opérations de sécurité (SOC) une visibilité sur les événements de corrélation dans ArcSight ESM. Ces données peuvent être intégrées aux ServiceNow AI Platform incidents de sécurité de Réponse aux incidents de sécurité (SIR) pour une enquête plus approfondie et une correction. Des profils sont créés dans votre ServiceNow AI Platform instance pour gérer les différents types d'événements de corrélation qui sont créés et mis à disposition via les visionneuses de requêtes de corrélation dans ArcSight ESM. Ces profils personnalisent la façon dont les différents ArcSight ESM champs d'événements corrélés sont affichés sur les incidents de sécurité SIR.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Créez plusieurs profils d'ingestion d'événements pour créer SIR des incidents de sécurité pour des types de menaces spécifiques tels que les programmes malveillants et les tentatives d'accès non autorisé.
- Effectuez un mappage par glisser-déposer des valeurs de champs d'événements de corrélation vers les champs d'incident ArcSight ESM de sécurité associés SIR .
- Aperçu de la mise en page de l'incident SIR de sécurité en fonction d'un échantillon d'événements de corrélation pour valider les détails du mappage d'événements.
- Ingérer des événements de corrélation historiques ainsi que de nouveaux événements notables sur des intervalles configurables.
- Filtrer les événements de corrélation qui ne répondent pas aux SIR critères de génération d'incidents, par exemple les événements de priorité faible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Regroupez les événements aux incidents de sécurité existants SIR en fonction des valeurs de champ correspondantes pour éviter les incidents de sécurité en double.
- Mettez à jour les événements de corrélation en fonction SIR des conditions de création et/ou de fermeture d'incident via une interface bidirectionnelle.

Versions prises en charge ServiceNow AI Platform

Cette intégration prend en charge les versions New York Patch 6 et Orlando ServiceNow AI Platform .

Les applications Security Operations suivantes doivent être installées et activées à partir de .ServiceNow Store Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour assurer une installation fluide :

1. Cadre de travail d'intégration de sécurité
2. Security Support Common
3. Security Incident Response
4. Ingestion d'événements et d'alertes pour Security Operations
5. Modules d'extension du concentrateur d'intégration
   a. Exécution du concentrateur d'intégration ServiceNow
   b. Étape d'action du concentrateur d'intégration ServiceNow : REST

Pour plus d'informations sur l'installation Opérations de sécurité des applications principales, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

ArcSight ESM Versions prises en charge

Cette intégration a été testée avec la ArcSight ESM version 7.0.0.2436 du gestionnaire. L'intégration prend en charge les environnements de services sur site et dans le ArcSight ESM cloud/hébergés.

Serveur MID

Cette intégration nécessite l'installation et la configuration d'un ArcSight ESM serveur MID dans votre ServiceNow AI Platform® instance pour se connecter au service lorsque le ArcSight ESM serveur est déployé au sein de votre réseau d'entreprise. Si vous utilisez le service dans le cloud, un serveur MID n'est ArcSight ESM pas nécessaire. Consultez le site Web de la documentation produit ServiceNow pour plus d'informations sur les serveurs MID.

Références

Référence	Identificateur de document	Titre de document
1	ArcSight ESM Documentation du produit	Documentation sur le produit ArcSight .
2	ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer votre ServiceNow AI Platform® instance pour l'intégration d'ingestion d'événements ArcSight ESM

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre ServiceNow AI Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application afin de garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform® et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre ServiceNow AI Platform® instance. • Un utilisateur disposant du rôle d'administrateur ServiceNow AI Platform® (admin) installe l'application à partir de et ServiceNow Store lui affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans le ServiceNow AI Platform®: ◦ Nomme, crée et modifie les profils d'événements. ◦ Sélectionne et mappe les valeurs des événements de corrélation aux incidents de ArcSight ESM sécurité. ◦ Prévisualise les détails de l'incident de sécurité pour plus d'exactitude avant de finaliser la configuration. ◦ Planifie l'ingestion des événements corrélés en cours. ◦ Active les mises à jour des événements corrélés lorsqu'un incident SIR est créé et fermé. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Les utilisateurs disposant du sn_si.analyst travaillent sur des incidents de sécurité. Pour plus d'informations sur les rôles et l'attribution de rôles aux utilisateurs, voir Rôles sur le site Web de la documentation produit ServiceNow .
Vérifiez que vous utilisez la ArcSight ESM version 7.0.0.2436 ou ultérieure du	Si vous avez accès à la ArcSight ESM visionneuse de requêtes, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
gestionnaire. Les versions antérieures ne sont pas prises en charge.	
Configurez la visionneuse de requêtes dans ArcSight ESM.	Avant de pouvoir ingérer des événements de corrélation, vous devez configurer la visionneuse de requêtes dans la ArcSight ESM console. Consultez Configurer la visionneuse de ArcSight ESM requêtes pour en savoir plus.
Optionnel Créez des étapes personnalisées pour les mises à jour d'événements de ArcSight ESM corrélation.	Un événement de corrélation passe par de nombreuses étapes dans son cycle de vie avant d'être fermé. ArcSight ESM fournit des étapes par défaut telles que Initial, Surveillance, Mis en file d'attente et Fermé. Certaines de ces étapes nécessitent des entrées de l'utilisateur, mais d'autres sont automatiquement appliquées à l'événement sans aucune intervention de l'utilisateur (le champ **Requis pour l'utilisateur** est décoché dans la ArcSight ESM console. Vous pouvez créer des étapes personnalisées qui ne nécessitent aucune intervention de l'utilisateur et les utiliser dans votre ServiceNow AI Platform® instance. Consultez Options supplémentaires : automatiser les mises à jour et la fermeture des événements corrélés en fonction de l'état SIR de l'incident pour en savoir plus.
Vérifiez que vous avez installé et configuré une application de Serveur MID.	Application de Serveur MID configurée Un Serveur MID dans votre ServiceNow AI Platform® instance est requis pour se connecter au ArcSight ESM service si le serveur est déployé au sein de ArcSight ESM votre réseau d'entreprise. Consultez pour Installer et configurer l'application ServiceNow pour l'intégration d'ingestion d'événements ArcSight ESM obtenir des instructions sur la configuration d'une application de Serveur MID. Voir Serveur MID pour plus d'informations sur les serveurs MID. Si vous utilisez un service hébergé ou dans le cloud, c'est-à-dire accessible par Internet, un serveur MID n'est pas nécessaire.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Ingestion d'événements et d'alertes pour Security Operations : Cette application nécessite :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	○ com.glide.hub.integration.runtime => Exécution du Centre d'intégration ServiceNow ○ com.glide.hub.action_step.rest => Étape d'action du Centre d'intégration ServiceNow : REST **5.** Threat Core Pour plus d'informations sur l'installation Opérations de sécurité des applications principales, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Que faire ensuite

Vous avez correctement configuré votre ServiceNow AI Platform® instance pour l'intégration. L'étape suivante consiste à installer l'application ArcSight ESM Ingestion d'événements de sécurité pour Security Operations à partir de ServiceNow Store pour l'intégration.

Configurer la visionneuse de ArcSight ESM requêtes

Créez une visionneuse de requêtes et définissez des filtres qui incluront les événements de corrélation récemment créés qui seront ingérés ServiceNow.

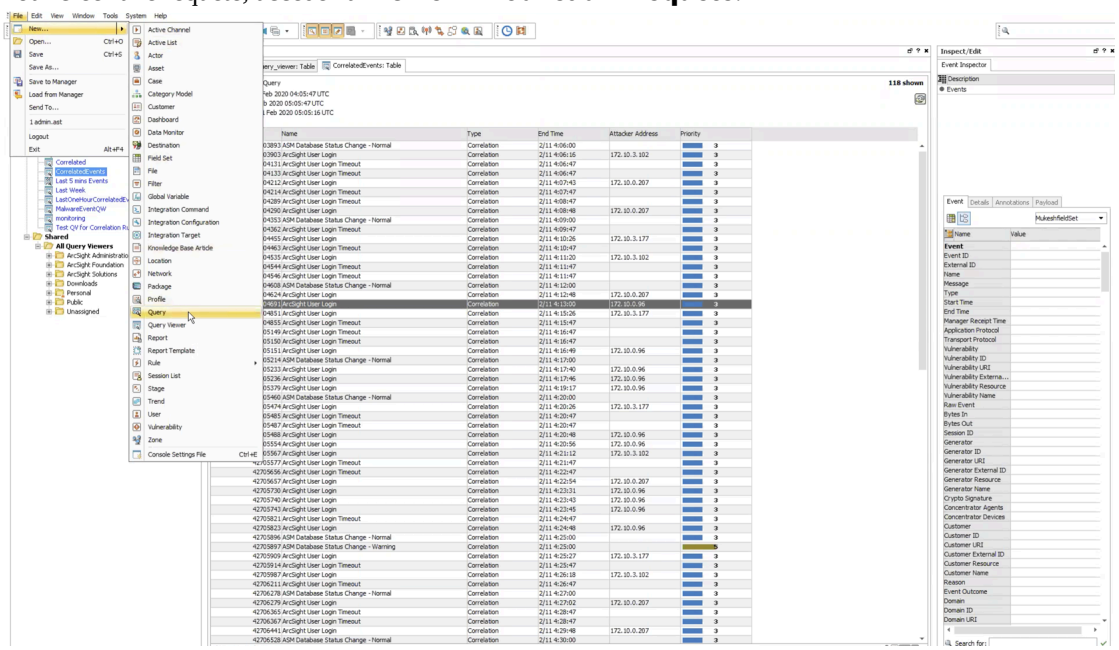
Avant de commencer

Rôle requis : Administrateur ArcSight

Procédure

1. Connectez-vous à la ArcSight ESM console pour créer une visionneuse de requêtes.

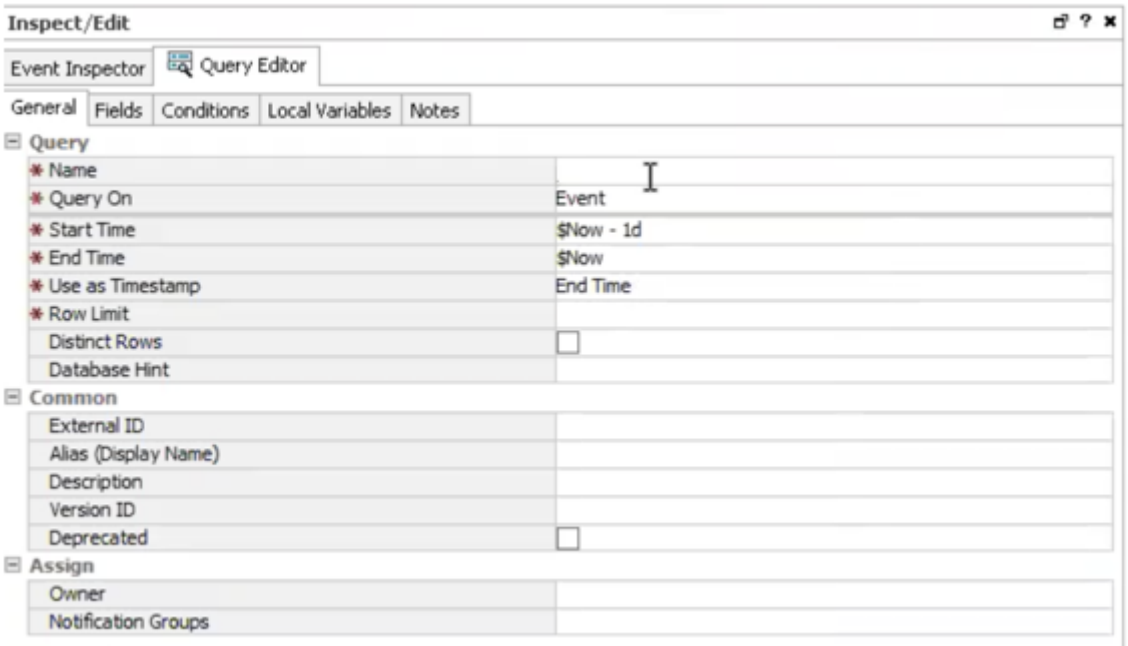
2. Pour créer une requête, accédez à **Fichier** > **Nouveau** > **Requête**.



3. Définissez des conditions pour la visionneuse de requêtes dans le panneau **Inspecter/Modifier** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

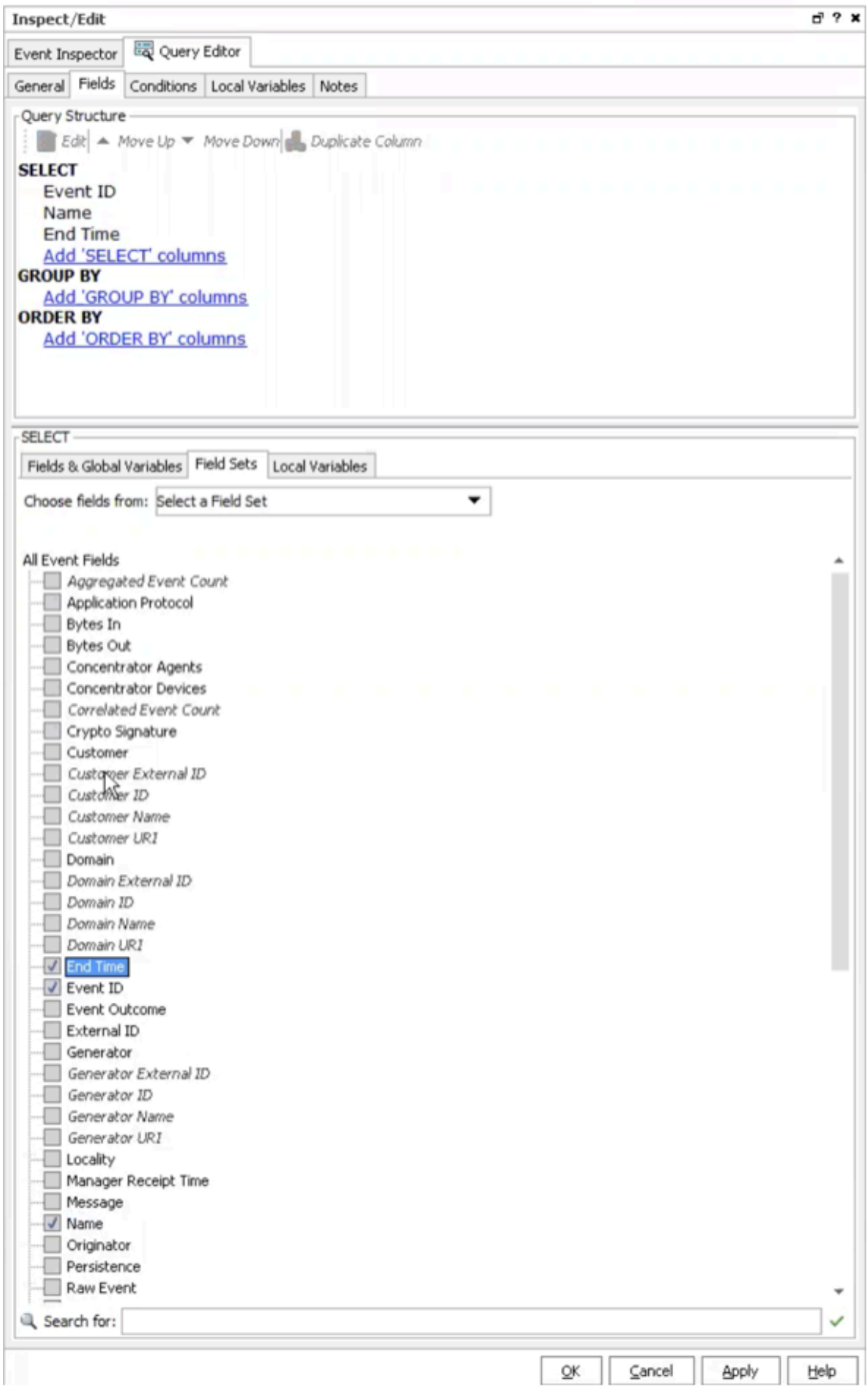


Nom de champ	Description
Nom	Entrez un nom pour la requête.
Requête sur	Sélectionnez **Événement** dans la liste déroulante.
Heure de début	Pour ingérer les données les plus récentes, sélectionnez la date des événements à ingérer. Spécifiez une date antérieure d'un jour ou de quelques jours à la date actuelle. **Remarque :** Vous ne pouvez pas spécifier une date antérieure de plus de 7 jours à la date actuelle. Si vous gérez un grand nombre d'événements, vous devez spécifier une date antérieure de 1 ou 2 jours à la date actuelle.
Heure de fin	Il s'agit de la date actuelle.
Limite de ligne	Nombre maximal d'événements pouvant être ingérés simultanément. Spécifiez une valeur inférieure à 5 000 ici.

4. Cliquez sur l'onglet **Champs** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

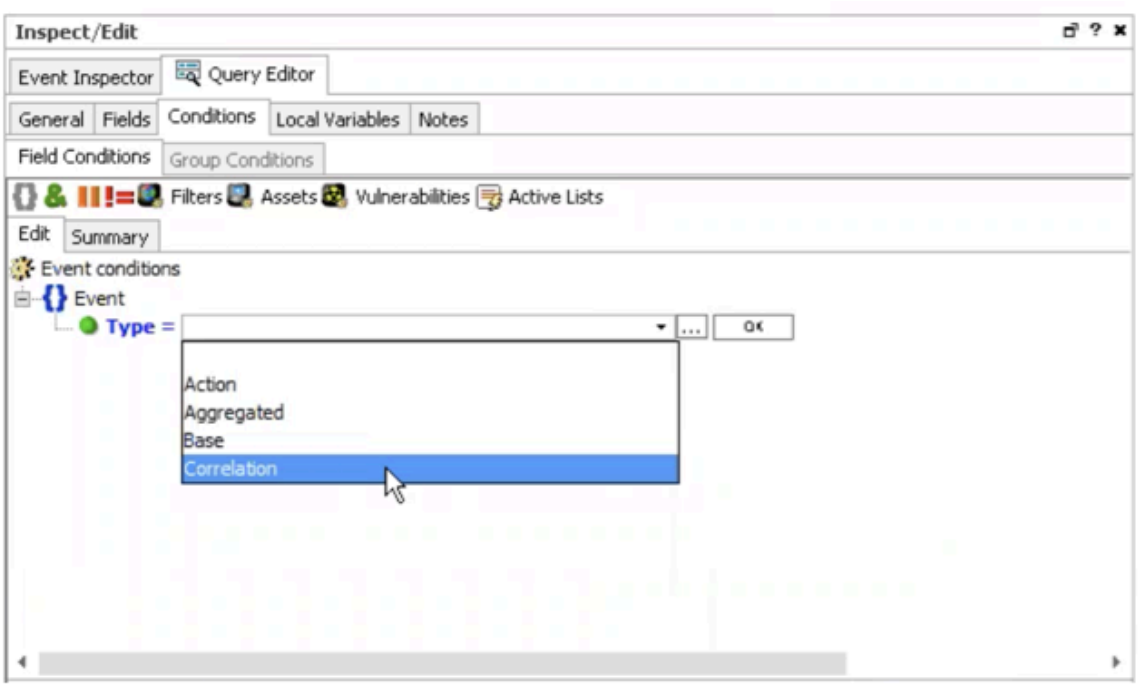


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez les champs qui doivent être inclus lors de l'ingestion.
   Pour que l'ingestion réussisse, vous devez sélectionner les champs *`ID de l'événement`*, *`Nom`* et *`Heure de fin`*.
6. Cliquez sur le lien **Ajouter des colonnes « TRIER PAR »,** sélectionnez le champ **ID d'événement** et spécifiez l'ordre de tri par **ordre décroissant** pour vous assurer que les derniers événements sont ingérés.
7. Cliquez sur l'onglet **Conditions** .
8. Cliquez avec le bouton droit sur **Événement** sous **Conditions d'événement** sous la section **Résumé** .
9. Cliquer sur **Nouvelle condition** > **Racine** > **Type** et sélectionnez le type d'événement comme **Corrélation**.

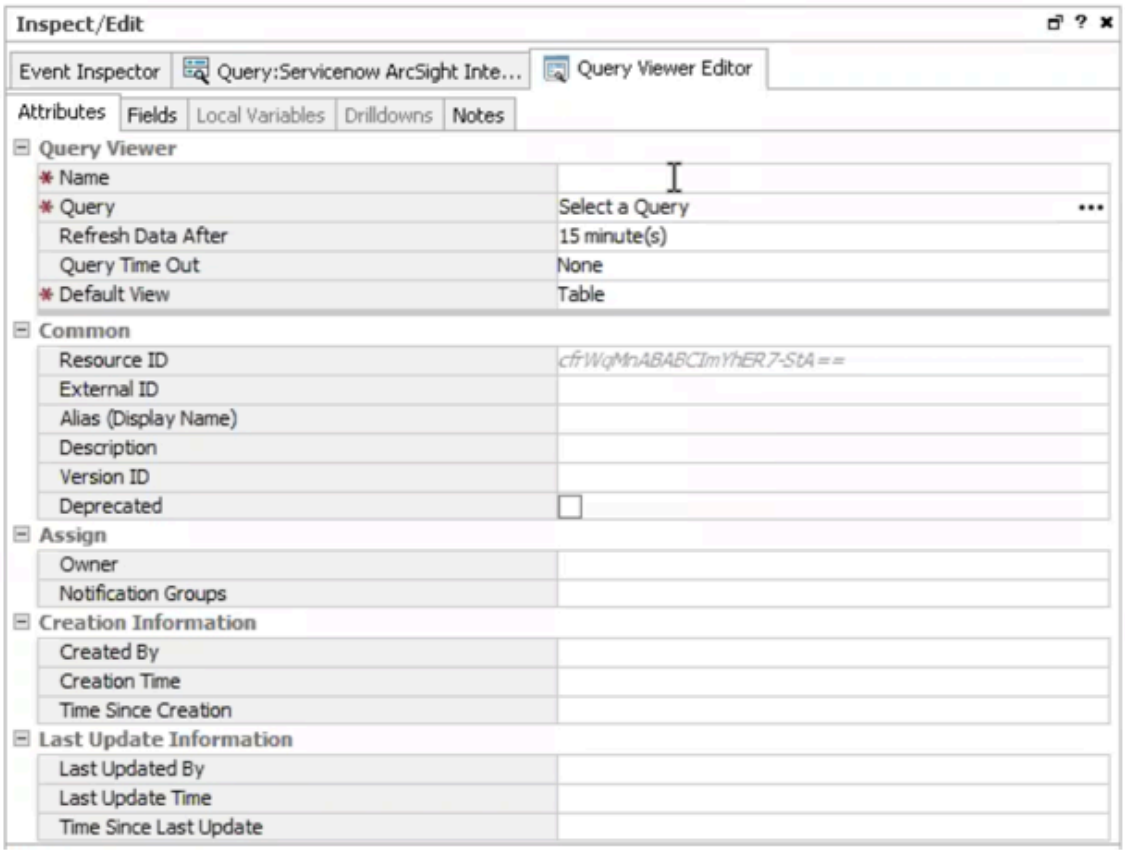
> **Important :** Seuls les événements de corrélation seront récupérés ; Les événements de base pour les corrélations ne seront pas récupérés.



10. Cliquez sur **OK** pour enregistrer la requête.
    L'étape suivante consiste à créer un visualiseur de requêtes pour cette requête.
11. Accédez à la **Fichier** > **Nouveau** > **Visionneuse de requête**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



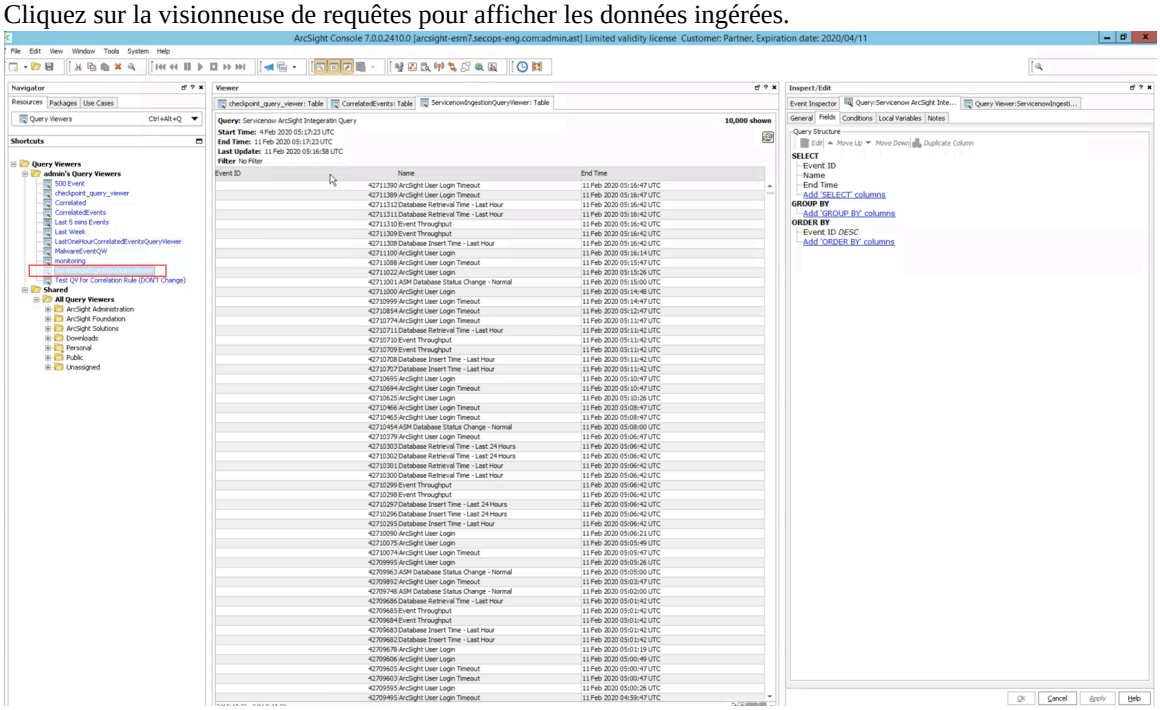
Nom de champ	Description
Nom	Entrez un nom pour la visionneuse de requêtes.
Requête	Sélectionnez la requête que vous venez de créer.
Actualiser les données après	Spécifiez la fréquence à laquelle les données doivent être actualisées.

12. Cliquez sur l'onglet **Champs** et assurez-vous que les champs obligatoires (*`ID d'événement`*, *`Nom`*, *`Heure de fin`*) que vous avez spécifiés dans votre requête sont sélectionnés.
13. Cliquez sur **Appliquer** pour enregistrer la visionneuse de requêtes.
    La nouvelle visionneuse de requêtes que vous avez créée est répertoriée dans la section Visionneuses de requêtes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

14. Cliquez sur la visionneuse de requêtes pour afficher les données ingérées.



Installer et configurer l'application ServiceNow pour l'intégration d'ingestion d'événements ArcSight ESM

Avant d'exécuter l'intégration sur votre ServiceNow AI Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre correctement aux Réponse aux incidents de sécurité produits sur Opérations de sécurité votre ServiceNow AI Platform instance.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si vous n'avez pas installé l'application ArcSight ESM à partir de pour ServiceNow Store l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la ArcSight ESM tuile.
3. Pour configurer l'application, cliquez sur **Nouveau**.
4. Sinon, si un bouton **Configurer** est affiché sur une tuile, cliquez dessus pour modifier une configuration existante.
5. Remplissez les champs du formulaire.

Champ	Description
Nom	Nom unique du gestionnaire, qui sera utilisé dans la ArcSight ESM configuration du profil d'intégration pour distinguer plusieurs ArcSight ESM sources de gestionnaire, si nécessaire. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL du point de terminaison d'API ArcSight	URL de votre ArcSight ESM serveur de gestionnaire. Notez que l'URL doit inclure le port de l'API, par exemple : https://arcsight-esm.com:8443
Nom d'utilisateur du compte API	Nom d'utilisateur que vous avez créé pour votre compte d'utilisateur d'API dans la console du ArcSight ESM gestionnaire.
Mot de passe de l'API	Mot de passe que vous avez créé pour votre compte d'utilisateur d'API dans la console du ArcSight ESM gestionnaire.
Déploiement sur site	Il n'est pas coché par défaut. Si vous utilisez la version cloud qui dispose d'un ArcSight ESM accès direct à Internet, vérifiez que la case est décochée. Pour un déploiement sur site, cochez cette case et spécifiez l'application Serveur MID.
Application de serveur MID	Spécifiez un nom d'application de Serveur MID ici. Cette application de Serveur MID peut pointer vers n'importe lequel des serveurs MID configurés et tout Serveur MID disponible sera utilisé. Si aucune application de Serveur MID n'est configurée, vous devez créer une nouvelle application de Serveur MID pour cette intégration. **Remarque :** L'application Serveur MID ne peut être configurée que par les utilisateurs ayant le rôle d'administrateur système.

Pour créer une application de Serveur MID, procédez comme suit :

a. Accédez à la **Serveur MID** > **Applications** et cliquez sur **Nouveau**.

b. Entrez un nom pour l'application de Serveur MID et sélectionnez un serveur MID à utiliser par défaut.

c. Décochez la case Inclus dans l'application TOUT et cliquez sur **Enregistrer**.

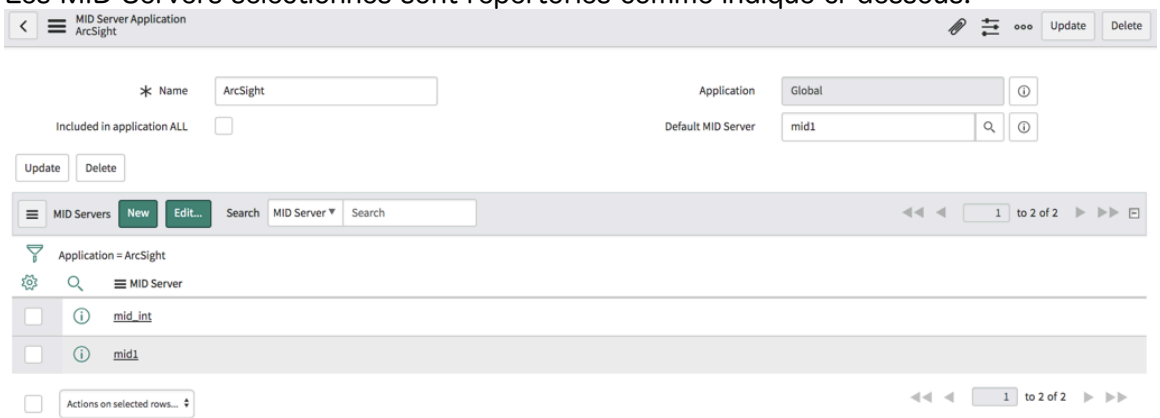


d. Cliquez sur **Modifier**. Dans la page **Modifier les membres** , sélectionnez tous les serveurs MID disponibles, déplacez-les vers la liste des serveurs MID, puis cliquez sur **Enregistrer**.

Traduction automatique

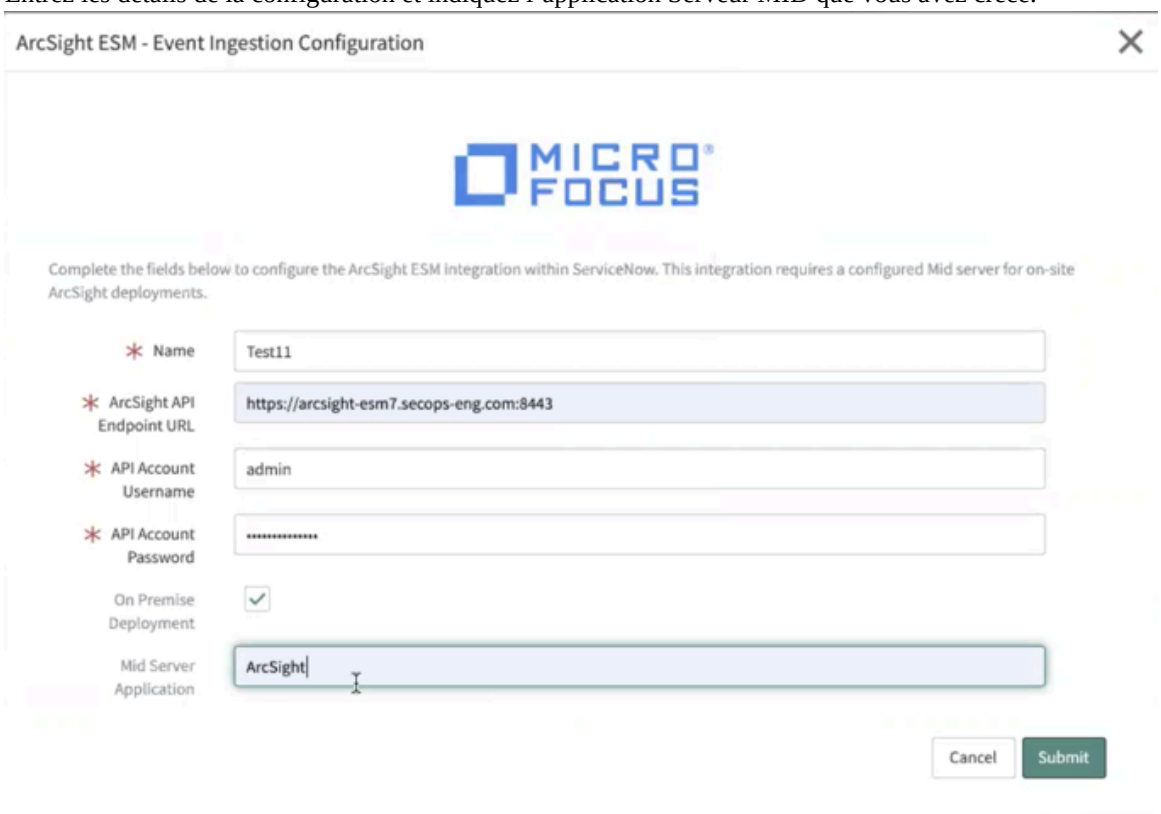
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Les MID Servers sélectionnés sont répertoriés comme indiqué ci-dessous.



En fonction de la disponibilité, l'un des MID Servers configurés avec l'application MID Server est utilisé.

6. Entrez les détails de la configuration et indiquez l'application Serveur MID que vous avez créée.



Chaque événement de corrélation que vous ingérez à partir de votre ArcSight ESM Manager Console nécessite un profil d'événement unique dans votre instance. Toutefois, la ArcSight ESM source que vous configurez dans le formulaire Configuration de l'ingestion d'événements peut être réutilisée pour plusieurs profils tant que chaque profil ingère des types d'événements de corrélation uniques.

7. Cliquez sur **Envoyer**.
Une fois validée et soumise, chaque ArcSight ESM configuration de serveur est enregistrée sur la page Intégrations de sécurité sous forme de tuile. Si les tuiles de configuration que vous avez enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste de choix Afficher les configurations, cliquez sur **Oui**.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer un profil d'événement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un profil

En tant qu'utilisateur disposant du rôle sn_si.admin, vous créez un profil dans votre ServiceNow AI Platform instance et déterminez quels événements de corrélation créent des incidents de sécurité. Avant ServiceNow AI Platform Réponse aux incidents de sécurité que les incidents de sécurité (SIR) ne soient créés à partir d'événements de corrélation, les valeurs de champ des événements sont affichées sur une mise en page d'un ServiceNow AI Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera créé.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Les événements de corrélation sont automatiquement ingérés dans l'environnement Opérations de sécurité de votre ServiceNow AI Platform instance en fonction du type de profil défini. Un profil est une encapsulation d'un type d'événement de corrélation comme les tentatives d'accès non autorisé ou les programmes malveillants.

Une fois qu'un événement de corrélation a été ingéré, vous pouvez mapper les champs d'événement de corrélation individuels aux champs correspondants de l'incident de sécurité. Vous pouvez filtrer les événements de corrélation pour spécifier quels événements créent des incidents de sécurité. Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les événements de corrélation identifiés comme à haut risque. Vous pouvez également définir des critères d'agrégation d'événements supplémentaires afin que les événements de corrélation en double entrants soient regroupés en un incident de sécurité ouvert. Enfin, vous pouvez définir un calendrier d'ingestion et activer le profil.

Les noms des profils d'événements dans votre ServiceNow AI Platform instance doivent être uniques et ne peuvent être mappés qu'à un seul profil d'événement actif à la fois.

Créer et nommer le profil pour ArcSight ESM l'intégration de l'ingestion d'événements

Vous pouvez configurer un profil pour ingérer des événements de corrélation.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Pour créer un profil d'événement pour un événement de corrélation dans votre ServiceNow AI Platform instance, accédez à **Intégration ArcSight ESM** > **Profil d'événement ArcSight ESM**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs.

Un exemple de formulaire rempli suit la table.

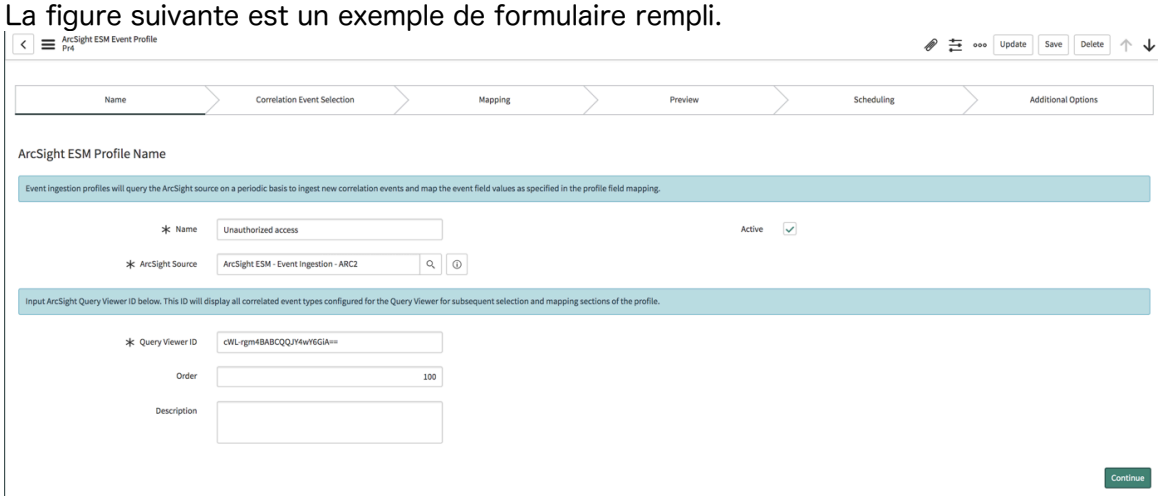
Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre ServiceNow AI Platform instance doivent être uniques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Heck Box est vide par défaut. Si cette option est désactivée, le profil n'est pas actif et l'ingestion n'aura pas lieu. **Remarque :** Vous devez remplir toutes les sections du profil avant de l'activer.
Source ArcSight	Serveur ArcSight ESM configuré lors de l'étape d'authentification initiale. Si plusieurs serveurs sont ArcSight ESM configurés, sélectionnez le serveur approprié pour les types d'événements de corrélation qui seront ingérés pour le profil. Vous devez sélectionner une valeur.
ID de la visionneuse de requête	Entrez l'ID de ressource de la visionneuse de requêtes configurée dans la ArcSight ESM console. L'ID de ressource est un identificateur unique pour toute visionneuse de requêtes configurée dans le serveur ArcSight ESM. Une fois l'ID de ressource soumis, le nom de la vue de requête est renvoyé pour s'assurer que la visionneuse de requêtes appropriée a été sélectionnée. Consultez la section ci-dessous pour une capture d'écran de la façon de déterminer l'ID de ressource pour la visionneuse de requêtes sélectionnée dans ArcSight ESM.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Le workflow dans le profil avec le numéro le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli.

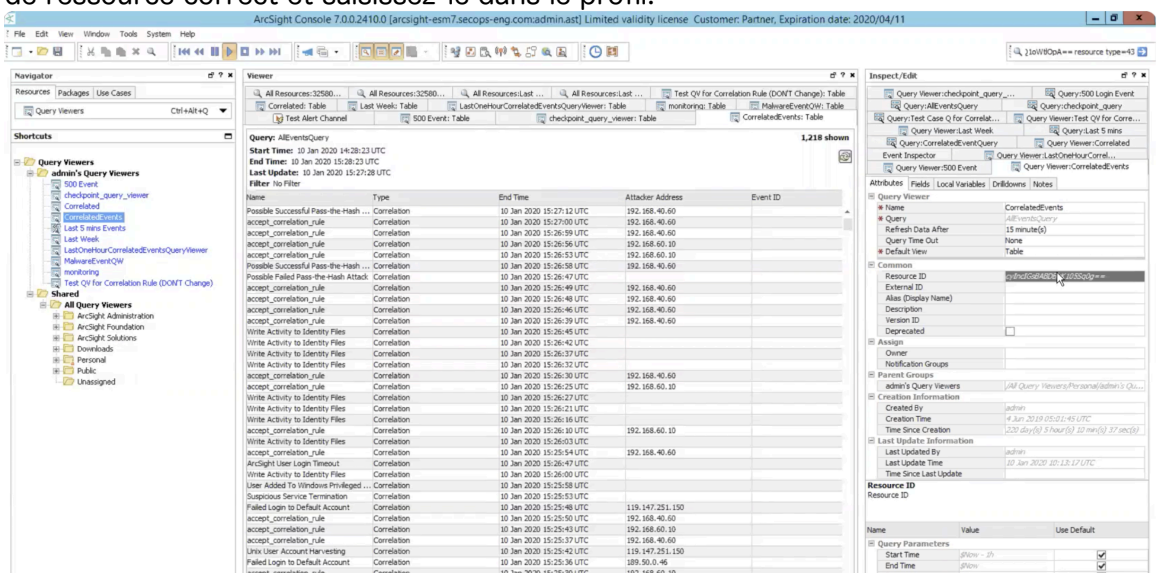


Une fois que vous avez saisi les détails du profil, cliquez sur **Continuer**. L'ID de la visionneuse de requêtes est validé et si un ID de ressource correspondant est présent

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

dans la ArcSight ESM visionneuse de requêtes, le nom de la visionneuse de requêtes est renvoyé comme indiqué ci-dessous. Si la validation échoue, vérifiez si l'ID de ressource existe dans la ArcSight ESM console. Si l'ID de ressource est introuvable, recherchez l'ID de ressource correct et saisissez-le dans le profil.



Que faire ensuite

L'étape suivante consiste à sélectionner les types d'événements de corrélation à ingérer dans la visionneuse de requêtes sélectionnée à l'étape précédente.

Sélectionner les événements de corrélation pour ArcSight ESM l'intégration de l'ingestion d'événements

En fonction de la source et de la ArcSight ESM visionneuse de requêtes configurées, sélectionnez une règle d'événement de corrélation pour le profil.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Affichez les événements de corrélation disponibles répertoriés dans la sélection d'événements de corrélation dans votre ServiceNow AI Platform instance afin de pouvoir déterminer les événements de corrélation que vous souhaitez ingérer et créer des incidents de sécurité. Vous ne pouvez sélectionner qu'un seul type de règle de corrélation dans la liste pour chaque profil.

L'ID et le nom de la visionneuse de requêtes, tels que spécifiés dans le formulaire Visionneuse de requêtes, s'affichent. Sélectionnez un événement de corrélation dans la liste que vous pouvez utiliser pour créer un mappage de configuration pour l'événement corrélé ingéré.

Cliquez sur la liste déroulante dans le champ Liste d'événements de corrélation. La liste des événements de corrélation présents dans la console de la visionneuse de requêtes s'affiche ArcSight ESM .

Cliquez sur **Continuer** pour passer à l'étape suivante de l'assistant.

Mappage des champs d'événement de corrélation pour l'intégration d'ingestion d'événements ArcSight ESM

Une fois que vous avez identifié la règle d'événement de corrélation spécifique dans la liste, l'étape suivante consiste à mapper les champs d'événement de corrélation aux champs du formulaire d'incident de sécurité.

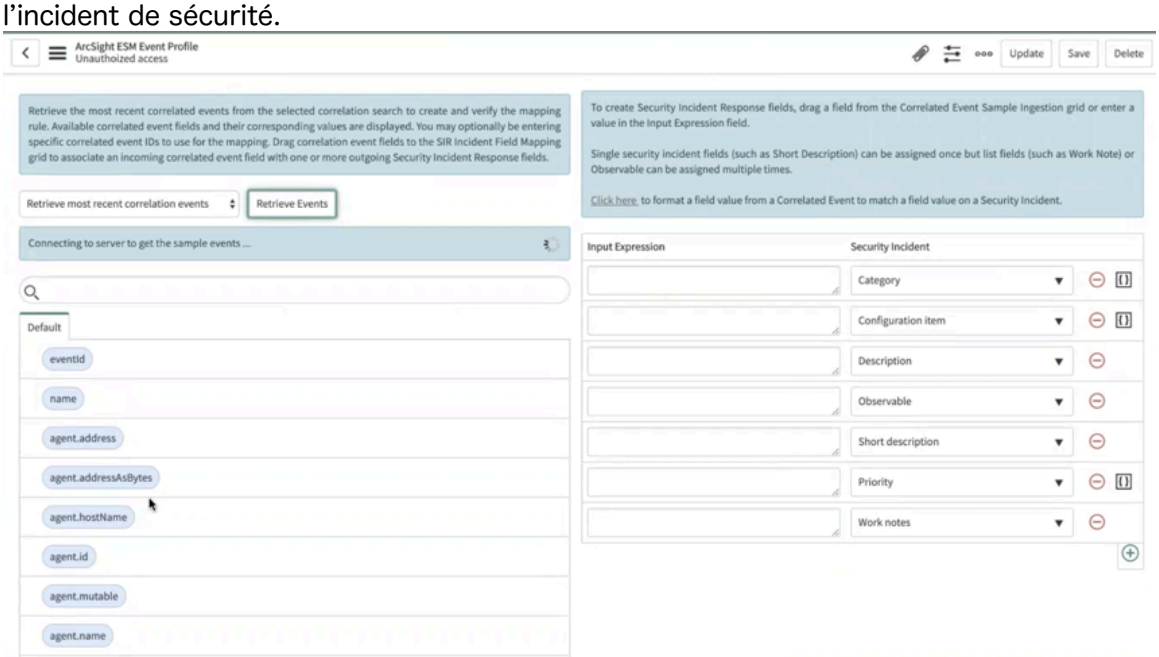
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble du mappage des champs d'événements de corrélation

Pour l'étape de mappage, vous pouvez ingérer des exemples d'événements de corrélation pour la règle de corrélation sélectionnée. Au cours de cette phase de mappage, vous pouvez vous assurer que toutes les données de champ d'événement de corrélation pertinentes sont mappées à l'endroit approprié sur le formulaire d'incident SIR , puis visualiser l'incident SIR dans la section d'aperçu.

La figure suivante montre la configuration de mappage par défaut fournie pour créer le profil d'événement de corrélation. Vous pouvez personnaliser les champs qui renseignent l'incident de sécurité.



Lorsque vous cliquez sur **Récupérer les événements**, les noms des champs d'événements de corrélation et les valeurs correspondantes sont renseignés sur le côté gauche du formulaire. Il s'agit des champs d'événement ArcSight ESM de corrélation qui peuvent être mappés aux champs d'incident de sécurité.

Vous préférez peut-être examiner quelques échantillons d'événements de corrélation sur votre console à ingérer pour l'étape de configuration du mappage de champ. Cette étape est étiquetée Mappage dans la barre de progression. Si cette page n'est pas affichée, cliquez sur **Mappage** dans la barre de progression. Vous pouvez ingérer jusqu'à cinq échantillons d'événements de corrélation à partir ArcSight ESM du gestionnaire pour la règle de corrélation sélectionnée afin de faciliter le processus de mappage de champ. Il existe des options permettant soit d'ingérer les cinq événements de corrélation les plus récents pour l'événement de corrélation sélectionné, soit d'ingérer jusqu'à cinq événements de corrélation spécifiques en fonction des ID d'événements.

Vous trouvez ci-dessous un résumé des étapes requises pour mapper des événements de corrélation :

- Mappage de champs : modifiez la configuration de mappage en faisant glisser les champs d'événements de corrélation du côté gauche et en les déposant dans la section de mappage d'incidents SIR à droite. Le mappage sur la droite associe le champ d'événement de corrélation entrant à un champ d'incident de sécurité sortant.
- Expérience de mappage : personnalisez la grille de mappage en ajoutant ou en supprimant des champs à l'aide de l'icône + située en bas de la section de mappage des champs d'incidents SIR. Suivez les champs négligés ou précédemment mappés avec

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le code couleur fourni (les champs mappés sont grisés, les champs bleus ne sont pas mappés).

- Conditions de génération d'incidents : une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de filtrer les événements de corrélation qui doivent créer des incidents de sécurité par rapport aux événements de corrélation qui doivent être filtrés, par exemple, les événements de corrélation de faible priorité. Cette opération est effectuée dans la section Conditions de génération d'incidents située sous la section Ingestion d'échantillons d'événements de corrélation.
- Critères d'agrégation d'événements : définissez des critères d'agrégation d'événements supplémentaires qui regroupent un événement de corrélation entrant à un incident de sécurité existant SIR au lieu de créer des incidents similaires, potentiellement en double. En utilisant des critères de correspondance de valeur de champ pour chaque profil, cette option d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'événement notables de sécurité connexes sur un seul incident de sécurité.
- Formater la traduction du champ : dans certains cas, les valeurs des champs d'événement dans l'événement ArcSight ESM de corrélation peuvent ne pas être directement traduites dans les champs de l'incident SIR de sécurité. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques.

  Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident de sécurité à l'aide de la SIR fonctionnalité Formater la traduction du champ.

L'étape suivante consiste à ingérer des exemples d'événements de corrélation et à mapper les valeurs aux champs d'incident SIR de sécurité.

Créer des mappages pour ArcSight ESM l'intégration de l'ingestion d'événements

Dans cette étape, vous ingérez des exemples d'événements de corrélation et mappez les valeurs aux champs d'incident de sécurité SIR.

Avant de commencer

Rôle requis : admin, sn_si.admin

Pourquoi et quand exécuter cette tâche

En tant qu'utilisateur disposant du rôle sn_si.admin, vous pouvez examiner jusqu'à cinq échantillons d'événements de corrélation à partir de la colonne Événement de corrélation Intégration d'exemples à gauche du formulaire pour faciliter le mappage et la traduction des valeurs de champ d'événement en champs d'incident de sécurité dans la colonne Mappage du champ d'incident SIR à droite.

Créez des mappages personnalisés en ajoutant ou en supprimant des champs sur la grille de mappage sur le côté droit du formulaire. Les champs affichés par défaut sont généralement des champs importants à renseigner sur le formulaire de réponse aux incidents de sécurité. Toutefois, ces champs peuvent être supprimés et tous les champs supplémentaires peuvent être affichés à l'aide des boutons + et -. Créez des cartes personnalisées en ajoutant ou en supprimant des champs sur la grille de mappage située à droite du formulaire. La personnalisation des champs vous permet de mapper ArcSight ESM les champs qui ne sont pas affichés sur la grille de mappage par défaut de l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

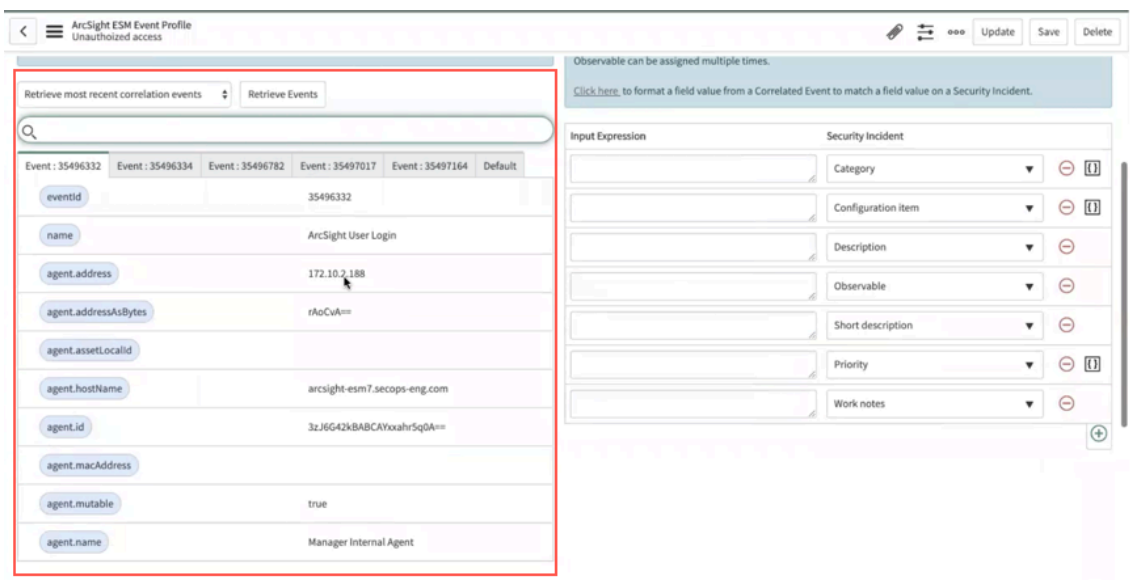
1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Vous pouvez soit extraire les échantillons d'événements de corrélation les plus récents pour la règle de corrélation sélectionnée, soit fournir les ID d'événements de corrélation uniques pour les événements de corrélation spécifiques que vous souhaitez utiliser pour votre expérience de mappage d'événements de corrélation.
3. Dans la liste déroulante, sélectionnez l'une des options suivantes :
   - Récupérer les événements de corrélation les plus récents
   - Sélectionner les événements de corrélation en fonction de l'ID d'événement

   Cliquez sur **Récupérer les événements** pour extraire les derniers échantillons d'événements de corrélation à partir de la ArcSight ESM console pour la règle de recherche de corrélation sélectionnée.

   Les résultats des champs et des valeurs d'événements de corrélation sont affichés sous forme d'onglets individuels.

   L'extraction des échantillons d'événements de corrélation peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran.

   Dans la figure suivante, les paires de valeurs de nom de champ de l'événement de corrélation ingéré ou des exemples d'événements importés s'affichent sur le côté gauche de ce formulaire une fois l'extraction d'ingestion terminée. Il s'agit des valeurs que vous mappez aux champs d'incident de sécurité du côté Mappage du champ d'incident SIR du formulaire.



4. Pour faire correspondre une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez tout en maintenant enfoncé le nom d'un champ bleu sur le côté gauche du formulaire.
5. Faites glisser le nom du champ, par exemple agent.hostname, et déposez-le sur un champ de la colonne Expression d'entrée à côté d'un nom de champ dans la colonne Incident de sécurité.

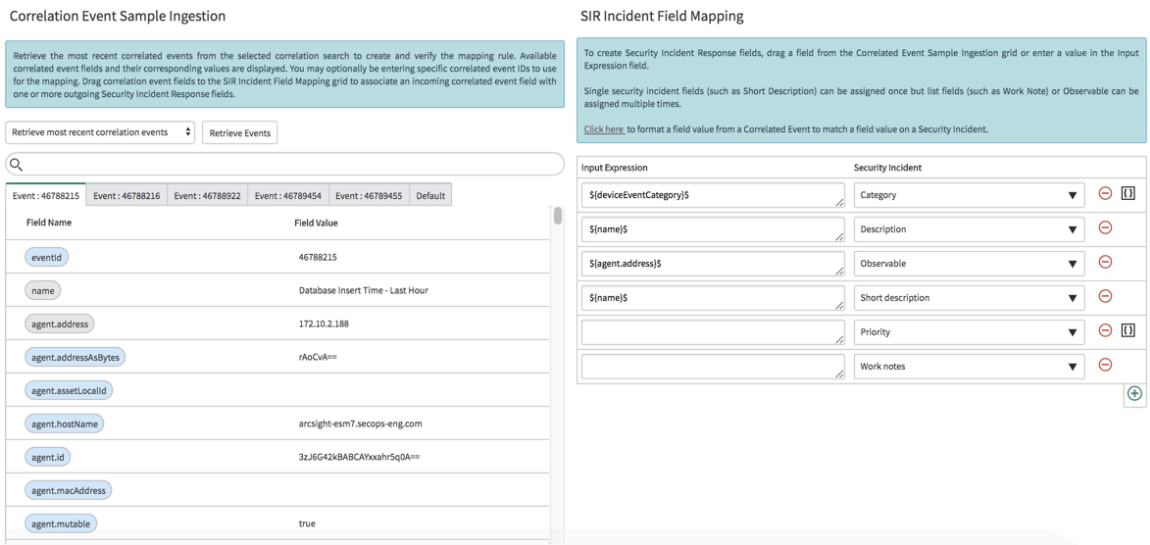
   Pour vous assurer qu'aucun champ d'événement n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Les champs bleu clair sur la gauche indiquent qu'un champ d'événement de corrélation n'est pas encore sélectionné

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ de corrélation entrant à plusieurs champs sur un incident de sécurité.

Un champ gris indique qu'un champ a été sélectionné et mappé à un champ de l'incident de sécurité. Ce code couleur vous aide à suivre les champs d'événements qui ont déjà été utilisés pour les futurs mappages de champs d'incidents de sécurité.

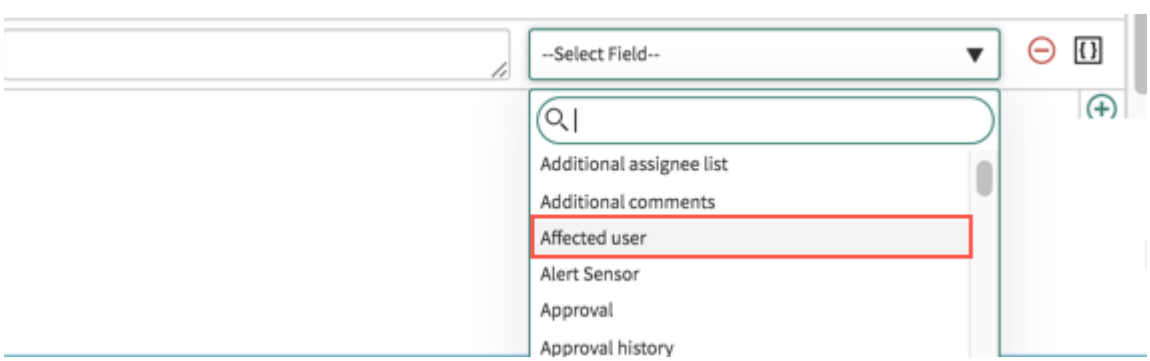


6. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit.

a. À droite du formulaire, dans la section Mappage du champ d'incidents SIR, au bas de la grille, cliquez sur l'icône plus.
Un nouveau champ s'affiche.

b. Dans la colonne Incident de sécurité, développez la liste de choix qui s'affiche, puis sélectionnez un champ.

Dans la liste de choix développée pour le nouveau champ, certains champs sont ombrés. Dans la figure suivante, l'utilisateur affecté a un arrière-plan gris, car il a été mappé dans l'incident de sécurité. Semblable au code couleur pour les champs d'événements de corrélation sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident SIR déjà mappés.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Afin que plusieurs observables puissent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs.
Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité possède une liste de choix dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste de choix, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher de la nouvelle ligne.

d. Sur le côté gauche du formulaire, cliquez avec le bouton gauche pour sélectionner **l'ID d'événement** souhaité dans le champ **expression d'entrée** .
Avec la fonction glisser-déposer, mappez-le à côté de votre nouveau champ.

7. Facultatif : Ouvrez l'éditeur de script et poursuivez la modification.

(Optional) Pour plus d'informations sur l'éditeur de script, reportez-vous à la section Utiliser l'éditeur de script pour formater les valeurs d'événements de corrélation.**Conditions de filtrage de génération d'incidents**

8. Facultatif : Une fois que vous avez terminé les étapes de mappage de champ précédentes, vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir des critères supplémentaires qu'un événement de corrélation entrant doit satisfaire pour créer un incident de SIR sécurité.
Pour définir les conditions de génération d'incidents, procédez comme suit.

a. Faites défiler la page jusqu'à la section Conditions de génération d'incidents sur le formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

(Optional) Le générateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

Les options des listes de choix pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'événements de corrélation pour les événements que vous avez ingérés. Ces champs sont dynamiques et changent en fonction des événements de corrélation que vous ingérez. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'événement ArcSight ESM de corrélation.

À l'aide des listes de choix et des champs du générateur de conditions, définissez des filtres pour la première ligne.

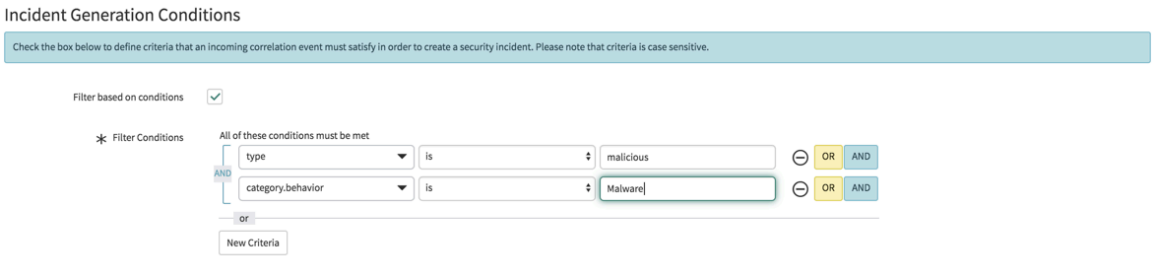
b. Pour ajouter plus de conditions, à droite des champs, cliquez sur **ET** ou **OU**.
Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

c. Facultatif : Sur la deuxième ligne, définissez une deuxième condition de filtre.

(Optional) L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création d'incidents de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



(Optional) Vous avez défini les conditions de génération d'incidents afin que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

Ce type de filtrage des conditions de génération d'incidents vous aide à affiner les événements de sécurité et à limiter le nombre d'incidents de sécurité inutiles que vous créez sans modifier la recherche de corrélation sous-jacente ou filtrer les événements dans ArcSight ESM. Si des critères de filtrage supplémentaires sont définis, seuls les événements de corrélation qui correspondent à tous les critères sont mappés aux incidents.

Remarque : Si l'un des noms de champs d'événements contient des caractères spéciaux tels que des guillemets («), des traits d'union ('), des traits de soulignement (-) ou des esperluettes (@), ces caractères devront peut-être être remplacés à des fins de mappage de traduction et éventuellement créer un nom d'événement en double. Le mappage peut être effectué de manière appropriée, mais un suffixe numérique est ajouté pour différencier les champs avec des noms d'événements en double. Par exemple, si le premier champ d'événement est `events.event` et le deuxième champ d'événement est `events.event`, ces champs ne peuvent pas être identifiés de façon unique, car les caractères de texte standard restants sont identiques. Dans ce cas, un suffixe est ajouté au deuxième champ d'événement et le champ est renommé en `events@event(1)`.

Critères d'agrégation d'événements pour gérer des événements de corrélation similaires et empêcher les incidents en double

9. **Facultatif :** Pour éviter de créer des incidents de sécurité en double, définissez des critères d'agrégation d'événements supplémentaires afin que les événements de corrélation entrants soient regroupés en un incident de sécurité ouvert.
   Pour définir les critères, procédez comme suit ci-dessous :

   a. Faites défiler la page jusqu'à la section **Critères d'agrégation d'événements** sur le formulaire et cochez la case Conditions d'agrégation pour activer cette option.

   (Optional) Les colonnes Valeurs correspondantes au champ Incident s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés sur l'incident SIR de sécurité.

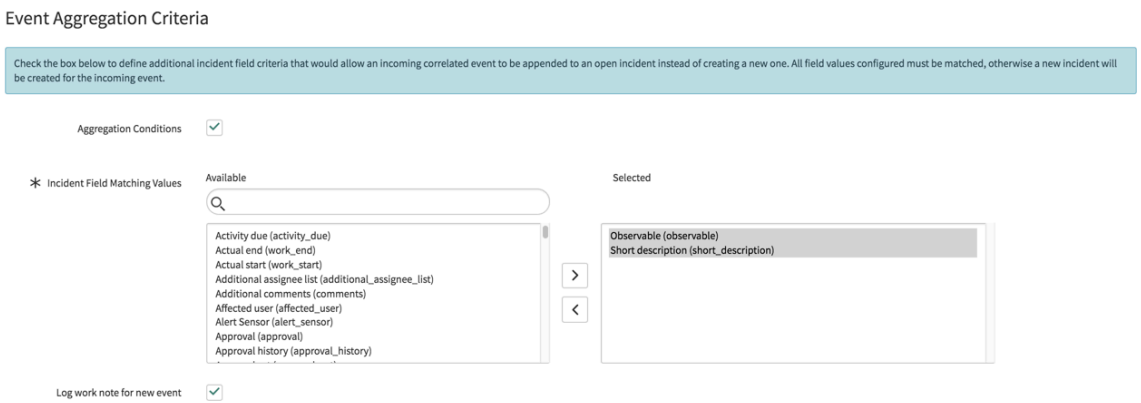
   b. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans ServiceNow AI Platform votre et déplacez-les vers la liste Sélectionné.

   (Optional) Toutes les valeurs de champ que vous sélectionnez doivent être mises en correspondance pour ajouter cet événement de corrélation entrant à un incident de sécurité existant. Cela inclut les champs, tels que les observables et les éléments de configuration, auxquels plusieurs valeurs de champs d'événements de corrélation peuvent être mappées. Toutes les valeurs doivent correspondre. Si seul un sous-ensemble de valeurs correspond, les conditions d'agrégation d'événements ne seront

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

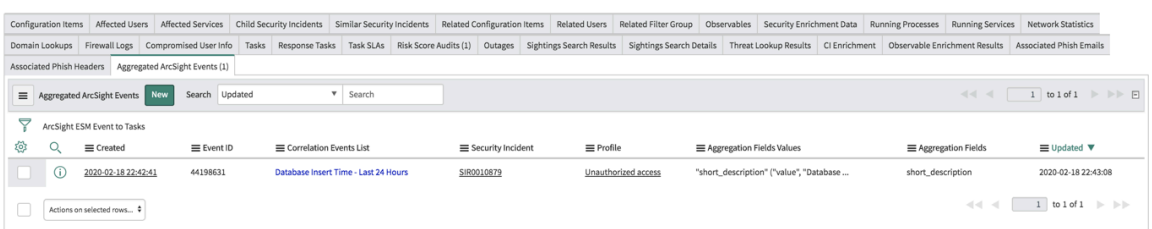
pas remplies et un nouvel incident de sécurité sera créé. Voir la capture d'écran ci-dessous pour le mappage de champs à valeurs multiples.



Si un nouvel événement de corrélation correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation à l'étape de mappage, le nouvel événement de corrélation est automatiquement ajouté à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'analyste SOC travaillant sur des incidents de sécurité, vous pouvez afficher tous les événements de corrélation agrégés ajoutés sur une liste connexe d'un incident de sécurité. Tous les événements de corrélation agrégés sur un incident de sécurité sont affichés dans la liste connexe **Événements ArcSight agrégés** . Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi ces événements de corrélation sont regroupés aux incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous **Liens connexes** et cliquez sur le lien **Afficher toutes les listes connexes** .

Remarque : Si vous ne voyez pas cette liste connexe, procédez comme suit :

- Cliquez avec le bouton droit sur l'en-tête du formulaire Incident de sécurité, puis cliquez sur **Configurer** > **Listes connexes**.
- Sélectionnez **Événements ArcSight agrégés** dans la liste Disponible, déplacez-le vers la liste Sélectionné et cliquez sur **Enregistrer**.
- Cliquez sur **Afficher les listes connexes**. L'onglet **Événements ArcSight agrégés** s'affiche maintenant dans la section Liste connexe.



c. Facultatif : Pour consigner une note de travail chaque fois qu'un événement est regroupé sur l'incident de sécurité, cochez la case pour activer cette option.
La note de travail indique qu'un nouvel événement corrélé a été ajouté ainsi qu'un lien vers les détails de l'événement corrélé.

Vous avez mappé avec succès les valeurs d'un événement de corrélation aux champs d'un SIR incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage de génération d'incidents. Vous avez également agrégé des événements

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de corrélation avec des incidents de sécurité existants SIR lorsque les valeurs de champ d'événement correspondent aux critères d'agrégation configurés.

10. Choisissez-en un pour poursuivre la configuration du profil.

Option	Description
Continuer	Le formulaire Mappage s'affiche. **L'aperçu** est sélectionné dans la barre de progression. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements s'affiche ArcSight ESM .
Précédent	Le formulaire Sélection d'événement de corrélation s'affiche.
Supprimer	Supprimez ce profil d'événement pour afficher la liste des profils d'événement.

Prévisualiser l'incident de sécurité pour l'intégration d'événement ArcSight ESM

Une fois l'étape de mappage terminée, affichez un aperçu des valeurs que vous avez mappées dans un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR). Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs de corrélation que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin.

Pourquoi et quand exécuter cette tâche

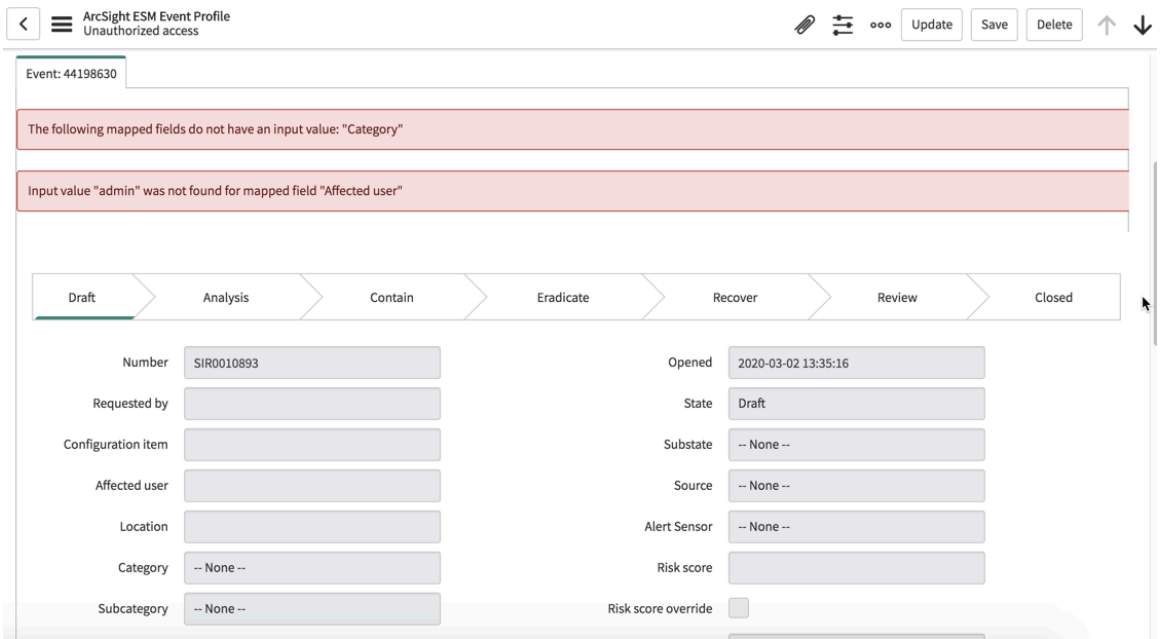
En tant qu'utilisateur disposant du rôle sn_si.admin, prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs erronés ou pour renseigner les données manquantes. Si l'aperçu n'est pas effectué avec succès, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de sécurité ne sont pas enregistrés en tant qu'incidents réels dans le Réponse aux incidents de sécurité produit.

Procédure

1. Si l'aperçu de l'incident de sécurité ne s'affiche pas, cliquez sur **Aperçu** dans la barre de progression.
2. Dans la liste de choix ID d'exemples d'événements, sélectionnez un élément.
   L'incident de sécurité s'affiche. Ne modifiez aucune information dans les champs. Cette vue est en lecture seule et aucun enregistrement de cet incident de sécurité n'est enregistré.
3. Examinez le mappage de champs des valeurs d'événements de corrélation sur l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'image précédente est un exemple d'aperçu avec une erreur de mappage. Dans cet exemple, une valeur de champ de l'événement de corrélation n'a pas de valeur acceptable pour le champ de référence sur le formulaire d'incident SIR. Un message d'erreur s'affiche indiquant qu'une valeur d'entrée n'a pas été trouvée pour le champ Catégorie qui est un champ de référence avec un ensemble spécifique de valeurs. Par conséquent, la valeur de ce champ mappé n'apparaîtra pas sur le formulaire d'incident SIR de sécurité sans autre modification.

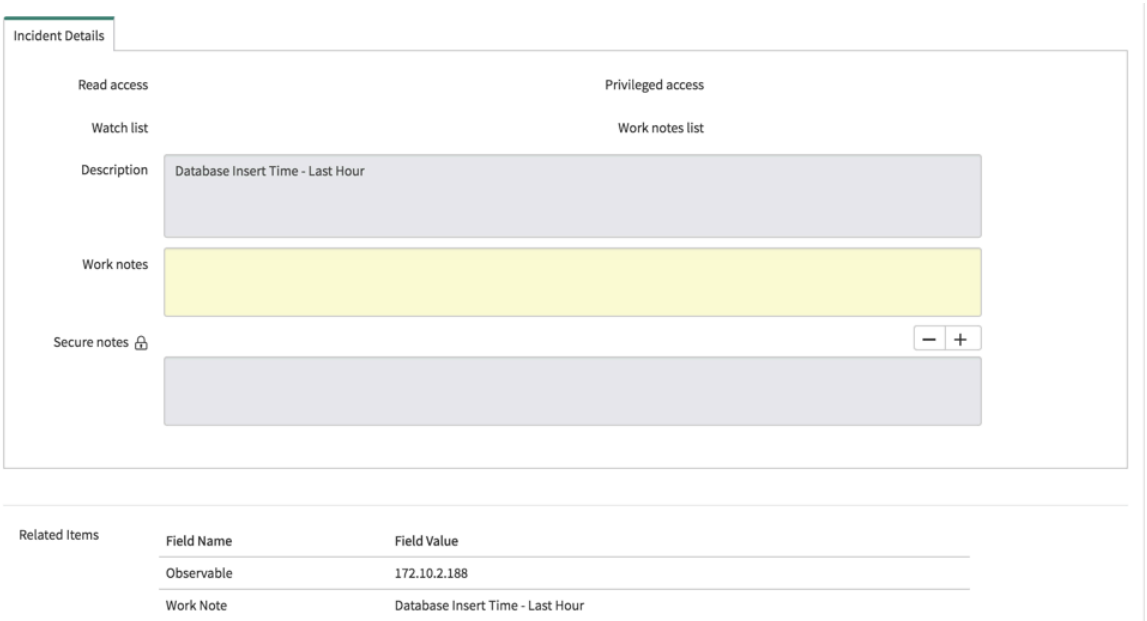
4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

La figure suivante est un exemple d'onglet Détails de l'incident dans la moitié inférieure d'un incident de sécurité une fois que tous les messages d'erreur ont été résolus. Pour cet exemple, les champs Description et Notes de travail ont été mappés, et ces

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

champs sont renseignés avec les valeurs des paires de valeurs extraites des échantillons d'événements de corrélation ArcSight ESM .



Que faire ensuite

Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à définir le calendrier.

Créer un calendrier pour ArcSight ESM l'ingestion d'événements

Vous pouvez définir la planification d'interrogation ou d'extraction pour les nouveaux événements corrélés. Au cours de cette étape, vous pouvez vérifier les paramètres existants pour la récupération de l'événement de corrélation ou modifier la planification si nécessaire. Cette étape vous permet également de récupérer les événements de corrélation historiques à l'aide d'une plage de dates.

Avant de commencer

Rôle requis : sn_si.admin.

Pourquoi et quand exécuter cette tâche

Vous pouvez choisir d'ingérer des événements de corrélation historiques pendant l'étape de planification. Vous choisissez également la fréquence à laquelle vous interrogerez les nouveaux événements de corrélation futurs qui correspondent à la configuration du profil.

En tant qu'utilisateur disposant du rôle sn_si.admin, vous configurez ces intervalles d'interrogation pour chaque profil. Les performances de l'intégration de l'ingestion ArcSight ESM d'événements de corrélation peuvent être impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférerez peut-être trouver un équilibre entre la réduction de la surcharge d'interrogation sur le serveur et le ArcSight ESM désir d'être averti dès que possible lorsqu'un événement est créé ou mis à jour. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférez peut-être modifier ce paramètre à une minute si nécessaire.

Extraction d'événements de corrélation nouveaux et mis à jour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

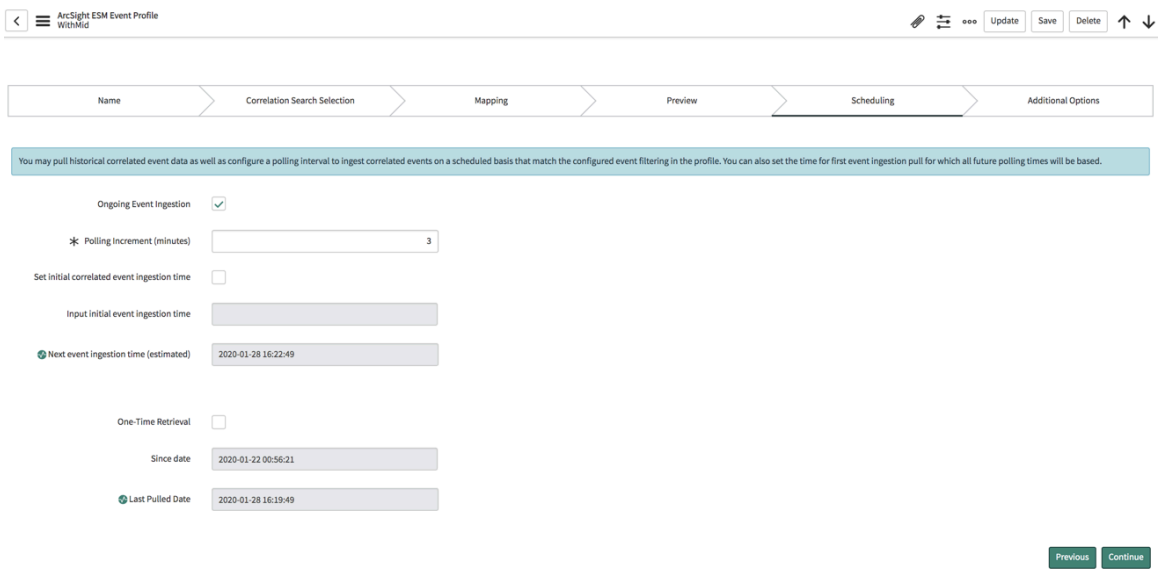
Procédure

1. Si la page Planification de la barre de progression ne s'affiche pas, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les événements de corrélation sont extraits de la console <ArcSight>.

Option	Description
◦ Champ d'ingestion d'événements en cours sélectionné ◦ Champ Récupération ponctuelle effacé	Événement en cours En fonction du paramètre par défaut, l'instance ServiceNow AI Platform extrait du ArcSight ESM serveur de nouveaux événements de corrélation toutes les cinq minutes. Les incidents de sécurité sont créés si des événements de corrélation sont trouvés et que les critères de filtrage de génération d'incidents correspondent. Pour équilibrer le désir d'obtenir les données les plus récentes, le paramètre par défaut est de cinq minutes. Toutefois, cette valeur peut être réduite à une minute si nécessaire.
◦ Champ d'ingestion de l'événement en cours effacé ◦ Champ de récupération ponctuelle sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez une extraction ponctuelle pour ingérer des événements de corrélation historiques. Lorsque ce paramètre est configuré, un profil est utilisé une fois pour récupérer les événements de corrélation à partir d'événements historiques basés sur une plage de dates. À droite du champ Depuis la date, cliquez sur l'icône Calendrier. Dans le calendrier qui s'affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire des alertes. À partir de la valeur Depuis la date, les événements de corrélation sont récupérés jusqu'à la date actuelle. Notez que vous pouvez récupérer des événements jusqu'à sept jours en arrière à partir de la date actuelle. Cette fonctionnalité n'est pas destinée à récupérer un nombre important d'événements historiques pour des raisons d'archivage, mais plutôt un nombre minimal d'événements en cours qui sont activement traités au moment de l'activation du profil. Une fois les événements de corrélation extraits, ce paramètre ne récupère plus d'événements de corrélation pour ce profil à partir de la date actuelle. Ce paramètre renseigne l'incident de sécurité avec tous les événements de corrélation trouvés pour la plage que vous saisissez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Par exemple, pour planifier un délai d'ingestion d'événement de corrélation initial, si vous avez un contrôle de sécurité quotidien ArcSight ESM qui s'exécute une fois par jour à 4 h (heure locale), vous pouvez configurer le profil d'événement de corrélation correspondant dans votre ServiceNow AI Platform instance pour qu'il s'exécute à 4 h 05, heure locale, afin de capturer immédiatement l'événement de défaillance de sécurité et de créer un incident de sécurité. Saisissez `04 05 00` dans le champ Ingestion de l'événement initial. Dans le champ Incrémentation (minutes), saisissez `1 440` (24 heures) pour planifier la prochaine ingestion d'événement pendant 24 heures à compter de l'ingestion d'événement initiale. Le délai d'ingestion de l'événement initial et l'heure d'ingestion de l'événement suivant sont affichés dans les champs.

3. Pour configurer les paramètres de cet exemple, procédez comme suit.

   a. Une fois la page Planification affichée, cochez la case **Ingestion d'événements en cours** pour activer cette option.

   b. Dans le champ Incrémentation (minutes), saisissez `1 440` (24 heures).

   c. Cochez la case **Définir le délai d'ingestion des événements corrélés initiaux** pour activer la modification des champs Ingestion d'événement initial et Ingestion de l'événement suivant.

   d. Dans le champ Délai d'ingestion de l'événement initial, saisissez `04 05 00`.
   Dans le champ Délai d'ingestion de l'événement suivant (estimé), l'heure de l'ingestion de l'événement suivant s'affiche.

4. Cliquez sur **Continuer** pour accéder à la page Options supplémentaires.

   Remarque : Le nombre par défaut d'incidents de sécurité qui peuvent être créés et regroupés en une journée, ainsi que la période de flux sont définis dans les paramètres d'intégration ArcSight ESM . Vous pouvez modifier ces paramètres si nécessaire. Consultez ArcSight ESM Paramètres d'intégration pour l'intégration de l'ingestion d'événements pour en savoir plus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Options supplémentaires : automatiser les mises à jour et la fermeture des événements corrélés en fonction de l'état SIR de l'incident

L'intégration ArcSight ESM dispose d'une interface bidirectionnelle qui permet à la fois aux événements de corrélation de créer des incidents de sécurité, ainsi qu'à la possibilité de mettre à jour les événements de corrélation une fois l'incident de sécurité créé et/ou fermé avec les détails pertinents de l'incident tels que le numéro de l'incident de sécurité, le groupe d'affectation, SIR l'URL de l'incident, etc.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si la page Options supplémentaires de la barre de progression ne s'affiche pas, sélectionnez **Options supplémentaires**.
2. Suivez les instructions ci-dessous pour terminer la configuration de la mise à jour des événements corrélés lors de la création de l'incident de sécurité.

Option ou champ	Description
Mettre à jour les événements corrélés lors de la création d'incidents SIR	Sélectionnez cette option si vous souhaitez mettre à jour l'étape ArcSight ESM d'événement de corrélation et mettre à jour l'événement avec des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'événement de corrélation. Cela peut se produire pour des événements de corrélation qui pourraient soit créer un nouvel incident de sécurité, soit regrouper des incidents de sécurité existants. **Remarque :** Si cette option n'est pas sélectionnée, l'étape de l'événement ne sera pas mise à jour lors de la création de l'incident de sécurité.
Mise à jour de l'étape d'événement corrélé	Sélectionnez une option d'étape dans la liste de choix d'étapes d'événements corrélés Mettre à jour qui affiche toutes les étapes disponibles récupérées à partir du ArcSight ESM serveur.

Étape d'événement corrélé non configurée : si vous n'avez configuré aucune étape d'événement corrélé dans votre ServiceNow AI Platform instance, vous ne verrez que **l'étape d'affectation : configuration initiale** dans la liste de choix Mise à jour de l'étape d'événement corrélé. Pour configurer l'étape, procédez comme suit :

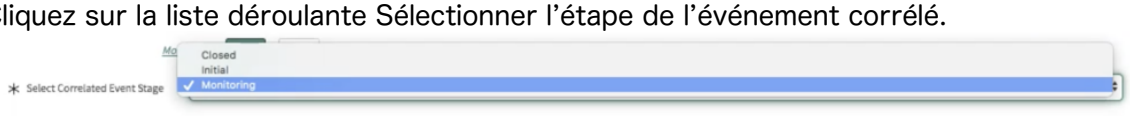
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Entrez un ID de ressource dans le champ Entrer l'ID de ressource d'étape et cliquez sur **Soumettre**. L'ID de ressource est validé dans la ArcSight ESM console et l'écran suivant s'affiche.



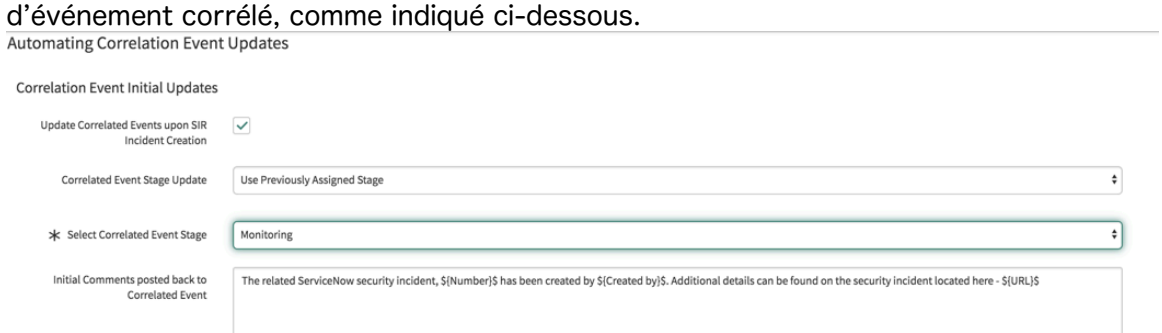
- Cliquez sur **Enregistrer** pour enregistrer la nouvelle étape (**Surveillance**).
- Cliquez sur la liste déroulante Sélectionner l'étape de l'événement corrélé.



- Vous pouvez sélectionner l'étape nouvellement créée dans la liste.

Étape d'événement corrélé déjà configurée : si vous avez déjà configuré l'étape d'événement corrélé, procédez comme suit :

- Sélectionnez **Utiliser l'étape précédemment affectée** dans la liste de choix de mise à jour de l'étape d'événement corrélé.
- Sélectionnez une étape existante dans la liste de choix Sélectionner l'étape d'événement corrélé, comme indiqué ci-dessous.



- Commentaires initiaux publiés sur l'événement corrélé : en plus de mettre à jour la valeur de l'étape de l'événement de corrélation, vous pouvez également publier des commentaires sur les annotations de l'étape de corrélation. Comme indiqué dans les instructions, vous pouvez modifier le texte par défaut affiché dans la section Commentaires, y compris ajouter ou modifier les variables de substitution en utilisant le format ${nom de champ}$ pour n'importe quel champ sur le formulaire d'incident de Réponse aux incidents de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez utiliser les étapes par défaut définies dans la ArcSight ESM console ou créer vos propres étapes personnalisées. Pour créer une étape, procédez comme suit :

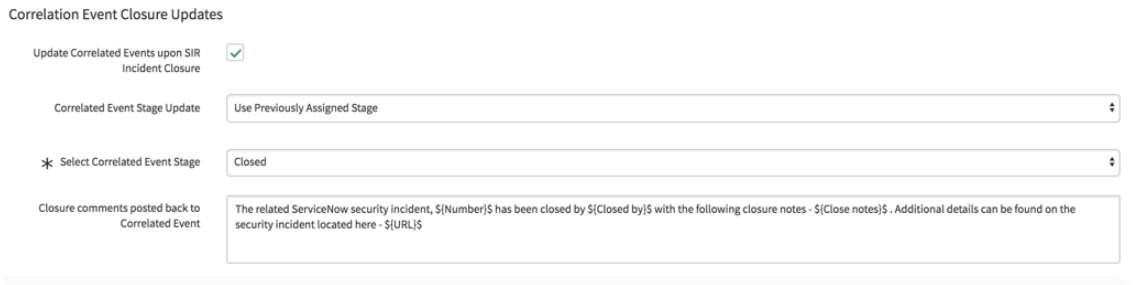
- Dans la ArcSight ESM console, sélectionnez **Fichier** > **Nouveau** > **Étape**. L'onglet Inspecter/Modifier s'affiche.
- Définissez la nouvelle étape et ne cochez pas la case **Utilisateur requis** . Assurez-vous que l'étape est définie correctement et qu'elle se trouve à la bonne position dans le cycle de vie de l'événement.

3. Dans la section Automatisation de la fermeture des événements corrélés, vous pouvez définir comment mettre à jour l'incident de sécurité lorsqu'il est fermé.
4. Remplissez les champs du formulaire.

Option ou champ	Description
Mettre à jour les événements corrélés lors de la fermeture d'incidents SIR	Sélectionnez cette option si vous souhaitez mettre à jour l'état de l'événement de corrélation et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est fermé à partir de l'événement corrélé. Cela se produit à la fois pour les événements notables déclencheurs initiaux qui créent l'incident de sécurité et pour les événements agrégés. **Remarque :** Si cette option n'est pas sélectionnée, l'étape de l'événement ne sera pas mise à jour lorsque l'incident de sécurité sera clôturé.
Mise à jour de l'étape d'événement corrélé	Sélectionnez une option d'étape dans le menu qui affiche toutes les étapes disponibles récupérées à partir du ArcSight ESM serveur. Sélectionnez la valeur d'étape à définir pour tous les événements de corrélation lorsqu'un incident de sécurité doit être fermé. **Remarque :** Les étapes affichées ici sont basées sur les étapes configurées dans la section Mises à jour initiales de l'événement de corrélation.
Sélectionner l'étape d'événement corrélé	Sélectionnez un état approprié ici.
Commentaires de fermeture republiés sur l'événement corrélé	Outre la mise à jour de la valeur de l'état de l'événement de corrélation, vous pouvez également publier des commentaires de fermeture dans les annotations d'événement de corrélation. Comme indiqué dans les instructions, vous pouvez modifier le texte par défaut affiché dans la section Commentaires, y compris ajouter ou modifier les variables de substitution en utilisant le format ${nom de champ}$ pour n'importe quel champ sur le formulaire d'incident de Réponse aux incidents de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



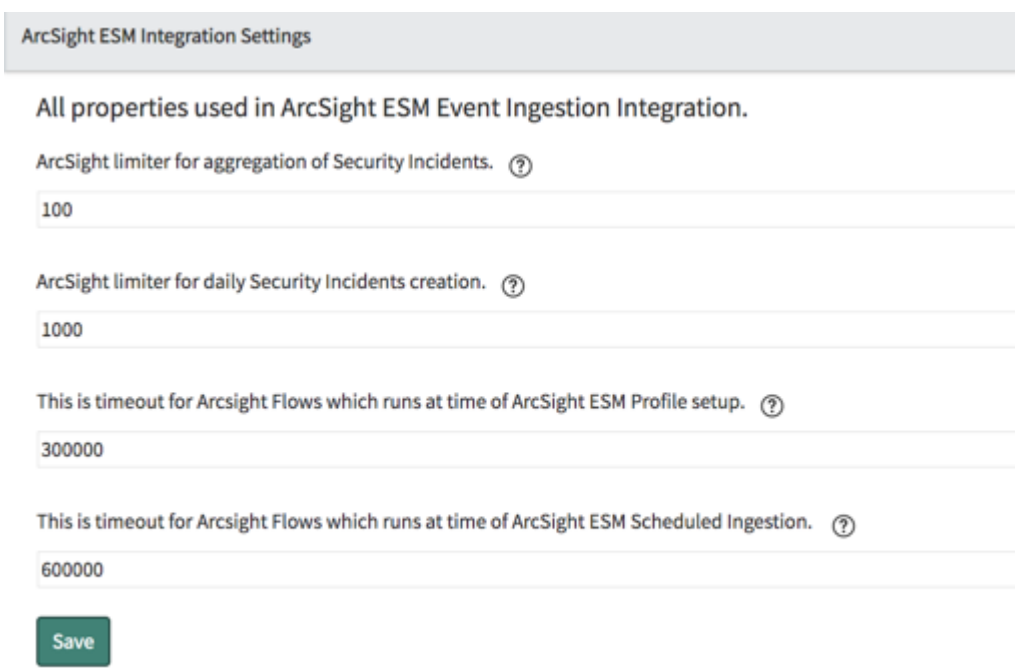
5. Cliquez sur **Terminer** pour terminer la configuration.
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Activez ce profil pour extraire des événements de corrélation de la ArcSight ESM console en fonction de votre planification.

ArcSight ESM Paramètres d'intégration pour l'intégration de l'ingestion d'événements

Utilisez cette option pour modifier les paramètres d'ingestion ArcSight ESM par défaut.

Pour modifier les propriétés système, connectez-vous en tant qu'utilisateur disposant du rôle *sn_si.admin* et accédez à **Intégration ArcSight ESM** > **Paramètres d'intégration ArcSight ESM**.

Les paramètres de configuration par défaut s'affichent. Vous pouvez modifier ces paramètres si nécessaire.



Dépannage de ArcSight ESM l'intégration d'ingestion d'événements

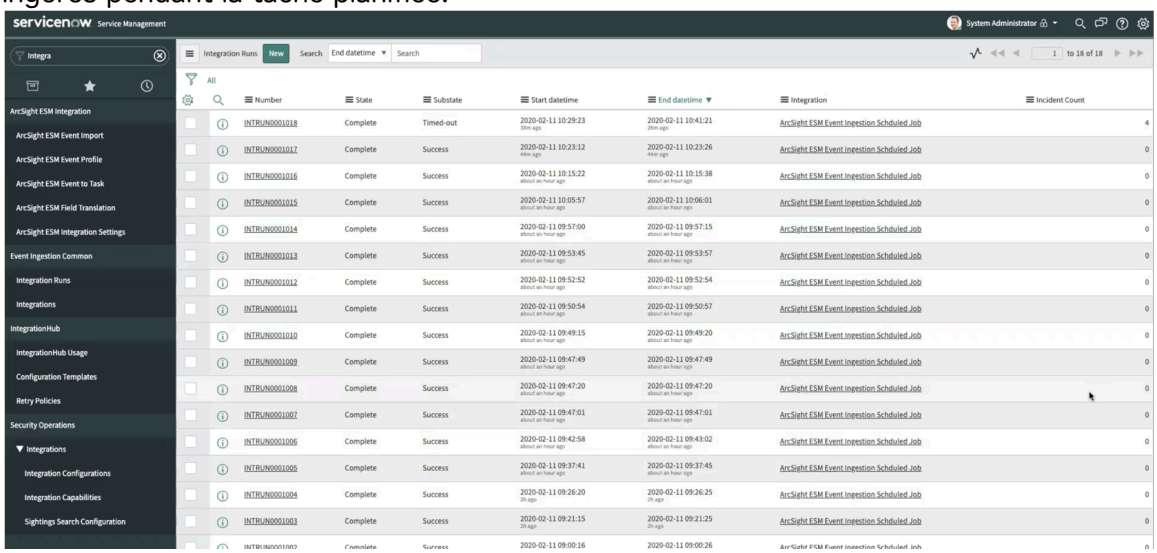
Cette section fournit des informations sur la façon de résoudre les erreurs pouvant se produire lors de l'ingestion d'événements.

Traduction automatique

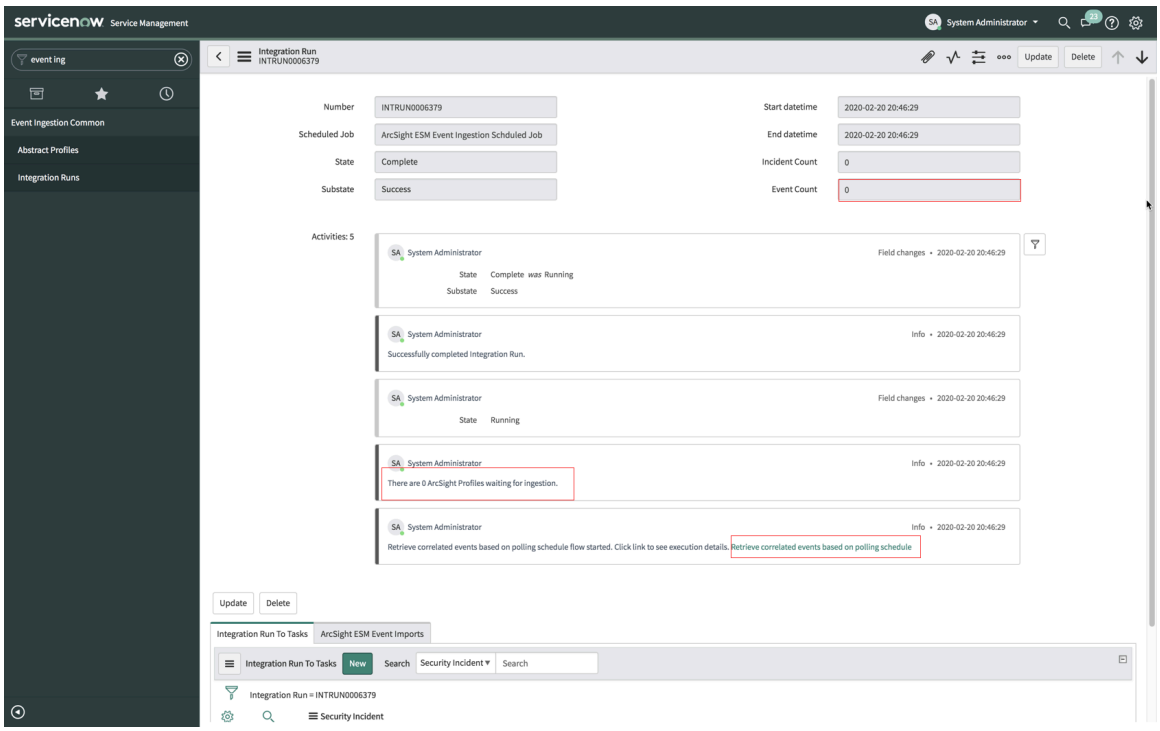
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exécutions des intégrations

Accédez à la **Ingestion d'événements courante** > **Exécutions des intégrations**. Une exécution de l'intégration a lieu toutes les minutes et capture des détails concernant les événements ingérés pendant la tâche planifiée.



Vous pouvez voir la liste des exécutions d'intégration et l'état de chaque exécution (Réussite, Expiré, En attente) ainsi que le nombre d'incidents de sécurité qui ont été créés. Cliquez sur le lien Numéro pour accéder à la page d'exécution de l'intégration détaillée.



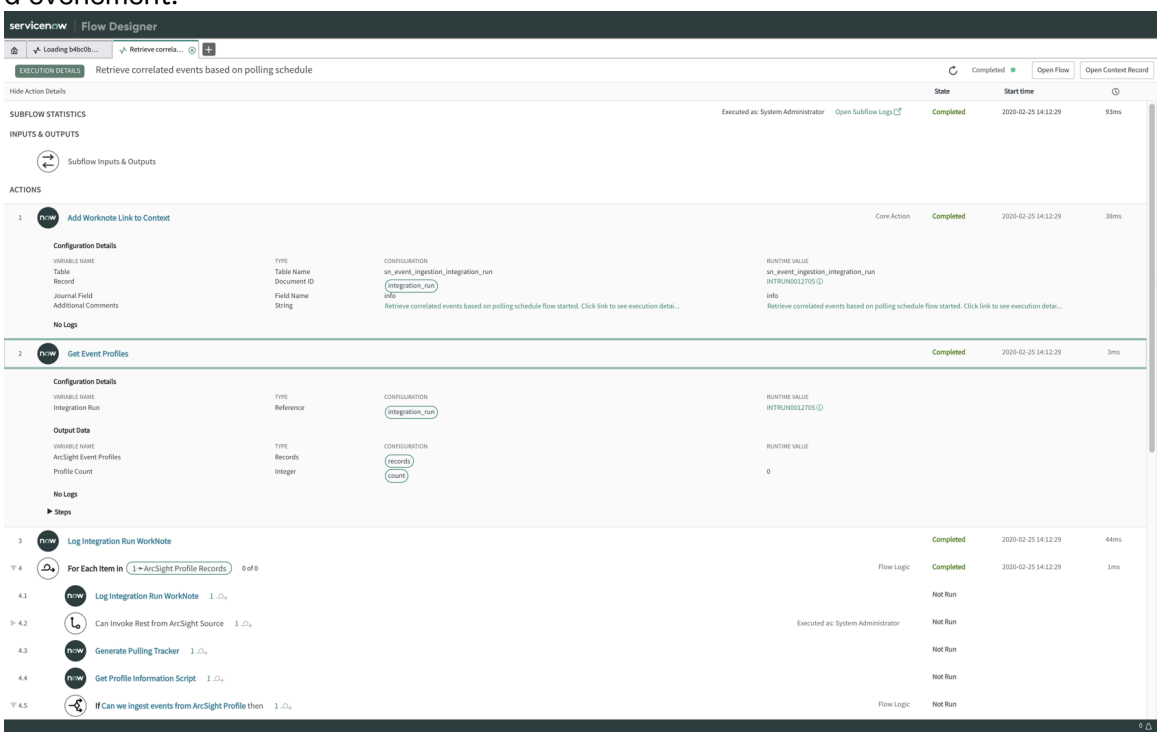
Vous pouvez afficher des détails tels que le nombre d'événements qui ont été ingérés, l'état, l'événement qui a été transformé en incident de sécurité et les différentes tâches qui ont été effectuées pendant l'ingestion. De plus, vous pouvez cliquer sur le lien pour afficher les détails de l'exécution du flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails d'exécution du flux

Cliquez sur le lien des détails de l'exécution pour afficher le flux associé à l'ingestion d'événement.



Vous pouvez afficher une exécution étape par étape du flux détaillant les différentes actions et flux secondaires qui ont été exécutés dans le cadre du flux.

Copier le ArcSight ESM profil pour l'intégration de l'ingestion d'événements

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils pour gagner du temps.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

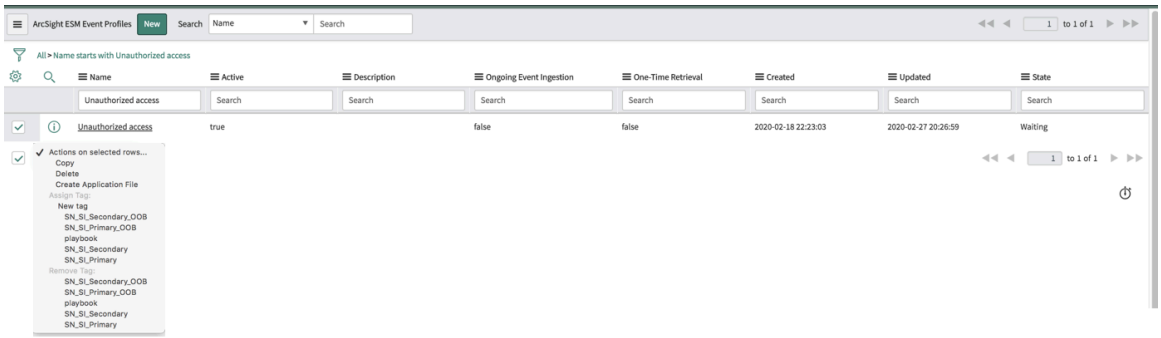
En tant qu'utilisateur disposant du rôle sn_si.admin, si vous copiez un profil, le nom du profil est initialement modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) et n'est donc pas activé accidentellement avant de terminer la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

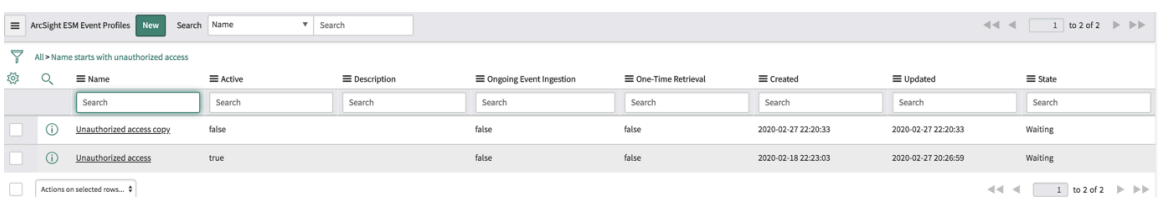
1. Accédez à la **Tous** > **Intégration ArcSight ESM** > **Profil d'événement ArcSight ESM**.
2. Dans la liste ArcSight Profiles qui s'affiche, sélectionnez un profil à copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (vrai), la copie est désactivée à ce stade (faux). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. Notez que l'état de la colonne **Actif** est défini sur faux, car le profil doit être activé.

Utiliser l'éditeur de script pour formater les valeurs d'événements de corrélation

En plus des champs directement mappés à partir des valeurs d'événements de corrélation ingérées, utilisez l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

L'éditeur de script modifie les valeurs d'un ArcSight ESM champ d'événement de corrélation de sorte que les valeurs prises en charge par l'incident ServiceNow AI Platform SIR de sécurité soient mappées aux champs Catégorie, Élément de configuration (CI), Observable et Autres champs d'incident de sécurité.

Dans certains cas, ArcSight ESM les valeurs de l'événement de corrélation sont mappées à des champs de référence tels que les champs Catégorie, Élément de configuration (CI) et Observable sur l'incident de sécurité. En tant qu'utilisateur disposant du rôle sn_si.admin, vous pouvez préférer modifier les valeurs de champ d'événement mappées à traduire les valeurs de format ou les valeurs de données pour les rendre conformes aux formats de champ d'incident et aux valeurs attendues. Si vous souhaitez convertir la valeur d'un ArcSight ESM événement de corrélation en une valeur prise en charge par ces champs sur l'incident SIR de sécurité, utilisez l'éditeur de script.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Une fois le formulaire de mappage affiché, cliquez sur le lien pour ouvrir l'éditeur de script.
2. Dans la liste de choix, sélectionnez un champ de destination pour la valeur que vous souhaitez modifier.
3. Sinon, dans la section Mappage du champ d'incidents SIR, cliquez sur l'icône de crochet [{}] en regard d'un champ pour ouvrir l'éditeur de script pour ce champ.

   Dans certains cas, un include de script peut être approprié pour le champ Élément de configuration. Pour un événement de corrélation, par exemple, une valeur de l'élément de configuration peut ne pas être mise en correspondance.

   Comme le montre la figure suivante, si une correspondance pour un nom d'hôte est introuvable dans la ServiceNow AI Platform CMDB pour le champ Élément de configuration, vous pouvez modifier la règle de sorte que si une adresse IP est trouvée, elle remplit le champ Élément de configuration.

   L'éditeur s'ouvre avec le champ affiché dans Champ de destination.
4. Entrez les modifications apportées au script et cliquez sur **Mettre à jour** pour enregistrer vos modifications. La ArcSight ESM table Traductions de champ s'affiche.
5. Fermez la table pour revenir au formulaire de mappage.

Utilisation de Concepteur de flux avec ArcSight ESM intégration d'ingestion d'événements

À l'aide du concentrateur d'intégration et de Concepteur de flux, plusieurs flux, flux secondaires et actions sont disponibles avec l'intégration ArcSight ESM .

Pour afficher ces flux secondaires, accédez à **Concepteur de flux** > **Concepteur** et cliquez sur l'onglet **Flux secondaires** . La figure ci-dessous montre les flux secondaires importants utilisés lors de la création du profil et de la tâche d'ingestion planifiée.



Ces flux secondaires sont répertoriés dans l'ordre dans lequel ils sont exécutés ci-dessous :

- **Validation de connexion et d'informations d'identification** : ce flux secondaire valide ServiceNow la connectivité avec le ArcSight ESM serveur et les informations d'identification spécifiées. Ce flux secondaire est utilisé lorsque vous cliquez sur le bouton **Configurer** dans la vignette **ArcSight ESM - Ingestion d'événements**dans le **Security Operations** > **Intégrations** > **Configuration des intégrations** la page.
- **Obtenir un jeton d'authentification ArcSight** : ce flux secondaire génère le jeton d'authentification ArcSight ESM à partir du nom d'utilisateur et du mot de passe à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'aide du ArcSight ESM service de connexion. Le service de connexion fournit le jeton d'authentification qui peut être utilisé pour appeler n'importe quel autre ArcSight ESM point de terminaison. Ce flux secondaire est utilisé dans tous les autres flux secondaires.

- **Validation de l'ID de la visionneuse de requêtes** : ce flux secondaire vérifie si l'ID de la visionneuse de requêtes spécifié lors de la création du profil est présent sur le ArcSight ESM serveur.
- **Récupération de règle de corrélation** : ce flux secondaire récupère les règles de corrélation en fonction de l'ID de la visionneuse de requêtes.
- **Obtenir un exemple d'événement** : ce flux secondaire extrait les échantillons d'événements de corrélation à partir ArcSight ESM du serveur. Ces exemples d'événements sont ensuite mappés aux champs d'incident de sécurité dans la section Mappage du profil.
- **Validation de l'ID de ressource d'étape** : ce flux secondaire valide l'ID de ressource d'étape spécifié dans la ArcSight ESM console et récupère le nom de la ressource.
- **Mettre à jour les commentaires sur les événements corrélés** : ce flux secondaire met à jour les commentaires sur les événements corrélés dans les sections Initial et Fermeture de l'incident de la page Options supplémentaires du profil.
- **Récupérer les événements corrélés en fonction du calendrier d'interrogation** : ce flux secondaire exécute la tâche planifiée qui extrait les événements corrélés en fonction de l'intervalle d'interrogation.

Au cours de l'exécution, les flux secondaires ci-dessus déclenchent également plusieurs autres flux secondaires et actions, directement ou indirectement, comme indiqué ci-dessous.

Flows | Subflows | Actions | Executions | Help — + New

Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Amazon Web Services intégration (AWS) Security Hub

Centre de sécurité AWS est un service de gestion de la posture de sécurité cloud (CSPM) qui fournit des contrôles de sécurité automatisés et continus ainsi que des vérifications des bonnes pratiques par rapport à vos ressources AWS.

Traduction automatique

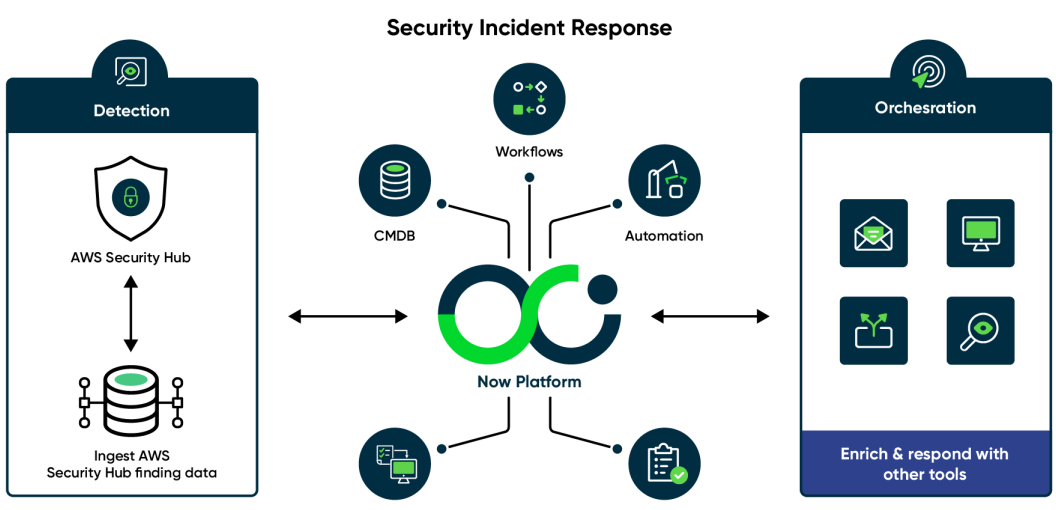
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble de l'intégration Centre de sécurité AWS

Centre de sécurité AWS vous permet d'identifier les problèmes dans vos configurations. Security Hub regroupe vos alertes de sécurité, appelées conclusions. Centre de sécurité AWS Génère ces résultats dans un format standardisé et les hiérarchise afin que vous puissiez les enrichir, les examiner et les corriger plus facilement. Vous pouvez utiliser l'intégration pour ingérer des Centre de sécurité AWS résultats Security Hub et créer automatiquement des incidents de sécurité dans Réponse aux incidents de sécurité.

Centre de sécurité AWS L'intégration dans SIR suit une architecture bidirectionnelle. SIR Ingère les données des Security Hub résultats pour créer un incident de sécurité et met simultanément à jour un Security Hub résultat avec toutes les mises à jour de l'incident de sécurité correspondant.

Consultez le diagramme suivant pour savoir comment AWS Security Hub s'intègre aux ServiceNow AI Platform Opérations de sécurité applications.



Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Fonctionnalités principales

Utilisez les fonctionnalités clés de cette intégration pour effectuer les actions suivantes :

- Détectez les résultats AWS Security Hub qui sont candidats aux incidents de sécurité et automatisez la création de ces incidents de sécurité.
- Mappez les résultats et les champs d'entité AWS Security Hub aux champs d'incident SIR de sécurité.
- Filtrez les résultats AWS Security Hub.
- Regroupez les résultats des incidents de sécurité ouverts existants afin de ne pas avoir à créer des incidents de sécurité en double.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Automatisez les mises à jour de l'état des résultats AWS Security Hub pour Security Incident Response afin de pouvoir créer et fermer les incidents de sécurité.

  Remarque : ServiceNow met également à jour l'état des résultats AWS Security Hub en fonction de la création, de la progression ou de la fermeture de l'incident de sécurité. Cette mise à jour comprend également des commentaires sur les résultats agrégés et nouveaux.

- Planifiez l'ingestion des résultats pour créer périodiquement des incidents de sécurité.
- Synchronisez les commentaires sur les résultats AWS Security Hub avec SIR les notes de travail.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Site web de la documentation produit AWS Security Hub	Site web de la documentation d'AWS Security Hub
ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Mise en route de l'intégration Centre de sécurité AWS

Activez et configurez l'intégration des résultats pour le Centre de sécurité AWS module d'extension Security Operation afin qu'il s'interface avec votre instance et Réponse aux incidents de sécurité votre ServiceNow® produit.

Avant de commencer
Rôle requis : sn_si.admin

Avant de pouvoir utiliser l'intégration Centre de sécurité AWS , vous devez la télécharger à partir du ServiceNow Store.

Pourquoi et quand exécuter cette tâche
Passez en revue la liste de vérification de configuration suivante et vérifiez que vous avez terminé toutes les tâches pour une intégration fluide.

Liste de vérification

Affectez et vérifiez la plateforme et Réponse aux incidents de sécurité les rôles requisServiceNow®.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus :
	• Le rôle administrateur installe l'intégration à partir de et ServiceNow Store attribue le rôle sn_si.admin.
	• Le rôle sn_si.admin effectue les tâches suivantes :
	  ○ Configure l'intégration.
	  ○ Crée des profils d'incident.
	  ○ Mappe les champs de données de Centre de sécurité AWS recherche aux champs d'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

	○ Planifie l'ingestion d'incidents en cours. ○ Active les mises à jour d'incident lorsqu'un Réponse aux incidents de sécurité incident est créé ou fermé.
Affectez les Centre de sécurité AWS rôles requis.	Les rôles suivants sont requis pour enregistrer Centre de sécurité AWS et configurer votre application : • SecurityHubReadOnlyAccess • SecurityHubFullAccess
Passer en revue les paramètres d'intégration Centre de sécurité AWS	Accédez à la **Tous** > **Intégration des résultats AWS Security Hub** > **Paramètres d'intégration des résultats AWS Security Hub**. Examinez ou modifiez les paramètres des propriétés en fonction de vos besoins.
Configurez votre application dans le AWS portail.	Enregistrez votre application dans le AWS portail et accordez à vos utilisateurs un accès en lecture et en écriture à l'application. Consultez les rubriques suivantes pour plus d'informations : • Configuration d'AWS Config avec la console • Intégrations de Security Hub.

Inscrire et configurer le Centre de sécurité AWS portail

Enregistrez votre application dans le Centre de sécurité AWS portail et accordez à vos utilisateurs un accès en lecture et en écriture à l'application.

Enregistrement d'un ServiceNow® profil d'utilisateur sur AWS le portail

Avant de commencer

Rôle requis : AWSSecurityHubFullAccess

Procédure

1. Connectez-vous au portail AWS.
2. Accédez à la **Gestion des accès et de l'identité (IAM)** > **Utilisateurs** > **Créer un nouvel utilisateur**.
3. La table suivante décrit les champs que vous devez configurer pour créer un profil d'utilisateur :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un profil d'utilisateur

Champ	Description
Spécifier les détails de l'utilisateur > **Nom d'utilisateur**	Nom du profil d'utilisateur.
Définir les autorisations > **Ajouter un utilisateur au groupe**	Ajoutez le profil d'utilisateur à un groupe avec des politiques d'autorisation prédéfinies. Vous pouvez créer un groupe selon vos préférences et lui affecter des politiques d'autorisation. Par la suite, vous pouvez ajouter des profils d'utilisateur au groupe et les politiques d'autorisation affectées au groupe sont automatiquement affectées aux profils d'utilisateurs.
Copiez des autorisations	Copiez les autorisations d'un profil d'utilisateur et affectez-les au nouveau profil d'utilisateur.
Joindre les politiques directement	Ajoutez AWSSecurityHubFullAccess en tant que politique d'autorisation pour votre profil d'utilisateur. Affectez une nouvelle politique d'autorisation au profil d'utilisateur en fonction de vos préférences.
Examiner et créer	Passez en revue tous les détails que vous avez ajoutés dans le profil d'utilisateur.

4. Sélectionnez **Créer un utilisateur**.
5. Sélectionnez **Afficher l'utilisateur** dans la fenêtre contextuelle affichée.
6. Créez une clé d'accès et une clé d'accès secrète pour le profil d'utilisateur.
   Vous avez besoin de ces clés pour accéder à l'intégration Centre de sécurité AWS à partir de votre ServiceNow® instance.
7. Accédez à la **Services AWS** > **Rechercher** > **AWS Security Hub** > **.**
8. Sélectionnez **Accéder à** *`Security Hub`*.
9. Dans la page Activer Centre de sécurité AWS , sélectionnez **Télécharger** pour activer AWS la configuration.
   Téléchargez les fichiers et exécutez-les dans votre compte. Cela vous autorise à rassembler toutes les informations provenant de divers services de reporting AWS et à les regrouper en Centre de sécurité AWS.
10. Sélectionnez **Activer** *`Centre de sécurité AWS`*en bas de la page.
    Le tableau de bord prend quelques instants *`Centre de sécurité AWS`* pour afficher tous les détails.
11. Changez la région de **Global** à **USA Est (Ohio).**
    Le code pour **USA Est (Ohio)** est **us-east-2**. Toutes les ServiceNow® ressources sont affectées à ce code de région.

Installer et configurer l'intégration Centre de sécurité AWS

Installez et configurez l'intégration Centre de sécurité AWS sur ServiceNow Store votre ServiceNow AI Platform instance pour commencer à ingérer des Centre de sécurité AWS résultats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Téléchargez l'intégration Centre de sécurité AWS à partir de et ServiceNow Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la Centre de sécurité AWS tuile et cliquez sur **Configurer**.
4. Remplissez les champs du formulaire.

Centre de sécurité AWS Formulaire de configuration

Champ	Description
Nom	Nom de la configuration d'instance Centre de sécurité AWS .
Nom de la région	Région que vous avez affectée dans le profil d'utilisateur sur Centre de sécurité AWS le ServiceNow® portail.
Clé secrète	Clé secrète que vous avez créée pour le profil d'utilisateur sur Centre de sécurité AWS le ServiceNow® portail.
Clé d'accès	Clé d'accès que vous avez créée pour le profil d'utilisateur sur Centre de sécurité AWS le ServiceNow® portail.

5. Cliquez sur **Envoyer**.

Résultats
Une fois que vous avez validé et soumis la configuration, chaque Security Hub configuration du serveur d'ingestion des résultats est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

Créer un profil pour Centre de sécurité AWS trouver l'intégration

Créez un Centre de sécurité AWS profil dans votre ServiceNow AI Platform instance que vous allez utiliser pour ingérer les données Centre de sécurité AWS et créer un incident de sécurité correspondant dans Espace de travail de la Réponse aux incidents de sécurité.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
L'intégration vous permet de créer des incidents de sécurité pour différents types de résultats sur la plateforme, tels que les tentatives d'accès non autorisé et les Centre de sécurité AWS programmes malveillants. Ces incidents sont créés en fonction des profils que vous configurez dans l'instance ServiceNow AI Platform . Tous les incidents sont initialement créés pour un type de résultat configuré dans un profil. Vous pouvez filtrer davantage les résultats que vous avez créés pour spécifier quels résultats créent des incidents de sécurité.

Tous les résultats qui répondent aux critères de sélection dans votre Centre de sécurité AWS locataire et qui sont disponibles via l'API Centre de sécurité AWS sont initialement ingérés dans votre ServiceNow AI Platform instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intégration des résultats AWS Security Hub** > **Profil des résultats AWS Security Hub**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Centre de sécurité AWS - Formulaire Configuration de l'ingestion des résultats

Champ	Description
Nom	Nom du profil. Ce nom vous permet d'identifier le type de profil et constitue également le nom par défaut de la balise de sécurité associée à ce profil.
Actif	Sélectionnez cette option pour activer le profil. Lorsque le profil est actif, cela implique que les données d'ingestion ServiceNow AI Platform active des résultats et des Centre de sécurité AWS incidents de sécurité correspondants sont créés lorsque SIR les conditions de filtrage sont vérifiées.
Source	Le Centre de sécurité AWS locataire d'intégration que vous avez configuré pour ingérer les résultats. Si vous avez configuré plusieurs locataires, sélectionnez le locataire approprié pour les types de résultats que vous prévoyez d'ingérer pour le profil.
Ordre	Saisissez une valeur pour ce champ qui indique l'ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400. La valeur par défaut est 100.
Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

Mapper les champs de Centre de sécurité AWS résultat

Mappez les champs de résultat individuels Centre de sécurité AWS aux champs de l'incident SIR de sécurité afin de pouvoir créer des incidents avec les données mappées.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

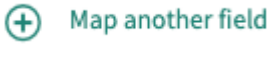
Procédure

1. Sur la page de mappage, dans la Centre de sécurité AWS section Mappage, sélectionnez l'une des méthodes d'intégration d'échantillons.

Méthodes d'intégration des exemples

Champ	Description
Tous les champs de résultats par défaut	Utilisez cette méthode d'ingestion pour afficher la liste statique de tous les champs de résultats. Cette méthode contient uniquement des noms de champs par défaut sans valeur. Vous pouvez utiliser ces informations pour mapper avec les SIR champs.
Récupérer les résultats récents Centre de sécurité AWS	Utilisez cette méthode d'ingestion pour importer les données des résultats les plus récents. Vous pouvez ingérer 5 résultats d'échantillon par défaut et un maximum de 20 résultats d'échantillon. Les valeurs du champ de résultat d'échantillon sont renseignées lorsque le profil ingère les résultats d'échantillon. Vous pouvez mapper ces résultats aux **champs cibles des incidents SIR**. Les champs et valeurs de résultat apparaissent sous forme d'onglets individuels.
Importer un échantillon de données	Sélectionnez **Importer un échantillon de données** pour importer les résultats d'échantillon à partir de .Centre de sécurité AWS Ce bouton s'affiche lorsque vous sélectionnez la méthode d'ingestion Récupérer les résultats récents Centre de sécurité AWS . La récupération des échantillons de résultats à partir du Centre de sécurité AWS serveur prend un certain temps. Mappez ces résultats aux **champs cibles des incidents SIR**. Les champs et valeurs de résultat apparaissent sous forme d'onglets individuels.

2. Pour ajouter des champs aux champs par défaut affichés dans l'incident de sécurité, procédez comme suit :

   Dans la section Champs cibles de l'incident SIR, sélectionnez le 

Il affiche une liste de SIR champs, à partir desquels vous pouvez choisir d'afficher un nouveau champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans la colonne Incident de sécurité, développez la liste qui s'affiche, puis sélectionnez un champ.

> **Remarque :** Plusieurs observables peuvent être affichés sur le même incident de sécurité. Par exemple, le champ **Observable** peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs **Élément de configuration** et **Notes de travail** prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, vous voyez un message d'erreur indiquant que ce champ ne prend pas en charge plusieurs valeurs. De même, si un champ d'un incident de sécurité comporte une liste dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste, le champ n'est pas renseigné sur l'incident de sécurité.

b. Dans la Centre de sécurité AWS section Champs sources, faites glisser votre champ pour le mapper à votre nouveau champ.

c. Lorsque vous cochez la case correspondant à un champ, toutes les modifications nouvelles ou mises à jour apportées sont Centre de sécurité AWS automatiquement mises à jour dans le SIR respectif avec les nouvelles données d'incident.

> **Remarque :** Dans le système de base, la propriété système sn_sec_security.finding_updates est définie par défaut sur Vrai pour recevoir les Centre de sécurité AWS mises à jour relatives aux nouvelles alertes liées au SIR.

- Par défaut, les champs Utilisateurs affectés, Éléments de configuration et Observables sont cochés. Cela signifie que chaque fois que de nouveaux observables ou éléments de configuration associés, ou des utilisateurs affectés sont ajoutés à l'incident, ces informations sont automatiquement extraites et renseignées dans les listes connexes respectives de Security Incident Response (SIR) pendant cet intervalle d'interrogation.
- Pour tous les autres champs, vous devez cocher la case correspondant à un champ pour toutes les modifications nouvelles ou mises à jour apportées au résultat dans Centre de sécurité AWS. Cela met automatiquement à jour les données d'incident SIR respectives avec les nouvelles données d'incident.

> **Important :** Une diligence raisonnable doit être effectuée avant de sélectionner cette fonctionnalité, car le remplacement des données existantes peut entraîner des données instables pour l'analyste et toute autre automatisation définie même par les valeurs de champ de l'incident de sécurité peut également être affectée. Il est donc important de faire preuve de diligence raisonnable avant de sélectionner une fonctionnalité de remplacement.

3. Pour supprimer un champ, utilisez le ⊖ (**Supprimer l'élément**) en regard du champ d'expression d'entrée dans la section Champs cibles des incidents SIR.

4. Pour mapper une valeur de champ de la Centre de sécurité AWS section Champs sources à un champ de la section Champs cibles de l'incident SIR, utilisez l'une des actions suivantes :

a. Faites glisser le nom du champ (par exemple, l'ID) et déposez-le à côté d'un nom de champ dans la colonne Champs cibles de l'incident SIR.

Vous pouvez faire correspondre n'importe quelle valeur de la Centre de sécurité AWS section Champs sources à un champ de la section Champs cibles d'incidents SIR. Les champs sont codés par couleur afin que vous ne négligez pas ou ne dupliquiez pas les champs de recherche dans le processus de mappage. Les champs bleu clair indiquent qu'un champ de résultat n'est pas encore sélectionné et mappé sur l'incident

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de sécurité. Vous préférez peut-être associer un champ de résultat entrant à plusieurs champs sur un incident de sécurité. Un champ gris indique qu'un champ de résultat a été sélectionné et mappé à un champ de l'incident de sécurité. De cette façon, vous pouvez visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations de résultat importantes restantes restent non mappées. Toutefois, certains champs de la Centre de sécurité AWS section Champs sources ne sont pas compatibles avec les champs de la section Champs cibles des incidents SIR. Si vous mappez ces valeurs, elles ne s'affichent pas lors de la création du SIR.

b. Vous pouvez ajouter une combinaison de texte et de champ.
Par exemple, le nom de la recherche est ${name}$. Ici, le nom du résultat peut être saisi manuellement tandis que ${name}$ est mappé à partir de la Centre de sécurité AWS section Champs sources.

c. Vous pouvez entrer manuellement un champ de recherche source et le mapper à un champ cible.
Utilisez le format ${nom de champ}$ pour mapper manuellement un champ de recherche source. Par exemple, pour mapper un champ de recherche Gravité, le format est ${properties(severity)}$.

Cette intégration classe certains sous-types d'observables. Lorsque vous mappez un champ de Centre de sécurité AWS recherche avec le champ observable SIR, l'observable ServiceNow AI Platform est classé automatiquement. Si vous souhaitez mapper de manière générique l'observable entrant Centre de sécurité AWS au type observable dans SIR, faites glisser et déplacez le Centre de sécurité AWS champ dans le champ Observable. Toutefois, si vous connaissez le type d'observable pour l'observable entrant Centre de sécurité AWS dans SIR, effectuez un mappage spécifique au champ Type d'observable SIR . Voici quelques exemples de types SIR d'observables spécifiques dans : Observable (nom de domaine), Observable (adresse e-mail), Observable (adresse IP (V4)) et Observable (nom d'hôte).

Parfois, la recherche de valeurs de champ dans Centre de sécurité AWS peut ne pas se traduire directement dans les champs de l'incident de sécurité SIR. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques.

5. Pour formater la traduction d'un nouveau champ à partir d'un Centre de sécurité AWS résultat afin qu'il corresponde à une valeur de champ sur un incident de sécurité, cliquez sur le lien **Cliquez ici** dans l'en-tête des **champs cibles de l'incident SIR** .
6. Pour modifier les champs qui prennent en charge la traduction de champ, cliquez sur l'icône Traduction de champ du  de champ.
Les champs qui prennent en charge la traduction des champs sont **Catégorie**, **Élément de configuration** et **Priorité**. Par exemple, cliquez sur l'icône du  à côté de la catégorie. L'éditeur Centre de sécurité AWS de script de traduction de champ des résultats s'ouvre.
7. Entrez les modifications apportées au script, cliquez sur **Mettre à jour** pour enregistrer les modifications et revenir à la page Mappage.
Par exemple, pour Catégorie, définissez les éléments suivants dans l'éditeur de script :

```
"<Incoming Security Hub finding Field Value>" : "<Category to assign to the Security Incident>".
```

Ce mappage garantit qu'un profil n'utilise que des catégories configurées.

8. Poursuivez votre mappage en ajoutant ou en supprimant des valeurs de champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir des critères supplémentaires qu'un résultat entrant doit satisfaire pour créer un incident de sécurité.

9. Pour passer à la section Filtrage et agrégation, cliquez sur **Continuer**.

Que faire ensuite

Définissez et définissez des conditions de filtre afin de pouvoir spécifier quels résultats créent des incidents de sécurité. Vous pouvez utiliser les mêmes valeurs de champ (définies dans la section Mappage) dans le générateur de conditions de génération d'incident (dans la section Filtrage et agrégation) pour définir des critères supplémentaires qu'un résultat entrant doit satisfaire pour créer un incident de sécurité.

Définir des critères de filtre et d'agrégation pour Centre de sécurité AWS l'ingestion des résultats

Vous pouvez définir et définir des conditions de filtre afin de spécifier quels résultats entrants doivent provoquer des incidents de sécurité. Vous pouvez également définir des critères de champ d'incident supplémentaires qui permettent d'ajouter un résultat entrant à un incident de sécurité ouvert au lieu de créer un autre incident de sécurité pour le même résultat.

Définir les conditions de filtrage des Centre de sécurité AWS conclusions afin de créer des incidents de sécurité

Définissez les conditions de filtrage afin que les incidents de sécurité ne soient créés que lorsque les conditions de filtrage correspondent.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Ce type de filtrage vous aide à isoler les incidents de sécurité et limite le nombre d'incidents de sécurité que vous créez. Si vous définissez des critères de filtrage supplémentaires, seuls les résultats requis sont ingérés sans avoir à modifier la requête ou la configuration de l'incident déclenché.

Effectuez les étapes suivantes pour définir les critères qu'un résultat entrant Centre de sécurité AWS doit satisfaire pour qu'un incident de sécurité soit créé :

Procédure

1. Sélectionnez **Appliquer le pré-filtre** dans la section Pré-filtrage.

   Vous pouvez utiliser cette option pour filtrer des résultats spécifiques et réduire la charge de l'ingestion des résultats.

   Dans le champ **Filtre d'API** , saisissez une condition JSON selon vos besoins qui filtre les résultats spécifiques en fonction de la condition. Par exemple, saisissez la valeur suivante pour filtrer les résultats dont l'état du workflow est Résolu dans Security Hub :

```
{"Filters"{
  "WorkflowStatus":[{
  "Comparison":"NOT_EQUALS",
  "Value": "RESOLVED"}]
 }
}
```

   En fonction de la condition fournie, Centre de sécurité AWS les résultats sont ingérés et affichés dans la table brute des Centre de sécurité AWS résultats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accédez à la **Tous** > **Intégration des résultats AWS Security Hub** > **Résultat brut AWS Security Hub** pour afficher les données brutes des résultats.

2. Dans la section Sélectionner les champs de recherche pour les conditions de filtre, sélectionnez **Afficher les champs de recherche disponibles** pour afficher une liste de tous les champs disponibles dans un Centre de sécurité AWS résultat.
   Dans **la liste Tous les champs de résultat** , sélectionnez les champs de résultat que vous souhaitez afficher dans la section Conditions de génération d'incident de sécurité.

   Remarque : Un résultat AWS Security Hub contient plusieurs champs et valeurs. Dans la liste **Tous les champs de résultat** , vous pouvez rechercher un champ de résultat selon vos besoins et le sélectionner.

3. Dans la section Conditions de génération d'incidents de sécurité, sélectionnez **Filtre basé sur les conditions** pour définir les critères qu'un résultat entrant Centre de sécurité AWS doit satisfaire pour qu'un incident de sécurité soit créé.

   Le premier champ des Conditions de filtre contient une liste par défaut de deux cents champs disponibles sur un résultat et les champs de recherche que vous avez sélectionnés dans la section Sélectionner les champs de recherche pour les conditions de Centre de sécurité AWS filtre.

   Le deuxième champ des conditions de filtre contient des opérateurs conditionnels. L'option que vous choisissez détermine la condition qui doit être remplie pour ingérer un résultat.

   Le troisième champ des conditions de filtre contient des valeurs prises en charge par les champs de résultat disponibles. Vérifiez que le champ de résultat que vous saisissez correspond aux valeurs des résultats.

   Par exemple, utilisez la condition *`de filtre contenue`* pour les champs suivants à valeurs multiples :

   - Workflow(Status)
   - WorkflowState

4. À l'aide des listes et des champs du générateur de conditions, définissez les filtres pour la première ligne.
5. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
6. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.

Résultats

En fonction des conditions de filtrage, Centre de sécurité AWS les résultats sont importés dans SIR. Accédez à la **Tous** > **Intégration des résultats AWS Security Hub** > **Importation des résultats AWS Security Hub** pour afficher les résultats importés.

Définir des conditions pour regrouper Centre de sécurité AWS les résultats en un incident de sécurité

Définissez des critères d'agrégation d'incidents supplémentaires qui regroupent un résultat entrant Centre de sécurité AWS à un incident de sécurité SIR existant au lieu de créer des incidents similaires, potentiellement en double. Lorsque vous utilisez des critères de valeur de correspondance de champ pour chaque profil, cette agrégation supplémentaire peut

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'incidents connexes sur un seul incident de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Si un nouvel incident correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, l'incident est automatiquement ajouté à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher tous les incidents agrégés ajoutés sur une liste connexe sur un incident de sécurité.
Tous les résultats agrégés Centre de sécurité AWS sur un incident de sécurité sont affichés dans la Centre de sécurité AWS liste connexe. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi Centre de sécurité AWS les résultats sont ajoutés aux incidents de sécurité existants.

Procédure
1. Pour définir des critères de champ d'incident supplémentaires qui permettent d'ajouter un résultat entrant Centre de sécurité AWS à un incident de sécurité ouvert au lieu de créer un nouvel incident, sélectionnez l'option **Conditions d'agrégation** .
2. Dans le champ **Champs d'incidents avec valeurs correspondantes** , saisissez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre ServiceNow AI Platform instance.
   Toutes les valeurs de champ que vous avez sélectionnées dans le champ d'entrée de sélection multiple doivent correspondre afin que les critères d'agrégation soient remplis et que cet incident entrant puisse être ajouté à un incident de sécurité existant. Cette sélection implique qu'il s'agit d'une condition *ET* dans laquelle des champs, tels que des observables et des éléments de configuration qui peuvent avoir plusieurs valeurs de champ, leur sont mappés. Si seul un sous-ensemble de valeurs est apparié, les conditions d'agrégation Centre de sécurité AWS des résultats ne sont pas remplies et un nouvel incident de sécurité est créé.
3. Pour ajouter plusieurs conditions de correspondance de champ, cliquez sur **Ajouter un nouveau critère**.
   L'agrégation se produit si l'une ou l'autre des conditions de champ de sélection multiple que vous définissez est remplie. Cette sélection implique la condition *OU* .
4. Pour mettre à jour la note de travail d'un nouveau résultat lorsqu'il est ajouté à un incident de sécurité, sélectionnez **Enregistrer la note de travail pour le nouveau résultat**.

   La note de travail indique qu'un nouveau résultat est ajouté et inclut un lien vers les détails du résultat. La note de travail du journal met également à jour d'autres détails que vous ajoutez au champ note de travail dans votre section de mappage.
5. Pour configurer le calendrier, cliquez sur **Continuer**.

Résultats
En fonction des conditions d'agrégation, les Centre de sécurité AWS résultats sont regroupés pour créer un SIR incident. Accédez à la **Tous** > **Intégration des résultats AWS Security Hub** > **Résultat à Tâche AWS Security Hub** pour afficher la liste des incidents de sécurité qui ont été créés.

Que faire ensuite
Définissez un calendrier pour récupérer les données de recherche et les incidents de recherche qui correspondent aux critères du profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Planifier la récupération des Centre de sécurité AWS résultats

Définissez un calendrier pour récupérer les données des résultats et ingérer les Centre de sécurité AWS résultats qui correspondent aux critères du profil.

Avant de commencer

Rôle requis : sn_sni.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier la fréquence à laquelle vous souhaitez interroger pour obtenir des résultats futurs Centre de sécurité AWS qui correspondent à la configuration du profil de Centre de sécurité AWS résultat.

L'intervalle d'interrogation est configuré individuellement pour chaque profil. Les différents intervalles d'interrogation peuvent avoir un impact sur les performances de l'intégration Centre de sécurité AWS des résultats. Lors de la planification, prévoyez d'équilibrer la charge du système par rapport à l'urgence d'un incident. Une valeur par défaut d'une minute est définie pour tous les profils. Vous pouvez modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

Toutes les alertes ajoutées à l'incident dans un intervalle d'interrogation particulier sont traitées, puis ajoutées aux listes associées aux alertes et aux Centre de sécurité AWS commentaires.

Procédure

1. Renseignez les champs du formulaire de planification.

Configurez le calendrier pour définir comment et quand extraire les Centre de sécurité AWS conclusions du locataire.

Formulaire de planification

Champ	Description
Ingestion des résultats en cours	Ingestion des résultats en cours que l'instance ServiceNow AI Platform extrait du locataire pour les Centre de sécurité AWS nouveaux incidents. Les incidents de sécurité sont créés si les résultats déclenchés sont trouvés et si les critères de filtrage de génération d'incident de sécurité correspondent.
Résultats fermés du sondage	Résultats d'interrogation qui ont été résolus. Ces résultats sont ingérés lors de l'ingestion de l'incident en cours.
Incrémentation du sondage (minutes)	Fréquence d'interrogation définie en minutes.
Définir le délai d'ingestion du résultat initial	Ingestion des conclusions basées sur la date et l'heure configurées. Vous pouvez utiliser cette option pour définir une date et une heure spécifiques pour l'ingestion initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation.
Délai d'ingestion du résultat initial d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Récupération ponctuelle	Cochez cette case pour permettre une récupération ponctuelle des résultats historiques Centre de sécurité AWS , puis procédez au rapprochement des données. Lorsque vous cochez cette case, l'application extrait tous les résultats ouverts et fermés Centre de sécurité AWS pour la période jusqu'à 90 jours environ. Lors du traitement des données, les résultats en cours et les données historiques sont extraits, mais le traitement des résultats en cours prime sur l'extraction historique. Dans le cas contraire, l'extraction historique peut prendre un certain temps en fonction de la durée et du nombre de résultats ingérés. **Remarque :** Les résultats historiques Centre de sécurité AWS récupérés sont soumis à des contrôles de déduplication pour empêcher tout doublon au sein de l'application Réponse aux incidents de sécurité .
Depuis date	Date depuis laquelle les résultats historiques sont ingérés à partir de Centre de sécurité AWS. **Remarque :** Les données sur les résultats sont extraites approximativement des 90 derniers jours.

La page de planification vous permet de définir comment et quand les Centre de sécurité AWS résultats sont extraits du locataire.

2. Pour accéder à la page Options supplémentaires, cliquez sur **Continuer**.

Automatiser les mises à jour et les fermetures de résultats Centre de sécurité AWS en fonction de l'état de l'incident SIR

Automatisez les mises à jour et les fermetures des résultats en Centre de sécurité AWS fonction de l'état de l'incident SIR . L'intégration Centre de sécurité AWS dispose d'une interface bidirectionnelle qui permet l'ingestion de résultats pour créer des incidents de sécurité et mettre à jour l'état des résultats en fonction des changements dans l'incident SIR .

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Renseignez les champs du formulaire.
   Suivez les instructions pour terminer la configuration de la mise à jour Centre de sécurité AWS des résultats lorsque vous créez ou fermez un incident de sécurité dans SIR.

Automatisation du formulaire de mise à jour des incidents

Catégorie	Champ	Description
Mettre à jour l'état	SIR État de l'incident	Affiche une liste des états d'incidents SIR . Sélectionnez une option dans cette

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catégorie	Champ	Description
		liste pour la mapper à un Security Hub état de résultat.
	Security Hub État du résultat	Affiche une liste des états du Security Hub workflow. Le statut de workflow d'un résultat est mis à jour lorsque l'état de l'incident de l'état Centre de sécurité AWS SIR correspondant change.
Mettre à jour la priorité	SIR Priorité de l'incident	Affiche une liste des niveaux de priorité de l'incident SIR . Sélectionnez une option de cette liste pour la mapper à un niveau de Security Hub priorité de résultat.
	Security Hub Priorité du résultat	Sélectionnez une option dans la liste des niveaux de Security Hub gravité. La gravité d'un résultat est mise à jour Centre de sécurité AWS lorsque la priorité de l'incident de sécurité correspondante change.
Mettre à jour les notes de travail	Sélectionnez cette option pour mettre à jour la section des notes lorsqu'une note deSecurity Hub travail est mise à jour pour l'incident correspondant.SIR La section des notes de travail a SIR une limite de 512 caractères, car la section des notes d'un Security Hub résultat prend en charge la même chose.	
Mettre à jour les commentaires supplémentaires	Sélectionnez cette option pour mettre à jour la section des commentaires sur les Centre de sécurité AWS résultats avec les commentaires supplémentaires que vous avez fournis dans SIR l'incident.	
Mettre à jour les notes de résolution	Sélectionnez cette option pour mettre à jour la section des commentaires de Centre de sécurité AWS fermeture avec les notes de résolution que vous avez fournies lors de la résolution de l'incident SIR .	

Remarque : Chaque mise à jour des notes de travail remplace la dernière mise à jour de la section des notes d'un Security Hub résultat. Nous vous recommandons d'ajouter des notes de travail pertinentes en cas d'incident SIR .

2. Sélectionnez **Finish** (Terminer).

Que faire ensuite

Le profil passe à l'état En attente. Lorsque le message de confirmation indique que l'installation et la configuration sont terminées, vous pouvez activer le profil.

SIR formulaire après une ingestion de Centre de sécurité AWS résultat

Une fois le ServiceNow AI Platform résultat ingéré Centre de sécurité AWS , un incident de sécurité est créé et des mises à jour sont apportées à cet enregistrement d'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notes de travail

Une note de travail est publiée lorsqu'un incident est agrégé et si vous avez configuré l'option **Enregistrer la note de travail pour le nouveau résultat** dans le Définir des critères de filtre et d'agrégation pour Centre de sécurité AWS l'ingestion des résultats.

Vous pouvez également afficher l'enregistrement d'importation des résultats internes qui contient les données brutes de l'incident.

Lorsque vous cliquez sur le lien **Cliquer ici** , vous pouvez afficher l'enregistrement dans l'environnement Centre de sécurité AWS . L'exemple suivant montre l'enregistrement dans l'environnement Centre de sécurité AWS .

Résultats agrégés Centre de sécurité AWS

Afficher les résultats agrégés Centre de sécurité AWS : affichez les incidents qui sont regroupés à l'incident de sécurité. Accédez à la **Afficher toutes les listes connexes** > **Résultats agrégés d'AWS Security Hub**.

Créer un incident de sécurité : Sélectionnez un incident dans la liste, cliquez sur le menu **Actions** , puis sur **Créer un incident de sécurité**. Cette option crée un nouvel incident de sécurité pour l'incident et cet incident est désagrégé de l'incident de sécurité parent.

Carbon Black : intégration de l'enrichissement des incidents

Utilisez l'intégration de Carbon Black pour enquêter sur les incidents de sécurité et y répondre à l'aide des API pour interroger et interagir avec les points de terminaison associés aux incidents de sécurité.

Trouver des ressources d'intégration Carbon Black - Enrichissement des incidents

- Premiers pas avec l'intégration Carbon Black - Enrichissement des incidents
- Intégration de Security Operations Carbon Black : obtenir le flux d'exécution des processus
- Intégration de Security Operations Carbon Black : isoler le flux de l'hôte
- Security Operations Carbon Black Integration : supprimer le flux d'isolement de l'hôte

Comprendre les concepts d'intégration

- Types d'intégrations ServiceNow fournies
- Opérations de sécurité Déclencheurs de workflow

Obtenir de l'aide depuis les ressources ServiceNow

- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance
- Effectuer une mise à niveau vers Madrid

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Premiers pas avec l'intégration Carbon Black - Enrichissement des incidents

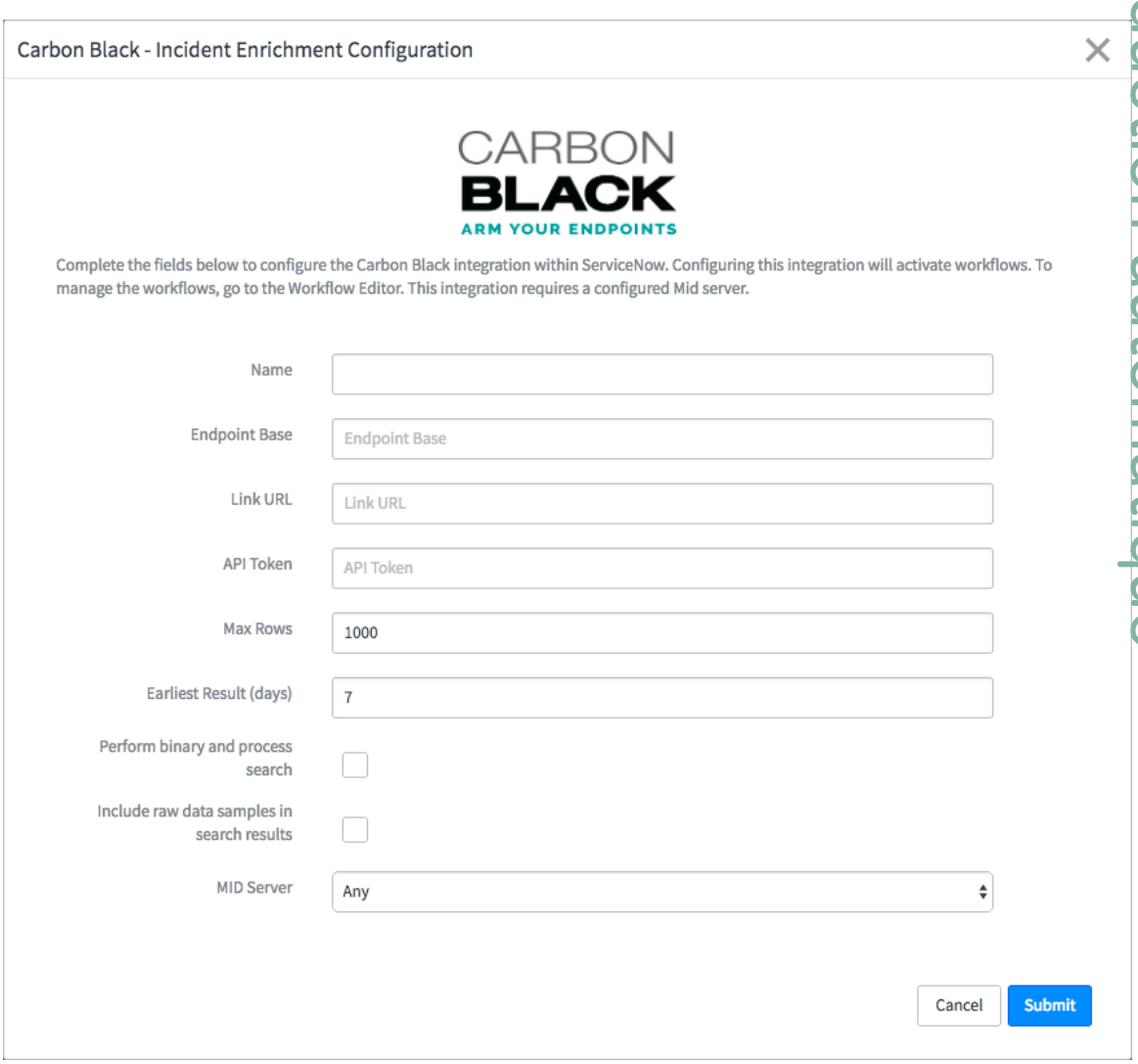
L'enrichissement d'incident Carbon Black facilite l'enquête sur un incident de sécurité en interrogeant les journaux à la recherche d'indicateurs potentiellement malveillants. Avant de pouvoir utiliser l'intégration Carbon Black - Incident Enrichment, vous devez la télécharger à partir de et ServiceNow Store ajouter l'URL de base du point de terminaison et le serveur MID appropriés.

Avant de commencer

Rôle requis : sn_si_admin

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois le téléchargement terminé, accédez au Carbon Black site Web et obtenez l'URL de base du point de terminaison et le jeton d'API sous votre profil.
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configuration de l'intégration**.
4. Dans la fiche Carbon Black - Incident Enrichment, cliquez sur **Configurer**.



5. Renseignez les champs nécessaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom de cette configuration.
Base du point de terminaison	L'URL du point de terminaison que vous avez acquise sur le site Carbon Black.
URL de lien	L'URL de lien qui renvoie à une instance Carbon Black, lorsqu'elle est disponible.
Jeton d'API	Le jeton API que vous avez acquis sur le site Carbon Black.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher. La valeur par défaut est de 1 000 lignes.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Effectuer une recherche binaire et de processus	Sélectionnez cette option pour effectuer des recherches binaires afin de trouver des fichiers binaires tels que des hachages de fichiers, et des recherches de processus pour .exe processus qui ont pu s'exécuter.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend de votre paramètre dans la propriété **nombre de lignes de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	**Sélectionnez N'importe lequel** pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

6. Cliquez sur **Envoyer**.
   La carte de configuration d'intégration s'affiche.
7. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Intégration Carbon Black

L'intégration de Carbon Black vous permet d'enquêter sur les incidents de sécurité et d'y répondre à l'aide d'API pour interroger et interagir avec les points de terminaison associés aux incidents de sécurité.

Explorer

- Intégrations de Réponse aux incidents de sécurité
- Carbon Black : intégration de l'enrichissement des incidents

Configurer

Premiers pas avec l'intégration Carbon Black

Utiliser

Développer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Opérations de sécurité Déclencheurs de workflow
- Afficher les éléments affectés pour un incident de sécurité
- Opérations de sécurité : obtenir le flux d'exécution des processus
- Intégration de Security Operations Carbon Black : obtenir le flux d'exécution des processus
- Afficher les éléments affectés pour un incident de sécurité
- Exécuter une demande de bloc
- Security Operations Integration - Bloquer le flux de demande
- Exécuter Isoler l'hôte
- Intégration de Security Operations Carbon Black : isoler le flux de l'hôte
- Security Operations Carbon Black Integration : supprimer le flux d'isolement de l'hôte
- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Premiers pas avec l'intégration Carbon Black

Carbon Black est un système de sécurité avancé qui s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration de Carbon Black, vous devez télécharger l'intégration à partir de et ServiceNow Store ajouter la base de point de terminaison et le jeton d'API appropriés.

Avant de commencer

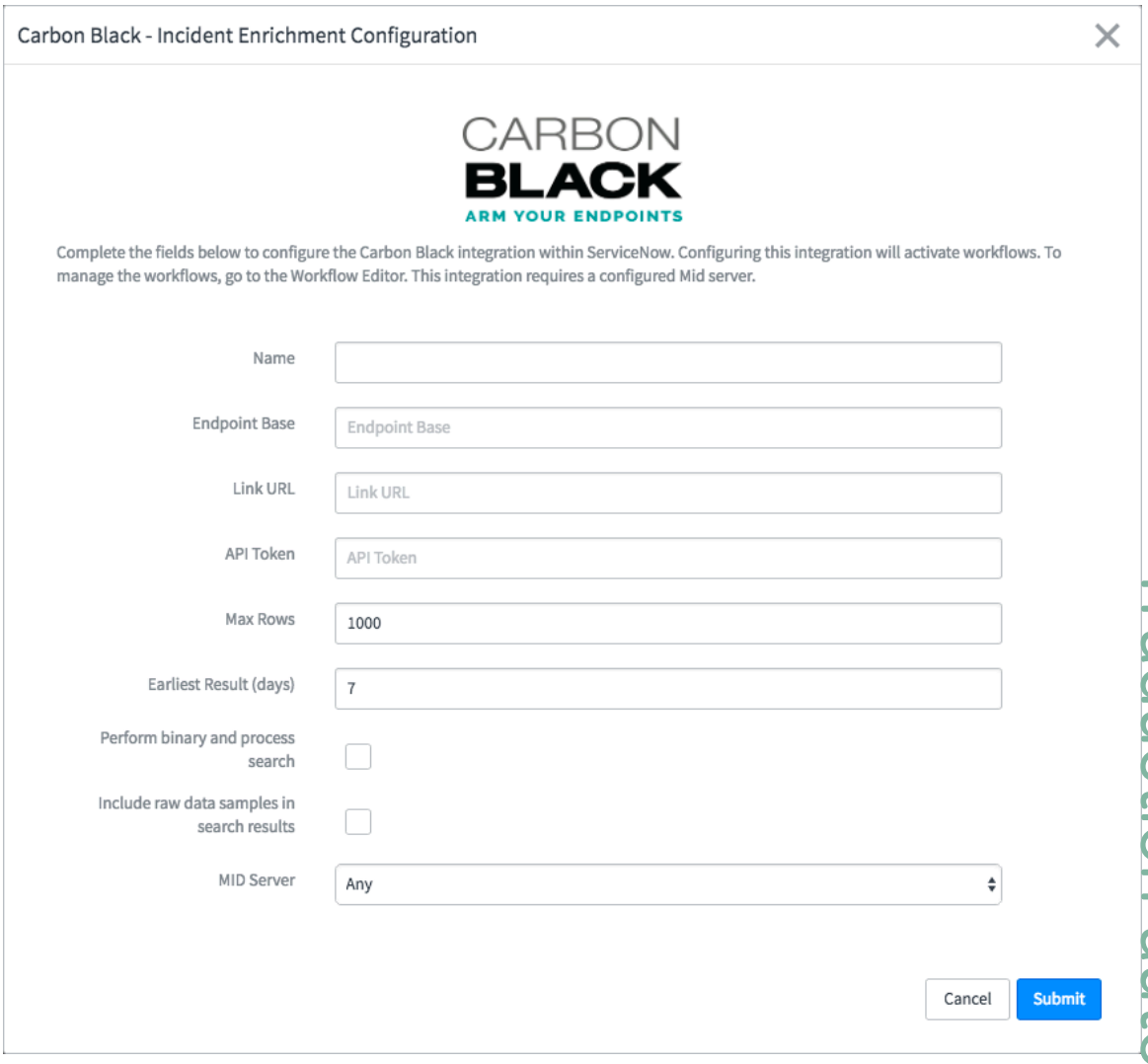
Rôle requis : sn_si_admin

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez au Carbon Black site web et obtenez l'URL de base du point de terminaison et le jeton d'API sous votre profil.
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**. Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Cliquez sur **Nouveau** sur la Carbon Black carte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
Base du point de terminaison	Base de point de terminaison que vous avez acquise sur le site Carbon Black.
Jeton d'API	Le jeton API que vous avez acquis sur le site Carbon Black.
Utiliser un serveur MID	Cochez cette case si elle n'est pas déjà cochée.
Serveur MID	**Sélectionnez N'importe lequel** pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.
Activer Isoler l'hôte	Cochez cette case pour permettre aux éléments de configuration sélectionnés d'être isolés de l'onglet de la liste connexe **Éléments de configuration** lors d'un incident de sécurité.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Envoyer**.
   La carte de configuration d'intégration s'affiche.
7. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Anti-robot Check Point - Intégration de l'analyseur d'e-mail

L'intégration Check Point Anti-bot - Analyseur d'e-mails est prise en charge à l'aide d'un analyseur d'e-mails qui consomme les notifications par e-mail de Check Point Anti-bot pour créer des incidents de sécurité et piloter les workflows d'enrichissement et de réponse.

Configurer l'intégration Check Point Anti-bot - Analyseur d'e-mails

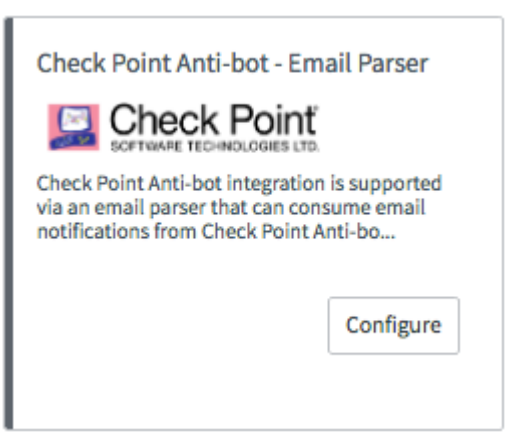
L'intégration Check Point Anti-bot - Analyseur d'e-mails utilise les notifications par e-mail pour gérer les workflows d'enrichissement et de réponse.

Avant de commencer
Rôle requis : sn_si_admin

Pourquoi et quand exécuter cette tâche
Un modèle d'analyseur d'e-mails Check Point Anti-bot est fourni pour l'intégration. Il doit être configuré et activé avant l'intégration. La mise à jour de l'analyseur l'active.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.



2. Dans la carte Check Point Anti-bot - Analyseur d'e-mails, cliquez sur **Configurer**.
3. Dans la boîte de dialogue **Check Point Anti-bot - Configuration de l'analyseur d'e-mails** , cliquez sur le lien **Configurer l'analyseur d'e-mails** .
4. Cliquez sur le lien **Check Point Anti-bot** pour modifier les paramètres dans le modèle d'analyseur d'e-mails fourni.
   Renseignez au minimum le champ L'e-mail provient de . Pour créer un analyseur d'e-mails, reportez-vous à la section Créer des analyseurs d'e-mails dans Security Operations.
5. Cochez la case **Actif** .
6. Cliquez sur **Mettre à jour** dans le formulaire **Analyseur d'e-mails** .
   L'analyseur d'e-mails est actif. Vous n'avez pas besoin de revenir aux **configurations d'intégration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration Check Point Next Generation Threat Prevention

Ce document décrit les étapes nécessaires pour intégrer les fonctionnalités de Check Point Next Generation Threat Prevention (NGTP) avec ServiceNow® Réponse aux incidents de sécurité (SIR) afin que les applications fonctionnent correctement ensemble.

Une fois l'installation et la configuration effectuées, l'analyste d'incidents de sécurité utilise cette intégration pour bloquer les adresses IP, les URL et les domaines malveillants à l'aide des options de liste de demandes de blocs avec les ServiceNow Réponse aux incidents de sécurité produits (SIR). Cette liste de demandes de blocs est configurée sur les passerelles Check Point en tant que flux de renseignements personnalisé. La fonctionnalité Flux de renseignements personnalisés permet d'ajouter des flux de cyber-intelligence personnalisés dans le moteur de prévention des menaces de nouvelle génération. Il permet d'extraire les flux d'un serveur tiers, en l'occurrence l'application ServiceNow Réponse aux incidents de sécurité , directement vers la passerelle Check Point Next Generation Gateway à appliquer par des lames antivirus et anti-bot. L'analyste de Security Incident Response crée des entrées pour la liste de blocs Check Point à partir d'observables déterminés comme malveillants sur ServiceNow les incidents de sécurité SIR.

Pour la plupart des implémentations, une liste de demandes de blocs est un fichier csv hébergé sur un serveur Web externe. Pour cette intégration, ce serveur Web est votre ServiceNow AI Platform instance, ce qui permet au moteur de prévention des menaces de nouvelle génération Check Point d'extraire la liste des adresses IP, des URL et des domaines à bloquer.

Pour appliquer les observables bloquants sur Check Point Gateway, assurez-vous que la politique de prévention des menaces est configurée avec les lames anti-bot et anti-virus activées. Au fur et à mesure que les entrées de la liste de blocs sont modifiées, le moteur de prévention des menaces importe dynamiquement la liste à l'intervalle configuré et applique la politique sans changement de configuration ni validation sur le pare-feu. Pour cette intégration, ServiceNow AI Platform a créé une table contenant les entrées de la liste de blocs qui sont récupérées par la passerelle Check Point de nouvelle génération autorisée aux intervalles de récupération configurés.

L'intégration comprend les fonctionnalités suivantes :

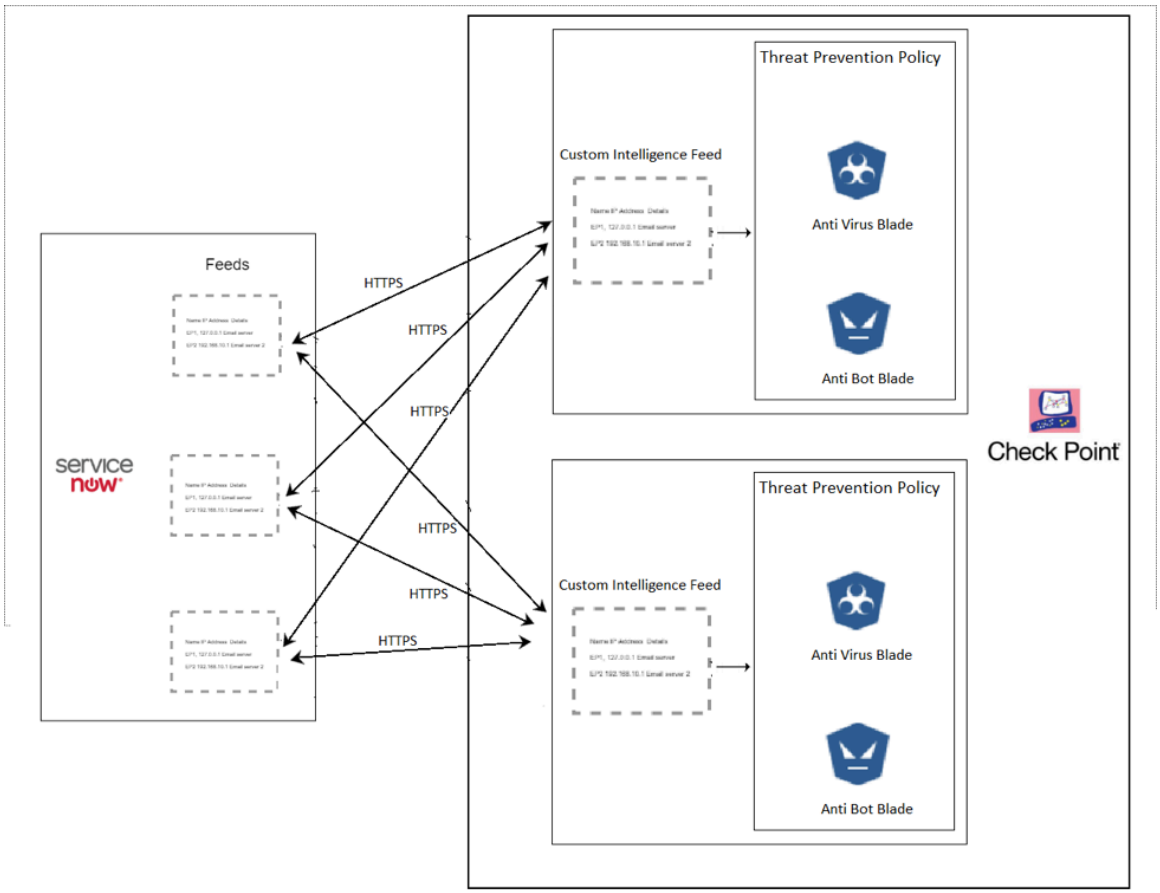
- Flexibilité pour créer plusieurs listes de blocs qui s'appliquent à plusieurs passerelles Check Point.
- Rapports détaillés sur les types de sites bloqués (hameçonnage, programmes malveillants et sites sur liste d'autorisation).
- Balisage des incidents de sécurité avec des entrées de liste de blocs par type d'observable ServiceNow AI Platform (URL, domaine, adresse IP).
- Configurer les périodes d'expiration de la liste de blocs pour conserver la taille de la liste de blocs en faisant automatiquement expirer ou en supprimant les entrées les plus anciennes.
- Recherche d'entrées de liste de blocs entre différentes listes de blocs.
- Liaison des entrées de la liste de blocs aux enregistrements d'observables et aux incidents de sécurité qui incluent des résultats de Threat Intelligence et des détails sur les raisons pour lesquelles une entrée est bloquée.

Diagramme d'architecture d'intégration

Vous trouverez ci-dessous le diagramme d'architecture de haut niveau décrivant les composants impliqués et les points d'intégration entre NOW Platform et Check Point Systems.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Le logo Check Point Systems, l'image Anti-Virus Blade et l'image Anti Bot Blade proviennent de Check Point Systems ©. Ils sont la propriété de Check Point Systems.

Modules d'extension

L'intégration nécessite que le module d'extension Réponse aux incidents de sécurité (com.snc.security_incident) soit activé.

Pour installer des modules d'extension Réponse aux incidents de sécurité :

1. Connectez-vous à votre instance avec vos informations d'identification HI.
2. Vérifiez que vous disposez du rôle d'administrateur (admin).
3. Accédez à Définition du système>plugins dans votre instance.
4. Sélectionnez et cliquez sur Réponse aux incidents de sécurité.

Une fois ces modules d'extension installés, vous pouvez charger le nouveau module d'extension d'intégration Check Point à partir du ServiceNow Store et suivre les instructions de configuration suivantes.

Versions du système d'exploitation Check Point prises en charge

Cette intégration nécessite le flux de renseignements personnalisé des lames Check Point et Anti-bot et Anti-virus. Ceux-ci sont pris en charge à partir de R80.20 et plus. Installez le correctif de la fonctionnalité d'intelligence personnalisée connue sous le nom de Check Point R80.10 Jumbo HF take 121 et versions ultérieures. Reportez-vous à la section Installation de la documentation du flux de renseignements personnalisé Check Point pour plus d'informations sur la matrice de compatibilité des produits.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Après avoir installé le correctif chaud, assurez-vous que les commandes ci-dessous sont accessibles sur Check Point Gateway. Connectez-vous à la passerelle et connectez-vous en mode expert.

```
[gw-93440b> expert
[Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

Versions de ServiceNow prises en charge

La version San Diego ou ultérieure est prise en charge.

Références

Vous trouverez ci-dessous quelques-unes des références Check Point qui sont utiles pour configurer les pré-requis.

1. Fonctionnalité des flux de renseignements personnalisés https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. Pour configurer les lames Anti-bot et Anti-Virus, reportez-vous au Guide de l'utilisateur Check Point. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Pour configurer l'inspection HTTPS sur Check Point, suivez le lien ci-dessous. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Autorisations et rôles

Les rôles ServiceNow suivants sont requis.

- Administrateur (admin) pour l'installation du module d'extension de l'application d'intégration
- Administrateur d'incident de sécurité (sn_si.admin) pour créer des listes de blocs dans ServiceNow et approuver les demandes d'ajout et de désactivation d'entrées de liste de blocage.
- Analyste de sécurité (également appelé ici analyste SOC, sn_si.analyst) pour la création et la gestion des enregistrements d'entrée de la liste de blocs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur l'affectation du rôle d'analyste de sécurité, sur le site Web de la documentation ServiceNow , naviguez vers Opérations de sécurité>Réponse aux incidents de sécurité> Affectation d'analystes de sécurité.

Configurer Check Point NGTP

Avant de pouvoir utiliser l'intégration Check Point NGTP , vous devez créer un compte API, configurer des politiques et activer l'intégration.

Créer un compte d'API pour l'intégration Check Point NGTP

Un rôle de compte API est requis dans votre ServiceNow AI Platform instance pour cette intégration. Le nom d'utilisateur et le ServiceNow AI Platform mot de passe associés à ce compte sont créés et saisis dans Check Point afin que Check Point s'authentifie avec le lors de la ServiceNow AI Platform récupération des entrées de la liste de blocs.

Avant de commencer

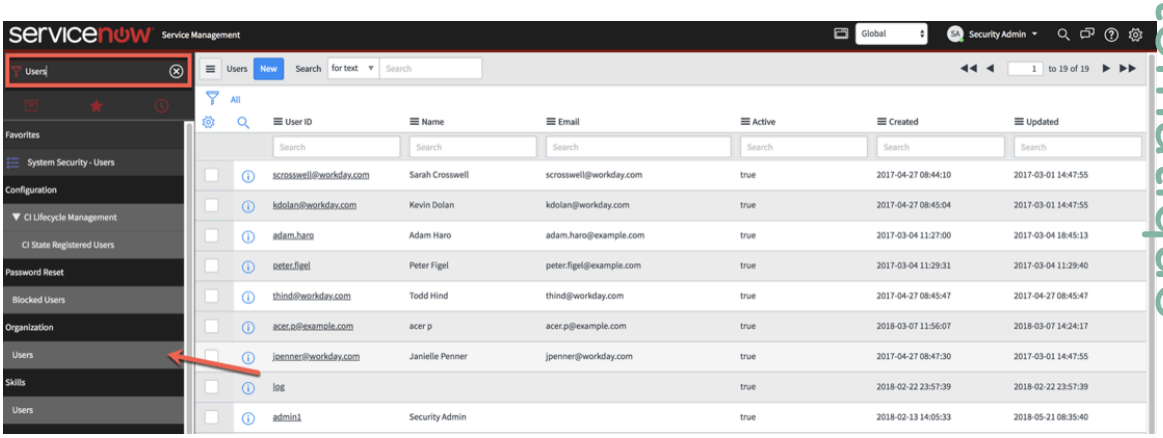
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

L'administrateur ServiceNow AI Platform crée un rôle de compte API (sn_sec_checkpoint.api_account_access). Ce compte est utilisé exclusivement pour saisir les informations d'identification requises pour l'authentification sur Check Point, afin que la passerelle puisse récupérer les listes de blocs à partir ServiceNow AI Platform du . Il s'agit d'un compte d'utilisateur d'API distinct et unique dans l'instance ServiceNow AI Platform , affecté à l'administrateur Check Point.

Procédure

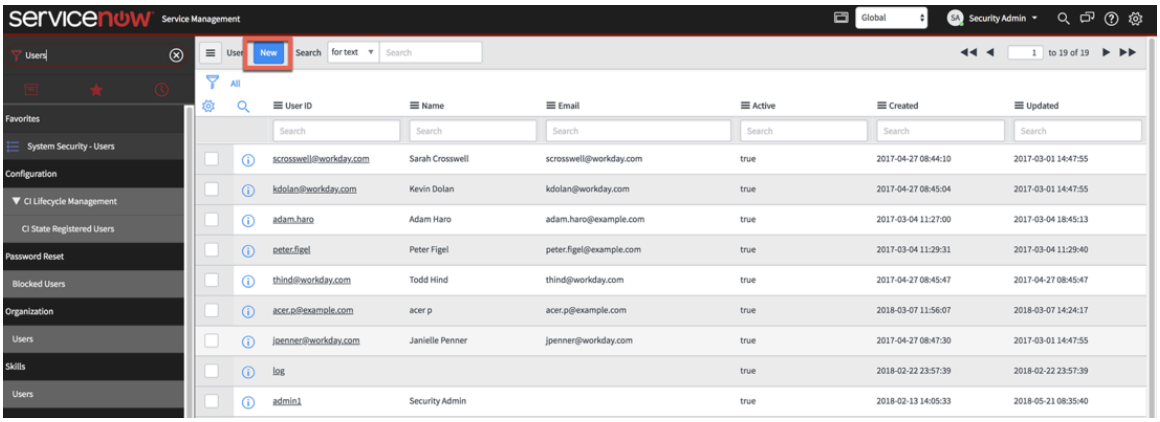
1. Accédez à la **Tous** > **Organisation** > **Utilisateurs**.
2. Cliquez sur le module **Utilisateurs** .



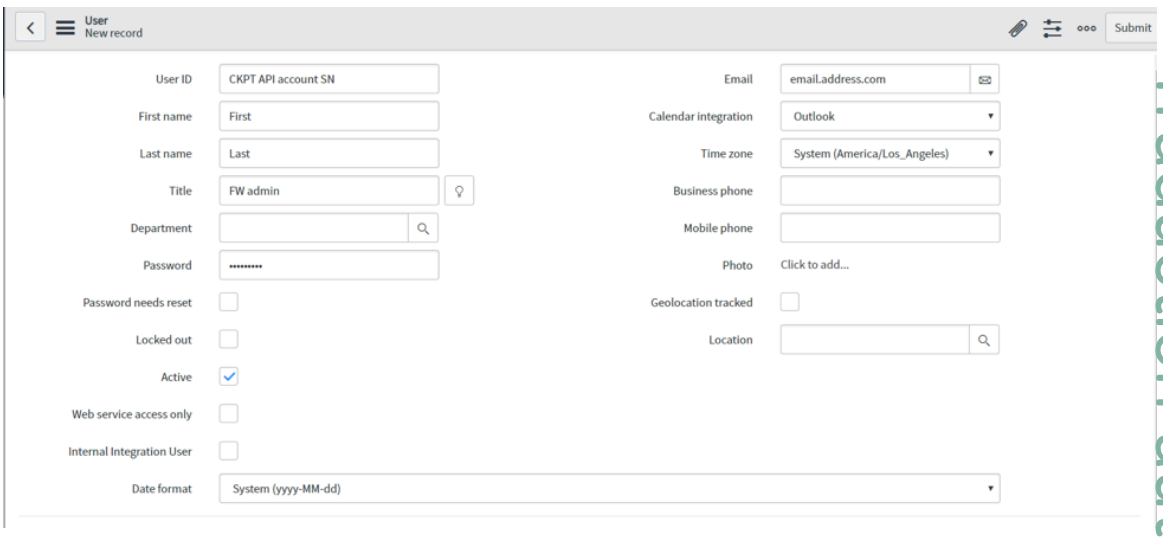
3. Cliquez sur **Nouveau** dans la liste Utilisateurs qui s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un nouveau formulaire s'affiche.



4. Remplissez le formulaire selon vos besoins.

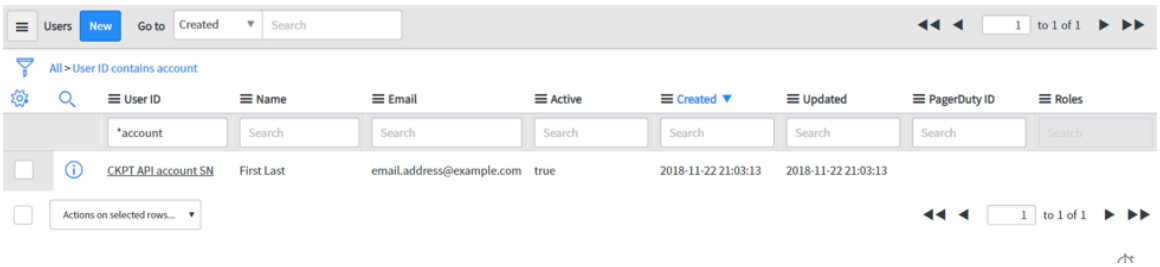
Remarque : Les valeurs d'ID d'utilisateur, de titre et d'adresse e-mail indiquées dans la table et la figure suivantes sont des exemples de valeurs.

Champ	Description
ID d'utilisateur	ID d'utilisateur unique pour le rôle dans votre ServiceNow AI Platform instance. Cet ID utilisateur est saisi dans le champ **Nom d'utilisateur** de la section **Authentification client** de la passerelle Check Point de configuration de la liste de blocs. Par exemple, le compte d'API CKPT SN.
Prénom	Personne que vous affectez
Nom	Personne que vous affectez
Titre	Fonction, par exemple, administrateur FW.
Mot de passe	Mot de passe unique créé pour ce rôle. Ce mot de passe est saisi dans le champ **Mot de passe** de la section **Authentification client** de la configuration de la liste de blocs sur la passerelle Check Point.
E-mail	Adresse e-mail unique

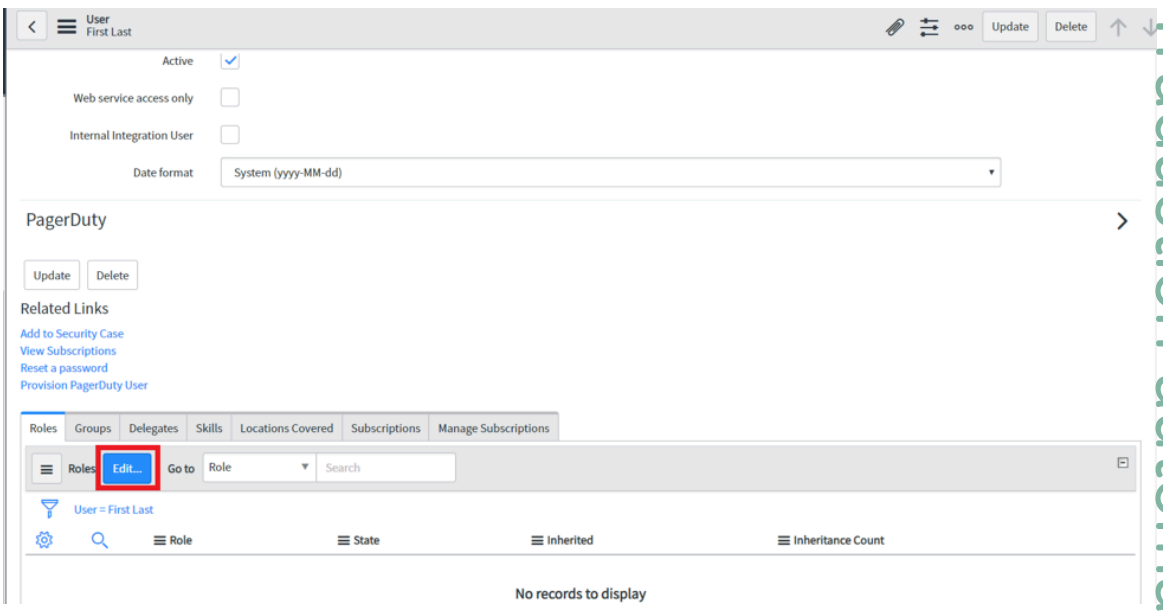
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Envoyer**.
   Une fois le rôle soumis, vous pouvez l'affecter.
6. Dans la liste des utilisateurs dans la colonne ID d'utilisateur, cliquez sur le nom de l'ID d'utilisateur que vous avez saisi, CKPTAPI account SN, par exemple.



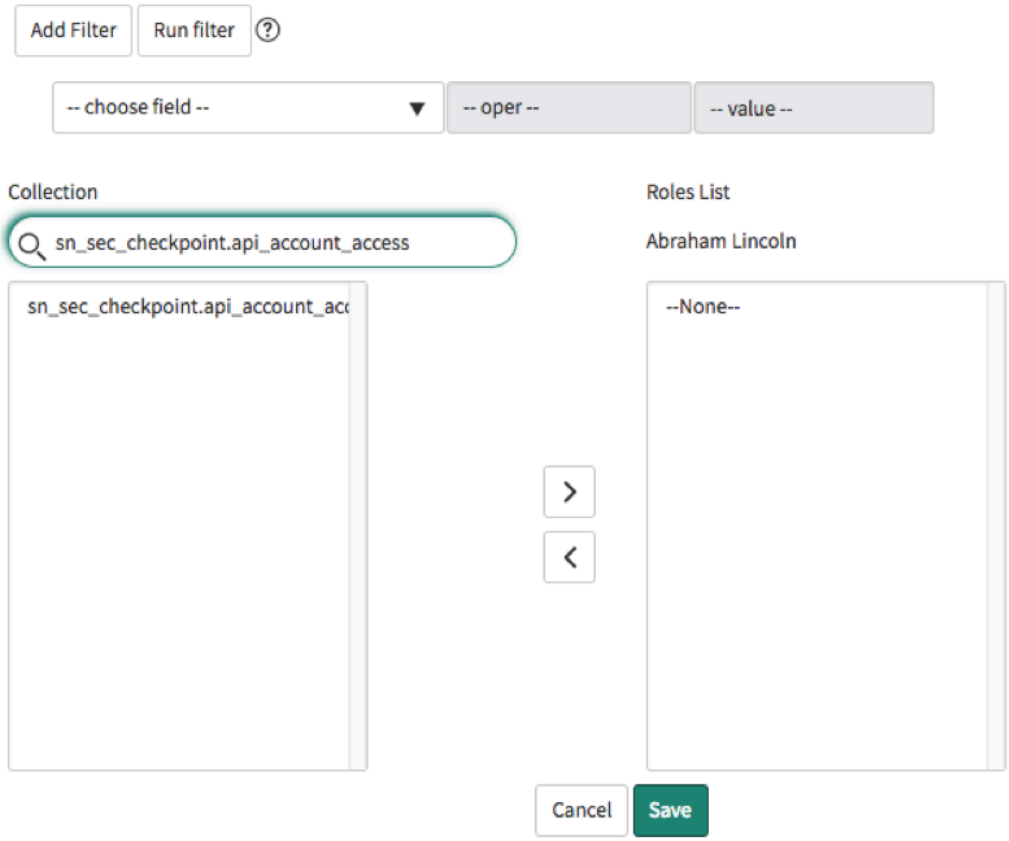
7. Dans l'enregistrement ouvert dans la section Rôles, cliquez sur **Modifier**.



8. Dans le formulaire **Modifier les membres** qui s'affiche, saisissez sn_sec_checkpoint.api_account_access dans le champ **Collecte** .

Traduction automatique

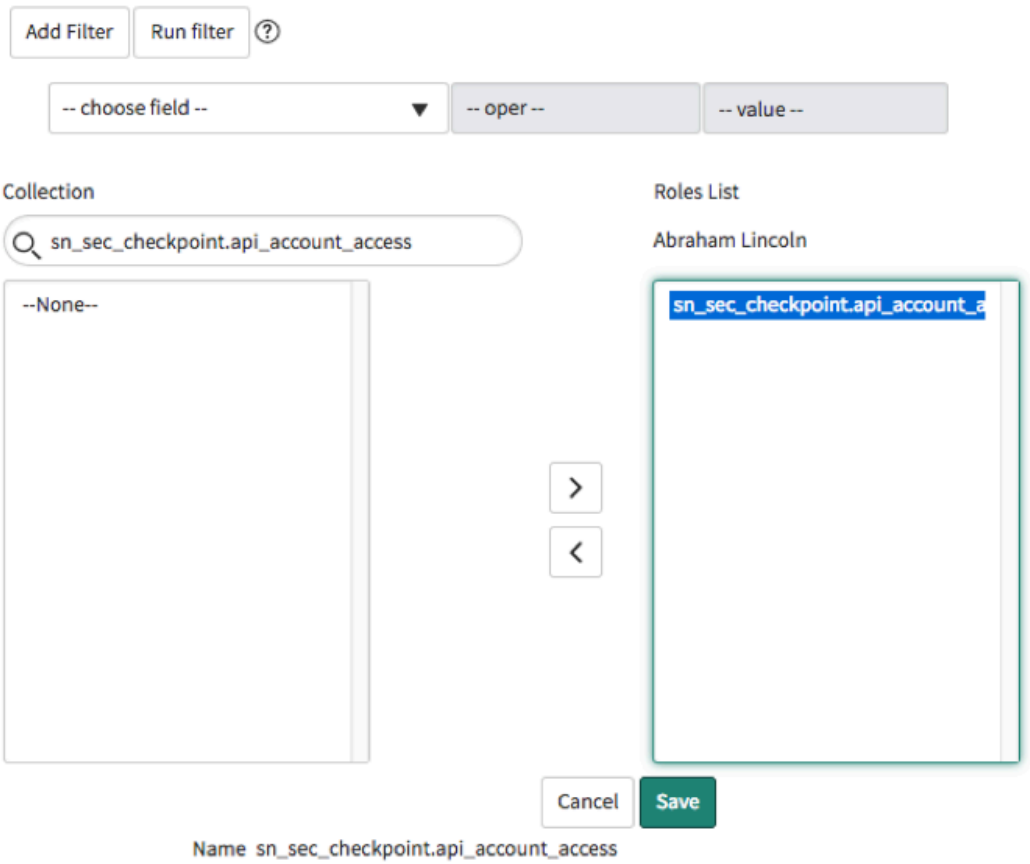
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Dans la colonne **Collecte** , sélectionnez puis déplacez sn_sec_checkpoint.api_account_access vers la **liste Rôles**.
10. Cliquez sur **Enregistrer**.
11. Accédez à **Utilisateurs** et, dans la colonne **Utilisateur** de la liste, cliquez sur le nom d'ID que vous avez créé pour le rôle (compte d'API CKPT SN).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





12. L’enregistrement utilisateur s’affiche. Cet enregistrement vérifie que le compte d’utilisateur a été affecté.

Configurer l'intégration Check Point NGTP

Effectuez les étapes suivantes pour configurer l’intégration Check Point Next Generation Threat Prevention . Cela permettrait de s’assurer que les conditions préalables à l’intégration sont en place.

Avant de commencer

Rôle requis : admin

Procédure

1. Vérifiez que la politique de prévention des menaces est configurée avec les lames antibot et antivirus activées.
   Reportez-vous au Guide de l’utilisateur Check Point mentionné dans la section Référence pour obtenir des informations détaillées sur la configuration des lames anti-bot et antivirus.

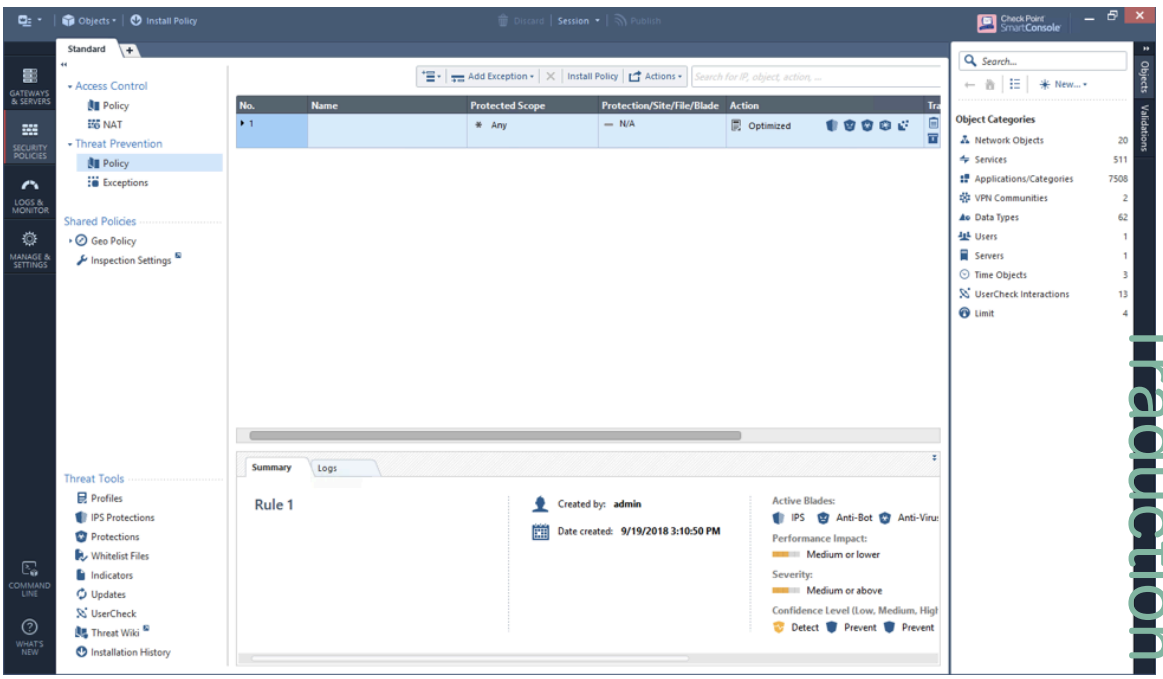
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

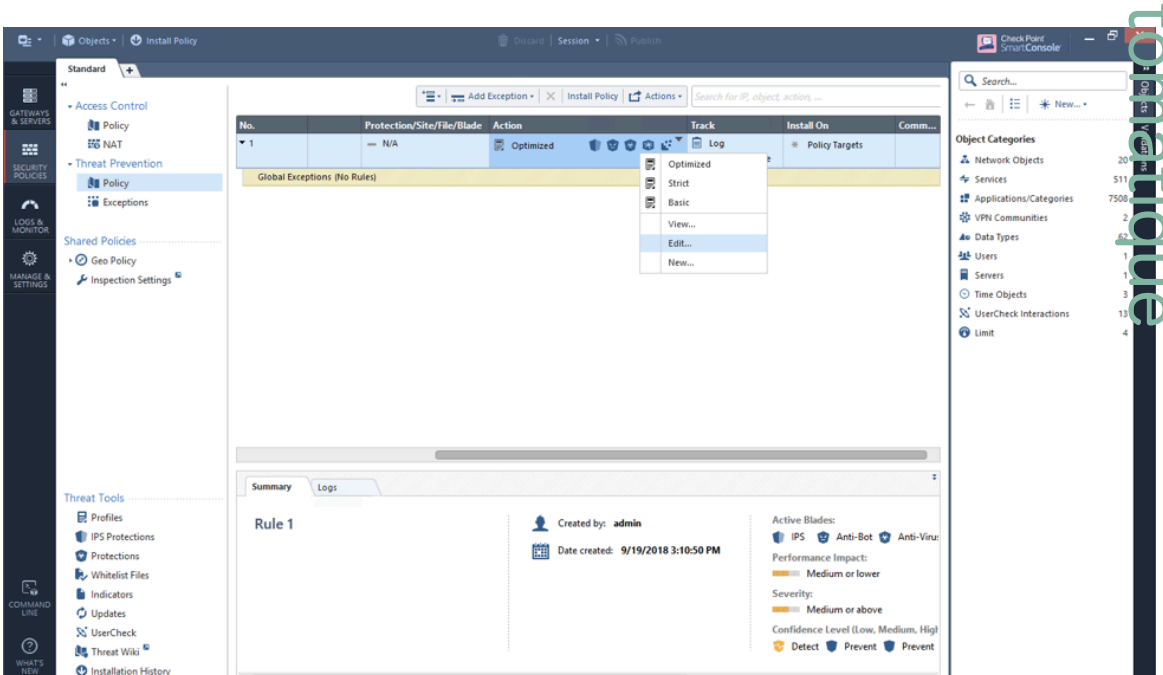
Remarque : Les images de cette rubrique sont privilégiées et exclusives et sont utilisées avec la permission de Check Point Software Technologies, Ltd.

a. Connectez-vous à **la Smart Console**.

b. Accédez à la **Politiques de sécurité** > **Prévention des menaces** > **Politique**.



c. Ouvrez la politique de prévention des menaces en mode d'édition.



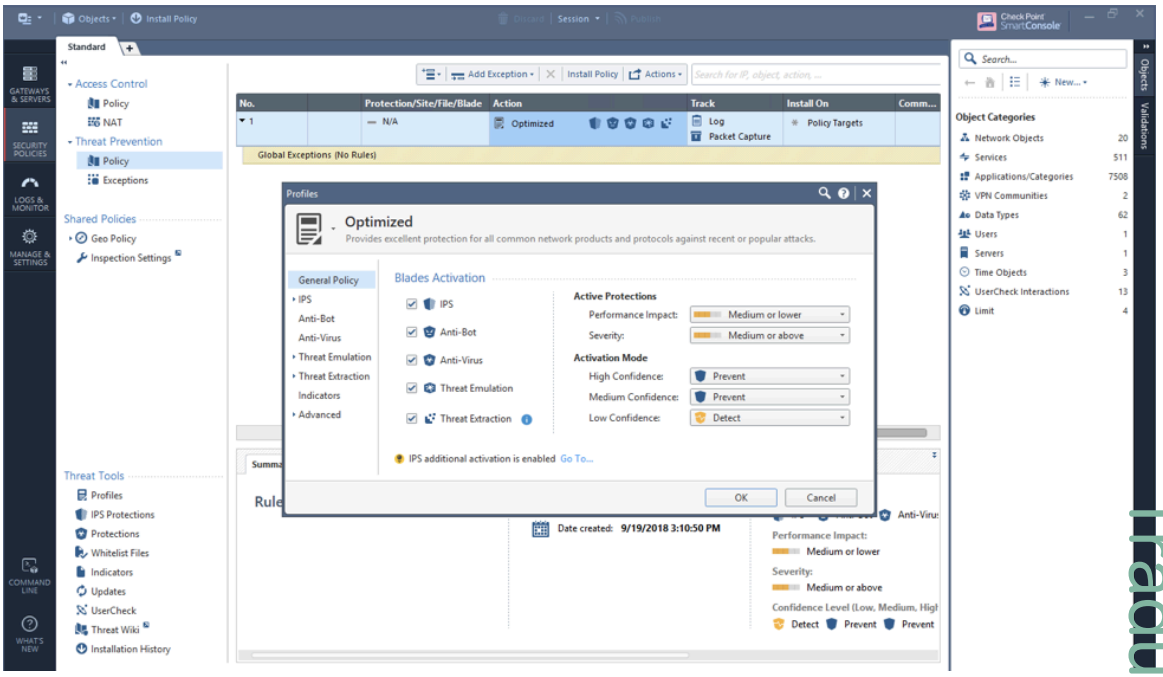
d. Protections actives # La gravité doit être « Moyenne ou supérieure »

e. Le mode d'activation # la confiance élevée doit être « Empêcher »

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Blades Activation à Anti-Virus et Anti-Bot doivent être sélectionnés.



g. Publiez les changements (le cas échéant) et installez la politique.

2. Si ce n'est pas déjà fait, les flux de renseignements personnalisés doivent être ajoutés après l'activation des lames anti-bot et antivirus.
Reportez-vous à la section Installation de la documentation de la fonctionnalité de flux de renseignements personnalisé Check Point. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

3. Si ce n'est pas déjà fait, configurez Check Point Gateway pour acheminer tout le trafic Internet via un proxy HTTP (si vous configurez HTTPS Inspection).

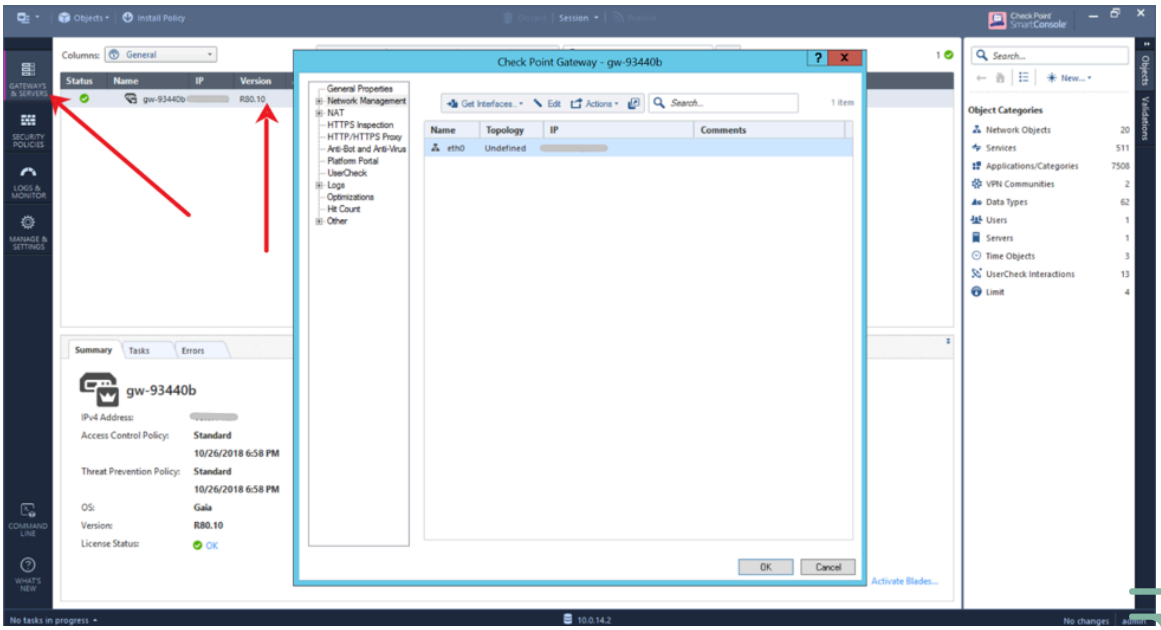
> **Remarque :** Pour le blocage d'URL sur Check Point NGTP, certains paramètres doivent être assurés. Le trafic Internet HTTPS utilise le protocole SSL (Secure Sockets Layer) et est crypté pour assurer la confidentialité des données. Cependant, HTTPS peut masquer le trafic malveillant qui aurait dû être bloqué. Pour que Check Point Gateway obtienne une visibilité sur le trafic HTTPS, acheminez le trafic via un proxy HTTP ou configurez une inspection HTTPS (recommandé). Cette section détaille les étapes à suivre pour configurer le proxy HTTP sur Check Point Gateway.

a. Connectez-vous à **la Smart Console**.

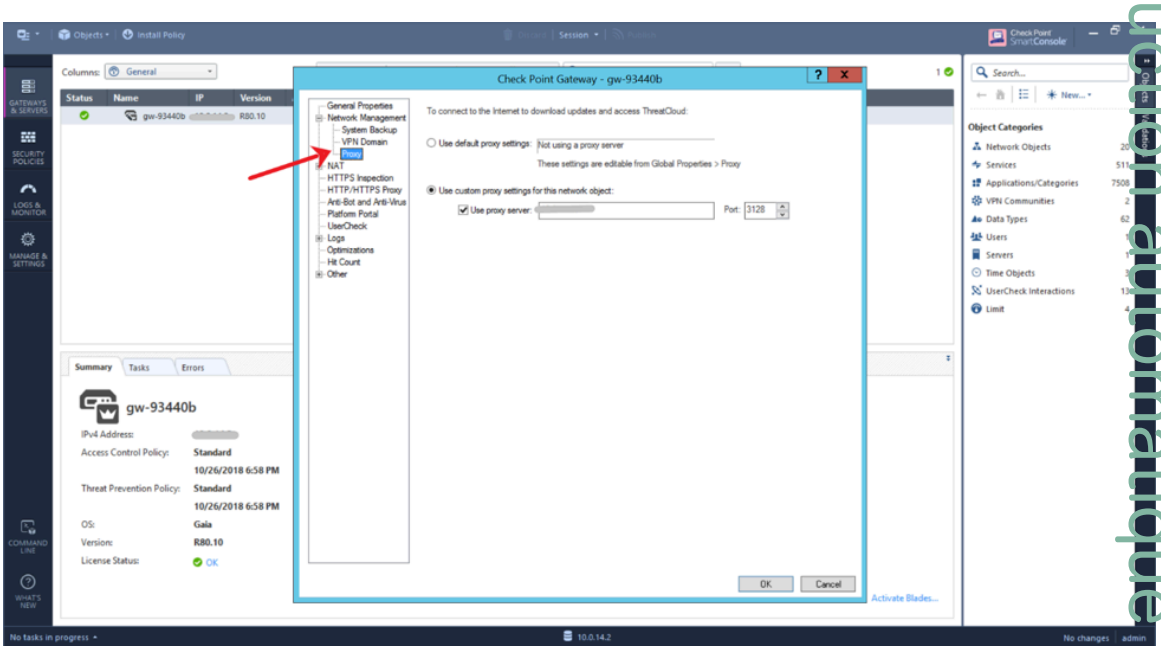
b. Accédez à **Serveurs et passerelles**, puis double-cliquez sur le serveur applicable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Accédez à la **Gestion du réseau** > **Proxy**.



d. Fournissez les détails du proxy à utiliser pour acheminer le trafic HTTP.

e. Assurez-vous que les requêtes HTTP du point de terminaison client sont envoyées via le proxy HTTP.

4. Si ce n'est pas déjà fait, activez l'inspection HTTPS (si le proxy HTTP est configuré).
Lorsque la majeure partie du trafic se fait via SSL, il est recommandé d'utiliser HTTPS Inspection Blade.
Cela rend le trafic transparent pour GW. Activez l'inspection HTTPS sur Check Point Gateway, comme suit.

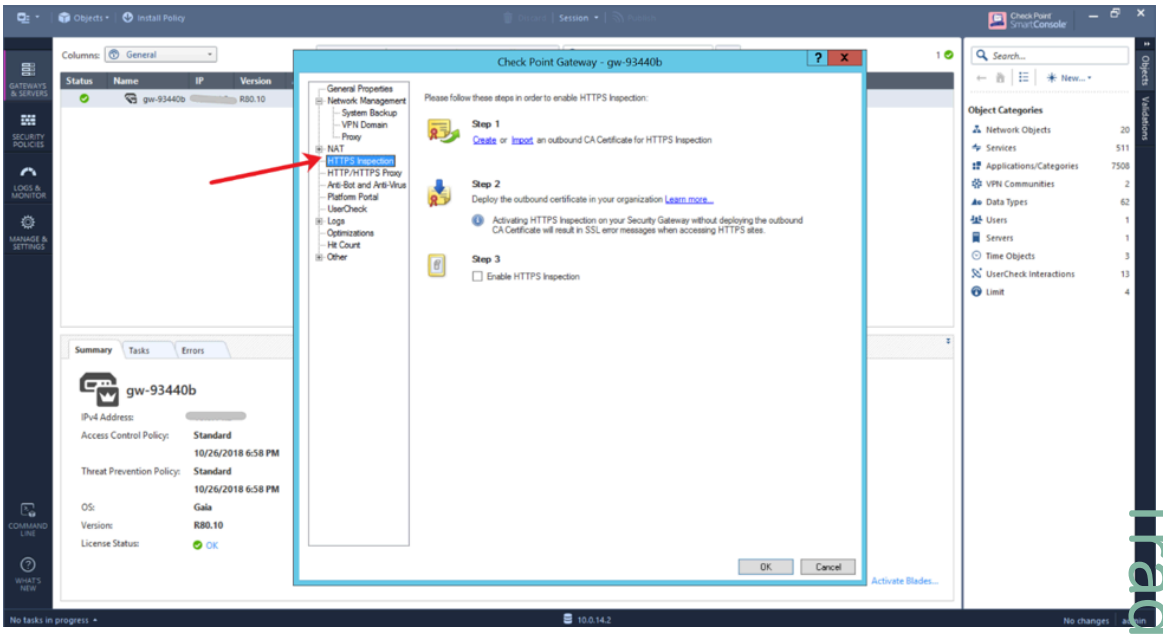
a. Connectez-vous à **la Smart Console**.

b. Accédez à **Serveurs et passerelles**, puis double-cliquez sur le serveur applicable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Accédez à **l'inspection HTTPS**.



d. Suivez les étapes de configuration de l'inspection HTTPS dans le guide de l'utilisateur Check Point.

Activer l'intégration Check Point NGTP

Si vous n'avez pas installé l'application, suivez les instructions pour l'installer.

Avant de commencer
Rôle requis : admin

Procédure

1. Connectez-vous à l'instance sur laquelle vous souhaitez installer l'application.
2. Accédez à la **Applications système** > **Applications**.
3. Cliquez sur l'onglet **Téléchargements** .
   Une liste des applications disponibles pour l'installation s'affiche.
4. Localisez l'application Check Point Next Generation Threat Prevention , sélectionnez-la, puis cliquez sur **Installer**.
   Votre application est automatiquement installée sur votre instance.

Utiliser des listes de blocs

L'intégration ServiceNow Check Point Next Generation Threat Prevention prend en charge les listes de blocs qui acceptent les observables d'adresse IP, d'URL et de domaine.

ServiceNow La liste de blocs configurée est un fichier CSV hébergé sur un serveur Web externe, qui est l'instance ServiceNow AI Platform pour cette intégration. Le flux d'intelligence personnalisé est configuré sur la passerelle Check Point, qui extrait les adresses IP, les URL et les domaines à partir de l'intervalle ServiceNow AI Platform préconfiguré.

Cette intégration prend en charge trois types de listes de blocs :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Adresse IP (comprend une adresse IP individuelle (IPv4 uniquement) pour la liste de blocs et des blocs CIDR (plages) d'adresses pour la liste d'autorisation).
- URL
- Domaine

Observables pris en charge par l'intégration Check Point NGTP

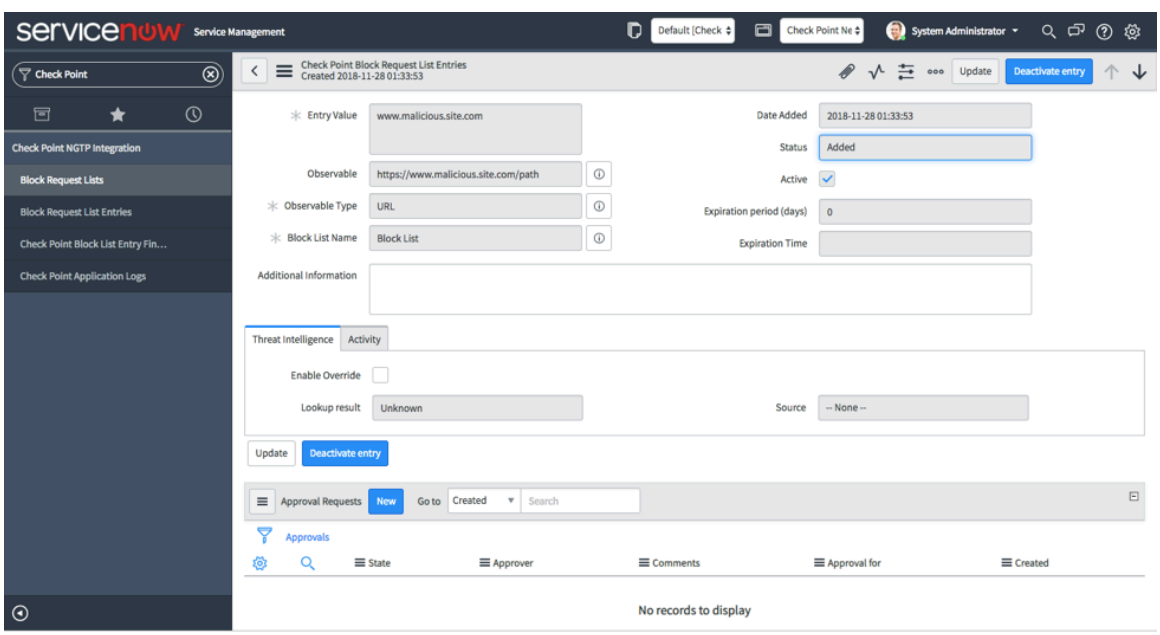
Cette section répertorie des descriptions des observables pris en charge par cette intégration et des exemples de formats pour chaque type.

Type d'observable	Exemples	Description
Domaine	• example.com • mail.example.com	Les caractères génériques ne sont pas pris en charge.
Adresse IP	95.153.103.54 (IPv4)	Représente une adresse d'interface unique et distincte. L'intégration ne prend en charge que les formats IPv4 et CIDR (le format CIDR n'est pris en charge qu'à des fins de liste d'autorisation). À des fins de liste d'autorisation, l'intégration prend en charge les observables d'adresse IP, notamment les plages CIDR (Classless Inter-Domain Routing), par exemple, 95.153.100.0/22. **Remarque :** Un message d'erreur s'affiche lorsque vous essayez de joindre une seule adresse IP à une liste de blocs que vous avez déjà autorisée répertoriée dans le cadre d'une plage CIDR. Par exemple, l'adresse unique 95.153.103.54 fait partie de la plage CIDR représentée par 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• https://www.example.com • http://www.example.com	Description : les URL HTTPS sont formatées par l'application pour couper le chemin d'accès à partir de l'URL et conserver uniquement le nom de domaine. Check Point NGTP s'appuie sur la requête HTTP CONNECT pour évaluer le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

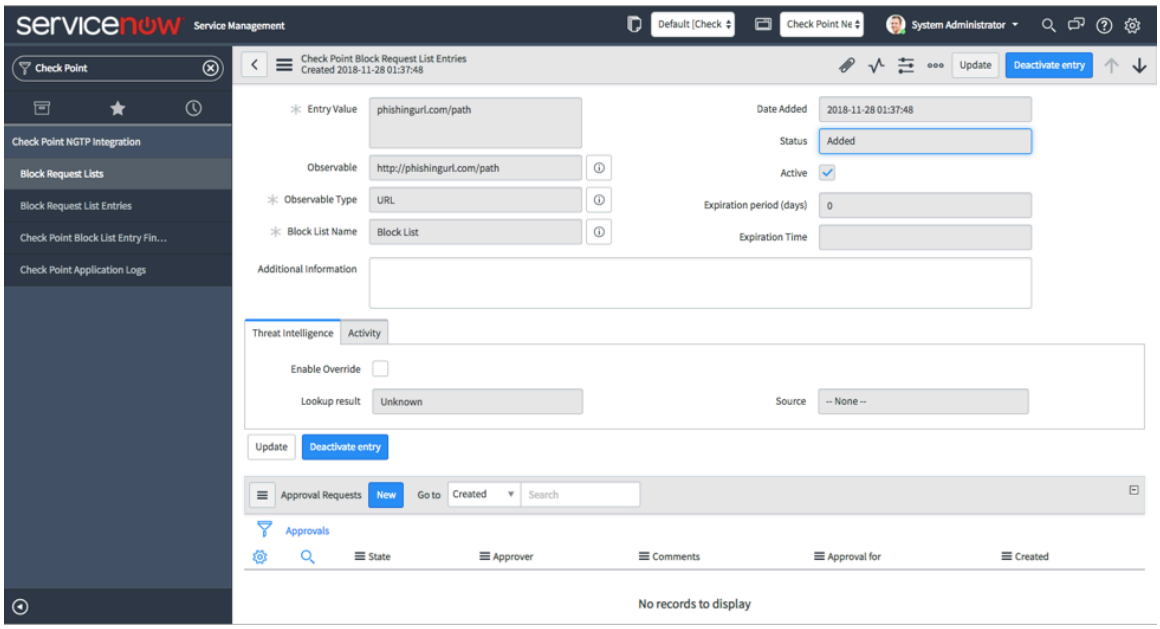
Type d'observable	Exemples	Description
		trafic Web et appliquer le blocage. Pour la demande HTTPS CONNECT, l'URL entière n'est pas visible dans la demande et seul le nom de domaine est visible. Lorsqu'un utilisateur bloque une URL HTTPS avec un chemin d'accès spécifique (exemple : https://www.example.com/path), l'application rogne automatiquement le chemin d'accès (www.example.com). L'application conserve la relation entre l'observable d'origine et l'URL formatée. Vous trouverez ci-dessous la capture d'écran de l'entrée de la liste de blocs qui montre l'URL formatée et l'observable d'origine.



Pour les URL HTTP avec un chemin spécifique (par exemple, http://www.example.com/path), Check Point bloque l'URL spécifiée, car l'URL entière est visible dans la requête CONNECT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Créer une liste de blocs pour l'intégration Check Point NGTP

Créez une liste de blocs dans votre ServiceNow AI Platform instance. Une fois approuvées et activées, vous pouvez créer des entrées pour ces listes de blocs à partir d'observables jugés malveillants sur les incidents de Réponse aux incidents de sécurité (SIR) de Now Platform et demander l'approbation pour les bloquer.

Avant de commencer

Rôle requis : Administrateur d'incidents de sécurité (sn_si.admin)

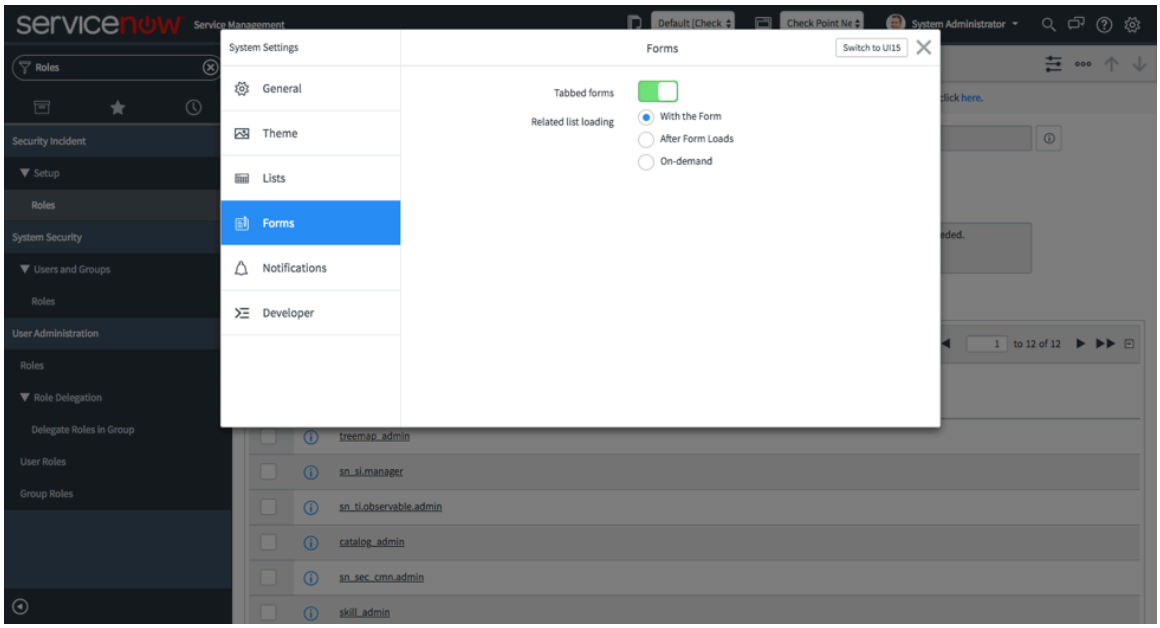
Pourquoi et quand exécuter cette tâche

Créez la liste de blocs sur votre ServiceNow AI Platform instance afin que Check Point puisse importer des objets (adresses IP, URL, domaines) inclus dans la liste. Le flux d'intelligence personnalisé est configuré sur la passerelle Check Point qui extrait les adresses IP, les URL et les domaines de la Now Platform à un intervalle préconfiguré. Pour garantir le blocage des observables, la politique de prévention des menaces doit être configurée avec les lames antibot et antivirus activées.

Remarque : Les figures de cette rubrique sont affichées avec **les formulaires à onglets** effacés dans Paramètres système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Procédure

1. Une fois l'installation de l'application terminée, accédez à **Intégrations** > **Configurations d'intégration**.
2. Localisez la carte **Check Point Next Generation Threat Prevention** et cliquez sur **Configurer**.

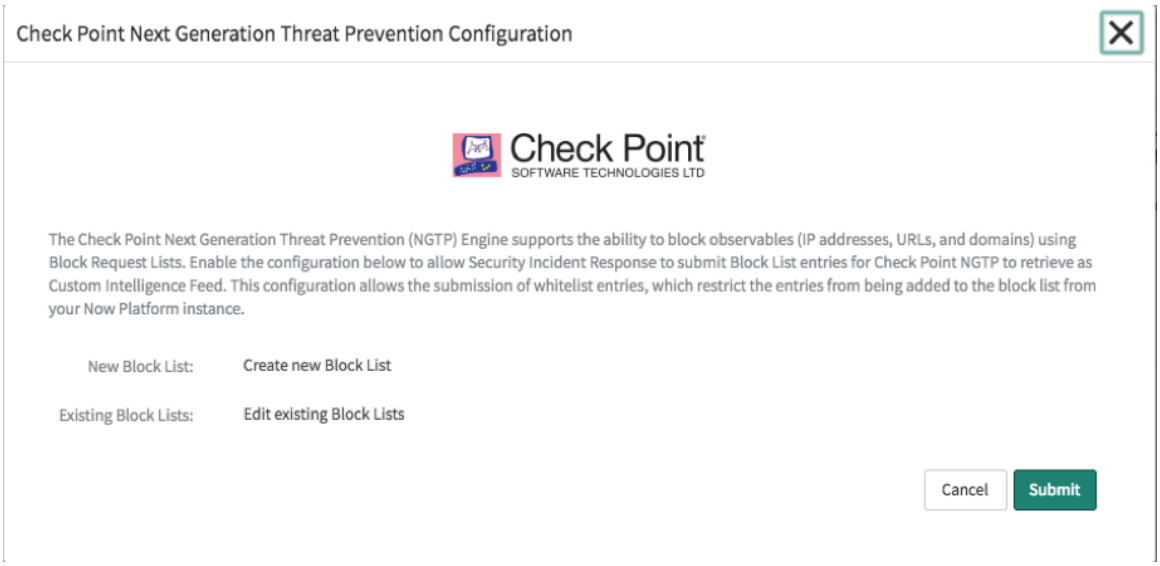


Remarque : Contenu privilégié et propriétaire utilisé avec l'autorisation de Check Point Software Technologies, Ltd.

3. Cliquez sur **Créer une nouvelle liste de blocs**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Remplissez les champs du formulaire.

Champ	Description
Nom	Nom de la liste de demandes de blocs Check Point. Incluez le type d'observable (URL, IP, domaine) dans ce champ afin que l'analyste de sécurité puisse facilement reconnaître l'intention de la liste de blocs par son nom. Le nom doit également indiquer clairement à quelle stratégie de pare-feu ces objets de liste de blocs sont mappés. Voici quelques exemples de noms de liste de blocage : IP de programme malveillant sortant ou URL de hameçonnage sortant.
Actif	Cette case est décochée par défaut pour indiquer que la liste de blocs est inactive. Lorsqu'elle est inactive, la liste de blocs ne peut pas recevoir d'entrées supplémentaires. Lorsque la case à cocher est sélectionnée (lorsque la demande de changement est fermée ou que la demande de changement n'est pas générée), la liste de blocs est activée et disponible pour les entrées de liste de blocs.
Balise d'affichage	La case à cocher est sélectionnée par défaut pour baliser automatiquement l'observable et l'enregistrement d'incident de sécurité associé si l'observable est bloqué sur la liste de blocage. Lorsque cette option est sélectionnée, le champ « Balise pour les observables » est disponible sur le formulaire. **Remarque :** Un nom de balise est créé par défaut à partir de la valeur que vous entrez dans le champ Nom avec un préfixe Check Point, par exemple, Check Point-Malware OutBound IP. Vous pouvez modifier le nom et la couleur de la balise. Le nom de la balise est affiché dans le champ « Balise pour les observables », une fois la liste de blocs enregistrée. Lorsque la case est décochée, aucune balise n'est créée et le champ « Balise pour les observables » n'est pas disponible sur le formulaire.

Traduction automatique

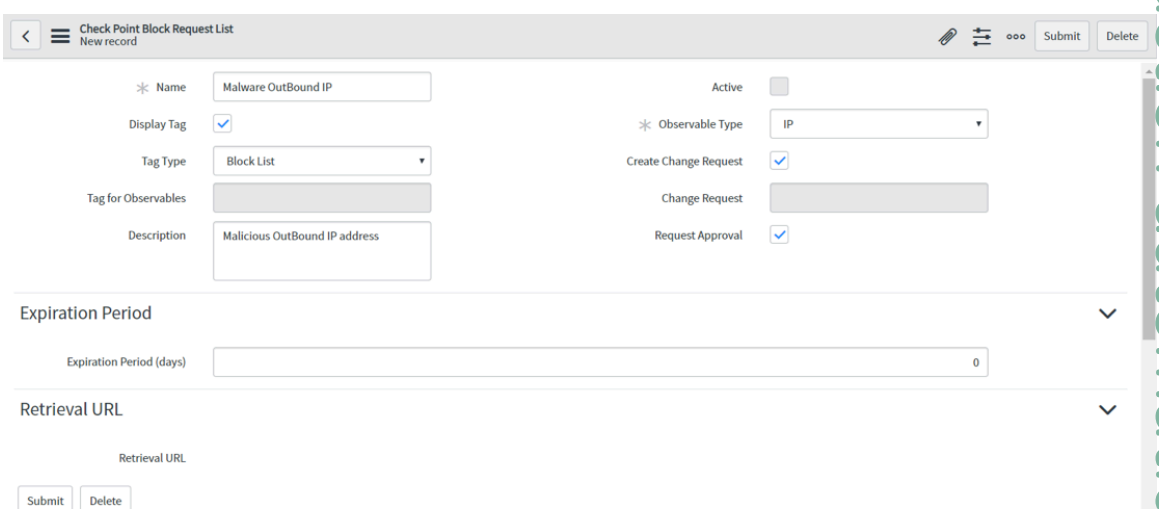
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type d'observable	Sélectionnez un type d'observable que cette liste de blocs accepte dans la liste : adresse IP (y compris CIDR pour la liste d'autorisation), URL ou domaine.
Type de balise	Balises disponibles dans la liste. Une liste de blocs est une liste d'observables que vous souhaitez que Check Point Next Generation Threat Prevention bloque. Une liste d'autorisation est une liste d'observables que vous ne souhaitez en aucun cas bloquer dans Check Point Next Generation Threat Prevention. Par défaut, la couleur de la balise de la liste de blocs est le noir et la couleur de la balise de la liste d'autorisation est le gris. Vous pouvez changer la couleur.
Créer une demande de changement	Cette case à cocher est sélectionnée par défaut pour créer automatiquement une demande de changement et des tâches de changement dans votre ServiceNow AI Platform instance, qui sont jointes à l'enregistrement de la liste de blocs. La demande de changement est utilisée pour configurer l'URL de récupération de la liste de blocs dans la passerelle de pare-feu Check Point Next Generation. Cette option est recommandée si votre administrateur de pare-feu utilise également le pour modifier la politique ou les règles du ServiceNow AI Platform pare-feu. Si vous créez une demande, une fois qu'elle est fermée, la liste de blocs est automatiquement activée. Décochez la case pour activer manuellement la liste de blocs après avoir reçu une notification par e-mail de l'administrateur du pare-feu indiquant que le flux de renseignements personnalisé a été configuré sur toutes les passerelles Check Point. Lorsque la case Créer une demande de changement est décochée, le champ Demande de changement n'est pas disponible.
Demander l'approbation	Cette case à cocher est sélectionnée par défaut pour demander des approbations pour activer/supprimer des entrées de liste de blocs des listes de blocs. L'approbation est demandée aux utilisateurs ayant le rôle d'administrateur d'incidents de sécurité (sn_si.admin). La demande d'approbation sera envoyée par e-mail aux approbateurs. Une fois l'approbation acceptée, l'entrée sera activée sur cette liste de blocage. Si la case n'est pas cochée, les entrées de cette liste de blocs ne suivent pas le workflow d'approbation et sont directement activées sur la liste de blocs.
Balise pour observable	ce champ n'est affiché que si la case Afficher la balise est cochée. Le champ est automatiquement renseigné une fois la liste de blocs enregistrée avec une valeur par défaut du champ Nom. Si la liste de blocage est créée avec le nom « URL du programme malveillant », le nom de la balise dérivé est « Liste de blocage – URL du programme malveillant »
Demande de changement	Lorsque la case Créer une demande de changement est cochée, le numéro de la demande de changement s'affiche sur l'instance Now Platform une fois la liste de blocs enregistrée.

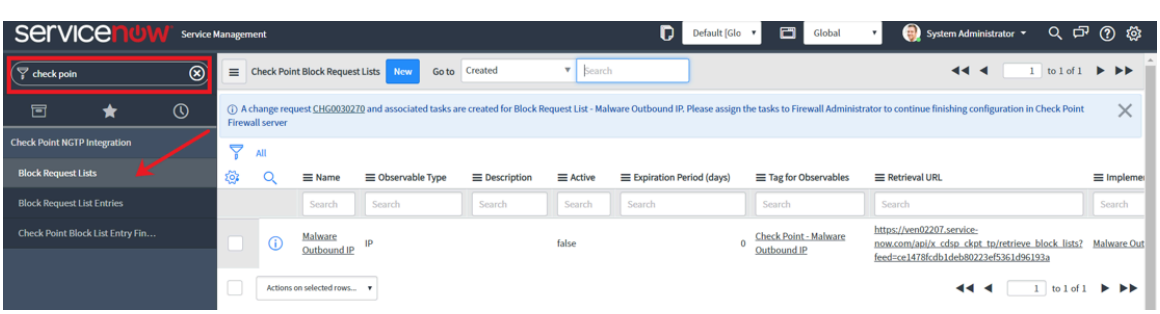
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Lorsque la case à cocher Créer une demande de changement est désactivée, ce champ n'apparaît pas.
Description	Description de la liste de blocs Check Point. Le nom contient généralement les types de sites et d'observables que vous vous attendez à voir figurer sur cette liste bloquée, et vous pouvez utiliser ce champ pour plus de détails.
Période d'expiration (jours)	Période d'expiration de la liste bloquée. 0 (valeur par défaut) indique que l'entrée de la liste de blocs n'expire jamais. Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous saisissez. Vous pouvez saisir une valeur minimale de 1, soit 24 heures, mais il n'y a pas de valeur maximale.
URL de récupération	L'URL de récupération sera générée automatiquement, une fois la liste de blocs enregistrée. Pour configurer cette liste de blocs sur les passerelles Check Point, vous devez utiliser cette URL. Une fois cette URL configurée, Check Point extrait les observables à bloquer au format CSV.



5. Cliquez sur **Envoyer**.
6. Si la liste de demandes de blocs Check Point n'est pas affichée, accédez à **Intégration Check Point NGTP** > **Listes de demandes de blocs**.

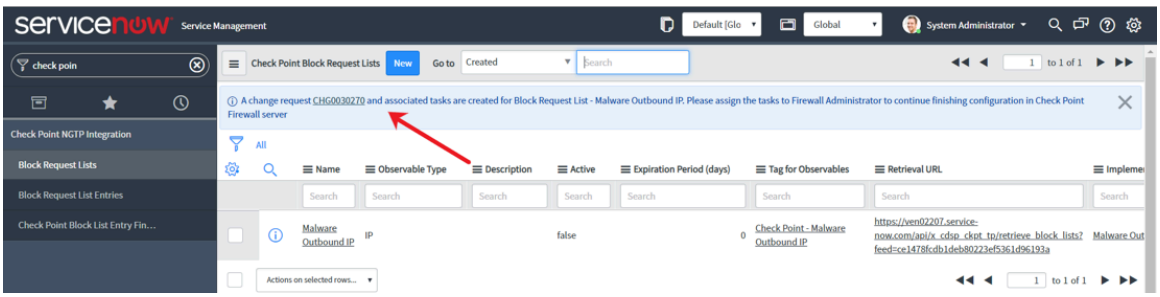


La nouvelle liste de blocs s'affiche. L'état de la liste de blocs est toujours inactif (faux), ce qui signifie que la liste de blocs n'est pas disponible pour accepter des entrées. Si la création d'une demande de changement

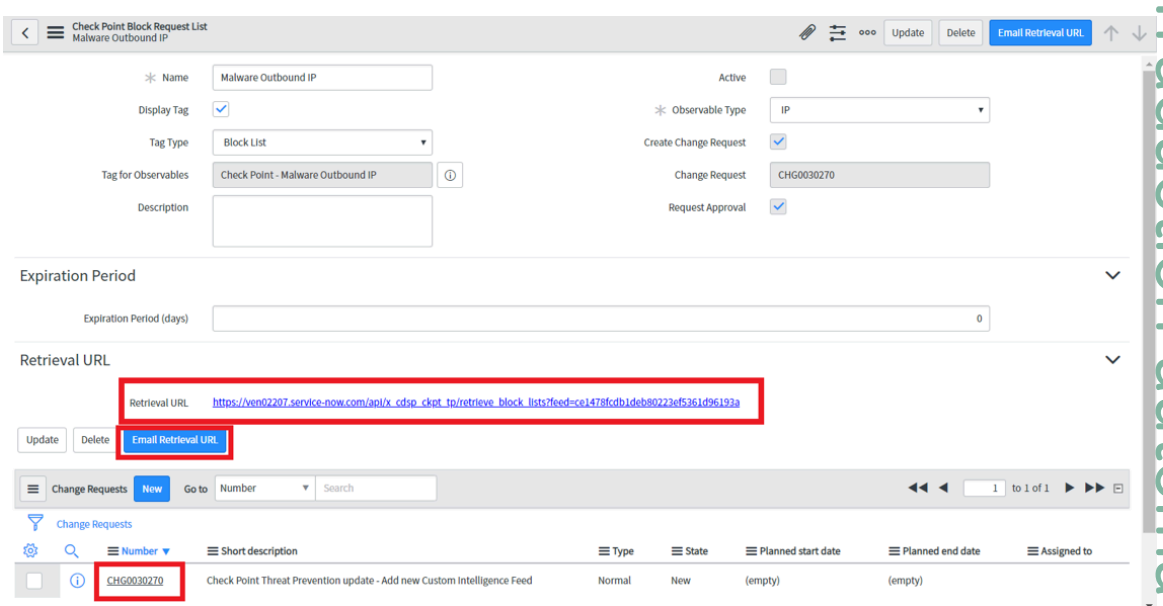
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a été configurée, un message s'affiche indiquant qu'une demande de changement et des tâches ont été créées dans votre ServiceNow AI Platform instance.



7. Dans la colonne **Nom** , cliquez sur un élément pour ouvrir l'enregistrement.
   L'enregistrement de la liste de blocs s'affiche. Cet exemple montre une liste de blocage d'adresses IP sortantes de programmes malveillants. Les champs, options et liens suivants sont affichés dans le nouvel enregistrement après soumission et décrits dans le tableau suivant.



Champ	Description
URL de récupération d'e-mail	Envoie par e-mail un avis indiquant que le lien de bloc est disponible pour configuration à l'administrateur du pare-feu Check Point.
URL de récupération	Cette URL est utilisée pour configurer le flux de renseignements personnalisé sur les passerelles Check Point. **Remarque :** Si vos paramètres système sont définis sur Formulaires à onglets, ce lien s'affiche dans l'onglet Informations de récupération de la liste de blocs au bas de l'enregistrement.
ServiceNow AI Platform Demande de changement	Un lien vers l'enregistrement de la demande de changement s'affiche dans la section Demandes de changement lorsqu'elle est configurée, et le numéro de la demande s'affiche dans le champ Demande de changement.
Mettre à jour	Modifiez les données et mettez à jour les champs modifiables.
Supprimer	Supprimez l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Créez et ajoutez d'autres listes de blocs selon vos besoins.
   Les listes de blocs sont affichées sur la page des listes de demandes de blocs Check Point.

Que faire ensuite

Activez la liste de demandes de blocs manuellement ou avec une demande de ServiceNow AI Platform changement.

Activer une liste de blocs pour l'intégration Check Point NGTP

Une fois que la liste de blocs a été créée dans Ur ServiceNow AI Platform et que l'URL est disponible, l'administrateur Check Point configure la liste de blocs en tant que flux de renseignements personnalisé sur toutes les passerelles Check Point Next Generation. Avant de pouvoir accepter des entrées de liste de blocs, la liste de blocs doit être configurée dans Check Point et activée dans le ServiceNow AI Platform.

Avant de commencer

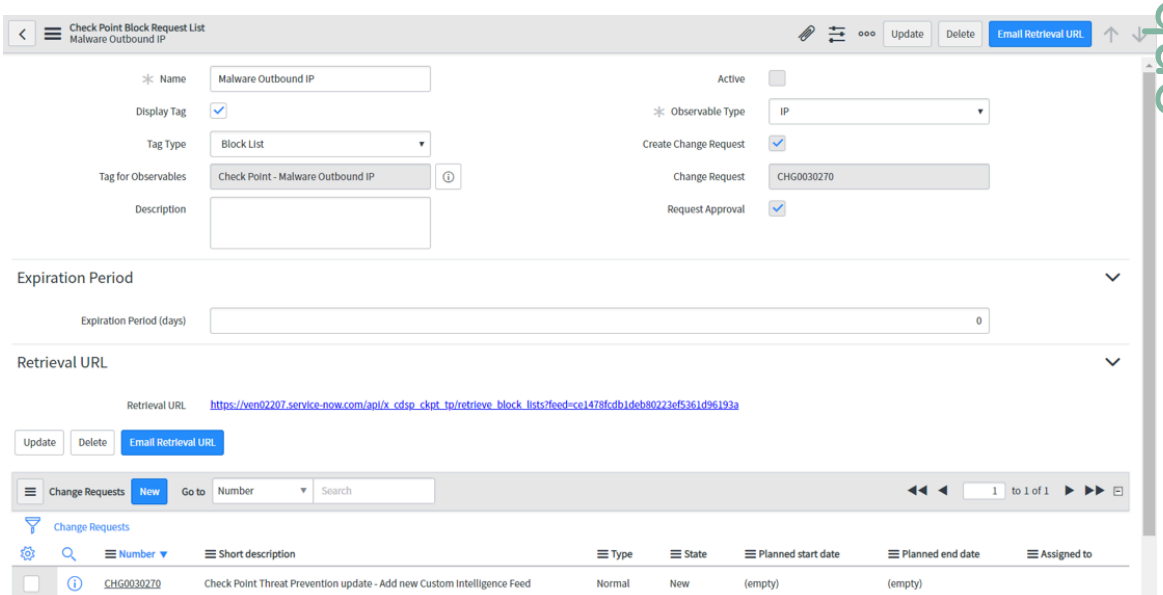
Rôle requis : Administrateur d'incidents de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Une fois la liste de blocs configurée, en tant qu'administrateur des incidents de sécurité, vous pouvez l'activer manuellement ou la liste de blocs est activée automatiquement à l'issue d'une ServiceNow AI Platform demande de changement. La demande de changement doit être approuvée et passer de l'état inactif à l'état actif avant de pouvoir accepter des entrées sur la liste de blocs.

Procédure

1. Accédez à la **Tous** > **Intégration Check Point NGTP** > **Listes de demandes de blocs**et sélectionnez le module **Listes de demandes de blocs** .
2. Dans la liste **des listes de demandes de blocs Check Point** qui s'affiche, sélectionnez votre nouvelle liste de blocs dans la colonne **Nom** .
3. Sur l'enregistrement qui s'affiche, notez le bouton **URL de récupération d'e-mail** , le lien URL de récupération de la liste de blocs actif et, le cas échéant, la demande de ServiceNow AI Platform changement dans la section Demandes de changement.
   Notez également que la case Actif est décochée.

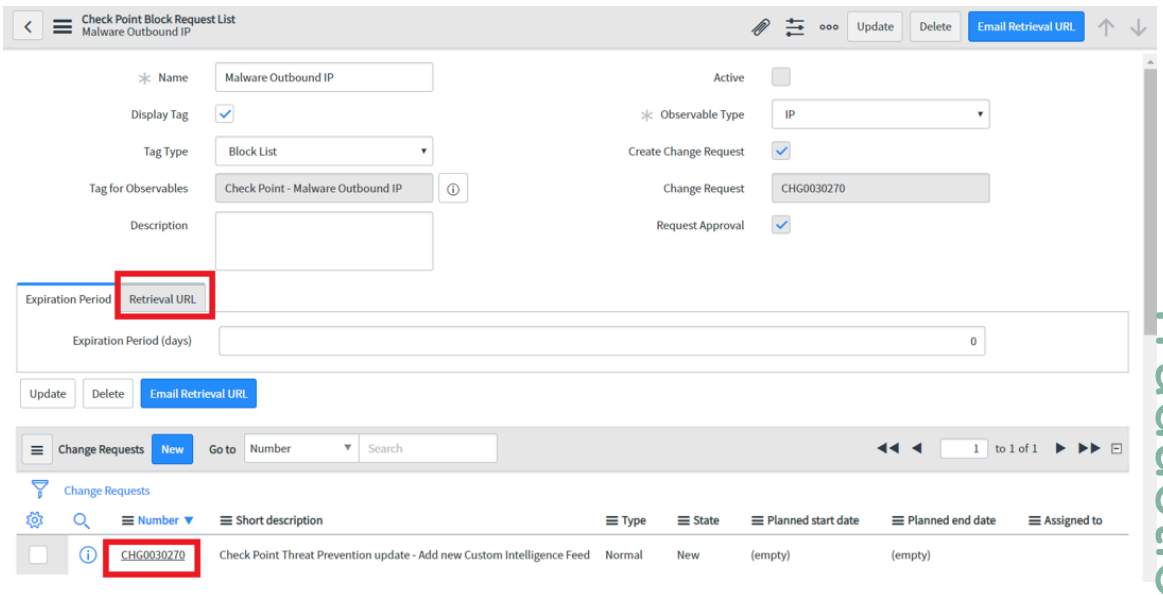


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Une fois les formulaires à onglets effacés dans vos paramètres système, l'URL de récupération de la liste de blocs apparaît dans la section URL de récupération.

4. Cliquez sur l'onglet URL de récupération de la **liste de blocs** pour afficher l'URL de récupération. La figure suivante montre l'URL de récupération de la liste de blocs affichée sous forme d'onglet avec des formulaires à onglets sélectionnés dans vos paramètres système. Le lien vers la demande de changement (CH0030270) est également affiché.



5. Pour terminer la configuration et faire passer la liste de blocs d'inactive à active, vous devez choisir l'une des options suivantes pour informer l'administrateur du pare-feu que l'URL de récupération est disponible.

Option	Description
Cliquez sur URL de récupération d'e-mail.	Envoyez par e-mail l'URL de récupération de la liste de blocage directement à l'administrateur du pare-feu. Cette option permet à l'administrateur de pare-feu de terminer la configuration sur la plateforme Check Point. Choisissez cette option si l'administrateur du pare-feu n'utilise pas le ServiceNow AI Platform.
Complétez la ServiceNow AI Platform demande de changement et affectez les tâches de configuration à l'administrateur du pare-feu.	Cette option n'est disponible que si l'administrateur de pare-feu de Check Point utilise également Now Platform et que les processus de gestion des changements et d'approbation ServiceNow AI Platform sont configurés. **Remarque :** Les utilisateurs disposant du rôle d'administrateur d'incident de sécurité (sn_si.admin) peuvent approuver la demande de ServiceNow AI Platform changement. Une fois les tâches de configuration terminées et la demande de changement fermée, la liste de blocs est activée automatiquement.

Que faire ensuite

Après avoir informé l'administrateur du pare-feu que l'URL de récupération est disponible et confirmé que la liste de blocs a été configurée dans Check Point, en tant qu'administrateur des incidents de sécurité, l'étape suivante consiste à activer la liste de blocage. Vous pouvez activer la liste de blocs manuellement ou, si elle est configurée, utiliser le ServiceNow AI Platform formulaire de demande de changement pour activer la liste

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de blocs. La liste de blocs est automatiquement activée lorsque la demande de changement est fermée.

Configurer une liste de blocs en tant que flux de renseignements personnalisé sur l'intégration Check Point NGTP

L'administrateur du pare-feu doit configurer le flux de renseignements personnalisé correspondant à la liste de blocs créée dans la Now Platform.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Cette tâche doit être effectuée sur chacune des passerelles NGTP Check Point. L'administrateur du pare-feu aurait besoin de l'accès SSH des serveurs de passerelle. Si votre organisation dispose ServiceNow AI Platform de processus d'approbation et de gestion des changements, vérifiez que l'aptitude d'envoi/réception d'e-mail est activée.

L'administrateur du pare-feu doit disposer de l'URL de récupération de la liste de blocs et des informations d'identification de l'utilisateur ServiceNow avec le rôle Check Point API Account Access Role (sn_sec_checkpoint.api_account_access).

Si l'administrateur de pare-feu n'utilise pas la plateforme NOW, l'administrateur d'incident de sécurité NOW peut fournir les informations requises par e-mail. Si l'administrateur de pare-feu utilise la Now Platform, la demande de changement associée à la liste de blocs peut également être affectée à l'administrateur du pare-feu. Cette demande de changement contient les informations requises pour configurer le flux de renseignements personnalisé.

Pour plus d'informations sur la configuration du flux de renseignements personnalisé sur les passerelles Check Point, consultez : https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Procédure

1. Vérifiez que l'option d'envoi/réception d'e-mail est activée dans votre ServiceNow AI Platform instance en accédant à **Propriétés d'e-mail** > **Administration** > **Propriétés d'e-mail**.
2. Sous Configuration des e-mails sortants, vérifiez que les options Envoi et **Réception d'e-mail** sont sélectionnées.
3. Modifiez SSH vers Check Point Gateway avec le mode expert.
4. Exécutez la commande pour ajouter un flux de renseignements personnalisé.
   L'exécution de la commande est interactive et demande le format du flux et le mot de passe.
   - Lorsque vous êtes invité à entrer le format du flux, saisissez « cp_csv »
   - Lorsqu'il est invité à entrer le mot de passe de l'utilisateur de la Now Platform avec l'accès API.

   L'exécution de la commande avertissait que le certificat du serveur (NOW platform) n'était pas approuvé par la machine et demandait d'ajouter le certificat de sécurité du serveur au magasin approuvé de la machine. Entrez **Y**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le message « État :Réussite » s'affiche, confirmant que le flux est ajouté avec succès.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Soumettre des entrées de liste de blocs à partir d'un incident de sécurité pour l'intégration Check Point NGTP

Les observables joints à un enregistrement d'incident de sécurité sont soumis pour approbation en tant qu'entrées de liste de blocs sur différentes listes de blocs. Un processus d'approbation facultatif pour les entrées de la liste de blocs fait partie du workflow préconfiguré. La passerelle importe les entrées de la liste de blocs (adresses IP, URL, domaines) qui sont incluses dans les listes de blocs.

Avant de commencer

Rôle requis :

- Analyste des incidents de sécurité (sn_si.analyst) pour soumettre les entrées de la liste de blocs.
- L'administrateur d'incident de sécurité (sn_si.admin) pour approuver les entrées de la liste de blocs. Cette autorisation peut être affectée en fonction des besoins de votre organisation.

Pourquoi et quand exécuter cette tâche

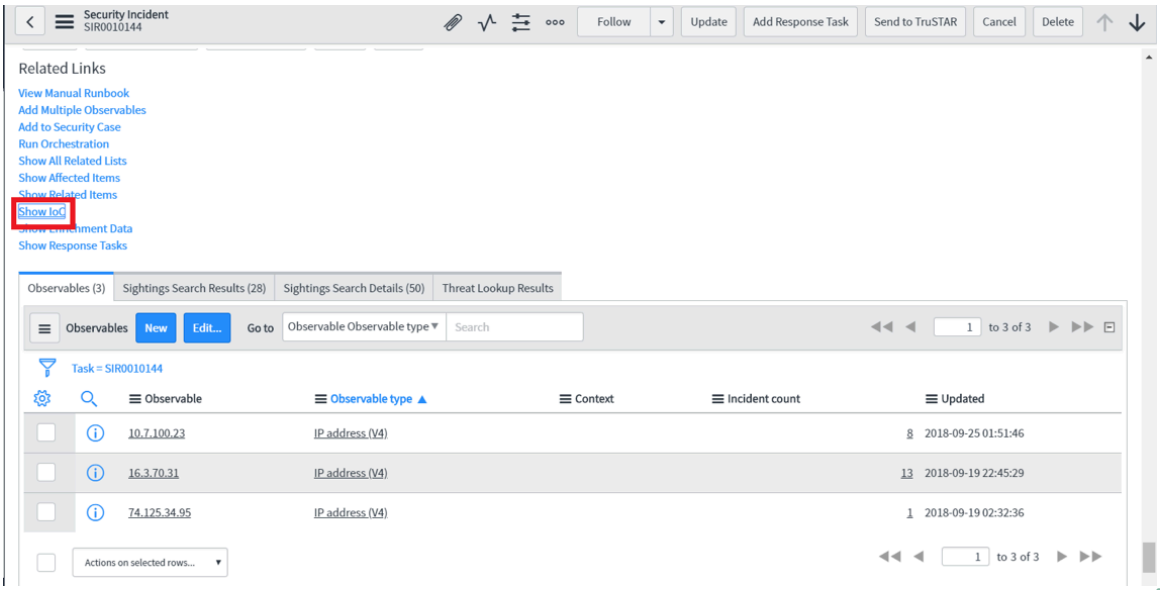
Les utilisateurs disposant du rôle sn_si.analyst soumettent des entrées de bloc en demandant un blocage sur les observables joints à un enregistrement d'incident de sécurité. Une fois soumise, une entrée de liste de blocs avec l'état En attente est générée et envoyée pour approbation. L'exemple suivant montre une demande de bloc pour un observable d'URL.

Procédure

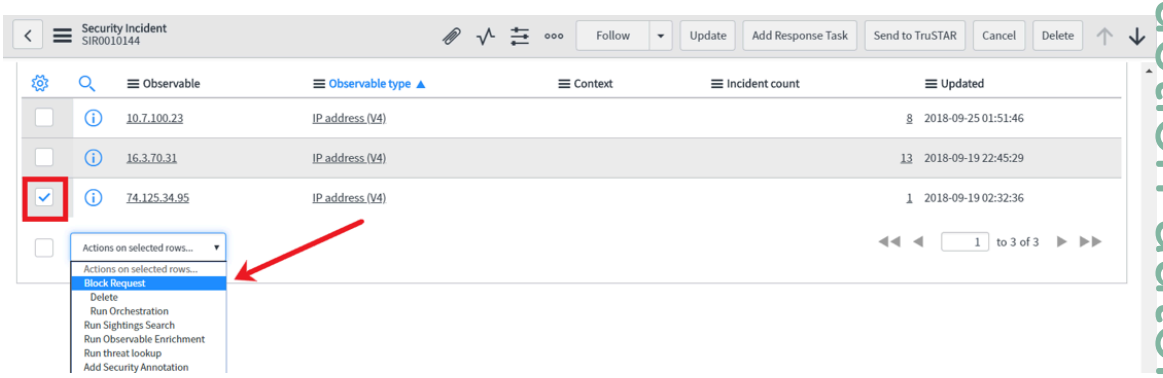
1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**et cliquez sur un enregistrement d'incident de sécurité pour l'ouvrir.
2. Cliquez sur le lien connexe **Afficher l'IoC** .

Traduction automatique

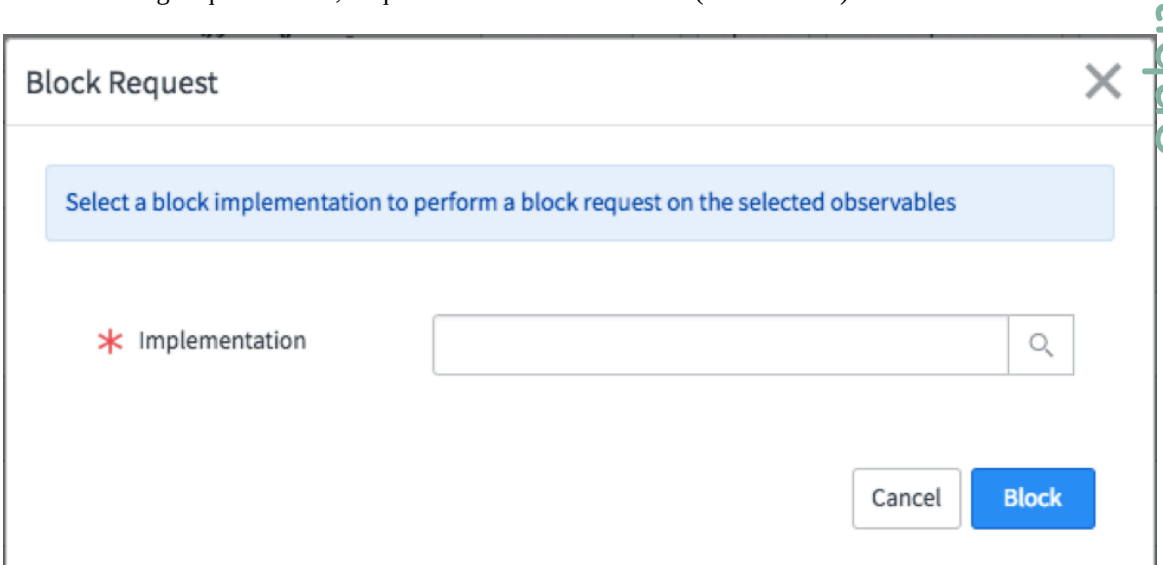
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans la liste connexe Observables, sélectionnez les observables que vous voulez bloquer et, dans la liste **Actions sur les lignes sélectionnées** , sélectionnez **Demande de bloc**.



4. Dans la boîte de dialogue qui s'affiche, cliquez sur l'icône de recherche (icône de)

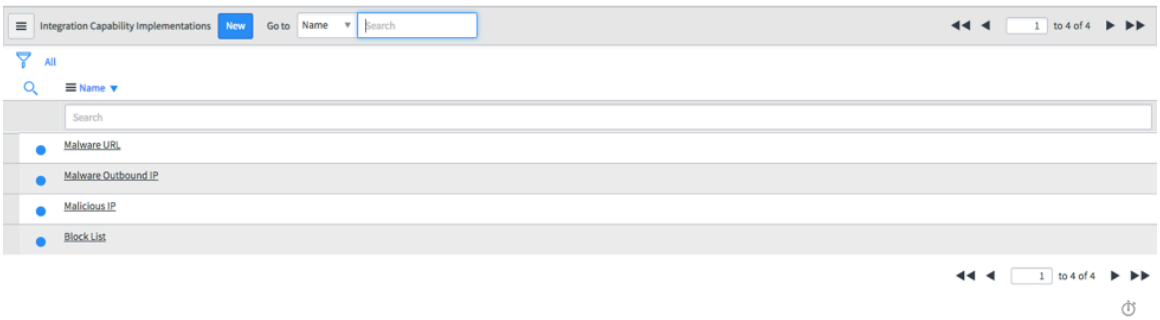


5. Dans la liste, sélectionnez la liste de blocs à laquelle vous souhaitez joindre cette entrée.

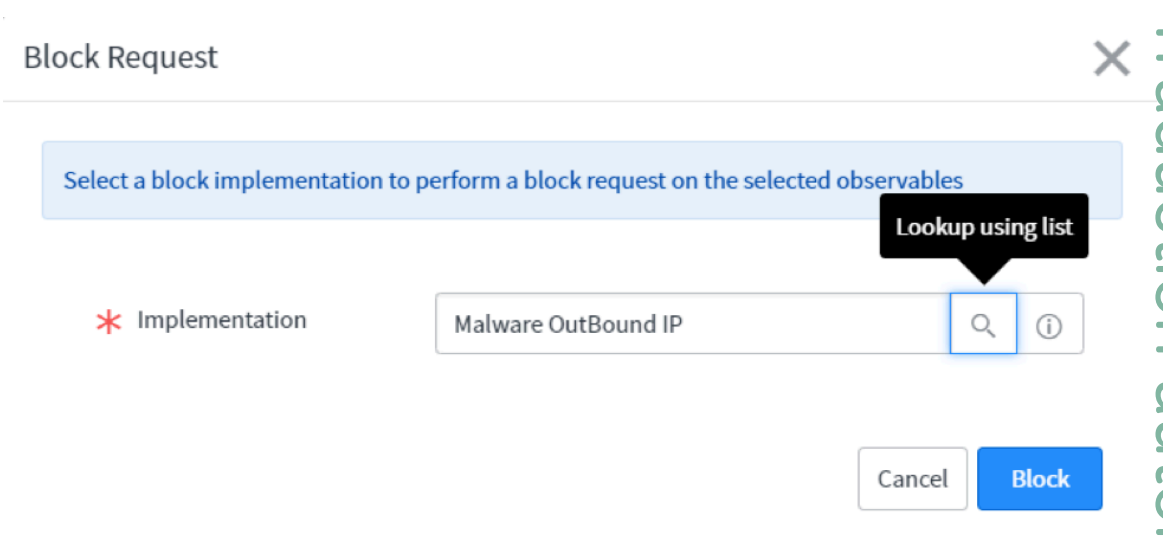
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Pour cet exemple, le type d'observable (IP) d'entrée doit correspondre au type d'observable (IP) de la liste de blocs.

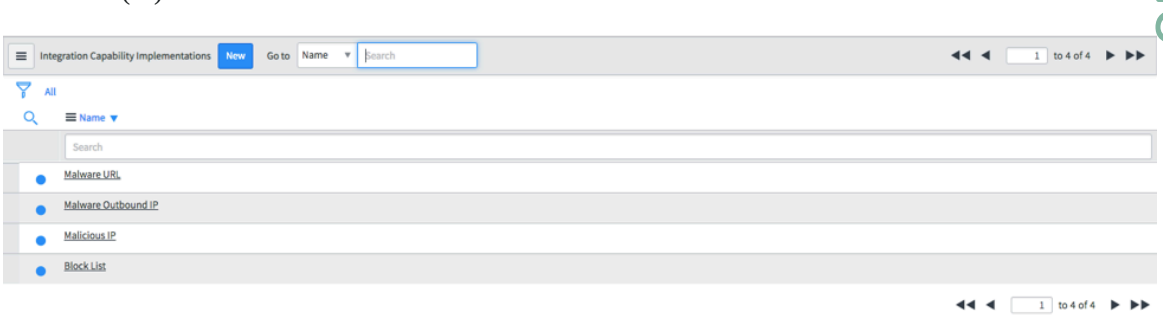


6. Dans la boîte de dialogue Demande de bloc avec le nom de la liste de blocs affiché dans le champ **Implémentation**, cliquez sur Bloquer.



7. Dans la liste qui s'affiche, sélectionnez la liste de blocs à laquelle vous souhaitez joindre cette entrée.

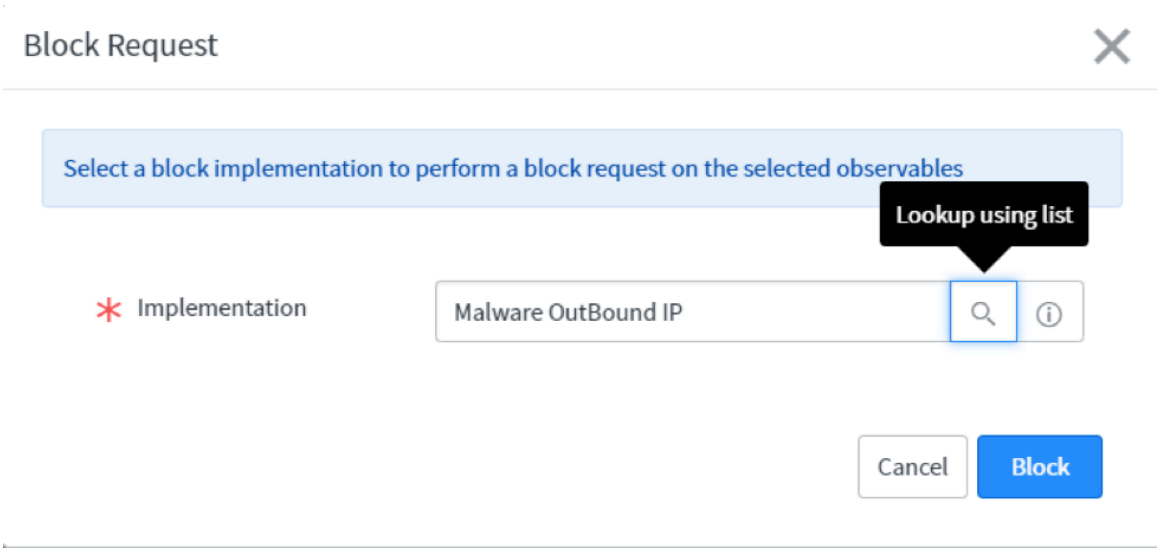
Remarque : Pour cet exemple, le type d'observable (IP) d'entrée doit correspondre au type d'observable (IP) de la liste de blocs.



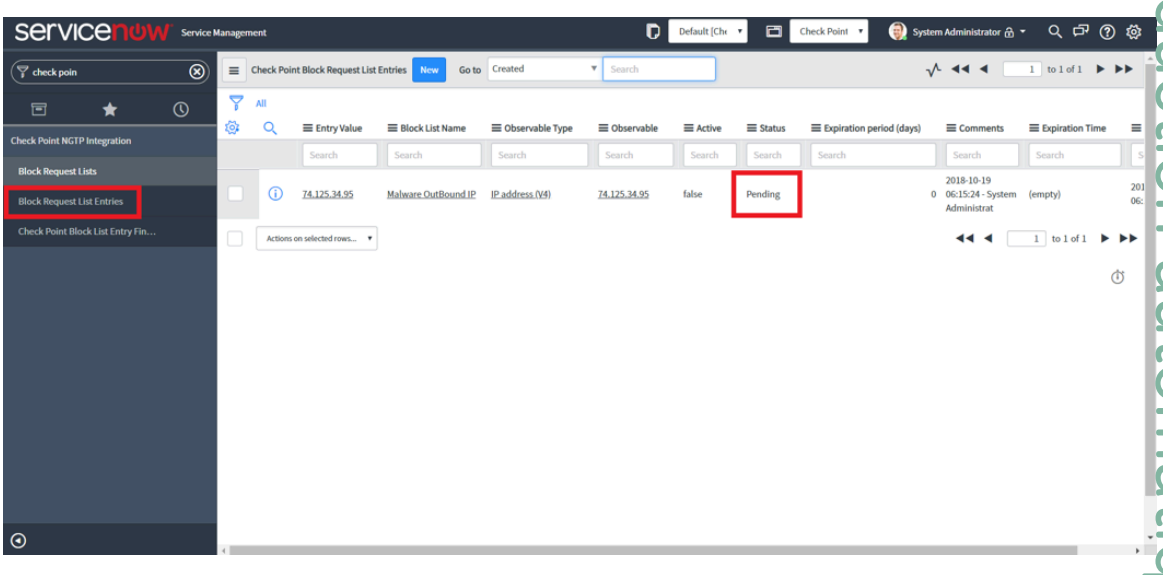
8. Dans la boîte de dialogue Demande de bloc avec le nom de la liste de blocs affiché dans le champ **Implémentation** , cliquez sur **Bloquer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



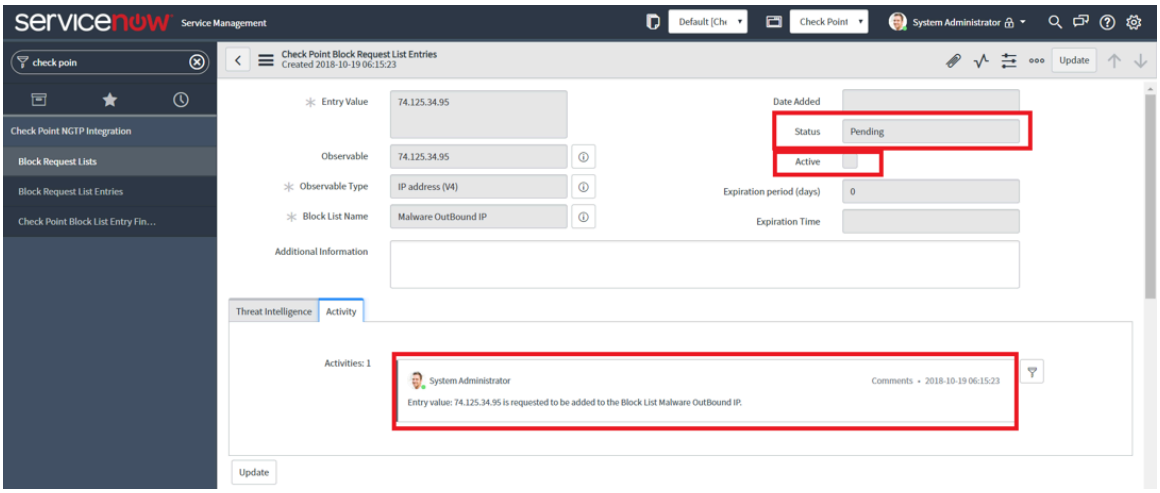
9. Accédez à la **Intégration Check Point NGTP** > **Entrées de la liste de demandes de blocs**et cliquez sur **Entrées de la liste de demandes de blocs**.



10. Dans la liste Entrées de la liste de demandes de blocs Check Point, cliquez sur votre observable dans la colonne **Valeur d'entrée** pour ouvrir l'enregistrement.
Pour cet exemple, l'enregistrement **de 74.125.34.95** s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'état est En attente, la case Actif est décochée et les notes de travail indiquent qu'il existe une demande d'ajout de l'observable. Cette demande d'entrée de la liste de blocs est prête à être approuvée.

L'icône en regard du champ Observable est un lien vers la ServiceNow AI Platform table Observable.

La valeur du champ Observable (74.125.34.95) est liée à la table Observable et elle correspond au format qui a été transféré de l'événement déclenchant l'incident de Réponse aux incidents de sécurité.

Soumettre des entrées de liste de blocs directement à partir de la table d'entrée de la liste de blocs

Pour les observables déterminés comme malveillants et non associés à un incident de sécurité Now Platform spécifique, vous soumettez des entrées de liste de blocs à partir de la liste de blocs.

Avant de commencer

Rôle requis : Administrateur d'incidents de sécurité (sn_si.analyst)

Pourquoi et quand exécuter cette tâche

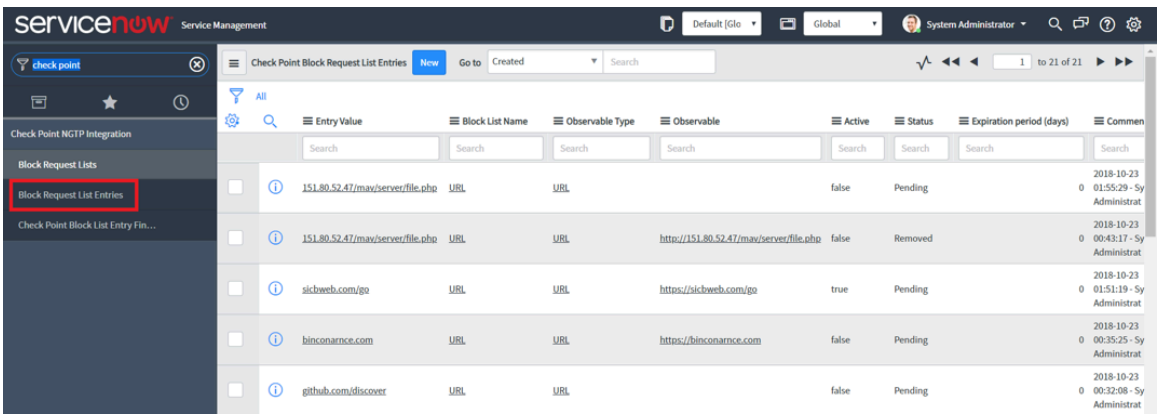
Lorsque vous souhaitez bloquer un observable que vous avez déterminé comme malveillant ou autoriser un observable que vous avez déterminé comme non malveillant et que l'observable n'est pas associé à un enregistrement d'incident de sécurité spécifique ServiceNow AI Platform , vous soumettez des entrées de liste de blocs directement à partir de la liste de blocs. Des exemples de ces types d'entrées de liste de blocage peuvent être des URL ou des domaines pour des sites spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

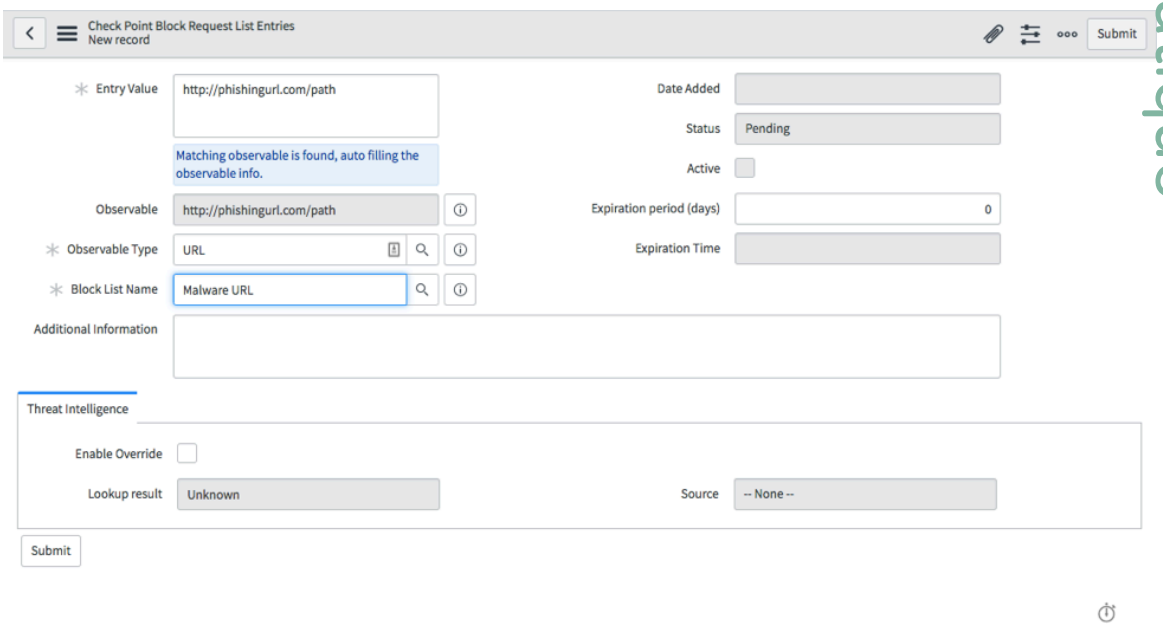
Procédure

1. Accédez à la **Tous** > **Intégration Check Point NGTP** > **Entrées de demandes de blocs**.



2. Cliquez sur le module **Listes de demandes de blocs** .
3. Dans la liste Entrées de la liste de demandes de blocs Check Point, cliquez sur **Nouveau**.
4. Dans le champ **Valeur d'entrée** , saisissez une valeur pour votre observable.
   Les deux résultats possibles de cette entrée :
   - Les autres champs du formulaire sont renseignés automatiquement.
   - Un observable correspondant est trouvé et un message s'affiche indiquant qu'un observable correspondant existe. Sélectionnez la liste de blocs à laquelle vous souhaitez joindre cette entrée, puis cliquez sur Soumettre. Sélectionnez la liste de blocs à laquelle vous souhaitez attacher cette entrée avant de définir la période d'expiration.

   Un message vous demandant de remplir le formulaire s'affiche. Aucun observable correspondant n'a été trouvé et vous devez remplir le formulaire. Une fois que vous l'avez terminée, sélectionnez la liste de blocs à laquelle vous souhaitez joindre l'observable, puis cliquez sur Soumettre. Un enregistrement d'observable est créé. La figure suivante montre un exemple d'observable de domaine existant et comment les champs sont complétés automatiquement.

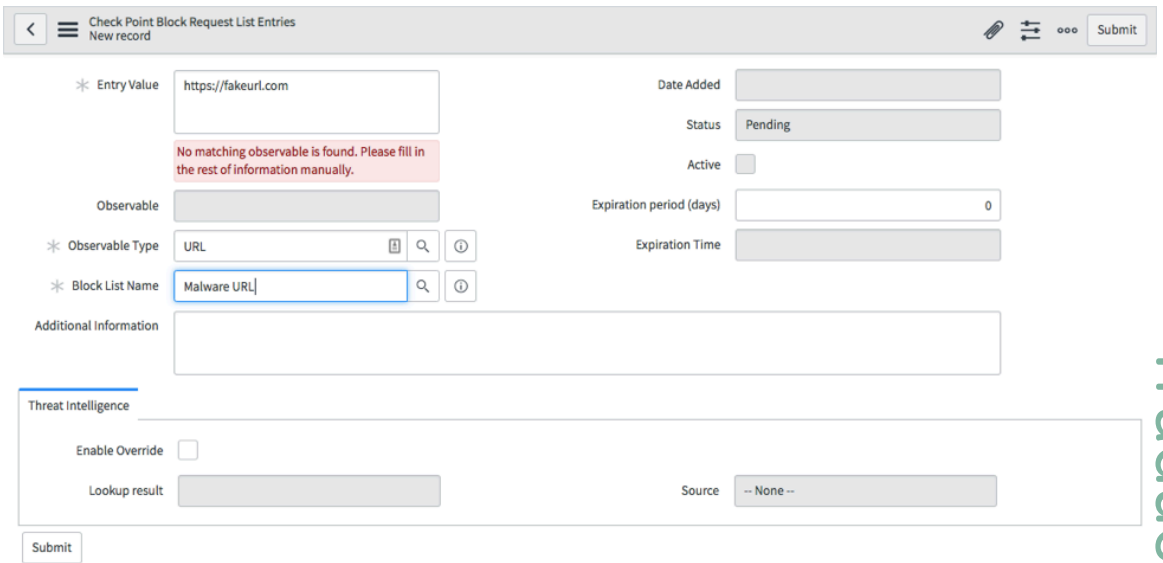


5. Cliquez sur l'icône de recherche pour sélectionner la liste de blocs à laquelle vous souhaitez joindre l'entrée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Envoyer**.
7. Si l'approbation par e-mail est configurée dans votre workflow, une demande d'approbation par e-mail est envoyée.
   Si un message s'affiche vous demandant de renseigner manuellement le reste des informations, renseignez les champs.



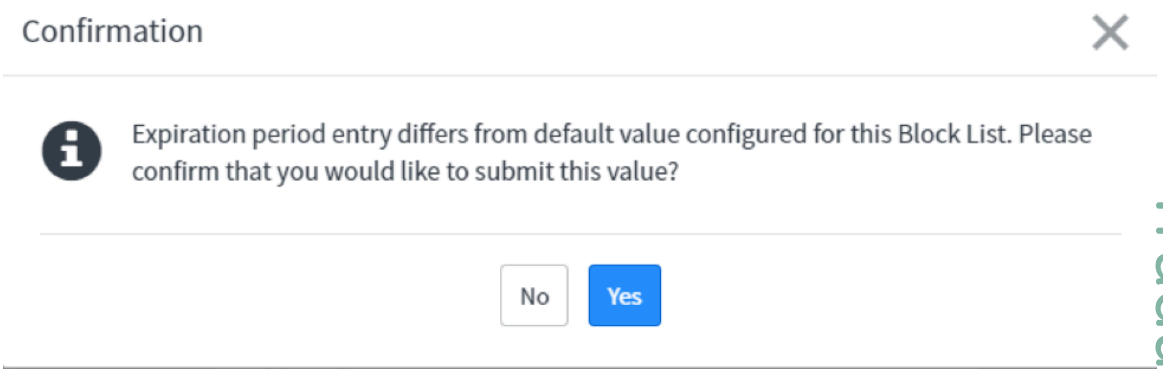
Champ	Description
Type d'observable	Type d'observable pris en charge à partir de la boîte de dialogue.
Nom de la liste de blocs	Liste de blocs à laquelle vous souhaitez ajouter l'entrée. **Remarque :** Sélectionnez la liste de blocs à laquelle vous souhaitez attacher l'entrée avant de définir la période d'expiration.
Activer le remplacement (sélectionné par défaut)	Rechercher le résultat ou la source. Une fois configurée, elle vous permet d'entrer un résultat de recherche et la source utilisée pour trouver les résultats. Ces champs sont généralement renseignés lors de la création d'un enregistrement d'incident de sécurité. Dans ce cas, il n'y a pas de résultat ou de source de recherche, et vous renseignez ces champs manuellement.
Résultat de la recherche	Sélectionnez **Inconnu** ou **Malicieux**.
Source	Source qui effectue une recherche de menaces sur l'entrée de la liste de blocs, par exemple, ThreatCrowd...
Période d'expiration	La période d'expiration héritée par défaut de la liste de blocs. Vous pouvez remplacer cette valeur, mais uniquement lors de la création de l'entrée. 0 indique que l'entrée de la liste de blocs n'expire jamais. Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous saisissez. Vous pouvez entrer une valeur minimale de 1, mais il n'y a pas de valeur maximale.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

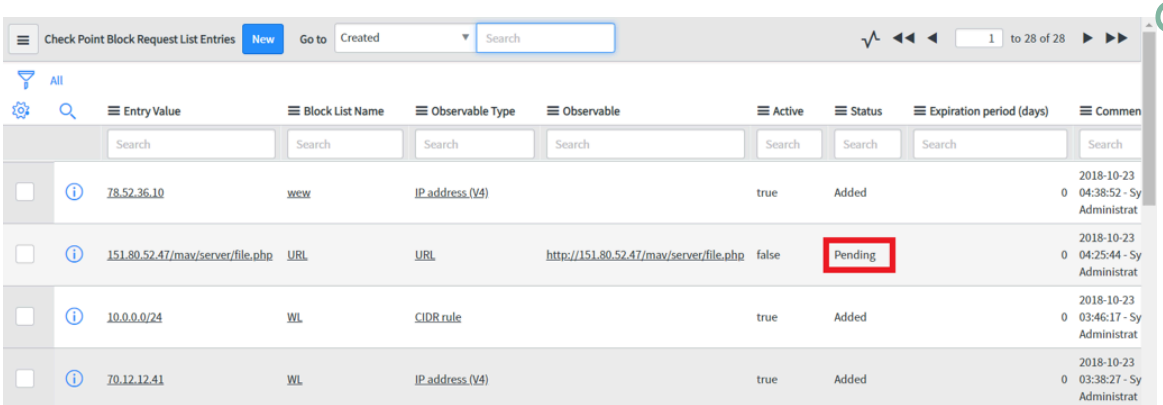
Champ	Description
	Par exemple, si vous entrez 30 jours à 14h01 le 1er mai, l'entrée de la liste de blocage expirera à 14h01 le 31 mai. Cependant, le planificateur vérifie les entrées expirées à 00h00 tous les jours et modifie l'état de l'entrée en « expiré » à 00h00 le 1er juin.

8. Cliquez sur **Envoyer**.
   Si vous avez modifié la période d'expiration par défaut de l'entrée de la liste de blocs, une boîte de dialogue de confirmation d'avertissement s'affiche indiquant que la période diffère de la liste de blocs sélectionnée.



Option	Description
Oui	Confirme votre remplacement d'expiration, sauvegarde l'enregistrement et vous renvoie aux entrées de la liste de blocs Check Point. Si l'approbation par e-mail est configurée dans votre workflow, une demande d'approbation par e-mail est envoyée.
Non	Annule le remplacement. À ce stade, vous pouvez modifier la valeur de la **période d'expiration**. Après avoir modifié la valeur, cliquez sur Soumettre pour revenir à la liste Entrées de bloc Check Point.

9. Si ce n'est pas le cas, accédez aux **entrées de la liste de demandes de blocs Check Point** et notez que l'état de l'entrée est **En attente**.



L'entrée est maintenant prête à être approuvée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Approuver les entrées de la liste de blocs pour l'intégration Check Point NGTP

Un processus d'approbation des entrées de la liste de blocs fait partie du workflow préconfiguré. Vous approuvez les entrées de la liste de blocs avant que les entrées ne soient activées sur les listes de blocs. Une fois que vous avez approuvé l'entrée de la liste de blocs, la passerelle récupère l'entrée et votre observable est bloqué à partir de ce moment-là.

Avant de commencer

- L'approbation des entrées de la liste de blocs est affectée par défaut à l'administrateur d'incident de sécurité (sn_si.admin), mais cette autorisation peut être attribuée à la demande de votre organisation. Dans l'exemple suivant, l'administrateur dispose d'un ServiceNow AI Platform pouvoir d'approbation.

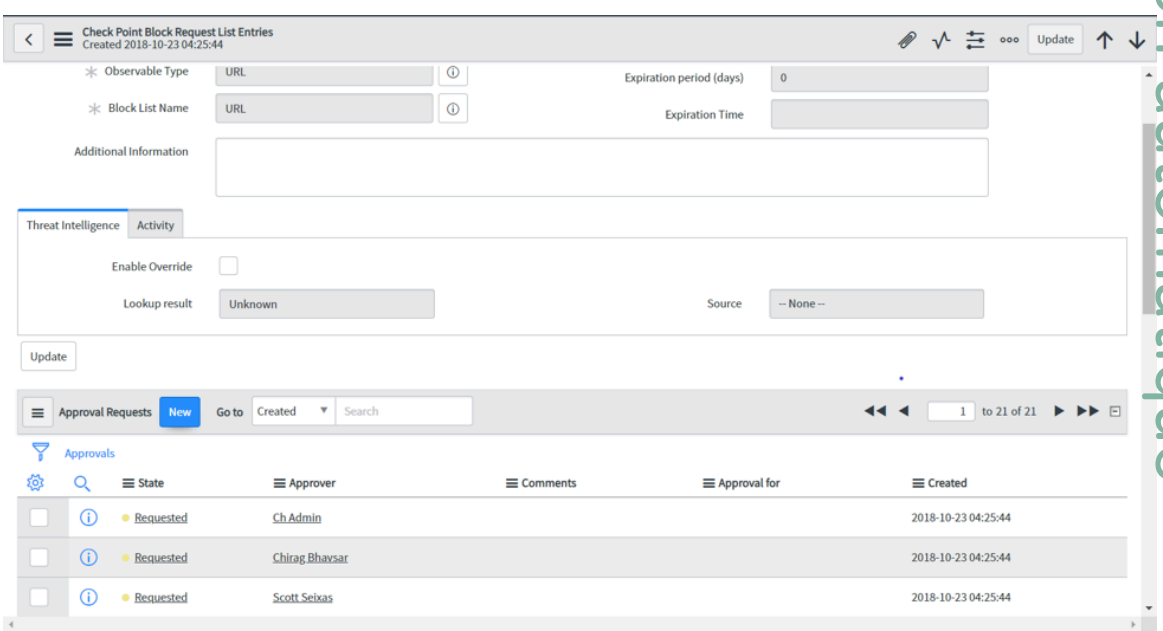
Rôle requis : sn.si.admin

Pourquoi et quand exécuter cette tâche

Lorsque le processus d'approbation est activé, une entrée de la liste de blocs n'est pas activée ou désactivée sur la liste de blocs tant qu'elle n'est pas approuvée.

Procédure

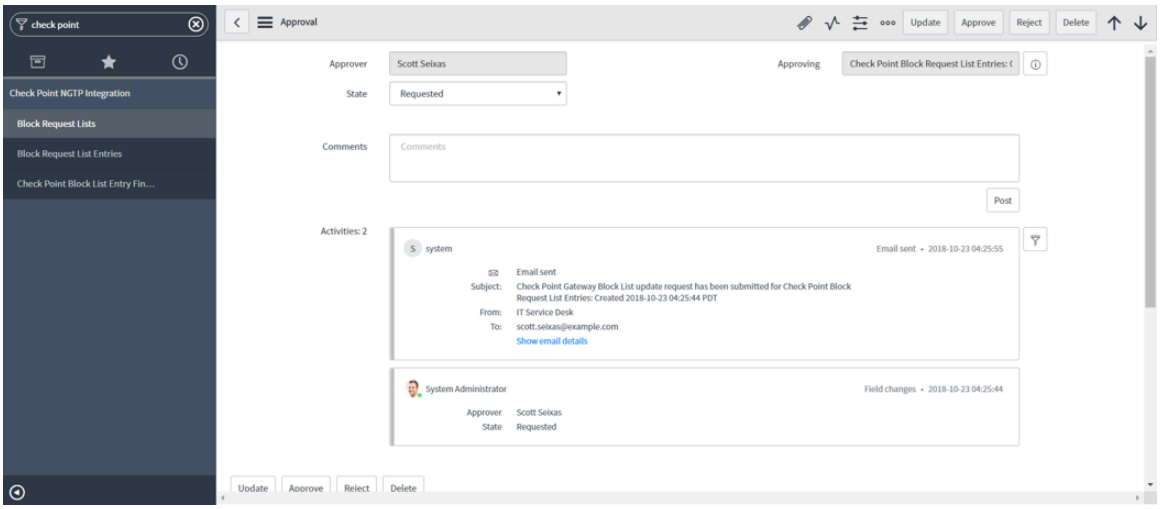
1. Accédez à la **Tous** > **Intégration Check Point NGTP** > **Entrées de la liste de demandes de blocs**et ouvrez l'enregistrement Entrée de la liste de blocs.
2. Dans l'enregistrement Entrée de la liste de blocs, accédez à la section **Demandes d'approbation** .



3. Dans Demandes d'approbation, cliquez sur un élément dans la colonne **État** pour l'ouvrir.
   L'enregistrement de l'approbation s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



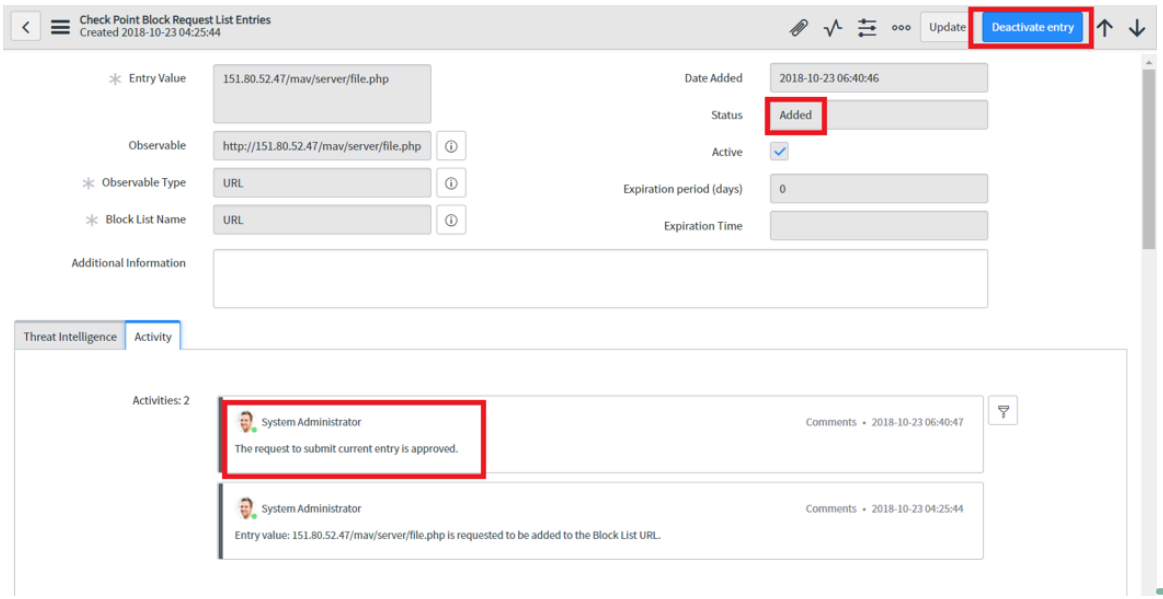
4. Choisissez une option pour approuver l'entrée de la liste de blocs.

Option	Description
Approuver	Sur l'enregistrement d'entrée, le champ État bascule sur Ajouté et la case Actif est cochée. Le bouton Désactiver est affiché et actif. Les notes de travail montrent que la demande d'entrée de la liste de blocs a été approuvée.
Refuser	Sur l'enregistrement de l'entrée, le champ État bascule sur Rejeté et la case Actif est décochée, indiquant que l'entrée n'est pas bloquée sur la passerelle. Les notes de travail montrent que la demande d'entrée de la liste de blocs a été rejetée.

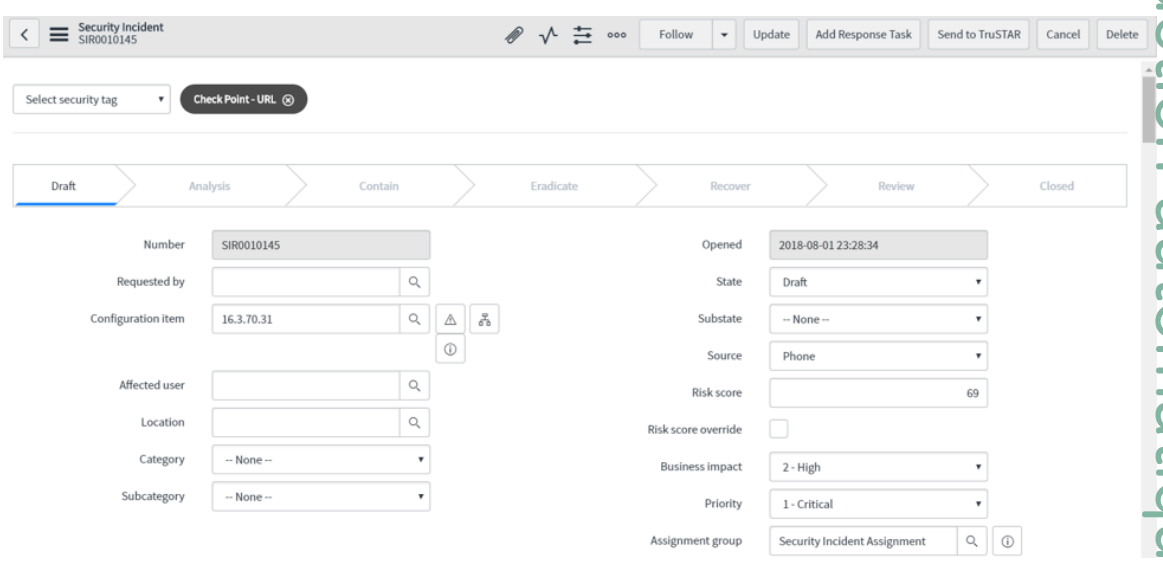
Une fois que vous avez approuvé l'entrée de la liste de blocs et qu'elle est activée, le pare-feu de nouvelle génération Check Point récupère l'entrée de la liste de blocs après l'intervalle de récupération suivant. Une fois l'entrée récupérée, l'observable est bloqué à partir de ce moment-là. Dans la figure suivante, notez que la case Actif est cochée, que l'état est Ajouté et que les notes de travail indiquent que la demande a été approuvée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



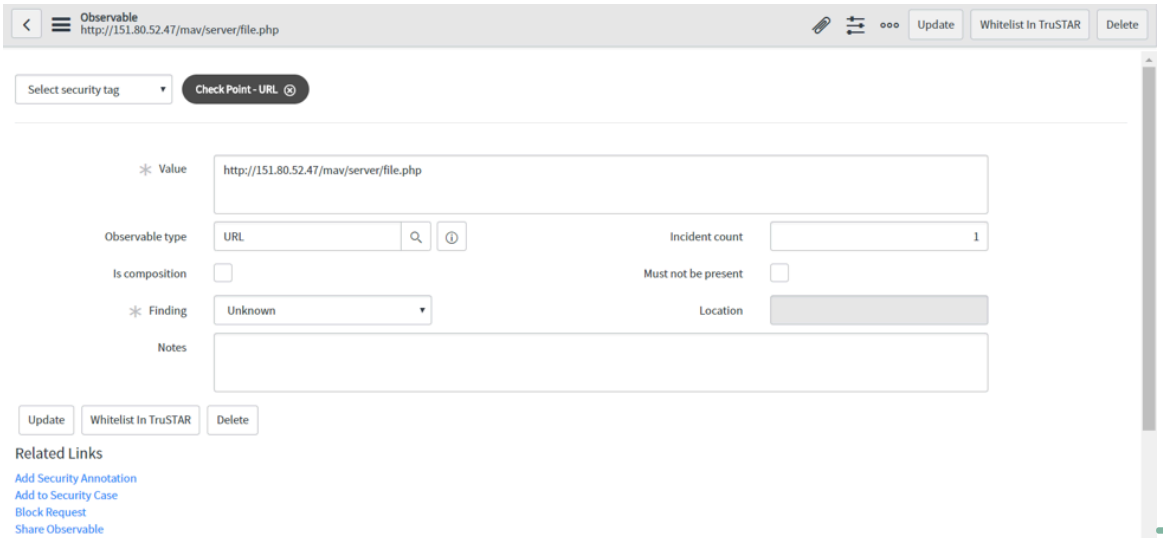
Une fois l'entrée de la liste de blocs approuvée et activée, l'enregistrement de l'incident de sécurité est marqué d'une balise de sécurité. La balise s'affiche en haut de l'enregistrement.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La balise de sécurité s'affiche également sur l'enregistrement de l'observable.



Exceptions d'entrée de liste de blocs pour l'intégration Check Point NGTP

Il existe des restrictions pour l'ajout d'entrées de liste de blocs aux listes de blocs. En cas de doublon, de compatibilité ou de conflits CIDR (Classless Inter-Domain Routing) lorsque vous essayez d'ajouter des entrées de liste de blocs à des listes de blocs, des messages d'erreur s'affichent pour vous aider à résoudre ces erreurs.

Exception de compatibilité

Chaque liste de blocs accepte uniquement les entrées compatibles avec son type d'observable. Si vous créez une liste de blocs de domaine et que vous essayez d'y joindre une adresse IP observable, un message d'erreur incompatible s'affiche. Par exemple, une liste de blocs de domaine ne peut accepter que des observables de domaine, comme illustré dans la figure suivante.

Formulaire de liste de blocs avec erreurs de compatibilité

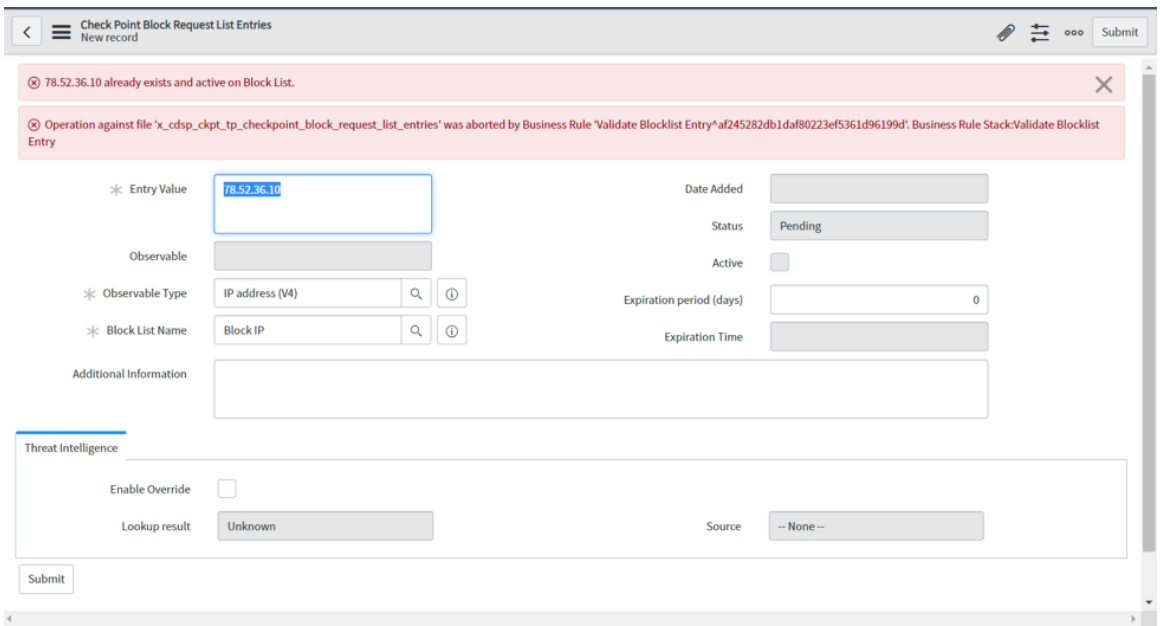


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

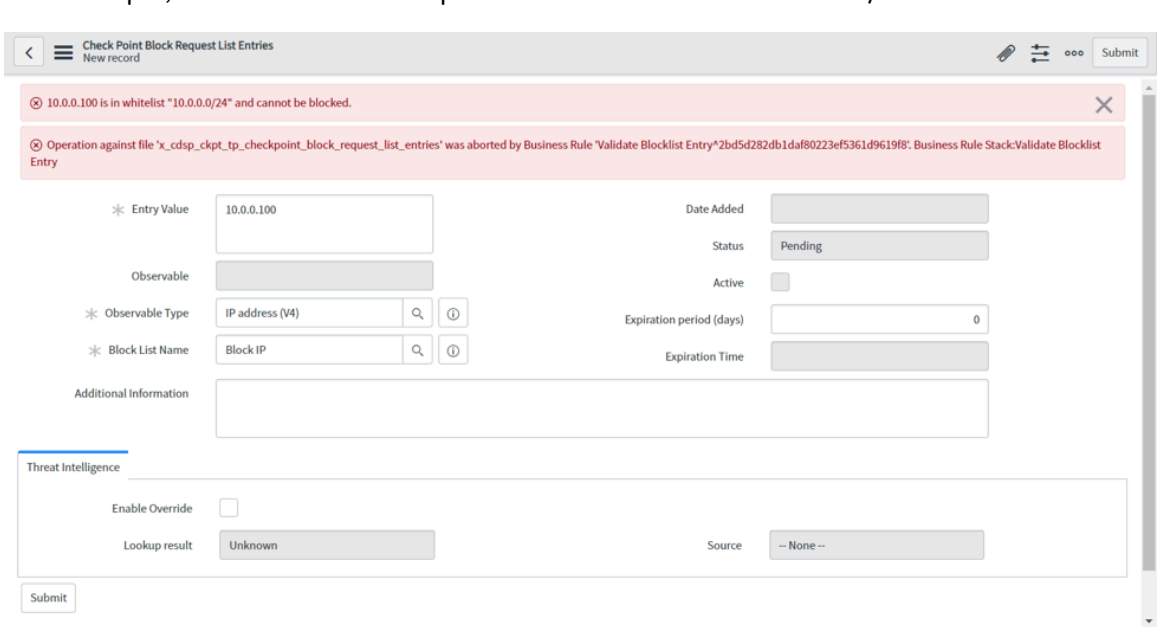
Exception de duplication

Un observable ne peut pas être activé sur plusieurs listes de blocs du même type d'observable. Si un observable d'URL est déjà activé sur une liste de blocage d'URL et que vous essayez d'activer le même observable sur une liste de blocage d'URL d'hameçonnage, un message d'erreur de duplication s'affiche.



Exception CIDR (Classless Inter-Domain Routing)

Si vous tentez de joindre une seule adresse IP à une liste d'autorisation et que cette adresse IP fait partie d'un observable CIDR déjà sur une liste de blocs/liste d'autorisation, une erreur de conflit CIDR s'affiche. Cette erreur indique que l'adresse IP unique est déjà incluse dans la liste de blocs ou la liste d'autorisation dans le cadre de l'observable CIDR. Par exemple, 192.168.24.25 fait partie du bloc CIDR 192.168.0.0/22.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modifier le nom de la balise de sécurité pour l'intégration Check Point NGTP

Si la case Afficher la balise est cochée lorsque vous créez l'enregistrement Liste de blocs, vous pouvez modifier les noms et les couleurs des balises de sécurité. Les balises de sécurité vous aident à suivre les observables qui sont déjà bloqués.

Avant de commencer

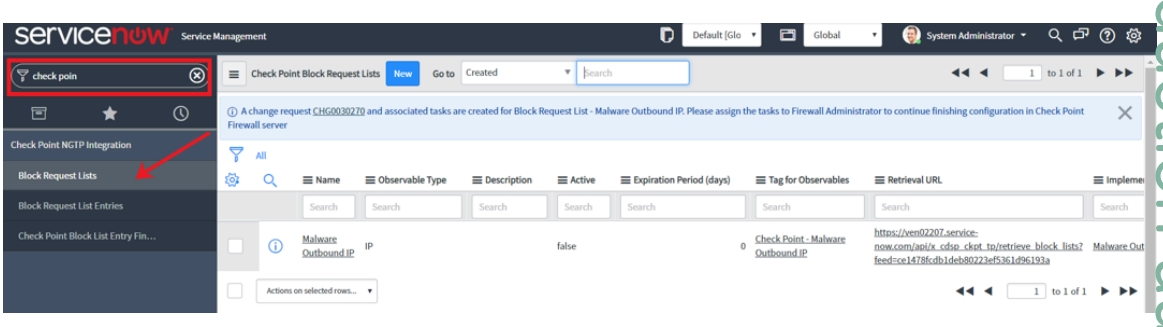
Rôle requis : sn.si.admin

Pourquoi et quand exécuter cette tâche

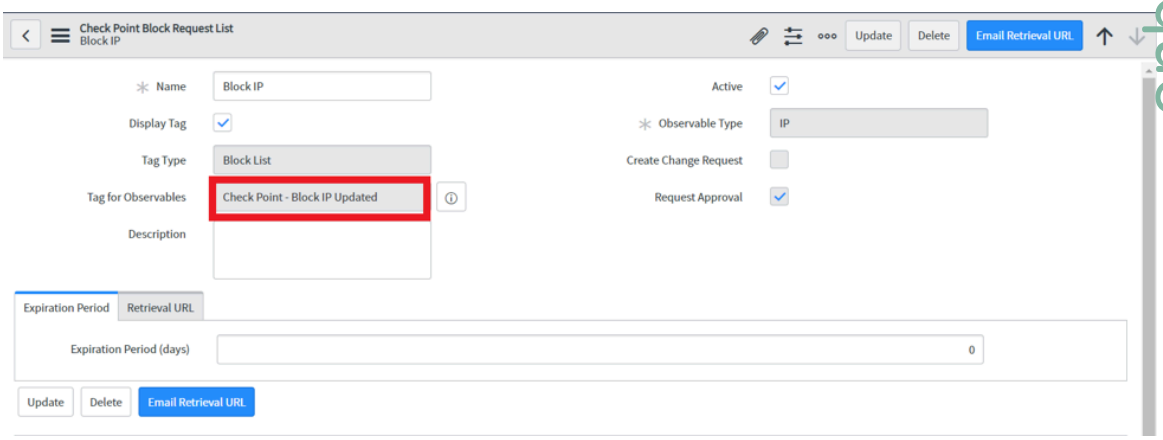
Les balises de sécurité vous aident à identifier rapidement quels incidents de sécurité ont des observables sur une liste bloquée. Les balises vous aident également à déterminer si un observable est déjà bloqué ou s'il a été supprimé d'une liste bloquée. Par défaut, la couleur de la balise de sécurité est le noir pour les entrées de la liste de blocs et le gris pour les entrées de la liste d'autorisation. Vous pouvez modifier les noms et les couleurs des balises pour vous aider à reconnaître plus facilement certaines balises.

Procédure

1. Accédez à la **Tous** > **Intégration Check Point NGTP** > **Configuration de la liste de demandes de blocs**.



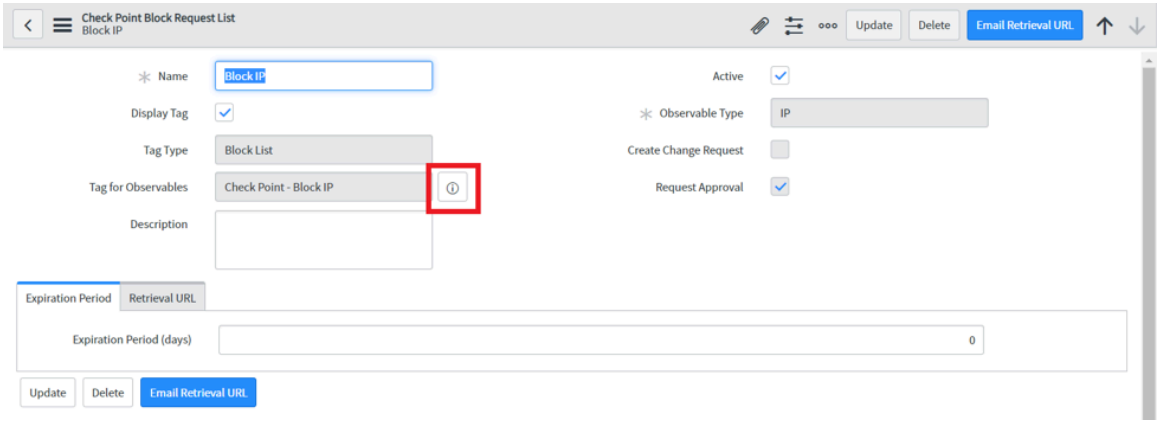
2. Cliquez sur un élément dans la colonne **Nom** pour l'ouvrir.
   L'enregistrement de la liste de blocs s'affiche. Par défaut, le nom de la balise de sécurité est la même que celle que vous avez saisie dans le champ Nom de la liste de blocage lors de sa création. Par défaut, le nom comprend également un préfixe de liste de blocage, par exemple, Liste de blocage – URL malveillantes de logiciels malveillants.



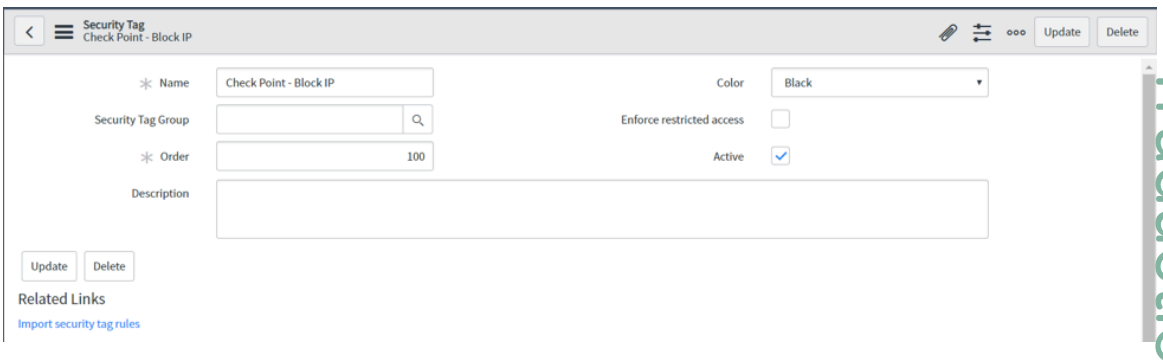
3. Cliquez sur l'icône d'informations à côté de la balise pour les observables, puis sur Ouvrir l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

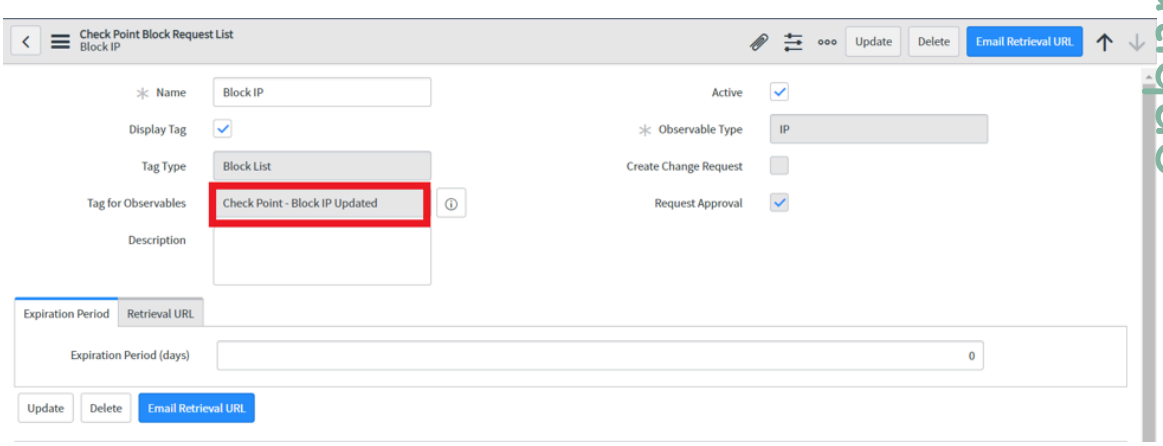


Le formulaire Balise de sécurité s'affiche.



4. Dans le champ **Nom** , modifiez le nom de la balise de sécurité.
5. Cliquez sur **Mettre à jour**.
   L'enregistrement de la liste de blocs mis à jour s'affiche avec le nom de balise modifié.

> **Remarque :** Dans l'exemple suivant, sortant a été ajouté au nom de la balise. Conservez le préfixe Check Point dans le nom de votre nouvelle balise pour vous aider à identifier la balise associée à l'intégration de pare-feu de nouvelle génération Check Point.

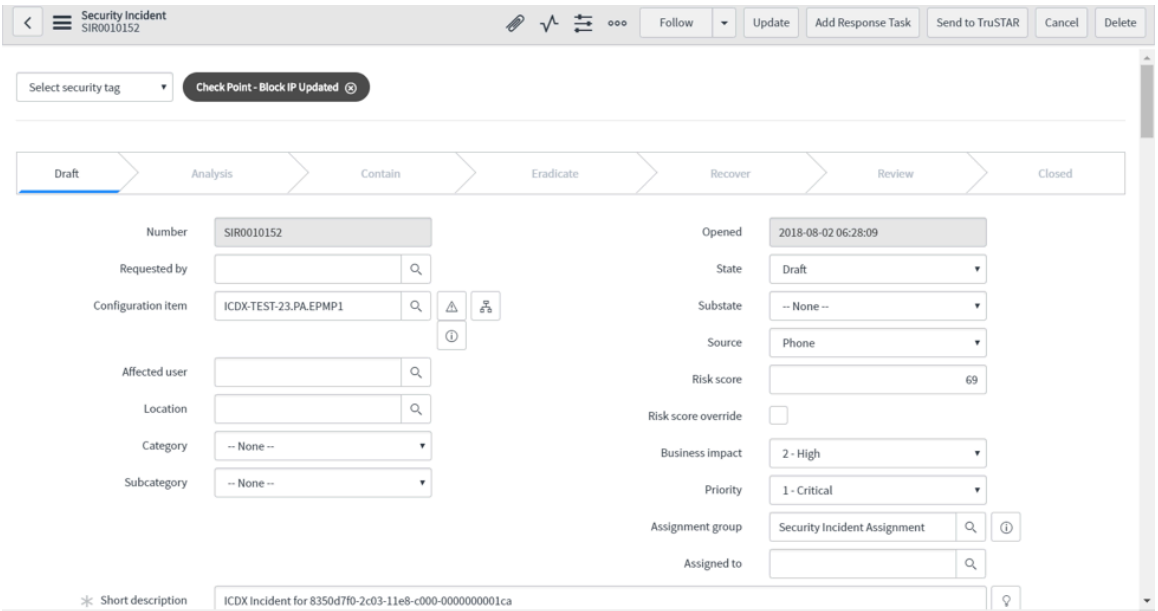


Les balises de sécurité sont affichées pour chaque type d'observable (IP, URL, domaine) sur l'enregistrement d'incident de sécurité et l'enregistrement d'observable chaque fois que cet observable est ajouté à la liste de blocage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats



Si un observable a déjà été ajouté à une liste bloquée et qu'une balise de sécurité est affichée sur un incident de sécurité pour cet observable, la balise de sécurité de la liste bloquée s'affiche également automatiquement sur tous les enregistrements d'incident de sécurité ultérieurs qui sont créés. Cette duplication vous indique que l'observable figure déjà sur une liste bloquée. Vous n'avez pas besoin d'ajouter cet observable et de le bloquer à nouveau.

Lorsqu'un observable n'est plus bloqué, aucune balise de sécurité ne s'affiche sur l'enregistrement d'incident de sécurité ou l'enregistrement d'observable. Dans ce cas, aucune balise de sécurité n'indique que la date d'expiration de l'observable est peut-être passée ou que l'observable a été désactivé d'une liste bloquée.

Désinstaller l'intégration Check Point NGTP

Si vous souhaitez désinstaller Check Point NGTP Integration de votre ServiceNow AI Platform instance et supprimer tous les restes de l'intégration, consultez le site de documentation ServiceNow pour obtenir des instructions sur la désinstallation des applications.

Rôle requis : admin

Intégration de l'hôte CrowdStrike Falcon

L'intégration CrowdStrike Falcon Host vous permet de transférer les observables d'un incident de sécurité dans une liste de surveillance, ce qui leur permet de générer des alertes supplémentaires. Cette intégration est une implémentation du workflow CrowdStrike Falcon Host - Publier dans la liste de surveillance.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

Mise en route de l'intégration CrowdStrike Falcon Host

Utiliser

Effectuer des recherches sur les observables

Développer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l’écriture d’intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l’intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Opérations de sécurité CrowdStrike Falcon Host : flux de publication dans la liste de surveillance

Le concepteur de flux **CrowdStrike Falcon Host - Publier dans la liste de surveillance** de Security Operations est utilisé pour spécifier la liste de surveillance pour la génération d’alertes ou d’événements. Les alertes et les événements sont affichés dans le système CrowdStrike Falcon Host en fonction de sa configuration.

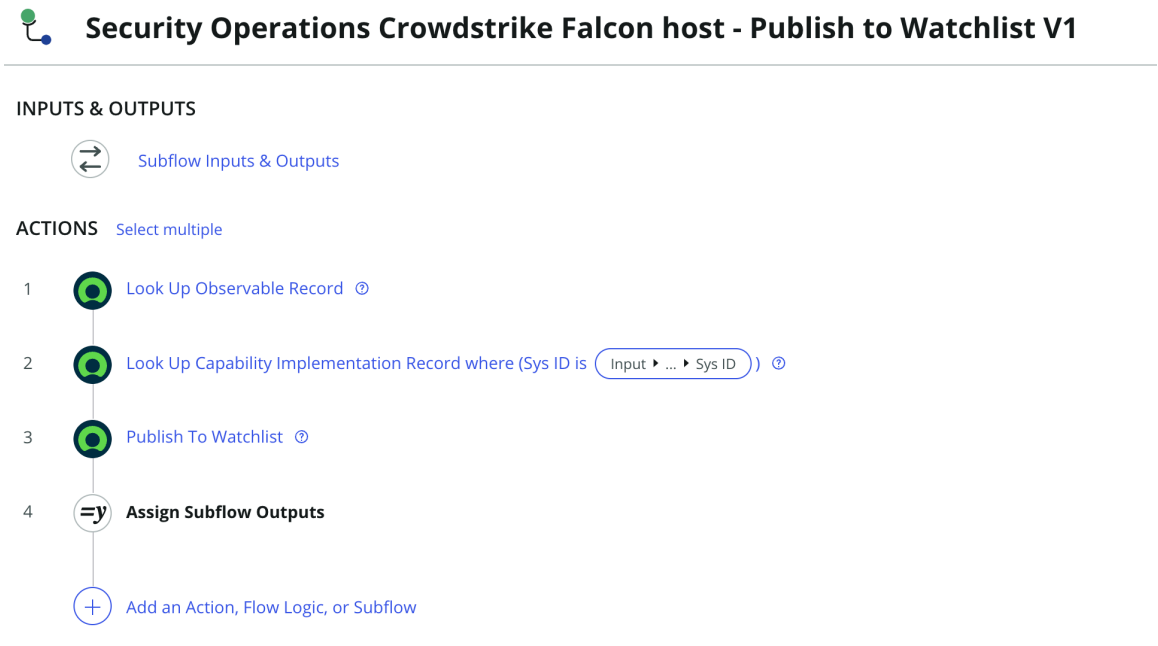
Flux de publication dans la liste de surveillance

Ce concepteur de Security Operations Integration : aptitude de publication dans la liste de surveillance flux est déclenché lorsque vous sélectionnez un ou plusieurs observables associés à un incident de sécurité et que vous utilisez l’action d’interface utilisateur Publier dans la liste de surveillance pour transférer les observables vers une liste de surveillance. Les observables peuvent ensuite être utilisés pour générer des alertes supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations, consultez Publier des observables dans une liste de surveillance



tierce.

Mise en route de l'intégration CrowdStrike Falcon Host

La fonctionnalité Configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration CrowdStrike Falcon Host . Avant de pouvoir utiliser l'intégration CrowdStrike Falcon Host , vous devez la télécharger à partir de puis ajouter un nom d'utilisateur et un ServiceNow Store mot de passe.

Avant de commencer

- Si vous mettez à niveau CrowdStrike Falcon Host l'intégration à partir d'une version précédente, vous devez supprimer la configuration existante et en configurer une nouvelle. La nouvelle intégration prend en charge l'authentification OAUTH2. Cette mise à jour nécessite que vous saisissiez **l'ID et** le **secret du client API** pour vous authentifier et terminer la configuration.
- Dans les **champs d'application de l'API** du CrowdStrike Falcon Host portail, activez le paramètre **Lecture** et **écriture** pour les **IOC (indicateurs de compromission).**

Rôle requis : sn_si_admin

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la carte CrowdStrike Falcon Host, cliquez sur **Configurer**.
4. Renseignez les champs du formulaire pour terminer la configuration :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de l'hôte CrowdStrike Falcon

Champ	Description
Nom	Nom de l'intégration, par exemple `demo-1`.
ID client API	L'ID client que vous obtenez à partir de la section des paramètres de votre profil de compte dans CrowdStrike Falcon Host le portail.
Secret client API	Clé secrète du client que vous obtenez à partir de la section des paramètres de votre profil de compte dans CrowdStrike Falcon Host le portail.

5. Cliquez sur **Envoyer**.

Résultats

Une fois configurée, l'intégration CrowdStrike Falcon Host peut être sélectionnée pour publier des observables dans des listes de surveillance dans Réponse aux incidents de sécurité.

Intégration CrowdStrike Falcon Insight

Avec l'intégration CrowdStrike Falcon Insight For Opérations de sécurité , vous pouvez effectuer des actions de rattrapage sur les points de terminaison en temps réel, utiliser des profils pour recueillir des détails sur l'hôte et effectuer des requêtes ou des actions spécifiques sur le point de terminaison à l'aide du ServiceNow AI Platform Réponse aux incidents de sécurité produit.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

L'intégration CrowdStrike Falcon Insight de Opérations de sécurité fonctionne avec afin ServiceNow AI Platform que vous puissiez obtenir un aperçu supplémentaire de la portée d'un incident. Le CrowdStrike Falcon Insight capture toutes les activités d'événement de point de terminaison pertinentes, vous pouvez utiliser pour ServiceNow AI Platform vous concentrer sur les enquêtes et les actions de rattrapage.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identificateur de document	Titre de document
CrowdStrike Falcon Insight pour Opérations de sécurité	Mise en route de l'intégration CrowdStrike Falcon Insight

Mise en route de l'intégration CrowdStrike Falcon Insight

Vous pouvez activer et configurer l'interface CrowdStrike Falcon Insight avec votre instance et Réponse aux incidents de sécurité votre ServiceNow AI Platform produit.

Rôle requis : admin

Avant de pouvoir l'utiliser CrowdStrike Falcon Insight pour l'intégration Opérations de sécurité , vous devez la télécharger à partir du ServiceNow Store.

Liste de vérification

Tâche de configuration	Description
Affectez et vérifiez les rôles et Réponse aux incidents de sécurité requisServiceNow AI Platform.	Ces rôles sont requis pour la configuration et la vérification des résultats attendus : • Le rôle administrateur installe l'intégration à partir de et ServiceNow Store attribue le rôle sn_si.admin. • Le rôle sn_si.admin configure l'intégration, crée et active les profils, puis affecte le rôle sn_si.analyst. • Le rôle sn_si.analyst répond aux incidents de sécurité, lance manuellement des profils et peut soumettre des demandes d'actions telles que l'isolement de l'hôte et la suppression de l'isolement de l'hôte pour un groupe approuvé.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.	Le ServiceNow Centre d'intégration module d'extension Enterprise Pack Installer [com.glide.hub.integrations.enterprise] est requis. Ce module d'extension permet l'exécution des actions et des flux du Centre d'intégration : Le Réponse aux incidents de sécurité module d'extension (com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ces applications ne sont pas déjà installées, vous devez installer et activer chaque application une par une dans l'ordre suivant pour assurer une installation fluide : **1.** Réponse aux incidents de sécurité Dépendance (com.snc.si_dep) **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Orchestration du support de sécurité **5.** Renseignements sur les menaces Prise en charge commune **6.** Trusted Security Circles **7.** Opérations de sécurité Assistant de configuration **8.** Réponse aux incidents de sécurité
Configurez un groupe d'approbation.	Une aptitude d'approbation facultative est disponible pour isoler les machines hôtes, les restaurer dans le réseau et initier des recherches de perceptions. Pour activer cette option, vous devez obtenir l'approbation préalable du rôle sn_si.admin avant que les ordinateurs hôtes ne soient isolés et restaurés sur votre réseau, ou lorsque des recherches de perceptions sont effectuées. Si vous avez besoin d'un niveau de contrôle supplémentaire sur ces actions, activez l'option **Exiger l'approbation** lors de la configuration du profil. L'autorisation d'approbation est affectée à l'utilisateur disposant du rôle sn_si.admin. Vous pouvez également réaffecter cette autorisation d'approbation à un groupe d'approbation.
Affectez et vérifiez les rôles de la plateforme CrowdStrike Falcon.	Les rôles suivants sont requis sur CrowdStrike Falcon Platform pour la configuration de l'intégration :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	• Le rôle administrateur Falcon est requis pour afficher, créer ou modifier les clients ou les clés de l'API. • Le rôle Intervenant en temps réel : administrateur est requis pour créer et exécuter des scripts personnalisés. • Le rôle Répondant en temps réel : intervenant actif est requis pour créer et exécuter des scripts personnalisés.
Vérifiez que les scripts, rôles et autorisations personnalisés sont activés dans CrowdStrike Falcon Platform.	Cette intégration utilise les scripts personnalisés de CrowdStrike pour certaines des fonctionnalités d'enrichissement. • Vérifiez que les rôles Intervenant en temps réel – Administrateur et Intervenant en temps réel – Intervenant actif sont disponibles. • Vérifiez que l'option de **politique par défaut (Windows)** est activée dans Politiques de configuration > de réponse de l'interface utilisateur CrowdStrike Falcon. • Vérifiez que les **options Réponse en temps réel** et **Scripts personnalisés** sous la fonctionnalité en temps réel sont activées dans l'interface utilisateur CrowdStrike Falcon.
Générer des clients et des clés d'API dans CrowdStrike Falcon Platform.	Créez les clients ou les clés de l'API CrowdStrike dans la plateforme CrowdStrike Falcon Platform à utiliser dans la configuration de l'intégration ServiceNow AI Platform .

Traduction automatique

Créer un client d'API CrowdStrike et générer des clés

Créez le client de l'API CrowdStrike et générez l'ID et la clé client que vous utilisez pour configurer l'intégration CrowdStrike Falcon Insight .

Avant de commencer

Rôle requis : administrateur CrowdStrike Falcon

Procédure

1. Sur CrowdStrike Falcon Platform, accédez à **Clients et clés API**.
2. Dans la table Clients de l'API OAuth2, cliquez sur **Ajouter un nouveau client d'API**.
3. Entrez les détails suivants pour définir votre client API :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du client	Entrez le nom du client. Ce champ est obligatoire.
Description	Entrez la description du nom du client.
Périmètres de l'API	Il est nécessaire de définir les champs d'application. **Important :** Assurez-vous d'activer le compte API et assurez-vous que les champs d'application suivants sont activés pour le compte API : ○ Activer les champs d'application en lecture et en écriture pour l'API hôtes ○ Activer la lecture du périmètre pour l'API des indicateurs

4. Cliquez sur **Ajouter** pour enregistrer le client d'API et générer l'ID client et la clé secrète.

Installer et configurer CrowdStrike Falcon Insight

Installez et configurez l'application ServiceNow Store sur Opérations de sécurité votre CrowdStrike Falcon InsightServiceNow AI Platform instance.

Avant de commencer

Rôle requis : admin

Remarque : Vous ne pouvez associer une option qu'à un seul profil. Vous ne pouvez pas associer une option à plusieurs profils. Lorsque vous configurez des serveurs CrowdStrike, vous ne pouvez pas réutiliser une aptitude CrowdStrike avec plusieurs profils qui partagent le serveur CrowdStrike. Vos profils peuvent avoir la même aptitude CrowdStrike, chaque profil doit utiliser son propre serveur CrowdStrike.

Procédure

1. Téléchargez la pour CrowdStrike Falcon Insight l'intégration de Security Operations à partir de et ServiceNow Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette d'intégration CrowdStrike Falcon InsightOpérations de sécurité , puis cliquez sur **Configurer**.
4. Renseignez les champs du formulaire pour terminer la configuration :

CrowdStrike Falcon Insight Configuration

Champ	Description
Nom	Nom de l'intégration, par exemple `demo-1`.
URL de l'API CrowdStrike Falcon Insight	URL de base qui héberge l'API CrowdStrike. Entrez l'URL avec le protocole HTTPS. Par exemple, https://api.crowdstrike.com.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID client	L'ID client que vous obtenez à partir de la section des paramètres de votre profil de compte dans le CrowdStrike Falcon Insight portail.
Secret client	Clé secrète du client que vous obtenez à partir de la section des paramètres de votre profil de compte dans le CrowdStrike Falcon Insight portail.



5. Cliquez sur **Envoyer**.

Résultats
Une fois l'intégration validée et soumise, elle est enregistrée sur la page Intégrations de sécurité sous forme de tuile. Vous pouvez afficher le module dans le CrowdStrike Falcon Insight navigateur d'application.

Créer un groupe d'approbation

Créez un groupe d'approbation pour l'intégration CrowdStrike Falcon InsightOpérations de sécurité qui peut approuver les demandes d'isolement des ordinateurs hôtes, de restauration sur le réseau et de lancement de recherches de perceptions.

Avant de commencer
Vous ne pouvez pas réaffecter l'autorisation d'approbation à un groupe, sauf si un groupe d'approbation est disponible dans votre instance.

Remarque : L'option d'approbation dans la configuration du profil s'affiche uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte.

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Groupes**.
2. Dans la liste des groupes, cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Groupe d'approbation

Champ	Description
Nom	Nom du groupe qui s'affiche lorsque vous soumettez une demande d'approbation.
E-mail de groupe	Liste de distribution d'e-mails ou adresse e-mail du point de contact du groupe, par exemple le gestionnaire de groupe.
Responsable	Nom du gestionnaire de groupe. Cliquez sur l'icône de recherche pour afficher la liste.
Parent	Nom du groupe parent, s'il est associé à un parent.
Type	Catégories de groupes.
Fournisseurs	vendor_manager rôle que vous affectez aux utilisateurs dans le processus de gestion des fournisseurs de votre organisation.
Description	Informations supplémentaires sur le groupe.

4. Cliquez sur **Envoyer**.
   Le nouveau groupe s'affiche dans la liste Groupes.

Ce groupe est disponible pour traiter les demandes lorsque vous activez l'option **Exiger l'approbation** pendant la configuration de ce profil.

Pour surveiller et traiter les demandes soumises par les utilisateurs disposant du rôle sn_si.analyst, chaque membre du groupe d'approbation accède à l'onglet **Mes approbations** dans le ServiceNow AI Platform.

Que faire ensuite

L'étape suivante consiste à installer et configurer l'application CrowdStrike Falcon Insight à partir du ServiceNow Store.

Créer un profil d'aptitude pour l'intégration CrowdStrike Falcon Insight

Créez un profil et sélectionnez les CrowdStrike Falcon Insight options que vous souhaitez que le profil exécute.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Réfléchissez aux raisons pour lesquelles vous souhaitez créer un profil avant de lui ajouter CrowdStrike Falcon Insight des options. Le tableau suivant répertorie les options que vous devez ajouter à un profil lorsque vous souhaitez que celui-ci effectue certaines requêtes ou actions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez créer un profil unique qui exécute des requêtes pour les détails du système, répertorie les utilisateurs connectés, extrait les services en cours d'exécution, extrait les processus en cours d'exécution, extrait les statistiques réseau, isole l'hôte et supprime l'hôte isolé. Vous pouvez également créer plusieurs profils, chacun ayant sa propre capacité.

Remarque : Les options Isoler l'hôte, Supprimer l'isolement et Obtenir un fichier ne peuvent pas être fusionnées avec d'autres fonctionnalités lors de la création d'un profil.

Types de profils et options CrowdStrike Falcon Insight requises

Objectif du profil	Options de CrowdStrike
Collecter les détails de l'hôte et les utilisateurs connectés	• **Obtenir les détails de l'hôte** • **Obtenir les utilisateurs connectés**
Extraire les statistiques réseau, les processus et les services en cours d'exécution pour un hôte	• **Obtenir les statistiques réseau** • **Obtenir les processus en cours d'exécution** • **Obtenir les services d'exécution**
Isoler un hôte	**Isoler l'hôte**
Supprimer l'isolement d'un hôte	**Supprimer l'isolement**
Obtenir un fichier à partir d'un point de terminaison hôte	**Obtenir un fichier**

Procédure

1. Accédez à la **Tous** > **Intégration de CrowdStrike Falcon Insight** > **Profils des aptitudes de CrowdStrike**.
2. Cliquez sur **Nouveau**.
3. Sur le formulaire, renseignez les champs.

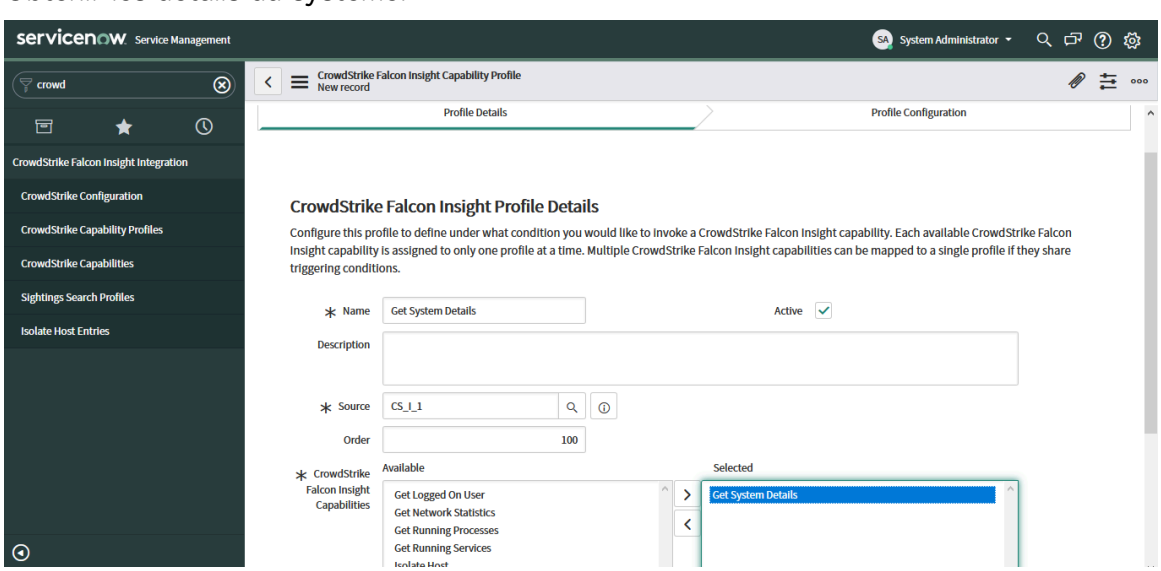
Champ	Description
Nom	Nom du nouveau profil d'aptitude. Ce nom vous permet d'identifier le type de profil et constitue également le nom par défaut de la balise de sécurité associée à ce profil.
Actif	Indique si le profil est actif ou non. Lorsque le profil est actif, il se déclenche automatiquement lorsqu'un incident de sécurité correspondant aux conditions de filtrage que vous avez spécifiées dans la configuration est créé.
Description	Description unique du profil d'aptitude.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Nom du serveur. Vous ne pouvez afficher que les serveurs précédemment configurés à partir de la liste.
Ordre	Priorité du flux. La valeur de ce champ indique l'ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400. Par défaut : 100
Options de CrowdStrike Falcon Insight	Options du profil CrowdStrike Falcon Insight. Sélectionnez les options souhaitées pour ce profil dans la colonne **Disponible** à **Sélectionné**.

L'exemple suivant montre un formulaire complet pour un profil avec la fonctionnalité Obtenir les détails du système.



4. Cliquez sur **Suivant**.

Que faire ensuite

Vous pouvez maintenantconfigurer votre profil. Assurez-vous d'avoir passé en revue les concepts de configuration des profils et des conditions de déclenchement avant de configurer le profil.

Configurer les profils et les incidents de sécurité pour l'intégration CrowdStrike Falcon Insight

Configurez les paramètres de votre profil de sorte que le profil ne se déclenche que dans les conditions que vous définissez.

Avant de commencer

Rôle requis : sn_si.admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Pourquoi et quand exécuter cette tâche

Définissez les conditions qui déclenchent automatiquement les CrowdStrike Falcon Insight options que vous avez sélectionnées pour le profil. Vous pouvez également sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI). Dans cet autre champ, vous pouvez définir des conditions de filtrage afin que seuls les incidents de sécurité liés à votre événement déclencheur déclenchent automatiquement le profil.

Remarque : Accédez à la page Configuration du profil uniquement après avoir saisi les détails du profil. Pour plus d'informations, consultez Créer un profil d'aptitude pour l'intégration de CrowdStrike Falcon Insight.

Procédure

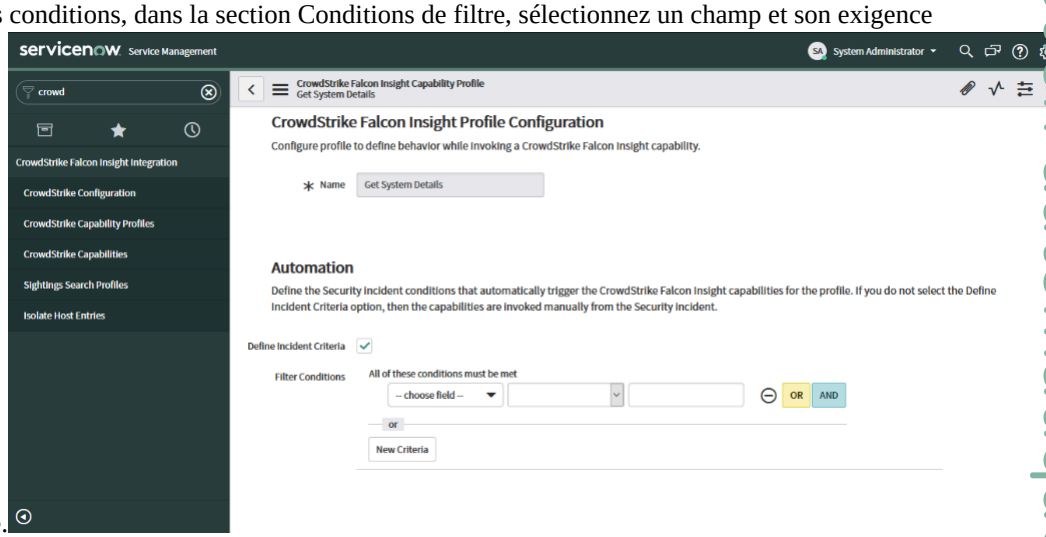
1. Sur la page Configuration du profil, examinez et configurez les sections suivantes :

Définir un critère d'incident (automatisation)

Définissez les conditions d'incident de sécurité qui déclenchent automatiquement les CrowdStrike Falcon Insight options pour le profil. Si vous ne sélectionnez pas l'option **Définir des critères d'incident** , les options sont invoquées manuellement à partir de l'incident de sécurité.

a. Sélectionnez l'option **Définir un critère d'incident** .

b. Pour définir les conditions, dans la section Conditions de filtre, sélectionnez un champ et son exigence correspondante.



c. Dans le champ **Nouveau critère**, saisissez le nouveau critère, puis définissez **la conditionOU** ou ET.



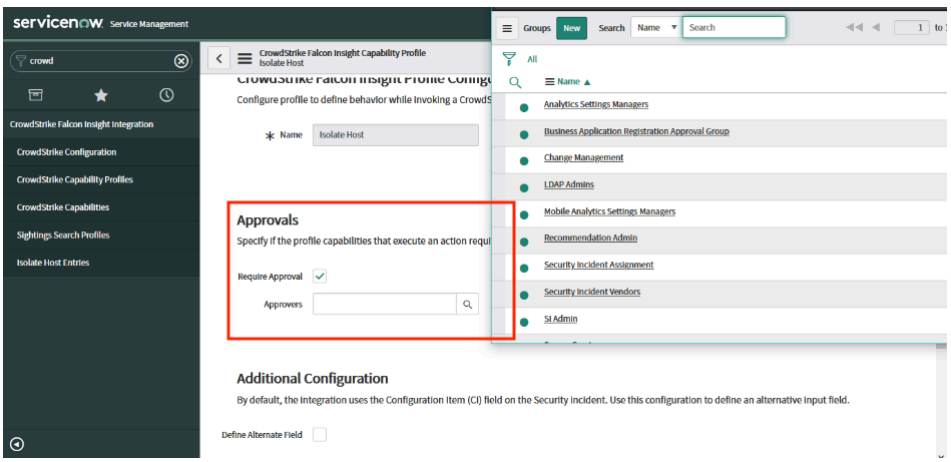
Approbations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour fournir un niveau de contrôle supplémentaire lorsque vous utilisez les options de CrowdStrike Falcon Insight, sélectionnez l'option **Exiger une approbation** . L'option d'approbation dans la configuration du profil s'affiche uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte.

Remarque : L'autorisation d'approbation est affectée à l'utilisateur disposant du rôle sn_si.admin. Vous pouvez également réaffecter cette autorisation d'approbation à un groupe d'approbation. Pour plus d'informations, voir Configurer un groupe d'approbation.



Configuration supplémentaire

Sélectionnez un autre champ sur l'incident de sécurité pour afficher toutes les données de CI correspondantes que vous trouvez lors de l'analyse de vos actifs. Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité.

a. Sélectionnez l'option **Définir un autre champ** .

b. Dans le **champ Autre déclencheur CI**, sélectionnez un champ d'entrée.

Remarque : Pour plus d'informations, consultez Comprendre comment les conditions de déclenchement fonctionnent avec un élément de configuration pour un profil.

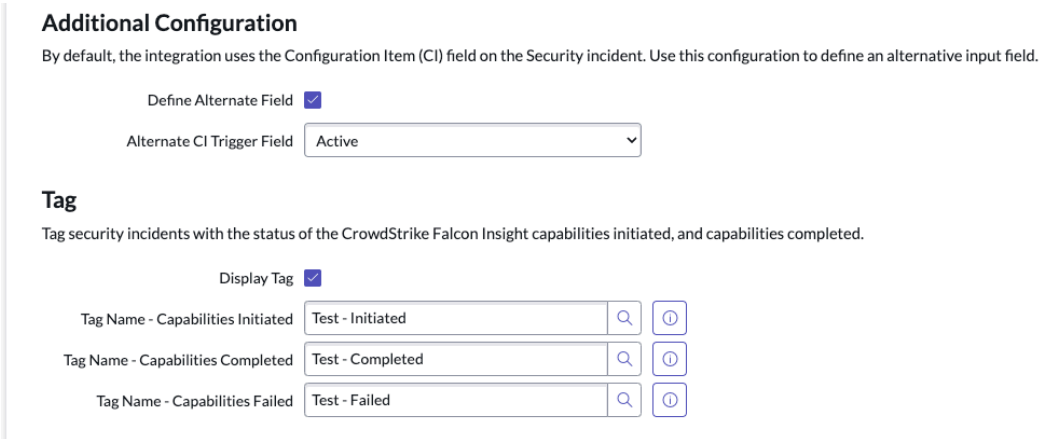
Balises

Pour baliser les incidents de sécurité avec les CrowdStrike Falcon Insight balises Capacités lancées, Capacités terminées et Capacités échouées, sélectionnez l'option **Balises d'affichage** . Par défaut, cette option est désactivée pour tous les profils.

Remarque : Ces balises sont fournies avec le système de base. Vous pouvez créer vos propres balises si nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Cliquez sur **Terminé**.

Comment les conditions de déclenchement fonctionnent avec un élément de configuration pour un profil

Vous pouvez configurer les paramètres de profil de sorte qu'un profil s'exécute uniquement lorsqu'un ensemble de conditions spécifiques est rempli, ou vous pouvez configurer un profil pour rechercher des valeurs de champ spécifiques sur un incident de sécurité.

Après avoir créé un profil et sélectionné les CrowdStrike Falcon Insight options sur lesquelles vous souhaitez que le profil s'exécute, vous pouvez définir des conditions de déclenchement afin que votre profil s'exécute automatiquement lorsque les valeurs de champ par défaut correspondent à l'incident ServiceNow AI Platform de sécurité.

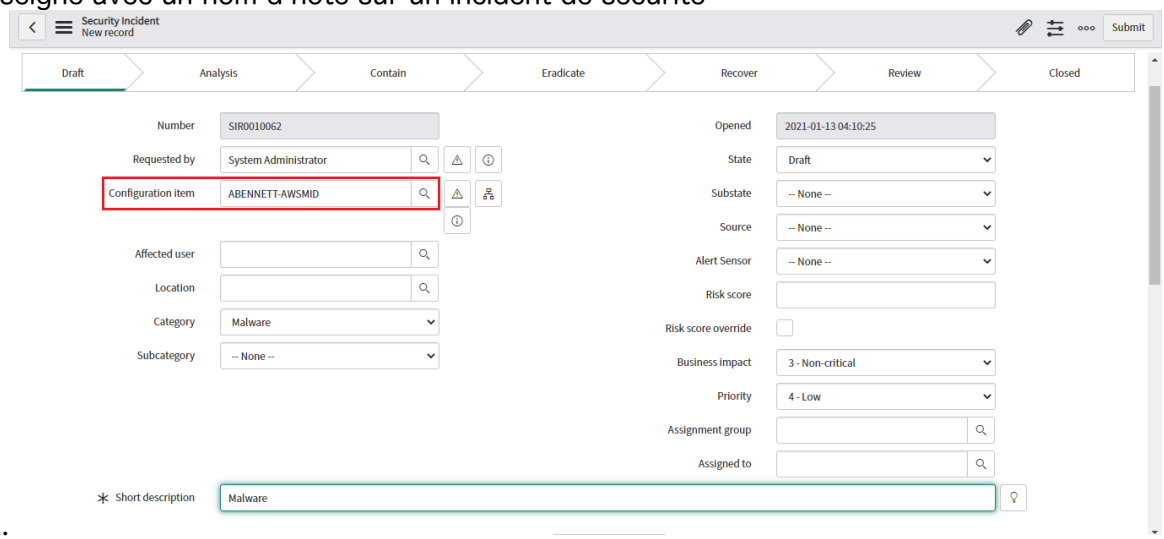
Par défaut, l'intégration utilise le champ **Élément de configuration** (CI) sur un incident de sécurité. Ce champ est utilisé pour faire correspondre vos ID d'actifs avec les informations stockées dans la ServiceNow AI Platform base de données. Lorsqu'un incident de sécurité SIR est créé par un événement de sécurité et qu'un profil est activé, vos actifs sont analysés pour rechercher une valeur correspondante sur le nom d'hôte ou une adresse IP.

Lorsqu'une valeur correspondante est trouvée dans la base de données, cette donnée est collectée à partir de la CrowdStrike Falcon Insight console et est transférée vers votre ServiceNow AI Platform instance où elle s'affiche dans les listes connexes d'un incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'exemple suivant montre un champ Élément de configuration renseigné avec un nom d'hôte sur un incident de sécurité

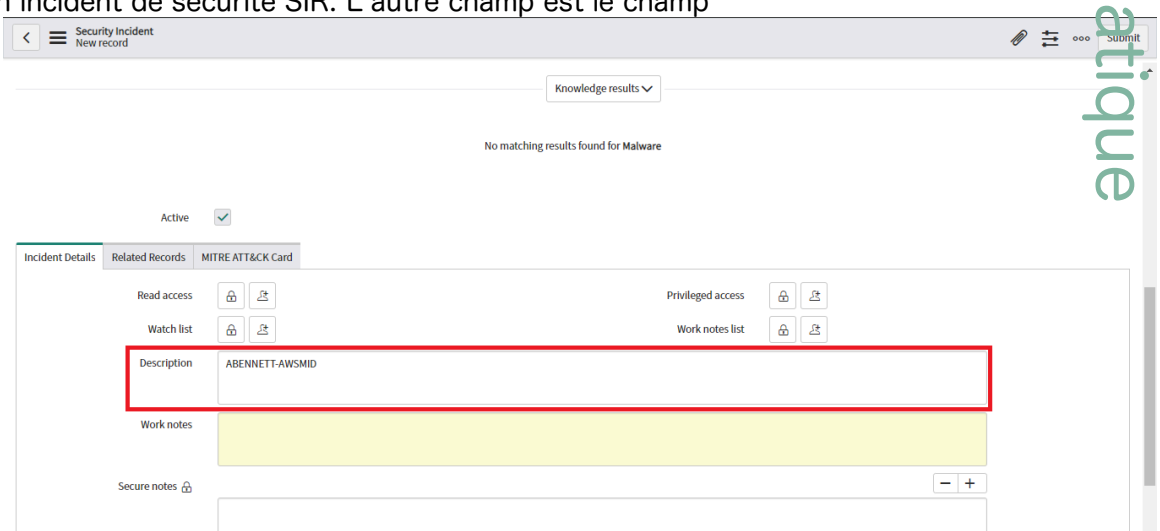


SIR.

Lorsque le champ **Élément de configuration** (CI) n'est pas renseigné avec un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour afficher toutes les données de CI correspondantes que vous trouvez lors de l'analyse de vos actifs.

Lorsque vous configurez la configuration du profil, vous pouvez sélectionner un autre champ de **déclenchement CI** pour l'identification du point de terminaison afin de vous assurer que les données CI de la CrowdStrike Falcon Insight recherche sont renseignées sur l'incident de sécurité associé. Vous pouvez sélectionner n'importe quel champ de l'incident de sécurité comme champ de déclenchement CI alternatif, y compris les champs personnalisés que vous créez. Si le champ CI n'est pas renseigné sur l'incident de sécurité associé lors de la création de l'incident, sélectionnez l'autre champ CI pour vous assurer que vos profils sont déclenchés.

L'exemple suivant montre un autre champ renseigné avec un nom d'hôte sur un incident de sécurité SIR. L'autre champ est le champ



Description .

Vérifier les CrowdStrike Falcon Insight conditions de déclenchement du profil

Testez le profil et vérifiez que les filtres de condition de déclenchement que vous avez configurés fonctionnent comme prévu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

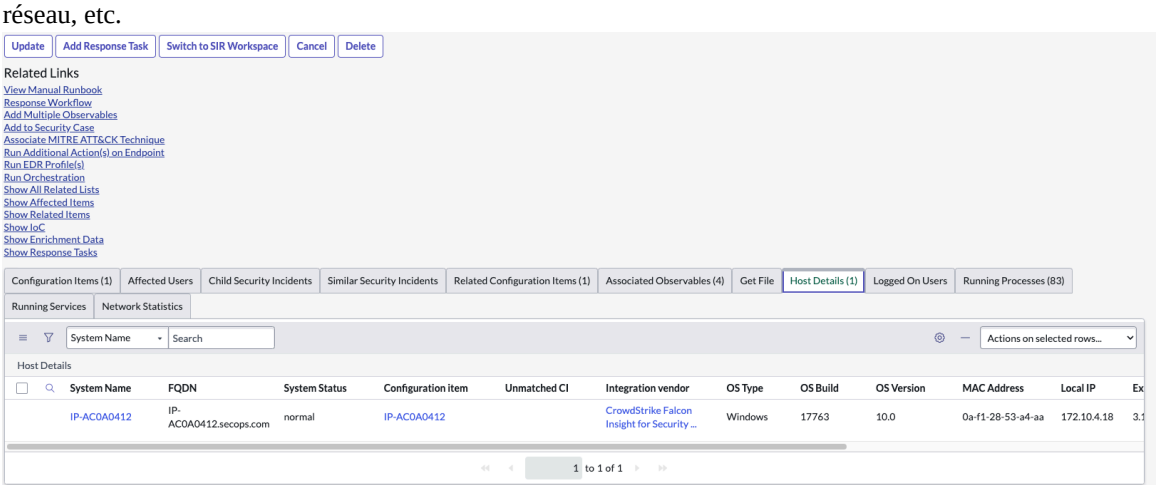
Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Activez le profil basé sur les conditions de déclenchement configurées que vous avez spécifiées afin de pouvoir afficher les résultats de la requête dans les ServiceNow AI Platform incidents de sécurité.

Procédure
1. Accédez à la **Tous** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez **Nouveau** pour créer un incident de sécurité.
3. Pour créer un incident de sécurité, renseignez les informations requises et cliquez sur **Enregistrer**.
4. Passez en revue la section Notes de travail et activités pour afficher les balises initiées et terminées par le profil.



5. Examinez les détails dans les listes connexes Détails, telles que Obtenir un fichier, Détails de l'hôte CrowdStrike Falcon Insight , Utilisateurs connectés, Processus en cours, Services en cours, Statistiques réseau, etc.



Déclencher manuellement un CrowdStrike Falcon Insight profil à partir d'un incident de sécurité

Déclenchez manuellement un profil après avoir examiné un incident de sécurité.

Avant de commencer
Rôle requis : admin

Traduction automatique

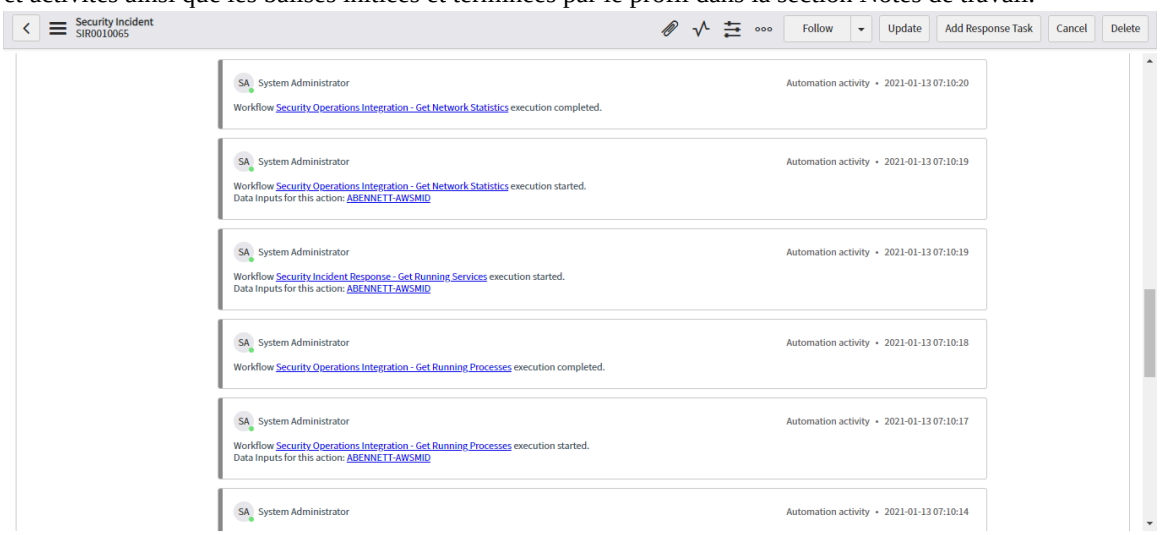
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

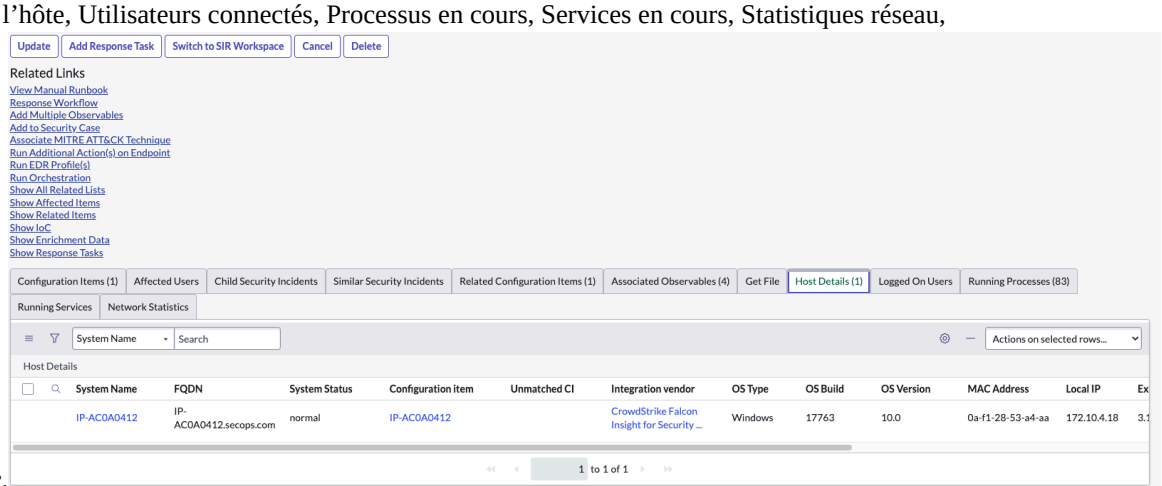
Une fois que vous avez activé le profil, en fonction des conditions de déclenchement configurées, vous pouvez afficher les résultats de la requête dans les ServiceNow AI Platform incidents de sécurité. CrowdStrike Falcon Insight vous permet également d'exécuter des options individuelles sur des éléments de configuration (CI) sans utiliser de profil.

Procédure

1. Accédez à la **Tous** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les CrowdStrike Falcon Insight informations.
3. Dans la section des listes connexes, sélectionnez **Exécuter le(s) profil(s) EDR**.
4. Parcourez et sélectionnez un profil dans la liste des profils disponibles.
5. Sélectionnez **Inclure le CI connexe** pour exécuter ce profil sur tous les CI associés du profil.
   Par exemple, si cinq CI sont associés à l'incident de sécurité, le profil sélectionné s'exécute sur les cinq CI.
6. Cliquez sur **Envoyer**.
   Le profil sélectionné est déclenché manuellement. Vous pouvez consulter la section Notes de travail et activités ainsi que les balises initiées et terminées par le profil dans la section Notes de travail.



7. Les résultats s'affichent sous la forme de listes connexes telles que Obtenir un fichier, Détails de l'hôte, Utilisateurs connectés, Processus en cours, Services en cours, Statistiques réseau, etc.



8. Pour exécuter des options individuelles sur un CI, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans la liste connexe Éléments de configuration, sélectionnez le CI requis.

b. Cliquez sur la liste déroulante **Actions sur les lignes sélectionnées...** et sélectionnez l'option requise que vous souhaitez exécuter pour le CI sélectionné.
Par exemple, Isoler l'hôte.

c. Recherchez l'implémentation de l'aptitude requise pour le CI à l'aide de l'option de recherche, puis sélectionnez **Isoler l'hôte de CrowdStrike Falcon Insight**.

d. Cliquez sur **Isoler l'hôte** pour l'exécuter sur le CI sélectionné.

Créer et configurer un profil pour la recherche de perception

Utilisez les recherches CrowdStrike Falcon Insight de perceptions pour localiser les machines infectées sur le réseau de votre organisation et pour traiter les tickets de réponse aux incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Sélectionnez un ou plusieurs observables et effectuez une recherche de perception manuelle pour CrowdStrike Falcon Insight déterminer la prévalence d'une menace au fil du temps.

Procédure

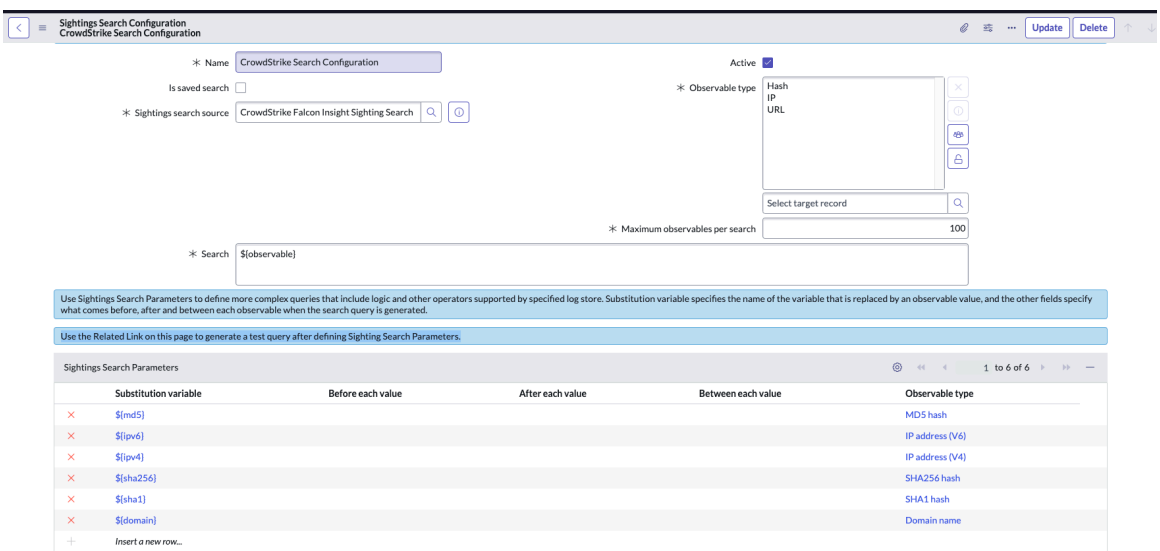
1. Accédez à la **Tous** > **Intégration de CrowdStrike Falcon Insight** > **Profils de recherche de perception**.
2. Cliquez sur **Nouveau**.
3. Configurez ce profil pour déterminer les serveurs à rechercher pour une option de recherche CrowdStrike Falcon Insight spécifique.
4. Renseignez les champs du formulaire :

Champ	Description
Nom	Nom du profil de recherche de perceptions.
Est une recherche enregistrée	La configuration de recherche enregistrée est créée si vous sélectionnez cette option.
Source de recherche de perceptions	La source de la recherche d'observations. Sélectionnez la **recherche d'observation de CrowdStrike Falcon Insight** comme source.
Actif	Option permettant d'indiquer si le supplémentaire est actif ou non.
Type d'observable	L'intégration de CrowdStrike Falcon Insight prend en charge les types d'observables suivants : ○ Hachage ○ IP ○ URL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La recherche de perception est prise en charge pour les types d'observables suivants : ○ Nom du domaine ○ Adresse IP (V4) ○ Adresse IP (V6) ○ Hachage MD5 ○ Hachage SHA1 ○ Hachage SHA256
Nombre maximum d'observables par recherche	Nombre maximal d'observables que vous pouvez afficher à partir d'une requête de recherche.
Rechercher	La chaîne de recherche par défaut est $(observable), mais vous pouvez définir votre propre requête de recherche en spécifiant les paramètres pris en charge par l'intégration CrowdStrike Falcon Insight .
Paramètres de la recherche de perceptions	Paramètres pour définir des requêtes plus complexes qui incluent la logique et d'autres opérateurs pris en charge par le magasin de journaux spécifié Vous pouvez utiliser les liens connexes en bas de la page pour générer une requête de test après avoir défini des paramètres de recherche de perceptions.



5. Cliquez sur **Envoyer**.
   La configuration est terminée et vous pouvez invoquer la recherche de perceptions à partir de l'incident ServiceNow AI Platform de sécurité.
6. Pour vérifier la configuration et exécuter une recherche de perception, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Ouvrez un incident de sécurité, faites défiler jusqu'au bas de l'incident de sécurité, puis cliquez sur **Afficher toutes les listes connexes**.

b. Si vous sélectionnez un ou plusieurs éléments de configuration (CI) dans les listes connexes **Exécution des processus** .

> **Remarque :** Si vous exécutez une recherche de perception pour un CI à partir de la liste connexe Exécution des processus, il ne s'agira alors que d'une recherche de perception de hachage de processus.

c. Cliquez sur la liste déroulante **Actions sur les lignes sélectionnées...** , puis sélectionnez **Exécuter la recherche d'observations CrowdStrike**.

d. Recherchez le profil de recherche de perceptions requis à l'aide de l'option de recherche.

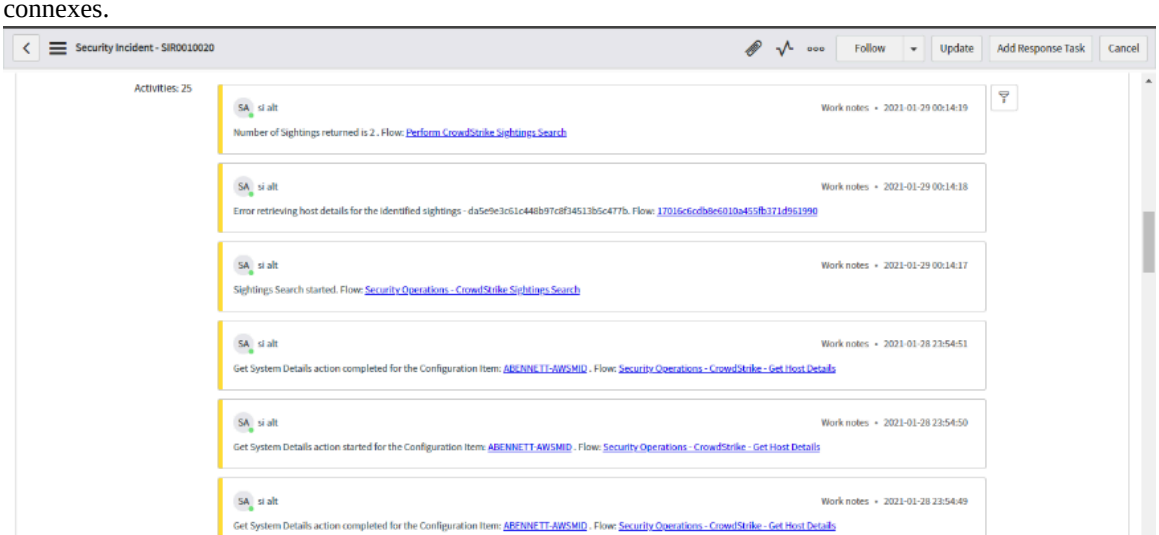
e. Sélectionnez le profil de recherche de perception requis, puis cliquez sur **Soumettre**.

f. Si vous sélectionnez un ou plusieurs observables dans les listes connexes **Observables associés** .

g. Cliquez sur la liste déroulante **Actions sur les lignes sélectionnées...** , puis sélectionnez **Exécuter la recherche de perceptions**.

h. Dans la fenêtre contextuelle du délai, sélectionnez une valeur aléatoire et cliquez sur **Rechercher**.

i. Une fois la recherche terminée, validez les résultats et les détails dans les notes de travail et les listes connexes.



j. Sélectionnez l'onglet **Perceptions** pour afficher les détails de l'observation.

k. Cliquez sur l'icône **Aperçu** en regard du CI pour afficher plus d'informations sur les détails d'observation de CrowdStrike.

l. Cliquez sur **Détails de recherche de perceptions** pour afficher les détails de la recherche de perceptions, puis sur l'onglet **Résultats de recherche de perceptions** pour les résultats de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer et déclencher des actions supplémentaires dans CrowdStrike Falcon Insight

L'intégration CrowdStrike Falcon Insight prend en charge l'exécution d'actions supplémentaires telles que l'expression régulière (regex). L'intégration CrowdStrike Falcon Insight fournit 40 actions supplémentaires avec le système de base.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

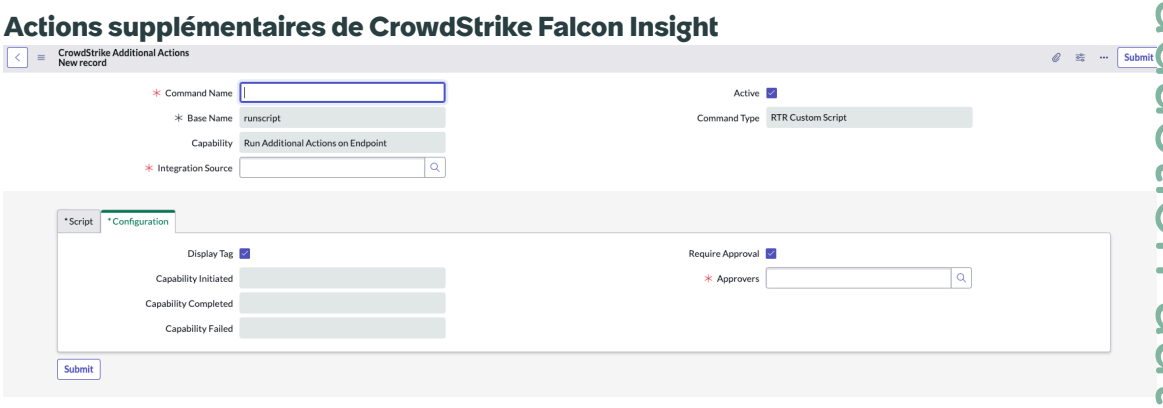
1. Accédez à la **Tous** > **Intégration de CrowdStrike Falcon Insight** > **Actions supplémentaires de CrowdStrike**.
2. Cliquez sur **Nouveau** pour créer votre propre action supplémentaire ou sélectionnez une action existante fournie avec le système de base.
   Par exemple, créons une action supplémentaire.
3. Renseignez les champs du formulaire.

Champ	Description
Nom de la commande	Nom de la commande de l'action supplémentaire. Par exemple, ensemble d'enregistrements.
Nom de base	Nom de base de l'action supplémentaire. Ce champ est défini par défaut. Par exemple, reg.
Option	Nom de l'aptitude de l'action supplémentaire. Ce champ est défini par défaut. Par exemple, exécuter des actions supplémentaires sur le point de terminaison.
Source d'intégration	La source de l'action supplémentaire. Par exemple, Intégration de CrowdStrike Falcon Insight.
Actif	Option permettant d'indiquer si le supplémentaire est actif ou non.
Type de commande	Type de commande pour l'action supplémentaire. Ce champ est défini par défaut. Par exemple, Script personnalisé RTR.
Script	○ **Type de système d'exploitation** : option permettant de sélectionner le type de système d'exploitation pour votre script. Sélectionnez l'une des options suivantes : ▪ **Windows** ▪ **Mac OS X** ▪ **Linux** ▪ **Aucun** ○ **Script** : option permettant d'entrer votre script si vous avez sélectionné l'un des systèmes d'exploitation suivants, à l'exception de l'option Aucun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Configuration	○ **Balise d'affichage** : option permettant d'afficher la balise pour la configuration. Vous pouvez sélectionner la balise pour les champs suivants : ▪ Aptitude : initiée. Par exemple, reg set - Initié. ▪ Aptitude : terminée. Par exemple, reg set - Completed. ▪ Aptitude : échec. Par exemple, reg set - Échec. ○ **Exiger l'approbation** : option permettant de sélectionner un approbateur ou un groupe qui doit approuver la configuration.



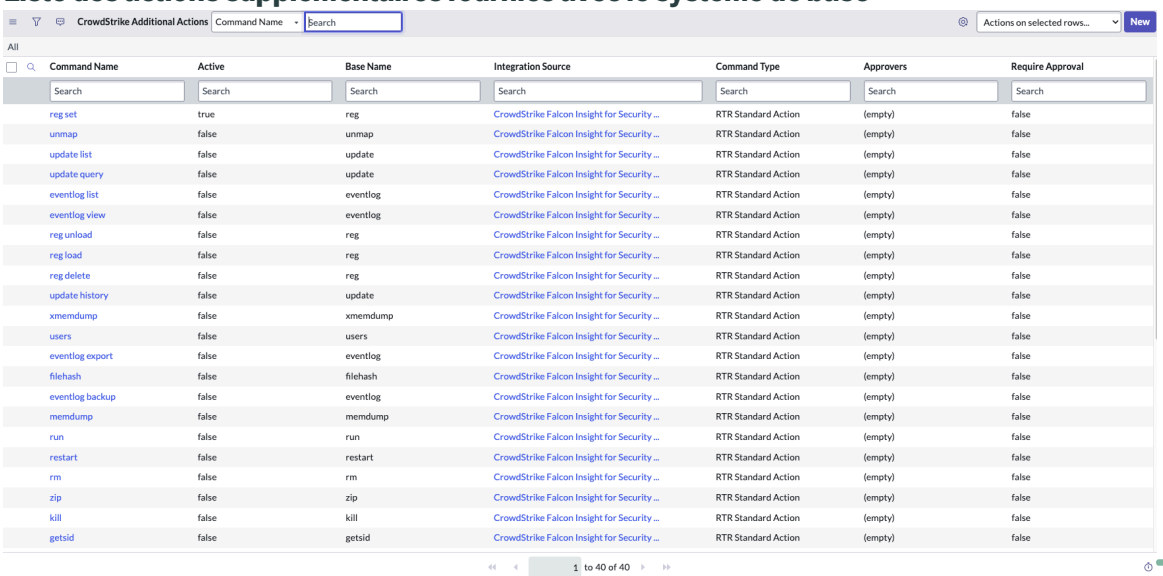
4. Cliquez sur **Envoyer**.
5. Vous pouvez également choisir parmi les actions supplémentaires existantes.
   Le système de base fournit 40 actions supplémentaires que vous pouvez utiliser pour effectuer des configurations supplémentaires.

> **Remarque :** Assurez-vous d'ouvrir la liste Actions supplémentaires de CrowdStrike et de définir l'action supplémentaire requise sur **vrai**, sinon l'action supplémentaire ne sera pas disponible dans l'espace de travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste des actions supplémentaires fournies avec le système de base



Command Name	Active	Base Name	Integration Source	Command Type	Approvers	Require Approval
reg set	true	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
unmap	false	unmap	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update list	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update query	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog list	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog view	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg unload	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg load	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg delete	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update history	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
xmemdump	false	xmemdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
users	false	users	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog export	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
filehash	false	filehash	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog backup	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
memdump	false	memdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
run	false	run	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
restart	false	restart	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
rm	false	rm	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
zip	false	zip	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
kill	false	kill	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
getsid	false	getsid	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false

1 to 40 of 40

6. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
7. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec l'exécution d'actions supplémentaires sur le point de terminaison.
   a. Dans la section Liens connexes, cliquez sur **Exécuter des actions supplémentaires sur le point de terminaison**.
   b. Parcourez et sélectionnez l'option requise.
   Par exemple, cliquez sur **l'option de définition d'enregistrement** .
   c. Sélectionnez **Inclure le CI connexe** pour exécuter les actions supplémentaires sur tous les CI associés du point de terminaison.
   d. Vous pouvez définir la **sous-clé** pour l'exécution des actions supplémentaires sur le point de terminaison. Cette sous-clé peut être une clé HKLM/Logiciel/nouvelle.
8. Pour lancer l'exécution d'actions supplémentaires sur le point de terminaison, cliquez sur **Exécuter une action supplémentaire**.
9. Affichez les activités d'automatisation de l'exécution et validez-les.
10. Validez l'état de l'action dans les listes connexes Actions supplémentaires sur le point de terminaison.

Utilisation de l'intégration CrowdStrike Falcon Insight dans Analyst Workspace

Utilisez l'intégration CrowdStrike Falcon Insight pour tirer parti des CrowdStrike Falcon Insight options de l'espace de travail d'analyste SIR.

Avant de commencer

Rôle requis : sn_si.admin

Avant d'utiliser CrowdStrike Falcon Insight l'intégration dans l'espace de travail de Réponse aux incidents de sécurité, vous devez la télécharger à partir de et la ServiceNow Store configurer. Pour plus d'informations, consultez Mise en route de l'intégration CrowdStrike Falcon Insight.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'intégration CrowdStrike Falcon Insight pour effectuer des actions de rattrapage sur les points de terminaison en temps réel, utiliser des profils pour recueillir des détails sur l'hôte et effectuer des requêtes ou des actions spécifiques sur le point de terminaison à l'aide de l'espace de Réponse aux incidents de sécurité travail.

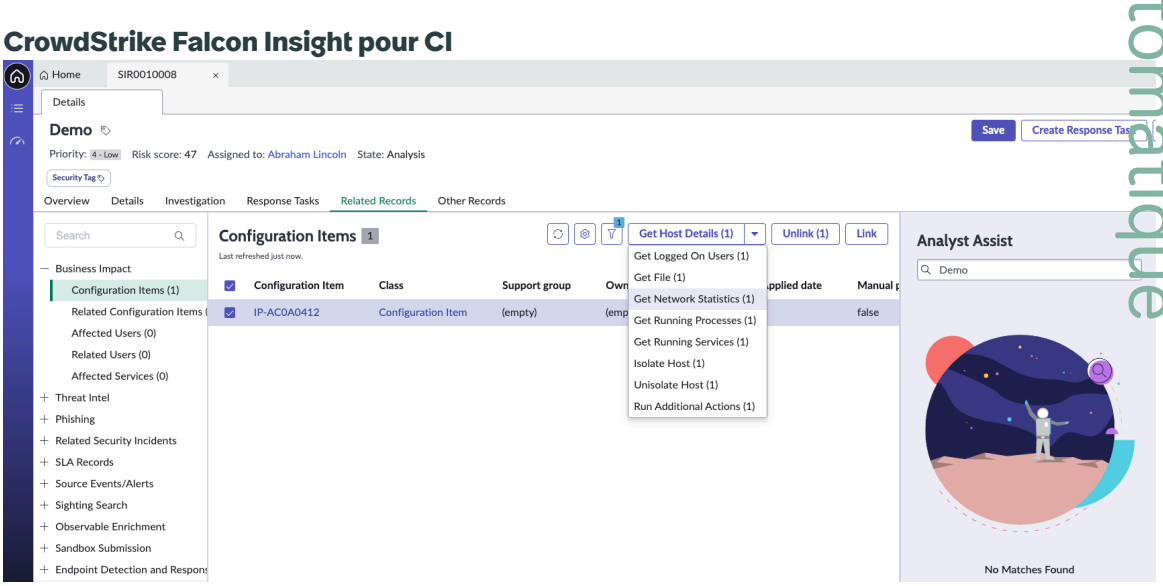
L'intégration CrowdStrike Falcon Insight permet aux analystes d'utiliser les options suivantes CrowdStrike Falcon Insight sur Analyst Réponse aux incidents de sécurité Workspace :

- **Obtenir les détails de l'hôte**
- **Obtenir les utilisateurs connectés**
- **Obtenir les statistiques réseau**
- **Obtenir les processus en cours d'exécution**
- **Obtenir les services d'exécution**
- **Isoler l'hôte**
- **Supprimer l'isolement**
- **Obtenir un fichier**

Procédure

1. Dans l'espace de travail SIR, ouvrez l'incident de sécurité requis et sélectionnez l'onglet **Enregistrements connexes** .
2. Vous pouvez utiliser les options de CrowdStrike Falcon Insight sur la liste connexe Impact sur l'entreprise à des fins d'analyse.

   a. Sélectionnez un **élément de configuration**, puis choisissez une option dans la liste déroulante.



   b. Sélectionnez l'implémentation de **CrowdStrike Falcon Insight** , puis cliquez sur **Soumettre**. L'aptitude Obtenir les statistiques réseau est invoquée sur le CI. Vous pouvez consulter les notes de travail pour connaître les résultats et les conclusions.

3. Vous pouvez utiliser les options de CrowdStrike Falcon Insight sur la liste connexe **Détection et réponse des points de terminaison (EDR)** à des fins d'analyse.

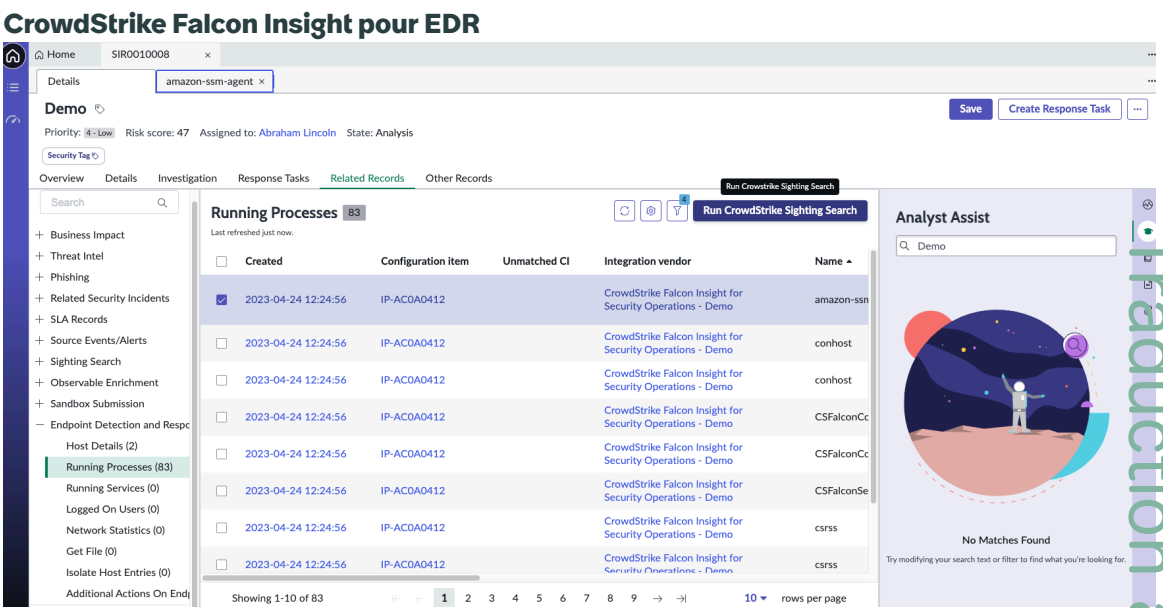
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans la liste connexe à Détection et réponse des points de terminaison (PEPT), choisissez un PEPT.

b. Cliquez sur un processus en cours particulier pour afficher les détails du processus en cours de CrowdStrike Falcon Insight.

c. Pour exécuter une recherche d'observation des faucons de CrowdStrike sur un processus en cours d'exécution particulier, sélectionnez le processus en cours et cliquez sur **Exécuter l'observation de CrowdStrike**.



d. Sélectionnez l'implémentation de **CrowdStrike Falcon Insight** , puis cliquez sur **Exécuter la recherche**.
Ensuite, une recherche de perception de hachage est exécutée sur le processus en cours sélectionné. Vous pouvez consulter les notes de travail pour connaître les résultats et les conclusions.

4. Vous pouvez utiliser les options de CrowdStrike Falcon Insight sur **Threat Intelligence** à des fins d'analyse.

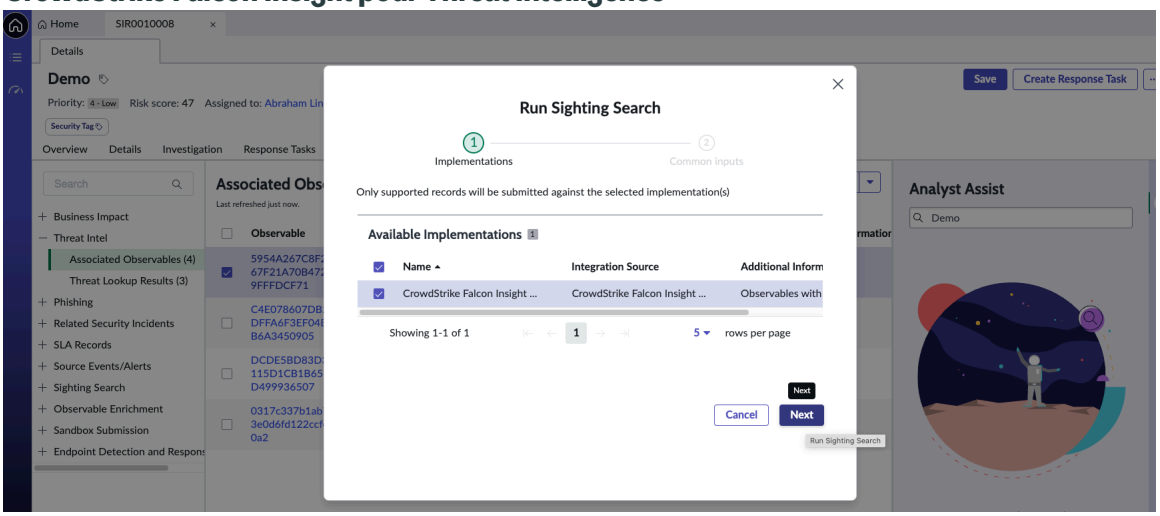
a. Dans le groupe Threat Intel, sélectionnez un **observable**, puis choisissez une CrowdStrike Falcon Insight aptitude dans la liste déroulante.

b. Sélectionnez l'implémentation de **CrowdStrike Falcon Insight** , puis cliquez sur **Suivant**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

CrowdStrike Falcon Insight pour Threat Intelligence



c. Dans la fenêtre contextuelle Sélectionner la date/l'heure, sélectionnez une valeur aléatoire et cliquez sur **Soumettre**.
Ensuite, une recherche d'observation est exécutée sur l'observable sélectionné. Vous pouvez consulter les notes de travail pour connaître les résultats et les conclusions.

Intégration CrowdStrike Next-Gen SIEM

L'intégration CrowdStrike Next-Gen SIEM ingère automatiquement les données de détection qui peuvent indiquer des incidents de sécurité potentiels et rationalise la création d'incidents de sécurité dans Security ServiceNow® Incident Response (SIR), garantissant ainsi une réponse rapide et efficace.

Demander des applications dans l'App Store

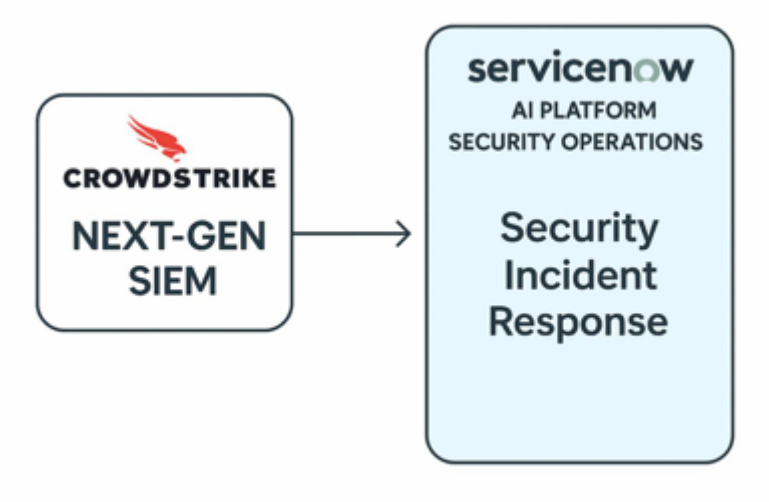
Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Vue d'ensemble de l'intégration CrowdStrike Next-Gen SIEM

Consultez le graphique suivant pour découvrir comment CrowdStrike Next-Gen SIEM s'intègre aux ServiceNow AI Platform Opérations de sécurité applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Fonctionnalités principales

Utilisez les fonctionnalités clés de cette intégration pour effectuer les actions suivantes :

- Découvrez CrowdStrike Next-Gen SIEM les détections qui sont candidates aux incidents de sécurité et automatisez la création de ces incidents de sécurité.
- Mappez CrowdStrike Next-Gen SIEM les champs de défaut et d'entité aux champs d'incident SIR de sécurité.
- Défauts des filtres CrowdStrike Next-Gen SIEM .
- Regroupez les incidents aux incidents de sécurité ouverts existants afin de ne pas avoir à créer des incidents de sécurité en double.
- Automatisez CrowdStrike Next-Gen SIEM les mises à jour de l'état de détection pour Réponse aux incidents de sécurité afin de pouvoir créer et fermer des incidents de sécurité.

> **Remarque :** ServiceNow Met à jour l'état des détections en fonction de CrowdStrike Next-Gen SIEM la création ou de la fermeture de l'incident de sécurité. Cette mise à jour inclut également des commentaires sur les détections agrégées et les nouvelles détections.

- Planifiez l'ingestion de détection pour créer des incidents de sécurité périodiquement.
- Synchronisez les commentaires de détection avec SIR les CrowdStrike Next-Gen SIEM notes de travail.

Mise en route de l'intégration CrowdStrike Next-Gen SIEM

Activez et configurez l'intégration du module d'extension Security Operation pour qu'il s'interface CrowdStrike Next-Gen SIEM avec votre instance et Réponse aux incidents de sécurité votre ServiceNow AI Platform produit.

Avant de pouvoir utiliser l'intégration CrowdStrike Next-Gen SIEM , vous devez la télécharger à partir du ServiceNow Store.

Passez en revue la liste de vérification de configuration suivante et vérifiez que vous avez terminé toutes les tâches pour une intégration fluide.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification

Tâche de configuration	Description
Affectez et vérifiez les rôles et Réponse aux incidents de sécurité requisServiceNow AI Platform.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • Le rôle administrateur installe l'intégration à partir de et ServiceNow Store attribue les rôles sn_si.ingestion_profile_admin et sn_si.analyst. • Le rôle sn_si.ingestion_profile_admin effectue les tâches suivantes : ◦ Configure l'intégration. ◦ Crée des profils de détection. ◦ Mappe les CrowdStrike Next-Gen SIEM champs de données de détection aux champs d'incident de sécurité. ◦ Planifie l'ingestion de détection en cours. ◦ Active les mises à jour de détection lorsqu'une Réponse aux incidents de sécurité détection est créée ou fermée.
Affectez les rôles requis dans CrowdStrike.	Les rôles suivants sont requis dans CrowdStrike pour enregistrer et configurer votre application : • Développeur d'application pour l'enregistrement de l'application. • Administrateur du locataire pour donner des autorisations à l'application en appelant le point de terminaison de consentement de l'administrateur.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.	Le Réponse aux incidents de sécurité module d'extension (com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration.
Installer et configurer	Installez et configurez l'intégration pour l'application CrowdStrike Next-Gen SIEMServiceNow Store sur Opérations de sécurité votre instance de plateforme IA ServiceNow.

Installer et configurer

Installez et configurez l'intégration pour l'application CrowdStrike Next-Gen SIEMServiceNow Store sur Opérations de sécurité votre instance de plateforme IA ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car ce rôle hérite des autorisations requises par défaut.

Procédure

1. Téléchargez l'intégration CrowdStrike Next-Gen SIEM à partir de et ServiceNow Store installez-la.
   Pour plus d'informations, voir Télécharger une application à partir de ServiceNow Store pour la première fois
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette d'intégration CrowdStrike Next-Gen SIEM et sélectionnez **Configurer**.
4. Remplissez les champs du formulaire.

Formulaire d'intégration CrowdStrike Next-Gen SIEM

Champ	Description
Nom	Nom de l'intégration CrowdStrike Next-Gen SIEM .
ID client	L'ID client que vous obtenez à partir de la section des paramètres de votre profil de compte sur le portail CrowdStrike.
Secret client	La clé secrète du client que vous obtenez à partir de la section des paramètres de votre profil de compte sur le portail CrowdStrike.
Région	Centre de données depuis lequel extraire les données. Spécifiez la région : US-1, US-2, EU-1, US-GOV-1, US-GOV-2 Par défaut, ce champ est défini sur US-1

5. Sélectionnez **Soumettre**.
   La vignette d'intégration configurée s'affiche.

Que faire ensuite

Créer un profil de détection

Créer un profil de détection

Déterminez les CrowdStrike Next-Gen SIEM détections appropriées pour créer des incidents de sécurité en créant un profil de détection dans votre ServiceNow AI Platform instance.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > *CrowdStrike Next-Gen SIEM* > **Profil de détection**.
2. Sélectionnez **Nouveau**.
3. Remplissez les champs du formulaire.

CrowdStrike Next-Gen SIEM - Formulaire Configuration de l'ingestion de détection

Champ	Description
Nom	Nom du profil. Ce nom est également le nom par défaut de la balise de sécurité associée à ce profil.
Actif	Option permettant d'activer le profil. Lorsqu'un profil est actif, les ServiceNow AI Platform détections interrogent CrowdStrike Next-Gen SIEM activement et les détections de sécurité correspondantes sont créées lorsque Réponse aux incidents de sécurité les conditions de filtrage sont vérifiées.
Source	CrowdStrike Locataire que vous avez configuré pour ingérer des détections. Si vous avez configuré plusieurs locataires, sélectionnez le locataire approprié pour les types de détection que vous prévoyez d'ingérer pour le profil.
Ordre	Priorité dans laquelle les profils sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Les valeurs de priorité sont généralement fournies sous la forme 100 (valeur par défaut), 200, 300, etc. Le profil avec le numéro le plus bas a la priorité la plus élevée.
Description	Description facultative du profil.

4. Sélectionnez **Mettre à jour** .

   Le profil de détection initial est créé avec des informations de base. L'enregistrement du profil à ce stade vous permet de continuer à définir le profil au cas où vous seriez interrompu.

5. **Facultatif :** Poursuivez immédiatement le processus de définition de profil.
   a. Sur la page Profils de détection CrowdStrike-NextGen, sélectionnez le profil que vous venez de créer.
   b. Dans la barre de progression, sélectionnez **Règles de corrélation**.

Que faire ensuite

Définir des règles de corrélation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir des règles de corrélation

Après avoir créé un profil de CrowdStrike Next-Gen SIEM détection, sélectionnez des règles de corrélation pour mapper les détections correspondantes à un incident de sécurité. Les règles de corrélation sont actualisées chaque fois qu'un profil est ouvert et de nouvelles règles sont disponibles pour la sélection. L'intégration CrowdStrike Next-Gen SIEM prend en charge plusieurs profils.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Si vous ne poursuivez pas à partir de la section précédente du processus de définition du profil de détection, accédez au profil que vous définissez.
   a. Accédez à la **Tous** > *CrowdStrike Next-Gen SIEM* > **Profil de détection**.
   b. Sélectionnez le profil que vous continuez à définir.
   c. Sélectionnez **Règles de corrélation** dans la barre de progression.
2. Décochez **la case Toutes les règles de corrélation sélectionnées** .
3. Dans le champ de recherche Liste de règles de corrélation, entrez le nom de la règle de corrélation créée dans le CrowdStrike portail.
4. Sélectionnez la règle de corrélation.
5. Utilisez la flèche vers la droite pour déplacer la **règle de Disponible** vers la colonne **Sélectionnée** .
6. Terminez cette section du processus de définition du profil de détection en sélectionnant **Continuer** .

Que faire ensuite

Mappez les champs de détection individuels CrowdStrike Next-Gen SIEM aux champs de l'incident ServiceNow AI Platform Réponse aux incidents de sécurité de sécurité. Pour plus d'informations, consultez Mapper les champs de détection.

Mapper les champs de détection

Mappez les champs de détection CrowdStrike Next-Gen individuels aux champs de l'incident SIR de sécurité afin de pouvoir créer des détections avec les données mappées.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sur la page de mappage, dans la section Mappage des champs de nouvelle génération de CrowdStrike, sélectionnez l'une des méthodes d'intégration d'échantillons.

Méthodes d'intégration des exemples

Champ	Description
Tous les champs de détection et d'événements par défaut	Utilisez cette méthode d'ingestion pour afficher la liste statique de toutes les détections et tous les champs d'événement. Cette méthode contient uniquement des noms de champs par défaut sans valeur. Vous pouvez utiliser ces informations pour mapper avec les SIR champs.
Récupérer les détections récentes	Utilisez cette méthode d'ingestion pour importer les données de détections et d'entités les plus récentes. Si la détection CrowdStrike Next-Gen contient plusieurs alertes, la première alerte qui fait partie de la détection est affichée dans la section de mappage. Lors de l'ingestion également, les premières valeurs de champ d'alerte de sécurité seront utilisées. Vous pouvez ingérer 5 détections d'échantillons. Les valeurs du champ de détection d'échantillon sont renseignées lorsque le profil ingère les détections d'échantillon. Vous pouvez mapper ces détections aux **champs cibles d'incidents SIR**. Les champs et les valeurs de détection apparaissent sous forme d'onglets individuels.

2. Pour ajouter des champs aux champs par défaut affichés dans l'incident de sécurité, procédez comme suit :

   a. Dans la section Champs cibles des incidents SIR, sélectionnez le Map another field Bouton Mapper un autre champ.
   Il affiche une liste de champs, à partir desquels SIR vous pouvez sélectionner un champ pour un nouveau champ à afficher.

   b. Dans la colonne Incident de sécurité, développez la liste qui s'affiche, puis sélectionnez un champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Plusieurs observables peuvent être affichés sur le même incident de sécurité. Par exemple, le champ **Observable** peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs **Élément de configuration** et **Notes de travail** prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, vous voyez un message d'erreur indiquant que ce champ ne prend pas en charge plusieurs valeurs. De même, si un champ d'un incident de sécurité comporte une liste dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste, le champ n'est pas renseigné sur l'incident de sécurité.

c. Dans la section Champs de détection et d'événement, faites glisser et déplacez votre champ pour le mapper à votre nouveau champ.

d. Lorsque vous cochez la case qui correspond à un champ, toute modification nouvelle ou mise à jour apportée dans CrowdStrike mettra automatiquement à jour les données d'incident SIR respectives avec les nouvelles données d'incident.

Remarque : Dans le système de base, la propriété système sn_sec_cs_ngsiem.detection_updates est définie par défaut sur False pour recevoir les mises à jour CrowdStrike Next-Gen relatives aux nouvelles alertes liées à SIR.

- Par défaut, les champs Utilisateurs affectés, Éléments de configuration et Observables sont cochés. Cela signifie que chaque fois que de nouveaux observables ou éléments de configuration associés, ou des utilisateurs affectés sont ajoutés à l'incident, ces informations sont automatiquement extraites et renseignées dans les listes connexes respectives dans Security Incident Response (SIR) au cours de cet intervalle d'interrogation.
- Pour tous les autres champs, vous devez cocher la case qui correspond à un champ pour toutes les modifications nouvelles ou mises à jour apportées à l'enregistrement de détection CrowdStrike dans CrowdStrike. Cela met automatiquement à jour les données d'incident SIR respectives avec les nouvelles données de détection.

Important : Une diligence raisonnable doit être effectuée avant de sélectionner cette fonctionnalité, car le remplacement des données existantes peut entraîner des données instables pour l'analyste et toute autre automatisation définie même par les valeurs de champ de l'incident de sécurité peut également être affectée. Il est donc très important de faire preuve de diligence raisonnable avant de sélectionner une fonctionnalité de remplacement.

3. Pour supprimer un champ, utilisez le ⊖ en regard du champ d'expression d'entrée dans la section Champs cibles de l'incident SIR.

4. Pour mapper une valeur de champ de la section Champs de détection et d'événement à un champ de la section Champs cibles de l'incident SIR, utilisez l'une des actions suivantes :

a. Faites glisser le nom du champ de détection (par exemple, ID) et déposez-le à côté d'un nom de champ dans la colonne Champs cibles de l'incident SIR.

Vous pouvez faire correspondre n'importe quelle valeur de la section Champs de détection et d'événement à un champ de la section Champs cibles de l'incident SIR. Les champs sont codés par couleur afin que vous ne les oubliiez pas ou ne les dupliquiez pas durant le processus de mappage. Les champs bleu clair indiquent qu'un champ de détection n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer des champs de détection entrante à plusieurs champs sur un incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

mappé à un champ de l'incident de sécurité. De cette façon, vous pouvez visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations d'incident importantes restantes restent non mappées.

b. Vous pouvez ajouter une combinaison de texte et de champ.
Par exemple, le nom de la détection est ${Detections : name}$. Ici, le nom de détection peut être saisi manuellement, tandis que ${Detections : name}$ est mappé à partir de la section Champs de détection et d'événement.

c. Vous pouvez saisir manuellement et mapper directement des champs de détection ou d'événements sources sur un champ cible.

- Pour mapper manuellement un champ de détection source, utilisez le format ${nom de champ}$. Par exemple, pour mapper la gravité d'un champ de détection, le format est ${Detections : severity}$.
- Pour ajouter manuellement des champs d'événements sources, utilisez le format ${events names : events fields}$. Par exemple, pour mapper un champ d'événements Description des événements Alerte de sécurité, le format est ${Events : description}$.

Cette intégration classe certains sous-types d'observables. Lorsque vous mappez un champ CrowdStrike Next-Gen avec le champ observable SIR, l'observable ServiceNow AI Platform classe automatiquement. Si vous souhaitez mapper de manière générique l'observable CrowdStrike Next-Gen entrant au type d'observable dans SIR, faites glisser et déplacez le champ Détection et événement dans le champ Observable. Toutefois, si vous connaissez le type d'observable pour l'observable CrowdStrike Next- Gen entrant dans SIR, effectuez un mappage spécifique au champ Type d'observable SIR . Voici quelques exemples de types SIR d'observables spécifiques dans : Observable (nom de domaine), Observable (adresse e-mail), Observable (adresse IP (V4)) et Observable (nom d'hôte).

Si vos champs CrowdStrike Next-Gen entrants contiennent des MITRE-ATT&CK informations, mappez-les MITRE-ATT&CK au champ Technique. Assurez-vous que le champ CrowdStrike Next- Gen entrant contient l'ID ou le nom de la MITRE-ATT&CK technique.

Parfois, les valeurs des champs de détection dans CrowdStrike Next-Gen peuvent ne pas être directement traduites dans les champs de l'incident de sécurité SIR. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques.

5. Pour formater la traduction d'un nouveau champ à partir d'une détection CrowdStrike Next-Gen afin qu'elle corresponde à une valeur de champ d'un incident de sécurité, sélectionnez le lien **Cliquez ici** dans l'en-tête des **champs cibles de l'incident SIR** .

6. Pour modifier les champs qui prennent en charge la traduction de champs, sélectionnez l'icône Traduction de champ du  de script de format.
Les champs qui prennent en charge la traduction des champs sont **Utilisateur affecté**, **Élément de configuration** et **Priorité**. Par exemple, cliquez sur l'icône du  à côté de la catégorie. L'éditeur de scripts CrowdStrike Next-Gen Field Translation s'ouvre.

7. Entrez les modifications apportées au script et sélectionnez **Mettre à jour** pour enregistrer les modifications et revenir à la page de mappage.
Par exemple, pour Catégorie, définissez les éléments suivants dans l'éditeur de script :

```
"<Incoming CrowdStrike Detection Field Value>" : "<Category to assign to the Security Incident>".
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce mappage garantit qu'un profil n'utilise que des catégories configurées.

8. Poursuivez votre mappage en ajoutant ou en supprimant des valeurs de champ.
   Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération de détection pour définir des critères supplémentaires qu'une détection entrante doit satisfaire pour créer un incident de sécurité.
9. Pour passer à la section Filtrage et agrégation, sélectionnez **Continuer**.

Que faire ensuite

Définissez et définissez des conditions de filtre afin de pouvoir spécifier quelles détections doivent provoquer des incidents de sécurité. Vous pouvez utiliser les mêmes valeurs de champ (définies dans la section Mappage) dans le générateur de conditions de génération de détection (dans la section Filtrage et agrégation) pour définir des critères supplémentaires qu'une détection entrante doit satisfaire pour créer un incident de sécurité.

Définir des critères de filtre et d'agrégation

Définissez et définissez des conditions de filtre pour spécifier quelles détections entrantes CrowdStrike Next-Gen SIEM doivent provoquer des incidents de sécurité. Vous pouvez également définir des critères de champ de détection supplémentaires qui permettent d'ajouter une détection entrante à un incident de sécurité ouvert au lieu de créer un incident.

Définir les conditions de filtrage

Définissez les conditions de filtrage afin que les incidents de sécurité ne soient créés que lorsque les conditions de filtrage correspondent.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Ce type de filtrage vous aide à isoler les incidents de sécurité et limite le nombre d'incidents de sécurité que vous créez. Si vous définissez des critères de filtrage supplémentaires, seules les détections requises sont ingérées sans avoir à modifier la requête ou la configuration de détection déclenchée.

Procédure

1. Pour définir les critères qu'une détection CrowdStrike Next-Gen entrante doit satisfaire pour qu'un incident de sécurité soit créé, sélectionnez **Filtre basé sur les conditions**.

   Les options du premier champ des Conditions de filtre correspondent aux champs affichés dans la section Ingestion de détection d'échantillons de CrowdStrike Next-Gen pour la détection que vous avez ingérée. Ces champs sont dynamiques et changent en fonction de la détection que vous ingérez. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de la détection.

   Utilisez la `detection_id` de condition de filtre pour les champs suivants à valeurs multiples :

   - composite_id
   - host_names
   - seconds_to_resolved
   - seconds_to_triaged

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étant donné que la condition de filtre ne peut récupérer que des chaînes, vous devez utiliser la condition de filtre *detection_id* pour les champs ci-dessus afin de vous assurer que les données sont filtrées correctement.

2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres pour la première ligne.
3. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.

Définir les conditions d'agrégation

Définissez des critères d'agrégation d'incidents supplémentaires qui regroupent une détection entrante à un incident de sécurité SIR existant au lieu de créer des détections similaires potentiellement en double. Lorsque vous utilisez des critères de valeur de correspondance de champ pour chaque profil, cette agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données de détection connexes sur un seul incident de sécurité.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Si un nouvel incident correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, l'incident est automatiquement ajouté à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.ingestion_profile_admin travaillant sur des incidents de sécurité, vous pouvez afficher tous les incidents agrégés ajoutés sur une liste connexe d'un incident de sécurité.

Tous les incidents agrégés relatifs à un incident de sécurité sont affichés dans la CrowdStrike Next-Gen SIEM liste connexe des incidents agrégés. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi des incidents s'ajoutent aux incidents de sécurité existants.

Procédure

1. Pour définir des critères de champ d'incident supplémentaires qui permettent d'ajouter une détection entrante CrowdStrike Next-Gen SIEM à un incident de sécurité ouvert au lieu de créer un nouvel incident, sélectionnez l'option **Conditions d'agrégation** , comme illustré dans la figure suivante.
2. Dans le champ **Champs d'incidents avec valeurs correspondantes** , saisissez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre ServiceNow AI Platform instance.
   Toutes les valeurs de champ que vous avez sélectionnées dans le champ d'entrée de sélection multiple doivent correspondre afin que les critères d'agrégation soient remplis et que cet incident entrant puisse être ajouté à un incident de sécurité existant. Cette sélection implique qu'il s'agit d'une condition *ET* dans laquelle des champs, tels que des observables et des éléments de configuration qui peuvent avoir plusieurs valeurs de champ, leur sont mappés. Si seul un sous-ensemble de valeurs correspond, les conditions d'agrégation d'incidents CrowdStrike Next-Gen SIEM ne sont pas remplies et un nouvel incident de sécurité est créé.
3. Pour ajouter plusieurs conditions de correspondance de champ, cliquez sur **Ajouter un nouveau critère**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’agrégation se produit si l’une des conditions de champ de sélection multiple que vous définissez est remplie. Cette sélection implique la condition *OU* .

4. Pour mettre à jour la note de travail d’un nouvel incident lorsqu’elle est ajoutée à un incident de sécurité, sélectionnez **Enregistrer la note de travail pour le nouvel incident**.

   La note de travail indique qu’un nouvel incident est ajouté et comprend un lien vers les détails de l’incident. La note de travail du journal met également à jour d’autres détails que vous ajoutez au champ note de travail dans votre section de mappage.

5. Pour configurer le calendrier, cliquez sur **Continuer**.

Que faire ensuite

Définissez un calendrier pour récupérer les données d’incident et les incidents ingérés qui correspondent aux critères du profil.

Planifier la récupération de détection

Configurez un calendrier pour définir comment et quand extraire les détections du CrowdStrike Next-Gen SIEM locataire.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Si vous ne poursuivez pas à partir de la section précédente des critères de filtrage et d’agrégation, accédez au profil que vous définissez.
   a. Accédez à la **Tous** > *CrowdStrike Next-Gen SIEM* > **Profil de détection**.
   b. Sélectionnez le profil que vous continuez à définir.
   c. Sélectionnez **Planification** dans la barre de progression.
2. Renseignez les champs du formulaire de planification.

CrowdStrike Next-Gen SIEM Formulaire de planification

Champ	Description
Ingestion de détection en cours	Option permettant de définir l’ingestion de détection continue que l’instance ServiceNow AI Platform extrait du locataire pour les CrowdStrike Next-Gen SIEM nouvelles détections. Les incidents de sécurité sont créés si des détections déclenchées sont trouvées et que les critères de filtrage de génération de détection correspondent.
Incrémentation du sondage (minutes)	Fréquence d’interrogation définie en minutes.
Définir le temps d’ingestion de détection	Option permettant d’ajouter la date et l’heure de l’ingestion initiale.
Délai d’ingestion de la détection initiale	Date et heure que vous spécifiez pour l’ingestion de détection.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Récupération ponctuelle	Option permettant d'activer la récupération ponctuelle des détections historiques CrowdStrike Next-Gen SIEM , suivie du rapprochement des données. Lors du traitement des données, les détections en cours et les données historiques sont extraites. **Remarque :** Les détections historiques CrowdStrike Next-Gen SIEM récupérées subissent des contrôles de déduplication pour éviter tout doublon au sein de l'application Réponse aux incidents de sécurité .
Depuis date	Date depuis que les détections historiques ont été ingérées à partir de CrowdStrike Next-Gen SIEM.

3. Terminez cette section du profil en sélectionnant **Continuer**.

Que faire ensuite

Automatiser les mises à jour et les fermetures de détection

Automatiser les mises à jour et les fermetures de détection

Automatisez les mises à jour et les fermetures de détection en fonction de l'état de l'incident Réponse aux incidents de sécurité . L'intégration CrowdStrike Next-Gen SIEM permet aux détections de créer des incidents de sécurité et de mettre à jour les incidents une fois qu'ils ont été créés ou fermés.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Si vous ne poursuivez pas à partir de la section précédente du processus de planification, accédez au profil que vous définissez.
   a. Accédez à la **Tous** > *CrowdStrike Next-Gen SIEM* > **Profil de détection**.
   b. Sélectionnez le profil que vous continuez à définir.
   c. Sélectionnez **Options supplémentaires** dans la barre de progression.
2. Remplissez les champs du formulaire.

Automatisation du formulaire de mises à jour de détection

Catégorie	Champ	Description
Mises à jour de création d'incidents de sécurité	Mettre à jour l'état de détection de CrowdStrike Next-Gen lors de la création de l'incident SIR	Option permettant d'utiliser la fonctionnalité de mise à jour de détection automatisée. L'état CrowdStrike Next-Gen SIEM de détection est mis à jour dans CrowdStrike Next-Gen SIEM la détection

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catégorie	Champ	Description
		avec les commentaires après la création de l'incident SIR dans le ServiceNow AI Platform.
	Mise à jour de l'état de détection initiale	État de détection initial qui est mis à jour dans l'environnement CrowdStrike Next-Gen SIEM , soit Nouveau soit En cours.
	Commentaires initiaux renvoyés à la détection	Commentaires initiaux publiés sur la détection dans l'environnement CrowdStrike Next-Gen SIEM .
Mises à jour des fermetures de détection	Fermer la détection CrowdStrike Next-Gen lors de la fermeture de l'incident SIR	Option permettant d'utiliser la fonctionnalité de mise à jour de l'état de détection automatisée. CrowdStrike Next-Gen SIEM Les détections sont fermées dans le CrowdStrike Next-Gen SIEM portail avec les commentaires donnés après la fermeture de l'incident SIR dans le ServiceNow AI Platform.
	Mise à jour de l'état de détection de fermeture	Mise à jour du statut dans la CrowdStrike Next-Gen SIEM détection lorsque l'incident de sécurité est fermé dans SIR.
	Commentaires de fermeture renvoyés à la détection	Commentaires publiés sur la détection dans la CrowdStrike Next-Gen SIEM détection lorsque l'incident de sécurité est fermé dans SIR.
Transmettre par pull les détections fermées	Transmettre par pull les détections fermées	Option permettant d'extraire les détections fermées pendant l'ingestion en cours et la récupération ponctuelle. Les incidents fermés SIR ne seront pas mis à jour avec les nouvelles données de CrowdStrike Next-Gen SIEM
Synchronisation des commentaires de détection et des notes de travail SIR	Mettre à jour l'activité d'automatisation SIR avec les commentaires de détection CrowdStrike Next-Gen	Option permettant de mettre à jour vos CrowdStrike Next-Gen SIEM commentaires dans l'activité d'automatisation SIR . Le commentaire dans l'activité d'automatisation SIR apparaît avec le préfixe `Commentaire de CrowdStrike`.
	Mettre à jour CrowdStrike Next-Gen SIEM les commentaires de détection avec les notes de travail SIR	Option permettant de mettre à jour vos SIR notes de travail dans les commentaires de CrowdStrike Next-Gen SIEM détection. Le commentaire apparaît CrowdStrike Next-Gen SIEM avec le préfixe `Commentaire de ServiceNow`.

3. Sélectionnez **Finish** (Terminer).
4. Activez le profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sélectionnez la section **Nom** de la barre de progression.

b. Sélectionnez la case à cocher **Activé**.

c. Sélectionnez **Continuer**.

Intégration de CrowdStrike Falcon X Sandbox pour Security Operations

Avec l'intégration de Opérations de sécurité forCrowdStrike Falcon X Sandbox, vous pouvez soumettre des fichiers et des URL dans le cadre du processus de réponse aux incidents de sécurité afin CrowdStrike Falcon X Sandbox d'effectuer une analyse détaillée des programmes malveillants et des menaces.

L'intégration CrowdStrike Falcon X Sandbox vous fournit un environnement virtuel isolé à la demande où vous pouvez effectuer l'analyse des programmes malveillants et fournir des résultats à l'incident ServiceNow de sécurité via l'intégration.

Lorsque vous soumettez vos incidents de programme malveillant, ils sont conservés dans le cadre de l'enregistrement de l'incident de sécurité. Vous pouvez utiliser ces enregistrements pourpoursuivre la résolution des incidents et automatiser la soumission de fichiers et d'URL.

L'intégration prend en charge l'automatisation des playbooks de réponse au phishing et aux programmes malveillants, ce qui permet au personnel de votre Opérations de sécurité centre d'être plus productif et efficace dans la réponse aux incidents de sécurité.

Avantages clés

Avec cette intégration, vous pouvez effectuer les opérations suivantes :

- Automatisez la soumission de fichiers et d'URL provenant d'un hameçonnage signalé par un utilisateur (URP), d'e-mails, de pièces jointes et d'autres incidents de sécurité.
- Soumettez manuellement ou soumettez à nouveau les fichiers et URL précédemment analysés pour une analyse mise à jour.
- Créez plusieurs configurations de soumission qui appliquent CrowdStrike Falcon X Sandbox automatiquement des paramètres de soumission tels que le système d'exploitation, le type d'analyse et les options d'exécution.
- Analysez les résultats de logiciels malveillants et de menaces dans un rapport au format HTML au sein de l'incidentSIR. Vous pouvez afficher les résultats de la recherche et l'historique des indicateurs pour les fichiers et les URL qui ont été analysés plusieurs fois.
- Balisez ServiceNow les incidents avec l'état de traitement de la soumission, ainsi que les résultats de recherche de menace.

Voir aussi

Identificateur de document	Titre de document
CrowdStrike Falcon X Sandbox	CrowdStrike Falcon Sandbox FAQ
ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise en route de l'intégration CrowdStrike Falcon X Sandbox

Activez et configurez l'interface avec votre CrowdStrike Falcon X Sandbox instance et Réponse aux incidents de sécurité votre ServiceNow produit.

Avant de commencer

- Avant de pouvoir utiliser pour l'intégration CrowdStrike Falcon X Sandbox de Security Operations, vous devez la télécharger à partir du ServiceNow Store.
- Passez en revue la liste de vérification de configuration suivante et vérifiez que vous avez terminé toutes les tâches pour une intégration fluide CrowdStrike Falcon X Sandbox .

Rôle requis : admin, sn_si.admin

Liste de vérification

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles et requis ServiceNow AI PlatformRéponse aux incidents de sécurité .	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • L'administrateur installe l'intégration sandbox à partir de l'App Store ServiceNow et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Le sn_si.admin crée et modifie la configuration et les paramètres globaux, puis affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). • L'analyste des incidents de sécurité (sn_si.analyst) répond aux incidents de sécurité, tels que l'envoi de fichiers et d'URL au sandboxet l'analyse des résultats de soumission.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.	Cette intégration est prise en charge sur Paris et Orlando dans les versions. Assurez-vous que ces modules d'extension dépendants sont installés. Ces modules d'extension permettent l'exécution d'actions et de Centre d'intégration flux : • ServiceNow Étape d'action du Centre d'intégration : REST (com.glide.hub.action_step.rest) • ServiceNow Moteur d'exécution du Centre d'intégration (com.glide.hub.integration.runtime)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	Remarque : Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au ServiceNow personnel. Pour demander un module d'extension, suivez les étapes présentées dans Demander un module d'extension . Le Réponse aux incidents de sécurité module d'extension (com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Réponse aux incidents de sécurité Dépendance (com.snc.si_dep) **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Orchestration du support de sécurité **5.** Renseignements sur les menaces Support commun (requis pour vouspermettre d'intégrer le bac à sable) **6.** Trusted Security Circles **7.** Opérations de sécurité Assistant de configuration **8.** Réponse aux incidents de sécurité Pour plus d'informations sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une application Security Operations et Activer une application ServiceNow Store.
Vérifiez que vous disposez de la licence pour la clé API privée Falcon Sandbox et	Cette intégration prend uniquement en charge le cloud privé Falcon Sandbox.

Traduction automatique

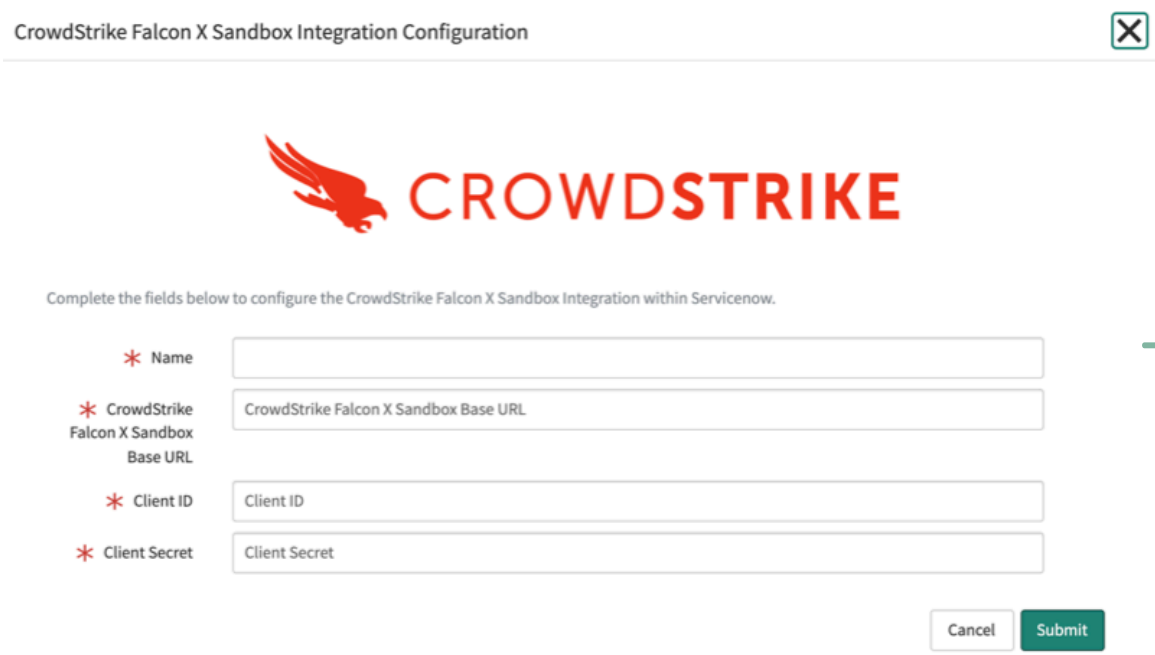
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
que vous conservez la CrowdStrike Falcon X Sandbox clé API complète.	**Remarque :** Cette version ne prend pas en charge l'intégration de Falcon X. CrowdStrike Falcon X Sandbox offre une clé API restreinte auto-signée et une clé API complète mise à niveau. Utilisez la clé API complète pour cette intégration , car elle permet un accès illimité pour les soumissions automatisées. Pour plus d'informations, consultez la base de connaissances CrowdStrike Falcon Sandbox .

Procédure

1. Téléchargez l'intégration de CrowdStrike Falcon Sandbox pour Security Operations à partir du ServiceNow Store.
2. Une fois l'installation terminée, naviguez vers **Intégrations > opérations de sécurité** > **Configurations d'intégration.**
3. Recherchez la vignette d'intégration CrowdStrike Falcon X Sandbox , puis cliquez sur **Configurer**.



4. Entrez les détails suivants pour terminer la configuration :

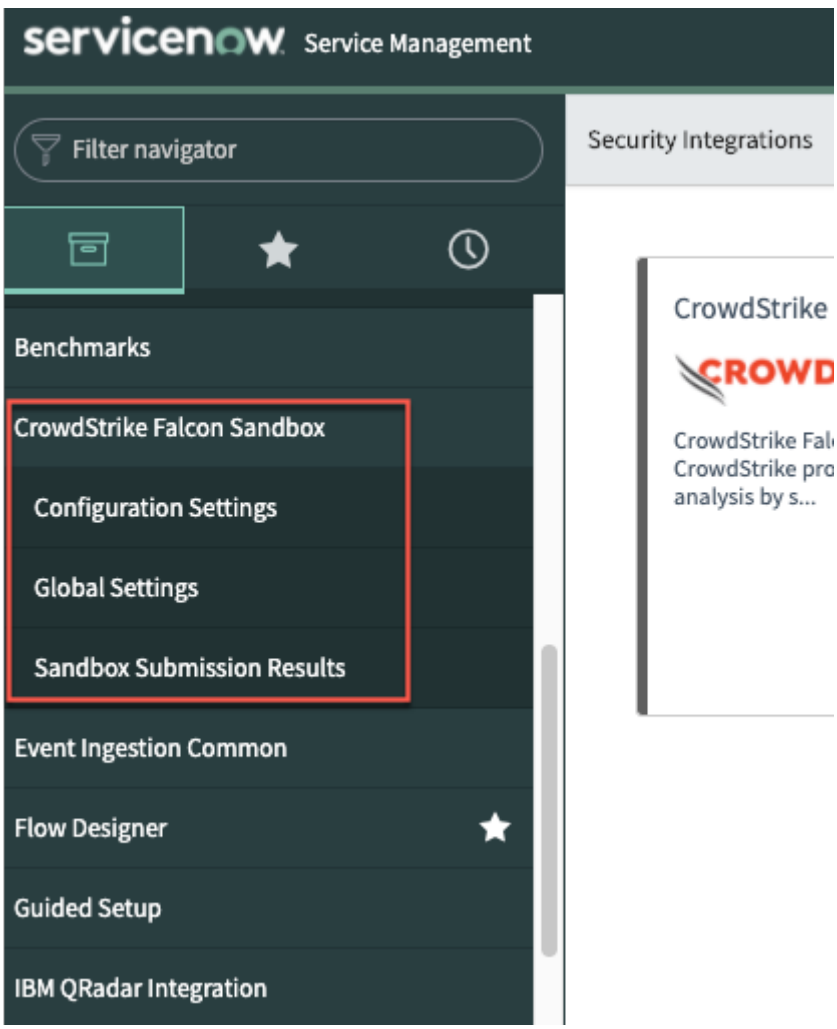
Champ	Description
Nom	Nom de cette intégration, par exemple `demo-1`. Bien qu'il s'agisse d'un nom unique pour identifier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	la configuration sandbox, vous ne pouvez configurer qu'une seule intégration par instance ServiceNow.
CrowdStrike Falcon Sandbox Base URL	URL de base Sandbox. Cette URL est disponible après avoir configuré le sand box.Par exemple, https:// servicenow.falcon-sandbox.com est une URL de base.
ID client	ID client de l'API OAuth2. Pour plus d'informations, consultez Clients et clés API .
Secret client	Clé secrète du client de l'API OAuth2. Pour plus d'informations, consultez Clients et clés API .

5. Cliquez sur **Envoyer**.
   Une fois le bac à sable validé et soumis, il est enregistré sur la page Intégrations de sécurité sous forme de tuile. Vous pouvez maintenant afficher le module Sandbox dans le navigateur d'application.



Que faire ensuite

Une fois l'intégration terminée, l'étape suivante consiste à configurer les configurations de soumission du bac à sable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les configurations de soumission à Sandbox

Configurez la configuration Sandbox pour définir l'environnement d'analyse et les options d'exécution de vos soumissions d'enregistrements d'incidents de sécurité pour l'analyse de programme malveillant.

Avant de commencer

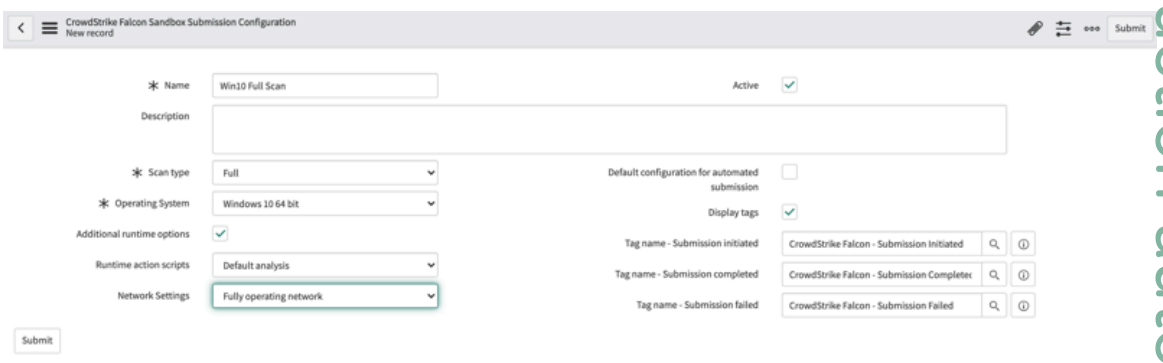
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Avant de pouvoir soumettre des fichiers ou des URL à l'aide de CrowdStrike Falcon X Sandbox l'intégration, vous devez configurer au moins une configuration de soumission. La configuration de la soumission définit le système d'exploitation Sandbox, le type d'analyse, les options de temps d'exécution et d'autres caractéristiques de gestion des incidents. Vous pouvez créer plusieurs configurations pour utiliser les différentes options disponibles dans l'environnementCrowdStrike Falcon X Sandbox.

Procédure

1. Accédez à la **Tous** > **Bac à sable de CrowdStrike Falcon X** > **Paramètres de configuration**.
2. Cliquez sur **Nouveau**.



3. Renseignez les champs suivants pour créer une configuration pour un **type d'analyse** complète.

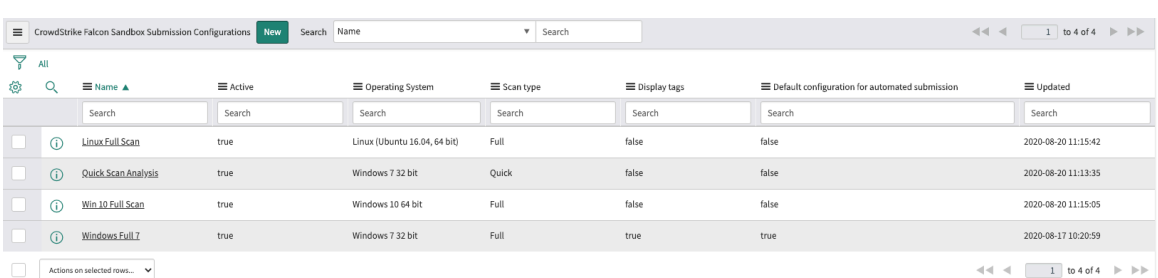
Champ	Description
Nom	Nom unique pour la configuration de la soumission. Ce nom apparaît aux analystes lorsqu'ils soumettent un fichier. Il est important de s'assurer que le nom est descriptif et facilement distinguable des autres configurations (exemple, Win 10 Full Scan). Si le nom n'est pas unique, une erreur s'affiche et les noms d'enregistrements de configuration en double ne sont pas enregistrés.
Type d'analyse	Speut taper **Complet**. Un type d'analyse **rapide** fournit une analyse limitée des menaces.
Système d'exploitation	Environnementd'ordinateur virtuel nalysis dans lequel le sand box analyse le fichier ou l'URL.
Actif	Option que vous sélectionnez lors de l'envoi manuel de fichiers ou d'URL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Configuration par défaut pour la soumission automatisée	Opération qui est effacée par défaut. La sélection de cette option permet à cette configuration d'être disponible pour automatiser les soumissions d'analyses de programmes malveillants. **Remarque :** Vous ne pouvez avoir qu'une seule configuration de soumission active comme configuration par défaut pour les soumissions automatisées.
Balises d'affichage	Opération qui est effacée par défaut. Lorsque vous sélectionnez cette option, des balises s'affichent pour indiquer l'état d'un fichier ou d'une soumission d'URL. Le traitement de l'analyse peut prendre plusieurs minutes. Les balises d'affichage sont soumission initiée, soumission terminée ou soumission échouée.
Options Runtime supplémentaires	Opération qui est effacée par défaut. Lorsque vous sélectionnez cette option, des paramètres d'exécution supplémentaires pris en charge par Sandbox sont disponibles.
Scripts d'action Runtime	Option qui vous permet d'utiliser un script qui simule le comportement humain et interagit avec le fichier ou l'URL pendant l'analyse. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ Voir la CrowdStrike Falcon X Sandbox documentation pour plus de détails.
Paramètres réseau	Option qui vous permet de sélectionner le type de paramètres réseau utilisés lors de la soumission d'une URL ou d'un fichier à Sandbox.

4. Cliquez sur **Envoyer**.
   Une fois que vous avez envoyé la configuration, elle est enregistrée sur la page Paramètres de configuration en tant qu'enregistrement. La configuration doit être **active** pour être utilisée dans les soumissions des andbox.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Une fois que vous avez configuré les soumissions sandbox, l'étape suivante consiste à soumettre manuellement des fichiers ou des ULR à Sandbox

.

Soumettre manuellement des fichiers ou des URL au bac à sable

Vous pouvez soumettre manuellement un fichier ou une URL à un bac à sable lorsque certains critères d'incident, tels que la catégorie est hameçonnage, sont remplis.

Avant de commencer

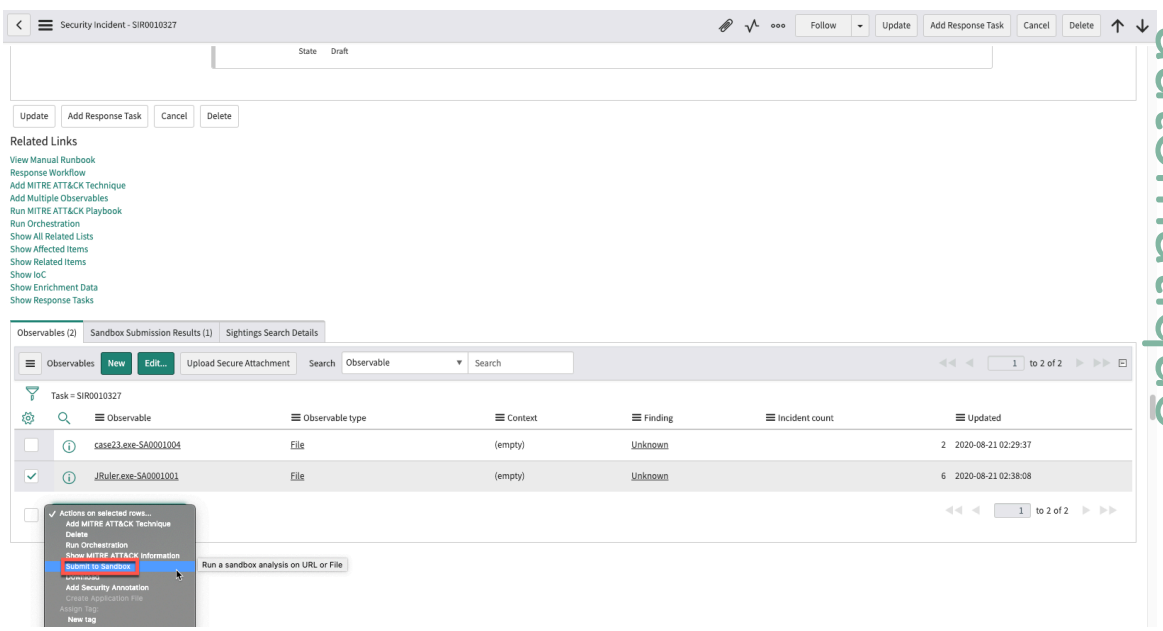
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Après avoir examiné l'incident de sécurité et le fichier ou l'URL, vous pouvez sélectionner l'option **Soumettre au bac à sable (sandbox**) pour effectuer une analyse de programme malveillant.

Procédure

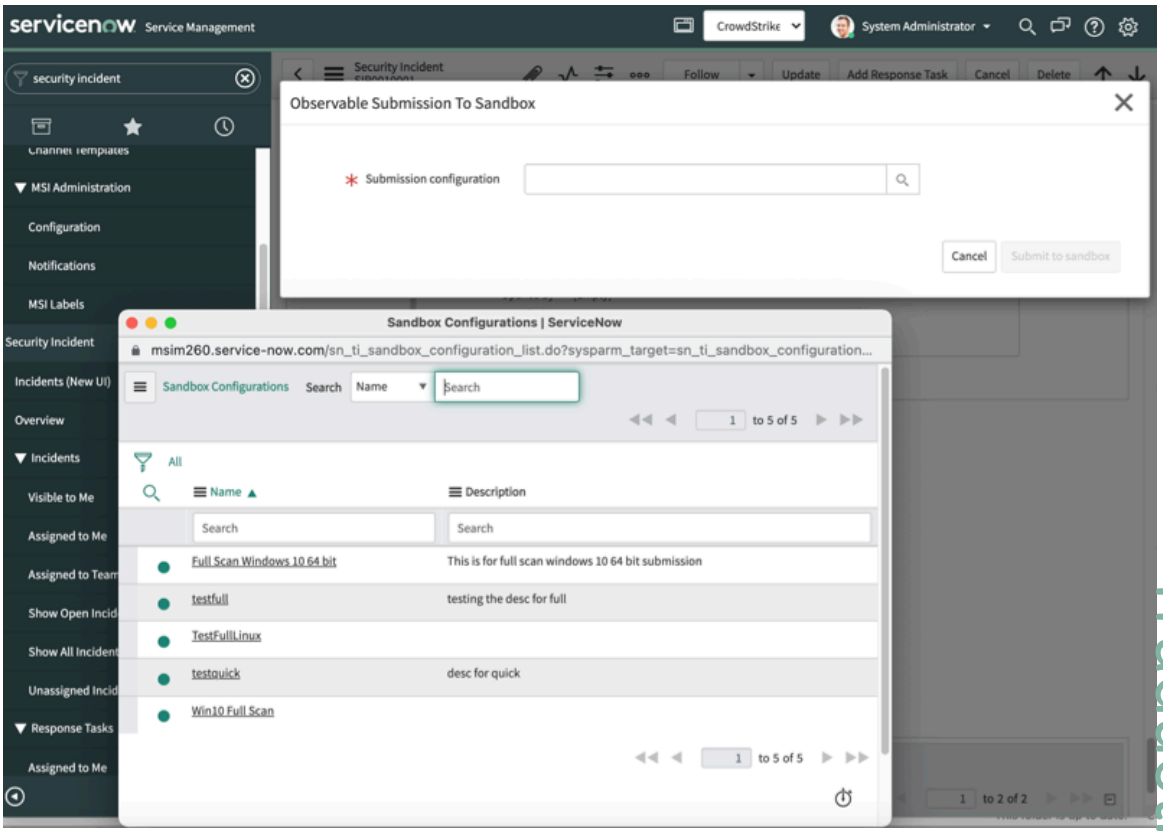
1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents** et ouvrez un incident de sécurité auquel vous souhaitez soumettre un enregistrement de type observable de fichier ou d'URL.
2. Cliquez sur le lien connexe **Afficher l'IoC** .
3. Sous l'onglet **Observables** , sélectionnez un ou plusieurs enregistrements pour lesquels vous souhaitez effectuer une analyse des menaces ou des programmes malveillants, puis cliquez sur **Soumettre au bac à sable**.



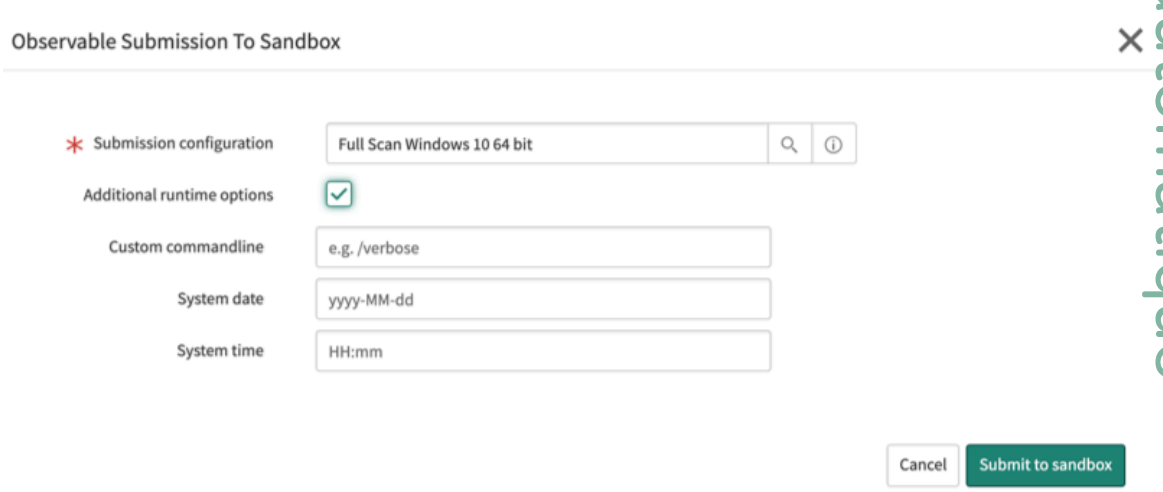
4. Lorsque le filtre Soumission de fichier apparaît, sélectionnez votre configuration de bac à sable préférée dans **Configuration de soumission**, puis cliquez sur **Soumettre au bac à sable**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. **Facultatif :** Sélectionnez **Options d'exécution supplémentaires** si vous souhaitez fournir d'autres options personnalisées.



Champ	Description
Ligne de commande personnalisée	Ligne de commande d'application normale ou opération spéciale.
Date du système	Date du système au format aaaa-MM-jj.
Heure du système	Heure du système au format HH :mm.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que vous avez initié la soumission, vous pouvez afficher les notes de travail pour voir l'état de votre soumission. Pour plus d'informations sur l'état de la soumission ou pour analyser les résultats, consultez les résultats de soumission de **Sandbox**.

Remarque : Dans CrowdStrike Falcon X Sandbox, l'analyse rapide n'est pas prise en charge pour les URL. Si les notes de travail contiennent trop d'informations, vous pouvez utiliser l'option Filtre pour explorer les notes de travail requises qui vous intéressent.

Que faire ensuite

Lorsque vous soumettez les observables au bac à sable pour analyse de programme malveillant, affichez les résultats de soumission du bac à sable pour prendre les mesures suivantes concernant les menaces potentielles.

Automatiser les CrowdStrike soumissions Falcon Sandbox à l'aide de Concepteur de flux

L'intégration CrowdStrike Falcon X Sandbox inclut des modèles de flux créés à l'aide de Concepteur de flux qui fonctionnent avec les enregistrements d'incidents de sécurité.

Avant de commencer

- Vérifiez que vous avez créé une configuration de soumission Sandbox et que vous avez activé une configuration comme **configuration par défaut pour la soumission automatisée**. Lorsque le flux est déclenché, la soumission du bac à sable se produit sur votre configuration par défaut.

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Ces flux sont principalement conçus pour vous aider à automatiser les soumissions de fichiers ou d'URL dans le cadre de votre workflow de réponse aux incidents.

Lorsque vous activez un exemple de flux, vos pièces jointes de fichier d'hameçonnage sont automatiquement envoyées si vous définissez les incidents de sécurité comme étant de l'hameçonnage dans votre échantillon de flux. Vous pouvez également soumettre tous les fichiers .exe lorsque ce type de fichier est joint à un enregistrement observable.

Vous pouvez modifier ces exemples de flux pour déclencher une soumission automatisée dans différentes conditions, catégories, conditions composées, etc.

L'intégration sandbox se compose de deux flux système de base qui sont désactivés par défaut.

- **Soumettre un fichier lorsque la catégorie est Hameçonnage** : ce flux soumet un fichier au bac à sable pour analyse de programme malveillant lorsque la catégorie d'incident de sécurité est définie comme Hameçonnage. Vous devez joindre un fichier à l'enregistrement observable sur l'incident de sécurité. Si vous utilisez la fonctionnalité User Reported Phishing (URP), toute pièce jointe d'e-mail est automatiquement analysée et ajoutée à l'enregistrement d'incident SIR en tant qu'enregistrement observable. Aucune autre action n'est requise pour automatiser la soumission.
- **Soumettre lorsque le type de fichier de l'observable est exe** : ce flux soumet un fichier au bac à sable pour analyse de programme malveillant lorsque l'observable d'incident de sécurité est un exe. Comme pour le flux de catégorie d'hameçonnage, vous devez joindre un fichier à un enregistrement observable sur l'incident de sécurité. Vous pouvez le faire manuellement en téléchargeant le fichier ou automatiquement si une pièce jointe d'e-mail d'hameçonnage ou tout autre mécanisme à l'origine de l'incident est associé aux enregistrements observables.

Lorsque les flux sont configurés et que les conditions de l'incident satisfont les paramètres, les soumissions de bac à sable se déclenchent automatiquement lorsque vous examinez l'incident de sécurité. Passez en revue la note de travail qui indique qu'une soumission

Traduction automatique

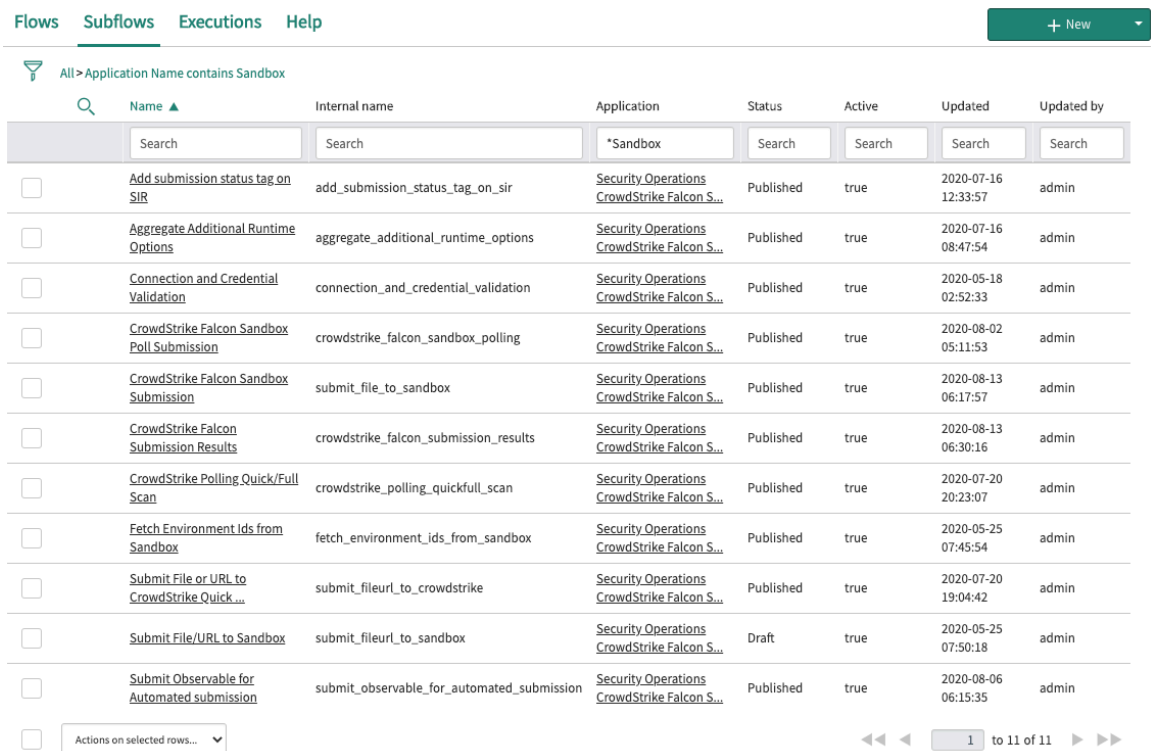
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a été initiée, qu'une balise s'affiche si elle est activée dans la configuration et qu'un enregistrement des résultats de soumission est en attente.

L'intégration de bac à sable contient également plusieurs flux secondaires. Les flux secondaires sont des composants internes des options de soumission de l'intégration globales. Vous pouvez personnaliser et modifier les flux secondaires en fonction de vos critères de sécurité.

Vous pouvez consulter les flux secondaires pour résoudre les problèmes liés aux soumissions de bac à sable. Un enregistrement d'exécution est créé chaque fois que vous appelez un flux secondaire. Cet enregistrement indique où une erreur particulière s'est produite dans le flux et vous permet de résoudre le problème.

Intégration Sandbox : plusieurs workflows



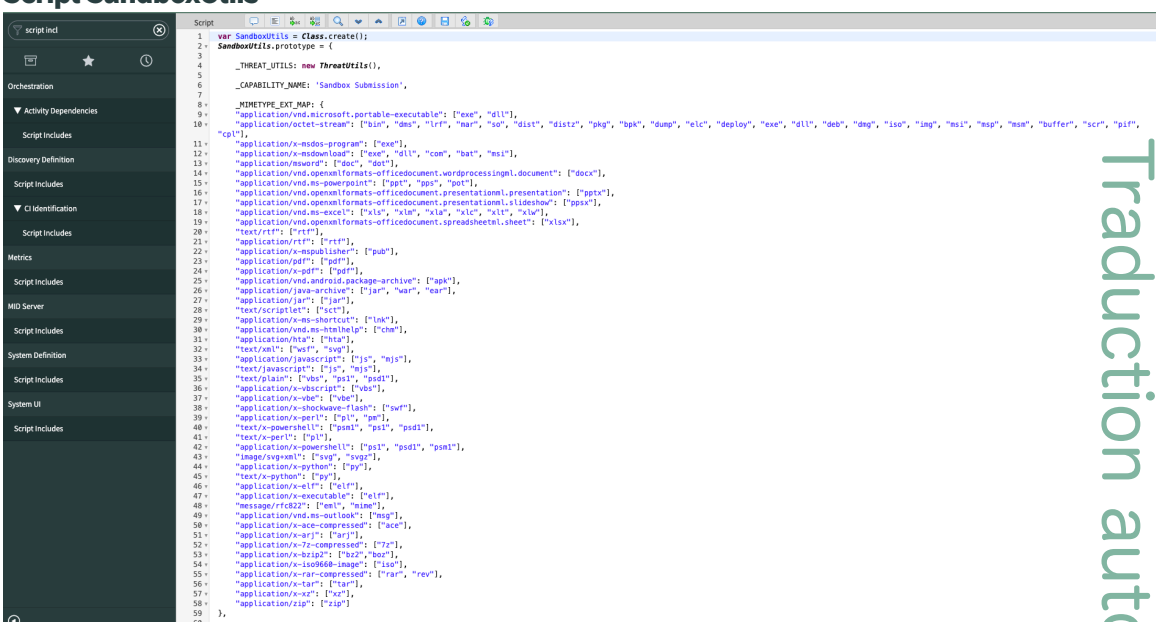
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

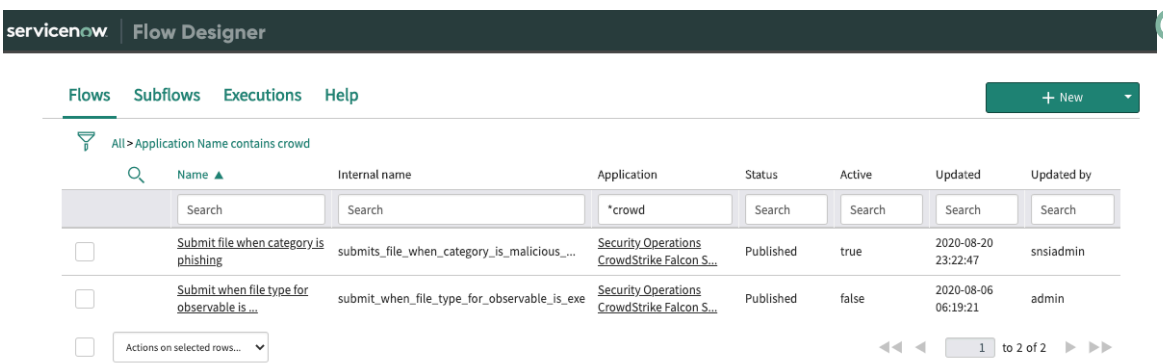
- Si vous choisissez de personnaliser les flux par défaut, vous devez vérifier que le flux secondaire Soumettre l'observable pour soumission automatisée est inclus dans votre flux pour déclencher les soumissions automatiques.
- Vous pouvez personnaliser et définir vos extensions de fichier pour un exe. Créer une copie du flux **Soumettre lorsque le type de fichier de l'observable est exe** et apporter des changements à la copie. Le type de contenu et les extensions de fichier sont mappés dans le script SandboxUtils . Pour accéder aux includes de script, naviguez vers **Définitions du système > Includes de script** et recherchez SandboxUtils.

Script SandboxUtils



Procédure

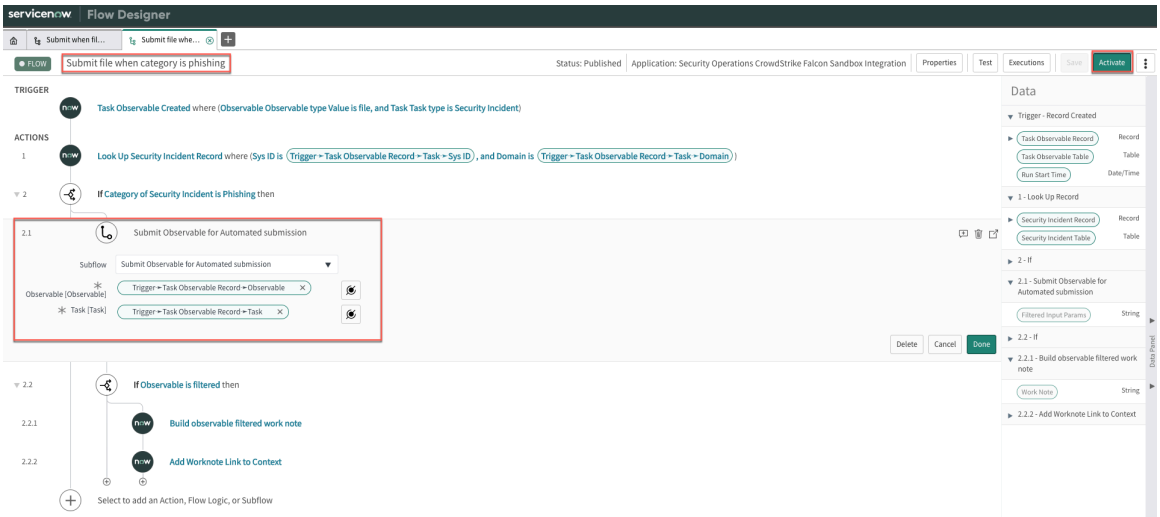
1. Accédez à la **Tous** > **Concepteur de flux** > **Concepteur** > **Flux**.
2. Filtrez les flux par type **d'application** .
   Par exemple, *crowd filtre les deux CrowdStrike Falcon X Sandbox flux.



3. Sélectionnez un flux pour en afficher les détails.
   L'exemple ci-dessous montre la catégorie Soumettre le fichier lorsque la catégorie est flux d'hameçonnage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Activer** , puis sur **OK** lorsque le message de confirmation s'affiche.

Que faire ensuite

Après avoir configuré les flux de soumission automatisés, vous pouvez afficher les résultats de soumission du bac à sable pour analyser les menaces.

Surveiller les résultats de soumission dans le bac à sable

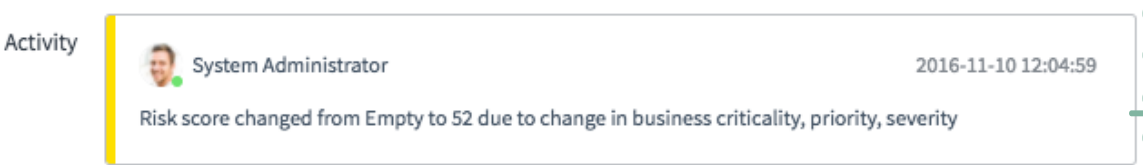
Les résultats de toutes les soumissions de Sandbox sont affichés dans l'onglet **Résultats de soumission Sandbox** pour chaque incident de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

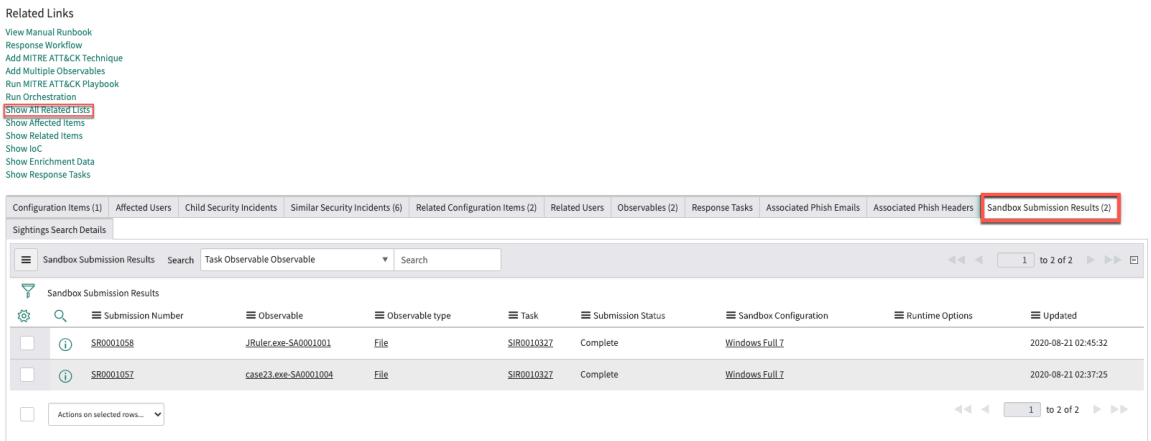
1. Ouvrez l'incident de sécurité avec lequel vous travaillez et vérifiez que l'envoi de S and Box est réussi.



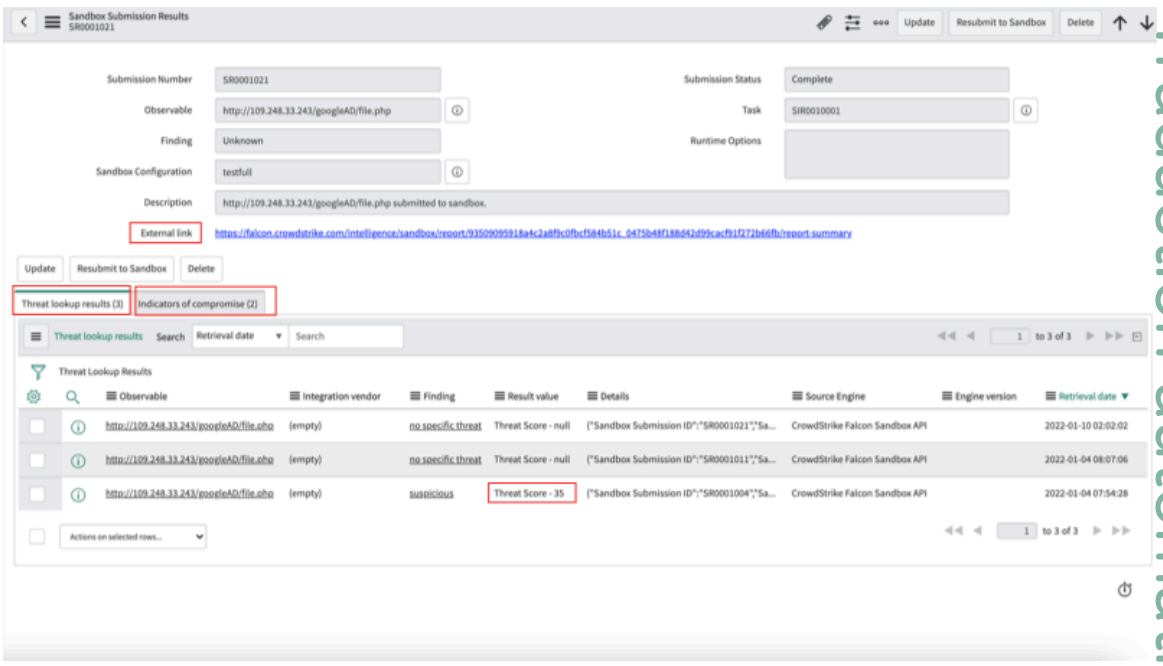
2. Passez en revue les notes sur les Work pour plus d'informations et découvrez comment procéder si vous ne pouvez pas vérifier que le scan est réussi.
3. Cliquez sur le lien Résultats complets dans les notes de sécurité ou, au bas de l'incident de sécurité, accédez à **Afficher toutes les listes connexes**> **Résultats de soumission du bac à sable**.
   Les résultats sont affichés dans l'onglet Résultats de soumission du bac à sable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur ouvrir n'importe quel enregistrement pour afficher l'analyse complète dela boîte de commande.



5. Facultatif : Cliquez sur **Soumettre à nouveau au bac à sable** pour traiter à nouveau l'observable.

Résultats

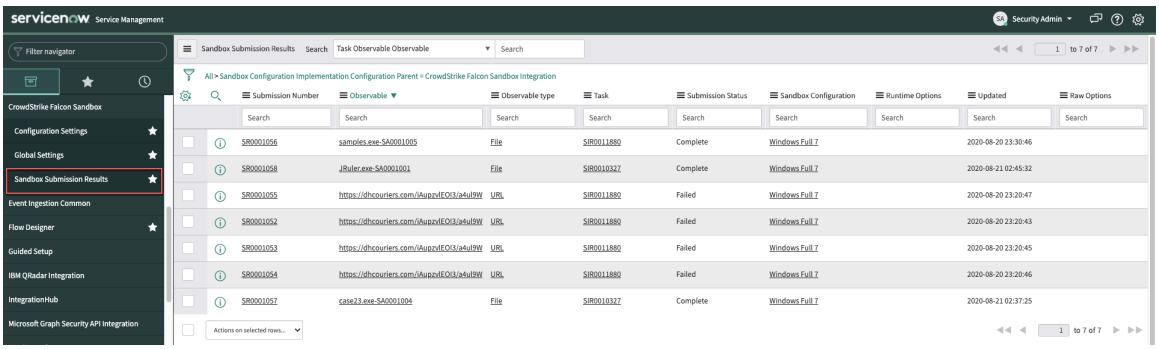
- **L'onglet Résultats de la recherche de menaces fournit l'évaluation** de la menace, y compris les résultats malveillants, les scores de menace et des détails supplémentaires. Cesdétails sont fournis dans la structure de format de recherche de menaces standard pour toutes les ServiceNow intégrations de recherche de menaces.
- L'onglet **Indicateurs de compromission** fournit les résultats s and box malveillantsou suspects avec les scores de confiance. Les scores de confiance sont similaires aux autres informations d'indicateur stockées dans la ServiceNow plateforme. Les indicateurs classifiés comme informatifs ne sont pas inclus dans cet onglet.
- Cliquez sur le **lien externe** pour afficher les résultats du bac à sable dans le CrowdStrike Falcon X Sandbox portail.

> **Remarque :** Pour procéder à cette option, vous devez disposer du CrowdStrike Falcon X Sandbox rôle afin d'afficher les résultats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez également surveiller les résultats de soumission dela boîte de commande pour tous les incidents de sécurité en accédant à **CrowdStrike Falcon Sandbox** > **Résultats de soumission du bac à sable**.



Baliser les incidents de sécurité avec l'état de soumission du bac à sable

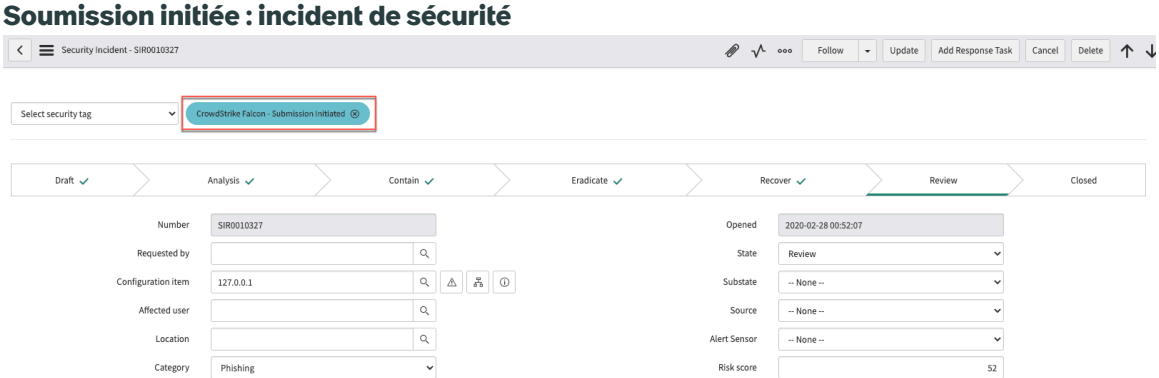
Vous pouvez éventuellement baliser les incidents de sécurité avec les balises Soumission initiée et Soumission terminée.

Lorsque vous sélectionnez l'option **Afficher les balises** dans la configuration de soumission de Sandbox, des balises s'affichent pour indiquer l'état d'un fichier ou d'une soumission d'URL. Cette vérification de l'état est utile car le traitement de l'analyse sand box peut prendre plusieurs minutes.

Les balises d'affichage sont appelées soumission initiée, soumission terminée et soumission échouée.

L'exemple suivant montre un incident de sécurité où la soumission a été initiée.

Soumission initiée : incident de sécurité

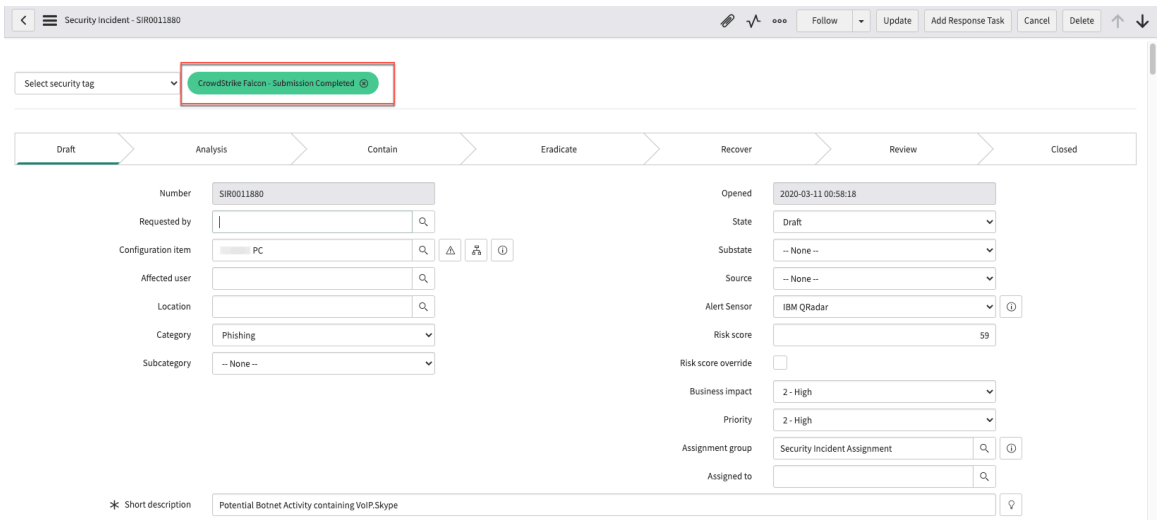


L'exemple suivant montre un incident de sécurité où la soumission a été effectuée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Soumission terminée : incident de sécurité



Examiner les paramètres globaux du bac à sable

Examinez et modifiez les paramètres globaux du bac à sable si vous rencontrez des problèmes avec les résultats de soumission de fichiers ou d'URL.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **CrowdStrike Falcon Sandbox** > **Paramètres globaux**.
2. Remplissez les champs du formulaire.

Champ	Description
Limite de taille de fichier (Mo)	Limite de taille de fichier de chargement de bac à sable en mégaoctets. **Remarque :** La limite de taille des fichiers de 256 Mo est configurée par défaut. N'augmentez pas la valeur au-delà de 256 Mo. Toutefois, vous pouvez réduire la limite de taille maximale des fichiers pour éviter de soumettre des fichiers volumineux.
Délai maximal pour les résultats de soumission (minutes)	Délai maximal pour les résultats de soumission à partir du bac à sable. **Remarque :** Le délai par défaut est de 30 minutes. Si vos résultats prennent plus de 30 minutes, vous pouvez augmenter le temps. Vous pouvez également afficher les résultats dans le portail du bac à sable.

3. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration de l’enrichissement des incidents Elasticsearch

L’intégration Elasticsearch - Enrichissement des incidents recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

- Introduction à l’intégration Elasticsearch - Enrichissement des incidents
- Créer des enregistrements de configuration de recherche de perceptions

Utiliser

- Exécuter une recherche de perceptions
- Security Operations Integration - Flux de recherche de perceptions
- Opérations de sécurité : flux de recherche de perceptions Elasticsearch

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l’écriture d’intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l’intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Traduction automatique

Introduction à l’intégration Elasticsearch - Enrichissement des incidents

Elasticsearch est un moteur de recherche et d’analyse RESTful distribué qui s’intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l’intégration d’enrichissement Elasticsearch des incidents, vous devez la télécharger à partir de et ServiceNow Store ajouter l’URL de base de l’API et les informations d’identification de connexion appropriées.

Avant de commencer

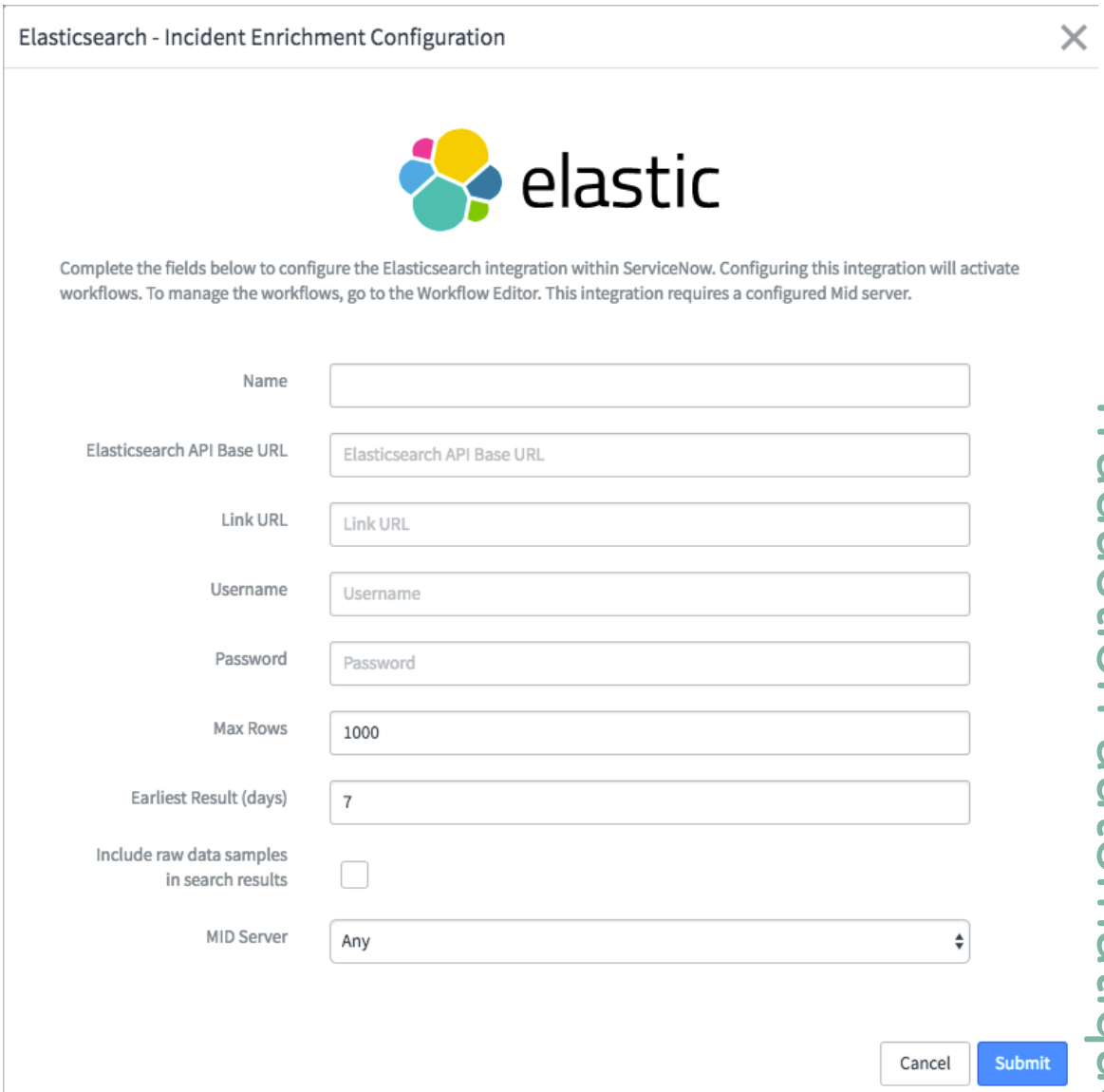
Rôle requis : sn_si.admin

Procédure

1. Télécharger l’intégration à partir de ServiceNow Store.
2. Une fois l’installation terminée, accédez Elasticsearch à l’URL de base de l’API et obtenez-la sous votre profil Elasticsearch.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**. Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte - Enrichissement de l'incident Elasticsearch , cliquez sur **Nouveau**.



Traduction automatique

5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
URL de base de l'API Elasticsearch	URL de base que vous avez acquise sur le Elasticsearch site.
URL de lien	[Facultatif] Liens vers une instance Kibana, le cas échéant
Nom d'utilisateur	Votre nom d'utilisateur Intel Elasticsearch .
Mot de passe	Votre mot de passe Intel Elasticsearch .
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend de votre paramètre dans la propriété **nombre de lignes de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	**Sélectionnez N'importe lequel** pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

6. Cliquez sur **Envoyer**.
   La carte de configuration d'intégration s'affiche.
7. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
8. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Résultats

Une fois configurée, l'intégration Elasticsearch - Enrichissement des incidents peut être sélectionnée pour publier des observables dans des listes de surveillance dans Réponse aux incidents de sécurité.

Intégration de la sécurité du point de terminaison FireEye

FireEye Endpoint Security (série HX) aide les entreprises à inspecter et à analyser les menaces connues et inconnues sur n'importe quel point de terminaison.

Les attaquants qualifiés contournent aujourd'hui les défenses traditionnelles sur lesquelles la plupart des équipes de sécurité comptent depuis des années pour protéger leurs terminaux. Même lorsqu'une défense traditionnelle arrête une menace connue, elle ne peut pas déterminer ce que cette menace essayait de faire. FireEye HX Endpoint Security aide votre équipe de sécurité à traquer et à arrêter les menaces avancées connues et inconnues qui pèsent sur vos terminaux.

L'intégration de référence de Security Incident Response avec FireEye HX, permet aux analystes de sécurité d'enquêter plus facilement et efficacement sur les incidents de sécurité et d'y remédier en un instant, sans avoir à naviguer entre les outils. Vous pouvez utiliser l'imbrication du réseau pour effectuer des actions de rattrapage sur les points de terminaison, implémenter des profils pour recueillir des détails spécifiques sur l'hôte et effectuer des requêtes ou des actions spécifiques sur le point de terminaison.

Fonctionnalités principales

- Possibilité d'effectuer des actions d'enrichissement de l'hôte pour recueillir plus de détails sur le point de terminaison, tels que les détails de l'hôte, les statistiques réseau, les détails de l'utilisateur, les détails du fichier, les détails du processus et les détails du service.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Capacité à effectuer une recherche de sécurité d'entreprise pour identifier les observables potentiellement malveillants sur les points de terminaison et à prendre des mesures correctives.
- Capacité à collecter des données de triage et d'acquisition pour une inspection et une analyse approfondies des points de terminaison.

Limitations

Les limitations connues de cette intégration sont les suivantes :

1. La valeur du champ Application MID doit être saisie manuellement.
2. Isoler l'hôte et obtenir les services d'exécution ne peut pas être effectué sur l'agent Linux.
3. Supprimer l'isolement ne prend pas en charge l'agent Linux.
4. L'acquisition de triage ne prend pas en charge l'agent Linux.
5. Les utilisateurs doivent configurer les liens connexes Afficher les données d'enrichissement. Il n'est pas disponible prêt à l'emploi.
6. Pour la recherche de perceptions, seules cinq recherches actives peuvent être présentes à la fois. Les autres seront mis en file d'attente et commenceront après la fin de l'une des observations en cours.
7. Les perceptions sont disponibles prêtes à l'emploi, qui seront faux/actives par défaut.
8. Le hachage n'est pas pris en charge pour Obtenir l'exécution des processus.

Configurer votre instance NowPlatform pour l'intégration FireEye

Vérifiez et examinez la procédure de configuration suivante pour configurer l'instance NowPlatform pour l'intégration FireEye.

Avant de commencer
Rôle requis : ServiceNow AI Platform administrateur (sn_si.admin)

La section suivante répertorie les tâches de configuration qui doivent être effectuées dans votre instance NowPlatform avant d'installer l'application pour l'intégration FireEye.

Vérifiez que vous avez effectué les tâches suivantes avant d'installer l'application à partir de ServiceNow Store.

Tâche	Description
Vérifiez que vous avez affecté les rôles requis Now Platform et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis : 1. L'utilisateur disposant du rôle d'administrateur système (admin) est requis pour installer l'application pour l'intégration. 2. L'utilisateur disposant du rôle d'administrateur d'incident de sécurité (sn_si.admin) est requis pour configurer l'intégration, créer, activer et supprimer des profils. 3. L'utilisateur disposant du rôle d'analyste des incidents de sécurité (sn_si.analyst) est requis pour travailler avec des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
	incidents de sécurité. Un utilisateur disposant de ce rôle peut initier n'importe quelle option disponible dans l'intégration.
Vérifiez que vous avez installé et configuré un Serveur MID.	Configurer Serveur MID : un Serveur MID dans votre instance NowPlatform est requis pour gérer les fichiers et se connecter au service FireEye déployé au sein du réseau de votre organisation. Pour plus d'informations sur les serveurs MID, voir https://servicenow.com/docs
Vérifiez que les applications principales ServiceNow nécessaires à la prise en charge de l'intégration sont installées et activées avant d'installer l'application.	Les applications suivantes doivent être installées et activées à partir du ServiceNow Store avant d'installer cette application. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour assurer une installation fluide : **1.** Assistance pour Security Incident Response **2.** Base de support de la sécurité **3.** Security Support Common **4.** Security Incident Response **5.** Structure commune de prise en charge de Threat Intelligence **6.** Programme d'installation du pack d'intégration ServiceNow Enterprise
Avant d'activer l'option d'approbation des profils, vérifiez que vous avez créé un groupe d'approbation.	Un workflow d'approbation facultatif permet d'isoler les machines hôtes, de les restaurer sur le réseau, d'obtenir des fichiers et d'exécuter des actions supplémentaires sur le point de terminaison. Si votre organisation souhaite un niveau de contrôle supplémentaire sur ces actions, activez l'option Exiger l'approbation lors de la configuration des profils. En l'absence de profil, si une aptitude est invoquée directement à partir de la liste connexe, les approbations peuvent être traitées à partir du module de configuration par défaut FireEye. En tant qu'administrateur de sécurité, vous pouvez configurer l'approbation tout en configurant les profils et les paramètres par défaut. Un groupe d'approbation doit être disponible sur la liste des groupes de votre instance.

Traduction automatique

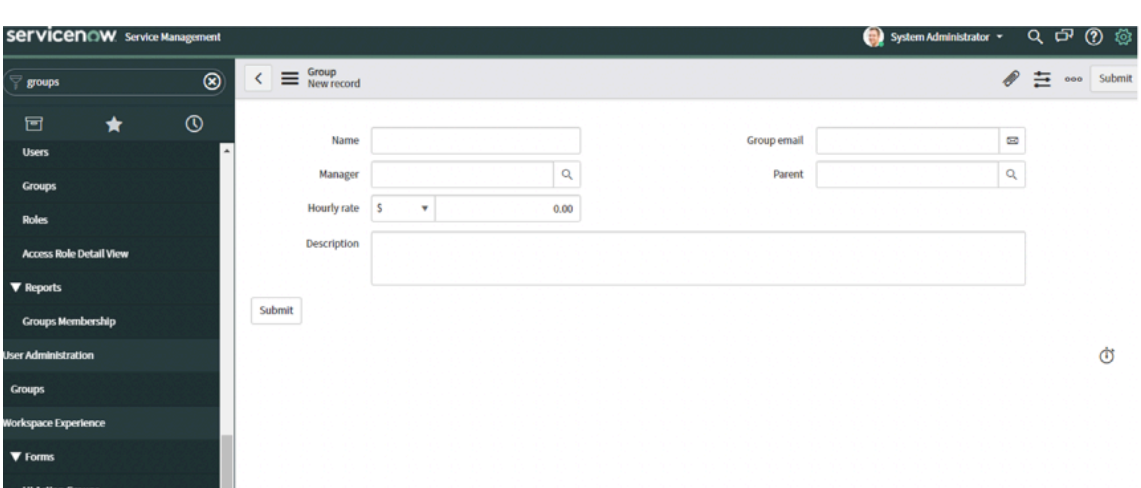
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Administration utilisateurs** > **Groupes**.
2. Cliquer sur **Nouveau** dans la liste Groupes.
3. Remplissez le formulaire avec les détails suivants :

Champ	Description
Nom	Nom du groupe qui s'affiche lorsqu'une demande d'approbation est soumise.
E-mail de groupe	(Facultatif) Liste de distribution d'e-mails de groupe ou adresse e-mail du point de contact, tel que le gestionnaire de groupe.
Responsable	(Facultatif) Nom du gestionnaire de groupe. Cliquez sur l'icône de recherche pour afficher la liste.
Parent	(Facultatif) Nom du groupe parent, s'il est associé à un parent.
Taux horaire	(Facultatif) Le montant payé pour chaque heure travaillée.
Description	(Facultatif) Informations supplémentaires sur le groupe.

4. Cliquer sur **Envoyer**.



Le nouveau groupe s'affiche dans la liste Groupes. Vous avez créé un groupe d'approbation avec succès. Ajoutez des utilisateurs à votre nouveau groupe, selon vos besoins, qui peuvent approuver les demandes soumises par l'analyste de sécurité. Un utilisateur hérite des rôles de tous les groupes auxquels il appartient. Vous pouvez également affecter des rôles directement à un utilisateur.

Pour surveiller et traiter les demandes soumises par les utilisateurs disposant du rôle sn_si.analyst, chaque membre du groupe d'approbation doit accéder à Mes approbations dans le ServiceNow AI Platform. Les approbateurs peuvent également trouver les demandes soumises spécifiquement pour l'intégration de FireEye sous les approbations FireEye.

Que faire ensuite

L'étape suivante consiste à installer et configurer l'application à partir de ServiceNow Store.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration des paramètres d'horodatage pour l'acquisition du triage

Configurez et vérifiez les paramètres d'horodatage avant la procédure d'installation.

Avant de commencer
Rôle requis : administrateur d'incident de sécurité NowPlatform (sn_si.admin)

Avant d'installer l'application FireEye, vous devez effectuer certaines conditions préalables sur FireEye.

L'acquisition du triage peut être demandée avec une entrée du champ « Autour de l'horodatage » ou du champ « Standard ». Environ l'horodatage demande des informations collectées pendant une période spécifiée avant l'horodatage jusqu'à une durée spécifiée après l'horodatage. L'horodatage est l'heure à laquelle l'événement qui a généré l'alerte s'est produit. Si vous sélectionnez Standard, le dispositif Endpoint Security demande des informations à l'hôte pour toutes les données relatives à un événement.

Lorsqu'un utilisateur de Endpoint Security demande une collecte de triage en fonction d'une date et d'une heure spécifiques, l'agent renvoie des informations pour une fenêtre de temps spécifiée avant et après l'alerte. Les paramètres d'horodatage contrôlent la longueur de la fenêtre pour la collecte de triage. Les paramètres d'horodatage s'appliquent uniquement aux événements d'URL d'agent (événements de surveillance d'URL) et de clé de registre (événements de clé d'enregistrement).

Vous pouvez utiliser l'onglet Paramètres d'horodatage pour spécifier la durée avant et après l'horodatage pendant laquelle les informations sont collectées. Les paramètres d'horodatage peuvent aller de 0 à 86 400 secondes. La valeur par défaut pour les deux paramètres est de 600 secondes.

Vous pouvez utiliser l'onglet Paramètres d'horodatage de la page Paramètres de triage automatique pour spécifier la durée avant et après l'horodatage pendant laquelle les informations sont collectées. L'horodatage est l'heure à laquelle l'événement qui a déclenché l'alerte s'est produit.

Procédure

1. Accédez à la **Interface utilisateur Web de sécurité du point de terminaison**.
2. Sélectionner **Administrateur** > **Paramètres de triage**.
3. Cliquer sur **Paramètres d'horodatage** onglet sur le **Paramètres de triage automatique** la page.
4. Spécifiez la durée avant et après l'horodatage pendant laquelle les informations sont nécessaires.
5. Entrez le nombre de secondes avant l'horodatage spécifié pendant lequel les informations sont nécessaires.
6. Entrez le nombre de secondes après l'horodatage pendant lesquelles les informations sont nécessaires.
7. Cliquer sur **Enregistrer**.

Remarque : Vous pouvez rétablir les paramètres par défaut de toutes les valeurs de la page en cliquant sur **Rétablir les valeurs par défaut**, puis cliquez sur Enregistrer.

- **Zone d'espace d'acquisition**: la page Acquisitions indique l'espace disque restant pour les acquisitions.
- **Définition des limites d'utilisation du disque pour les acquisitions :**
  - Les triages, les acquisitions de fichiers et les acquisitions de données peuvent s'accumuler au fil du temps et utiliser une quantité croissante d'espace disque. Pour contrôler cela, vous pouvez leur allouer une quantité définie d'espace disque. Dix pour cent de l'espace disque que vous spécifiez est réservé aux acquisitions

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

automatiques de triage. Lorsque la surface d'acquisition totale allouée est dépassée, les triages automatiques les plus anciens sont supprimés.

- Lorsque la taille totale du disque des acquisitions terminées dépasse une limite spécifiée, l'appliance Endpoint Security supprime les acquisitions terminées les plus anciennes jusqu'à ce que suffisamment d'espace disque soit dégagé pour ramener le total sous la limite spécifiée. Les acquisitions qui ne sont pas encore terminées ne sont pas touchées.
- L'appliance Endpoint Security supprime automatiquement les acquisitions si un administrateur, un analyste ou un enquêteur utilise l'interface utilisateur Web Endpoint Security pour supprimer manuellement l'agent associé.

Pour définir des limites d'utilisation du disque pour les acquisitions complètes à l'aide de l'interface utilisateur Web :

- Accédez à **l'interface utilisateur web de la sécurité du point de** terminaison.
- Sélectionner **Limites d'utilisation du disque** à partir de **Administrateur** menu.
- Dans le **Limite d'espace d'acquisition** , spécifiez la quantité maximale d'espace disque (en Go) qui peut être utilisée pour stocker le triage, les acquisitions de fichiers et de données. Les valeurs valides et les valeurs par défaut varient en fonction du modèle de votre dispositif Endpoint Security. Les valeurs appropriées pour votre modèle sont affichées sur la page Limites d'utilisation du disque.
- Cliquer sur **Enregistrer**.

Remarque : Tous les paramètres mentionnés sont respectés et en cas de défaillance ou d'erreur, ServiceNow AI Platform il renvoie simplement ces erreurs.

Installez l'application et configurez une source pour l'intégration

Installez et configurez l'application à partir de ServiceNow Store sur votre ServiceNow AI Platform instance.

Avant de commencer

Rôle requis : administrateur NowPlatform (admin)

Remarque : Un Serveur MID actif est obligatoire pour configurer une source.

Téléchargez l'intégration de Security Incident Response avec FireEye HX l'application à partir du ServiceNow Store et installez-la.

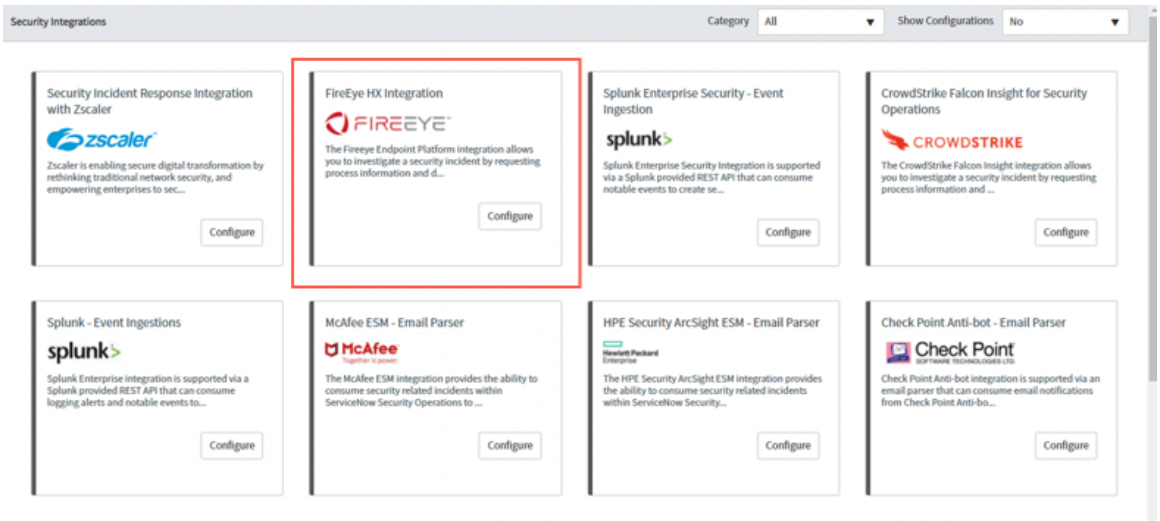
Une fois l'application installée, procédez comme suit pour la configurer :

Procédure

1. Accédez à la **Intégrations** > **Configurations d'intégration**.
2. Sélectionnez le **Configurations d'intégration** pour afficher les intégrations disponibles et localiser le **FireEye** carreau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

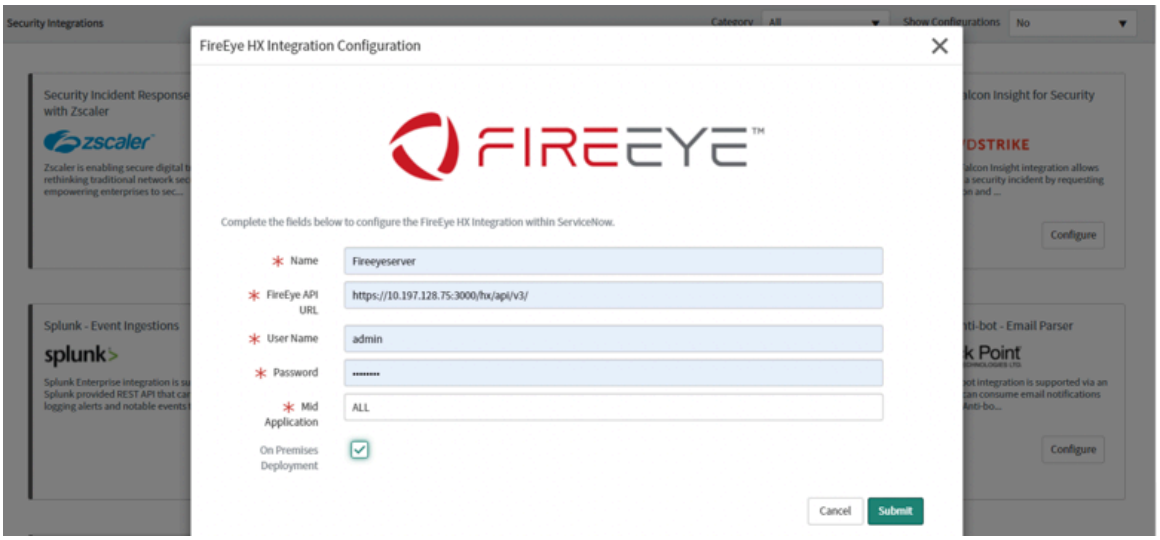


3. Cliquer sur **Configurer** sur la vignette FireEye.
4. Fournissez les détails suivants pour configurer l’intégration FireEye :

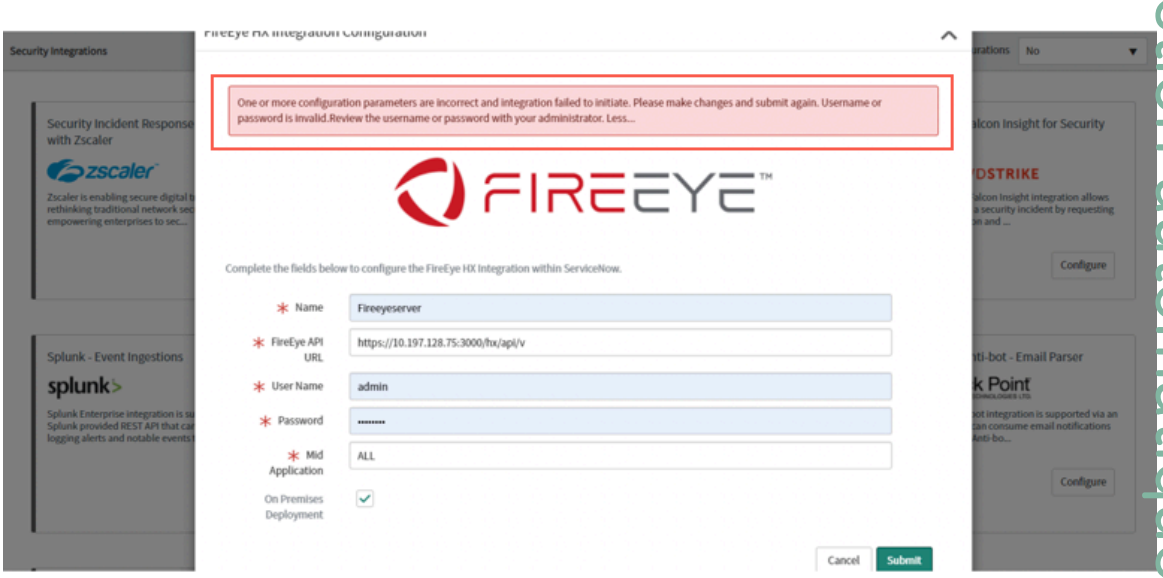
Champ	Description
Nom	Nom de la configuration FireEye. Ce nom est utilisé pour identifier la source, ainsi que les informations d’identification et la configuration associées. Ce nom vous permet de distinguer les informations d’identification et les comptes, ainsi que d’identifier chaque source pour éviter les conflits avec les profils.
URL D'API	URL de base hébergeant l’API FireEye.
Nom d'utilisateur	Entrez le nom d’utilisateur du compte FireEye.
Mot de passe	Entrez le mot de passe du compte FireEye.
Application MID	Application MID configurée dans votre environnement. Le serveur MID est requis pour traiter les fichiers zip pour certaines des options d’enrichissement. Par défaut, ce sera TOUT. Les utilisateurs doivent fournir manuellement un nom d’application valide.
Déploiement sur site	Désactivé par défaut. Si vous utilisez la version cloud de FireEye, vérifiez que la case est décochée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquer sur **Envoyer**.
   La liste des configurations FireEye s'affiche avec votre nouvel enregistrement de configuration. Vous avez terminé la configuration d'un serveur FireEye. Si vous ne pouvez pas vous connecter au FireEye ou si vos informations d'identification sont incorrectes, un message d'erreur de validation s'affiche comme illustré dans la figure suivante. Vérifiez que vos informations d'identification sont correctes et réessayez.



Traduction automatique

Paramètres par défaut FireEye

Voici les paramètres de configuration supplémentaires une fois l'installation terminée.

Une fois l'installation terminée, vous pouvez trouver le module Paramètres par défaut FireEye dans le menu de navigation de gauche. Il contient les paramètres par défaut des différentes fonctionnalités FireEye.

Configurations supplémentaires

Les paramètres de configuration supplémentaires sont les suivants :

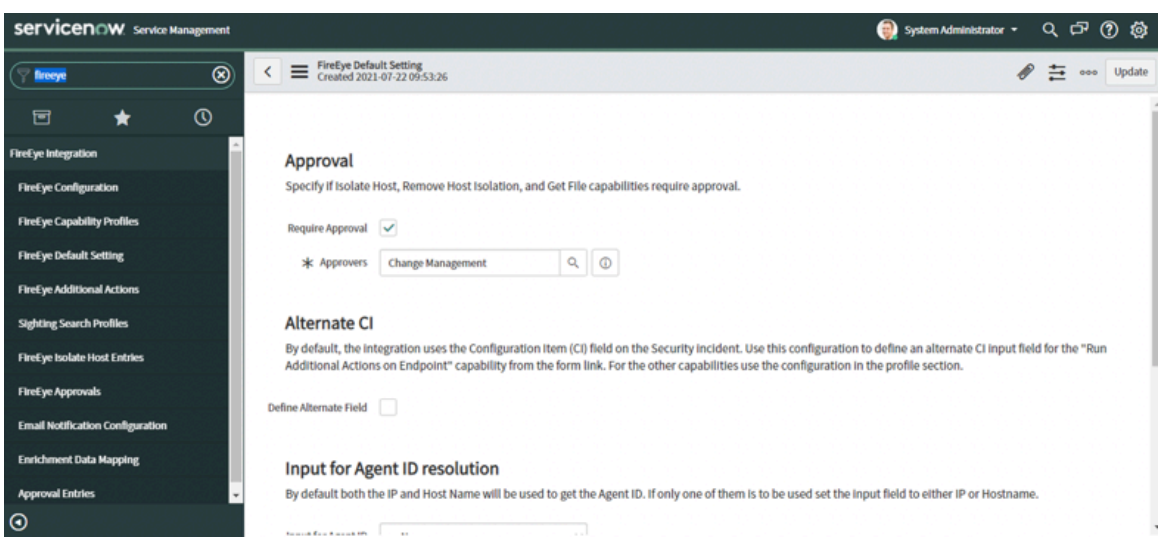
1. **Approbation**: cette approbation est spécifiquement destinée aux fonctionnalités Isoler l'hôte, Supprimer l'isolement de l'hôte et Obtenir un fichier lorsqu'elles sont déclenchées directement à partir de la liste connexe et en l'absence de profils pour celles-ci. S'il existe

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

un ou plusieurs profils existants pour ces options, la configuration d'approbation dans le profil sera respectée.

- **Exiger l'approbation :** Lorsque vous activez l'option Exiger l'approbation, le champ Approbateurs est disponible sur le formulaire.
- **Approbateurs**: liste des groupes d'approbateurs. Après avoir soumis une demande, l'approbation du groupe est requise pour terminer la demande.

2. **CI alternatif**: si vous cochez cette case, la liste des champs disponibles pour passer un CI alternatif à la capacité s'affiche. Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité. Cette configuration est applicable uniquement pour l'aptitude « Exécuter des actions supplémentaires sur le point de terminaison ». Utilisez donc cette configuration pour définir un champ d'entrée CI alternatif pour l'aptitude « Exécuter des actions supplémentaires sur le point de terminaison » uniquement. Pour les autres options, utilisez la configuration dans la section de profil. Si les profils ne définissent pas d'autre CI, les options sélectionnent le champ CI dans le formulaire Incident de sécurité.
3. **Entrée pour la résolution de l'ID d'agent**: par défaut, l'adresse IP et le nom d'hôte sont utilisés pour obtenir l'ID de l'agent. Si un seul d'entre eux doit être utilisé, définissez le champ d'entrée sur IP ou Nom d'hôte.

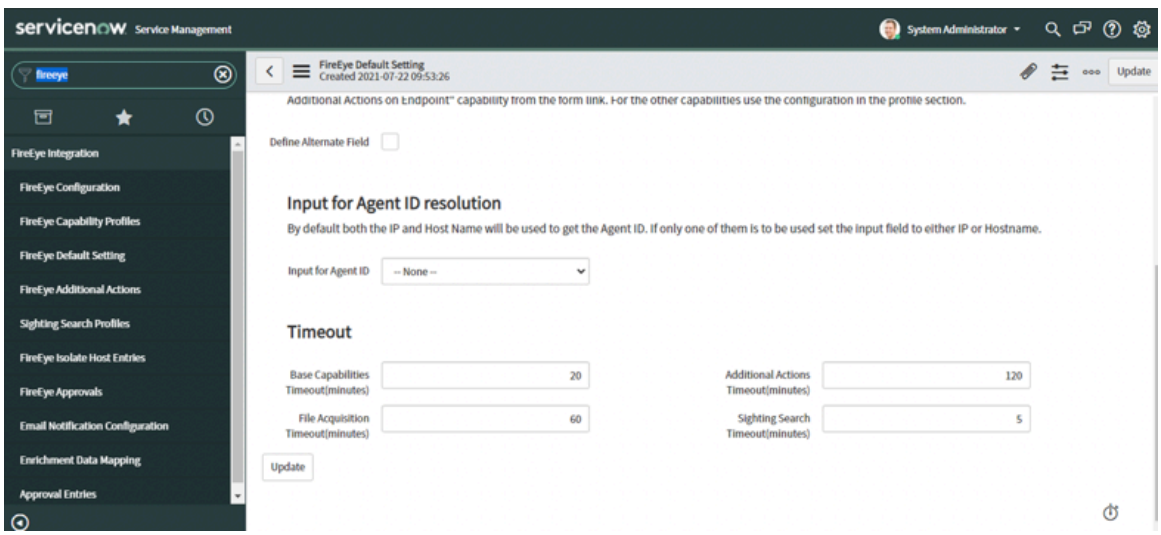


4. **Délai**:
   - **Délai d'expiration des options de base (minutes) :** Les options Enrichissement, Isoler l'hôte et Supprimer l'isolement de l'hôte échoueront si aucune réponse n'est restituée dans le temps imparti.
   - **Délai d'expiration de l'action supplémentaire (minutes) :** La fonctionnalité Exécuter des actions supplémentaires sur le point de terminaison échouera si aucune réponse n'est restituée dans le temps imparti.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Délai d'expiration de l'acquisition du fichier (minutes) :** L'aptitude d'obtention de fichier échouera si aucune réponse n'est restituée dans le temps imparti.
- **Délai d'expiration de la recherche de perception (minutes) :** La recherche sera interrompue passé le délai défini.



Créer un profil d'aptitude pour l'intégration du point de terminaison FireEye

Créez un profil et sélectionnez les FireEye HX options que vous souhaitez que le profil exécute.

Avant de commencer

Rôle requis : administrateur d'incident de sécurité NowPlatform (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Des profils sont créés pour regrouper les capacités et aideraient les analystes à effectuer facilement l'enquête/la correction.

Voici la liste des fonctionnalités que vous pouvez ajouter au(x) profil(s) :

1. Obtenir les détails de l'hôte
2. Obtenir les utilisateurs connectés
3. Obtenir les statistiques réseau
4. Obtenir les processus en cours d'exécution
5. Obtenir les services d'exécution
6. Obtenir un fichier
7. Isoler l'hôte
8. Supprimer l'isolement

Vous ne pouvez pas associer les options Obtenir un fichier, Isoler l'hôte et Supprimer l'isolement de l'hôte avec d'autres options lors de la création d'un profil. Les profils de ceux-ci doivent être créés individuellement. D'autre part, Obtenir les détails du système, Obtenir les utilisateurs connectés, Obtenir les statistiques réseau, Obtenir les processus en cours d'exécution et Obtenir les services d'exécution peuvent être regroupés. Vous pouvez créer des profils individuellement ou en les matraquant en entier ou en partie selon vos besoins. Une fois qu'une option est incluse dans un profil, elle ne peut pas être incluse dans un autre profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour créer un nouveau profil d’aptitude, procédez comme suit :

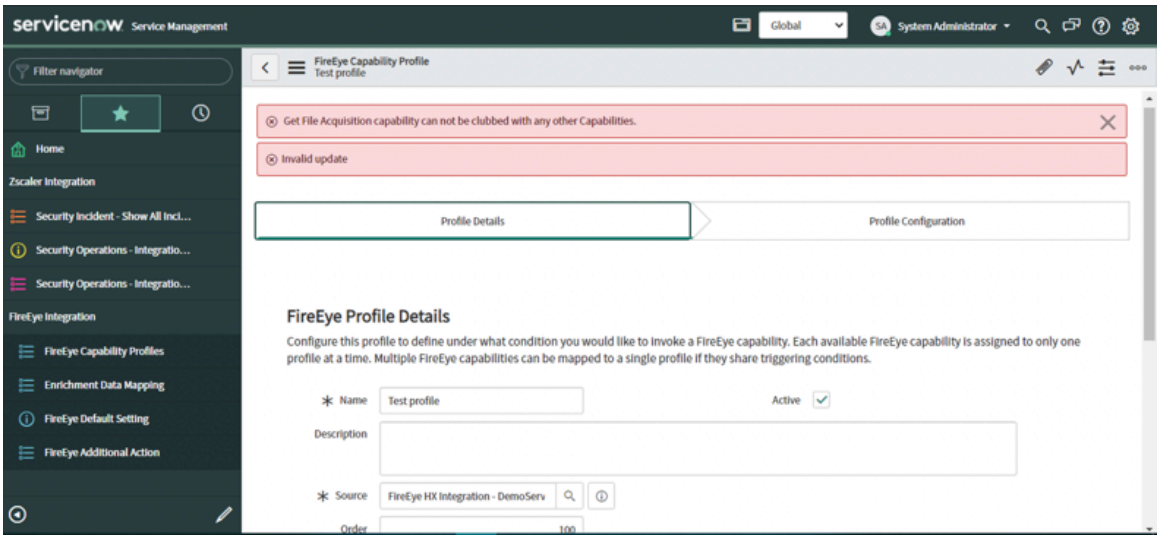
Procédure

1. Accédez à la **Intégration de FireEye** > **Profils d'aptitude FireEye**.
   La liste des profils d’aptitudes s’affiche.
2. Cliquer sur **Nouveau**.
3. Renseignez les champs du formulaire.

Nom	Nom du profil d’aptitude FireEye HX . Ce nom vous permet d’identifier le type de profil et de le décrire.
Description	Informations supplémentaires sur le profil qui décrit plus en détail le profil.
Source	Nom de la FireEye HX source. Seules les sources configurées sont disponibles dans la liste de choix.
Options FireEye HX	Aptitudes du FireEye HX profil. Sélectionnez les options souhaitées pour ce profil dans la colonne Disponible et déplacez-les vers la colonne Sélectionné.
Ordre	Priorité du flux. La valeur par défaut est 100. La valeur de ce champ indique l’ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux avec le numéro le plus bas a la priorité la plus élevée. Pour définir l’ordre d’opération, saisissez une valeur. Par exemple, 100, 200, 300, 400.
Actif	Cela indique que le profil est actif. Lorsque le profil est actif, il se déclenche automatiquement lorsqu’un incident de sécurité correspondant aux conditions de filtrage que vous avez spécifiées dans la configuration est créé.

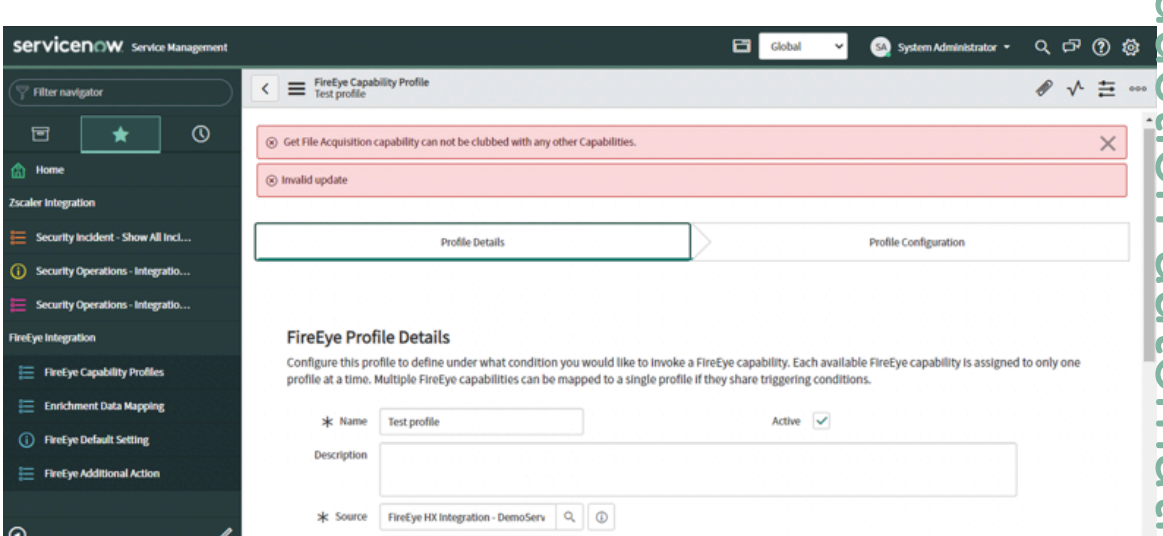
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La figure suivante est un exemple de formulaire rempli pour les détails du profil avec l'aptitude Obtenir les détails de l'hôte.

4. Cliquer sur **Suivant** pour passer à la configuration du profil.



Remarque : Les options Isoler l'hôte, Supprimer l'isolement de l'hôte et Obtenir des fichiers ne peuvent pas être associées à d'autres options.

Que faire ensuite

L'étape suivante consiste à configurer votre profil. Avant de configurer les paramètres du profil, vous pouvez passer en revue les concepts de configuration des profils et des conditions de déclenchement. Pour plus d'informations, consultez Comprendre comment les conditions de déclenchement fonctionnent avec un élément de configuration pour un profil.

Comprendre comment les conditions de déclenchement fonctionnent avec un élément de configuration

Une fois que vous avez créé un profil et sélectionné les options FireEye que vous souhaitez que le profil exécute, configurez les paramètres du profil de sorte qu'il ne s'exécute que lorsqu'un ensemble de conditions spécifiques est rempli.

Vous pouvez définir des conditions de déclenchement afin que le profil s'exécute automatiquement chaque fois qu'un incident de sécurité correspondant à la condition de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

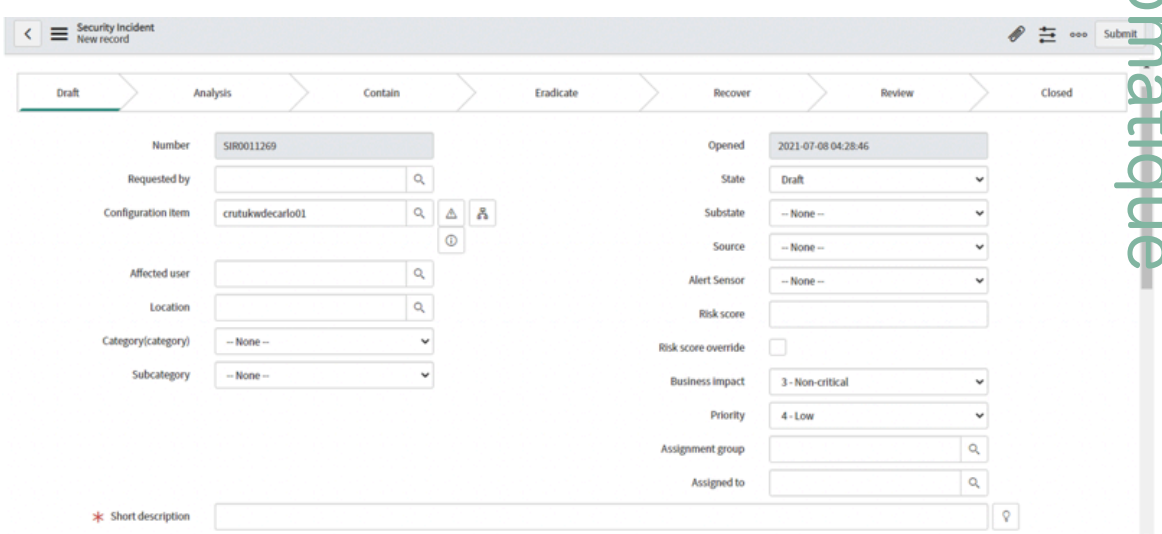
déclenchement est créé. Si la condition de déclenchement n'est pas définie, ces profils peuvent être exécutés manuellement en cliquant sur le formulaire « Exécuter le(s) profil(s) EDR » sur l'incident de sécurité et en sélectionnant le profil.

Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité. Cette valeur est utilisée pour faire correspondre les ID de vos actifs avec les informations stockées dans la CMDB Now Platform. Lorsqu'un incident de sécurité est créé et qu'un profil est exécuté automatiquement ou manuellement, une recherche est effectuée dans la CMDB pour récupérer le nom d'hôte et/ou l'adresse IP en fonction de la valeur du champ CI. Le nom et/ou l'adresse IP d'hôte sont utilisés pour résoudre l'ID de l'agent afin FireEye HX d'identifier le point de terminaison.

Dans l'idéal, une valeur correspondante est trouvée dans la base de données et les données sont collectées à partir de la FireEye HX console pour l'actif correspondant. Les données relatives aux différentes options sont extraites dans votre ServiceNow AI Platform instance et affichées dans les listes connexes d'incidents de sécurité. Lorsque le champ Élément de configuration (CI) de l'incident de sécurité avec un nom d'hôte ou une adresse IP correspondant à la base de données n'est pas renseigné, vous pouvez sélectionner un autre champ de l'incident de sécurité qui contient le nom d'hôte ou l'adresse IP pour effectuer la résolution de l'ID d'agent.

Au cours de l'étape de configuration du profil, vous pouvez sélectionner un autre champ CI pour l'identification du point de terminaison afin de vous assurer que vous êtes en mesure d'identifier le point de terminaison sur FireEye HX. Vous pouvez sélectionner n'importe quel champ de l'incident de sécurité comme champ de déclenchement CI alternatif, y compris les champs personnalisés que vous créez. En sélectionnant cet autre champ CI comme sauvegarde, vous vous assurez que vos profils s'exécutent même si le champ CI n'est pas renseigné sur l'incident de sécurité associé lors de la création de l'incident.

Remarque : Les champs CI alternatifs ne sont pris en compte que pour les options qui peuvent être ajoutées à un profil. Pour toutes les actions supplémentaires, le CI alternatif est sélectionné à partir de la page des paramètres par défaut.



Traduction automatique

Configurer les profils et les incidents de sécurité pour l'intégration FireEye HX

Une fois que vous avez créé un profil et sélectionné les FireEye HX options que vous souhaitez que le profil exécute, configurez les paramètres afin que le profil puisse être invoqué uniquement dans les conditions définies.

Avant de commencer
Rôle requis : sn_si.admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurez le profil de sorte qu'il s'exécute uniquement lorsque les conditions spécifiées sont remplies. Sélectionnez un autre champ d'entrée pour le champ Élément de configuration (CI), si nécessaire, et définissez des conditions de filtrage afin que le profil puisse être déclenché automatiquement lorsqu'un incident de sécurité répondant aux conditions de déclenchement est créé.

Remarque : Vous pouvez accéder au modèle suivant : **Configuration du profil** page uniquement une fois que vous avez saisi la page **Détails du profil**.

Procédure

1. Accédez à la **Intégration de FireEye** > **Profils d'aptitude FireEye**.
2. Cliquer sur **Suivant** sur le **Détails du profil** après avoir rempli la section Détails du profil.
3. Examinez et configurez les sections suivantes :
   - **Définir un critère d'incident (automatisation)**: définissez les conditions d'incident de sécurité qui déclenchent automatiquement les FireEye HX options du profil. Si vous ne sélectionnez pas l'icône **Définir un critère d'incident** , le profil et les options sous-jacentes peuvent être invoqués manuellement à partir de l'incident de sécurité.
     - Sélectionner **Définir un critère d'incident** Option permettant de déclencher FireEye HX automatiquement les options du profil.
     - Dans le **Conditions de filtre**, sélectionnez le champ requis.
     - Vous pouvez ajouter **Nouveau critère** et définissez également la condition OU ou ET.

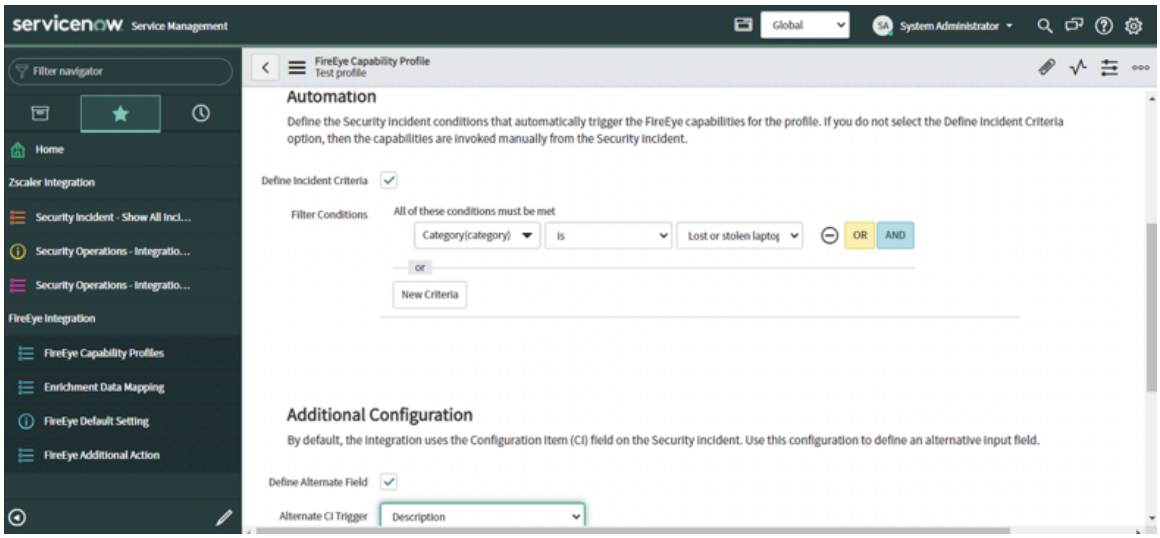
       Remarque : Isoler l'hôte, Supprimer l'isolement de l'hôte, Obtenir le fichier ne peut pas être déclenché automatiquement.

   - **Configuration supplémentaire**: lorsque le champ Élément de configuration (CI) n'est pas renseigné sur l'incident de sécurité avec un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour interroger les FireEye HX API.
     - Sélectionnez le **Définir un champ alternatif** Option permettant de définir un champ d'entrée alternatif.
     - Sélectionner le champ d'entrée dans le **Champ de déclenchement CI alternatif**.

       Remarque : Pour plus d'informations, consultez Comprendre comment les conditions de déclenchement fonctionnent avec un élément de configuration.

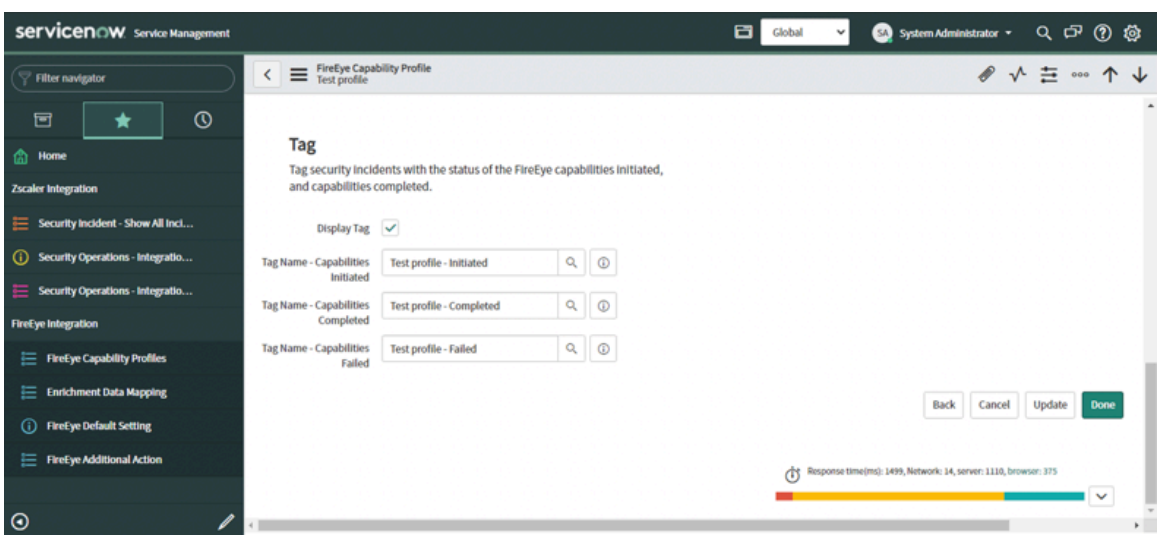
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- **Balises**: vous pouvez éventuellement baliser les incidents de sécurité avec les balises de profil initié, de profil terminé et de FireEye HX profil échoué.

  Sélectionnez le **Balise d'affichage** Case à cocher permettant d'activer le balisage des incidents de sécurité, le nom du profil est précédé d'un préfixe sur l'activation de la balise. Par défaut, cette option est désactivée pour tous les profils.

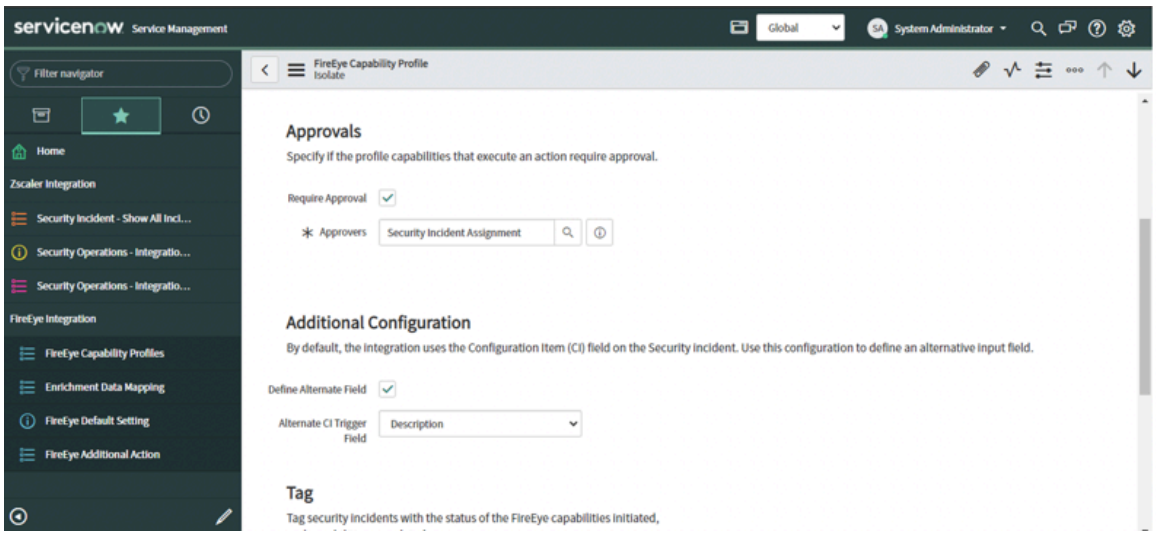


- **Approbations**: sélectionnez le **Exiger l'approbation** Case à cocher pour fournir un niveau de contrôle supplémentaire lors de l'utilisation des options d'isolation FireEye HX des machines hôtes, de restauration sur le réseau et d'obtention des fichiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’option d’approbation dans la configuration du profil s’affiche uniquement pour les options Isoler l’hôte, Supprimer l’isolement de l’hôte et Obtenir un fichier.



4. Cliquez sur **Terminé**.
5. Vérifiez les FireEye HX conditions de déclenchement.

Vérifier les filtres des conditions de déclenchement

Testez le profil et vérifiez que les filtres de condition de déclenchement que vous avez configurés fonctionnent comme prévu.

Avant de commencer
Rôle requis : sn_si.admin ou sn_si.analyst

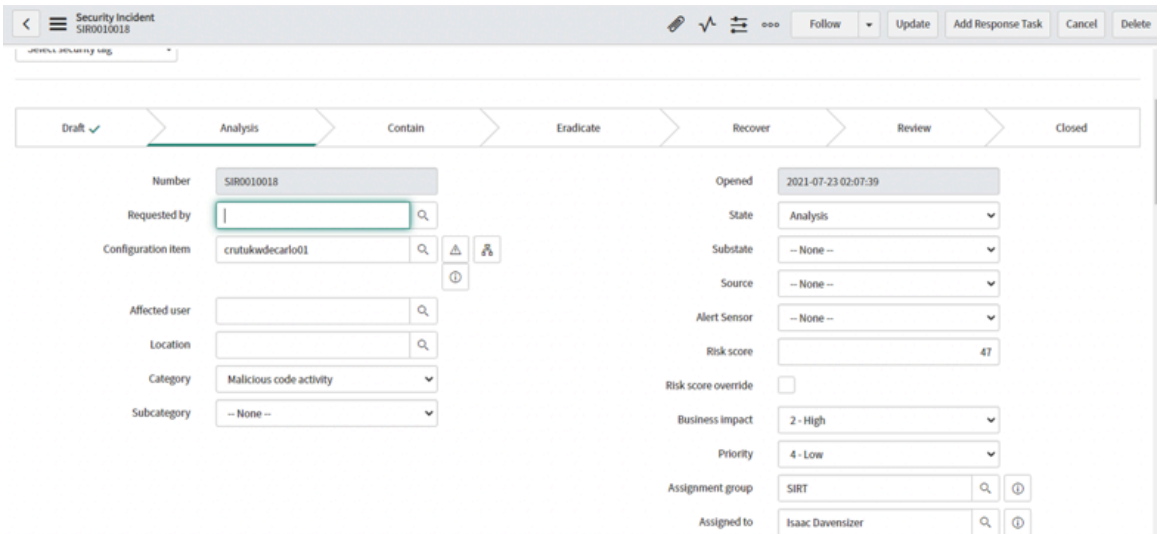
Une fois que vous avez activé le profil, en fonction des conditions de déclenchement configurées, vous pouvez afficher les résultats de la requête dans les ServiceNow AI Platform incidents de sécurité.

Procédure

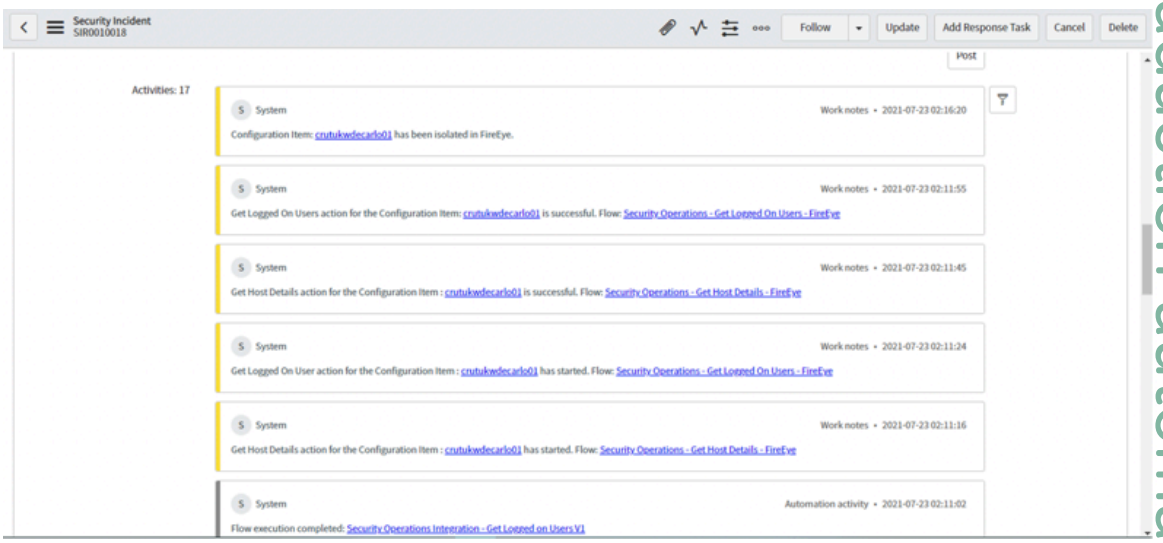
1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionner **Nouveau** pour créer un nouvel incident de sécurité.
3. Fournissez les conditions de filtre telles que données dans le profil d’aptitude pour déclencher le profil respectif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquer sur **Enregistrer**.

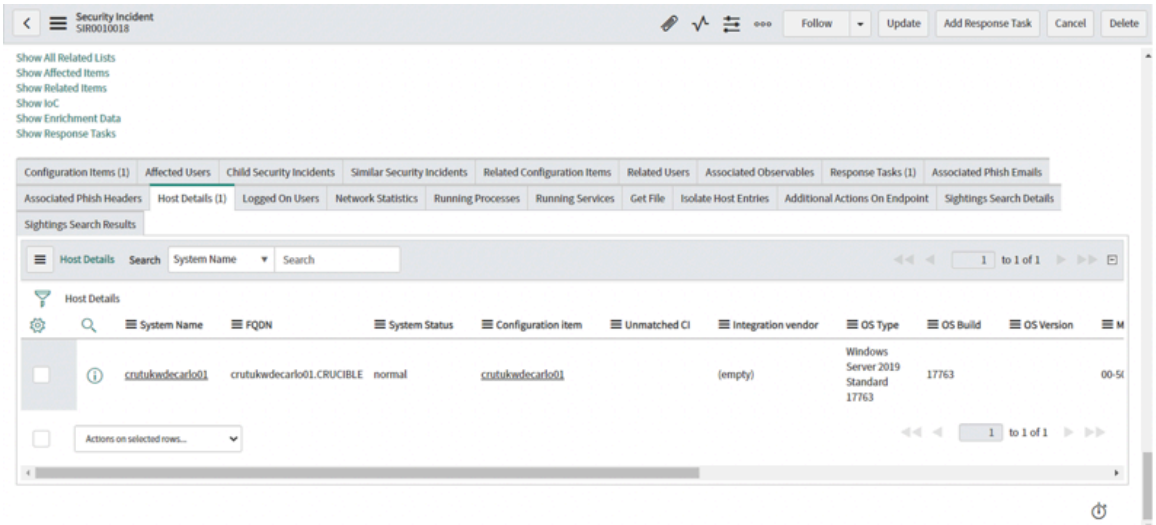


5. Examinez la section Notes de travail et activités.
6. Affichez les balises profil initié, profil terminé ou profil échoué.
7. Cliquer sur **Afficher toutes les listes connexes**.
8. Cliquez sur n’importe quelle liste connexe (onglet).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, Détails de l’hôte.



Déclencher un profil d’aptitude FireEye à partir de Liens connexes

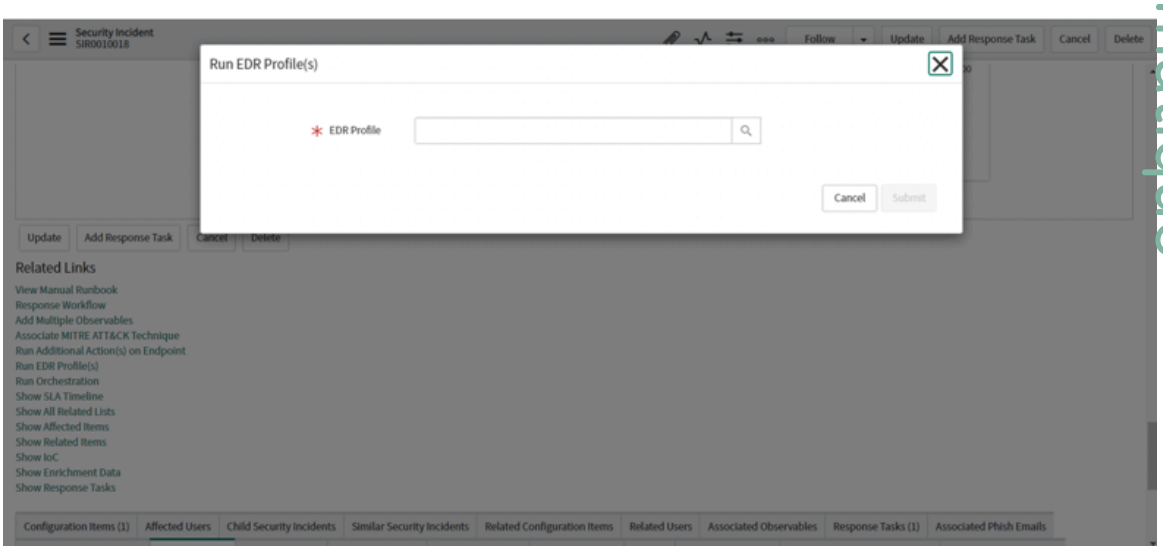
Déclenchez manuellement un profil d’aptitude après avoir examiné un incident de sécurité à partir des liens connexes.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Procédure

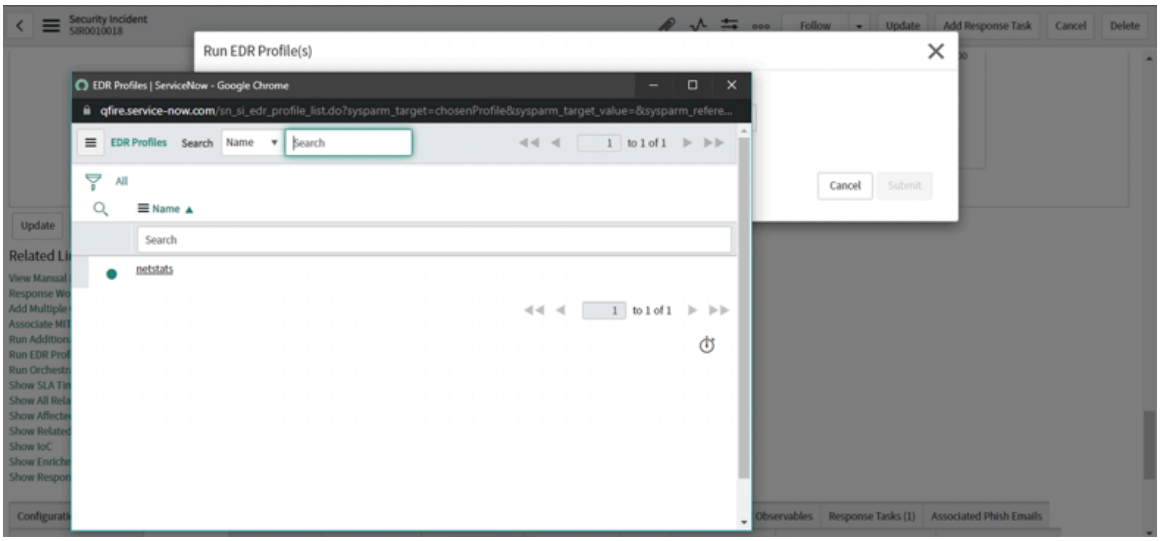
1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l’incident de sécurité que vous souhaitez examiner.
3. Cliquer sur **Exécuter le(s) profil(s) EDR**dans la section Liens connexes.

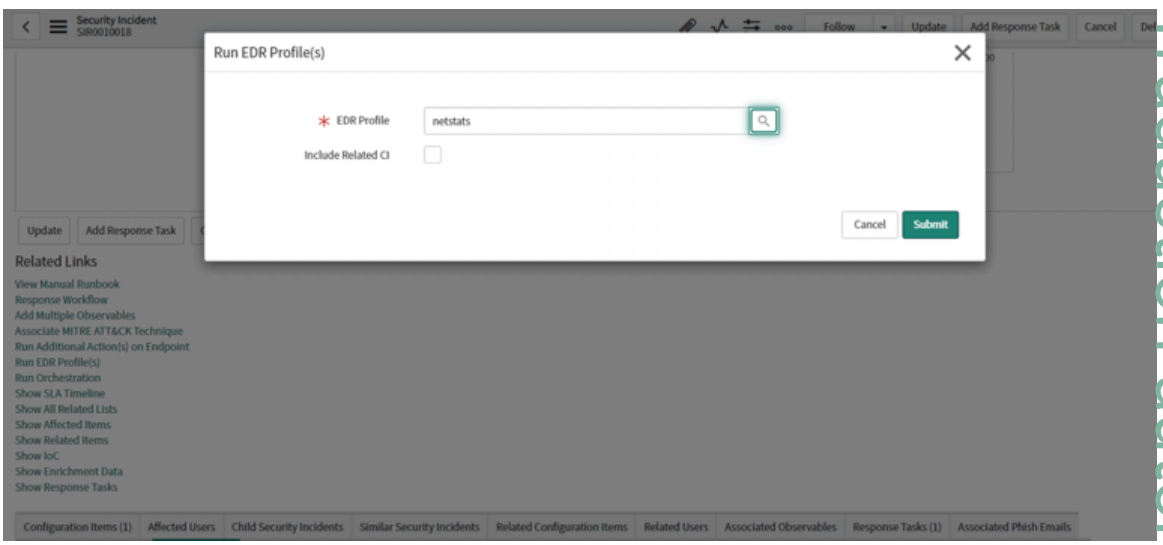


4. Parcourez et sélectionnez un profil dans la liste des profils disponibles, puis cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





5. Le profil sélectionné est déclenché manuellement.
6. Examinez la section Notes de travail et activités.
7. Affichez les balises et vérifiez les listes connexes pour les données.

> **Remarque :** En plus d'exécuter le profil pour le CI ou le CI alternatif de l'incident de sécurité, vous pouvez également exécuter le profil pour les valeurs CI présentes dans la liste connexe des éléments de configuration en cochant l'option Inclure le CI connexe dans la boîte de dialogue. Cette opération permet également de récupérer les données des valeurs de CI présentes dans la liste connexe. Vous pouvez également exécuter le profil uniquement pour les valeurs de CI présentes dans la liste connexe.

Déclencher un profil d'aptitude FireEye à partir de la liste connexe d'éléments de configuration

Déclenchez manuellement un profil d'aptitude à partir de la liste connexe des éléments de configuration.

Avant de commencer

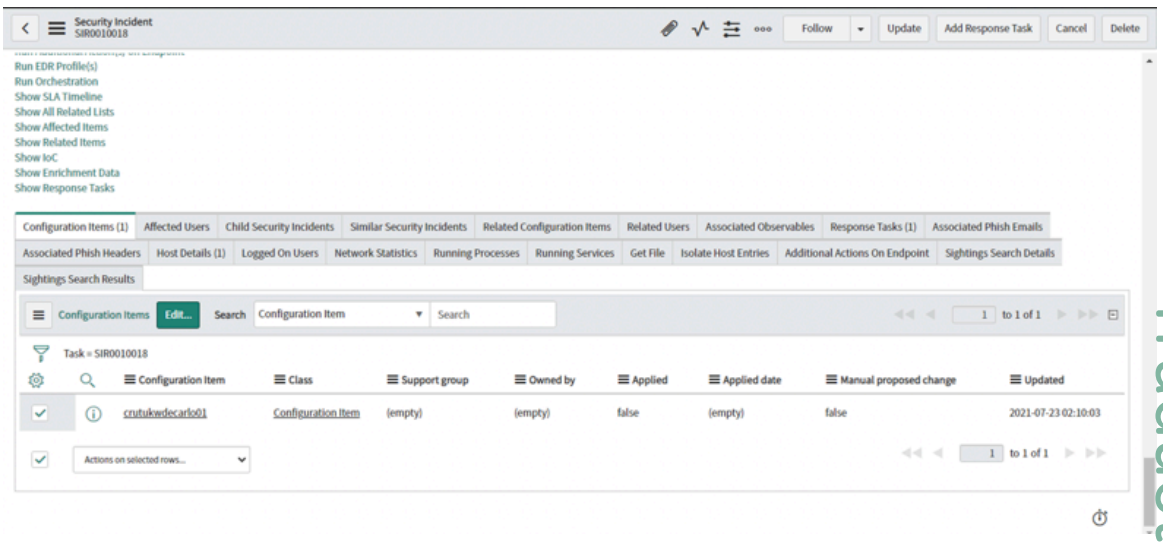
Rôle requis : sn_si.admin, sn_si.analyst

Traduction automatique

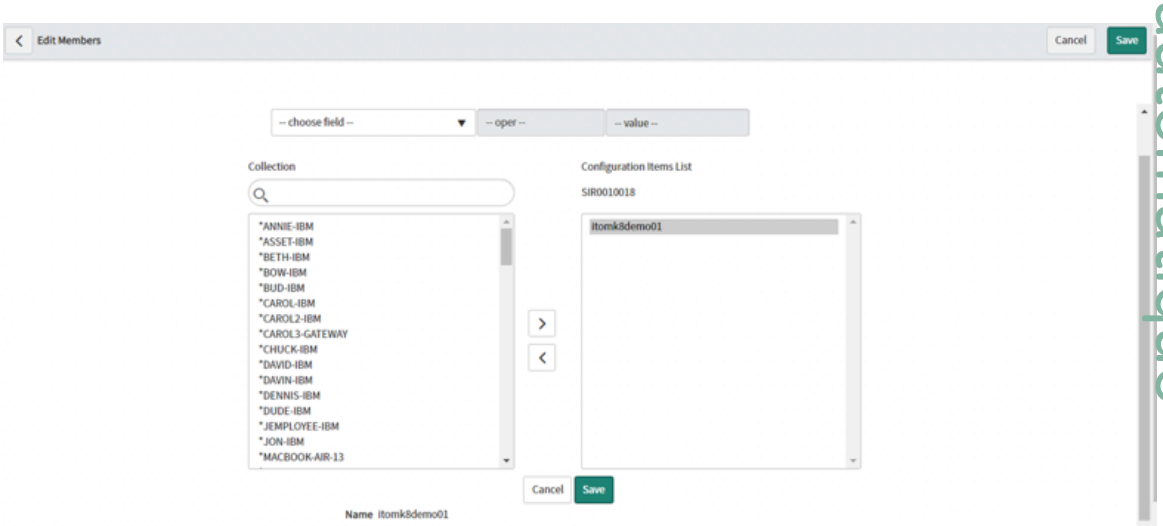
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les FireEye HX informations.
3. Cliquer sur **Afficher toutes les listes connexes** dans la section Listes connexes.
4. Cliquez sur **Élément de configuration** liste connexe.



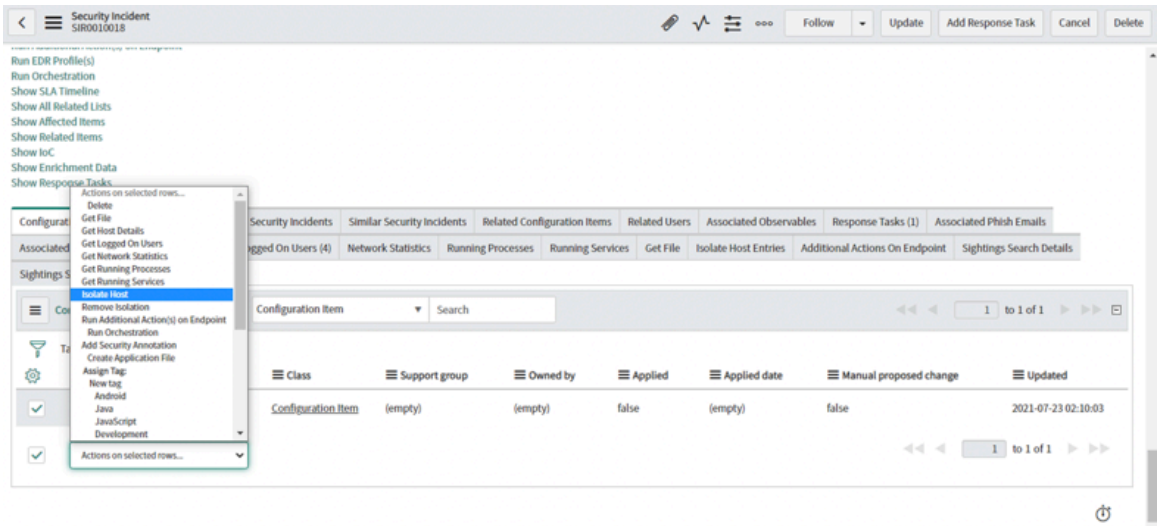
5. Cliquer sur **Modifier** pour ajouter les éléments de configuration disponibles, si elles ne sont pas déjà présentes, puis cliquez sur **Enregistrer**.



6. Sélectionnez le ou les éléments de configuration ajoutés, puis dans Actions sur les lignes sélectionnées, sélectionnez une option.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. L'aptitude sélectionnée est déclenchée manuellement.
8. Examinez la section Notes de travail et activités.
9. Affichez les balises et vérifiez les données dans les listes connexes.

Aptitude d'obtention de fichier FireEye

Les demandes d'acquisition de fichiers demandent à un agent de sécurité du point de terminaison d'obtenir un fichier à partir de son point de terminaison hôte. Les acquisitions de fichiers sont utilisées pour l'analyse statique ou dynamique des compromissions potentielles ou vérifiées, ainsi que pour la conservation des preuves lors d'enquêtes sur les menaces internes. L'aptitude Obtenir un fichier doit être créée en tant que profil distinct.

Avant de commencer

Rôle requis : admin

Déclenchement de l'option Obtenir un profil de fichier et créer un profil d'aptitude FireEye HX avec **Obtenir un fichier** capacité.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner.
3. Cliquer sur **Exécuter le(s) profil(s) EDR**dans la section Liens connexes.
4. Parcourez et sélectionnez Obtenir un profil de fichier dans la liste des profils disponibles.
5. Fournir le **Nom de fichier** et **Chemin d'accès au fichier**.

> **Remarque :** Entrez le nom du fichier pour lequel vous souhaitez acquérir. Spécifiez un nom de chemin d'accès précis ou une autre variable d'environnement Windows appropriée basée sur le chemin d'accès. Vous devez spécifier la lettre du lecteur ou les noms de chemin d'accès. Différents points de terminaison peuvent avoir des mappages de lecteur différents. Si vous spécifiez explicitement un nom de dossier, vous pouvez terminer le chemin d'accès par une barre oblique inverse. Cependant, la barre oblique inverse finale n'est pas obligatoire.

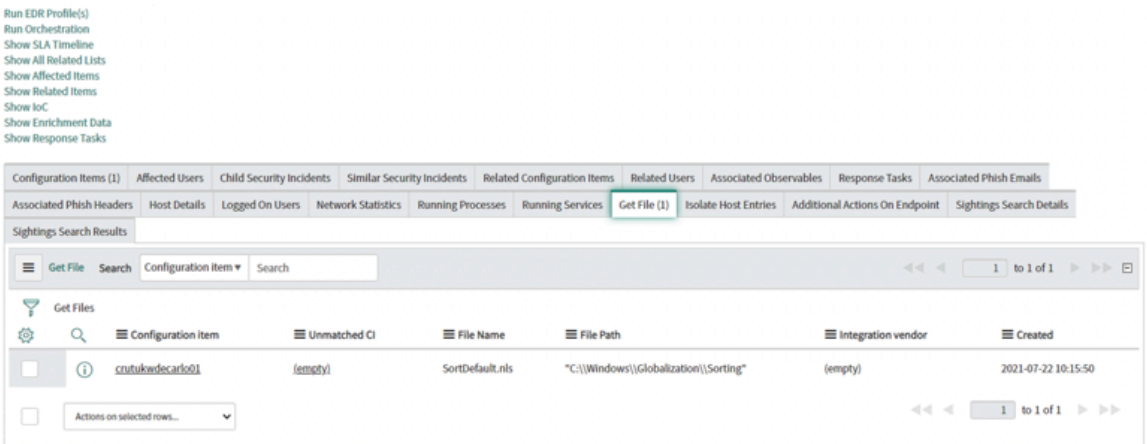
6. Cliquer sur **Envoyer**.
7. Examinez la section Notes de travail et activités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Afficher les balises et vérifier les résultats dans le **Obtenir un fichier** liste connexe.

Remarque : Le profil Obtenir un fichier est maintenant déclenché manuellement.



Pour examiner l'acquisition d'un fichier téléchargé :

- Ouvrez l'acquisition du fichier .zip fichier.
- Entrez le mot de passe requis pour ouvrir le fichier. Le mot de passe peut être consulté en survolant le lien de téléchargement dans FireEye HX la console. Suivez les étapes ci-dessous pour afficher le mot de passe :
  - Connectez-vous à la console FireEye HX.
  - Accédez à la **Acquisitions** et filtrer par type d'acquisition – Fichier.
  - Sélectionnez l'enregistrement souhaité.

    Remarque : Vous pourrez voir les détails du fichier acquis sur l'onglet de droite.

  - Passez la souris sur le **Télécharger** Lien disponible en haut pour obtenir le mot de passe.

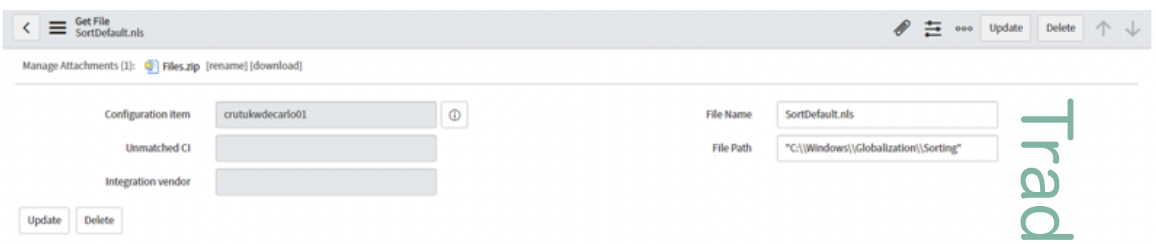
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

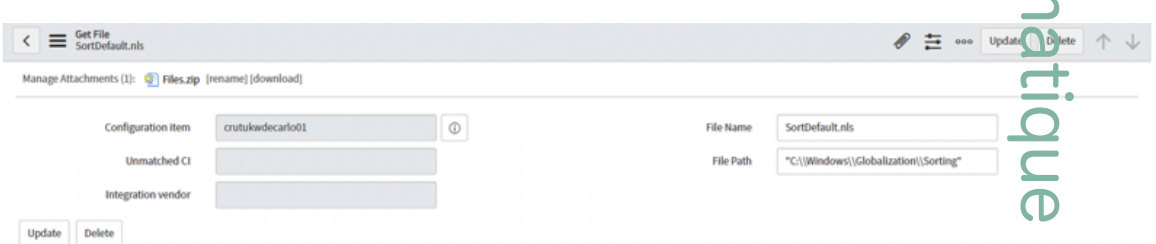
- Ouvrez et examinez les fichiers dans le fichier .zip à l'aide de n'importe quel éditeur de texte ou XML.

Remarque :

- Il est recommandé d'ajouter manuellement le fichier récupéré en tant qu'observable, afin qu'il puisse être suivi en tant que preuve contre l'incident de sécurité. Cela aidera également à visualiser les fichiers à l'avenir, lorsque le mot de passe est oublié ou modifié.
- La taille maximale de fichier prise en charge pour l'action Obtenir un fichier est de 1 024 Mo, et cette valeur peut être configurée en changeant **com.glide.attachment.max_size**, et le délai par défaut est de 60 minutes et peut être configuré à partir de la FireEye HX page Paramètres par défaut.



- L'option Obtenir un fichier peut également être déclenchée à partir de la liste connexe des éléments de configuration.



Traduction automatique

Actions supplémentaires FireEye sur le point de terminaison

L'intégration de FireEye prend en charge l'exécution d'actions supplémentaires au-delà des actions de référence.

Ces actions comprennent l'acquisition de triage et l'acquisition de données. Deux acquisitions de données prêtes à l'emploi sont prises en charge :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Script des détails de l'enquête complète
- Script des détails d'enquête standard

De plus, l'acquisition du triage est également prise en charge prête à l'emploi. Ces trois éléments sont créés par défaut en même temps que la source. Les clients peuvent également créer leurs propres actions, c'est-à-dire des acquisitions de données à partir du module Actions supplémentaires FireEye. [1] La taille maximale de fichier prise en charge pour les actions supplémentaires FireEye est de 1024, et cette valeur peut être configurée en changeant **com.glide.attachment.max_size**, et le délai par défaut est de 120 minutes et peut être configuré à partir de la page Paramètres par défaut de FireEye.

Script des détails de l'enquête complète

Permet de collecter tous les artefacts d'expertise et d'enquête à partir du point de terminaison, mais constitue l'option la plus coûteuse. Cette configuration est idéale dans les situations où il n'y aura qu'une seule fenêtre pour collecter des données à partir du point de terminaison en question, et la possibilité d'acquérir plus de données ne peut être garantie ultérieurement. Utilisez donc cette action avec prudence.

Script des détails d'enquête standard

Active les options les plus courantes pour la collecte d'artefacts d'expertise et d'enquête à partir d'un point de terminaison. Il s'agit du principal outil d'intervention lorsque vous soupçonnez qu'un point de terminaison peut être compromis et que vous devez effectuer une analyse approfondie de ce point de terminaison. Vise à trouver un équilibre entre la collecte des données les plus pertinentes et les plus précieuses tout en évitant les options coûteuses qui peuvent être collectées ultérieurement une fois qu'une enquête plus approfondie s'avère nécessaire.

Acquisition du triage

Les collections de triage contiennent des informations provenant du cache de vérification ainsi que des informations supplémentaires sur les audits d'expertise, telles que l'historique des téléchargements d'URL, l'historique des téléchargements de fichiers, les listes des processus et des ports et les informations système standard. Vous pouvez examiner ces informations lorsqu'un trafic réseau anormal est détecté et vous souhaitez avoir plus de visibilité sur les actions des points de terminaison.

Gestion des scripts d'acquisition de données sur FireEye

Les demandes d'acquisition de données (parfois appelées demandes Live Response) vous permettent d'acquérir toutes les données dont vous avez besoin à partir d'un seul point de terminaison en cours d'exécution. À l'aide de la page Scripts d'acquisition de données de FireEye, vous pouvez créer, modifier, copier et supprimer les scripts d'acquisition de données utilisés pour les demandes d'acquisition de données.

Accéder à la page Scripts d'acquisition de données sur FireEye

Pour accéder à la page Scripts d'acquisition de données :

1. Accédez à l'interface utilisateur web de la sécurité du point de terminaison.
2. Sélectionnez les scripts d'acquisition de données dans le menu Admin.

Création d'un script sur FireEye

Pour créer un script d'acquisition de données :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Sélectionner **Scripts d'acquisition de données** > **Administrateur** de l'interface utilisateur Web de Sécurité du point de terminaison.
2. Cliquer sur **Créer un script**.
3. Entrez un nom pour le nouveau script dans le **Nom du script** champ.
4. Vous pouvez également entrer une description du script.
5. Sélectionnez le système d'exploitation auquel le script s'applique. Vous ne pouvez sélectionner qu'un seul système d'exploitation dans la boîte de dialogue Créer un script.
6. Cliquer sur **Créer** pour démarrer la définition du script.
7. Sélectionner un type de données d'acquisition dans le **Ajouter un type d'acquisition**, puis cliquez sur **Ajouter**. Les options pour le type d'acquisition que vous avez demandé s'affichent à droite de la liste des scripts.
8. Fournissez des valeurs pour les options de type d'acquisition ou utilisez les valeurs par défaut déjà sélectionnées. L'interface utilisateur Web ne vous avertit pas et ne supprime pas les tabulations, les espaces ou les caractères indésirables (tels que \n) dans vos spécifications.
9. Répétez les 2 étapes précédentes pour demander des données supplémentaires pour le script d'acquisition de données. Certains types de données d'acquisition ne sont disponibles qu'une seule fois pour un script, tandis que d'autres peuvent être spécifiés plusieurs fois. Après avoir ajouté un type d'acquisition à un script, la liste des types d'acquisition disponibles dans le **Ajouter un type d'acquisition**la liste déroulante s'ajuste de manière appropriée.
10. Pour supprimer un type de données d'acquisition du script, cliquez sur l'icône x ( ) dans l'onglet Acquisition sur le côté gauche de la page.

Remarque : Cette intégration ne prend pas en charge **Autoriser les modifications avant l'acquisition** lors de la création de scripts. Assurez-vous donc que la case à cocher n'est pas cochée.

Exportation d'un script à partir de FireEye

Vous pouvez exporter un script d'acquisition de données vers un fichier JSON. Pour exporter un script d'acquisition de données :

1. Sélectionner **Scripts d'acquisition de données** > **Administrateur** de l'interface utilisateur Web de la sécurité du point de terminaison.
2. Sélectionnez les scripts d'acquisition de données dans le menu Admin.
3. Sélectionnez le script que vous souhaitez exporter sur le côté gauche de la page.
4. sélectionner **Actions** > **Exporter le script**.
5. Un fichier JSON est téléchargé sur votre ordinateur. Le nom du fichier JSON inclut le système d'exploitation afin que vous puissiez facilement déterminer quels scripts sont destinés à quel système d'exploitation.

Création d'une nouvelle action d'acquisition de données dans le ServiceNow AI Platform

Pour créer une action, procédez comme suit :

1. Accédez à la **Intégration de FireEye** > **Actions supplémentaires FireEye**. La liste Actions supplémentaires FireEye s'affiche.
2. Cliquer sur **Nouveau**. Le formulaire pour la nouvelle action s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Remplissez le formulaire.

Nom de l'action	Nom de l’action FireEye effectuée. Ce nom vous aide à identifier le type d’action et à le décrire.
Achat	Une acquisition obtient les données à analyser. Il s’agit d’un champ en lecture seule, défini par défaut sur Acquisition de données.
Source	Nom de la source FireEye. Seules les sources configurées sont disponibles dans la liste de choix.
Option	Il s’agit d’un champ en lecture seule. Il est renseigné avec l’aptitude Exécuter une ou plusieurs actions supplémentaires
Type d'acquisition	Type d’action d’acquisition à obtenir et à analyser.
Actif	Cela indique que l’action est active.
Exiger l'approbation	Lorsque vous activez l’option Exiger l’approbation, le champ Approbateurs est disponible sur le formulaire. Après avoir soumis une demande, l’approbation du groupe est requise pour terminer la demande.
Balise d'affichage	Type de système d’exploitation tel que Windows, Mac, Linux pour l’ajout de scripts. **Remarque :** Un seul type de système d’exploitation est actuellement pris en charge. Vous pouvez créer une action par système d’exploitation. Pour les autres systèmes d’exploitation, créez de nouvelles actions selon vos besoins.
Scripts	Le script importé de FireEye doit être fourni pour le type de système d’exploitation sélectionné. Un seul script peut être ajouté à chaque type de système d’exploitation.

4. Cliquer sur **Envoyer**.

Déclenchement des acquisitions de données à partir d’un incident de sécurité

Les actions supplémentaires créées peuvent être exécutées via le lien connexe appelé **Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison** sur l’incident de sécurité.

Remarque : Autoriser les modifications avant l’acquisition La fonctionnalité FireEye n’est pas prise en charge pour les actions supplémentaires sur le point de terminaison.

Configurer un profil pour la recherche de perceptions avec l’intégration FireEye

Configurez le profil de recherche de perceptions en suivant la procédure suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur d'incident de sécurité NowPlatform (sn_si.admin)

Chaque fois qu'une source est créée, des configurations de recherche de perceptions individuelles pour cinq types (Fichier, IP (v4), MD5, SHA1 et SHA256) sont créées et désactivées par défaut. Vous devez l'activer avant d'utiliser la recherche de perception. Chaque type d'observable a une requête de recherche différente pour récupérer des observations. Nous lancerons une recherche différente pour chaque type d'observable. La recherche de plusieurs observables pour une recherche de perception n'est pas possible dans FireEye, car elle effectuerait une opération ET sur les observables et le résultat pourrait être inexact.

Remarque : Pour la recherche de perceptions, seules cinq recherches actives peuvent être présentes à la fois. Les autres seront mis en file d'attente et commenceront après la fin de l'une des observations en cours.

Si vous souhaitez créer un nouveau profil de recherche d'observations, suivez les étapes ci-dessous pour en créer un :

Procédure

1. Accédez à la **Intégrations** > **Configuration de la recherche de perceptions**.
2. Cliquer sur **Nouveau**.
3. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom du profil d'aptitude.
Est une recherche enregistrée	Exécutera une recherche enregistrée, par exemple, le champ Nom doit correspondre au nom de la recherche enregistrée.
Source de recherche de perceptions	Définit la source configurée pour l'intégration.
Rechercher	Ajoutez une chaîne de recherche native pour former une requête.
Actif	La requête s'exécute uniquement si elle est active.
Type d'observable	Définit le type de catégorie d'observable.
Nombre maximum d'observables par recherche	Le nombre d'observables avant que la requête de recherche ne soit fractionnée en plusieurs requêtes. Définissez cette valeur sur 1 pour cette intégration.
Paramètres de la recherche de perceptions	Utilisez les paramètres de recherche de perceptions pour définir des requêtes plus complexes qui incluent la logique et d'autres opérateurs pris en charge par le magasin de journaux spécifié.

4. Cliquer sur **Envoyer** pour terminer la configuration.

Invoquer la recherche de perception à partir d'un incident de sécurité

Invoquez la recherche de perceptions à partir d'un incident de sécurité SIR en suivant la procédure ci-dessous.

Traduction automatique

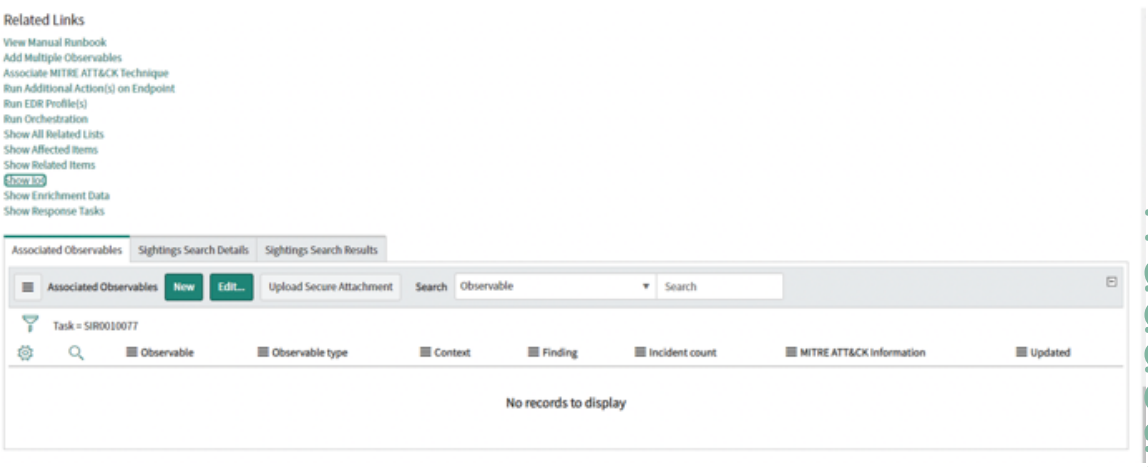
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

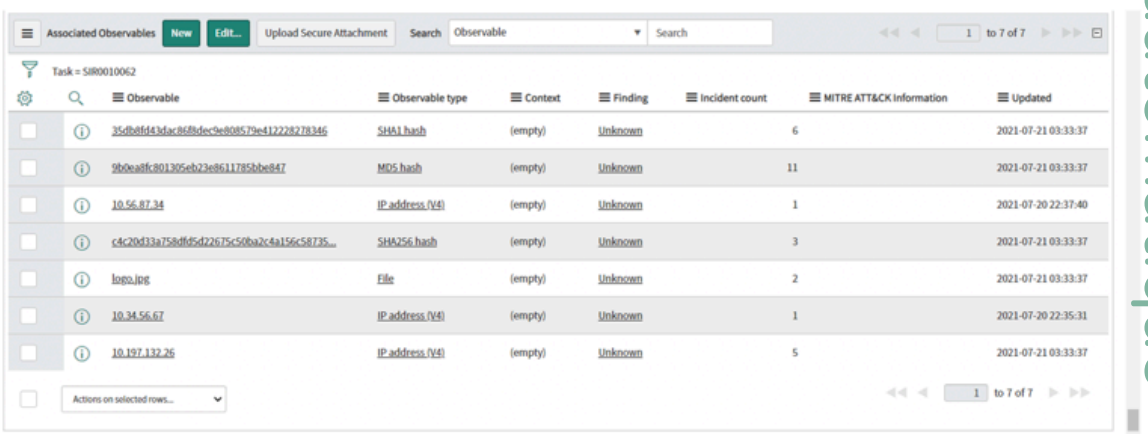
Rôle requis : ServiceNow AI Platform administrateur (sn_si.admin)

Procédure

1. Accédez aux incidents de sécurité.
2. Ouvrez un SIR existant ou créez un nouveau SIR.
3. Cliquez sur Afficher IoC dans les liens connexes.
4. Cliquer sur **Observables associés** listes connexes.



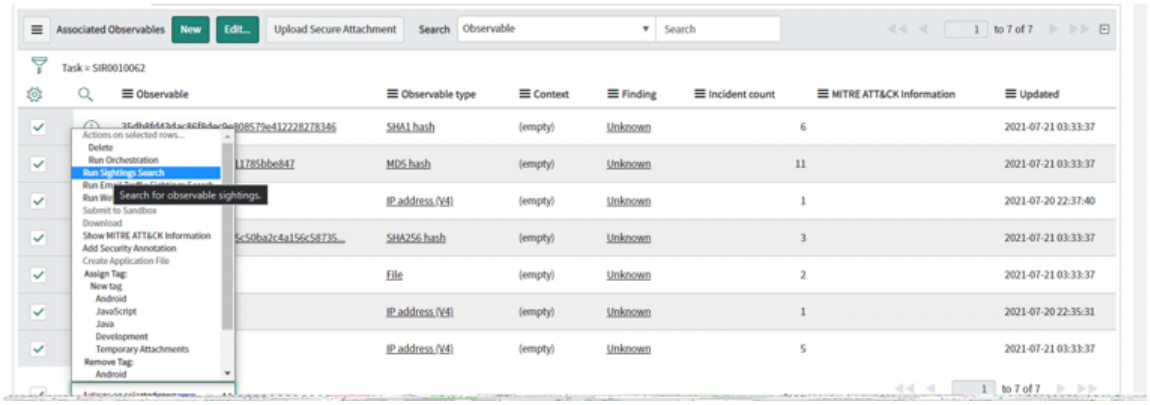
5. Ajoutez des observables existants ou créez-en de nouveaux.



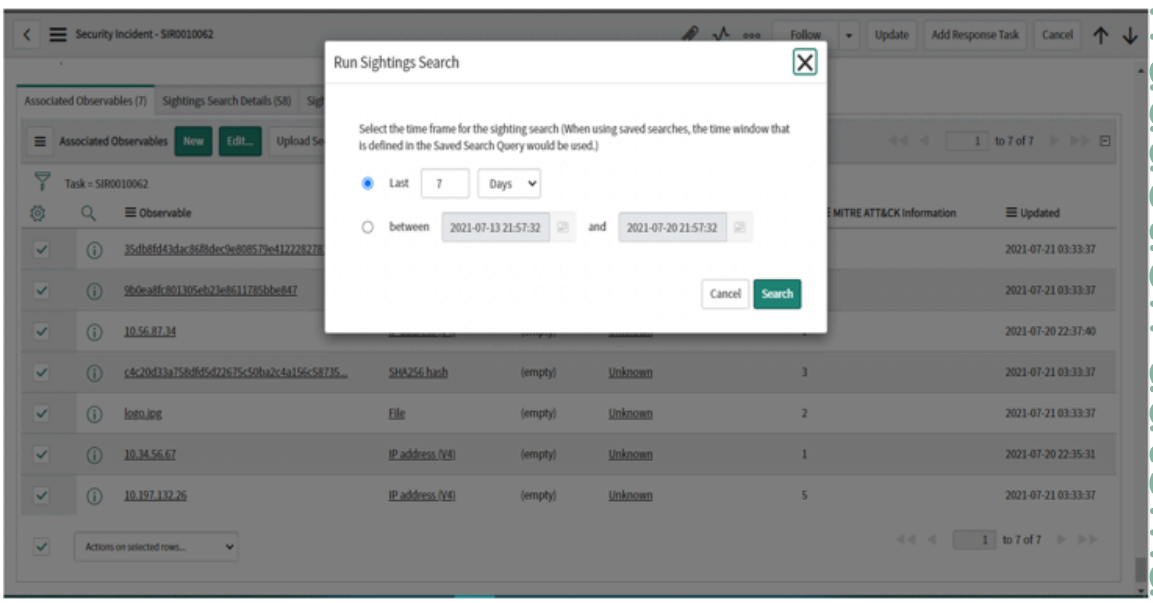
6. Sélectionnez les observables et dans Actions sur les lignes sélectionnées, cliquez sur **Exécuter la recherche de perception**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



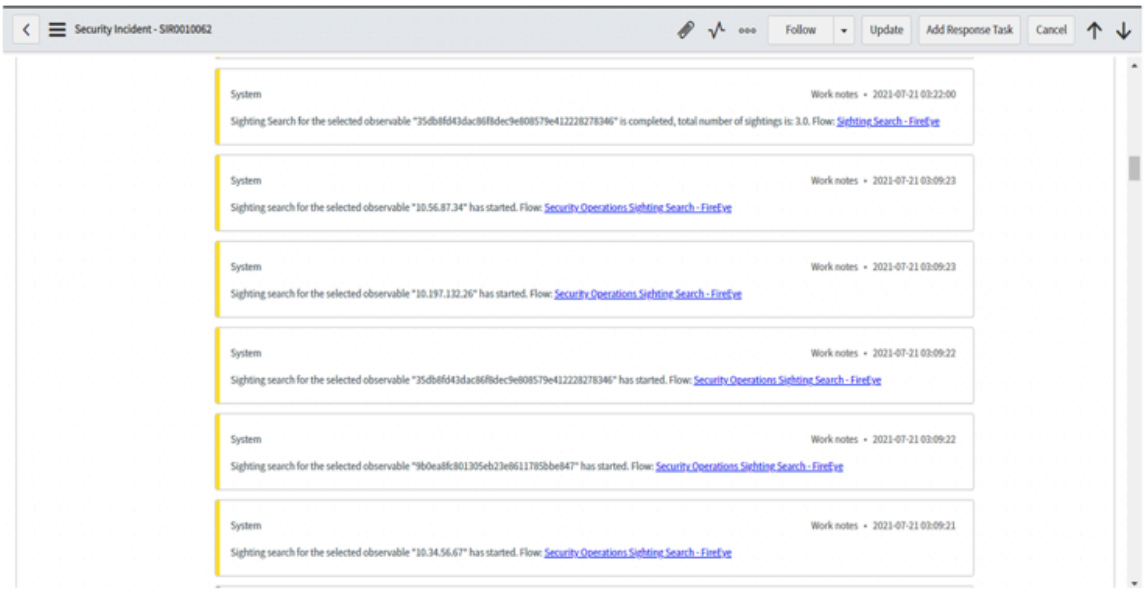
7. Ignorez les entrées de la boîte de dialogue suivante qui demande des données horaires.
   Il y a des valeurs par défaut renseignées. Toutefois, la recherche est effectuée en temps réel et les valeurs de temps sont ignorées pour cette intégration.



8. Vérifiez l’état dans les notes de travail.

Traduction automatique

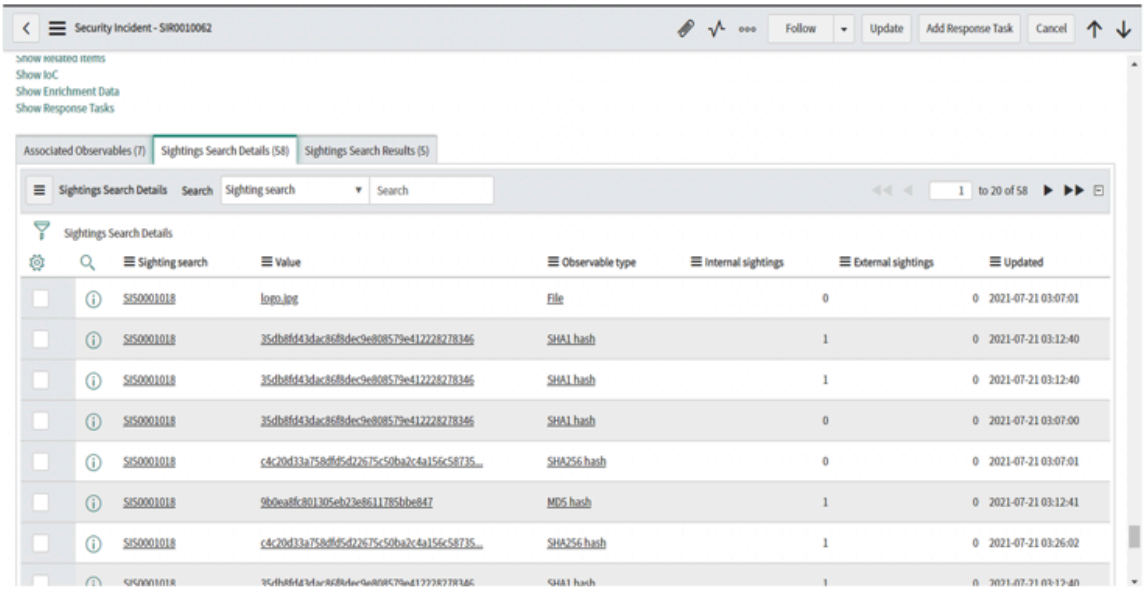
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

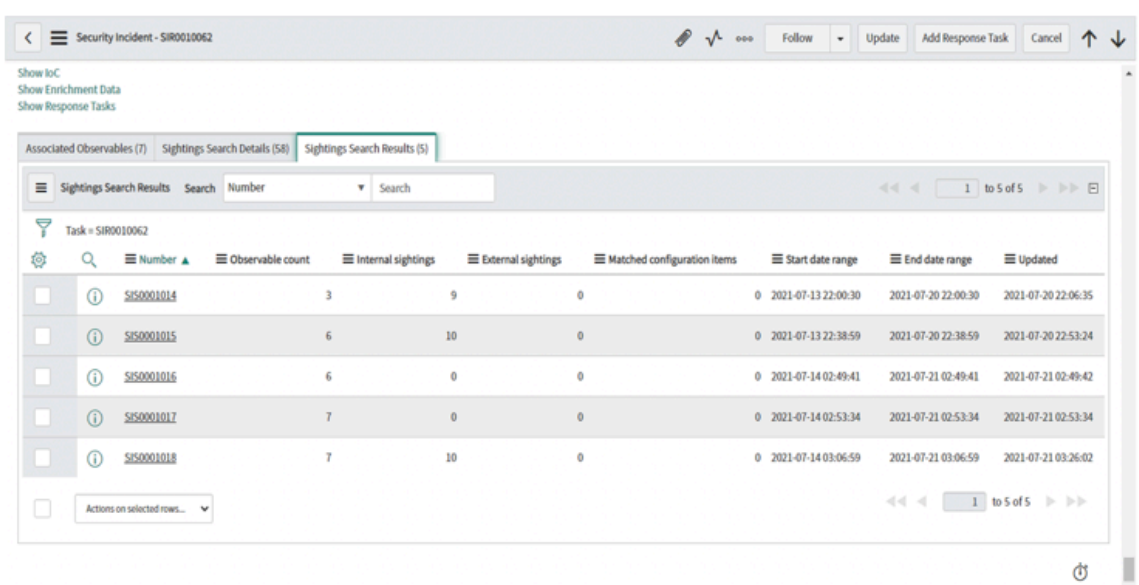


9. Une fois la recherche terminée, vérifiez les résultats et les détails dans les listes connexes.
10. Cliquez sur **Détails de la recherche de perception** pour les détails et **Résultats de recherche de perceptions** pour les résultats de la recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





Traduction automatique

Intégration Have I been pwned?

L'intégration Opérations de sécurité Have I been pwned? vous permet de soumettre des recherches de noms de domaine et d'adresses e-mail afin de déterminer si les données personnelles des utilisateurs ont été compromises par des violations de données.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

- Configuration de l'intégration Have I been pwned?
- Activer

Utiliser

Développer

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

Effectuer des recherches sur les observables
Recherche de menaces : Have I been pwned? flux

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Configuration de l'intégration Have I been pwned?

Have I been pwned? est une ressource gratuite utilisée pour évaluer si une personne a pu être mise en danger en raison de la compromission de son compte en ligne ou d'une violation de données. Il s'intègre facilement à Opérations de sécurité.

Avant de pouvoir utiliser l'intégration Have I been pwned? , vous devez activer le module d'extension. Si nécessaire, vous pouvez également mettre à jour votre certification SSL X509.

Les modules d'extension Réponse aux incidents de sécurité, Renseignements sur les menaces, et Opérations de sécurité Have I been pwned? sont nécessaires pour implémenter l'intégration Opérations de sécurité Have I been pwned? .

Recherche de menaces : Have I been pwned? flux

Le flux de recherche Have I been pwned? de menace effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par Have I been pwned?, ils sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés.

Rôle requis : sn_si_admin

Ce flux est déclenché lorsque Security Operations Integration - Aptitude de recherche de menace vous effectuez une recherche de menace sur un ou plusieurs observables et que l'implémentation Have I been pwned? est sélectionnée. Pour plus d'informations, consultez Effectuer des recherches sur les observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ai-je été pwned flow



Pour en savoir plus sur les activités utilisées par ce flux, reportez-vous à la rubrique Flux d'intégration et activités d'orchestration courants de Security Operations.

Activer

La fonctionnalité Configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration Opérations de sécurité Have I been pwned? . Avant de pouvoir utiliser l'intégration Have I been pwned? , vous devez la télécharger à partir du ServiceNow Store.

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être installé et activé avant de pouvoir utiliser l'intégration Opérations de sécurité Have I been pwned? .

Rôle requis : sn_si_admin

Procédure

Télécharger l'intégration à partir de ServiceNow Store.
Cette intégration prend en charge une API ouverte et ne nécessite pas de configuration supplémentaire. Have I been pwned? peut désormais être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Mettre à jour votre certificat X.509

Si vous avez besoin d'une connexion SSL pour l'intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou ait expiré. Cette tâche est facultative.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Obtenez le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

   b. Cliquez sur l'icône de verrou dans la ligne d'adresse.

   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

   e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

   f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
   Il doit commencer par `----- COMMENCER LE CERTIFICAT -----` et se terminer par `----- CERTIFICAT DE FIN -----`.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Ajoutez le certificat à l'enregistrement du fournisseur d'identité.
   a. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
   b. Sélectionnez le fournisseur d'identité par défaut actif pour lequel vous avez créé le nouveau certificat.
   c. Faites défiler jusqu'à la liste connexe des **certificats X.509** , puis cliquez sur **Modifier**.
   d. Déplacez le certificat nouvellement créé vers la colonne **Sélectionnée** .
6. Cliquez sur **Enregistrer**.
   Les autres champs de l'enregistrement sont générés automatiquement.

Remarque : Si vous avez un certificat qui a expiré, vous devez le supprimer. Pour plus d'informations sur la suppression du certificat expiré, consultez KB0691439 Remplacement d'un certificat SAML arrivant à expiration .

HPE Security ArcSight ESM : intégration de l'analyseur d'e-mails

L'intégration de l'analyseur d'e-mails HPE Security ArcSight ESM est prise en charge à l'aide d'un analyseur d'e-mails qui utilise les notifications par e-mail d'ESM pour créer des incidents de sécurité.

Configurer HPE Security ArcSight ESM : intégration de l'analyseur d'e-mails

HPE Security ArcSight ESM : l'intégration de l'analyseur d'e-mails utilise les notifications par e-mail d'ESM pour diriger les workflows d'enrichissement et de réponse.

Traduction automatique

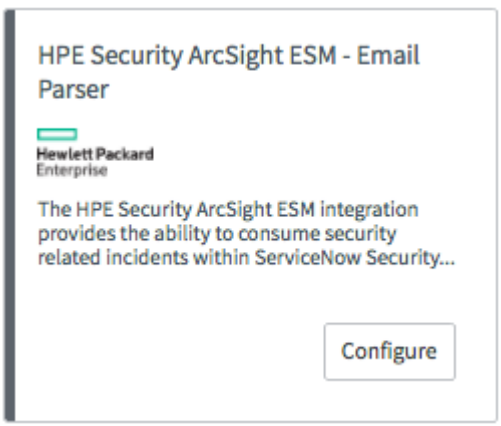
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si_admin

Pourquoi et quand exécuter cette tâche
Un modèle HPE Security ArcSight ESM - Analyseur d'e-mails est fourni pour l'intégration. Il doit être configuré et activé avant l'intégration. La mise à jour de l'analyseur l'active.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.



2. Dans la carte HPE Security ArcSight ESM - Analyseur d'e-mails, cliquez sur **Configurer**.
3. Dans la boîte **de dialogue HPE Security ArcSight ESM - Configuration de l'analyseur d'e-mails** , cliquez sur le lien **Configurer l'analyseur d'e-mails** .
4. Cliquez sur le lien **ArcSight ESM** pour modifier les paramètres dans l'analyseur d'e-mails du modèle fourni.
   Renseignez au minimum le champ L'e-mail provient de . Pour créer votre propre analyseur d'e-mails, reportez-vous à la section Créer des analyseurs d'e-mails dans Security Operations.
5. Cochez la case **Actif** .
6. Cliquez sur **Mettre à jour** dans le formulaire **Analyseur d'e-mails** .
   L'analyseur d'e-mails est actif. Vous n'avez pas besoin de revenir aux **configurations d'intégration**.

HPE ArcSight Logger - Intégration de l'enrichissement des incidents

L'intégration HPE ArcSight Logger - Enrichissement des incidents recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

- Introduction à HPE ArcSight Logger
- Créer des enregistrements de configuration de recherche de perceptions

---

Utiliser

Développer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Exécuter une recherche de perceptions
- Security Operations Integration - Flux de recherche de perceptions
- Opérations de sécurité : ArcSight Logger Flux de recherche de perceptions
- Afficher les détails de la recherche de perceptions
- Afficher les résultats de recherche de perceptions
- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l’écriture d’intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l’intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Introduction à HPE ArcSight Logger

HPE ArcSight Logger diffuse des données en temps réel et les classe dans des journaux spécifiques et s’intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l’intégration d’enrichissement des incidents, vous devez la télécharger à partir de et ajouter l’URL de l’API HPE ArcSight LoggerServiceNow Store et les informations d’identification de connexion.

Avant de commencer

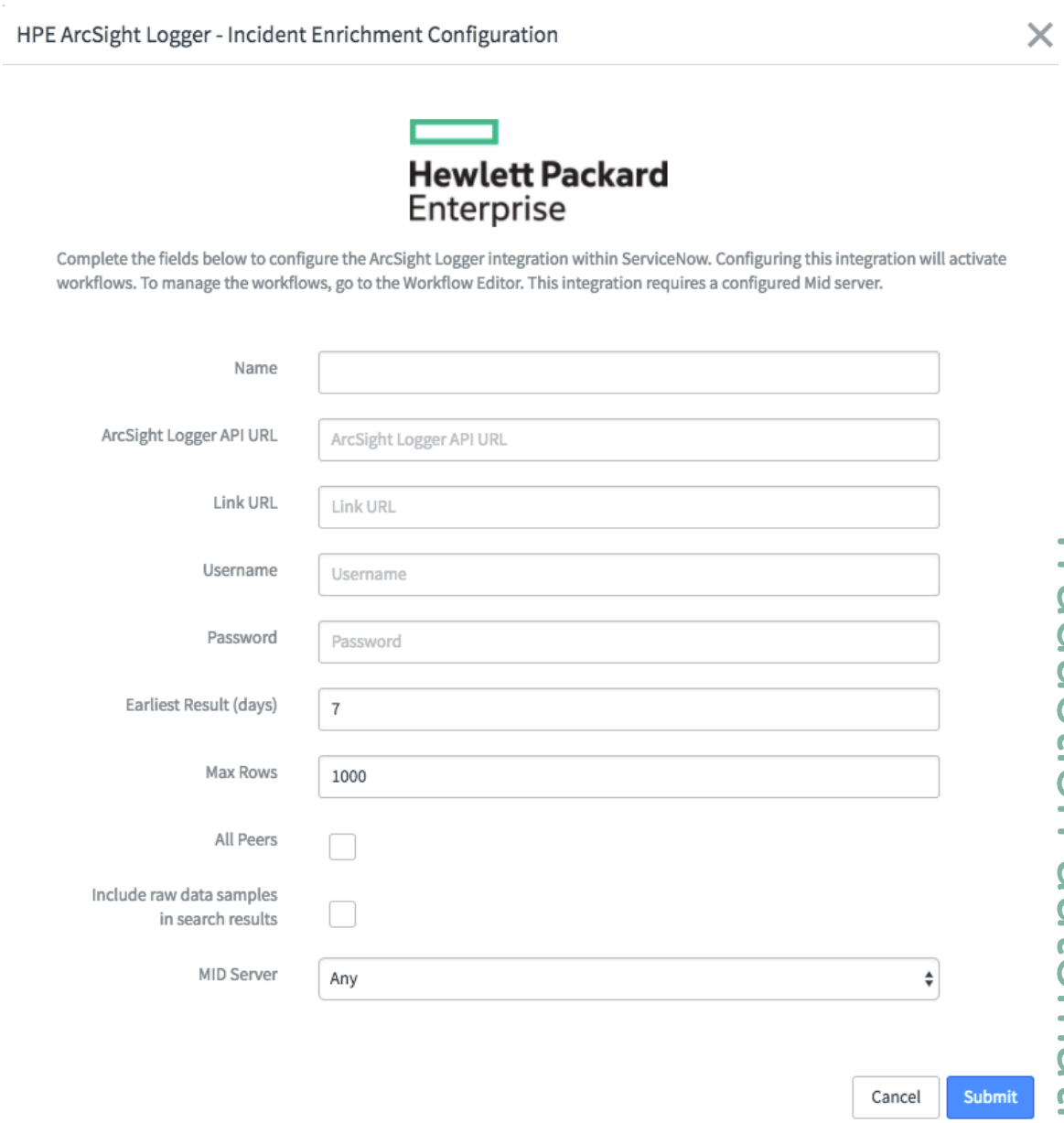
Rôle requis : sn_si_admin

Procédure

1. Télécharger l’intégration à partir de ServiceNow Store.
2. Une fois l’installation terminée, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d’une série de cartes.
3. Dans la carte - Enrichissement de l’incident HPE ArcSight Logger , cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

4. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
URL de base de l'API ArcSight Logger	URL de base que vous avez acquise sur le site HPE Security ArcSight Logger.
URL de lien	[Facultatif] URL de lien qui renvoie à une instance HPE Security ArcSight Logger, le cas échéant.
Nom d'utilisateur	Votre nom d'utilisateur Intel HPE ArcSight Logger .
Mot de passe	Votre mot de passe Intel HPE ArcSight Logger .
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tous les pairs	La valeur par défaut est décochée et ne recherche que l'enregistreur local auquel vous êtes connecté. Lorsque cette option est cochée, elle recherche tous les enregistreurs connectés les uns aux autres.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend de votre paramètre dans la propriété **nombre de lignes de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	**Sélectionnez N'importe lequel** pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

5. Cliquez sur **Envoyer**.
   La carte de configuration d'intégration s'affiche.
6. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
7. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Intégration Hybrid Analysis

L'application Hybrid Analysis fait partie d'une communauté en ligne ouverte dans laquelle les utilisateurs analysent les fichiers et les URL à la recherche de menaces. Vous partagez les résultats et utilisez les recherches de la communauté pour des réponses plus efficaces aux incidents. Lorsqu'elles sont intégrées au ServiceNow AI Platform Opérations de sécurité produit, les renseignements partagés sur les menaces vous fournissent un aperçu supplémentaire de la gravité de certains observables.

L'intégration Hybrid Analysis effectue des recherches de menaces sur les observables suivants :

- Hachages de fichiers
- Adresses IP
- URL

Le flux recherche de nouveaux observables à mesure qu'ils arrivent dans des incidents de sécurité. Si les observables sont d'un type reconnu par l'intégration de l'API, ils sont évalués. Les observables considérés comme malveillants sont balisés.

Installer et configurer

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que l'application s'intègre Hybrid Analysis correctement à ServiceNow AI Platform Opérations de sécurité.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles et requis ServiceNow AI PlatformRéponse aux incidents de sécurité .	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur (admin) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration et vérifie les résultats attendus. Ce rôle a également accès au Opérations de sécurité module et affecte le rôle sn_si.analyst.
Procurez-vous une clé API.	Visitez le site Web d'Hybrid Analysis pour plus d'informations sur les clés API et pour créer un compte : Site Web d'Hybrid Analysis . La configuration nécessite que vous saisissiez les clés API.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Pour la version Madrid et les versions de famille ultérieures, le module d'extension com.snc.si_dep est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications. Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour assurer une installation fluide : **1.** Cadre de travail d'intégration de sécurité **2.** Security Support Common **3.** Orchestration du support de sécurité **4.** Security Incident Response Pour en savoir plus sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

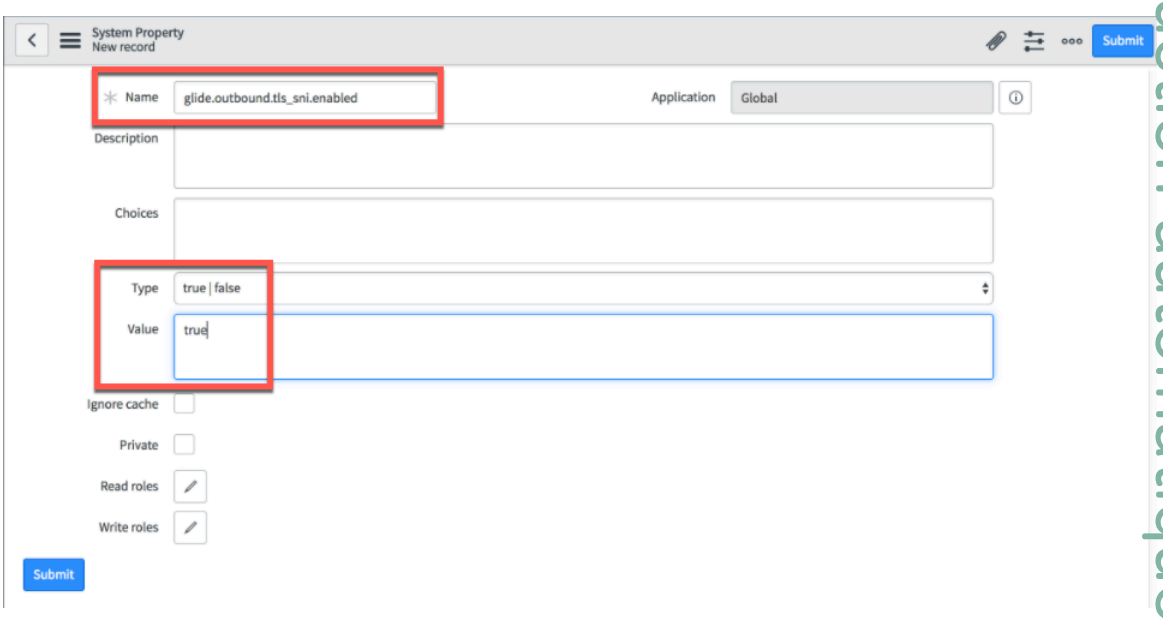
Pourquoi et quand exécuter cette tâche

Procédez comme suit pour mettre à jour les propriétés système, ainsi que pour installer et configurer l'intégration.

Procédure

1. Dans le filtre de navigation, saisissez `sys_properties.list`, puis appuyez sur la touche **Entrée**.
   La liste **Propriétés système** s'affiche.
2. Cliquez sur **Nouveau**.
   Un nouvel enregistrement s'affiche.
3. Renseignez les champs ou sélectionnez les valeurs répertoriées dans la table suivante et cliquez sur **Soumettre**.

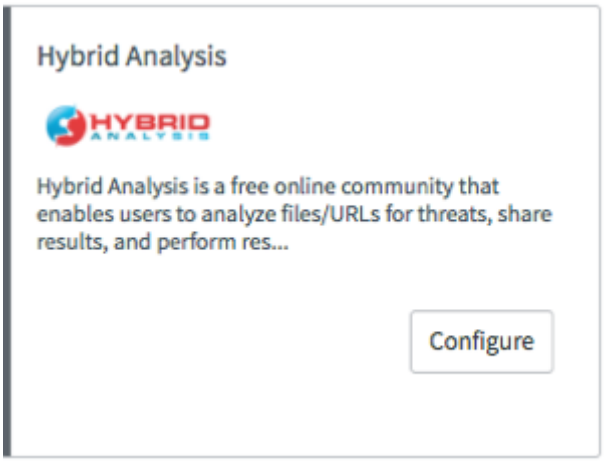
Nom de champ	Valeur
Nom	glide.outbound.tls_sni.activé
Type	Sélectionner **vrai l faux**
Valeur	true



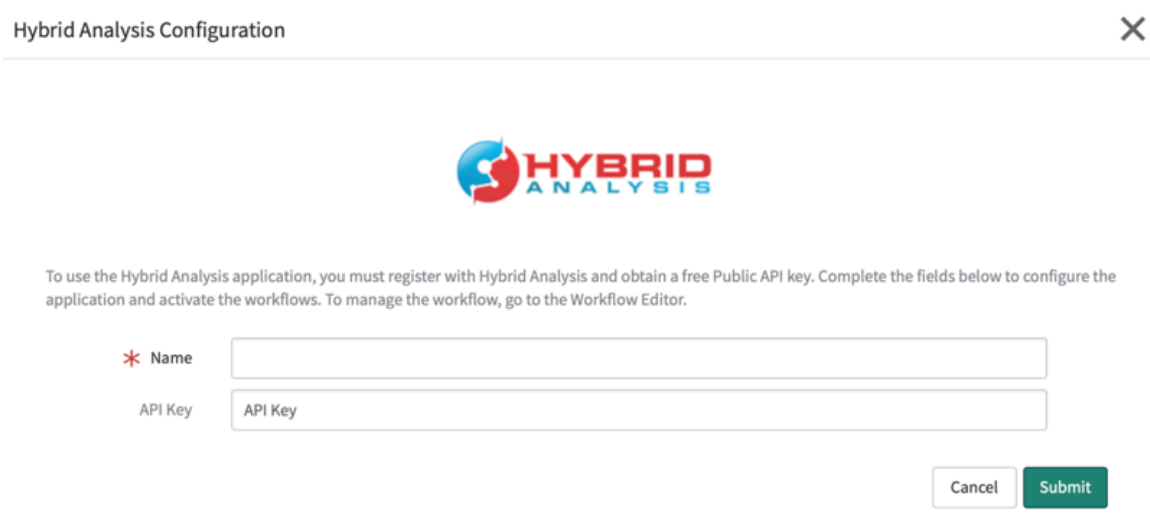
4. Si vous n'avez pas installé l'application pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes d'installation.
5. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la Hybrid Analysis tuile.
6. Cliquez sur **Configurer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Dans la boîte de dialogue **Configuration d'Hybrid Analysis** , entrez la clé API que vous avez obtenue sur le Hybrid Analysis site Web et cliquez sur **Soumettre**.



8. Vérifiez la réussite de la configuration.
   La configuration est terminée avec succès à moins qu'un message d'erreur ne s'affiche.

   Trouble?

   Si un message d'erreur s'affiche pendant la configuration, la clé API Hybrid Analysis peut être non valide.

Vérifier les résultats attendus

Les observables sont générés automatiquement par un incident de sécurité et analysés par l'application. Localisez les résultats de la recherche sur l'incident de sécurité pour vérifier que la recherche de menaces a été exécutée avec succès. Affichez également les données brutes et exécutez des recherches de menaces sur les observables enfants.

Avant de commencer

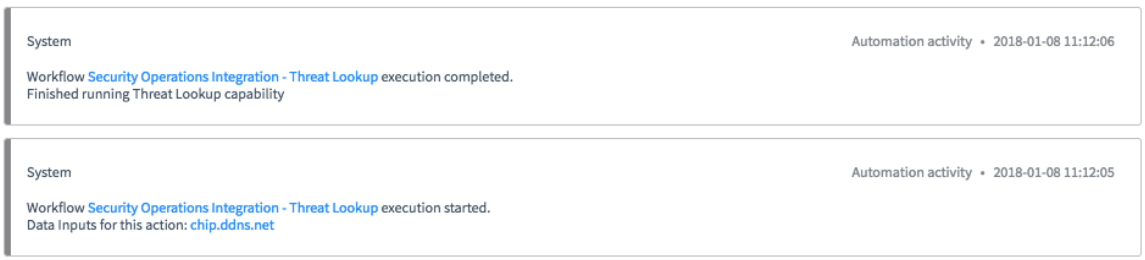
Rôle requis : sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez l'enregistrement d'incident de sécurité avec lequel vous travaillez et vérifiez que la recherche a été exécutée avec succès.

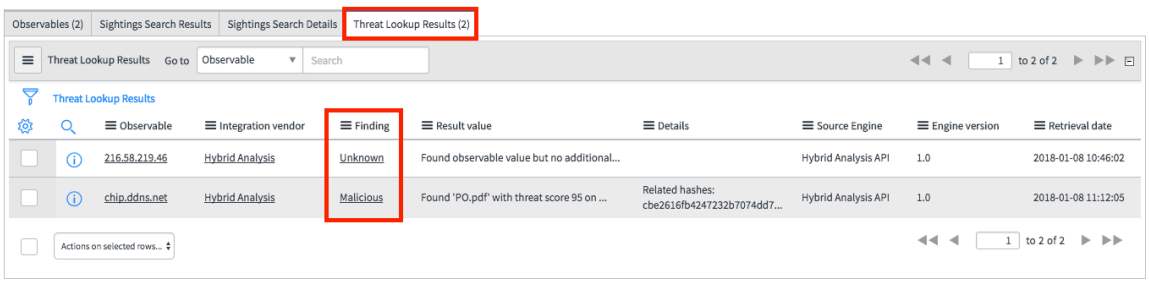


   Une fois l'application configurée, le flux se lance automatiquement lors de la création de l'incident. L'état d'exécution et d'achèvement de la recherche est ensuite affiché dans les notes de travail de l'incident de sécurité.

2. Passez en revue les notes de travail pour en savoir plus sur la façon de procéder si vous ne pouvez pas vérifier que la recherche a été effectuée avec succès.

3. Accédez au bas de l'enregistrement d'incident de sécurité et cliquez sur le lien connexe **Afficher toutes les listes connexes** pour afficher les résultats.

   Remarque : Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres système. Dans le coin supérieur droit de la bannière, cliquez sur l'icône d'engrenage Paramètres. Dans la boîte de dialogue **Paramètres système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que **Formulaires à onglets** et **Avec le formulaire** sont sélectionnés.

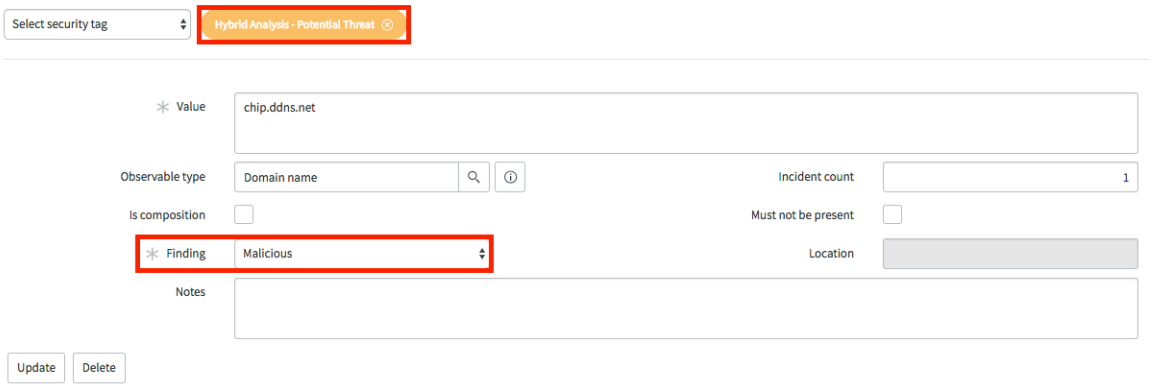


   L'onglet Résultats de la recherche de menace affiche les résultats de la recherche au bas de l'enregistrement d'incident de sécurité. Notez que la colonne **Recherche** affiche Inconnu pour les enregistrements qui ne sont pas déterminés comme malveillants. Pour les résultats correspondant à malveillant, la colonne **Recherche** affiche malveillant.

4. Dans la colonne **Observable** , cliquez sur un observable pour ouvrir l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

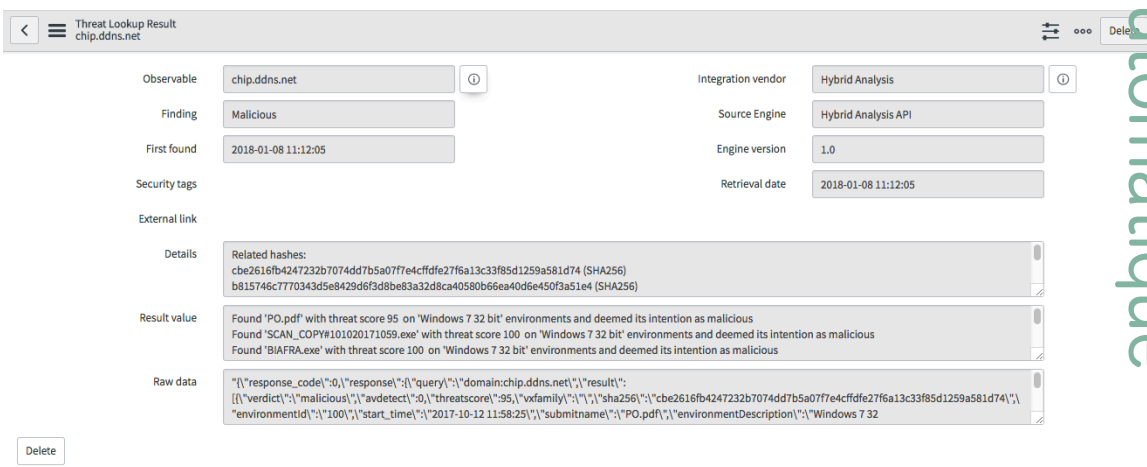


Pour les recherches correspondantes malveillantes, le champ **Recherche** affiche Malveillant et l'observable est étiqueté avec la Renseignements sur les menaces source qui l'a trouvé malveillant, dans ce cas, l'intégration Hybrid Analysis .

5. **Facultatif :** Suivez les étapes pour afficher les données brutes, afficher une liste d'observables enfants et exécuter une recherche de menace sur les observables enfants sélectionnés.

   a. Revenez à l'incident de sécurité et, dans **l'onglet Résultats de la recherche de menace, cliquez sur l'icône d'informations** bleues en regard d'un observable.

   b. Dans la fenêtre qui s'affiche, cliquez sur **Ouvrir l'enregistrement** pour afficher les données.
   À partir de tous les observables visibles dans les données brutes affichées à partir de la recherche, l'intégration Hybrid Analysis crée également des observables enfants ou connexes.



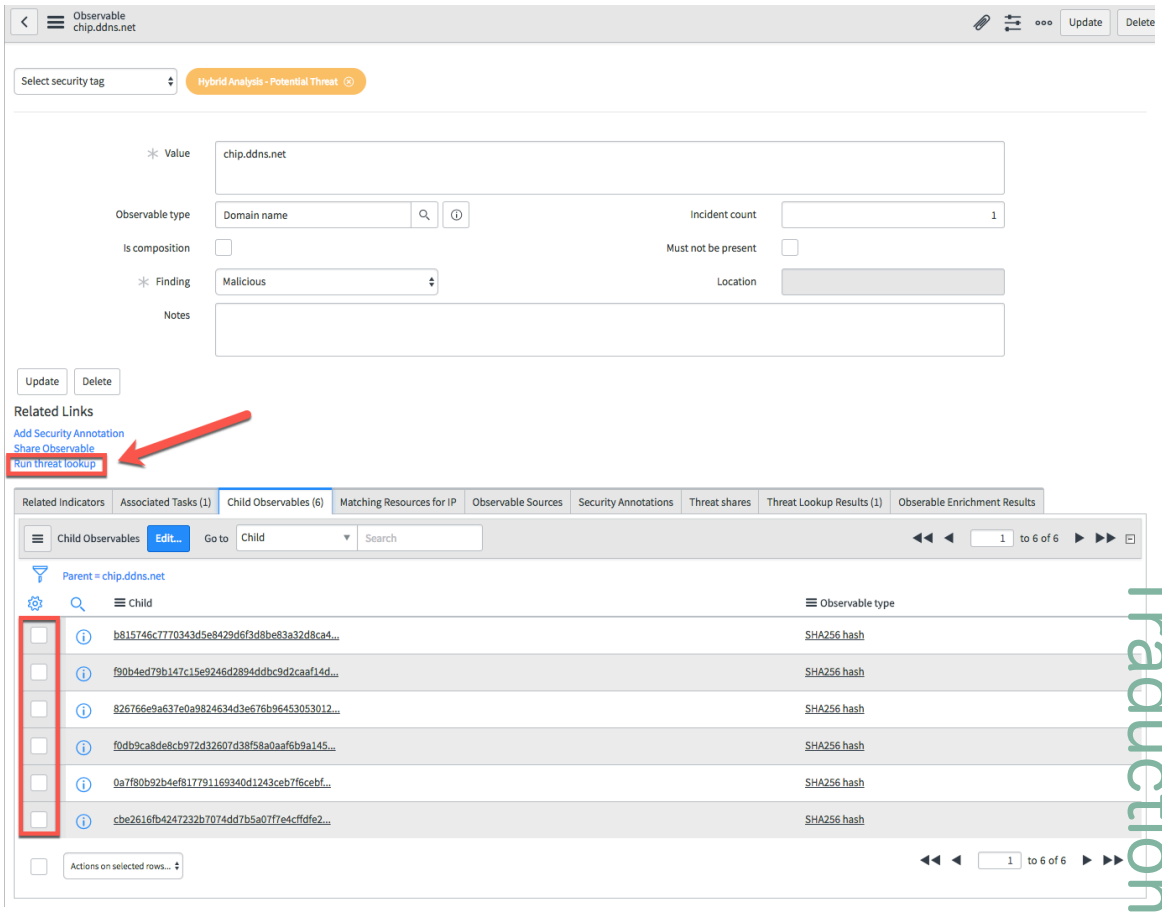
   Le lien créé par l'API, les données brutes et les autres informations s'affichent.

   c. Revenez à l'incident de sécurité et cliquez sur le lien connexe **Afficher l'IoC** .
   Les observables enfants sont affichés dans l'onglet **Observables enfants** de l'incident de sécurité, car la recherche a trouvé un lien existant entre ces observables connexes et l'observable initialement soumis.

   d. Cliquez sur le champ en regard d'un observable dans la colonne **Enfant** pour le sélectionner, puis sur le lien connexe **Exécuter une recherche de menace** pour effectuer une recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Dans la boîte de dialogue qui s'affiche, vérifiez que l'intégration Hybrid Analysis est sélectionnée, puis cliquez sur **Soumettre**.

f. Dans les notes de travail, vérifiez que la recherche a été exécutée avec succès et, dans **l'onglet Résultats de la recherche de menace de l'incident** de sécurité, localisez les résultats de la recherche pour les observables enfants.

Trouble?

Si vous ne voyez pas de résultats sous **l'onglet Résultats de la recherche de menace** , vérifiez que l'observable est d'un type pris en charge pour la recherche par l'intégration.

(Facultatif) Joindre manuellement un observable pour Hybrid Analysis

Vous pouvez joindre manuellement des observables lorsque vous souhaitez effectuer des recherches de menaces sur des observables qui ne sont pas joints à un incident de sécurité lors du déclenchement de l'événement initial. En outre, vous pouvez effectuer cette tâche lorsque vous souhaitez obtenir plus d'informations sur un observable connexe.

Avant de commencer

Vérifiez que l'observable est d'un type pris en charge par l'intégration. L'intégration effectue des recherches sur les types d'observables suivants :

- Hachages de fichiers
- Adresses IP
- URL

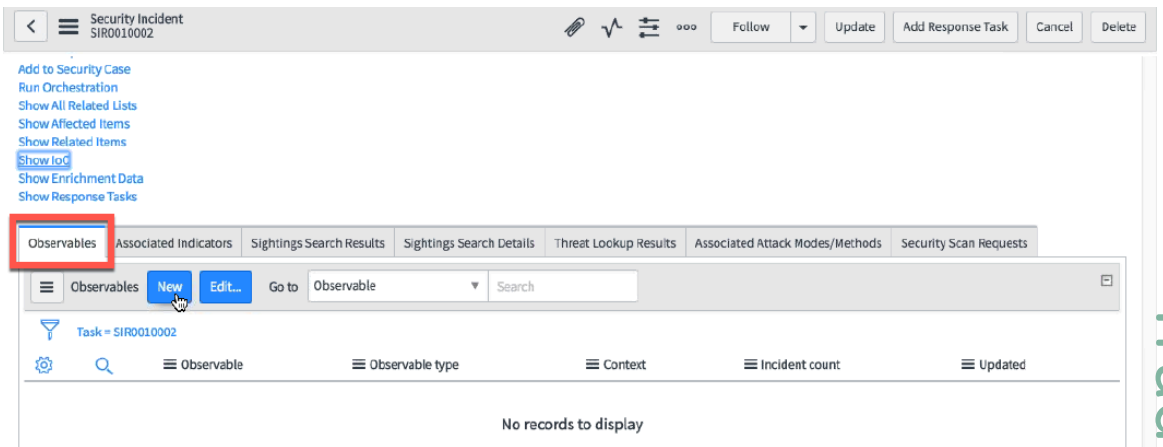
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_si.analyst

Procédure

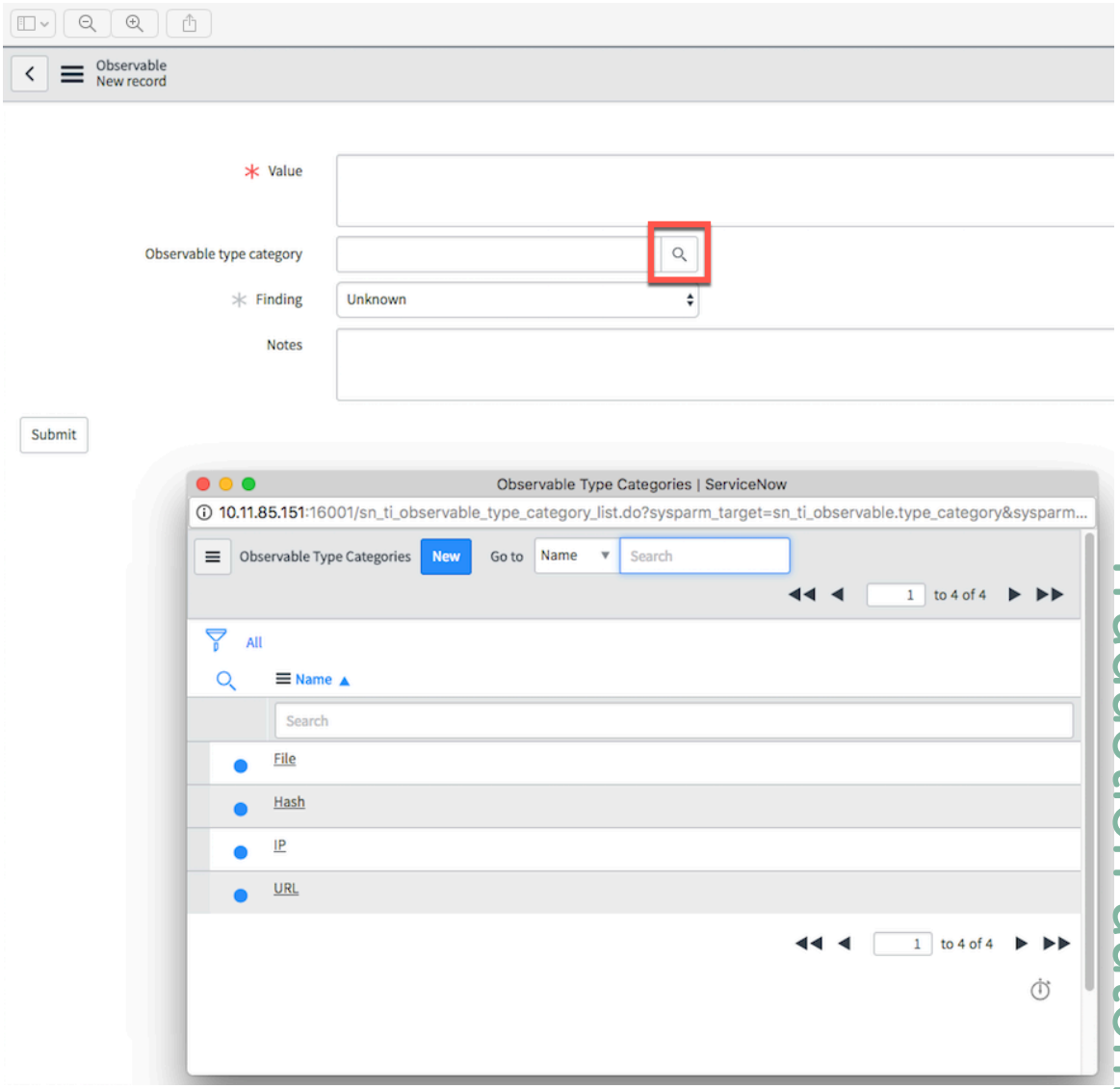
1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents** et ouvrez un incident de sécurité auquel vous souhaitez joindre l'observable.
2. Sur l'incident de sécurité ouvert, cliquez sur le lien **Afficher l'IoC**dans les **liens connexes**.



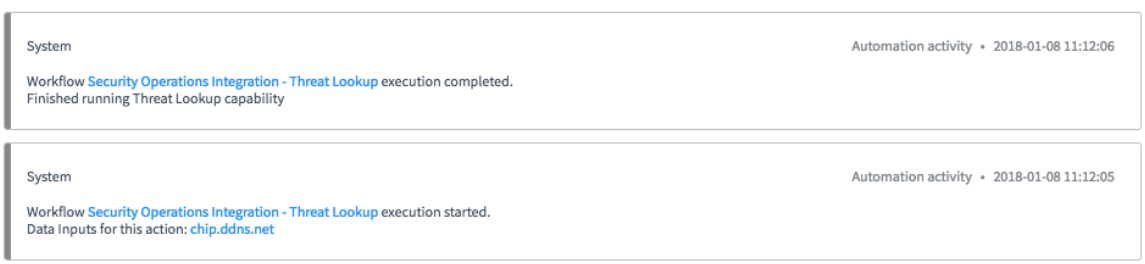
3. Dans l'onglet **Observables** , cliquez sur **Nouveau**.
   Le formulaire Observable s'affiche.
4. Dans le champ **Valeur** , saisissez un observable (hachage de fichier, adresses IP ou URL).
5. Cliquez sur l'icône de recherche puis, dans la boîte de dialogue **Catégories de type d'observable** , cliquez sur le type d'observable souhaité dans la liste pour remplir le champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



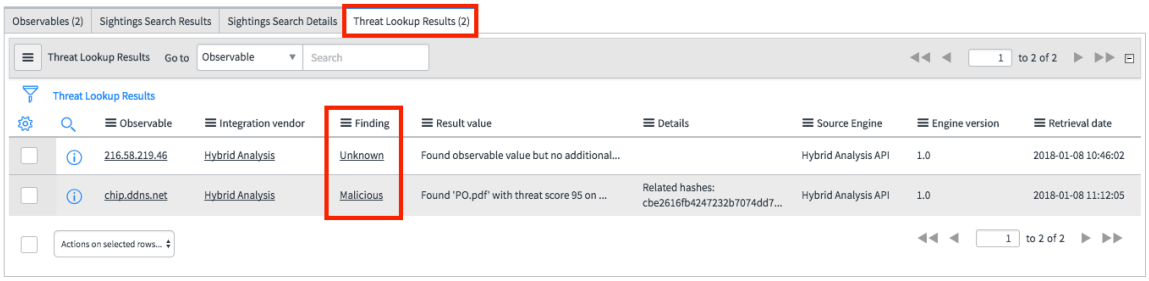
6. Cliquez sur **Envoyer**.
   Le flux se lance et recherche le nouvel observable. L'état d'exécution et d'achèvement est affiché dans la section des notes de travail de l'enregistrement d'incident de sécurité.
7. Accédez à votre incident de sécurité et passez en revue les notes de travail.



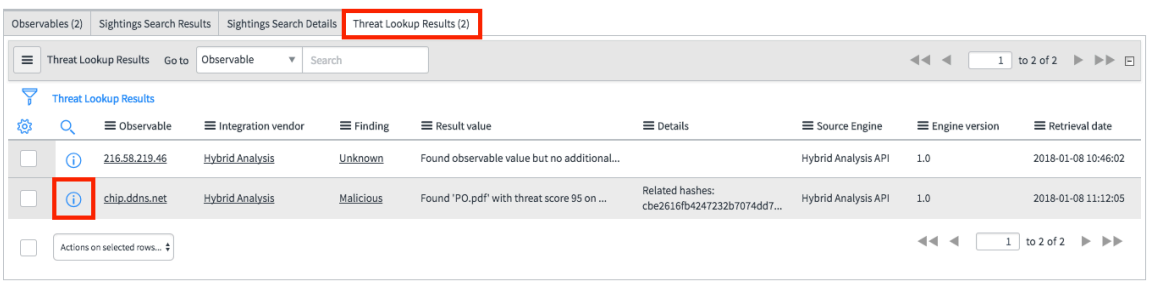
8. Au bas de l'enregistrement, cliquez sur le lien connexe **Afficher toutes les listes connexes** .
9. Cliquez sur **l'onglet Résultats de la recherche de menace** pour afficher les résultats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Dans la colonne **Observable** , cliquez sur l'icône d'information bleue en regard d'un observable donné pour obtenir plus d'informations et des données brutes.



11. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement** pour afficher les données brutes et plus de détails.
    Vous pouvez également joindre un observable existant à l'enregistrement d'incident de sécurité.
12. **Facultatif :** Une fois l'onglet **Observables** sélectionné, cliquez sur **Modifier**.
13. **Facultatif :** Dans le formulaire **Modifier les membres** qui s'affiche, déplacez un observable existant de **Collection** vers **Liste des observables** , puis cliquez sur **Enregistrer**.
    Vous êtes renvoyé à l'incident de sécurité.
14. Dans la colonne située tout à gauche, sélectionnez les observables sur lesquels vous souhaitez exécuter la recherche, puis dans la liste de choix **Actions sur les lignes sélectionnées...** , sélectionnez **Exécuter une recherche de menace**.
    Un message s'affiche en haut de l'enregistrement indiquant que la demande est en cours de traitement.
    Vérifiez que la recherche a été exécutée avec succès.

Trouble?
Passez en revue les notes de travail pour plus d'informations et sur la procédure à suivre si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

IBM QRadar Offense Ingestion Intégration

L'intégration IBM QRadar Offense Ingestion vous permet de récupérer IBM QRadar automatiquement les infractions et de les convertir en incidents de sécurité et d'activer des actions de réponse automatisées.

Cette intégration prend en charge les éléments suivants :

- Découverte des IBM QRadar infractions qui sont candidates à des incidents de sécurité
- Extraction des événements ou flux récents associés à une infraction.
- Suivez périodiquement les mises à jour clés des infractions.
- Mappage des champs d'infraction, d'événement et de flux aux champs d'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vue préliminaire des champs mappés.
- Configurez des ingestions programmées d'infractions pour créer des incidents de sécurité périodiquement.
- Fermez les infractions lorsque les incidents de sécurité sont fermés.

Installer et configurer l'application pour l'intégration de l'ingestion d'infractions ServiceNowIBM QRadar

Avant d'exécuter l'intégration sur votre ServiceNow AI Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre correctement aux Réponse aux incidents de sécurité produits sur Opérations de sécurité votre ServiceNow AI Platform instance.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si vous n'avez pas installé l'application IBM QRadar à partir de pour ServiceNow Store l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la IBM QRadar tuile.
3. Pour configurer l'application, cliquez sur **Nouveau**.
4. Sinon, si un bouton **Configurer** est affiché sur une tuile, cliquez dessus pour modifier une configuration existante.
5. Dans la boîte **de dialogue Configuration des ingestions d'infractions** qui s'affiche, renseignez les champs.

Champ	Description
Nom	Nom de la console ou de l'instance IBM QRadar-IBM QRadar utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge.
URL de base de l'API IBM QRadar	URL d'hôte de votre IBM QRadar instance. **Remarque :** Vous devez saisir uniquement l'URL et le numéro de port ici. Par exemple, https://ibm-qradar.com:8443. Si le numéro de port est 443, il n'est pas nécessaire de le saisir explicitement.
URL du tableau de bord IBM QRadar	URL du tableau de bord ou de IBM QRadar la console. Cette URL est utilisée pour construire automatiquement les liens hypertexte pour les infractions dans le tableau de IBM QRadar bord. Entrez uniquement l'URL de l'hôte, par exemple https://qradar.com. N'incluez pas le .jsp dans l'URL, par exemple, https://

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

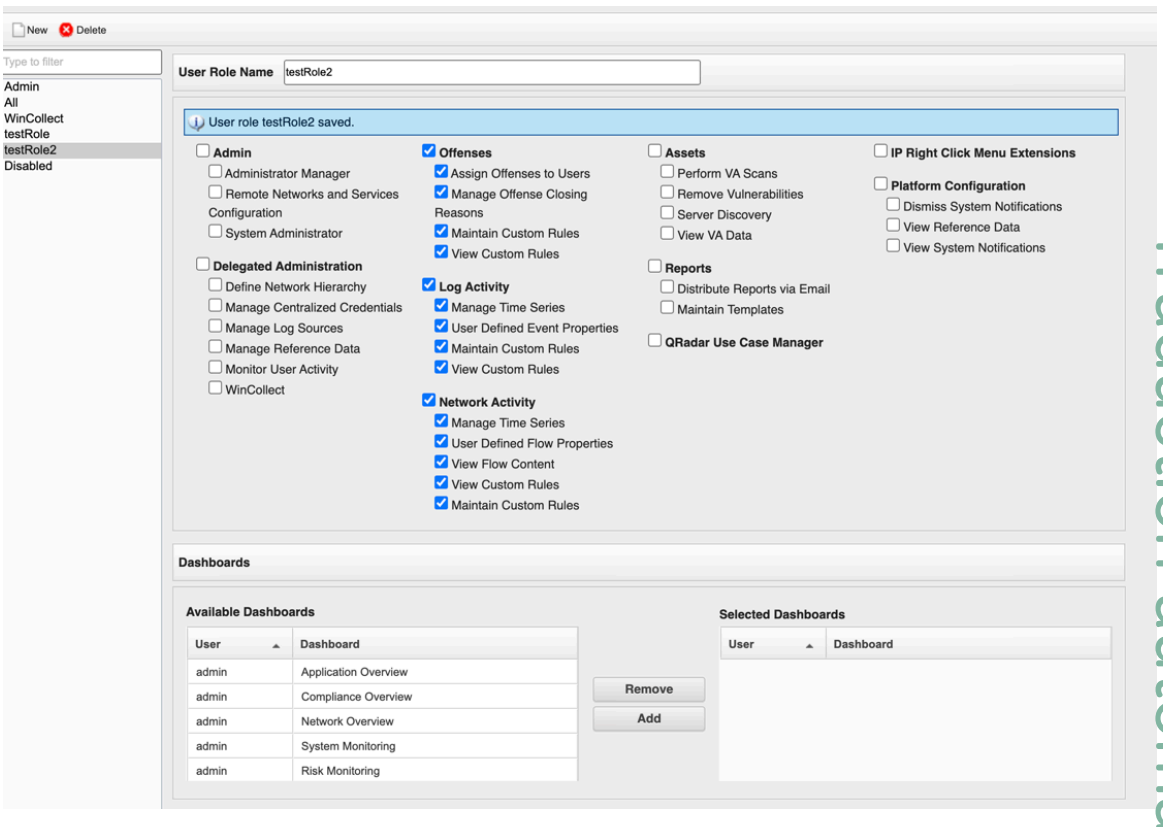
Champ	Description
	qradar.com/console/qradar/jsp/QRa–dar.jsp format n'est pas valide. **Remarque :** Si l'URL du tableau de bord n'est pas disponible, entrez l'URL de base de l'API IBM QRadar ici.
IBM QRadar Version de l'API	Les versions 10 et supérieures sont prises en charge.
IBM QRadar Jeton de service autorisé API (sur site)	Le IBM QRadar jeton de service autorisé est utilisé pour l'authentification. Le jeton de service autorisé doit avoir les rôles d'utilisateur minimum suivants : **Infractions**, **Activité du journal** et **Activité du réseau** , ainsi qu'un profil de sécurité utilisateur qui n'a aucune restriction. Pour générer le jeton de service autorisé, procédez comme suit : ○ Dans la IBM QRadar console, accédez à l'onglet **Administrateur** et cliquez sur **Services autorisés**. ○ S'il existe un jeton de service autorisé valide, vérifiez la date d'expiration et utilisez-le. Si un jeton de service autorisé n'est pas disponible, procédez comme suit : ○ Dans , IBM QRadar accédez à l'onglet **Administrateur** et cliquez sur **Service autorisé**. ○ Cliquez sur **Ajouter un service autorisé** et créez un jeton avec le rôle d'utilisateur et le profil de sécurité. Assurez-vous de spécifier une date d'expiration pour une longue période de validité.
IBM QRadar Jeton de service autorisé API (pour QRoC)	Si vous utilisez IBM QRadar on Cloud (QRoC), utilisez l'application en libre-service pour générer le jeton de service autorisé avec le rôle d'utilisateur administrateur et le profil de sécurité administrateur pour l'authentification.
Déploiement sur site	Désactivé par défaut. Si cette option est activée, vous devez spécifier un nom d'application MID. Si vous utilisez IBM QRadar dans le cloud (QRoC), vérifiez que la case est décochée.
Nom de l'application MID	Spécifiez une application de Serveur MID configurée dans votre environnement. Si vous n'avez pas configuré d'application de Serveur MID, vous devez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

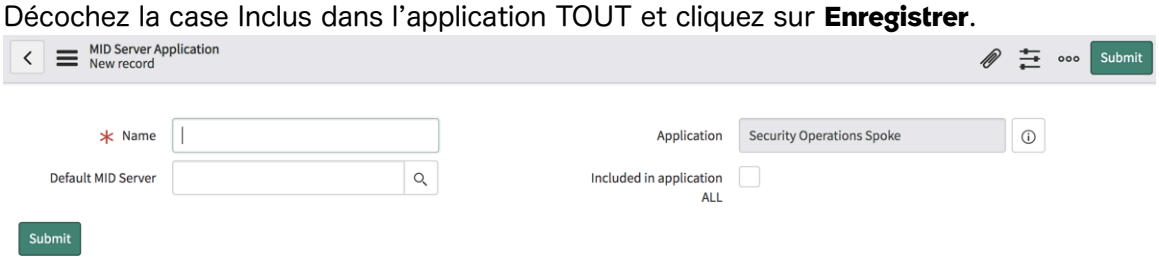
Champ	Description
	créer une nouvelle application de Serveur MID pour cette intégration. **Remarque :** L'application Serveur MID ne peut être configurée que par les utilisateurs ayant le rôle d'administrateur système.

Rôles d'utilisateur minimum



Pour créer une application de Serveur MID, procédez comme suit :

- Accédez à la **Serveur MID** > **Applications** et cliquez sur **Nouveau**.
- Entrez un nom pour l'application de Serveur MID et sélectionnez un serveur MID à utiliser par défaut.
- Décochez la case Inclus dans l'application TOUT et cliquez sur **Enregistrer**.

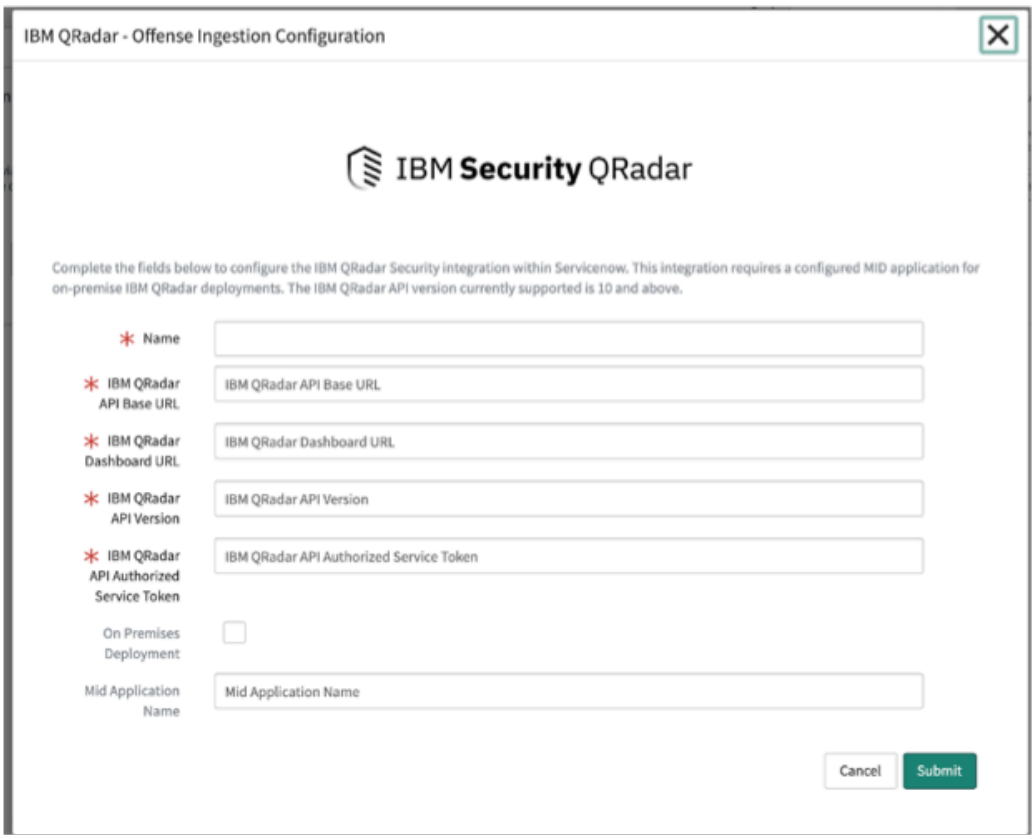


- Cliquez sur **Modifier**. Dans la page **Modifier les membres** , sélectionnez tous les serveurs MID disponibles, déplacez-les vers la liste des serveurs MID, puis cliquez sur **Enregistrer**. En fonction de la disponibilité, l'un des MID Servers configurés avec l'application MID Server est utilisé.

6. Entrez les détails de la configuration et indiquez l'application Serveur MID que vous avez créée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La source que vous configurez sur le formulaire **Configuration de l'ingestion d'infractions IBM QRadar** peut être réutilisée pour plusieurs ServiceNow AI Platform profils tant que chaque profil ingère des infractions.

7. Cliquez sur **Envoyer**.
   Une fois validée et soumise, chaque IBM QRadar configuration de serveur est enregistrée sur la page Intégrations de sécurité sous forme de tuile. Si les tuiles de configuration que vous avez enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste de choix Afficher les configurations, cliquez sur **Oui**.

   Remarque : Si vous rencontrez des problèmes avec la fonctionnalité de segmentation de domaine, contactez IBM QRadar l'assistance clientèle pour obtenir de IBM QRadar l'aide.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer le profil.

Configurer votre ServiceNow AI Platform® instance pour l'intégration d'ingestion d'infractions IBM QRadar

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre ServiceNow AI Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application afin de garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform® et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre ServiceNow AI Platform® instance. • Un utilisateur disposant du rôle d'administrateur ServiceNow AI Platform® (admin) installe l'application à partir de et ServiceNow Store lui affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans le ServiceNow AI Platform®: ◦ Nomme, crée et modifie les profils d'infraction. ◦ Sélectionne et mappe IBM QRadar les champs de données d'infractions aux champs d'incident de sécurité. ◦ Prévisualise les détails de l'incident de sécurité pour plus d'exactitude avant de finaliser la configuration. ◦ Planifie l'ingestion des infractions en cours. ◦ Active les mises à jour de l'infraction lorsqu'un incident SIR est créé et fermé. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Les utilisateurs disposant du sn_si.analyst travaillent sur des incidents de sécurité. Pour plus d'informations sur les rôles et l'attribution de rôles aux utilisateurs, voir Rôles sur le site Web de la documentation produit ServiceNow .
Vérifiez que vous utilisez les versions suivantes : • IBM QRadar version 7.3.2 ou ultérieure. • IBM QRadar Version d'API 10 ou ultérieure. Les versions antérieures ne sont pas prises en charge.	Si vous avez accès à la IBM QRadar console, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.
Vérifiez que vous avez installé et configuré une application de Serveur MID.	Application Serveur MID configurée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	Un Serveur MID dans votre ServiceNow AI Platform® instance est requis pour se connecter au IBM QRadar service si le serveur est déployé au sein de IBM QRadar votre réseau d'entreprise. Consultez le site Web de la documentation produit ServiceNow pour plus d'informations sur les serveurs MID. Si vous utilisez le IBM QRadar service Cloud, un Serveur MID n'est pas nécessaire.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Ingestion d'événements et d'alertes pour Security Operations : Cette application nécessite : ○ com.glide.hub.integration.runtime => Exécution du Centre d'intégration ServiceNow ○ com.glide.hub.action_step.rest => Étape d'action du Centre d'intégration ServiceNow : REST **Remarque :** Les composants du concentrateur d'intégration sont installés avec le module d'extension d'ingestion d'événements et d'alertes. Si ceux-ci ne sont pas installés, contactez le support client pour obtenir de l'aide. Pour plus d'informations sur l'installation Opérations de sécurité des applications principales, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Traduction automatique

Que faire ensuite

Vous avez correctement configuré votre ServiceNow AI Platform® instance pour l'intégration. L'étape suivante consiste à installer l'application IBM QRadar à partir de ServiceNow Store pour l'intégration.

Créer un profil pour IBM QRadar l'intégration de l'ingestion d'infractions

En tant qu'utilisateur disposant du rôle sn_si.admin, vous créez un profil d'infraction dans votre ServiceNow AI Platform instance et déterminez quelles infractions créent des incidents de sécurité. Avant ServiceNow AI Platform Réponse aux incidents de sécurité que les incidents de sécurité (SIR) ne soient créés à partir d'infractions, les valeurs de champ des infractions sont affichées sur une mise en page d'un ServiceNow AI Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera créé.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Du point de vue de l'intégration, à l'aide des API disponibles, IBM QRadar les infractions sont automatiquement ingérées dans l'environnement Opérations de sécurité de votre ServiceNow AI Platform instance en fonction du type de profil défini. Les workflows d'intégration ingèrent différents types d'infractions telles que les tentatives d'accès non autorisé et les logiciels malveillants, par exemple. Ces infractions sont ingérées en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance. Toutes les infractions sont initialement ingérées pour un type d'infraction configuré dans un profil. Les infractions ingérées peuvent ensuite être filtrées davantage pour spécifier quelles infractions créent des incidents de sécurité. Par exemple, vous pouvez préférer des filtres qui créent des incidents de sécurité uniquement pour les infractions identifiées comme à haut risque. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir d'infractions ingérées, les valeurs de champ individuelles des infractions sont mappées aux champs correspondants sur une mise en page d'incident de sécurité pour un aperçu.

Les noms des profils d'infraction de votre ServiceNow AI Platform instance doivent être uniques. Vous pouvez créer plusieurs configurations pour plusieurs sources, ainsi que plusieurs profils pour une seule source.

Créer des profils pour l'ingestion des IBM QRadar infractions

Vous pouvez configurer un profil pour ingérer des infractions.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Pour créer un profil pour une infraction dans votre ServiceNow AI Platform instance, accédez à **Intégration d'IBM QRadar** > **Profil IBM QRadar**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs.

   Un exemple de formulaire rempli suit la table.

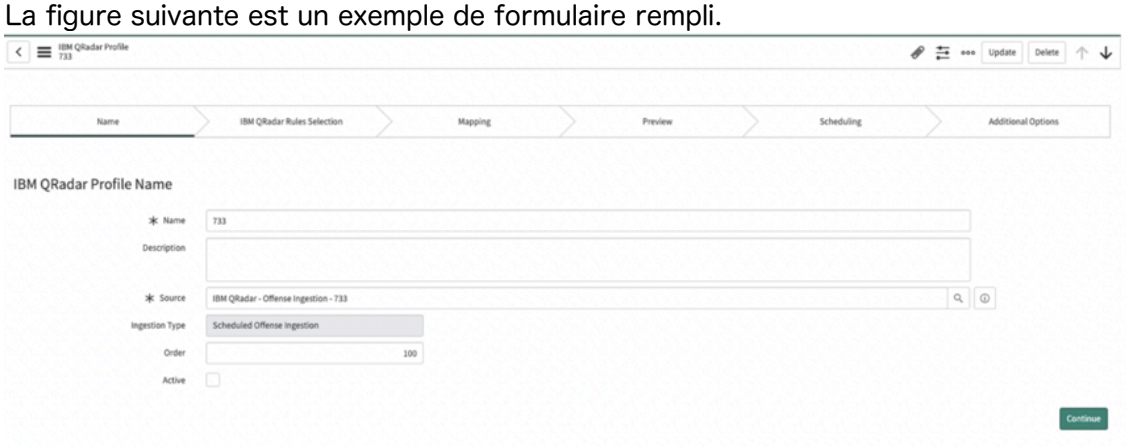
Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre ServiceNow AI Platform instance doivent être uniques.
Actif	La case à cocher est désactivée par défaut. Si cette option est désactivée, le profil n'est pas actif et l'ingestion n'aura pas lieu. **Remarque :** Vous devez remplir toutes les sections du profil avant de l'activer.
Source	Serveur IBM QRadar que vous avez configuré pour ingérer les infractions. Si vous avez configuré

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	plusieurs IBM QRadar serveurs, sélectionnez le serveur approprié pour les types d'infractions qui seront ingérées pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Le workflow dans le profil avec le numéro le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli.



Que faire ensuite
L'étape suivante consiste à sélectionner les infractions à ingérer.

Sélectionner des IBM QRadar règles

En fonction de la IBM QRadar source, sélectionnez une ou plusieurs IBM QRadar règles pour le profil.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Affichez les règles disponibles IBM QRadar dans votre ServiceNow AI Platform instance afin de connaître les règles actives IBM QRadar pour lesquelles vous souhaitez ingérer et créer des incidents de sécurité.

Dans IBM QRadar, vous pouvez identifier les règles par leur origine en tant que règles système, remplacement et utilisateur. Par défaut, l'origine d'une règle est liée à une règle système. Lorsque vous modifiez une règle système dans , son origine est définie sur IBM QRadar Remplacer.

Cliquez sur la liste dans le champ Liste de IBM QRadar règles. La liste des règles actives IBM QRadar présentes dans la console s'affiche IBM QRadar . Sélectionnez une ou plusieurs règles

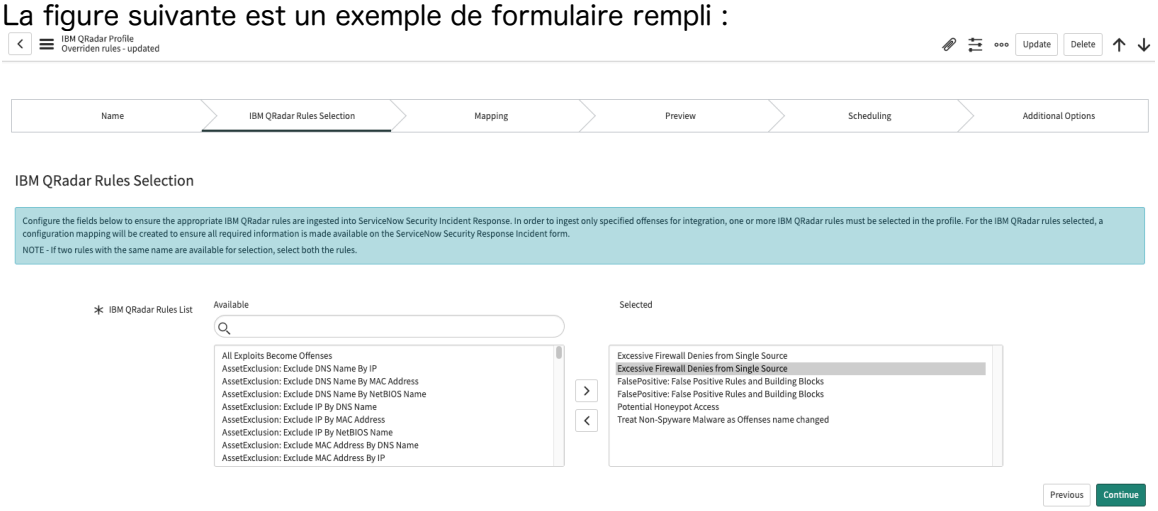
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

dans la liste et déplacez-les vers la colonne **Sélectionné** . Les infractions déclenchées par une ou plusieurs des IBM QRadar règles sélectionnées sont ingérées dans ce profil.

Règles du même nom : dans l'instance ServiceNow AI Platform , une liste des règles actives ou activées s'affiche. Si vous modifiez une règle système active ou activée dans IBM QRadar, une nouvelle règle de remplacement est créée. Ainsi, deux règles portant le même nom sont affichées dans le ServiceNow AI Platform fichier . Lorsque ce scénario se produit, sélectionnez les deux règles pour ingérer et créez des incidents de sécurité.

La figure suivante est un exemple de formulaire rempli :



Cliquez sur **Continuer** pour passer à l'étape suivante de l'assistant.

Mappage des champs d'infractions pour l'intégration IBM QRadar

Une fois les règles sélectionnées, l'étape suivante consiste à mapper les champs d'infraction, d'événement ou de flux aux champs du formulaire d'incident de sécurité.

Vue d'ensemble

Pour l'étape de mappage, vous devez d'abord ingérer des exemples d'infractions pour une ou plusieurs règles sélectionnées IBM QRadar . Ensuite, vous devez vous assurer que toutes les données de champ d'infraction pertinentes sont mappées à l'endroit approprié sur le formulaire d'incident SIR , puis visualiser l'incident SIR dans la section d'aperçu.

Le mappage des champs d'infractions témoins implique les éléments suivants :

- Extraction et remplissage des exemples de données : Voir Ingestion des exemples IBM QRadar d'infractions.
- Mappage des champs d'infraction à l'incident de sécurité : voir Mapper IBM QRadar les champs d'infraction aux champs de réponse aux incidents de sécurité.

Ingestion des exemples IBM QRadar d'infractions

Vous pouvez ingérer des exemples d'infractions pour une ou plusieurs règles sélectionnées IBM QRadar .

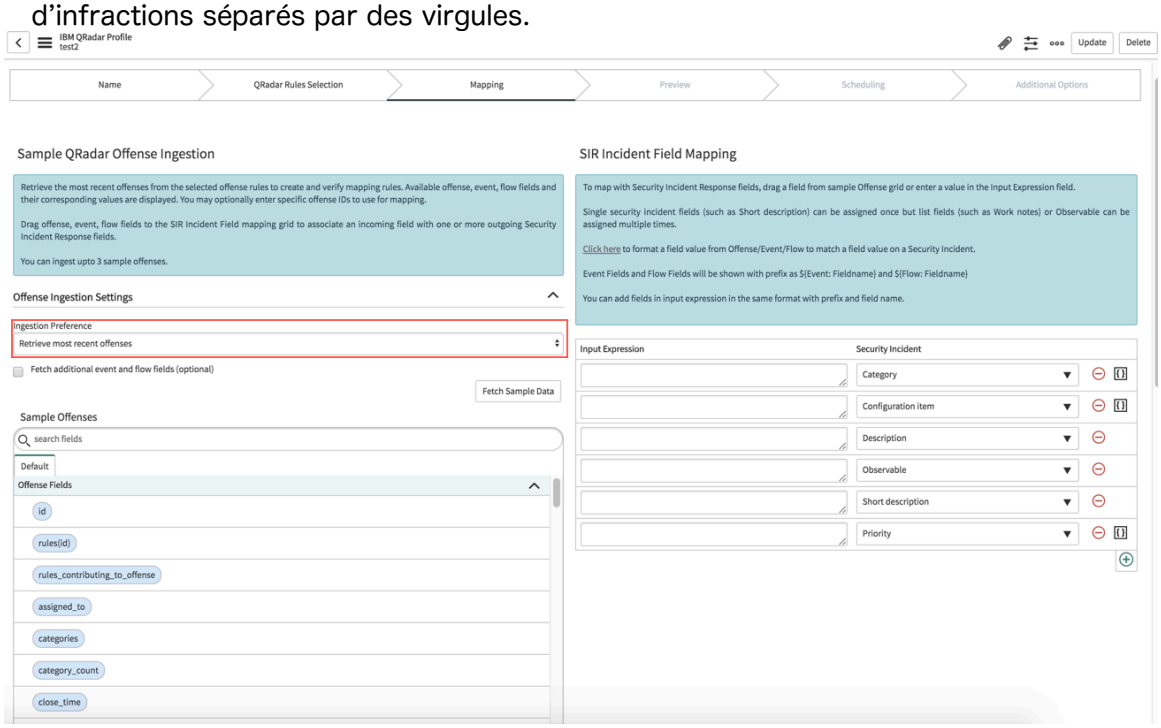
Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Vous pouvez soit extraire les trois exemples d'infractions les plus récents, soit fournir les ID d'infractions uniques pour les infractions spécifiques que vous souhaitez utiliser pour votre expérience de mappage. Dans la liste de choix **Préférence d'ingestion** , sélectionnez l'une des options suivantes :
   - Récupérer les infractions les plus récentes : les trois infractions les plus récentes pour les règles sélectionnées sont récupérées.
   - Sélectionner les infractions en fonction de l'ID des infractions : spécifiez l'ID d'infraction pour les infractions à récupérer. Vous pouvez spécifier un maximum de 3 ID d'infractions séparés par des virgules.



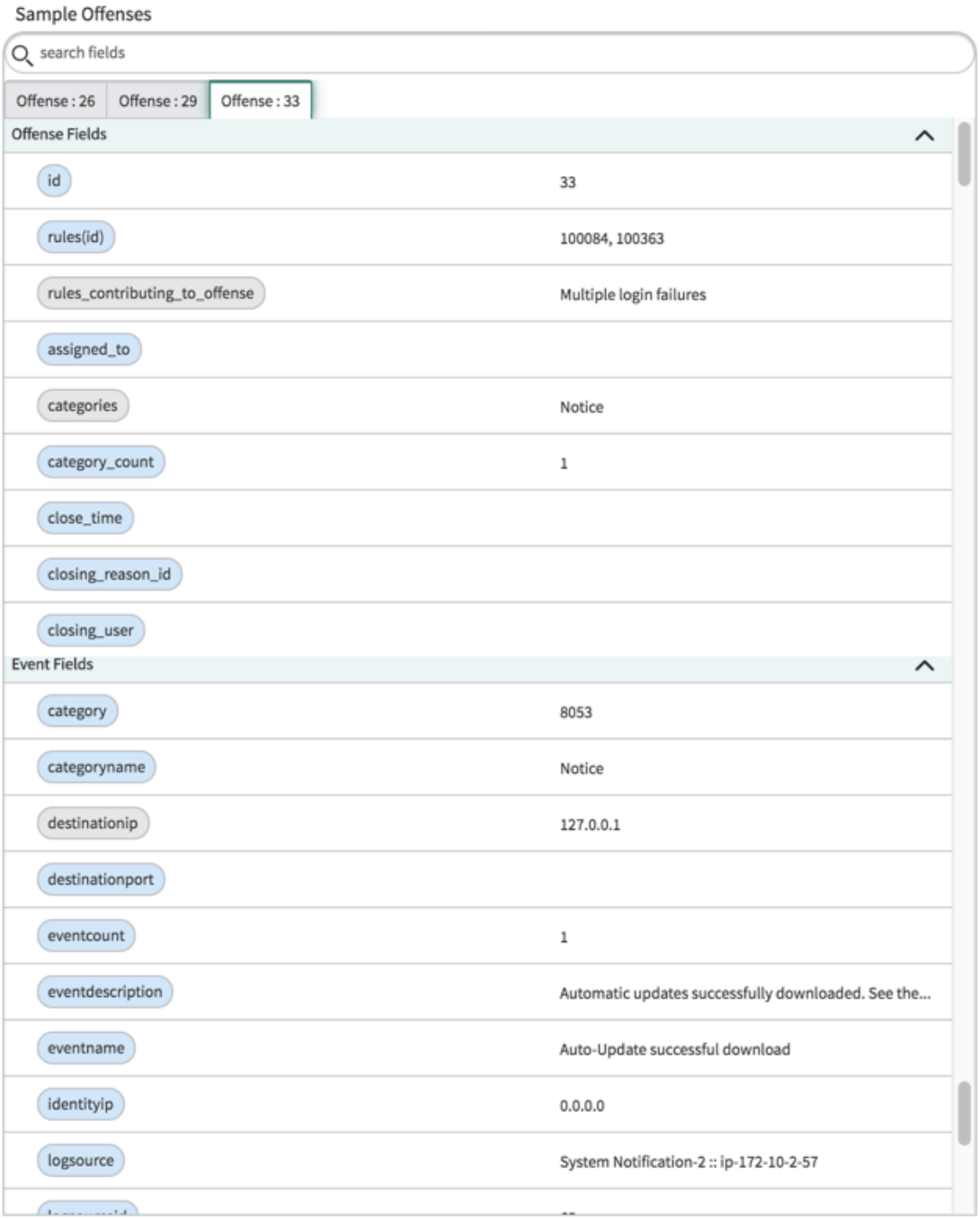
3. Cliquez sur **Extraire les données d'échantillon** pour extraire les dernières données d'échantillon d'infraction de la IBM QRadar console pour les règles d'infraction sélectionnées.

   Les champs d'offense et les résultats des valeurs sont affichés sous forme d'onglets individuels. Une infraction peut être déclenchée par trois types de règles :
   - Événement : dans cette règle, les journaux d'événements sont vérifiés et si les critères spécifiés sont remplis, une infraction est créée.
   - Flux : les données et le trafic réseau sont vérifiés et si certaines conditions sont remplies, une infraction est créée.
   - Commun : dans ce cas, vous pouvez spécifier des conditions pour les événements ou les flux et si l'une ou les deux conditions sont remplies, une infraction est créée.

   L'extraction des exemples d'infractions peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran. En fonction de la ou des règles qui ont déclenché l'infraction, en plus des champs d'infraction, les champs d'événement ou de flux sont renseignés comme illustré dans la figure ci-dessous :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Remarque : Les champs d'événement ou de flux affichés appartiennent au premier champ d'événement ou de flux qui a déclenché l'infraction en fonction de l'événement ou de la règle de flux correspondante.

4. Voici les champs d'infraction personnalisés créés pour cette intégration.
   Des champs d'infractions standard en plus de ces champs personnalisés sont disponibles pour le mappage.
   - rules_contributing_to_offense : IBM QRadar règles qui ont contribué à l'infraction en fonction de l'ID de règle.
   - utilisateurs : noms d'utilisateur pour l'infraction

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- remote_destination_ip : adresses IP de destination distantes pour l'infraction.

  En fonction des ID de destination locaux pour l'infraction, les champs d'adresse de destination locale personnalisés suivants sont disponibles :

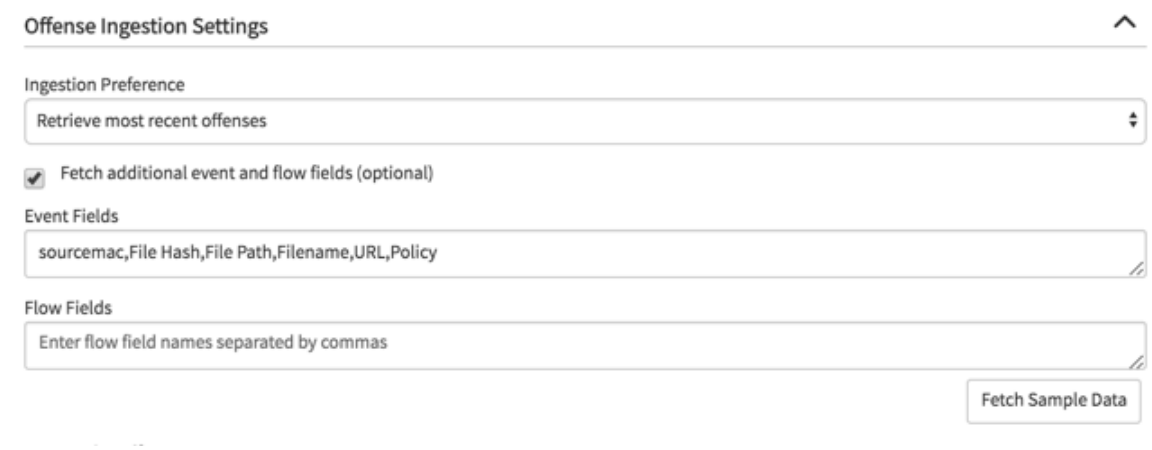
  - local_destination_address (domain_id)
  - local_destination_address (event_flow_count)
  - local_destination_address (first_event_flow_seen)
  - local_destination_address (ID)
  - local_destination_address (last_event_flow_seen)
  - local_destination_address (local_destination_address_ids)
  - local_destination_address (magnitude)
  - local_destination_address (réseau)
  - local_destination_address (offense_ids)
  - local_destination_address (local_destination_ip)

- Les adresses sources suivantes sont disponibles en fonction des ID sources de l'infraction :
  - source_addresses (domain_id)
  - source_addresses (event_flow_count)
  - source_addresses (first_event_flow_seen)
  - source_addresses (ID)
  - source_addresses (last_event_flow_seen)
  - source_addresses (source_address_ids)
  - source_addresses (magnitude)
  - source_addresses (réseau)
  - source_addresses (offense_ids)
  - source_addresses (source_ip)

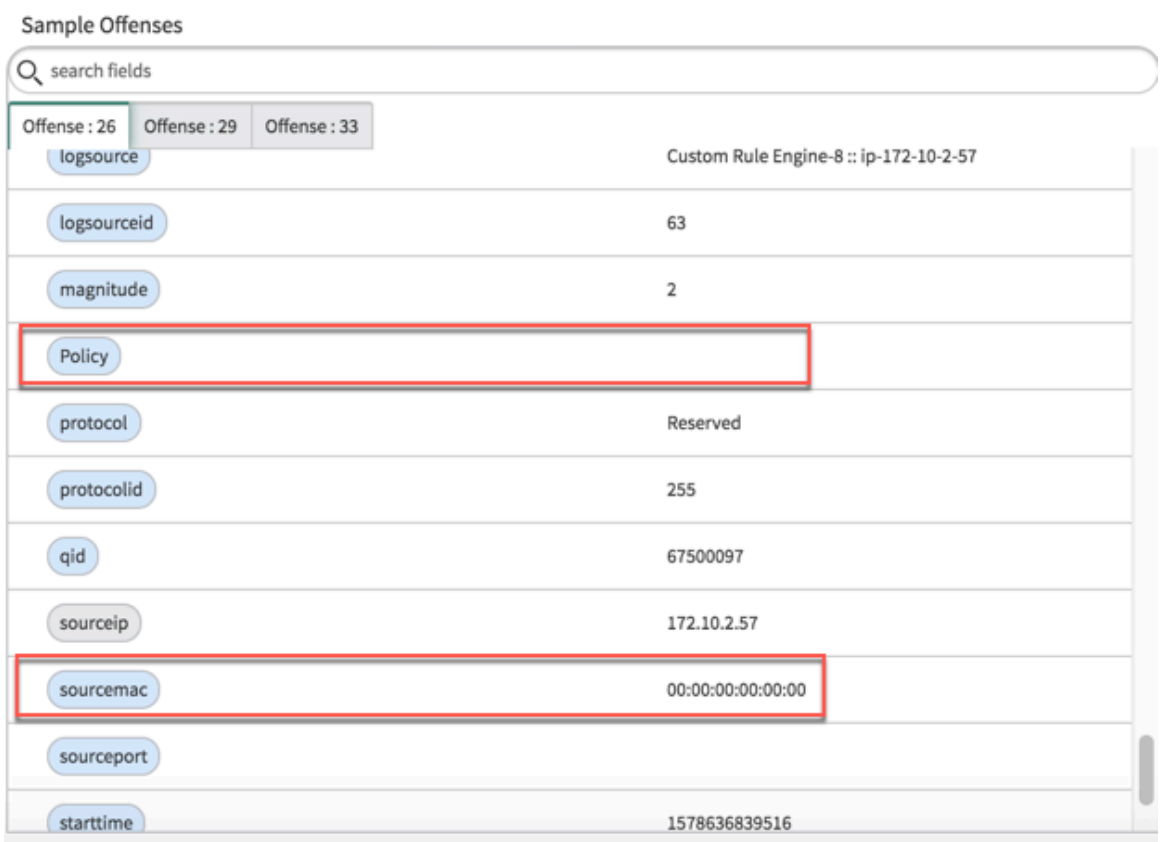
Cochez la case **Récupérer des champs d'événements et de flux supplémentaires (facultatif).** Vous pouvez extraire des exemples de données d'événement et de flux à partir de n'importe quel champ d'événement et de flux personnalisé actif et valide. Spécifiez les champs personnalisés séparés par des virgules, comme indiqué ci-dessous :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



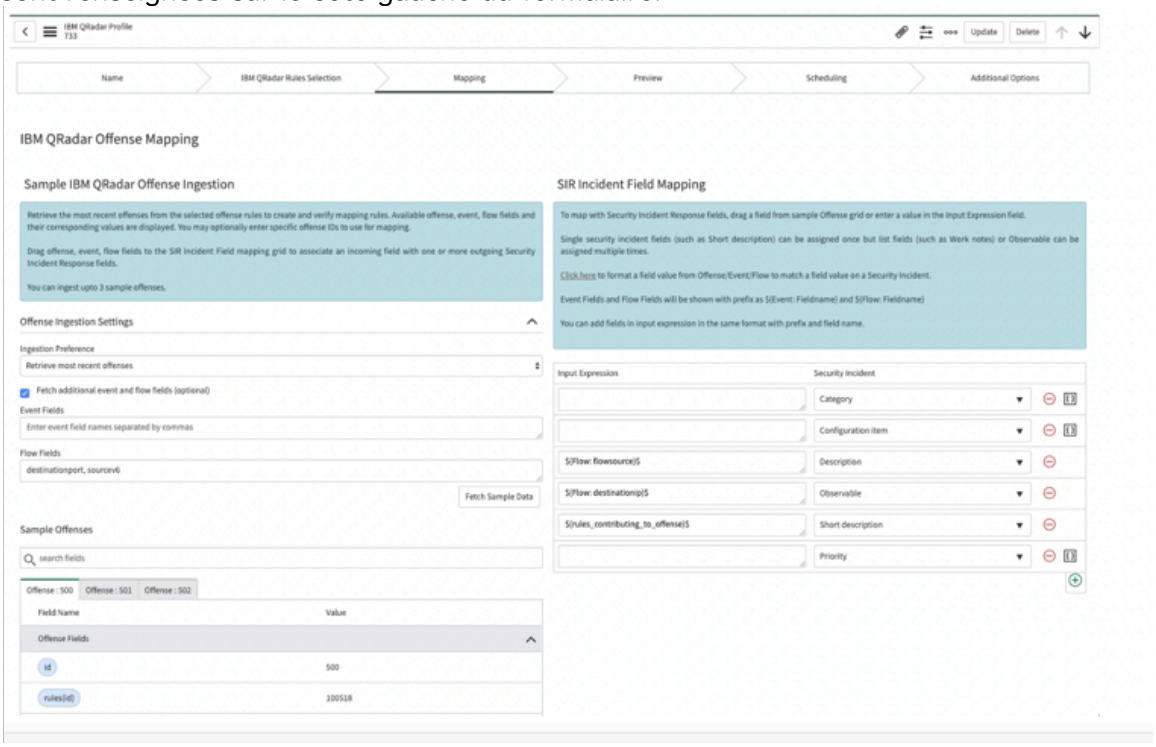
Cliquez sur **Extraire un exemple de données**. Les champs d'événement ou de flux spécifiés ainsi que leurs valeurs (le cas échéant) sont ajoutés à la section Événement ou Flux, comme indiqué ci-dessous :



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois les exemples de données extraits, les valeurs correspondantes de ces champs sont renseignées sur le côté gauche du formulaire.



Que faire ensuite

Une fois que vous avez extrait les exemples de données, l'étape suivante consiste à mapper les champs d'infraction à l'incident de sécurité.

Mapper IBM QRadar les champs d'infraction aux champs de réponse aux incidents de sécurité

Mappez les champs d'infraction, d'événement et de flux individuels aux champs d'un ServiceNow AI Platform SIR incident de sécurité.

Mappage de champs d'infractions

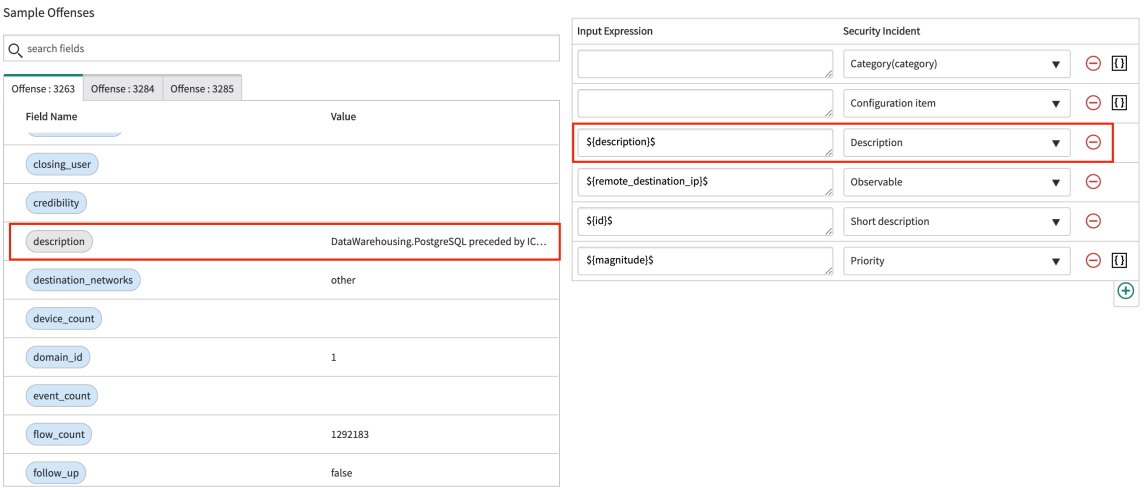
En tant qu'utilisateur disposant du rôle sn_si.admin, utilisez les champs de la section Exemples d'infractions à gauche et mappez-les aux champs d'incident de sécurité de la colonne Mappage du champ d'incident SIR. Modifiez la configuration de mappage en faisant glisser les champs d'infraction, d'événement ou de flux à gauche et en les déposant dans la section de mappage d'incident ServiceNow SIR à droite. Le mappage sur la droite associe le champ d'infraction entrant à un champ d'incident de sécurité sortant.

1. Une fois que vous avez extrait les exemples de données, l'étape suivante consiste à mapper les champs d'infraction, d'événement ou de flux à l'incident de sécurité. Pour faire correspondre une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez tout en maintenant enfoncé le nom d'un champ bleu sur le côté gauche du formulaire.
2. Faites glisser le nom du champ, par exemple, description, et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

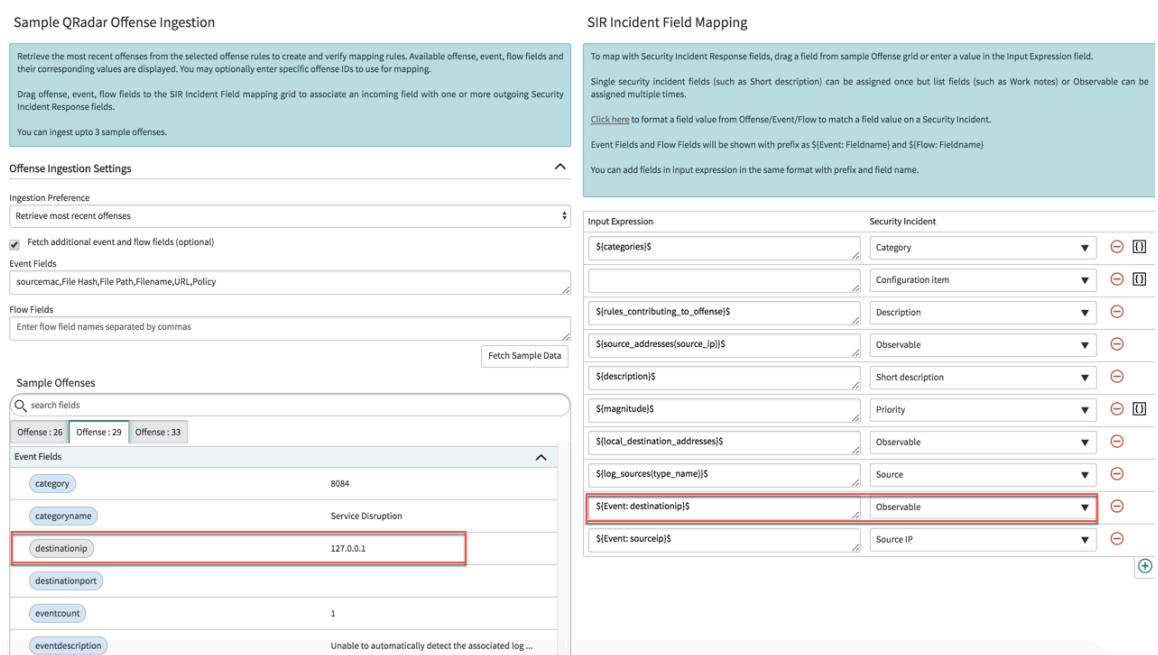
   La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, la description est mappée au champ Description de l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : Si vous saisissez manuellement le nom du champ d'événement ou de flux dans la section Expression d'entrée, vous devez ajouter un préfixe `comme ${Event :eventfield}$` ou `${Flow :flowfield}$` avant le nom du champ en cours de mappage.



Traduction automatique

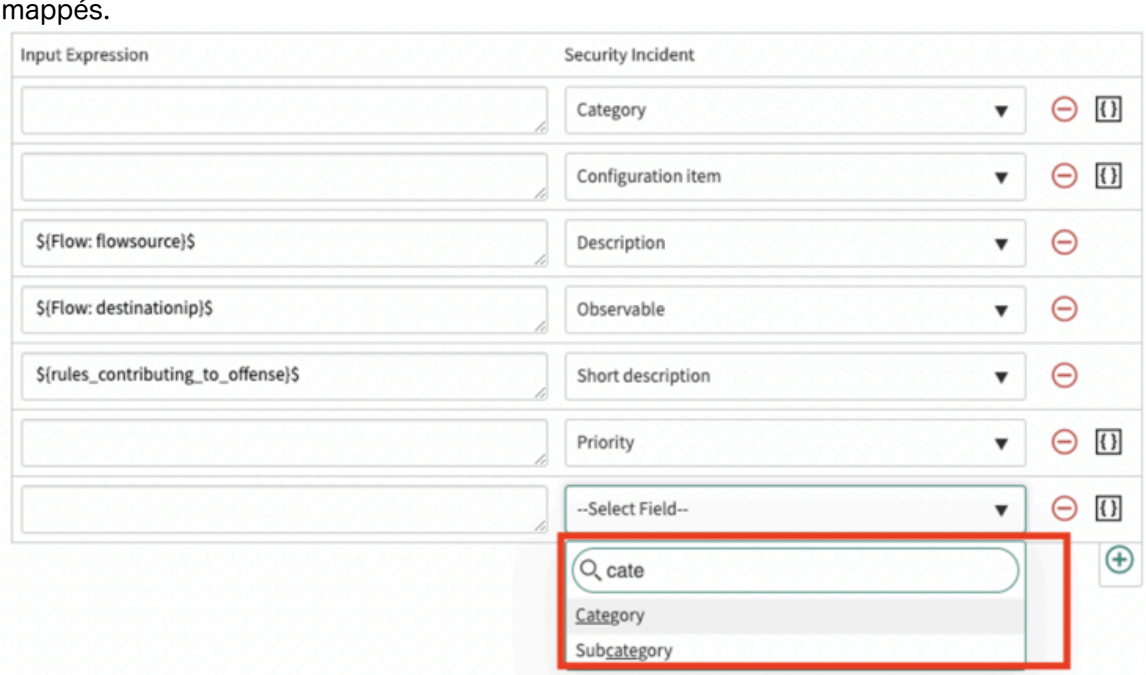
Pour vous assurer qu'aucun champ d'infraction, d'événement ou de flux n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Le code couleur des champs d'infraction vous aide à suivre les valeurs d'infraction que vous avez déjà mappées, car elles deviennent grisées, tandis que tous les champs non mappés restants apparaissent en bleu. Cela vous aide à mieux visualiser les valeurs de champ qui ont été ajoutées à l'incident de sécurité et si des informations importantes restantes sur l'infraction restent non mappées.

Les champs bleu clair sur la gauche indiquent qu'un champ d'infraction n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ d'infraction, d'événement ou de flux entrant à plusieurs champs d'un incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et mappé à un champ de l'incident de sécurité. Ce code couleur vous aide à suivre le mappage.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit :
   a. À droite du formulaire, dans la section Mappage du champ d'incidents SIR, au bas de la grille, cliquez sur l'icône plus (+). Un nouveau champ s'affiche.
   b. Dans la colonne Incident de sécurité, développez la liste de choix qui s'affiche, puis sélectionnez un champ.

      Dans la liste de choix développée pour le nouveau champ, certains champs sont ombrés. Dans la figure suivante, la catégorie a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. Semblable au code couleur pour les champs d'infraction sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident SIR déjà mappés.



> **Remarque :** Comme plusieurs observables peuvent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs.
> Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité possède une liste de choix dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste de choix, le champ n'est pas renseigné sur l'incident de sécurité.

   c. Vous pouvez également saisir une valeur dans le champ Rechercher de la nouvelle ligne.
   d. Sur le côté gauche du formulaire, sélectionnez le champ d'infraction et faites-le glisser vers un champ d'incident de sécurité approprié sur la droite.
4. Supprimez les champs à l'aide de l'icône - en regard du nom du champ dans la section de mappage de champ d'incident SIR.
5. Poursuivez le mappage en ajoutant ou en supprimant des valeurs de champ au mappage.

Champs d'infraction avec plusieurs valeurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les champs **d'incident** de sécurité tels que Catégorie et **Utilisateur** (par exemple, Utilisateur affecté, Affecté à) disponibles avec le produit de base ne prennent pas en charge plusieurs valeurs.
- Les champs suivants IBM QRadar prennent en charge plusieurs valeurs :
  - *Catégories*
  - *destination_networks*
  - *source_address_ids*
  - *local_destination_address_ids*
  - *remote_destination_ips*
  - *rules_contributing_to_offense*
  - *Utilisateurs*

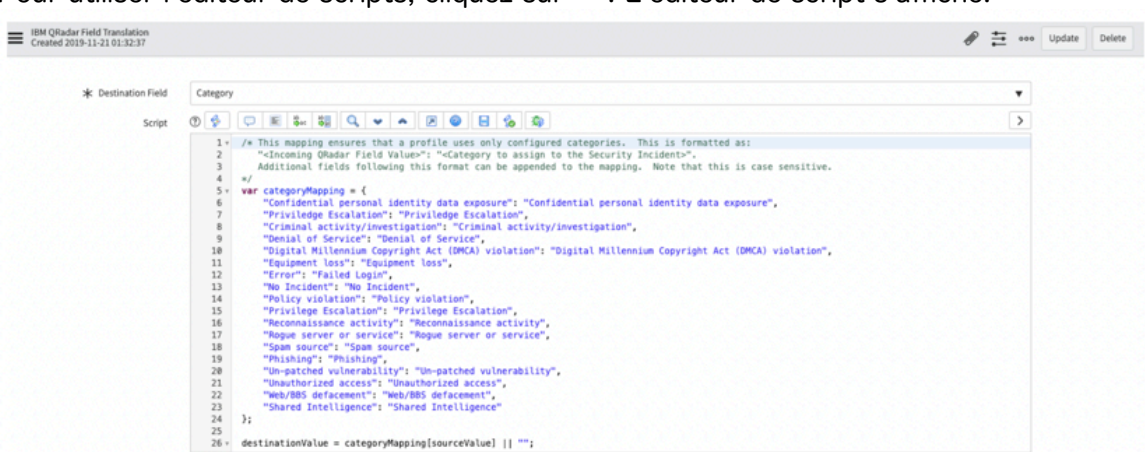
  Si vous devez mapper les champs ci-dessus à des Réponse aux incidents de sécurité champs autres que les champs de type CI et Observable, vous devez créer de nouveaux Réponse aux incidents de sécurité champs de type **Liste** et les utiliser pour le mappage.

Remarque : Par défaut, seuls les champs **de type liste** non référencés sont pris en charge.

Formater la traduction du champ

Dans certains cas, les valeurs du champ Infraction peuvent IBM QRadar ne pas être traduites directement dans les champs de l'incident de sécurité SIR. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident de sécurité SIR à l'aide de la fonctionnalité Formater la traduction du champ.

Pour utiliser l'éditeur de scripts, cliquez sur {}. L'éditeur de script s'affiche.



Entrez les modifications apportées au script, cliquez sur **Mettre à jour** pour enregistrer les modifications et revenir à la page Mappage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions de génération d'incidents

Une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de spécifier quelles infractions doivent créer des incidents de sécurité par rapport à celles qui doivent être filtrées (par exemple, les infractions de faible priorité). Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir des critères supplémentaires qu'une infraction entrante doit satisfaire pour créer un incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

1. Faites défiler la page jusqu'à la section **Conditions de génération d'incidents** sur le formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

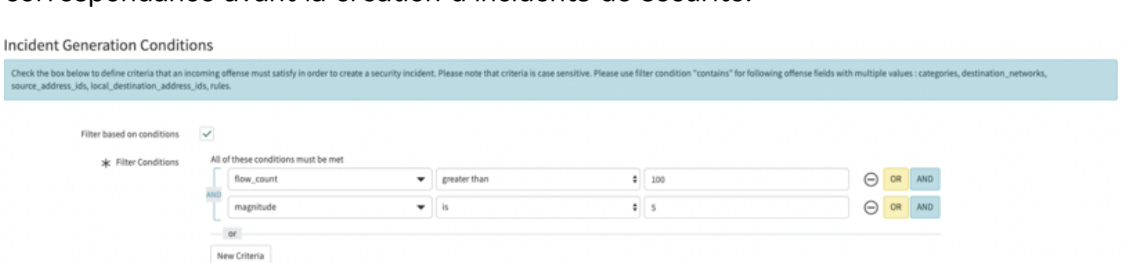
   Le générateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

   Les options des listes de choix pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Exemple d'ingestion d'infractions QRadar pour les infractions que vous avez ingérées. Ces champs sont dynamiques et changent en fonction des infractions que vous ingérez. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'infraction IBM QRadar . Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférerez peut-être retourner à votre IBM QRadar console et revoir vos infractions pour les mots-clés.

   Remarque : Les champs *`catégories`*, *`destination_networks`*, *`source_address_ids`*, *`local_destination_address_ids`*, *`remote_destination_ips`*, *`rules_contributing_to_offense`* et *`Infractions des utilisateurs`* peuvent avoir plusieurs valeurs (car les valeurs sont stockées dans des tableaux). Comme la condition de filtre ne peut récupérer que des chaînes, vous devez utiliser la condition de filtre *`contient`* pour ces champs afin de vous assurer que les données sont filtrées correctement.

2. À l'aide des listes de choix et des champs du générateur de conditions, définissez des filtres pour la première ligne.
3. Pour ajouter plus de conditions, à droite des champs, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. (Facultatif) Sur la deuxième ligne, définissez une deuxième condition de filtre.

   L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création d'incidents de sécurité.



   Vous avez défini les conditions de génération d'incidents afin que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce type de filtrage des conditions de génération d'incidents vous aide à réduire les infractions et le nombre d'incidents de sécurité inutiles que vous créez sans modifier la règle ou les filtres sous-jacents dans IBM QRadar. Si des critères de filtrage supplémentaires sont définis, seules les infractions qui correspondent à tous les critères sont mappées aux incidents.

Remarque : Si l'un des noms de champs d'infraction comporte des caractères spéciaux tels que des guillemets («), des traits d'union ('), des traits de soulignement (-) ou des esperluettes (@), ces caractères peuvent devoir être remplacés à des fins de filtrage, mais un suffixe numérique est ajouté pour différencier les champs avec des noms d'infractions en double. Par exemple, si le champ de la première infraction est `alerts.alert` et que le champ de la deuxième infraction est `alerts@alerts`, ces champs ne peuvent pas être identifiés de façon unique, car les caractères de texte standard restants sont les mêmes. Dans ce cas, un suffixe est ajouté au deuxième champ d'infraction et le champ est renommé en `alerts@alert(1)` lorsqu'il est affiché dans la liste Conditions de filtre.

Critères d'agrégation d'infractions pour gérer des infractions similaires et empêcher les incidents en double

Définissez des critères d'agrégation des infractions supplémentaires qui regroupent une infraction entrante à un incident de sécurité SIR existant au lieu de créer des incidents similaires, potentiellement en double. En utilisant des critères de correspondance de champ pour chaque profil, cette option d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'infraction connexes sur un seul incident de sécurité. Pour définir les critères, procédez comme suit ci-dessous :

1. Faites défiler jusqu'à la section Critères d'agrégation des infractions sur le formulaire et cochez la case **Conditions d'agrégation** pour activer cette option.

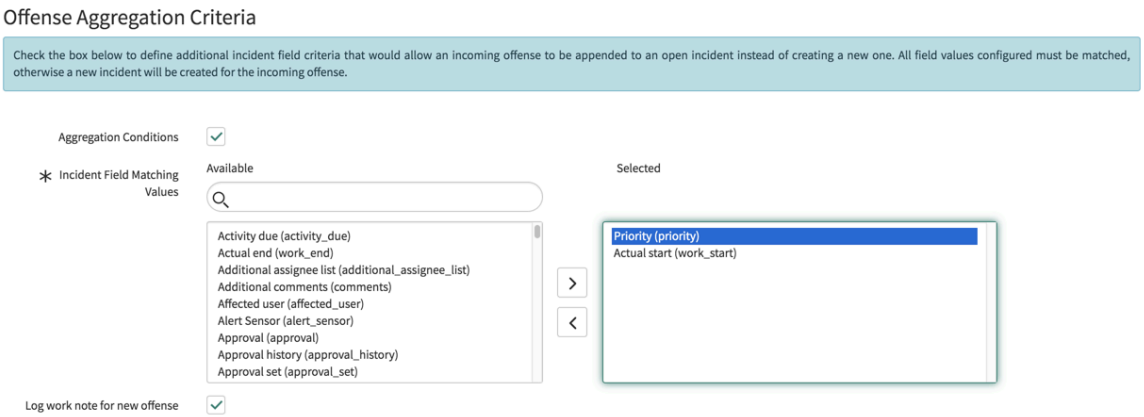
   Les colonnes Valeurs correspondantes au champ Incident s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés sur l'incident SIR de sécurité.

2. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans ServiceNow AI Platform votre et déplacez-les vers la liste Sélectionné.

   Toutes les valeurs de champ que vous sélectionnez doivent être mises en correspondance pour ajouter cette alerte entrante à un incident de sécurité existant. Cela inclut les champs, tels que les observables et les éléments de configuration, auxquels plusieurs valeurs de champ d'offense peuvent être mappées. Toutes les valeurs doivent correspondre. Si seul un sous-ensemble de valeurs correspond, les conditions d'agrégation des infractions ne seront pas remplies et un nouvel incident de sécurité sera créé. Voir la capture d'écran ci-dessous pour le mappage de champs à valeurs multiples.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Si une nouvelle infraction correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation à l'étape de mappage, la nouvelle infraction est automatiquement ajoutée à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher toutes les infractions agrégées ajoutées sur une liste connexe d'un incident de sécurité. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi ces infractions sont regroupées aux incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous Liens connexes et cliquez sur le lien **Afficher toutes les listes connexes** .

3. (Facultatif) Pour enregistrer une note de travail pour une nouvelle infraction récemment ajoutée à l'incident de sécurité, cochez la case pour activer cette option. La note de travail indique qu'une nouvelle infraction a été ajoutée, ainsi qu'un lien vers les détails de l'infraction et tout autre détail qui a pu être ajouté au champ Note de travail dans votre section de mappage.

   Vous avez mappé avec succès les valeurs d'une IBM QRadar infraction aux champs d'un incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage de génération d'incidents. Vous avez également ajouté des infractions aux incidents de sécurité existants lorsque les valeurs de champ d'infraction correspondent aux critères d'agrégation configurés.

4. Cliquez sur **Continuer** pour poursuivre la configuration du profil. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité

Aperçu de l'incident de sécurité

Une fois l'étape de mappage terminée, affichez un aperçu des valeurs que vous avez mappées dans un SIR incident de sécurité. Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs d'infraction que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
En tant qu'utilisateur disposant du rôle sn_si.admin, prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs erronés ou pour renseigner les données manquantes. Si l'aperçu n'est pas effectué avec succès, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le Réponse aux incidents de sécurité produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si l'aperçu de l'incident de sécurité ne s'affiche pas, cliquez sur **Aperçu** dans la barre de progression.
2. Dans la liste de choix Exemples d'ID d'infractions, sélectionnez un élément.
   L'incident de sécurité s'affiche. Cette vue est en lecture seule et aucun enregistrement de cet incident de sécurité n'est enregistré.
3. Examinez le mappage de champs des valeurs d'infraction sur l'incident de sécurité.



L'image précédente est un exemple d'aperçu avec une erreur de mappage des échantillons qui ont été ingérés.

4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

Que faire ensuite

Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à définir le calendrier.

Définir le calendrier

Vous pouvez définir le calendrier de l'ingestion d'infraction. Au cours de cette étape, vous pouvez vérifier les paramètres par défaut pour la récupération de l'infraction ou modifier la planification si nécessaire. Cette étape vous permet également de récupérer les infractions historiques à l'aide d'une plage de dates.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez choisir d'ingérer des infractions historiques pendant l'étape de planification. Vous choisissez également la fréquence à laquelle vous interrogerez les nouvelles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

infractions futures et les infractions mises à jour qui correspondent à la configuration du profil.

En tant qu'utilisateur disposant du rôle sn_si.admin, vous configurez ces intervalles d'interrogation pour chaque profil. Les performances de l'intégration de l'ingestion IBM QRadar d'infraction peuvent être impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférerez peut-être trouver un équilibre entre la réduction de la surcharge d'interrogation sur le serveur et le IBM QRadar désir d'être averti dès que possible lorsqu'une infraction est créée ou mise à jour. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférez peut-être modifier ce paramètre à une minute si nécessaire.

Extraction d'infractions nouvelles et mises à jour

Lorsque le calendrier d'interrogation est défini, la tâche planifiée extrait les infractions nouvelles et mises à jour qui ont été extraites précédemment, mais qui ne répondent pas aux critères de filtrage des incidents. Cela vous donne la possibilité de créer des incidents basés sur des critères qui peuvent ne pas être présents lors de la création d'une infraction pour la première fois, mais qui deviennent disponibles après une mise à jour, par exemple pendant la phase d'enquête. Une fois qu'un incident est créé pour une infraction spécifique, ses mises à jour ultérieures sont ignorées, car il est prévu que l'infraction soit maintenant traitée comme un incident de sécurité actif ServiceNow . Toutefois, toutes les autres infractions qui ont déjà été ingérées, mais qui ne répondent pas aux critères de génération d'incidents, continueront d'être extraites et vérifiées par rapport aux critères de génération d'incidents jusqu'à ce qu'elles fassent partie d'un incident actif.

Procédure

1. Si la page Planification de la barre de progression ne s'affiche pas, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les infractions sont extraites de la IBM QRadar console.

Option	Description
Champ d'ingestion d'infraction en cours sélectionné	Attaque en cours En fonction du paramètre par défaut, l'instance ServiceNow AI Platform extrait du IBM QRadar serveur les infractions nouvelles et mises à jour toutes les cinq minutes. Les incidents de sécurité sont créés si des infractions sont découvertes et que les critères de filtrage de génération d'incidents sont vérifiés. Pour équilibrer le désir d'obtenir les données les plus récentes, le paramètre par défaut est de cinq minutes. Toutefois, cette valeur peut être réduite à une minute si nécessaire.
○ Ingestion d'infractions en cours sélectionnée ○ Définir le délai d'ingestion de l'infraction initiale	Délai d'ingestion initial Si vous souhaitez planifier l'ingestion initiale à une heure précise, procédez comme suit :

Traduction automatique

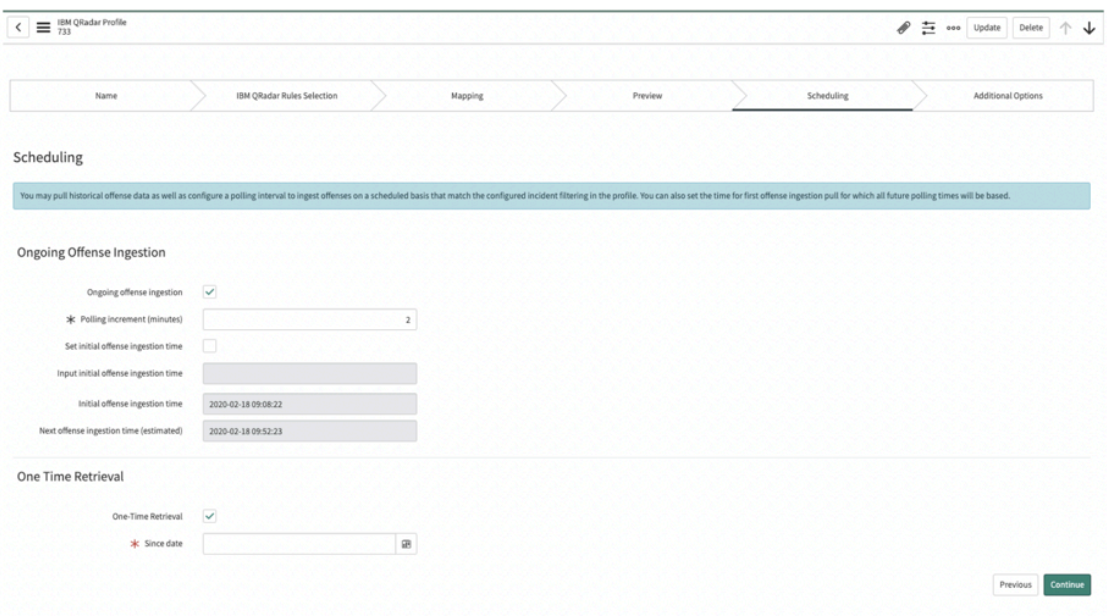
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	○ Sélectionnez les champs Ingestion de l'infraction en cours et Définir la durée d'ingestion de l'infraction initiale. ○ Spécifiez l'heure dans le champ Entrer le délai d'ingestion de l'infraction initiale. L'ingestion initiale aura lieu à l'heure spécifiée ici. Les ingestions suivantes seront basées sur le calendrier défini dans le champ Incrémentation de l'interrogation (minutes). Par exemple, pour planifier une heure d'ingestion d'infraction initiale, si vous avez un contrôle de sécurité quotidien IBM QRadar qui s'exécute une fois par jour à 4 heures du matin, heure locale, vous pouvez configurer le profil d'infraction correspondant dans votre ServiceNow AI Platform instance pour qu'il s'exécute à 4 h 05, heure locale, afin de capturer immédiatement la défaillance de sécurité et de créer un incident de sécurité. Saisissez `<date> 04 05 00` dans le champ d'ingestion de l'infraction initiale. Dans le champ Incrémentation du sondage (minutes), saisissez `<date> 1 440` (24 heures) pour planifier la prochaine ingestion d'infraction dans les 24 heures suivant l'ingestion de l'infraction initiale. Le délai d'ingestion de l'infraction initiale et le temps d'ingestion de l'infraction suivante sont affichés dans les champs. L'ingestion initiale aura lieu à 4h05. Les ingestions suivantes seront basées sur l'intervalle d'interrogation. Dans ce cas, étant donné que l'incrément d'interrogation est de 24 heures, la prochaine ingestion aura lieu le lendemain à 4h05.
Champ de récupération unique sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez une extraction ponctuelle pour ingérer des infractions historiques. Lorsque ce paramètre est configuré, un profil est utilisé une fois pour récupérer les infractions à partir d'événements historiques basés sur une plage de dates. À droite du champ Depuis la date, cliquez sur l'icône Calendrier. Dans le calendrier qui s'affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	infractions. À partir de la valeur Depuis la date, les infractions sont récupérées jusqu'à la date actuelle. Notez que vous pouvez revenir jusqu'à sept jours en arrière à partir de la date actuelle. Cette fonctionnalité n'est pas destinée à récupérer un nombre important d'infractions IBM QRadar historiques pour des raisons d'archivage, mais plutôt un nombre minimal d'infractions en cours qui sont activement traitées au moment de l'activation du profil. Une fois les infractions extraites, ce paramètre ne récupère plus d'infractions pour ce profil à partir de la date actuelle. Ce paramètre renseigne l'incident de sécurité avec toutes les infractions constatées pour la plage que vous saisissez.



3. Cliquez sur **Continuer** pour accéder à la page Options supplémentaires.

Automatiser les mises à jour et la clôture des infractions en fonction de l'état de l'incident SIR

L'intégration IBM QRadar dispose d'une interface bidirectionnelle qui permet aux deux infractions de créer des incidents de sécurité, ainsi qu'une possibilité de mettre à jour les infractions une fois l'incident de sécurité créé et/ou fermé avec les détails pertinents de l'incident tels que le numéro de l'incident de sécurité, le groupe d'affectation, l'URL de l'incident de sécurité, et ainsi de suite.

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

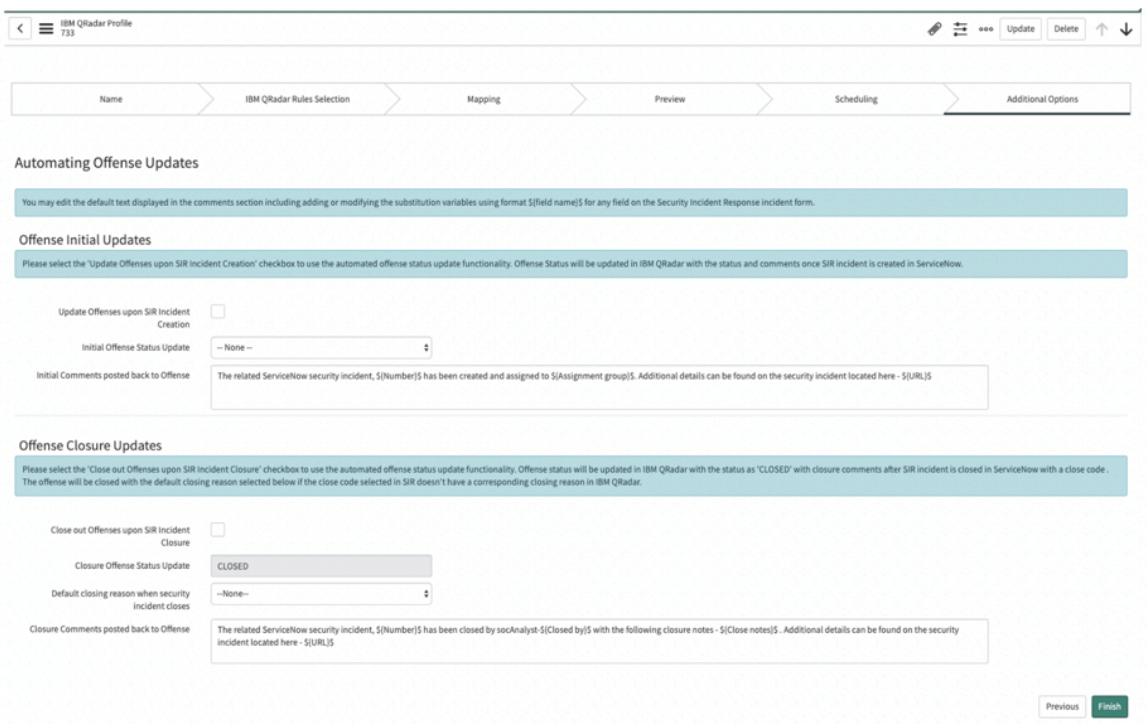
1. Si la page Options supplémentaires de la barre de progression ne s'affiche pas, sélectionnez **Options supplémentaires**.
2. Suivez les instructions ci-dessous pour terminer la configuration de la mise à jour des infractions lors de la création de l'incident de sécurité.

Option ou champ	Description
Mettre à jour les infractions lors de la création de l'incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour le statut de l'infraction et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'infraction. Cela peut se produire à la fois pour les infractions déclencheurs initiales qui créent l'incident de sécurité et pour les infractions agrégées.
Mise à jour de l'état de l'infraction initiale	Vous pouvez sélectionner : ○ Ouvert : l'état de l'infraction est défini sur **Ouvert** et un commentaire est ajouté indiquant qu'un incident de sécurité a été créé pour l'infraction. ○ Masqué : le statut de l'infraction est défini sur **Masqué** et cette infraction est masquée dans le tableau de IBM QRadar bord.
Commentaires initiaux renvoyés à l'attaque	En fonction de l'étape que vous avez sélectionnée, les commentaires initiaux tels que définis dans la IBM QRadar console sont affichés ici.
Clôturer les infractions lors de la fermeture de l'incident SIR	Sélectionnez cette option si vous souhaitez utiliser l'option de fermeture automatique des infractions. Lorsque l'incident de sécurité est fermé ServiceNow avec un code de fermeture pertinent, l'état de l'infraction est mis à jour sur IBM QRadar**Fermé** avec des commentaires de fermeture. **Remarque :** Le code de fermeture spécifié pour l'incident de sécurité doit correspondre au motif de fermeture spécifié dans le tableau de IBM QRadar bord. L'infraction n'est IBM QRadar fermée que si un motif de fermeture correspondant est trouvé. Si aucun motif correspondant n'est trouvé, l'infraction est fermée avec un code de fermeture par défaut.
Commentaires de fermeture renvoyés à l'attaque	Les commentaires de fermeture tels que définis dans le tableau de IBM QRadar bord sont affichés ici.
Motif de fermeture par défaut de l'incident de sécurité	Motif par défaut à utiliser lors de la fermeture d'un incident de sécurité, Lorsqu'un incident de sécurité est clos, un code de fermeture (ou le motif de fermeture) est spécifié dans l'enregistrement d'incident de sécurité, Si le code de fermeture ne correspond pas au motif de fermeture spécifié dans le tableau

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	de IBM QRadar bord et que vous essayez de fermer l'incident de sécurité, un message d'erreur s'affiche. Dans ce cas, le motif de fermeture par défaut spécifié ici est utilisé lors de la fermeture de l'incident de sécurité.



3. Cliquez sur **Terminer** pour terminer la configuration et faire passer le profil à l'état **En attente** .
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Activez ce profil pour extraire les infractions de la IBM QRadar console en fonction de votre planification.

Paramètres de configuration

Utilisez cette option pour modifier les propriétés système par défaut de l'intégration d'ingestion IBM QRadar .

Pour modifier les propriétés système, connectez-vous en tant qu'utilisateur disposant du rôle *sn_si.admin* et accédez à **Intégration d'IBM QRadar** > **Paramètres d'intégration d'IBM QRadar**.

Paramètres d'intégration d'IBM QRadar

Nom de la propriété	Description
Appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés dans la période de 24 heures. sn_sec_qradar.max_si_per_day	Spécifie le nombre maximal d'incidents de sécurité qui peuvent être créés en 24 heures. • Type : nombre entier • Valeur par défaut : 1 000

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Paramètres d'intégration d'IBM QRadar (suite)

Nom de la propriété	Description
Appliquez une limite au nombre d'infractions qui peuvent être regroupées en un seul incident. sn_sec_qradar.max_aggregation_per_si	Limite d'agrégation des infractions pour un incident de sécurité. Par exemple, s'il y a 102 infractions, les 100 premières infractions sont agrégées aux incident_1 de sécurité et les 2 autres aux incident_2 de sécurité. • Type : nombre entier • Valeur par défaut : 100
Cette propriété définit la période d'AQL pour extraire les événements/flux récents pour une infraction particulière. sn_sec_qradar.on_demand_recent_days_limit	Spécifie le nombre de jours pour extraire les événements ou flux récents pour une infraction particulière. • Type : nombre entier • Valeur par défaut : 7
Cette propriété limite le nombre d'événements récents récupérés pour une infraction particulière. sn_sec_qradar.on_demand_event_limit	Spécifie le nombre d'événements récupérés pour une infraction. Les événements les plus récents sont récupérés en premier en fonction de l'horodatage de l'événement. • Type : nombre entier • Valeur par défaut : 100
Cette propriété limite le nombre de flux récents récupérés pour une infraction particulière. sn_sec_qradar.on_demand_flow_limit	Spécifie le nombre de flux récupérés pour une infraction. Les flux les plus récents sont récupérés en premier en fonction de l'horodatage du flux. • Type : nombre entier • Valeur par défaut : 100
Cette propriété définit la valeur du délai d'expiration (secondes) pour l'AQL qui extrait les flux/événements récents pour une infraction particulière. sn_sec_qradar.on_demand_timeout	• Type : nombre entier • Valeur par défaut : 300
Délai d'expiration (secondes) des ID de recherche des enregistrements dans la file d'attente pour l'interrogation des AQL d'une infraction. sn_sec_qradar.sid_ttl	Délai d'expiration de l'AQL pour une infraction dans la file d'attente avant de créer un incident de sécurité. Par exemple, s'il y a 90 infractions, les 50 premières infractions sont traitées pour les données AQL dans le premier lot et les 40 infractions restantes dans le lot suivant dans le même intervalle d'interrogation. • Type : nombre entier • Valeur par défaut : 300

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres d'intégration d'IBM QRadar (suite)

Nom de la propriété	Description
Seuil permettant de contrôler le nombre de recherches qui peuvent être exécutées IBM QRadar à un moment donné et qui est déclenché par l'intégration planifiée job.sn_sec_qradar.records_threshold_in_que_for_val	Spécifie le nombre d'infractions que vous récupérez dans un seul lot dans un intervalle d'interrogation. • Type : nombre entier • Valeur par défaut : 50
Il s'agit du nombre de jours pour le nettoyage des tables d'intégration. sn_sec_qradar.queue_item_expire	Les tables d'intégration sont les suivantes : • sn_sec_qradar_events : événements IBM QRadar • sn_sec_qradar_flows : flux IBM QRadar • sn_sec_qradar_offense_updates - Mises à jour de l'attaque IBM QRadar • sn_sec_qradar_offense_to_task - Infraction IBM QRadar à Tâche • Type : nombre entier • Valeur par défaut : 30
Limite d'infractions par exécution de tâche planifiée par profil, que ce soit en récupération ponctuelle ou en ingestion continue. sn_sec_qradar.max_offense_limit_per_run	Spécifie le nombre d'infractions que vous récupérez dans le ServiceNow AI Platform en une seule récupération. • Type : nombre entier • Valeur par défaut : 1 000
Définissez cette propriété pour activer la fonctionnalité Mises à jour des infractions. sn_sec_qradar.get_offense_updates	**Remarque :** L'activation de ce paramètre peut entraîner un retard dans la création d'un incident de sécurité. • Type : vrai| faux • Valeur par défaut : faux

Tous les paramètres d'intégration modifiés seront appliqués au cours de l'intervalle d'interrogation suivant, tel que défini dans le profil.

Facultatif : copier un IBM QRadar profil

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils pour gagner du temps.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
En tant qu'utilisateur disposant du rôle sn_si.admin, si vous copiez un profil, le nom du profil est initialement modifié pour éviter les profils en double. En outre, le profil copié

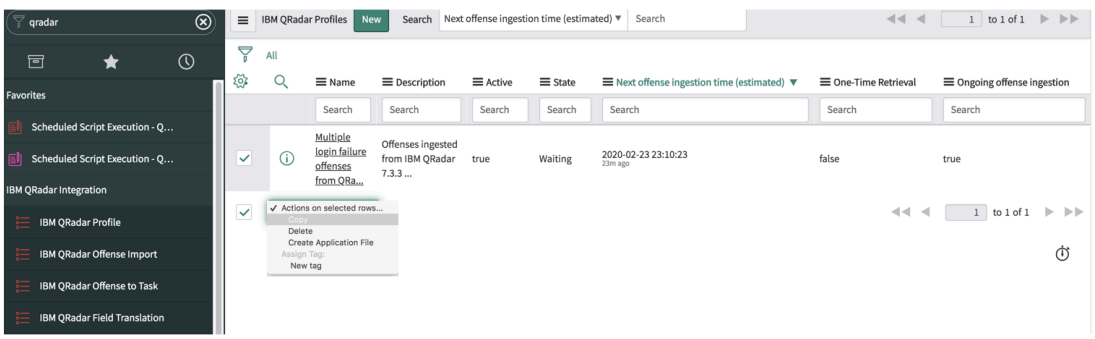
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

est désactivé (faux) et n'est donc pas activé accidentellement avant de terminer la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

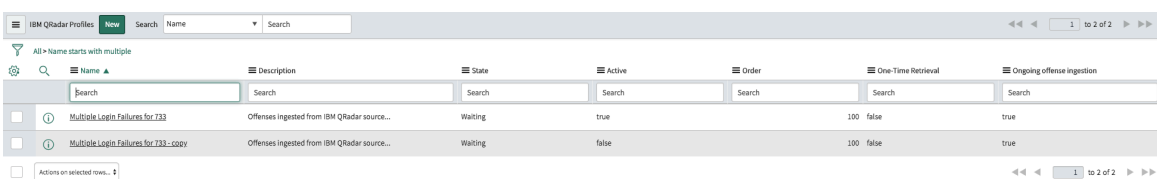
Procédure

1. Accédez à la **Tous** > **Intégration d'IBM QRadar** > **Profil IBM QRadar**.
2. Dans la liste IBM QRadar Profiles qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.



Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (vrai), la copie est désactivée à ce stade (faux). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.

Remarque : Si vous sélectionnez une source différente pour le profil, vous devez sélectionner de nouvelles règles (Sélectionner des IBM QRadar règles) pour le profil. Mais si vous utilisez la même source et sélectionnez de nouvelles règles, les infractions de l'échantillon seront effacées.



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. Notez que l'état de la colonne **Actif** est défini sur faux, car le profil doit être activé.

Que faire ensuite

Vous êtes invité à activer le nouveau profil une fois que vous avez terminé les étapes de configuration.

Séparation de domaine et IBM QRadar ingestion d'infractions

L'ingestion d'infractions prend en IBM QRadar charge Séparation de domaine. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau de prise en charge : basique

- Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de service de l'application.
- L'application prend en charge Séparation de domaine lors de l'exécution. Séparation de domaine inclut la séparation à partir de l'interface utilisateur, des clés de cache, du reporting, des déploiements et des agrégations.
- Le propriétaire de l'instance doit configurer l'application de sorte qu'elle fonctionne sur plusieurs locataires.

Exemple de cas d'utilisation : lorsqu'un fournisseur de service (SP) utilise la messagerie instantanée pour répondre au message d'un locataire-client, le client doit pouvoir afficher la réponse du SP.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

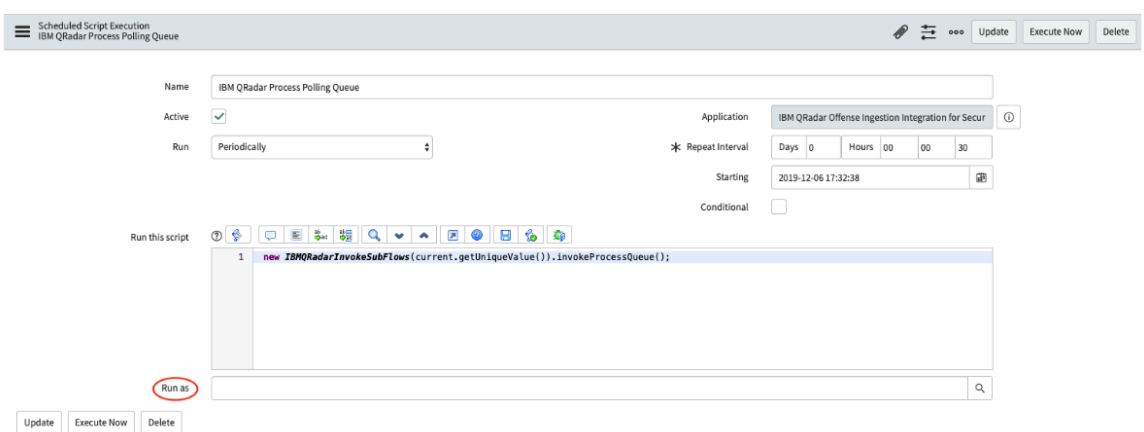
Fonctionnement de Séparation de domaine dans IBM QRadar Offense Ingestion

Pour procéder à la séparation en domaines, procédez comme suit :

- Créer un utilisateur avec le rôle `sn_si.admin` dans le domaine respectif.

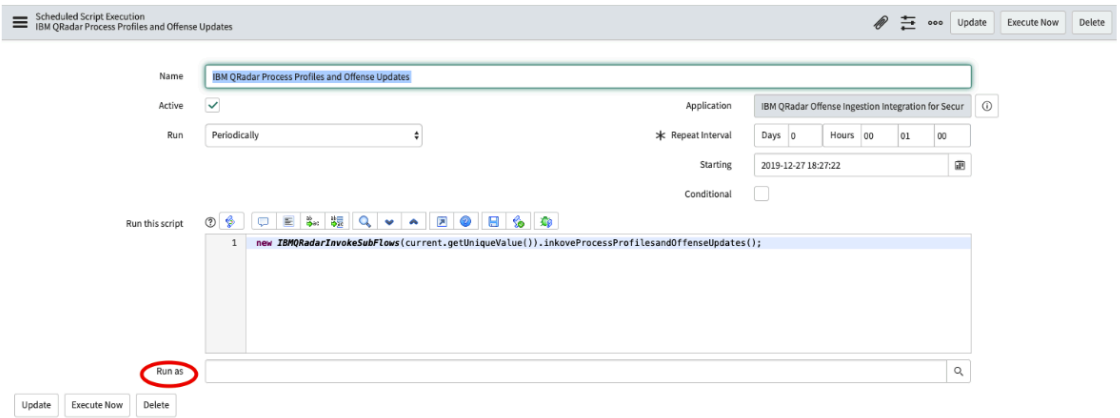
> **Remarque :** Lorsque vous créez le profil, utilisez le sélecteur de domaine pour sélectionner le domaine spécifique. Ne créez pas l'utilisateur dans le domaine parent et ne changez pas ultérieurement le domaine du profil. Vous devez avoir un utilisateur spécifique pour chaque domaine de votre profil avec le rôle `sn_si.admin` . Utilisez cet utilisateur pour créer ou modifier des paramètres dans le profil.

- Désactiver les travaux planifiés existants.
- Répliquer la file d'attente d'interrogation IBM QRadar du processus, les IBM QRadar profils de processus et l'attaque Met à jour les travaux planifiés pour chaque domaine.
- Passez « **Exécuter en tant que »** de l'utilisateur système à l'utilisateur disposant du rôle `sn_si.admin` dans le domaine respectif et exécutez la tâche planifiée.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Information associée

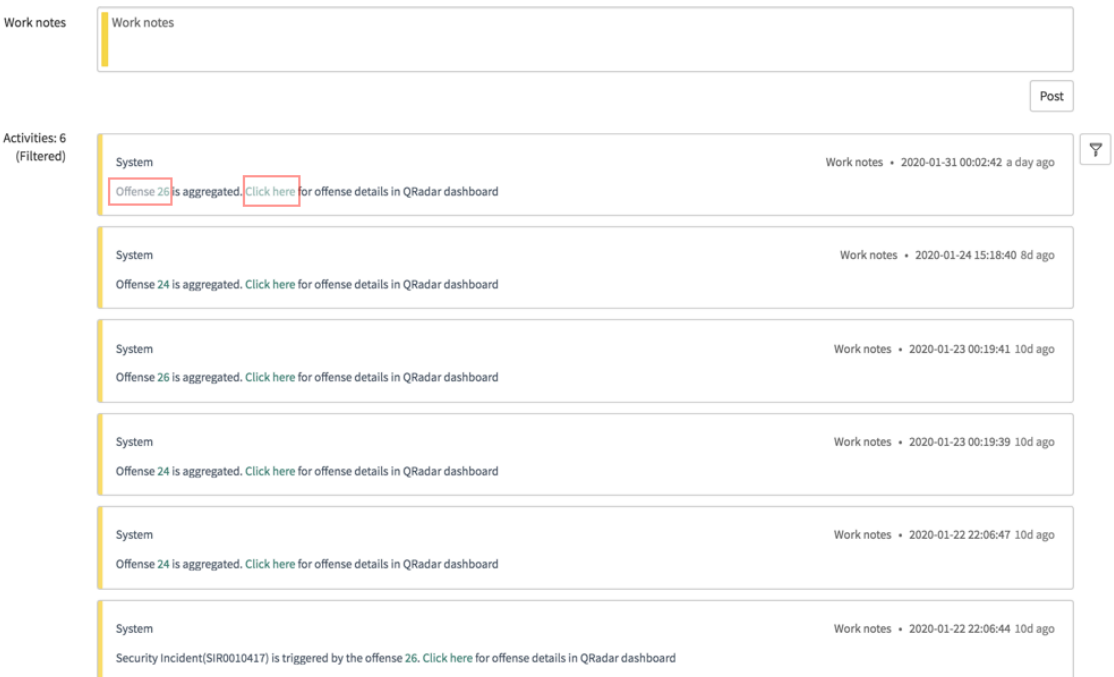
Séparation de domaine pour les fournisseurs de services

Formulaire Réponse aux incidents de sécurité après l'ingestion de l'infraction

Une fois qu'une IBM QRadar infraction a été ingérée, un incident de sécurité est créé et les mises à jour correspondantes sont apportées à l'enregistrement d'incident de sécurité.

Notes de travail

Une note de travail est publiée avec les détails de l'infraction qui a déclenché l'incident de sécurité.

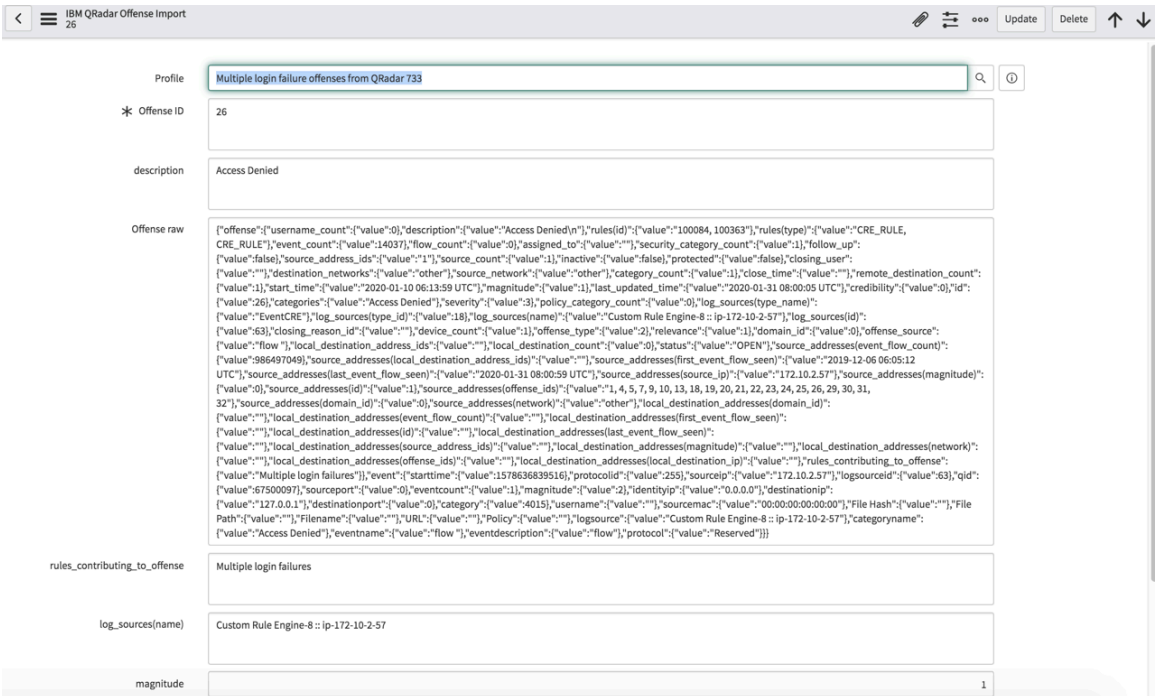


Cliquez sur le lien de l'infraction pour accéder à l'enregistrement d'incident de sécurité interne. Le lien hypertexte **Cliquez ici** vous amène au tableau de IBM QRadar bord où vous pouvez voir les détails de l'infraction.

Si vous aviez sélectionné l'option **Consigner la note de travail pour la nouvelle infraction** dans les critères d'agrégation des infractions, comme décrit dans le Mapper IBM QRadar les champs d'infraction aux champs de réponse aux incidents de sécurité, une note de travail est publiée lorsque l'infraction est agrégée.

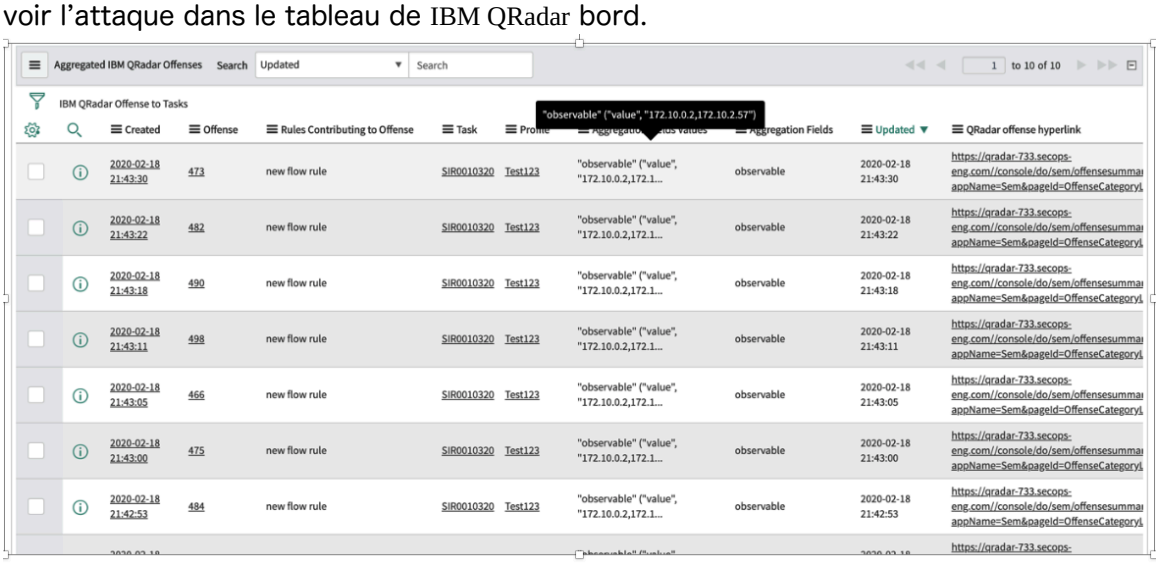
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Infractions agrégées

Cliquer sur **Listes connexes** > **Infractions IBM QRadar agrégées** pour afficher les infractions regroupées à l'incident de sécurité. Cliquez sur le lien hypertexte de l'attaque QRadar pour voir l'attaque dans le tableau de IBM QRadar bord.

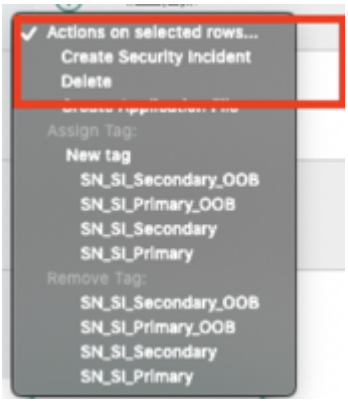


Créer un incident de sécurité : sélectionnez une infraction dans la liste, cliquez sur le menu **Actions** , puis sur **Créer un incident de sécurité**. Cette option crée un incident de sécurité pour l'infraction et cette infraction est désagrégée de l'incident de sécurité parent.

Supprimer l'enregistrement de l'infraction : sélectionnez une infraction dans la liste, cliquez sur le menu **Actions** , puis cliquez sur **Supprimer**. Cette option supprime l'enregistrement de l'infraction.

Traduction automatique

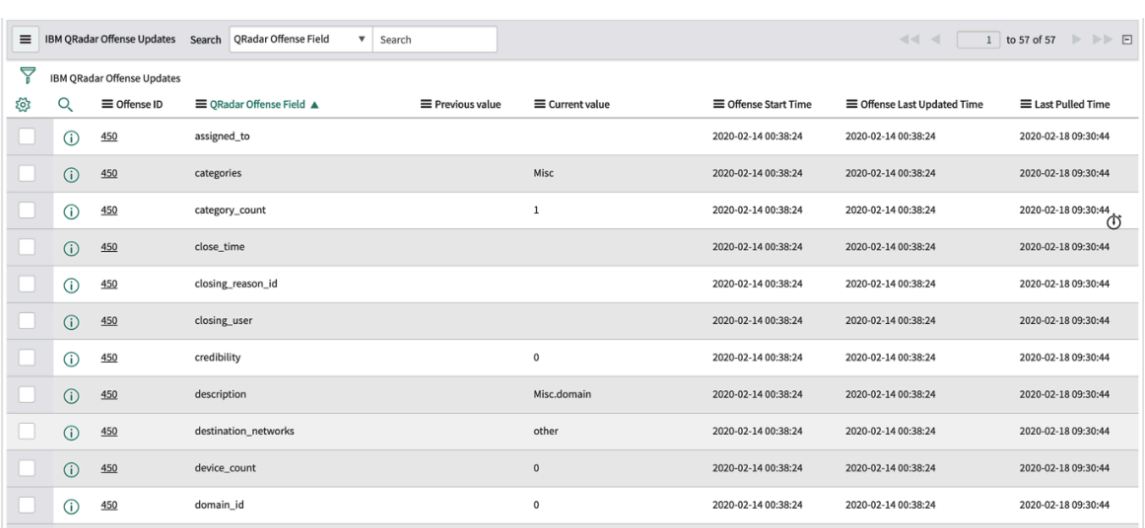
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Mises à jour de l'attaque IBM QRadar

Cela montre les champs d'attaque standard et personnalisés et suit les modifications apportées à l'attaque à chaque intervalle d'interrogation. Ceci est utile car vous pouvez voir les mises à jour des infractions directement sans naviguer vers le tableau de IBM QRadar bord. Tous les changements apportés aux valeurs sont affichés dans les champs Valeur précédente et Valeur actuelle.

Pour activer la fonctionnalité de mise à jour de l'infraction, accédez à **Intégration d'IBM QRadar** > **Paramètres d'intégration d'IBM QRadar** et activer **Définir cette propriété pour activer la fonctionnalité Mises à jour des infractions**. Par défaut, ce paramètre est désactivé.

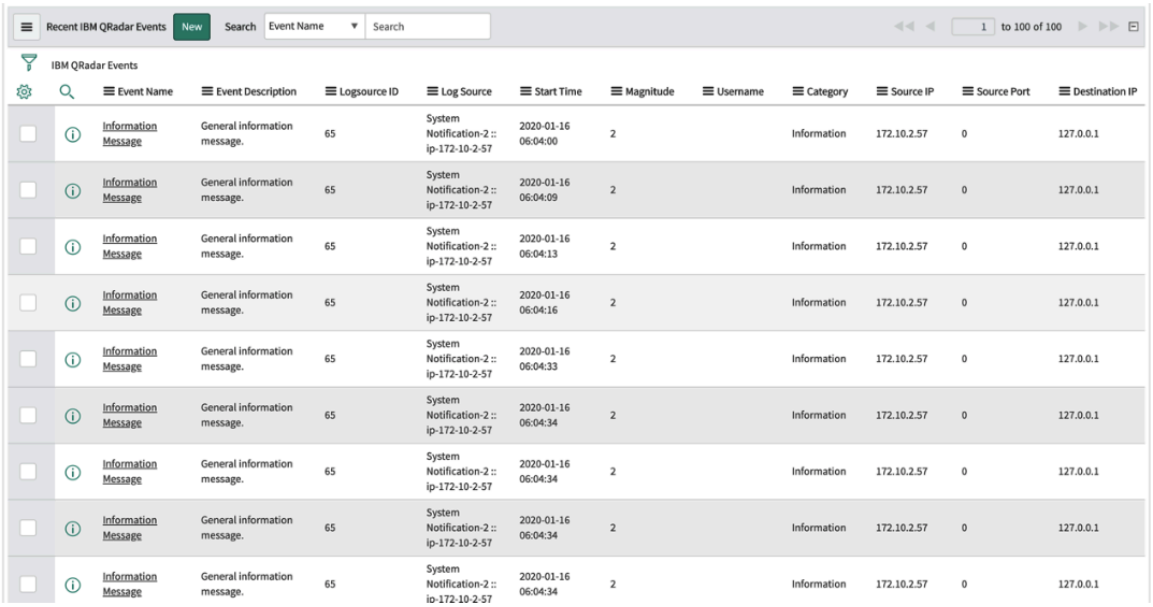


Événements IBM QRadar récents

Cliquez sur l'option **Extraire les événements IBM QRadar récents** sous **Liens connexes pour** afficher les événements les plus récents IBM QRadar .

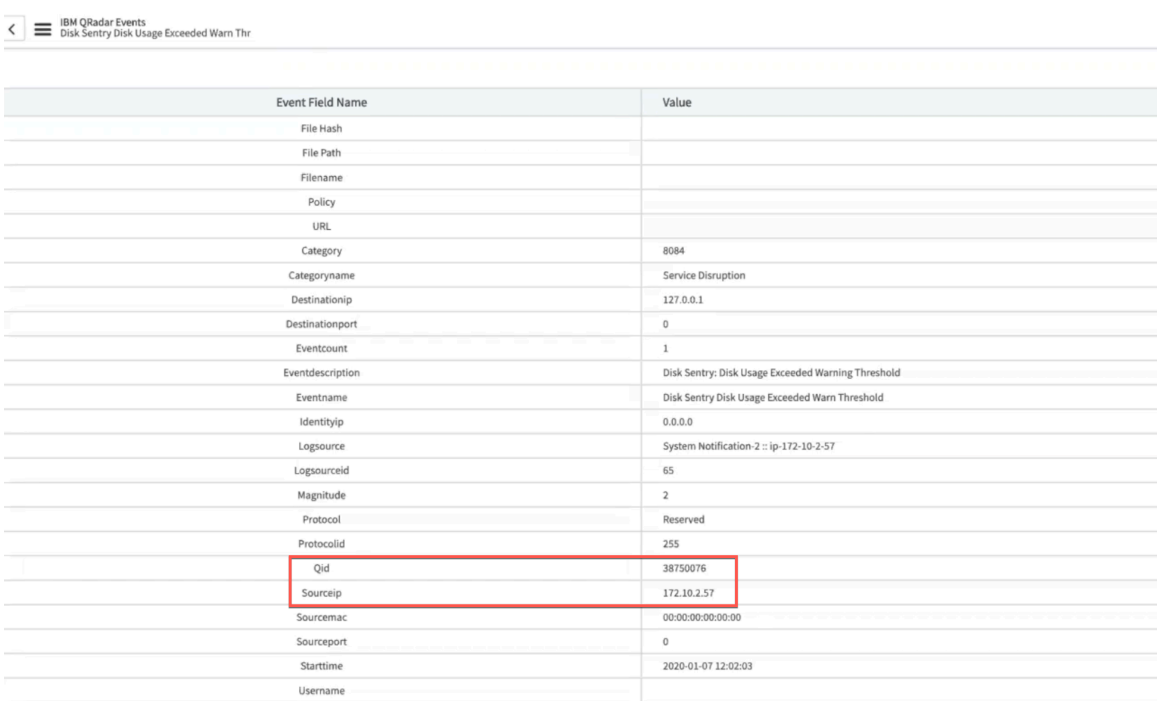
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Par défaut, un nombre maximal de 100 événements s'affiche. Vous pouvez modifier ce paramètre par défaut dans le Paramètres de configuration fichier .

Remarque : L'image ci-dessus montre les champs d'événement standard associés à l'infraction. Si vous avez configuré et mappé des champs d'événements personnalisés (reportez-vous à la section Mapper IBM QRadar les champs d'infraction aux champs de réponse aux incidents de sécurité), vous pouvez les afficher en mode Liste en cliquant sur le lien Nom de l'événement.



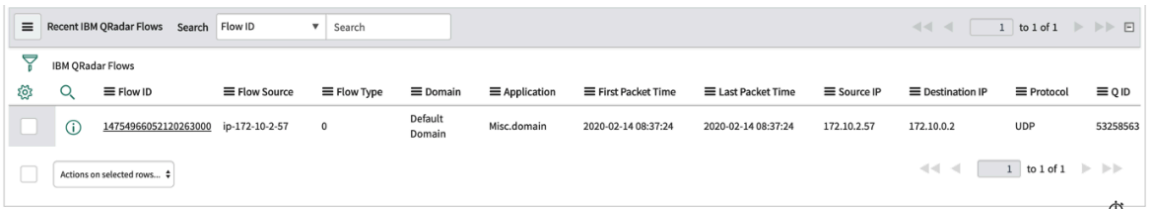
Flux IBM QRadar récents

À l'aide du concentrateur d'intégration et de Concepteur de flux, plusieurs flux, flux secondaires et actions sont disponibles avec l'intégration IBM QRadar . Lorsque vous cliquez sur l'option **Fetch Recent IBM QRadar Flows (Extraire les flux IBM QRadar récents**) sous les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

liens connexes, les flux les plus récents sont récupérés. Pour afficher ces flux, cliquez sur **Recent IBM QRadar Flows**.



Par défaut, un nombre maximal de 100 flux s'affiche. Vous pouvez modifier ce paramètre par défaut dans le Paramètres de configuration fichier .

Remarque : L'image ci-dessus montre les champs de flux standard associés à l'attaque. Si vous avez configuré et mappé des champs de flux personnalisés (voir Mapper IBM QRadar les champs d'infraction aux champs de réponse aux incidents de sécurité), vous pouvez les afficher dans la vue de listes en cliquant sur le lien ID de flux.

Utilisation de Flow Designer et du concentrateur d'intégration avec l'intégration de l'ingestion d'infractions IBM QRadar

À l'aide de Concepteur de flux et de la fonctionnalité IntegrationHub, plusieurs flux secondaires et actions ont été créés dans le cadre de l'intégration de l'ingestion IBM QRadar d'infraction.

Les flux secondaires suivants IBM QRadar sont disponibles :

- Validation de connexion et d'informations d'identification : elle est utilisée dans la tuile de configuration pour valider l'hôte et les informations d'identification dans la configuration initiale.
- Récupération des règles IBM QRadar : Cette option est utilisée dans la section Règles de la configuration du profil pour récupérer toutes les règles actives dans IBM QRadar. Ce flux secondaire est déclenché de façon asynchrone.
- Extraire des données d'exemples d'infractions à partir d'IBM QRadar : Ceci est utilisé dans la section Mappage de la configuration du profil pour extraire des données d'échantillon. Ce flux secondaire est déclenché de façon asynchrone.
- Mises à jour de l'état de l'infraction IBM QRadar : cette valeur est déclenchée par une tâche planifiée toutes les minutes et met à jour l'infraction lorsque IBM QRadar l'incident de sécurité est créé ou fermé.
- Traiter les profils à partir de la tâche planifiée et des infractions de file d'attente : cette action est déclenchée par une tâche planifiée toutes les minutes pour extraire les infractions par profil en fonction de l'intervalle d'interrogation. Cela extrait les infractions et les met en file d'attente vers la table d'interrogation pour un traitement ultérieur.
- Traiter la file d'attente d'interrogation et l'interrogation par lots : ceci est déclenché par une tâche planifiée toutes les 30 secondes pour traiter la file d'attente de la table d'interrogation.
- Extraire les flux IBM QRadar récents : cette opération est déclenchée à partir du lien du formulaire d'incident de sécurité pour obtenir les derniers flux d'infraction.
- Extraire les événements IBM QRadar récents : cette opération est déclenchée à partir du lien du formulaire d'incident de sécurité pour obtenir les derniers événements d'infraction.

Pour afficher ces flux secondaires, connectez-vous en tant qu'utilisateur disposant du rôle *sn_si.admin* et accédez à **Concepteur de flux** > **Concepteur**. Cliquez sur le lien Nom de l'un des flux secondaires répertoriés ci-dessus pour afficher le flux secondaire en détail.

Traduction automatique

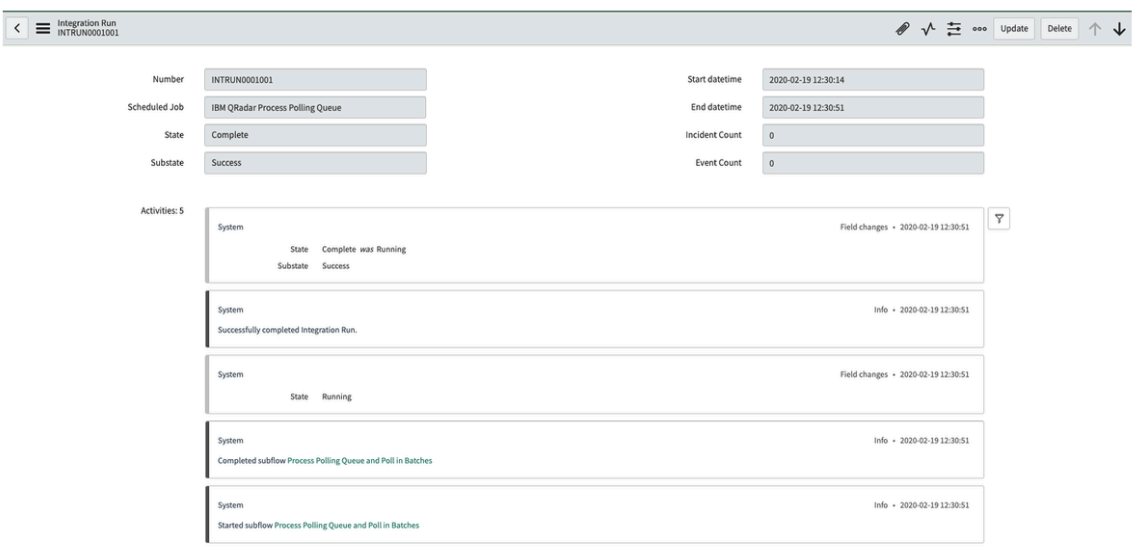
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage de l'intégration IBM QRadar de l'ingestion d'infractions

Cette section présente des conseils de dépannage importants et les questions fréquemment posées relatives à l'ingestion d'infractions IBM QRadar .

- Exécution de l'intégration : lorsqu'une tâche planifiée commence à s'exécuter, un enregistrement d'exécution de l'intégration avec des journaux, des erreurs et des avertissements s'affiche. Le nombre d'infractions extraites et le nombre d'incidents créés lors d'une exécution de tâche planifiée sont également affichés. Les utilisateurs disposant du rôle sn_si.analyst peuvent voir si des erreurs/profils ont échoué lors de l'extraction pendant l'exécution de l'intégration.

  Les notes de travail de l'exécution de l'intégration fournissent des liens vers les flux secondaires exécutés. Les utilisateurs disposant du rôle sn_si.analyst peuvent rechercher des erreurs survenues dans la table sn_event_ingestion_integration_run . Pour résoudre les problèmes d'intégration, vous devez d'abord vérifier l'exécution de l'intégration. Les erreurs sont enregistrées sous forme de notes de travail dans les enregistrements d'exécution de l'intégration pour chaque exécution de tâche planifiée.



- Problèmes SSL : lors de la connexion à IBM QRadar des instances dans le cloud, assurez-vous que l'instance dispose d'un certificat CA valide qui n'a pas expiré. Vous pouvez importer RSA ou vos propres certificats dans la plateforme et vous assurer que le nom commun du certificat correspond au nom d'hôte. Consultez https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 pour en savoir plus.
- Profil incomplet : lors de la configuration du profil, dans la section Options supplémentaires (Automatiser les mises à jour et la clôture des infractions en fonction de l'état de l'incident SIR), vous devez cliquer sur le bouton **Terminer** pour vous assurer que le profil est déplacé vers l'état En attente indiquant qu'il est en attente d'ingestion.
- Valider le profil : pour valider si l'intégration fonctionne correctement, vérifiez les états du profil, la date de la dernière extraction du profil, la table d'importation des infractions, les enregistrements de la table des infractions vers les tâches.
- Configuration du serveur MID : si vous installez l'application IBM QRadar sur site, après avoir configuré le serveur MID, vous devez créer une application de serveur MID. Le nom de l'application du Serveur MID doit être utilisé dans la vignette des configurations d'intégration au lieu du nom du Serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le délai d'expiration du service MID par défaut est de 30 secondes. Pour voir les instructions sur la désactivation du délai d'expiration, reportez-vous à la section <link>. Notez qu'il s'agit d'un changement à l'échelle du système qui peut avoir un impact sur d'autres intégrations.

- Mises à jour des infractions : si vous avez activé la propriété *sn_sec_qradar.get_offense_updates* et que vous remarquez un retard dans la création des incidents de sécurité, désactivez la propriété. N'activez pas cette propriété lorsque l'intervalle d'interrogation est faible et que la charge des infractions sur QRadar est élevée, car cela augmente la charge de la file d'attente.
- Données d'événement, de flux ou d'utilisateurs manquantes dans un incident de sécurité : si vous constatez que des données d'événement, de flux ou de remote_ip remote_ip ou des utilisateurs sont manquantes dans un incident de sécurité, augmentez le délai d'expiration (en secondes) du paramètre *sn_sec_qradar.sid_ttl* . L'augmentation de la durée retarde la création de l'incident de sécurité jusqu'à ce que les AQL terminent l'analyse de chaque infraction.
- Délais d'expiration : si vous affichez les erreurs de délai d'expiration dans les journaux d'application, examinez et modifiez les actions du Concepteur de flux suivantes :

Actions du Concepteur de flux

Paramètres	Action
Extraire des exemples d'infractions var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 60000) ;	Examinez et mettez à jour la durée en millisecondes.
Extraire des exemples d'infractions var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs) ;	Ajoutez un paramètre pour *executeAction* et entrez la durée en millisecondes.
Extraire les infractions pour les enregistrements de profil et de file d'attente dans la table d'interrogation var flow_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.fire_rest_for_offenses', flow_inputs, 180000) ;	Examinez et mettez à jour la durée en millisecondes.
Couche pour le test de la connexion REST var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.test_connection_rest', rest_inputs) ;	Ajoutez un paramètre pour *executeAction* et entrez la durée en millisecondes.
Couche pour le REST de validation des informations d'identification d'API var rest_outputs = sn_fd.FlowAPI.executeAction('sn_sec_qradar.validate_credentials_rest', rest_inputs) ;	Ajoutez un paramètre pour *executeAction* et entrez la durée en millisecondes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres	Action
Étape REST pour les mises à jour d'IBM QRadar Offense `var result = sn_fd. FlowAPI.executeAction('sn_sec_qradar.' +restStep, entrées,60000) ;`	Examinez et mettez à jour la durée en millisecondes.

IBM QRadar : intégration de l'enrichissement des incidents

L'intégration IBM QRadar - Enrichissement des incidents recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

- Introduction à l'intégration IBM QRadar - Enrichissement des incidents
- Créer des enregistrements de configuration de recherche de perceptions

---

Utiliser

- Exécuter une recherche de perceptions
- Security Operations Integration - Flux de recherche de perceptions
- Opérations de sécurité - Flux de recherche de perceptions QRadar
- Afficher les détails de la recherche de perceptions
- Afficher les résultats de recherche de perceptions

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Introduction à l'intégration IBM QRadar - Enrichissement des incidents

IBM QRadar est un produit SIEM (Knowledge Information and Event Management) d'entreprise qui s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration d'enrichissement des incidents, vous devez la télécharger à partir de et ajouter l'URL de base de l'API IBM QRadarServiceNow Store et la clé API appropriées.

Traduction automatique

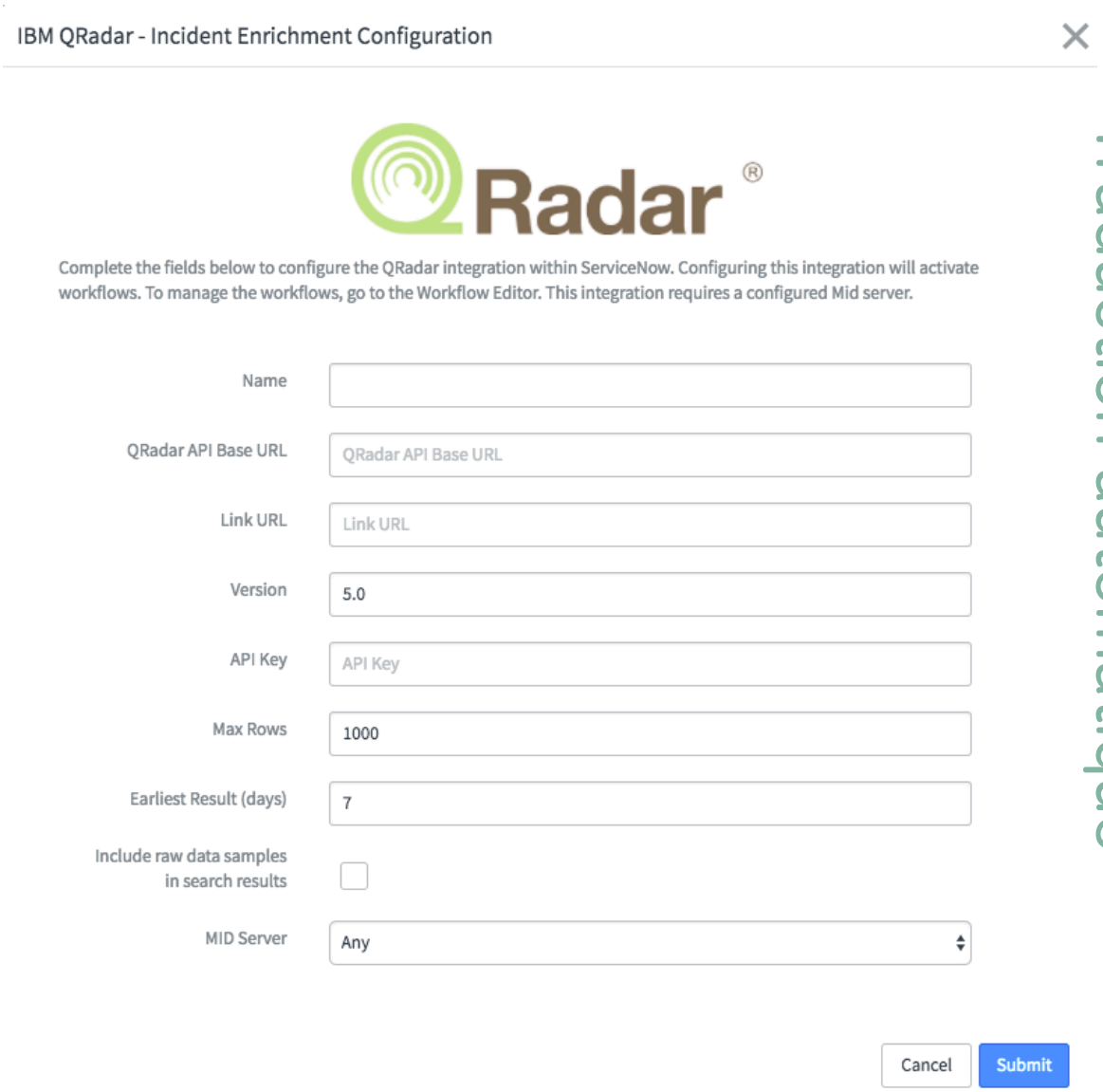
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_si_admin

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à IBM QRadar l'URL de base de l'API et à la clé API et procurez-les sous votre IBM QRadar profil.
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**. Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte - Enrichissement de l'incident IBM QRadar , cliquez sur **Nouveau**.



5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL de Base de l'API QRadar	URL de base que vous avez acquise sur le IBM QRadar site.
URL de lien	[Facultatif] L'URL de lien qui renvoie à une IBM QRadar instance, lorsqu'elle est disponible.
Version	La IBM QRadar version 5.0 est la version par défaut.
Clé API	La clé API que vous avez obtenue sur le IBM QRadar site.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend de votre paramètre dans la propriété **nombre de lignes de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	**Sélectionnez N'importe lequel** pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

6. Cliquez sur **Envoyer**.
   La carte de configuration d'intégration s'affiche.
7. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
8. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

LogRhythm Vue d'ensemble

La flexibilité de mappage de cette intégration fournit à l'analyste une visibilité sur les événements et les données d'alarme connexes qui peuvent être intégrés aux incidents de ServiceNow AI Platform sécurité pour une enquête et une correction plus approfondies.

Les profils d'alarme sont créés dans votre ServiceNow AI Platform instance pour personnaliser l'affichage des différents LogRhythm champs d'alarme sur un ServiceNow AI Platform incident de sécurité. Un mappage par défaut des champs d'alarme est fourni, qui peut être modifié pour répondre aux besoins spécifiques du client.

La figure suivante est un exemple d'environnement client. Lorsqu'un événement déclenche la création d'un incident de sécurité dans l'instance ServiceNow AI Platform® , une demande est envoyée à partir de votre ServiceNow AI Platform® instance pour déclencher des alarmes de la LogRhythm console client, soit via un serveur MID, soit sans.

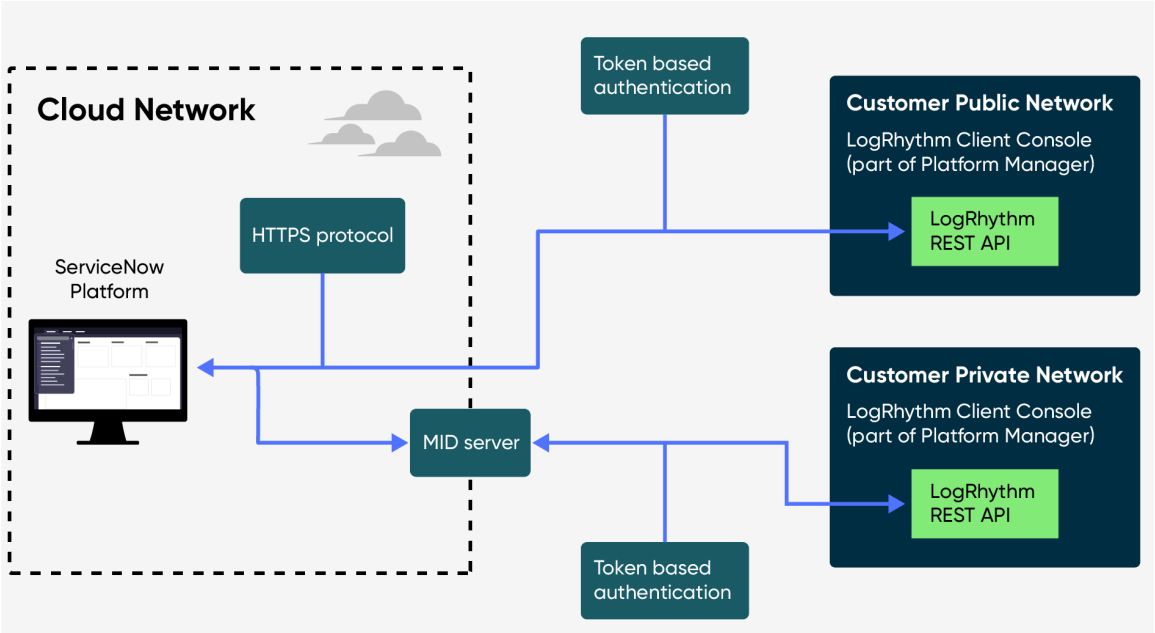
La clé API REST est utilisée par le pour s'authentifier ServiceNow AI Platform® auprès de la LogRhythm console client. Cette connexion permet à votre ServiceNow AI Platform instance de déclencher des alarmes individuelles LogRhythm en fonction des profils configurés.

L'API REST est utilisée pour collecter les détails des messages auxquels elle n'a pas accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration LogRhythm



Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Flexibilité de création de plusieurs profils d'alarme pour différents types d'alarmes tels que Hameçonnage et Programmes malveillants.
- Glisser-déposer le mappage des valeurs de champs d'alarme vers les champs d'incident LogRhythm de sécurité associés SIR .
- Un aperçu de la mise en page de l'incident de sécurité en fonction LogRhythm d'échantillons d'alarmesSIR.
- Ingérer les alarmes historiques, ainsi que les alarmes futures en cours à intervalles configurables.
- Fermeture automatisée LogRhythm de l'alarme lors de la fermeture de l'incident SIR . Une URL vers l'incident ainsi qu'un ID de l'incident sont fournis pour faciliter la SIR consultation.

Versions prises en charge de ServiceNow AI Platform

Cette intégration est compatible avec la version Quebec ou ultérieure du .ServiceNow AI Platform®

Versions prises en charge de LogRhythm

Cette intégration est compatible avec LogRhythm la version 7.8 ou ultérieure. Les versions antérieures ne sont pas prises en charge en raison des limitations de l'API.

Remarque : Les rubriques suivantes sont numérotées. Pour une installation fluide et pour vous aider à vérifier les résultats attendus, suivez les rubriques dans l'ordre dans lequel elles sont présentées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'API REST pour LogRhythm

Vous utilisez la clé API REST pour collecter des détails d'événement LogRhythm supplémentaires pour des champs d'alarme individuels. La clé API fournit des détails qui ne sont pas disponibles à l'aide de l'API LogRhythm REST.

Avant de commencer

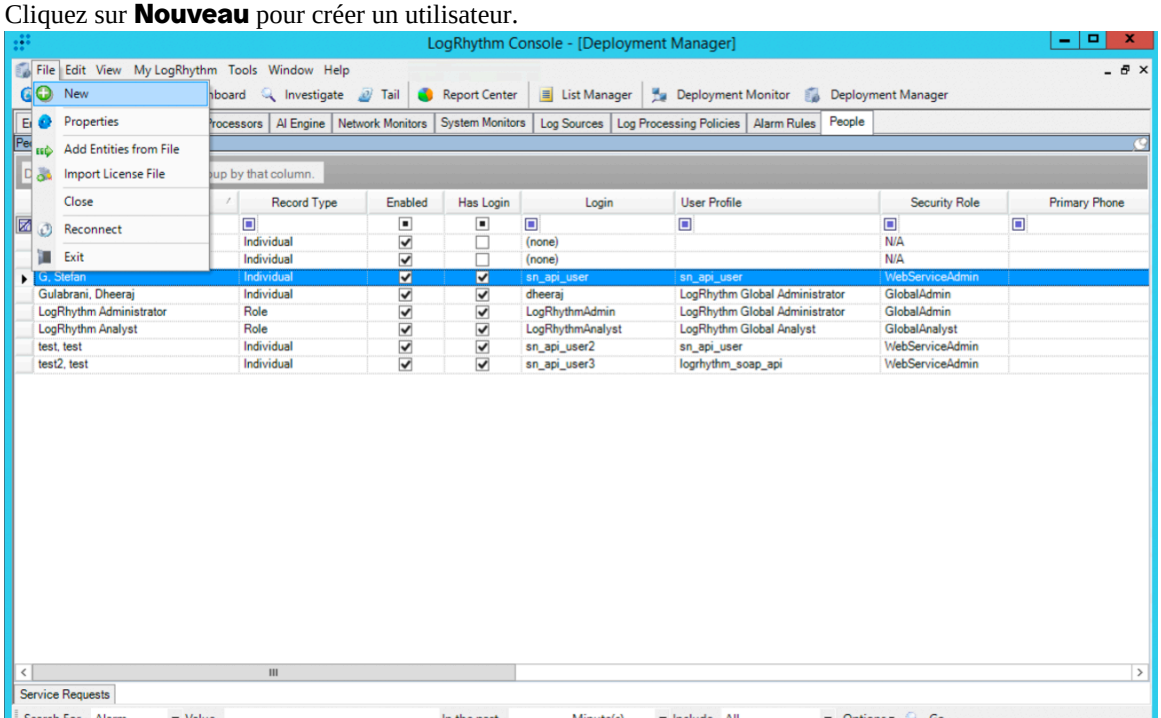
Rôle requis : LogRhythm administrateur de la console client/gestionnaire de la plateforme

Pourquoi et quand exécuter cette tâche

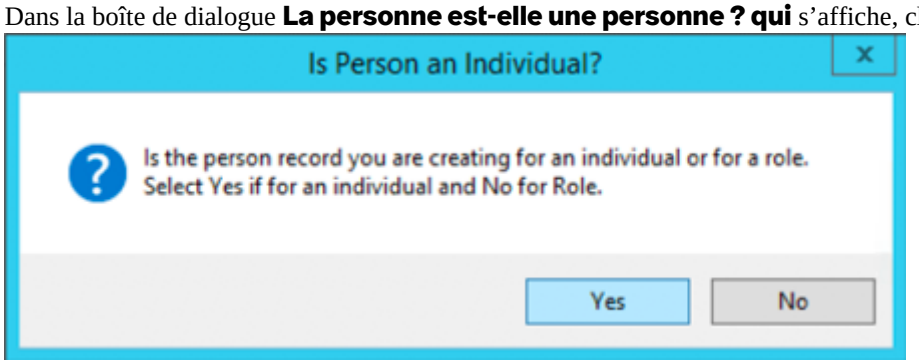
Cette tâche est effectuée sur la LogRhythm console client. Configurez l'API LogRhythm REST avant d'installer le module d'extension ServiceNow Storeà partir du .

Procédure

1. Accédez à la LogRhythm console client et sélectionnez le menu **Fichier** .
2. Cliquez sur **Nouveau** pour créer un utilisateur.



3. Dans la boîte de dialogue **La personne est-elle une personne ? qui** s'affiche, cliquez sur **Oui**.

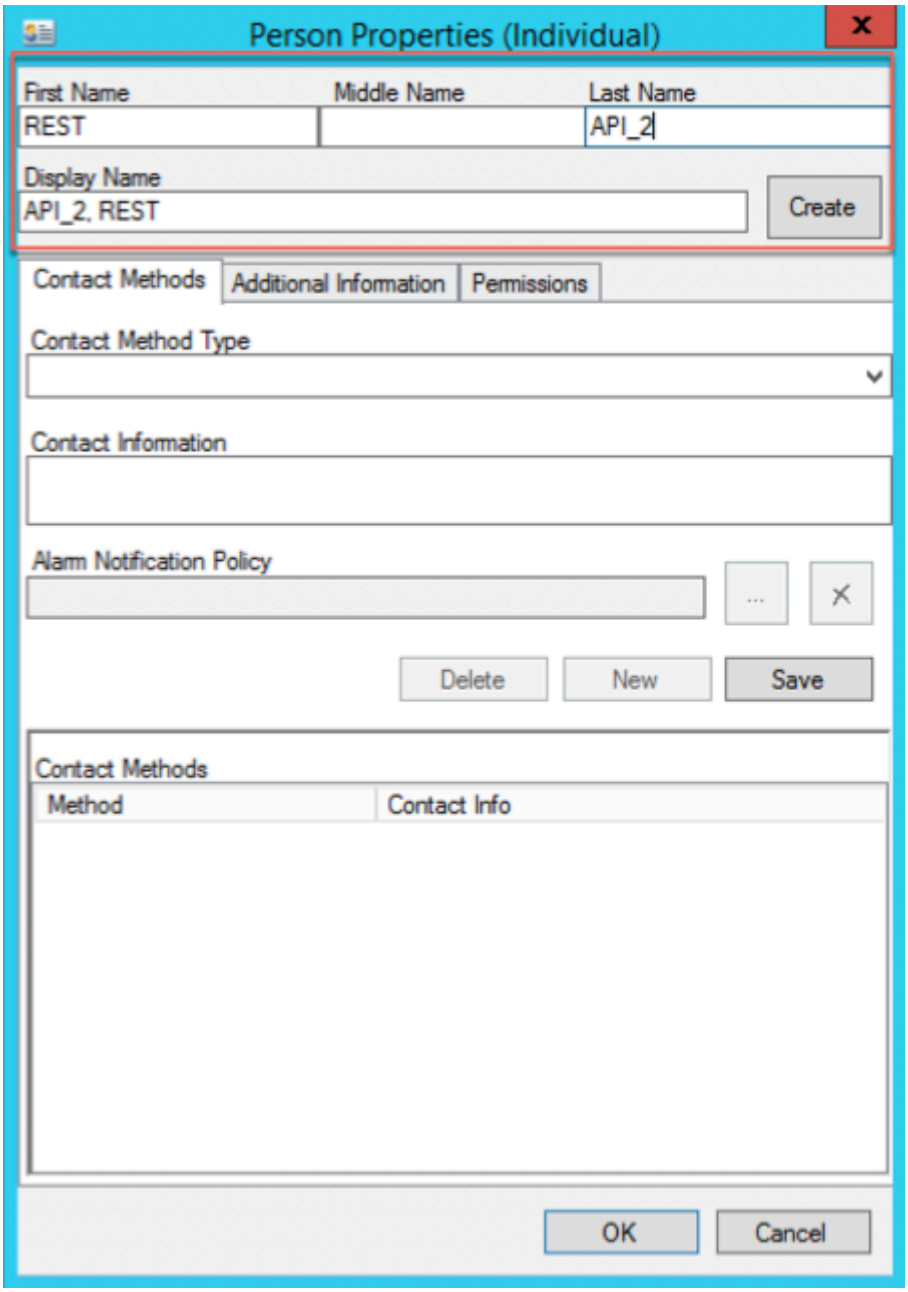


4. Dans la boîte de dialogue Propriétés de la personne qui s'affiche, renseignez les champs Nom.

   Utilisez un nom pour l'API LogRhythm REST différent de celui que vous avez utilisé pour créer l'API REST, par exemple, REST API_2.

Traduction automatique

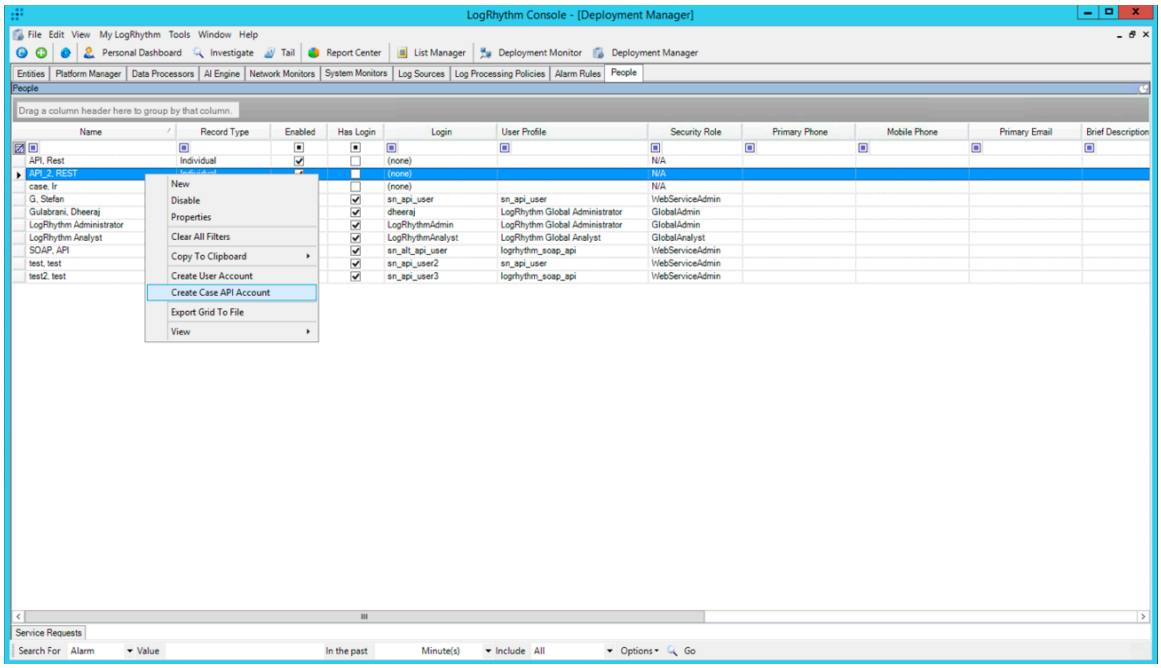
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **OK**.
6. Cliquez avec le bouton droit sur la nouvelle liste dans la colonne Nom (**API_2_REST**) et, dans la liste de choix, sélectionnez **Créer un compte API de ticket**.

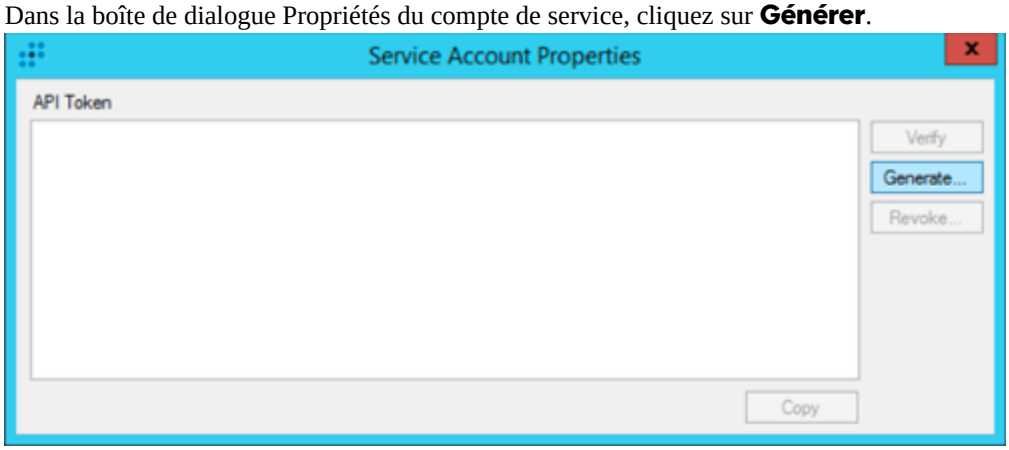
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

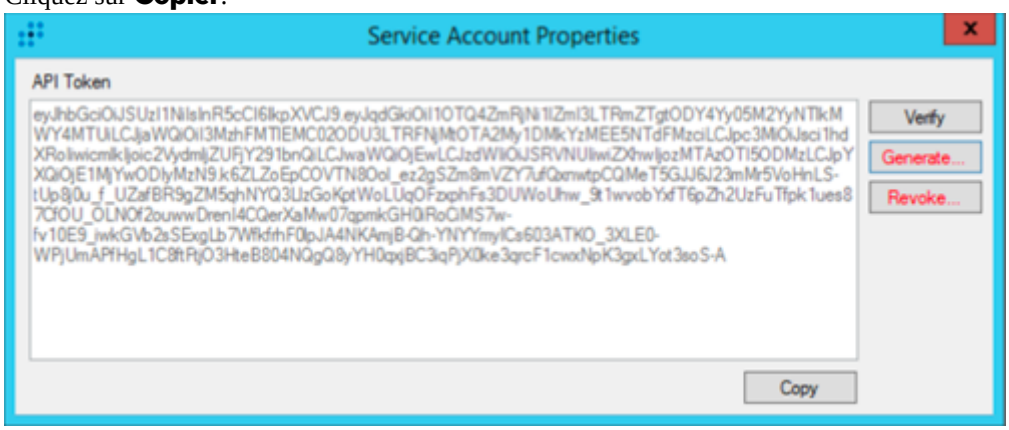


Remarque : L'API de ticket n'est pas utilisée, mais les informations d'identification du compte d'API de ticket et de l'API LogRhythm REST sont les mêmes.

7. Dans la boîte de dialogue Propriétés du compte de service, cliquez sur **Générer**.



8. Cliquez sur **Copier**.



Vous avez maintenant configuré l'API LogRhythm REST. Veuillez coller la chaîne que vous avez copiée à l'étape précédente dans votre ServiceNow AI Platform instance dans le champ Jeton d'API LogRhythm REST pendant les étapes de configuration répertoriées dans Installer le module d'extension et configurer LogRhythm.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Vous êtes maintenant prêt à Installer le module d'extension et configurer LogRhythm.

Installer le module d'extension et configurer LogRhythm

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que l'application s'intègre Opérations de sécurité correctement sur le ServiceNow AI Platform®.

Avant de commencer

Rôle requis : admin

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides. La dernière LogRhythm version est 7.8 ou ultérieure.

Remarque : Vos profils d'alarme existants ne seront plus pris en charge sur la dernière LogRhythm version, vous devez donc créer de nouveaux profils d'alarme et effectuer les configurations requises.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform® et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (admin) installe le module d'extension de l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Le (sn_si.admin) supervise les tâches suivantes : ◦ Nomme, crée et modifie les profils d'alarme. ◦ Mappe et filtre les alarmes : identifie les alarmes spécifiques LogRhythm qui créent des incidents de sécurité et configure la façon dont ces champs d'alarme sont mappés à un ServiceNow AI Platform® incident de sécurité. ◦ Prévisualise les détails de l'incident de sécurité pour plus d'exactitude avant de finaliser la configuration. ◦ Ingère les alarmes historiques et planifie les alarmes extraites. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Ce rôle a également accès au Opérations de sécurité module. • L'analyste des incidents de sécurité (sn_si.analyst) répond aux incidents de sécurité créés en fonction des paramètres du profil d'alarme.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
Obtenez un nom d'utilisateur et un LogRhythm mot de passe d'API et vérifiez que vous utilisez la version LogRhythm 7.8 ou ultérieure.	Visitez le site Web du produit pour plus d'informations sur les clés API et pour créer un compte : site Web de LogRhythm Enterprise . Les comptes d'utilisateurs, les informations d'identification et les certificats doivent être configurés correctement avant l'installation de l'application. L'intégration nécessite LogRhythm la version 7.8 ou ultérieure et les LogRhythm API REST. Consultez Configurer l'API REST pour LogRhythm.
Vérifiez que vous avez installé et configuré un Serveur MID.	Un Serveur MID est requis dans votre ServiceNow AI Platform environnement. Consultez le site Web de la documentation produit ServiceNow pour plus d'informations sur l'installation et la configuration des serveurs MID.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Pour la version Rome et les versions de famille ultérieures, le module d'extension Réponse aux incidents de sécurité Dépendance (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Orchestration du support de sécurité Pour en savoir plus sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une Opérations de

Traduction automatique

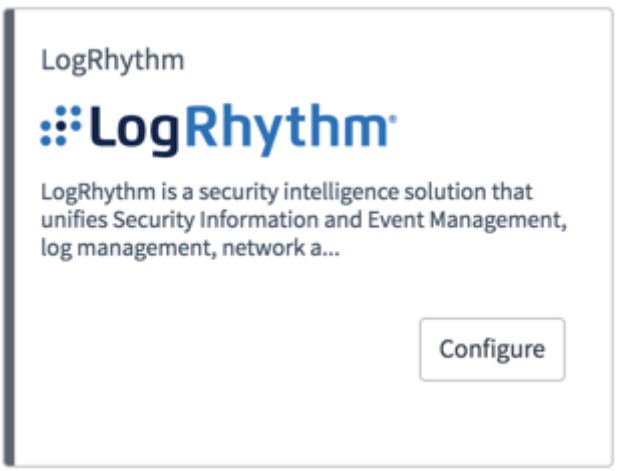
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	sécurité application et Activer une ServiceNow Store application.

Important : Si vous rencontrez des problèmes de connectivité à la LogRhythm console client, reportez-vous à la section Vérifier la connectivité pour LogRhythm.

Procédure

1. Si vous n'avez pas installé l'application pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes d'installation.
2. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la LogRhythm tuile.
3. Cliquez sur **Configurer**.



4. Cliquez sur le lien **Nouvelle configuration** .



5. Renseignez les champs suivants du formulaire :

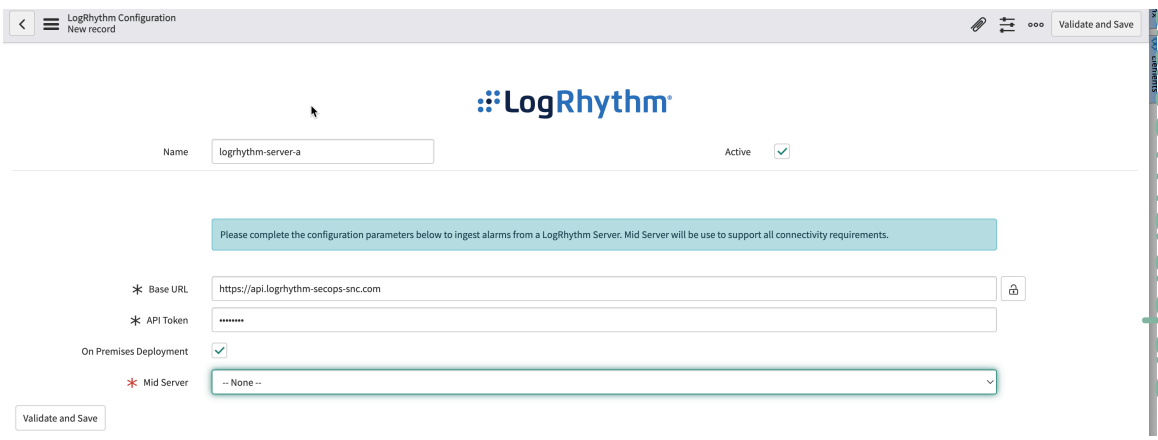
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration LogRhythm

Champ	Description
Nom	LogRhythm Nom du serveur, par exemple, logrhythm-server-a.
URL de base	URL de base hébergeant l'API LogRhythm REST. Le serveur MID permet d'accéder au réseau où la console cliente LogRhythm est hébergée. Cette URL est l'endroit où le serveur est hébergé au sein de LogRhythm ce réseau. Cliquez sur l'icône de verrou à droite pour modifier le champ et saisissez du texte pour une URL, par exemple, https://logrhythm.secops-eng.com:8501/.
Jeton d'API	Entrez le jeton associé à votre API REST que vous avez créé sur la LogRhythm console client.
Déploiement sur site	Option permettant de sélectionner s'il s'agit d'un LogRhythm déploiement sur site.
Serveur MID	Serveur MID spécifique configuré dans votre environnement. Seuls les MID Servers actifs et validés sont disponibles dans cette liste de choix.

La figure suivante est un exemple de formulaire rempli.



Traduction automatique

6. Cliquez sur **Valider et enregistrer**.
   Une fois la validation terminée, un message s'affiche et la LogRhythm page Configurations est rechargée. L'étape suivante consiste à créer un profil d'alarme.

Que faire ensuite

Une fois la validation terminée, l'étape suivante consiste à Création d'un profil d'alarme pour LogRhythm.

Création d'un profil d'alarme pour LogRhythm

Dans un profil d'alarme que vous créez et nommez, vous spécifiez les alarmes que vous souhaitez extraire de la LogRhythm console client. Vous définissez également la façon dont ils sont mappés aux champs d'un ServiceNow AI Platform incident de sécurité.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

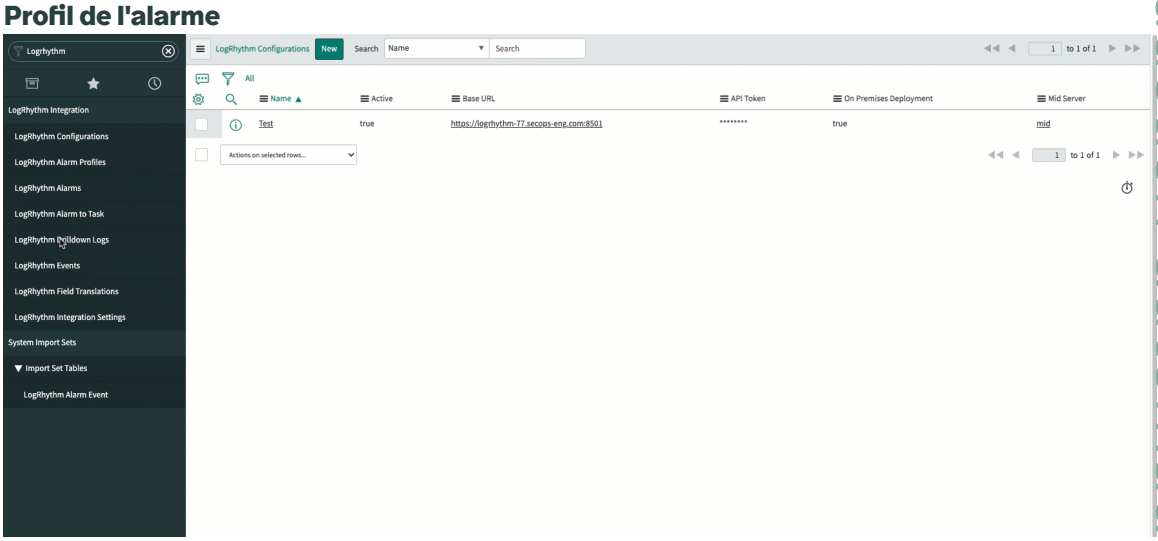
Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
En fonction du profil d'alarme configuré, un profil d'alarme peut ingérer tous les types d'alarmes prêtes à l'emploi, mais vous pouvez utiliser des critères de filtre pour ingérer des types d'alarmes spécifiques. Grâce à cette ServiceNow AI Platform intégration, toutes les règles d'alarme configurées ou spécifiques basées sur le profil créé sont ingérées. Les règles d'alarme, telles que les alarmes de niveau de risque élevé uniquement, peuvent ensuite être filtrées pour spécifier quelles alarmes doivent créer des incidents de sécurité. Avant la création d'incidents de sécurité, les valeurs de champ individuelles des alarmes filtrées sont mappées aux champs correspondants de l'incident ServiceNow AI Platform de sécurité. Cette configuration se fait via un profil d'alarme au sein de votre ServiceNow AI Platform instance.

Procédure

1. Accédez à la **Tous** > **Intégration de LogRhythm**.
2. Sélectionnez le module **Profils d'alarme LogRhythm** pour afficher la liste **des profils d'alarme** .

Profil de l'alarme



3. Pour créer un nouveau profil d'alarme, cliquez sur **Nouveau**.
   Un nouveau formulaire de profil d'alarme s'affiche. En haut de la page, dans la barre de progression, **le nom** est sélectionné. Cette barre suit votre progression au cours de la configuration.
4. Renseignez les champs du formulaire.

Profil de l'alarme

Champ	Description
Nom	Nom du profil d'alarme. Ce nom vous permet d'identifier les types d'alarmes tels que *Accès non autorisé* (*VPN*),*Programmes malveillants* ou *Hameçonnage*.
Description brève	Texte court pour plus d'informations sur le profil d'alarme, qui peut inclure le type d'alarmes ou une catégorie d'alarme. Un exemple de description : Toutes les alarmes associées à des tentatives d'accès non autorisées à Powershell et Sudo.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Serveur source dans la liste de choix. La liste se compose des LogRhythm configurations que vous avez déjà configurées, par exemple, `logrhythm-server-a`. Consultez Installer le module d'extension et configurer LogRhythm.
Ordre	Priorité du profil d'alarme. Ce champ indique l'ordre dans lequel les profils d'alarme sont exécutés lorsque deux profils d'alarme ou plus partagent les conditions de déclenchement.
Actif	Par défaut, cette option n'est pas sélectionnée. Une fois que vous avez terminé toutes les étapes de configuration du profil d'alarme et que vous avez cliqué sur **Terminer**, vous êtes invité à cocher cette case pour activer le profil d'alarme. Lorsque le profil d'alarme est actif, il déclenche automatiquement des alarmes de la LogRhythm console client.

5. Cliquez sur **Continuer** pour enregistrer vos données et passer au formulaire Mappage.

   Si la validation réussit, la page se recharge et le formulaire **de mappage** s'affiche. Vous ne pouvez pas procéder à la configuration tant que vous n'avez pas validé votre connexion et vos informations d'identification.

Information associée

Mappage

Mappage

Après avoir sélectionné la source que vous souhaitez ingérer, vous devez mapper les LogRhythm champs d'alarme individuels LogRhythm aux champs d'incident ServiceNow AI Platform de sécurité.

Le mappage des alarmes comprend les tâches suivantes :

- Alarmes de carte LogRhythm . Pour cette tâche, vous répertoriez et ingérez (pull) des échantillons d'alarmes à l'aide des ID d'alarme ou des alarmes les plus récentes de la LogRhythm console client.
- Les champs Échantillon d'alarme sont classés en trois groupes :
  - Champs d'alarme : les champs d'alarme disponibles et leurs valeurs correspondantes sont affichés.
  - Champs d'événement : les champs d'événement disponibles et leurs valeurs correspondantes sont affichés.
  - Champs DrillDownLog : les champs de journal d'exploration disponibles et leurs valeurs correspondantes sont affichés.
- Chaque ID d'alarme que vous avez extrait s'affiche sous forme d'onglet. Dans les onglets ID d'alarme, vérifiez que tous les champs d'alarme critiques de la section Ingestion d'échantillons d'alarme à gauche du formulaire sont mappés à la section Mappage du champ d'incident SIR à droite du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Une fois que vous avez mappé les alarmes au champ Mappage de champ d'incident SIR , vous pouvez voir la catégorie d'alarme s'afficher également dans le champ Expression d'entrée . Par exemple, ${Alarm : alarmid}$.
- Vous pouvez modifier la configuration en ajoutant ou en supprimant des champs sur l'incident de sécurité. Suivez les champs négligés ou dupliqués à l'aide du code couleur fourni.
- Vous pouvez filtrer les alarmes pour spécifier quelles alarmes sont ingérées dans l'application SIR. Vous pouvez filtrer les alarmes directement ou utiliser les catégories d'alarmes pour analyser votre recherche en fonction des alarmes, des événements ou des DrillDownLogs.
- Utilisez l'éditeur de script si vous souhaitez formater les valeurs pour les champs Priorité et Catégorie de l'incident de sécurité.

L'étape suivante consiste à Mapper LogRhythm les champs d'alarme aux champs d'incident de sécurité.

Information associée

Mapper LogRhythm les champs d'alarme aux champs d'incident de sécurité

Utiliser l'éditeur de script pour formater LogRhythm les valeurs

Filtrer les alarmes pour LogRhythm

Mapper LogRhythm les champs d'alarme aux champs d'incident de sécurité

Vous mappez les champs d'alarme individuels aux champs d'incident de sécurité. Le mappage préconfiguré peut être modifié et le code couleur fourni pour les champs vous aide à surveiller les alarmes que vous avez déjà mappées. Cette étape vous permet de visualiser l'impact de vos modifications sur les champs de l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

Si vous n'êtes pas familier avec les LogRhythm alarmes, accédez à la LogRhythm console client et passez en revue quelques exemples d'ID d'alarme. Pour l'exemple suivant, LogRhythm les alarmes 9468 et 9474 ont été utilisées pour mapper les alarmes à l'incident de sécurité.

Pourquoi et quand exécuter cette tâche

À l'aide de ce formulaire, vous mappez les règles d'alarme LogRhythm à gauche avec les champs d'incident de sécurité à droite.

La figure suivante montre le mappage par défaut des alarmes préconfiguré pour chaque profil d'alarme. Ce mappage par défaut peut être modifié et, grâce à ce formulaire, vous pouvez personnaliser les champs qui renseignent l'incident de sécurité. Une fois ce mappage terminé, vous pouvez voir comment l'ajout ou la suppression de champs d'alarme peut avoir un impact sur les valeurs de champ de l'incident de sécurité.

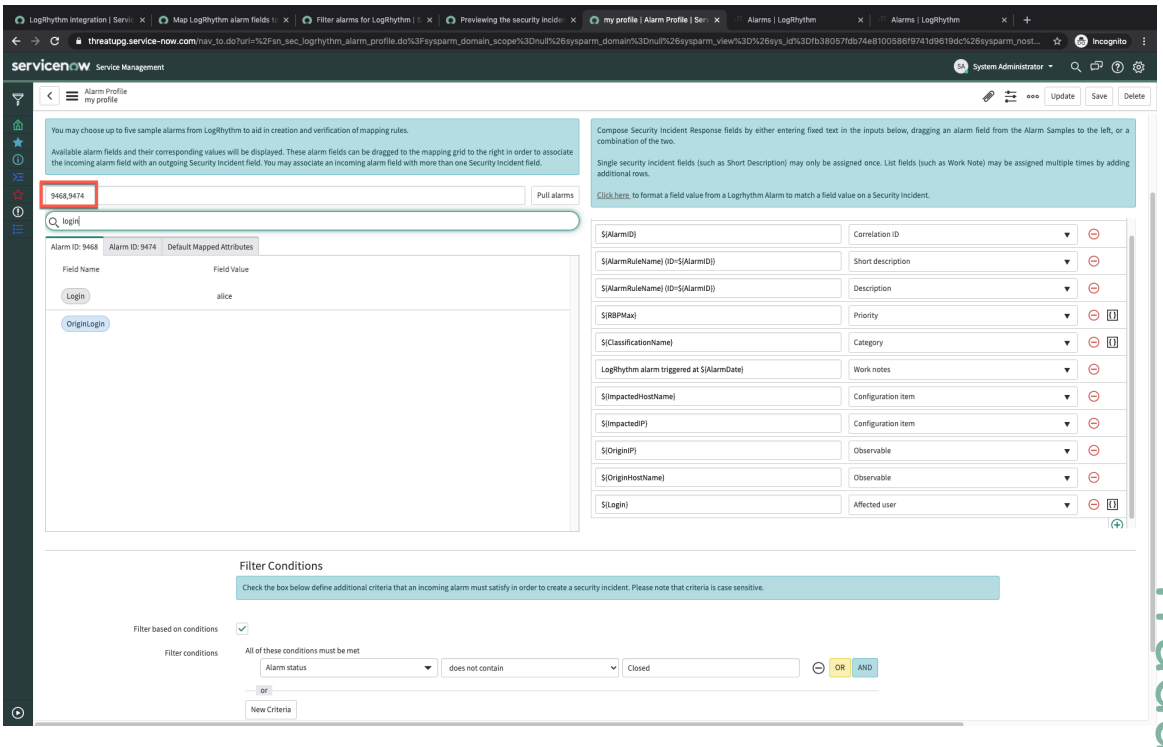
Sur le côté gauche de ce formulaire, dans la figure suivante, les règles d'alarme LogRhythm sont décrites. Les valeurs de ces règles d'alarme sont mappées aux champs d'incident de sécurité sur le côté droit du formulaire.

Procédure

1. Après avoir créé un profil d'alarme pour LogRhythm, cliquez sur **Mappage** dans la barre de progression.
2. Dans le champ **Ingestion d'échantillon d'alarme** , saisissez jusqu'à cinq ID LogRhythm d'échantillon d'alarme séparés par des virgules (9468, 9474).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. À côté du champ d'alarme, cliquez sur **Extraire les alarmes**.

L'extraction des échantillons d'alarmes peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran.

Une fois que les ID d'alarme d'échantillon ont été soumis et extraits avec succès du LogRhythm serveur, les champs d'alarme et leurs valeurs correspondantes sont affichés dans des onglets.

Remarque : Après l'extraction réussie d'un ID d'alarme, le ServiceNow AI Platform peut renvoyer le message suivant : Les nouveaux champs suivants seront disponibles pour le filtrage sous peu. Veuillez recharger ce profil dans quelques minutes si le filtrage basé sur ces champs est requis. itemspacketsin, itemspacketsout.

Ce message s'affiche lorsque l'alarme unique qui a été déclenchée contient des noms de champs qui n'ont pas encore été traités par le ServiceNow AI Platform. Ces champs sont disponibles pour le mappage, cependant, si ce message s'affiche, rechargez le formulaire afin que ces champs soient affichés et disponibles dans les listes de choix de filtres du générateur de conditions lorsque vous êtes prêt à définir les conditions de filtrage.

L'ingestion de ces échantillons d'alarmes dans la configuration du profil d'alarme vous aide à éviter de mapper à l'incident de sécurité les champs d'alarme qui ne contiennent aucune valeur. Il aligne également les champs d'alarme sur les valeurs sur les champs appropriés dans l'incident de sécurité. Cette étape garantit que tous les champs d'alarme critiques sont mappés et qu'il n'y a pas de valeurs de champ manquantes sur l'incident de sécurité.

Pour vous assurer qu'aucune alarme n'est négligée ou dupliquée dans le processus de mappage, les champs d'alarme sont codés par couleur. Un champ d'alarme bleu clair (Account, AlarmRuleID, AlarmStatus, entre autres) indique qu'aucun champ n'est encore sélectionné pour le mappage à un incident de sécurité.

Un champ gris (AlarmDate, AlarmID et AlarmRuleName) indique qu'un champ a déjà été sélectionné et a été mappé à un champ de l'incident de sécurité. Ce code couleur vous

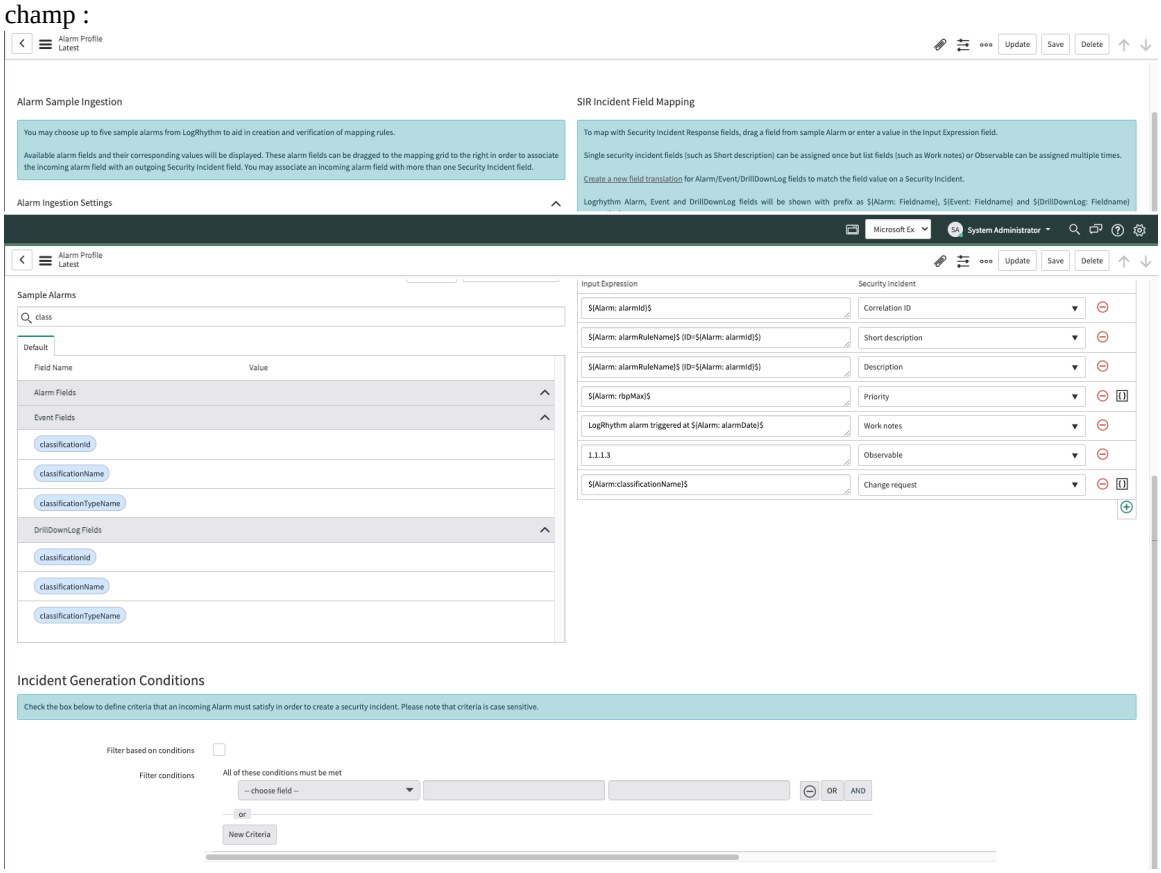
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

aide à suivre le mappage, car dans certains cas, un champ d'alarme peut être mappé à plusieurs champs d'un incident de sécurité. Par exemple, les champs Observables et Note de travail peuvent avoir plusieurs valeurs.

4. Pour effacer les données d'échantillon d'alarme, cliquez sur **Effacer les données d'échantillon d'alarme**.

5. Pour modifier la configuration par défaut de l'incident de sécurité, procédez comme suit pour ajouter un champ :



   a. En bas à droite du formulaire, cliquez sur l'icône plus.
   Un nouveau champ s'affiche.

   b. Dans la colonne Incident de sécurité, sélectionnez un champ disponible dans la liste de choix.

   Dans la liste de choix développée, certains champs sont ombrés. Par exemple, la catégorie a un fond gris, ce qui indique qu'elle a été mappée dans l'incident de sécurité. Semblable au code couleur pour LogRhythm les champs d'alarme, ce code couleur pour les champs d'incident de sécurité garantit que les valeurs des champs d'alarme ne sont pas mappées par inadvertance sur le même champ d'incident de sécurité.

   Dans l'illustration ci-dessus, la règle d'alarme ${Alarm :classificationName}$ est déjà mappée au champ Catégorie de l'incident de sécurité dans ce profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le champ Observable peut être mappé à plus d'un champ sur le même incident de sécurité afin que plusieurs observables puissent être affichés. De même, les champs Élément de configuration et Notes de travail peuvent être mappés pour afficher plusieurs valeurs.

Du côté de l'ingestion d'échantillons d'alarme du formulaire, le bleu indique qu'un champ de règle d'alarme n'a pas été mappé. Le gris indique qu'il a été mappé. Dans la liste de choix du côté Mappage du champ d'incident SIR du formulaire, le blanc indique qu'un champ n'a pas été mappé. Le gris indique qu'un champ a été mappé. Utilisez ce code couleur pour vous aider à suivre votre mappage de champs.

Dans l'illustration ci-dessus, l'utilisateur affecté a été sélectionné dans la liste de choix en tant que nouveau champ sur l'incident de sécurité.

c. Dans la section Ingestion d'échantillons d'alarme sur le côté gauche du formulaire, cliquez avec le bouton gauche pour sélectionner l'ID d'alarme souhaité dans le champ Expression d'entrée.

Dans l'illustration ci-dessus, la connexion a été sélectionnée.

d. Faites-le glisser vers le champ effacé et relâchez-le.
Dans la colonne de gauche de la section Mappage du champ d'incident SIR, la nouvelle valeur du champ Utilisateur affecté s'affiche. Dans ce cas, la valeur de connexion de l'alarme LogRhythm est affichée dans le champ Utilisateur affecté de l'incident de sécurité.

6. Alternativement, pour entrer manuellement une valeur pour les champs de la colonne Expression d'entrée, placez votre curseur dans le champ expression d'entrée et entrez la valeur d'alarme souhaitée.

Par exemple, dans l'illustration ci-dessus, un autre champ a été ajouté (groupe d'affectation) au formulaire d'incident de sécurité, et l'affectation d'incident de sécurité a été saisie manuellement dans le champ.

7. Continuez à modifier le mappage préconfiguré au besoin.
Si vous devez convertir les valeurs des champs d'alarme LogRhythm en valeurs prises en charge par les champs de l'incident de sécurité, vous pouvez utiliser l'éditeur de script. Consultez Utiliser l'éditeur de script pour formater LogRhythm les valeurs.

Que faire ensuite
Une fois le mappage de champs terminé, l'étape suivante consiste à Filtrer les alarmes pour LogRhythm.

Filtrer les alarmes pour LogRhythm

La définition de critères de filtrage pour les alarmes après avoir mappé les champs vous aide à déterminer quelles alarmes doivent être ingérées dans l'application SIR. Le filtrage des alarmes vous aide à réduire considérablement le nombre d'alarmes que vous ingérez lorsque le profil d'alarme est activé.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Utilisez les conditions de filtrage en bas du formulaire de mappage pour filtrer des alarmes spécifiques ou limiter l'ingestion aux seules alarmes qui répondent à certains critères au niveau du champ. Le filtrage réduit considérablement le nombre d'alarmes que vous ingérez une fois le profil d'alarme activé. Utilisez le filtrage pour ingérer une quantité gérable

Traduction automatique

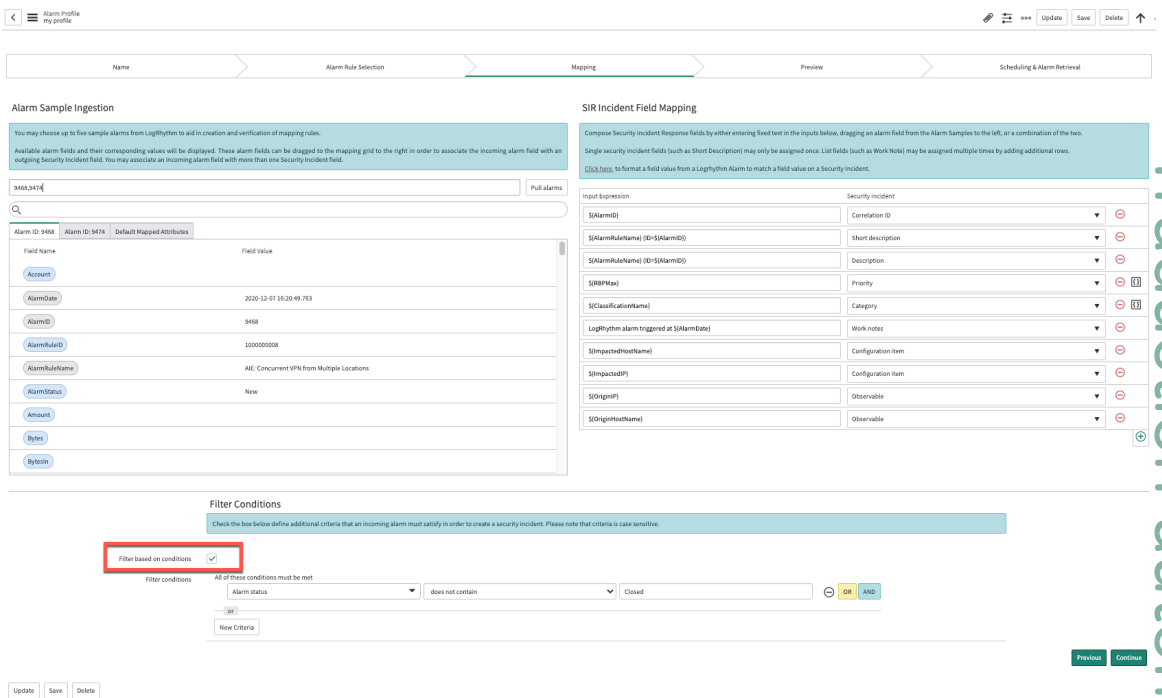
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d’alarmes que votre personnel du centre des opérations de sécurité (SOC) peut prendre en charge.

Remarque : L’exemple suivant montre un paramètre de filtre par défaut dans lequel l’état de l’alarme ne contient pas fermé est le paramètre par défaut. Ce filtre ne déclenche que les alarmes actives, et ce paramètre réduit le nombre d’alarmes extraites. Les étapes suivantes illustrent comment ajouter un autre filtre utile qui inclut uniquement les alarmes avec les valeurs de gravité ou de priorité les plus élevées.

Procédure

1. Pour modifier les critères de filtrage, cochez la case **Filtre basé sur les conditions** .

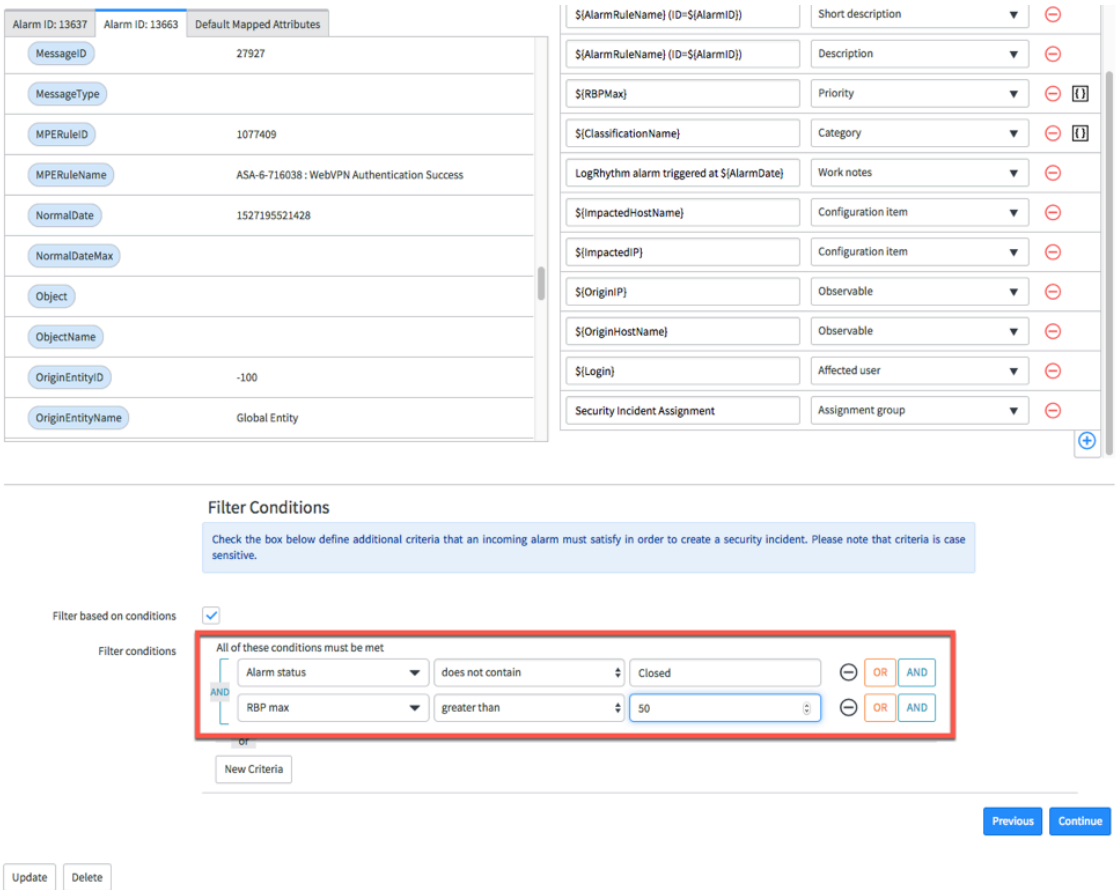


2. À droite du champ **Conditions de filtre** , cliquez sur **OU** ou **ET**.
3. Dans la nouvelle ligne qui s’affiche, sélectionnez les conditions de filtrage dans les listes de choix.

   L’image suivante montre un filtre supplémentaire ajouté aux critères dans lesquels la priorité basée sur le risque (RBP max) est supérieure à 50. Avec ce paramètre de filtre, seules LogRhythm les alarmes dont la valeur de priorité basée sur le risque est supérieure à 50 sont extraites.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Une fois que vous avez vérifié que tous les champs d'alarme critiques LogRhythm sont mappés à l'incident de sécurité et que vous avez défini des critères de filtrage pour limiter l'ingestion ServiceNow AI Platform d'alarmes, choisissez-en un pour poursuivre la configuration.

Option	Description
Continuer ou Prévisualiser	Le formulaire Aperçu de l'incident de sécurité avec votre configuration de mappage s'affiche. **L'aperçu** est sélectionné dans la barre de progression. L'étape suivante consiste à afficher l'incident de sécurité avec vos alarmes mappées.
Mettre à jour	Enregistrez vos données et retournez à la liste **des profils d'alarme** .
Précédent	L'enregistrement du profil d'alarme s'affiche.
Supprimer	Supprimez ce profil d'alarme et la liste **des profils d'alarme** s'affiche.

Que faire ensuite

L'étape suivante consiste à prévisualiser vos champs mappés sur l'incident de sécurité. Consultez Aperçu de l'incident de sécurité avec des valeurs d'alarme mappées LogRhythm.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçu de l'incident de sécurité avec des valeurs d'alarme mappées LogRhythm

Une fois que vous avez terminé l'étape de mappage, prévisualisez les valeurs que vous avez mappées aux champs de l'incident de sécurité. Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs d'alarme critiques LogRhythm que vous souhaitez afficher sur l'incident de sécurité.

Rôle requis : sn_si.admin.

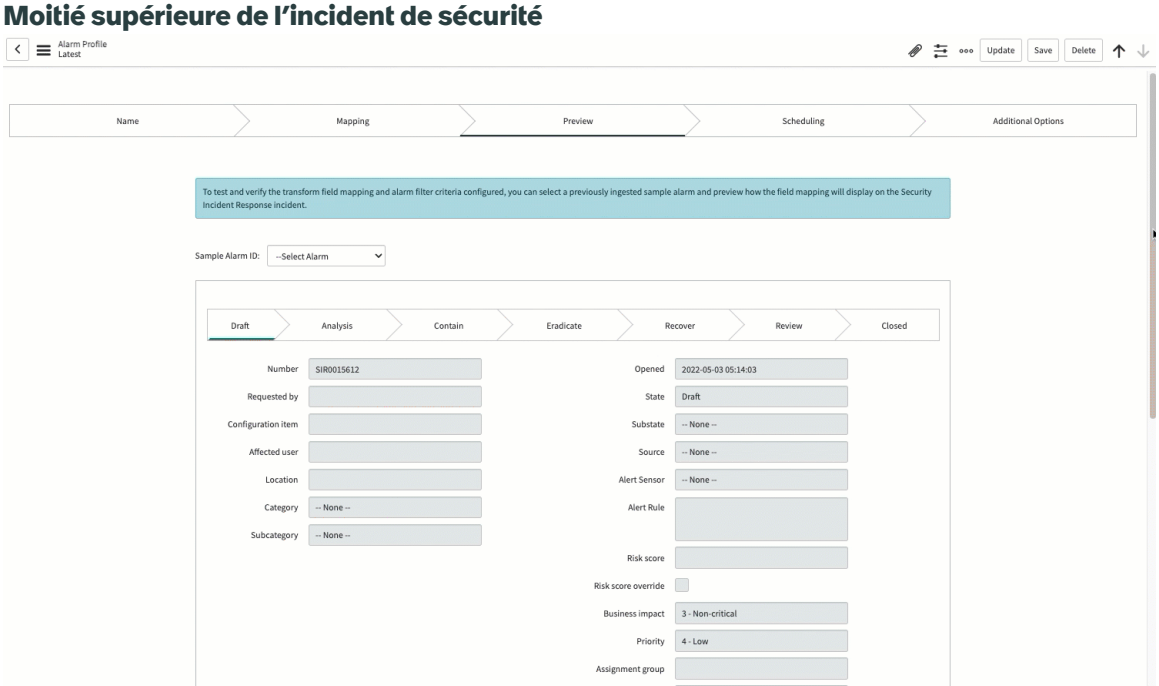
Incident de sécurité

Si l'aperçu de l'incident de sécurité ne s'affiche pas, cliquez sur **Aperçu** dans la barre de progression.

Les deux figures suivantes illustrent un exemple d'aperçu de l'ensemble de l'incident ServiceNow AI Platform de sécurité. Cet exemple d'aperçu de l'incident de sécurité est renseigné avec les champs d'alarmes mappés à partir de l'échantillon LogRhythm d'alarme 13663.

Dans la figure suivante, les champs Élément de configuration, Utilisateur affecté, Priorité, Groupe d'affectation et Description brève de l'incident de sécurité sont renseignés.

Moitié supérieure de l'incident de sécurité



Le champ Description est renseigné dans la moitié inférieure du formulaire d'incident de sécurité. Dans la section Éléments connexes, les champs Élément de configuration, Observable et Note de travail sont renseignés avec des valeurs. Si plusieurs valeurs sont mappées pour ces champs, chaque valeur est affichée sur l'incident de sécurité, car chacun de ces champs peut accepter plusieurs valeurs.

Conditions d'erreur dans l'aperçu

Les messages d'avertissement suivants peuvent s'afficher lors de l'aperçu de l'incident de sécurité. Si un échantillon d'alarme ne répond pas aux critères de filtrage, l'incident de sécurité n'est pas renseigné dans son intégralité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur d'entrée introuvable

Si l'ID d'alarme est inclus dans les conditions de filtrage, un message d'avertissement peut toujours s'afficher si des valeurs d'entrée spécifiques ne sont pas trouvées pour certains champs mappés. Pour les besoins de l'exemple suivant, dans l'aperçu de l'enregistrement, supposons qu'il n'y a aucune valeur dans le champ Affecté à , bien qu'il ait été mappé.

Pour ce type de message, dans l'enregistrement de mappage, vérifiez que la valeur d'entrée est correcte. Dans ce cas, la personne dans le champ Affecté à de l'incident de sécurité est incorrecte dans l'instance ServiceNow AI Platform . Lorsque cette alarme est ingérée et qu'elle crée un incident de sécurité avec cette condition, les champs avec cette valeur d'entrée (Abel Tuter) sont laissés vides dans l'incident de sécurité.

Les autres messages en bleu sont informatifs et indiquent que ces champs n'ont aucune valeur à afficher dans l'aperçu. Cet aperçu permet à l'administrateur d'incident de sécurité qui configure le profil d'alarme de vérifier que ces champs ne doivent avoir aucune valeur à l'étape de création initiale, car dans certains cas, les champs d'incident de sécurité peuvent être renseignés automatiquement plus tard. D'autres erreurs de mappage sont également affichées.

Une fois que vous êtes satisfait du mappage et de l'aperçu de l'incident de sécurité, choisissez-en un pour poursuivre la configuration.

Option	Description
Cliquez sur **Continuer** ou **Planification** dans la barre de progression.	Passez au formulaire **Planification et récupération des alarmes** . **Planification et récupération des alarmes** est sélectionné dans la barre de progression. L'étape suivante consiste à planifier la récupération de l'alarme.
Cliquez sur **Précédent**.	Revenez au profil d'alarme et continuez le mappage.
Entrez un autre ID d'alarme dans la liste de choix ID **d'échantillon d'alarme** en haut du formulaire d'aperçu.	La liste **de choix d'ID d'échantillon d'alarme** s'affiche pour chaque ID d'alarme que vous avez saisi. Vous pouvez sélectionner jusqu'à cinq alarmes. Cette option vous permet de prévisualiser un autre LogRhythm ID d'alarme sur un incident de sécurité.

Une fois que vous avez prévisualisé l'incident de sécurité et que vous êtes satisfait des résultats, l'étape suivante consiste à Planifier et récupérer LogRhythm des alarmes.

Planifier et récupérer LogRhythm des alarmes

Après avoir prévisualisé l'incident de sécurité avec les LogRhythm alarmes que vous avez sélectionnées et mappées, vous êtes prêt à planifier la récupération de l'alarme. Une fois cette étape terminée, le profil d'alarme est prêt à être activé.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
La planification vous permet de modifier la planification et les types d'alarmes sélectionnées pour la récupération. Vous filtrez les alarmes que vous ingérez en fonction d'une plage

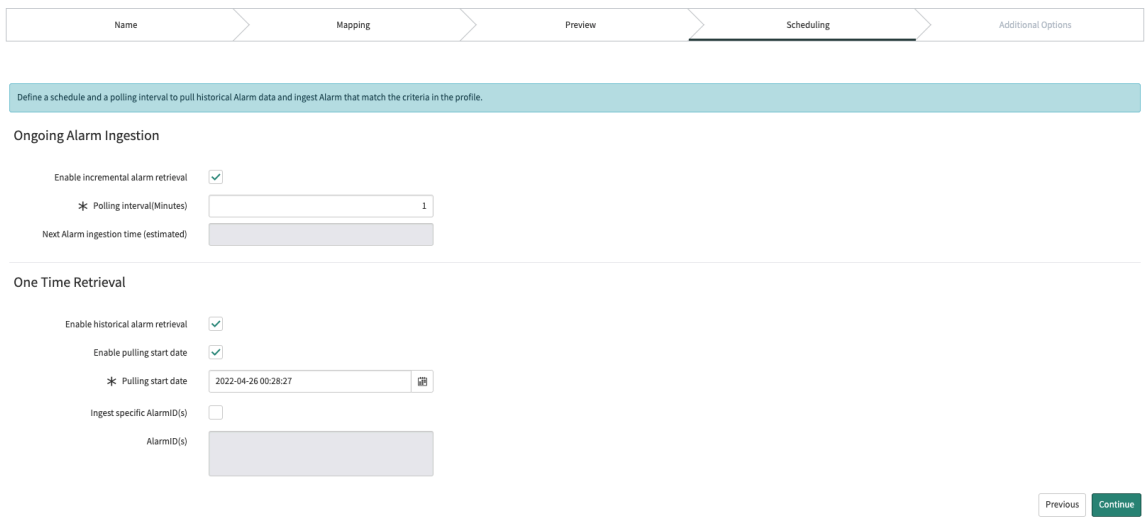
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de dates ou d'ID d'alarme spécifiques. Cette étape vous permet de déterminer si vous souhaitez ingérer des alarmes historiques et à quelle fréquence vous interrogez les alarmes futures qui correspondent à la configuration du profil d'alarme.

Procédure

1. Cliquez sur l'étape **Planification** dans la barre de progression.



2. Choisissez parmi les options suivantes pour configurer votre récupération d'alarme.

Option	Description
Activer la récupération d'alarme de pas	Sélectionné par défaut. Sélectionnez cette option pour récupérer les alarmes incrémentielles.
Intervalle d'interrogation (en minutes)	L'instance ServiceNow AI Platform extrait de la console client de nouvelles LogRhythm alarmes toutes les minutes. Si des alarmes mappées sont trouvées et que les critères de filtrage correspondent, des incidents de sécurité sont créés. Ce paramètre peut être modifié, cependant, le paramètre par défaut équilibre l'ingestion d'alarme par rapport à la charge du serveur et récupère les données les plus récentes.
Temps d'ingestion de la prochaine alerte (estimation)	Affiche la date de la prochaine ingestion planifiée pour le profil d'alarme actuel. Il ne s'agit que d'une estimation.
Activer la récupération d'alarme historique	La valeur par défaut est effacée. Aucune donnée historique n'est extraite. Si cette option est sélectionnée, les champs suivants s'affichent. Choisissez-en un pour configurer la récupération par date ou par ID d'alarme. **Activer la date de début de déclenchement**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	La valeur par défaut est effacée. Sélectionnez cette option pour activer la date d'extraction. **Date de début de déclenchement** La valeur par défaut est effacée. Sélectionnez cette option pour définir la date de début de l'extraction. Cliquez sur l'icône Calendrier pour entrer une date et une heure. Les alarmes sont déclenchées à partir de la date et de l'heure que vous saisissez jusqu'à la date actuelle. **Intégrer une alarme spécifique ID d'alarme** La valeur par défaut est effacée. Sélectionnez cette option pour ingérer des ID d'alarme spécifiques. **AlarmID(s)** Saisissez des ID d'alarme spécifiques. Vous extrayez les alarmes spécifiées et vous pouvez saisir plusieurs ID d'alarme séparés par des virgules. **Remarque :** Une fois qu'une extraction historique et ponctuelle des alarmes est terminée, cette case est décochée. Vous devrez cocher à nouveau cette case avant d'exécuter une autre extraction ponctuelle d'alarmes historiques.

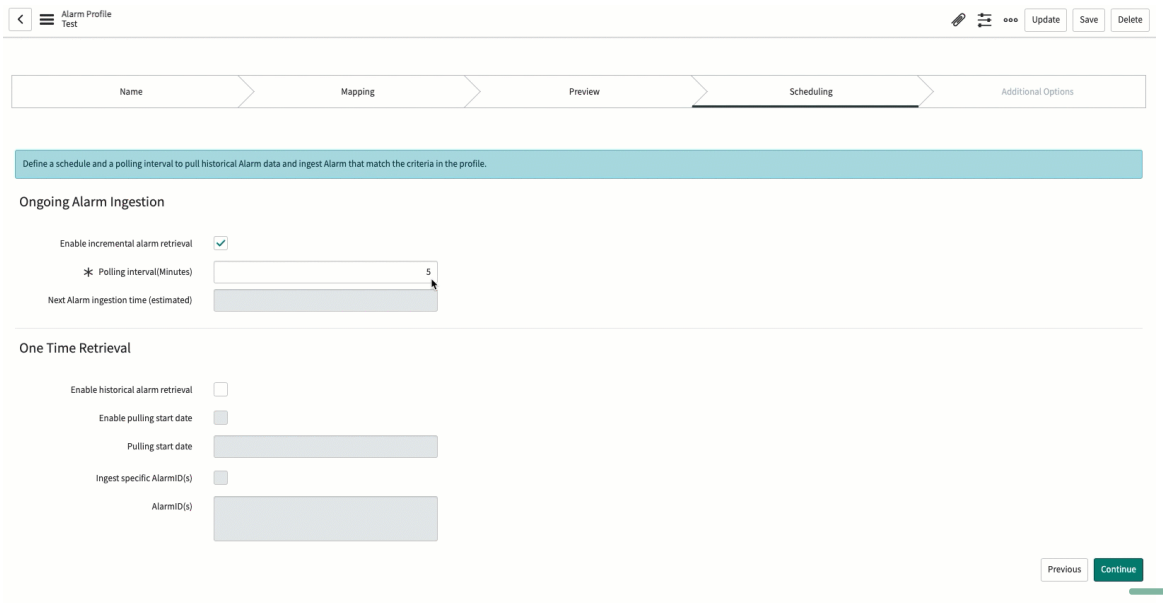
3. Pour modifier la récupération d'alarme historique, procédez comme suit pour entrer une date de récupération d'alarme ou un ID d'alarme spécifique.

   a. Sélectionnez **Activer la date de début de pull**, puis sélectionnez **Date de début de pull**.

   b. Dans le champ **Date de début de tirage** , cliquez sur le calendrier qui s'affiche, sélectionnez la date suivie de la coche verte pour enregistrer votre entrée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La date s'affiche.

c. Vous pouvez également sélectionner l'option **Ingérer un ou des ID d'alarme spécifiques** et, dans le champ **AlarmID(s),** saisir les ID d'alarme spécifiques pour les données historiques afin de récupérer des ID d'alarme spécifiques.

Vous pouvez saisir jusqu'à cinq alarmes séparées par des virgules.

d. Cliquez sur **Mettre à jour**.

4. Choisissez l'une des options suivantes pour poursuivre la modification ou terminer la configuration.

Option	Description
Mettre à jour	Enregistrez vos données et restez sur le formulaire.
Options supplémentaires (dans la barre de progression)	Pour accéder à l'étape Options supplémentaires.
Précédent	Revenir à l'étape de prévisualisation.
Supprimer	Supprimez ce profil d'alarme et la liste des profils d'alarme s'affiche.

Que faire ensuite

Une fois que vous avez configuré les détails de l'ingestion d'alarme en cours et de la récupération ponctuelle, l'étape suivante consiste à Options supplémentaires pour LogRhythm les alarmes.

Options supplémentaires pour LogRhythm les alarmes

L'intégration LogRhythm Enterprise vous offre la possibilité de mettre à jour ou de fermer automatiquement les LogRhythm alarmes en fonction des incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Lorsque vous activez l'option Mises à jour initiales de l'alarme, les alarmes sont automatiquement mises à jour dans les commentaires LogRhythm avec les mises à jour initiales de l'alarme. De même, lorsque vous activez l'option Mises à jour de fermeture d'alarme, les alarmes sont automatiquement fermées dans LogRhythm avec le code de fermeture SIR et les commentaires de fermeture.

L'ID LogRhythm d'alarme est connecté à l'ID d'incident ServiceNow AI Platform de sécurité tout au long du cycle de vie de l'incident. Cette corrélation permet la fermeture simultanée et automatisée d'un incident de sécurité/d'une alarme. Lorsque l'enregistrement d'incident Réponse aux incidents de sécurité de sécurité (SIR) est fermé, un commentaire est publié dans l'alarme sur la LogRhythm console Web. Ce commentaire indique que l'alarme a été fermée en fonction de la fermeture de l'incident ServiceNow AI Platform de sécurité. Le numéro de l'incident et une URL qui renvoie à l'incident de sécurité à des fins de référence sont également inclus dans la section des commentaires de l'alarme LogRhythm .

Procédure

1. Cliquez sur l'étape **Options supplémentaires** dans la barre de progression.
2. Pour utiliser la mise à jour automatisée de l'alarme pour la création d'incidents SIR, choisissez parmi les options suivantes pour configurer votre récupération d'alarme.

Option	Description
Mettre à jour les alarmes LogRhythm lors de la création de l'incident SIR	La valeur par défaut est effacée. Sélectionnez cette option pour mettre à jour automatiquement les LogRhythm alarmes lors de la création de l'incident SIR.
Commentaires initiaux envoyés à l'alarme LogRhythm	Indique les commentaires initiaux publiés pour l'alarme LogRhythm . Modifiez le texte par défaut affiché dans la section Commentaires en ajoutant ou en modifiant les variables de substitution à l'aide du format ${nom de champ}$ pour n'importe quel champ du formulaire d'incident SIR. Par exemple, L'incident de sécurité ServiceNow connexe, ${Number}$ a été créé et affecté à ${Assignment group}$. Des détails supplémentaires sont disponibles sur l'incident de sécurité situé ici : ${URL}$.

3. Pour utiliser la mise à jour automatisée de l'alarme pour la fermeture de l'incident SIR, choisissez parmi les options suivantes pour configurer votre récupération d'alarme.

Option	Description
Fermer les alarmes LogRhythm lors de la fermeture de l'incident SIR	La valeur par défaut est effacée. Sélectionnez cette option pour fermer automatiquement les LogRhythm alarmes lorsque l'incident SIR est fermé.
Commentaires de fermeture envoyés à l'alarme LogRhythm	Indique les commentaires de fermeture publiés pour l'alarme LogRhythm .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Modifiez le texte par défaut affiché dans la section Commentaires en ajoutant ou en modifiant les variables de substitution à l'aide du format ${nom de champ}$ pour n'importe quel champ du formulaire d'incident SIR. Par exemple, l'incident de sécurité ServiceNow connexe, ${Number}$, a été fermé par SOC Analyst-${Closed by}$ avec les notes de fermeture suivantes : ${Close notes}$. Des détails supplémentaires sont disponibles sur l'incident de sécurité situé ici : ${URL}$.

4. Cliquez sur **Terminer** pour enregistrer le profil d'alarme.

Trouble?
Si vous ne voyez pas de notes indiquant que l'alarme s'est fermée avec succès lors de l'incident de sécurité, consultez les notes de travail pour plus d'informations sur la procédure à suivre pour résoudre le problème. Vérifiez également la connexion de votre serveur. Si vous confirmez que l'incident de ServiceNow AI Platform sécurité a été fermé et que le serveur n'a pas expiré, vous devrez peut-être fermer manuellement l'alarme sur la LogRhythm console Web.

Configurations supplémentaires pour l'intégration LogRhythm

Utilisez les paramètres d'intégration LogRhythm pour modifier le système prédéfini et les propriétés de dépannage selon vos besoins.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Intégration de LogRhythm** > **Paramètres d'Intégration de LogRhythm**.
2. Configurez les propriétés système selon vos besoins.
3. Renseignez les champs du formulaire.

LogRhythm Propriétés système d'intégration

Champ	Description
Cela appliquera le filtre avant que les données ne soient enregistrées dans les tables ServiceNow.	Option permettant de déterminer si vous souhaitez appliquer le filtre avant que les données ne soient stockées dans les tables ServiceNow. Par défaut, la valeur est définie sur Oui.
Un incident de sécurité maximal peut être créé en une journée	Option permettant de définir le nombre maximal d'incidents de sécurité qui peuvent être créés en une journée. Par défaut, la valeur est définie sur 2 000.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
LogRhythm L'ingestion périodique peut être de 1000+ alarmes, d'où l'utilisation de la pagination pour ingérer les alarmes. Limite par page autorisée pour extraire le nombre d'alarmes par page.	Option permettant de définir le nombre maximal d'alarmes à récupérer dans une seule page. Par défaut, la valeur est 100.
Supprimez les enregistrements de table « Source à tâche » plus anciens que le nombre spécifié de jours.	Option permettant de supprimer les enregistrements de la source à la table de tâches lorsque le nombre spécifié de jours a été rompu. Par défaut, la valeur est définie sur 30.

4. Configurez les propriétés de dépannage selon vos besoins.
5. Renseignez les champs du formulaire.

Propriétés de dépannage de LogRhythm Integration

Champ	Description
Déboguer l'ingestion planifiée : active les journaux système de niveau débogage pour l'ingestion effectuée par la tâche planifiée. Cela consignera la totalité des messages/exceptions générés par l'ingestion planifiée lors de l'extraction des alarmes/ Drilldownlogs/Events de LogRhythm.	Option permettant d'activer les journaux système de niveau de débogage pour l'ingestion effectuée par la tâche planifiée. Par défaut, la valeur est définie sur Non.
Déboguer la carte de transformation : active les journaux système de niveau débogage pour la carte de transformation. Cela consignera tous les messages générés par les cartes de transformation lors de la création d'un incident de sécurité à partir de l'importation d'alarme. Cela a également activé l'action d'interface utilisateur sur la table d'importation d'alarme pour réexécuter la carte de transformation.	Option permettant d'activer les journaux système de niveau de débogage pour la carte de transformation. Par défaut, la valeur est définie sur Non.
Déboguer l'ingestion d'échantillons dans le profil d'alarme : active les journaux système de niveau débogage pour l'ingestion d'échantillons. Cela consignera tous les messages générés lorsque des échantillons sont ingérés.	Option permettant d'activer les journaux système de niveau de débogage pour l'ingestion d'échantillons. Par défaut, la valeur est définie sur Non.
Aperçu du débogage dans le profil d'alarme : active les journaux système de niveau débogage pour l'aperçu du profil d'alarme. Cela consignera tous les messages générés pendant que l'aperçu est affiché pour l'alarme d'échantillon.	Option permettant d'activer les journaux système de niveau de débogage pour l'aperçu du profil d'alarme. Par défaut, la valeur est définie sur Non.
Déboguer les appels REST sortants : l'activation de cette propriété permettra la journalisation du niveau de débogage dans la table Journaux système pour tous les appels REST (demande et réponse) qui se déroulent avec ou sans Serveur MID à partir de LogRhythm.	Option permettant d'activer la journalisation du niveau de débogage dans la table Journaux système pour tous les appels REST qui se déroulent avec ou sans Serveur MID à partir de LogRhythm. Par défaut, la valeur est définie sur Non.

6. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser l'éditeur de script pour formater LogRhythm les valeurs

Outre les champs directement mappés à partir des valeurs d'alarme extraites et les valeurs d'alarme que vous saisissez manuellement, vous pouvez utiliser l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage qui est facultative.

Avant de commencer

Rôle requis : sn_si.admin

L'éditeur de script modifie les valeurs d'une LogRhythm alarme afin que les valeurs mappées aux champs Priorité et Catégorie de l'incident de sécurité soient prises en charge.

Pourquoi et quand exécuter cette tâche

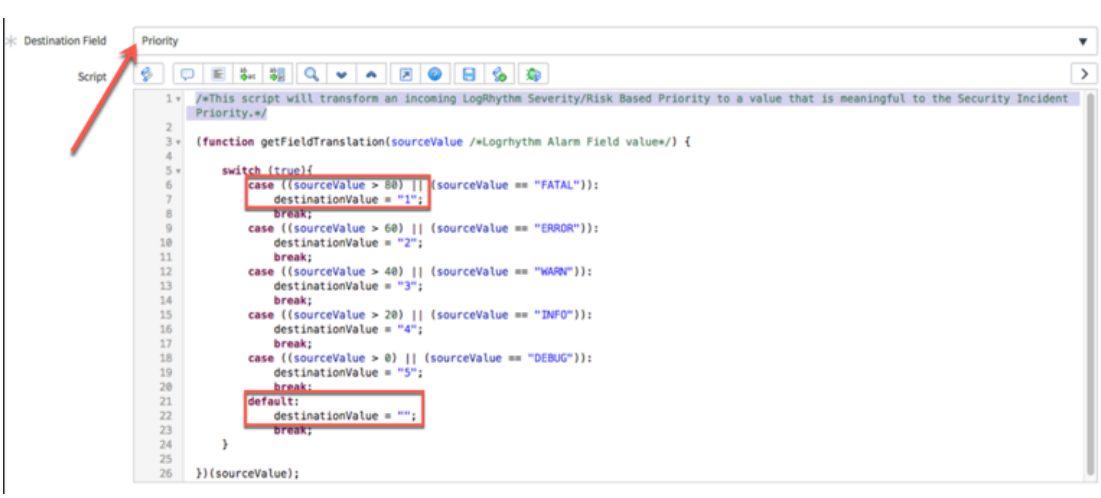
Dans certains cas, si LogRhythm les valeurs d'alarme sont mappées aux champs Priorité et Catégorie de l'incident de sécurité, vous voudrez peut-être modifier les valeurs mappées. Si vous souhaitez convertir la valeur d'une LogRhythm alarme en une valeur prise en charge par les champs Priorité ou Catégorie de l'incident de sécurité, utilisez l'éditeur de script.

Procédure

1. Une fois le formulaire de mappage affiché, dans la section Mappage du champ d'incident SIR, cliquez sur l'icône de crochet [{}] pour ouvrir l'éditeur de script.

Les valeurs par défaut sont incluses pour les champs Priorité et Catégorie de l'incident de sécurité. Vous pouvez modifier ces valeurs.

Pour cet exemple, dans l'éditeur ouvert, vérifiez que la **priorité** est affichée dans la liste de choix **Champ de destination** , comme illustré dans la figure suivante. Notez que ce champ est la *priorité* de l'incident de sécurité, et non la *priorité* basée sur les LogRhythm risques.



Dans certains cas, un include de script peut être approprié pour le champ Priorité . Pour une LogRhythm alarme, par exemple, un score de priorité basé sur le risque se voit attribuer une valeur comprise entre 0 et 100. Toutefois, dans le , le champ Priorité d'un ServiceNow AI Platform incident de sécurité prend en charge les valeurs comprises entre 1 et 5. Comme illustré dans la figure précédente, un include de script convertit les valeurs du LogRhythm champ d'alarme en valeurs appropriées prises en charge par le champ sur l'incident de sécurité dans le ServiceNow AI Platform.

Dans cet exemple pour le champ Priorité , si la valeur de l'alarme LogRhythm est supérieure ou égale à 80 , 1 s'affiche dans le champ Incident de sécurité (Priorité). Cette valeur

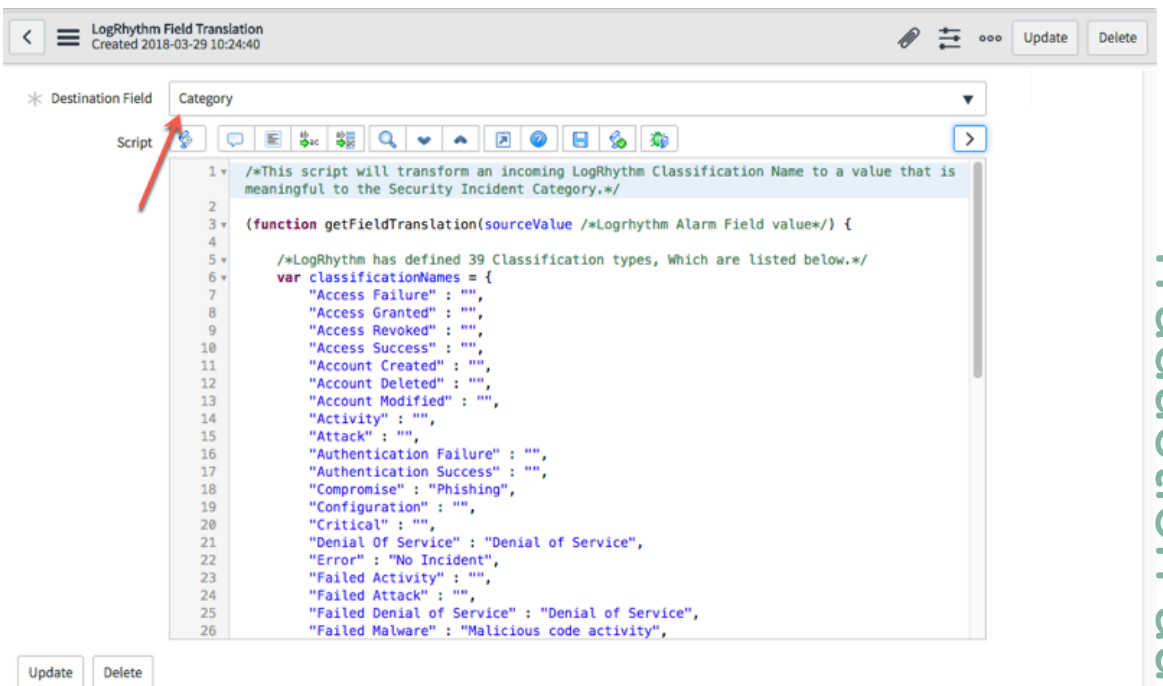
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

se traduit par une priorité critique dans l'incident de sécurité. Si aucune valeur n'est spécifiée pour l'alarme, le champ de l'incident de sécurité est défini sur Null.

2. Entrez les modifications, puis cliquez sur **Mettre à jour** pour enregistrer les modifications.
   La LogRhythm table Traductions de champ s'affiche.
3. Fermez la table pour revenir au formulaire de mappage.

   La figure suivante montre l'éditeur de script avec la catégorie sélectionnée dans la liste de choix Champ de destination.

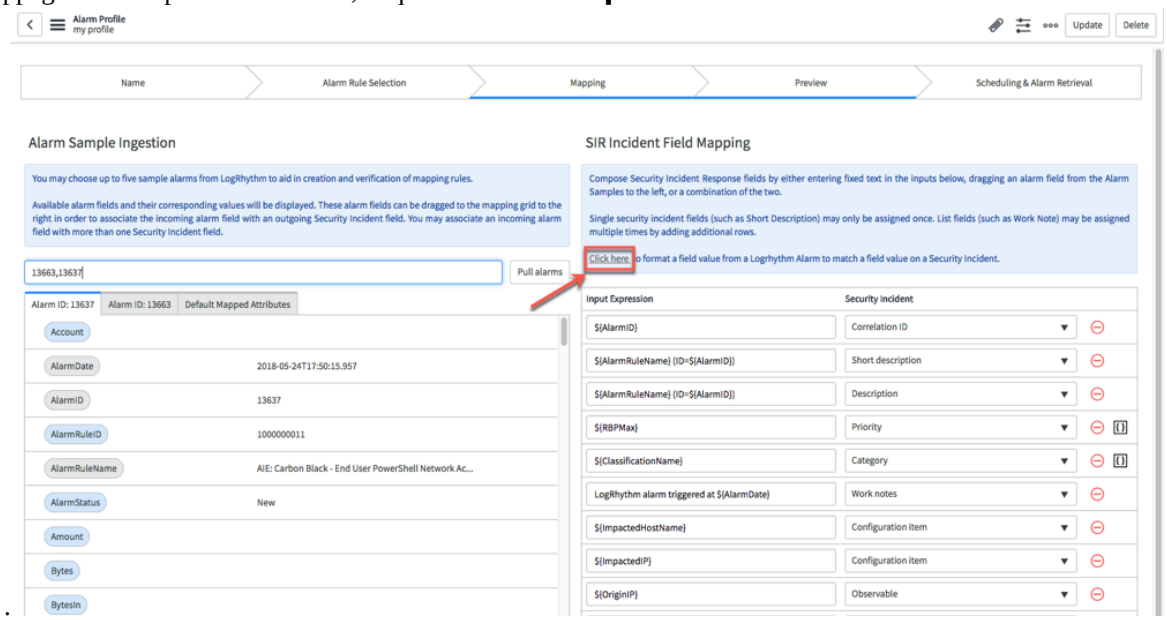


4. Si vous souhaitez ajouter un nouveau champ à la liste Traductions de champ, procédez comme suit pour ajouter un nouvel enregistrement.

Traduction automatique

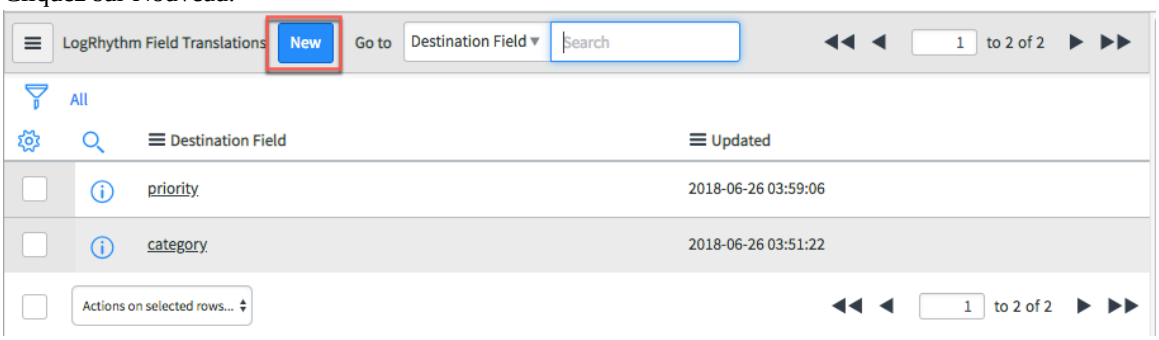
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Une fois le formulaire de mappage affiché, dans la section Mappage du champ d'incidents SIR, cliquez sur le lien **Cliquez ici** .



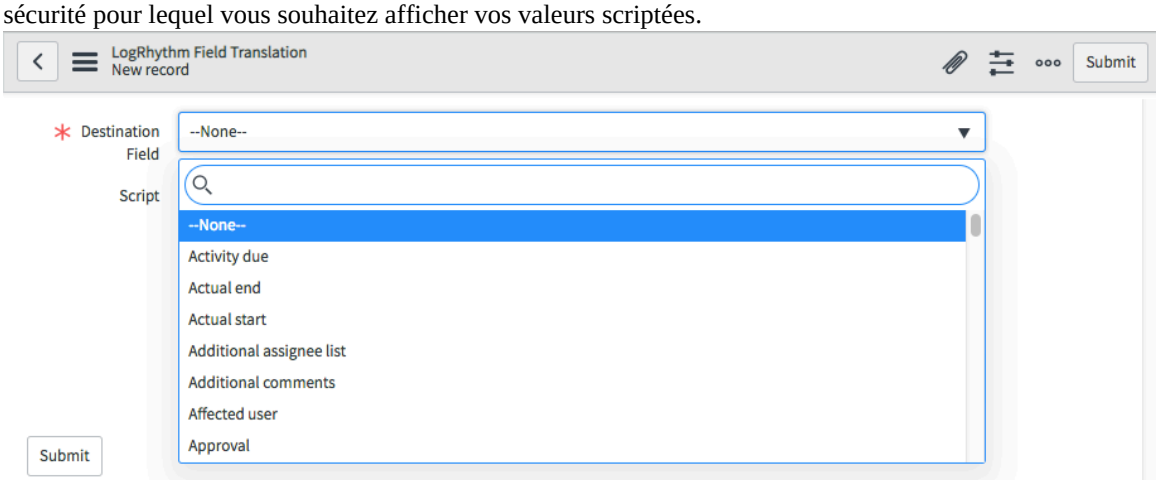
La LogRhythm liste Traduction du champ avec les champs de priorité et de destination de catégorie s'affiche.

b. Cliquez sur Nouveau.



Un nouvel enregistrement s'affiche.

c. Dans la liste de choix Champ de destination, sélectionnez un champ de destination sur l'incident de sécurité pour lequel vous souhaitez afficher vos valeurs scriptées.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Cliquez sur **Envoyer**.
L'éditeur de script s'affiche.

e. Entrez toutes les modifications dans l'éditeur, puis cliquez sur **Soumettre** pour enregistrer vos modifications.
La LogRhythm table Traductions de champ avec votre nouvel enregistrement s'affiche.

5. Fermez la table pour revenir au formulaire de mappage.

Copier un profil d'alarme pour LogRhythm

Copiez un profil existant et ses paramètres associés au lieu de créer un nouveau profil d'alarme. Si vous créez plusieurs profils d'alarme pour différents types d'alarmes et que vous souhaitez réutiliser les paramètres d'un profil existant, vous pouvez copier les profils d'alarme pour gagner du temps. Ce processus est facultatif.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Si vous copiez un profil, le nom du profil est initialement modifié pour éviter les profils en double. En outre, le profil copié est défini sur inactif afin qu'il ne soit pas activé accidentellement avant de terminer la configuration.

Procédure

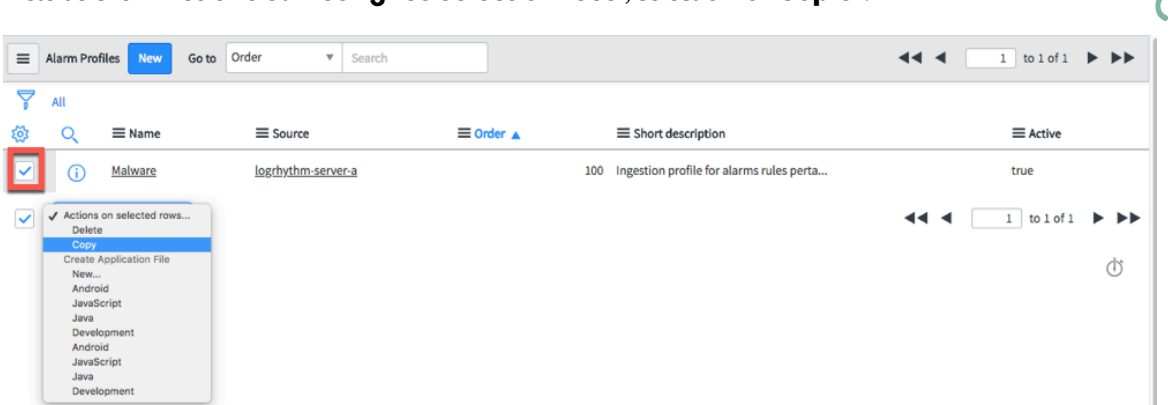
1. Accédez à la **Tous** > **Intégration de LogRhythm** > **Profils d'alarme LogRhythm**.

Dans la liste qui s'affiche, notez que la colonne Actif indique si le profil est actif (vrai).



2. Dans le champ situé à gauche de la colonne **Nom** , sélectionnez le nom de l'enregistrement.

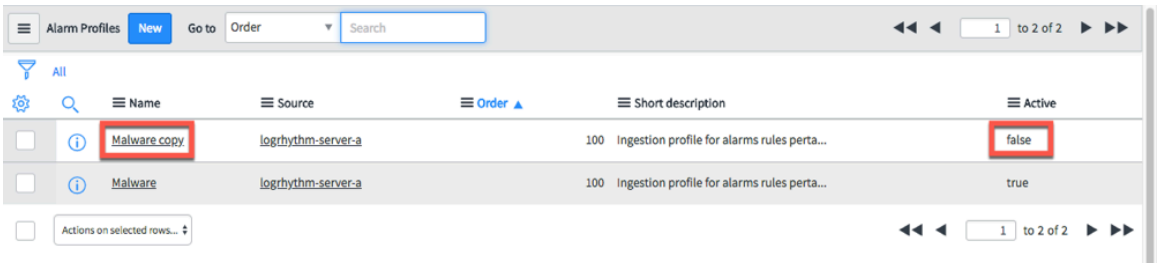
3. Dans la liste de choix **Actions sur les lignes sélectionnées** , sélectionnez **Copier**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans la liste **Profils d'alarme** , la copie et le profil d'origine sont affichés. Bien que l'enregistrement d'origine soit actif, la copie est inactive à ce stade (faux). Une fois que vous l'avez configuré, vous activez ce profil copié.



Vous pouvez modifier les valeurs du profil copié et le renommer pour que les règles d'alarme que vous extrayez s'appliquent au nouveau profil. Vous êtes invité à activer le nouveau profil une fois les étapes de configuration terminées.

Désactiver la fermeture automatique de l'alarme pour LogRhythm

Désactivez l'option de fermeture d'alarme automatisée si vous ne souhaitez plus afficher les informations de fermeture de l'incident de sécurité sur la LogRhythm console Web. Une fois désactivé, le ServiceNow AI Platform ne ferme plus les alarmes dans la LogRhythm console Web. Ce processus est facultatif.

Avant de commencer

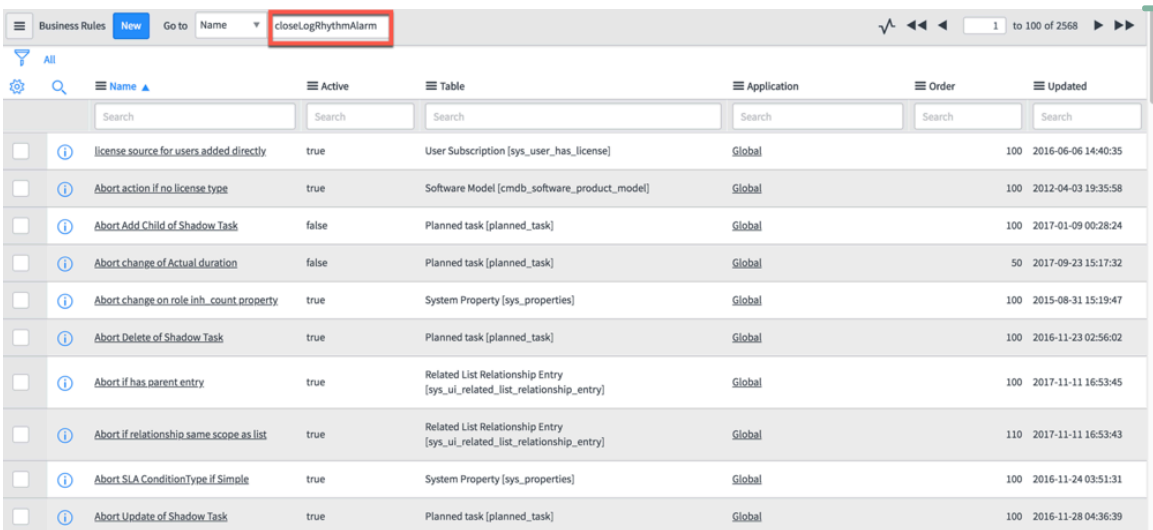
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Une fois désactivée, les notes d'état et autres informations de fermeture de l'incident de sécurité ne sont plus affichées sur la LogRhythm console Web.

Procédure

1. Accédez à la **Tous** > **Définition du système** > **Règles métier** et sélectionnez le module **Règles métier** .
2. S'il n'est pas affiché dans la liste **Règles métier** , entrez **LogRhythm Fermer l'alarme Lors de la fermeture SI** dans le champ de recherche et appuyez sur **Entrée**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la colonne **Nom** , cliquez sur le lien **LogRhythm Fermer l'alarme lors de la fermeture SI** pour ouvrir l'enregistrement.
4. Dans l'enregistrement qui s'affiche, décochez la case **Actif** .
5. Cliquez sur **Mettre à jour**.
   L'option de fermeture automatique d'alarme est maintenant désactivée.

Afficher les LogRhythm événements d'exploration

Affichez les événements bruts ou de base associés à une LogRhythm alarme dans l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.admin

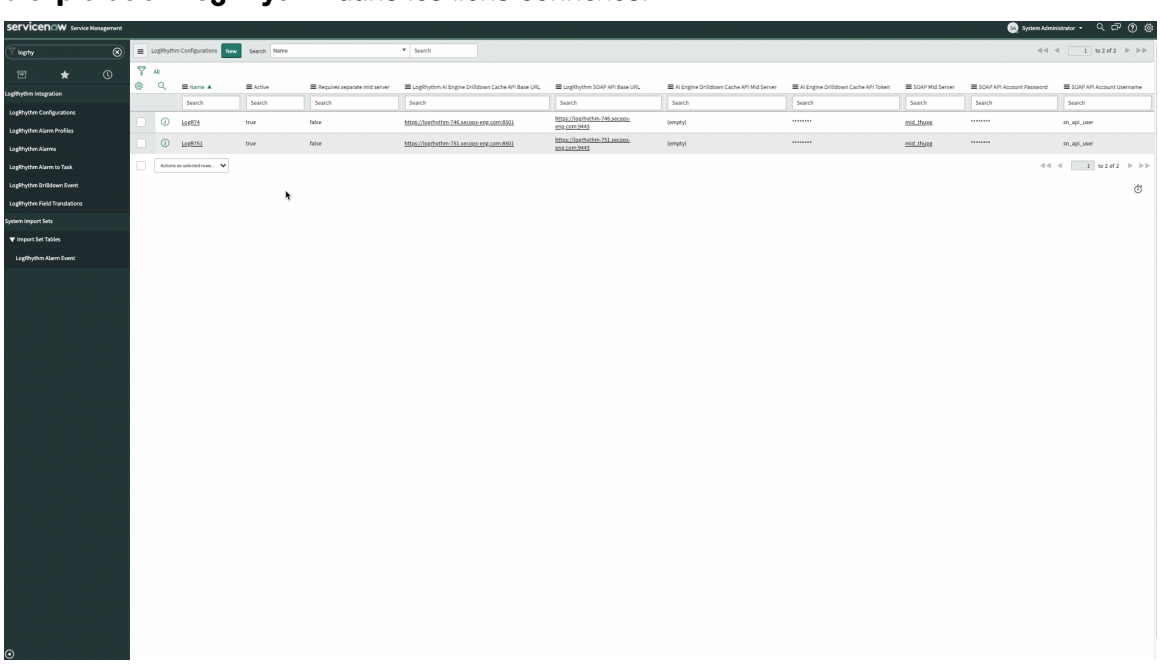
Pourquoi et quand exécuter cette tâche

En tant qu'analyste de sécurité, vous pouvez afficher les événements bruts ou de base associés à une LogRhythm alarme sans avoir à revenir à la LogRhythm console. Pour ce faire, accédez à une liste connexe contenant tous les événements d'exploration en détail de l'incident SIR .

Procédure

Accédez à la **Tous** > **Intégration de LogRhythm** > **Événements d'analyse LogRhythm**.

L'illustration suivante montre comment accéder au module **Événements LogRhythm Drilldown,** trier la liste des événements par **groupe par ID d'alarme** et cliquer sur l'incident de sécurité associé. Dans l'incident de sécurité, vous pouvez trouver l'onglet **Événements d'exploration LogRhythm** dans les liens connexes.



Dépannage de l'intégration LogRhythm

Résolvez les problèmes de connectivité et d'ingestion d'alarme.

Reportez-vous aux rubriques suivantes pour le dépannage :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifier la connectivité pour LogRhythm
- Exécution de script et journal système pour LogRhythm

Vérifier la connectivité pour LogRhythm

Vérifiez votre connexion à la LogRhythm console cliente en envoyant des demandes curl pour tester l'API LogRhythm REST. Le processus de vérification est facultatif.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Pour vérifier que la connexion à la LogRhythm console client fonctionne correctement après la LogRhythm configuration des API REST, envoyez deux demandes curl à partir de l'ordinateur hébergeant le serveur MID que vous avez configuré dans Installer le module d'extension et configurer LogRhythm.

L'API LogRhythm REST utilise WSSE pour l'authentification, ce qui nécessite des scripts externes pour fonctionner avec Curl et Postman.

L'API LogRhythm REST utilise un jeton pour l'authentification, afin que vous puissiez passer l'appel de validation réel utilisé par l'intégration. Le « 0 » à la fin de l'URL est un LogRhythm ID d'alarme. L'API LogRhythm REST avec une configuration par défaut nécessite le port 8501. Ce numéro de port doit être inclus dans l'URL que vous prévoyez d'utiliser pour le test.

Procédure

Mettez à jour l'URL **<URL REST LogRhythm>** et le jeton **<jeton d'API>** dans la demande curl suivante et envoyez-la pour valider l'API LogRhythm REST : `curl -k -i -v --trace-time -o /dev/null -H « Type-contenu : texte/json » -H « Autorisation : porteur <jeton d'API> » « https://<URL d'analyse du cache>/lr-drilldown-cache-api/drilldown/0 »`
Pour une connexion réussie à l'API LogRhythm REST, vous devez recevoir un HTTP 404, mais le corps de la réponse contient l'ID d'alarme : 0 introuvable.

Exécution du script et journal système

Si vous résolvez un problème d'ingestion d'alarme, vous pouvez remplacer l'intervalle d'interrogation par défaut de cinq minutes pour afficher les résultats immédiatement. Dans ce scénario, appelez manuellement l'exécution du script pour exécuter l'interrogation. Cette exécution est facultative.

Avant de commencer

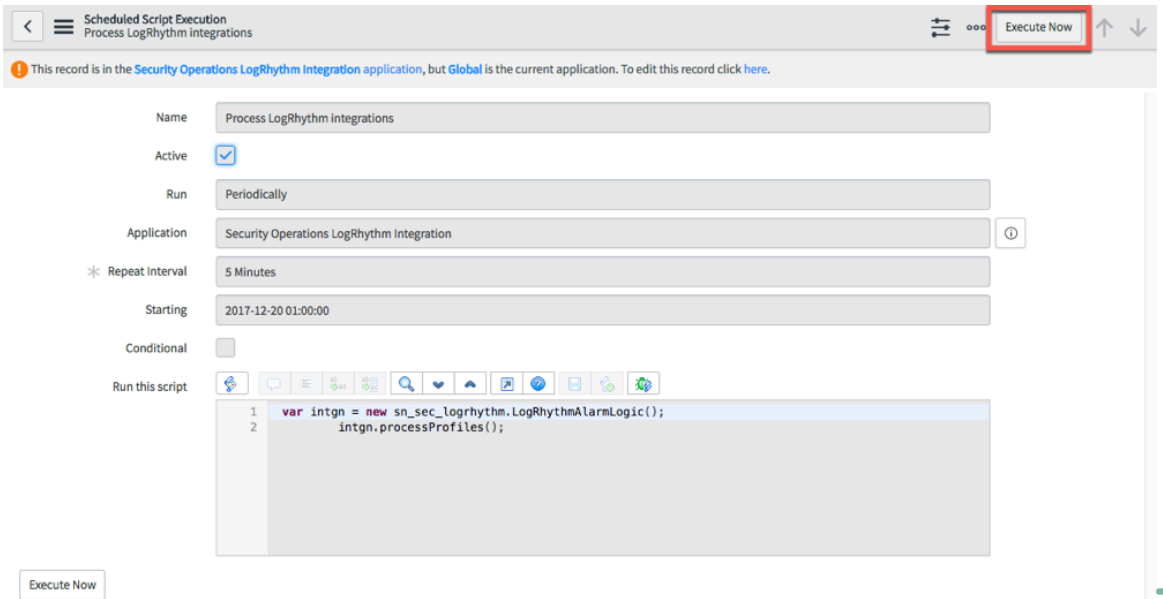
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Tâche planifiée** > **Travaux planifiés** et sélectionnez le module **Travaux planifiés** .
2. Cliquez sur l'enregistrement de tâche d'intégrations de processus LogRhythm .
3. Dans l'enregistrement Exécution de script planifiée qui s'affiche, cliquez sur **Exécuter maintenant**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Si vous avez besoin d'aide supplémentaire en matière de dépannage, vous pouvez accéder au journal système pour les LogRhythm requêtes.

4. Pour d'autres problèmes de dépannage généraux, procédez comme suit pour accéder aux journaux système.

   a. Accédez à la **Journal système** > **Tous** et sélectionnez **Tous**.

   b. Définissez le filtre (Accéder à) sur **Source** et saisissez `sn_sec_logrhythm`.

   c. Appuyez sur **Entrée**.
   Tous les messages générés par l'intégration sont affichés dans cette table. Les messages répertoriés peuvent fournir un aperçu des processus en cours d'exécution de l'intégration et peuvent vous aider à poursuivre le dépannage.

Intégration McAfee ePO

L'aptitude McAfee ePO d'intégration de détection et de réponse aux points de terminaison (EDR) qui aide les analystes du Centre des opérations de sécurité (SOC) à identifier les cybermenaces et à réparer les dommages causés par les fichiers malveillants.

Vue d'ensemble

Deux ensembles d'options sont utilisés dans cette intégration, les options qui appellent des actions, telles que l'isolement d'un hôte et le lancement d'une analyse anti-programme malveillant, et les options qui exécutent des requêtes pour recueillir les détails du système et les événements de McAfee ePO menace. Les deux types d'options, les actions et les requêtes, sont invoqués à partir de votre ServiceNow AI Platform® instance. Vous pouvez regrouper ces options afin qu'elles s'exécutent automatiquement lorsqu'un type spécifique d'événement de sécurité se produit, ou vous pouvez les invoquer manuellement à partir d'un ServiceNow AI Platform® incident de sécurité.

Les options suivantes McAfee ePO sont disponibles pour cette intégration.

Obtenir les détails du système

Rassemblez les détails du système, y compris ceux du système d'exploitation.

Lancer l'analyse anti-programme malveillant

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En fonction de la configuration et de la planification de l'analyse, lancez une analyse d'un point de terminaison impacté.

Isoler/Ne pas isoler l'hôte

Supprimez un système de l'accès réseau pour enquête et rétablissez l'accès au réseau.

Répertorier les événements de menace

Rassemblez l'état de conformité et les événements de menace les plus récents.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes.

- Prend en charge le déclenchement automatisé de requêtes basées sur les conditions d'incident McAfee ePO .
- Prend en charge le lancement McAfee ePO manuel d'options à partir d'incidents de ServiceNow AI Platform® Réponse aux incidents de sécurité sécurité (SIR) qui effectuent des actions à la demande.
- La possibilité de créer plusieurs profils pour déclencher différents types d'options McAfee ePOServiceNow AI Platform® Opérations de sécurité Ces profils recueillent des informations sur les événements de menace ou exécutent des actions en fonction des conditions de catégories d'incidents spécifiques, telles que les programmes malveillants.
- Validez la configuration de votre profil avec un aperçu des résultats sur SIR les McAfee ePO incidents de sécurité.
- Si le balisage est activé, les balises de sécurité identifient les McAfee ePO options initialement lancées par un workflow et lorsque les requêtes ou les actions sont terminées avec succès.
- Une piste d'audit complète des requêtes et des actions est publiée dans les notes de McAfee ePO travail sur SIR les incidents de sécurité, et les commandes de celles-ci ServiceNow AI Platform® sont enregistrées dans la McAfee ePO console.
- Prend en charge plusieurs McAfee ePO consoles.

ServiceNow Modules d'extension

Le module d'extension com.snc.si_dep est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications.

Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour assurer une installation fluide :

1. Cadre de travail d'intégration de sécurité
2. Security Support Common
3. Orchestration du support de sécurité
4. Security Incident Response
5. Espace de travail Réponse aux incidents de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, reportez-vous à la section Configurer votre ServiceNow AI Platform instance pour l'intégration McAfee ePO.

Module d'extension de l'extension ServiceNow

Le module d'extension ServiceNow Security Operations Extension for McAfee ePO# est requis pour cette intégration. Vous installez ce ServiceNow module d'extension dans votre McAfee ePO console. Pour plus d'informations, consultez Configurer votre ServiceNow AI Platform instance pour l'intégration McAfee ePO.

Serveur MID

Cette intégration nécessite l'installation et la configuration d'un serveur MID dans votre ServiceNow AI Platform® instance pour vous connecter au McAfee ePO serveur (console). Consultez le site Web de la documentation produit ServiceNow pour plus d'informations sur les serveurs MID.

Versions prises en charge de McAfee

L'intégration prend en charge les versions 5.9.1 et 5.10 de McAfee ePO. Il prend en charge McAfee Agent : MA 5.5.1.388 Pour plus d'informations sur les produits McAfee et ePolicy Orchestrator, consultez le site Web des produits McAfee .

L'intégration prend en charge la version 10.5 du produit McAfee Endpoint Security Threat Prevention. Si vous n'exécutez pas la version 10.5, consultez votre McAfee ePO administrateur pour voir si votre version peut prendre en charge les analyses à la demande via des actions de balise.

McAfee ePO Des balises de sécurité sont utilisées dans cette intégration. Vous devez créer ces balises dans votre McAfee ePO console. Pour plus d'informations sur ces balises, reportez-vous à la section Configurer votre McAfee ePO console à intégrer Réponse aux incidents de sécurité à (SIR).

Références

Référence	Identificateur de document	Titre de document
1	Site Web des produits McAfee	Site Web des produits McAfee
2	Documentation du produit McAfee Business pour ePolicy Orchestrator Cloud	Documentation produit McAfee
3	ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Pour obtenir une liste de contrôle permettant de suivre votre progression dans la configuration, l'installation et la vérification des résultats de l'intégration, reportez-vous à la section Liste de vérification pour l'intégration McAfee ePO.

Pour une installation fluide de l'application et pour vous aider à vérifier les résultats attendus, suivez les rubriques dans l'ordre dans lequel elles sont présentées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Architecture d’intégration pour McAfee ePO

Architecture d’intégration pour McAfee ePO

La rubrique suivante donne un aperçu de l’architecture du système et répertorie les principales fonctionnalités de l’intégration. Cette section fournit également des informations sur les étapes de configuration que vous devez effectuer dans votre ServiceNow AI Platform instance et dans la console McAfee ePolicy Orchestrator (McAfee ePO) avant d’installer l’application à partir de .ServiceNow Store

Termes clés pour l’intégration McAfee ePO

Les termes suivants sont utilisés dans la documentation d’installation et de configuration de l’intégration.

ServiceNow AI Platform

Un produit d’entreprise ServiceNow . Il ServiceNow AI Platform s’agit de la base sur laquelle reposent les composants individuels, tels que Réponse aux incidents de sécurité (SIR), IT Service Management (ITSM) et d’autres produits.

Réponse aux incidents de sécurité (SIR)

Une ServiceNow AI Platform application qui suit la progression des incidents de sécurité depuis la découverte et l’analyse initiale, en passant par le confinement, l’éradication et la récupération, jusqu’à la revue et la fermeture finales post-incident.

Module d'extension

Les modules d’extension sont des composants logiciels qui fournissent des fonctionnalités spécifiques au sein de votre ServiceNow AI Platform instance. Pour plus d’informations sur l’installation et la configuration des modules d’extension d’intégration, reportez-vous à la section Installez l’application et configurez un serveur pour l’intégration McAfee ePO.

Orchestrateur ePolicy (McAfee ePO)

Console utilisateur dans laquelle vous gérez les services, les produits et les paramètres McAfee.

Module d’extension McAfee

Ce ServiceNow module d’extension est requis pour cette intégration. Ce module d’extension réside sur votre McAfee ePO console et la connecte McAfee ePO à votre ServiceNow AI Platform instance.

Option

Une activité automatique lancée à partir de votre ServiceNow AI Platform instance qui s’exécute dans la McAfee ePO console pour effectuer des requêtes d’enrichissement et effectuer des actions sur vos actifs.

Profil

Les paramètres des McAfee ePO options que vous configurez pour spécifier quand et dans quelles conditions les options exécutent des requêtes d’enrichissement et effectuent des actions sur vos actifs.

Utiliser un Serveur MID

Application qui facilite la communication et le mouvement de données entre les applications, les sources de données et les ServiceNow AI Platform services externes.

ServiceNow Administrateur (admin)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un utilisateur disposant de ce rôle télécharge et installe les modules d'extension et SIRMcAfee ePO sur votre ServiceNow AI Platform instance. Un utilisateur disposant de ce rôle affecte également le rôle d'administrateur d'incident de sécurité selon les besoins.

ServiceNow Administrateur d'incident de sécurité (sn_si.admin)

Un utilisateur disposant de ce rôle effectue la configuration de l'intégration McAfee ePO avec le Réponse aux incidents de sécurité produit (SIR) dans votre ServiceNow AI Platform instance selon les besoins. Un utilisateur disposant de ce rôle affecte également le rôle d'analyste des incidents de sécurité selon les besoins.

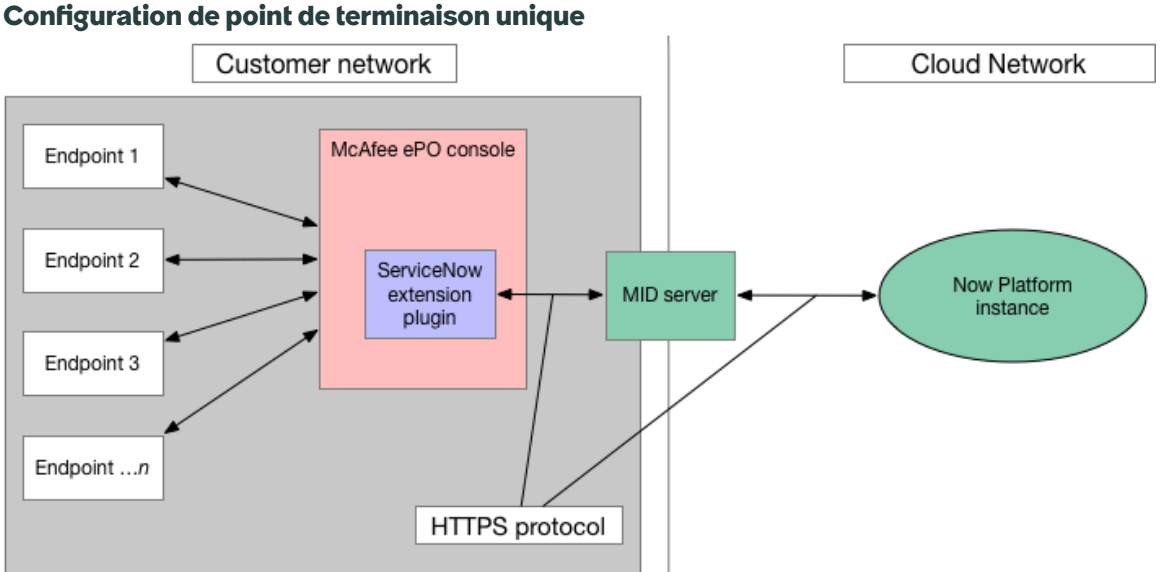
ServiceNow Analyste des incidents de sécurité (sn_si.analyst)

Un utilisateur disposant de ce rôle interagit avec les incidents de sécurité dans le produit SIR et les analyse.

Connexion système et flux de données

La figure suivante est un exemple d'environnement client. Un ServiceNow AI Platform Serveur MID est requis pour que votre ServiceNow AI Platform instance puisse se connecter à un McAfee ePO serveur (console) via un module d'extension ServiceNow Une fois connecté, vous appelez vos options pour lancer des analyses anti-programmes malveillants, isoler les ordinateurs hôtes et les restaurer sur votre réseau, récupérer les résultats de ServiceNow AI Platform la dernière analyse et collecter les détails système sur vos actifs. Lorsque ces fonctionnalités renvoient des résultats de vos actifs qui correspondent à vos critères de recherche, les données sont extraites via le serveur MID vers votre ServiceNow AI Platform instance. Les données sont affichées sur les listes connexes d'un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR). La figure suivante illustre le flux de données pour un groupe de points de terminaison gérés par une McAfee ePO seule console.

Configuration de point de terminaison unique

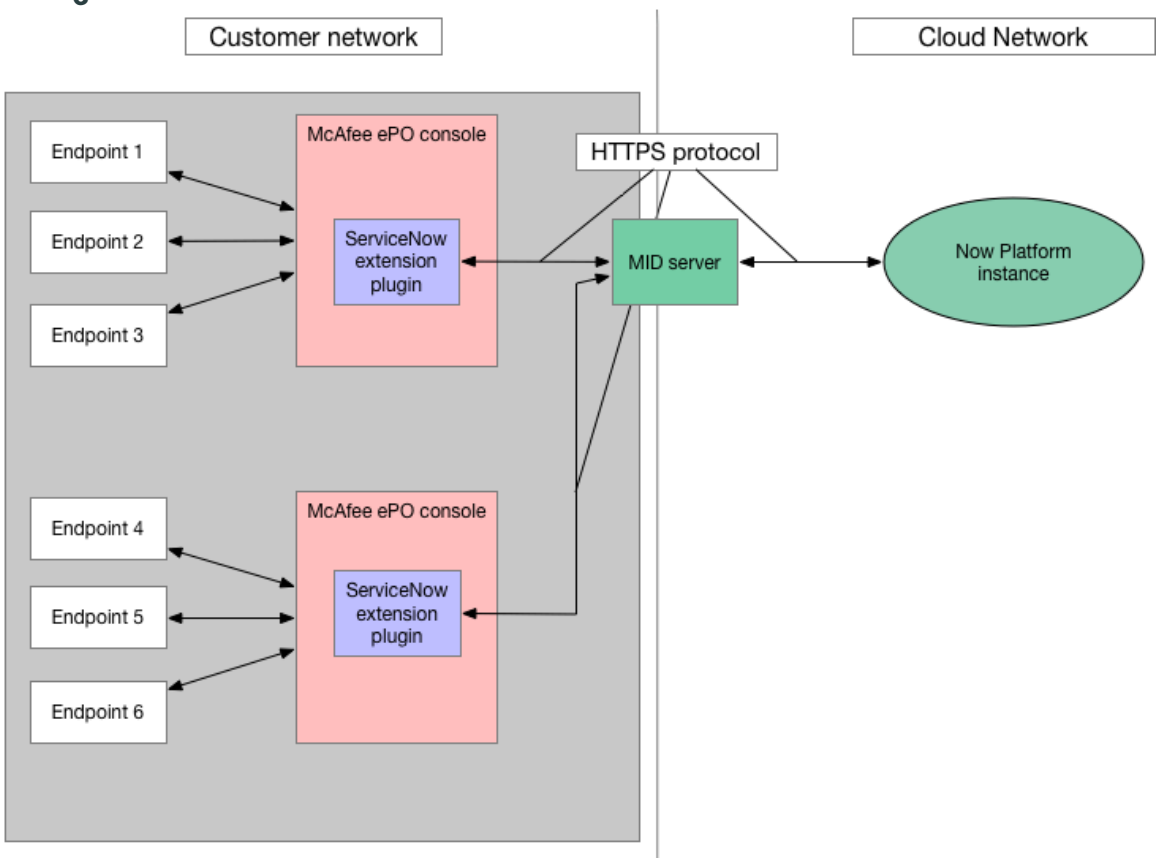


Comme le montre la figure suivante, cette intégration peut prendre en charge plus d'une McAfee ePO console. Vous pouvez avoir un groupe de points de terminaison géré par une McAfee ePO console et un autre groupe de points de terminaison géré par une autre McAfee ePO console. Les données de plusieurs McAfee ePO consoles sont extraites via un seul MID Server. Toutefois, vous pouvez également préférer configurer plusieurs serveurs MID si votre organisation l'exige.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration des MID Servers



Workflows pour l'intégration McAfee ePO

Cette intégration comprend les workflows suivants. Ces workflows sont préconfigurés et conçus spécifiquement pour cette intégration. Vous pouvez modifier ces workflows pour répondre aux besoins de votre organisation, selon vos besoins. Pour plus d'informations générales sur les workflows et l'utilisation de l'éditeur de workflow, voir Introduction aux workflows .

- Intégration de Security Operations à McAfee ePO : obtenir les détails de l'hôte
- Intégration de Security Operations à McAfee ePO : lancer l'analyse anti-programme malveillant
- Intégration de Security Operations à McAfee ePO : isoler l'hôte
- Opérations de sécurité Intégration McAfee ePO : liste Événements de menace
- Intégration McAfee ePO pour Opérations de sécurité - Supprimer l'isolement

Connexion aux systèmes externes

L'intégration nécessite que le serveur MID communique via une connexion de protocole HTTPS à la McAfee ePO console.

Liste de vérification pour l'intégration McAfee ePO

Utilisez cette liste de vérification pour vous guider à travers toutes les tâches de l'intégration. La liste de vérification suivante comprend des tâches de configuration et d'installation ainsi que des exemples de cas d'utilisation qui incluent les résultats attendus pour l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : les rôles sont répertoriés pour chaque étape.

Pourquoi et quand exécuter cette tâche
Suivez votre progression avec l'installation, l'installation et la configuration de l'intégration avec la table suivante. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante. Chaque ligne de la table répertorie les tâches et identifie les rôles requis pour effectuer les tâches. Les rubriques numérotées du guide d'installation et de configuration sont également référencées.

Procédure

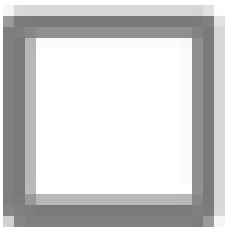
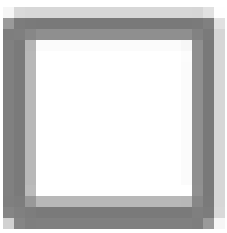
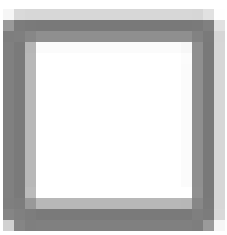
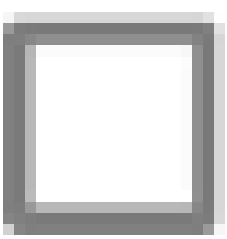
Suivez les étapes du tableau dans l'ordre dans lequel elles se présentent.

Liste de vérification

Élément	Description
☐	En tant qu'utilisateur disposant du rôle d'administrateur ServiceNow AI Platform® , configurez votre ServiceNow AI Platform® instance. **a.** Affecter ServiceNow AI Platform® et Réponse aux incidents de sécurité des rôles. **b.** Vérifiez que tous les ServiceNow Réponse aux incidents de sécurité autres modules d'extension prenant en charge l'intégration sont installés et activés pour votre version du ServiceNow AI Platform. **c.** Installez et configurez un Serveur MID dans votre ServiceNow AI Platform® instance. **d.** Créez un groupe d'approbation si vous souhaitez traiter les demandes envoyées par l'analyste d'incident de sécurité pour isoler l'hôte et lancer des actions d'analyse anti-programme malveillant. Pour plus d'informations, consultez Configurer votre ServiceNow AI Platform instance pour l'intégration McAfee ePO.
☐	En tant qu'administrateur McAfee ePO , configurez votre McAfee ePO console. **a.** Vérifiez que vous utilisez la version 5.9 de McAfee ePO. **b.** Installez le module d'extension ServiceNow dans votre McAfee ePO console. **c.** Vérifiez que vous avez créé des balises de sécurité dans votre McAfee ePO console pour isoler l'hôte et lancez des actions d'analyse anti-programme malveillant. Pour plus d'informations, consultez Configurer votre McAfee ePO console à intégrer Réponse aux incidents de sécurité à (SIR). Pour plus d'informations et pour obtenir le fichier du module d'extension dans votre ServiceNow AI Platform instance, accédez à **Base de connaissances** > **Articles** > **Tous** et, dans le champ Rechercher, entrez ServiceNow Security Operations Extension for McAfee ePO.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	En tant qu'utilisateur disposant du rôle d'administrateur ServiceNow AI Platform , installez l'application McAfee ePO à partir de , ServiceNow Store configurez un serveur et connectez-vous à la McAfee ePO console. Pour plus d'informations, consultez Installez l'application et configurez un serveur pour l'intégration McAfee ePO.
	En tant qu'utilisateur ayant le rôle d'administrateur d'incident ServiceNow AI Platform de sécurité, modifiez les noms des balises de sécurité dans votre ServiceNow AI Platform® instance afin qu'ils correspondent aux noms de balises que vous avez créés dans votre McAfee ePO console. Pour plus d'informations, consultez Modifier les balises de sécurité dans le ServiceNow AI Platform pour l'intégration McAfee ePO.
	En tant qu'utilisateur ayant le rôle d'administrateur d'incident de sécurité, créez un profil pour McAfee ePO les options. Pour plus d'informations sur les profils, reportez-vous à la section McAfee ePO Profils d'aptitude d'intégration. Pour connaître les étapes nécessaires à la création d'un profil, reportez-vous à la section Créer un profil d'aptitude.
	En tant qu'utilisateur ayant le rôle d'administrateur d'incident de sécurité, configurez un profil et testez les incidents de sécurité. **a.** Passez en revue les informations sur les conditions et les paramètres de déclenchement. **b.** Configurez un profil. **c.** Tester et prévisualiser les incidents de sécurité. **d.** Localisez les résultats de recherche et d'autres détails sur les listes connexes de l'incident de sécurité. **e.** Créez et configurez différents types de profils et testez les incidents de sécurité pour chaque type. Pour plus d'informations sur les conditions de déclenchement et le champ CI alternatif, reportez-vous à la section Définir des conditions de déclenchement avec un champ d'élément de configuration (CI). Pour connaître les étapes nécessaires à la configuration d'un profil, tester et prévisualiser les incidents de sécurité, ainsi que des exemples de types de profil, reportez-vous aux exemples ci-dessous Configurer les paramètres.
	En tant qu'utilisateur ayant le rôle d'analyste ServiceNow AI Platform des incidents de sécurité, soumettez des demandes supplémentaires pour les analyses de programme malveillant et répertoriez les événements de menace. Pour plus d'informations, voir Déclencher McAfee ePO manuellement le profil à partir d'un incident de sécurité Dans le ServiceNow AI Platform, en tant qu'utilisateur disposant d'un rôle d'approbation, ou en tant que membre d'un groupe d'approbation, approuvez les demandes d'isolement de l'hôte et de suppression de l'isolement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément	Description
	Pour plus d'informations sur le traitement des demandes d'approbation, reportez-vous à la section Créer un groupe d'approbation.

Vous avez terminé avec succès les étapes d'installation, installé et configuré l'application et vérifié les résultats attendus pour l'intégration.

Configurer votre ServiceNow AI Platform® instance pour l'intégration McAfee ePO

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre ServiceNow AI Platform® instance avant d'installer l'application pour l'intégration McAfee ePO .

Configurer les besoins

Rôle requis : ServiceNow AI Platform administrateur (admin). Examinez les informations suivantes devant votre ServiceNow AI Platform® instance pour l'intégration McAfee ePO .

La table suivante répertorie les exigences de configuration pour l'application. Vérifiez que vous avez effectué ces tâches avant d'installer l'application pour l'intégration à partir du ServiceNow Store.

Configurer la tâche	Description
Vérifiez que vous avez affecté les rôles et (SIR) requis.ServiceNow AI Platform®Réponse aux incidents de sécurité	Les rôles suivants sont requis : • Un utilisateur disposant du rôle d'administrateur système (admin) pour installer l'application. • Un utilisateur ayant le rôle d'administrateur d'incident de sécurité (sn_si.admin) configure l'application et crée, active et supprime des profils. • Un utilisateur ayant le rôle d'analyste des incidents de sécurité (sn_si.analyst) travaille sur les incidents de sécurité. Les tâches comprennent le lancement manuel de profils à partir d'incidents de sécurité. Si l'option d'approbation est sélectionnée dans un profil au cours de l'étape de configuration, les utilisateurs disposant de ce rôle soumettent également des demandes pour isoler les hôtes et les renvoyer sur le réseau.
Vérifiez que vous utilisez la version 5.9 de McAfee ePO.	L'intégration prend en charge la version 10.4.3 de McAfee ePolicy Orchestrator.
Vérifiez que vous avez installé le module d'extension ServiceNow dans votre McAfee ePO console.	Installez le module d'extension ServiceNow dans votre McAfee ePO console. Pour plus d'informations et pour obtenir le fichier du module d'extension, dans votre ServiceNow AI Platform instance, accédez à **Base de connaissances** > **Articles** > **Tous**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la tâche	Description
	et, dans le champ Rechercher, entrez ServiceNow Security Operations Extension for McAfee ePO .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Espace de travail Réponse aux incidents de sécurité **3.** Cadre de travail d'intégration de sécurité **4.** Security Support Common **5.** Orchestration du support de sécurité Pour plus d'informations sur l'installation des applications principales Security Operations, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.
Vérifiez que vous avez installé et configuré un Serveur MID.	Un Serveur MID installé et configuré est requis dans votre ServiceNow AI Platform® instance. Consultez le site Web de la documentation produit ServiceNow pour plus d'informations sur les serveurs MID.
Si vous souhaitez activer le processus d'approbation pour les profils, vérifiez que vous avez créé un groupe d'approbation pour traiter les demandes.	Il existe un processus d'approbation facultatif permettant d'isoler les machines hôtes et de les restaurer sur le réseau. Si cette option est activée, une approbation préalable est requise avant que les machines hôtes ne soient isolées et restaurées sur votre réseau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la tâche	Description
	Si votre organisation souhaite un niveau de contrôle supplémentaire sur ces actions, activez l'option **Exiger l'approbation** pendant l'étape de configuration d'un profil. Par défaut, l'autorisation d'approbation est affectée à l'administrateur d'incident ServiceNow AI Platform® de sécurité (sn_si.admin). Cette autorisation peut être réaffectée à un groupe d'approbation. Au sein du groupe, tout membre a la permission d'approuver ou de rejeter les demandes. Vous sélectionnez un groupe d'approbation actif pendant l'étape de configuration de la configuration de votre profil. Pour plus d'informations, consultez Créer un groupe d'approbation.

Configurer votre McAfee ePO console à intégrer Réponse aux incidents de sécurité à (SIR)

La section suivante répertorie les étapes de configuration que vous devez effectuer dans votre McAfee ePO console avant d'installer l'application à partir de ServiceNow Store pour l'intégration.

Avant de commencer

Rôle requis : McAfee ePO administrateur

En tant qu'utilisateur disposant de l'autorisation d'administrateur McAfee ePO , vérifiez que vous avez installé le module d'extension Servicenow.zip dans votre McAfee ePO console. Ce module d'extension est requis pour l'intégration. Pour plus d'informations et pour obtenir le module d'extension, accédez à votre ServiceNow AI Platform instance **Base de connaissances** > **Articles** > **Tous**. Dans le champ de recherche, saisissez ServiceNow Security Operations Extension for McAfee ePO.

Pourquoi et quand exécuter cette tâche

Le module d'extension ServiceNow connecte votre ServiceNow AI Platform instance à votre McAfee ePO console. Cette connexion vous permet de référencer les balises de sécurité que vous créez dans votre McAfee ePO console pour isoler l'hôte et lancer des actions d'analyse anti-programme malveillant vers les profils d'aptitude de votre ServiceNow AI Platform instance.

Les balises de sécurité de votre McAfee ePO console doivent correspondre aux balises de sécurité des enregistrements d'aptitude de votre ServiceNow AI Platform instance.

Les étapes suivantes vous montrent comment installer le module d'extension d'extension, créer une balise de sécurité dans votre McAfee ePO console et affecter une action à la balise. Pour plus d'informations sur les balises de sécurité de la McAfee ePO console, consultez le site Web de la documentation produit McAfee .

Remarque : Les chiffres de la section suivante proviennent de la McAfee ePO console.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si vous n’avez pas installé le module d’extension ServiceNow sur votre McAfee ePO console, procédez comme suit pour l’installer.

   a. Connectez-vous à votre McAfee ePO console à l’aide de votre nom d’utilisateur et de votre mot de passe McAfee.

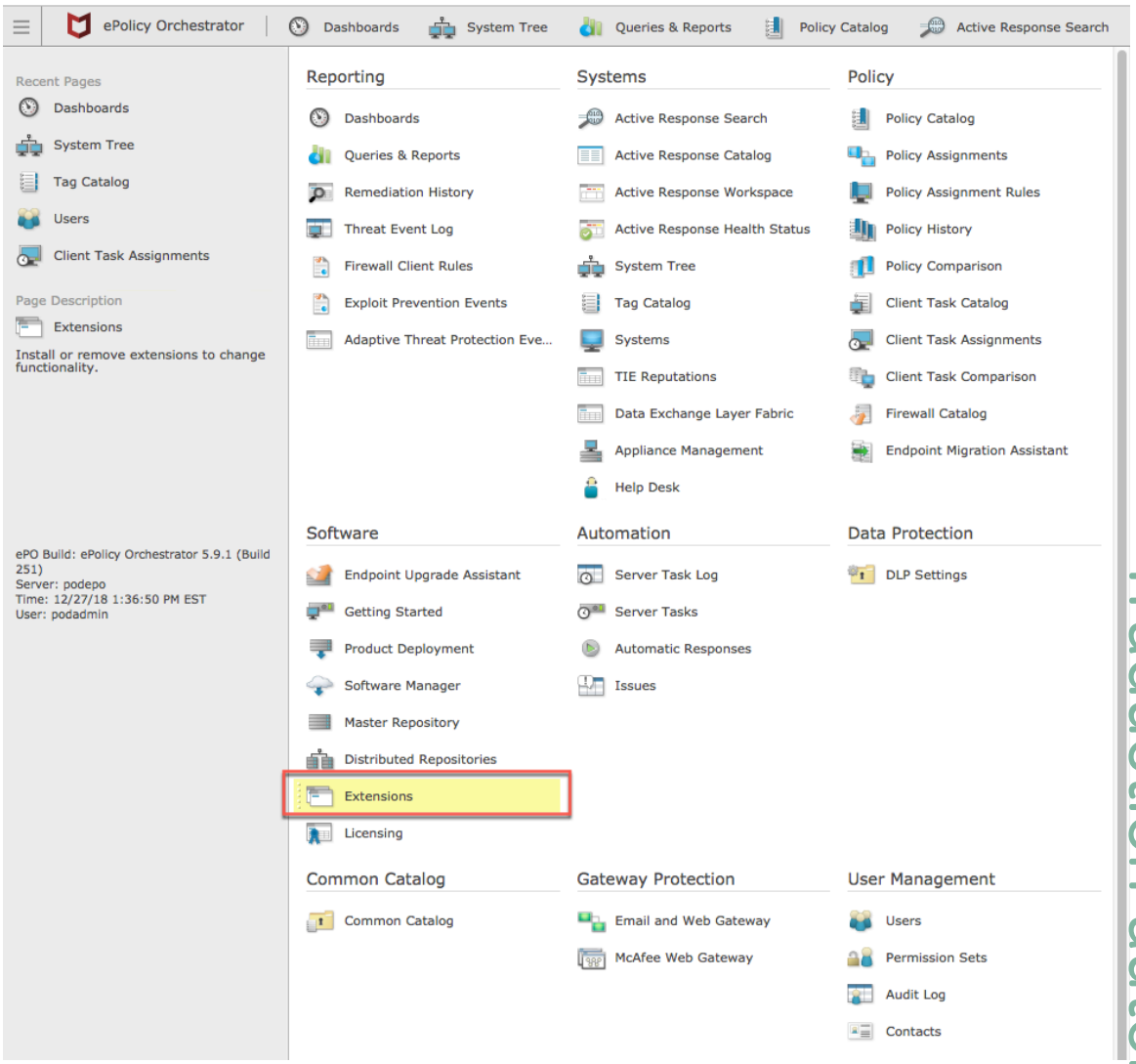


2. Si la page illustrée dans la figure suivante n’est pas affichée, cliquez sur l’icône de menu en haut à gauche de la bannière de la page d’accueil.

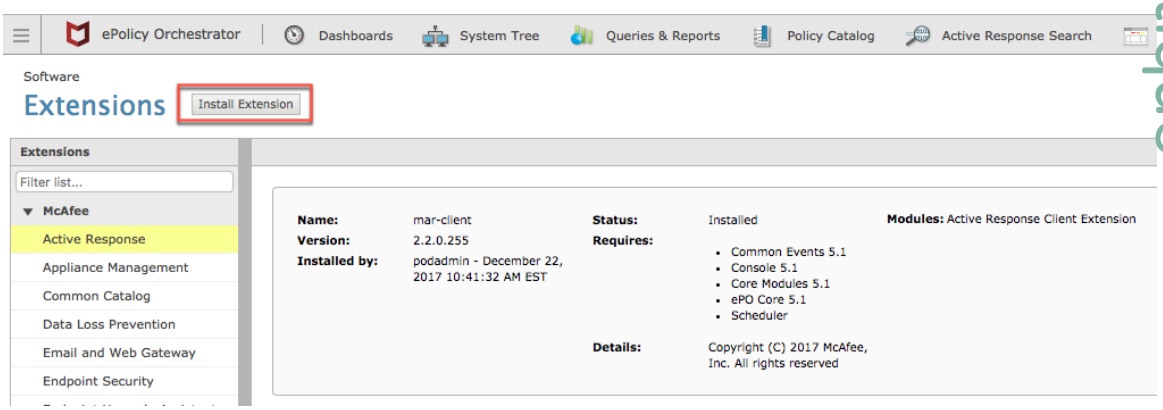
3. Dans la section Logiciel, cliquez sur le lien **Extensions** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



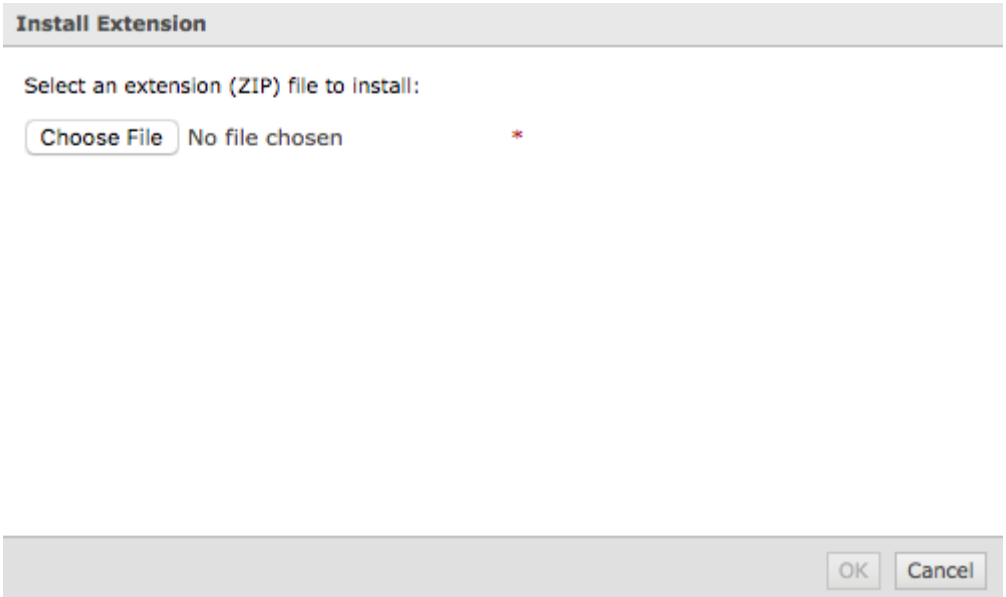
4. Sur la page Extensions qui s'affiche, cliquez sur **Installer l'extension**.



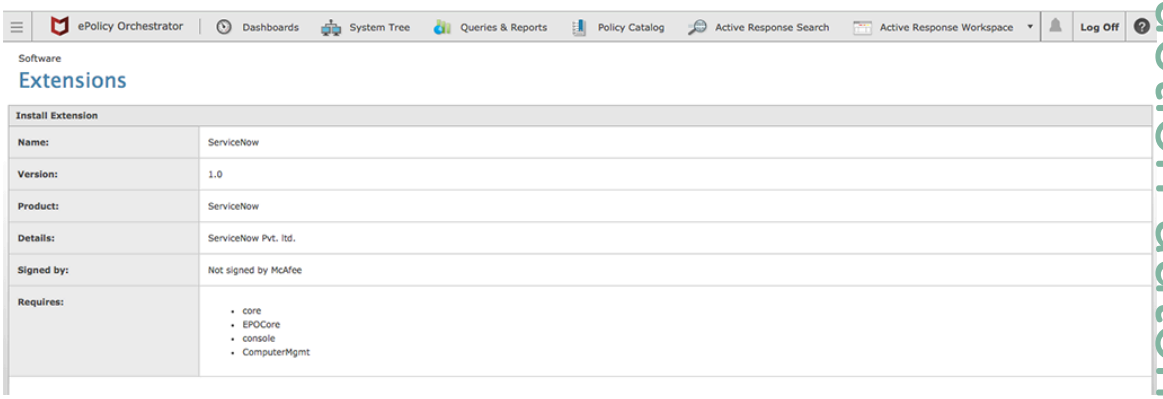
5. Dans la boîte de dialogue Installer l'extension, cliquez sur **Choisir un fichier**, accédez au fichier Servicenow.zip sur votre système, puis cliquez sur **OK** pour le télécharger.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois le téléchargement terminé, la page Software Extensions s'affiche avec le module d'extension ServiceNow Extension répertorié.



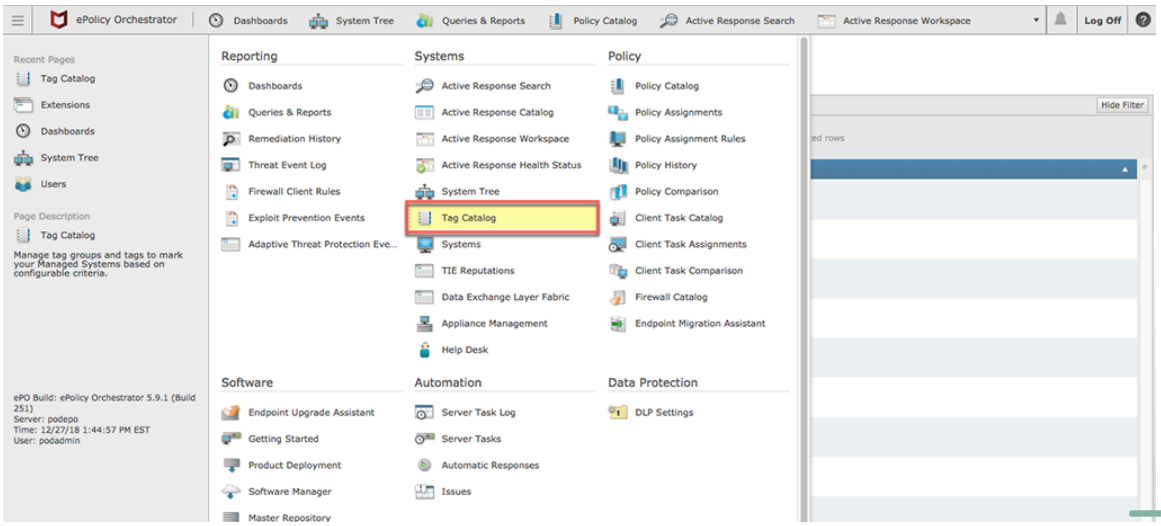
Vous avez correctement installé l'extension de module d'extension ServiceNow sur votre McAfee ePO console.

6. Si vous n'avez pas créé de balises de sécurité dans McAfee ePO la console pour lancer l'analyse anti-programme malveillant et isoler les actions de l'hôte, procédez comme suit.

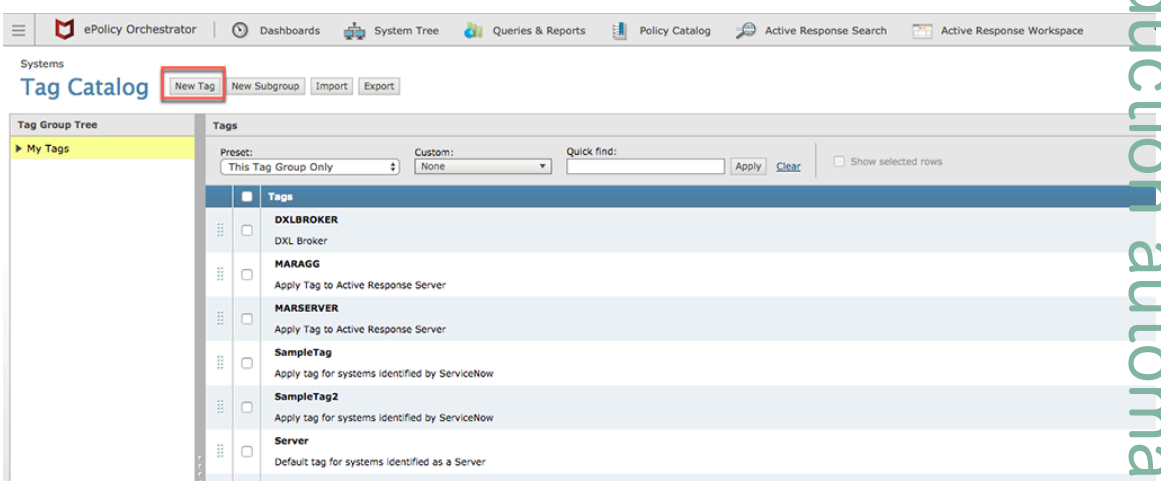
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la page d'accueil et cliquez sur le lien **Catalogue de balises** .

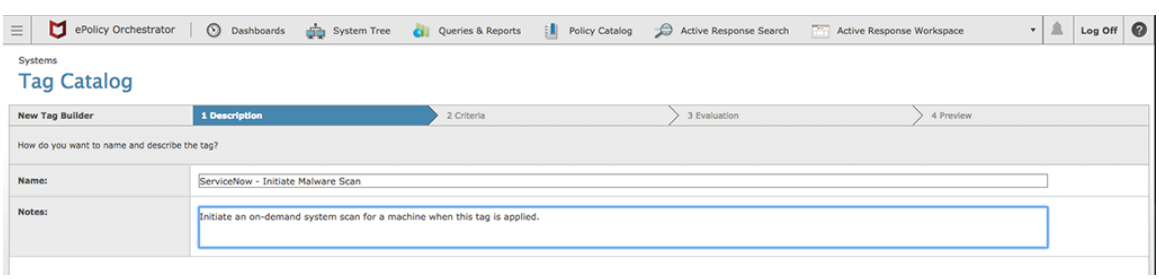


b. Sur la page Catalogue de balises qui s'affiche, cliquez sur **Nouvelle balise**.



c. Une fois l'étape Description sélectionnée dans la barre de progression qui s'affiche, saisissez un nom et une description pour la balise.

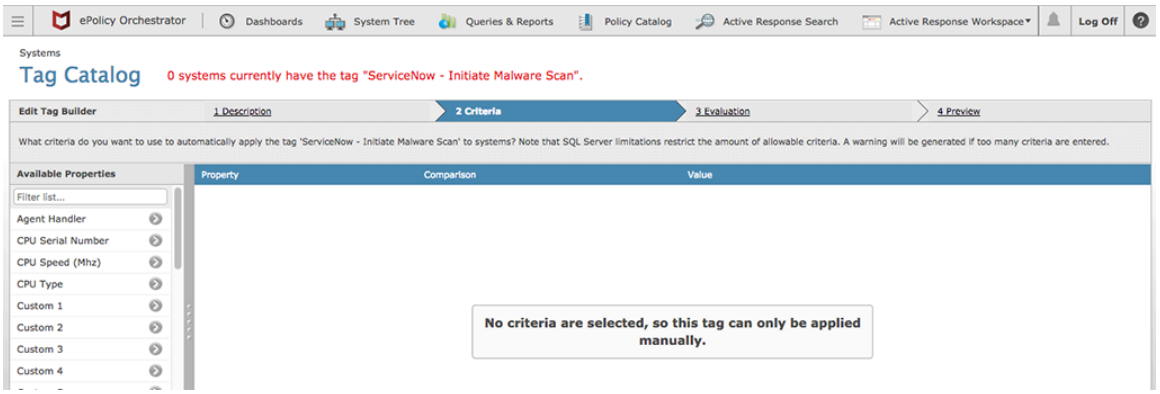
Pour cet exemple, une balise avec un nom et une description pour l'aptitude Lancer l'analyse anti-programme malveillant s'affiche. Ce nom de balise est ce qui est mis en correspondance et référencé dans votre ServiceNow AI Platform instance.



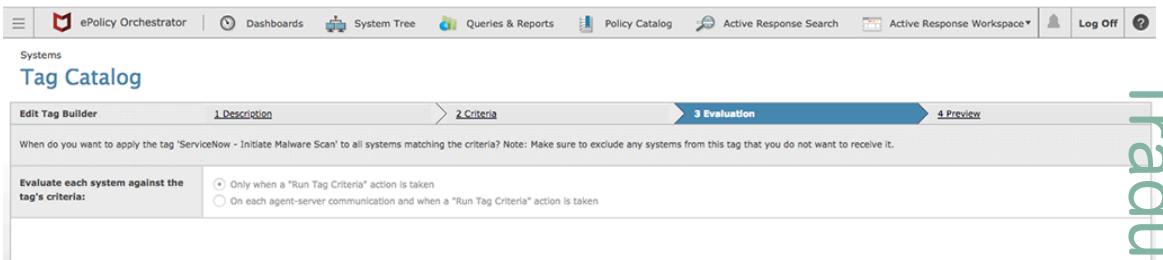
d. Pour passer à l'étape Critères, cliquez sur **Critères** dans la barre de progression.
Les messages qui s'affichent indiquent qu'aucune action n'est actuellement affectée à cette balise et que la balise ne peut être appliquée que manuellement.

Traduction automatique

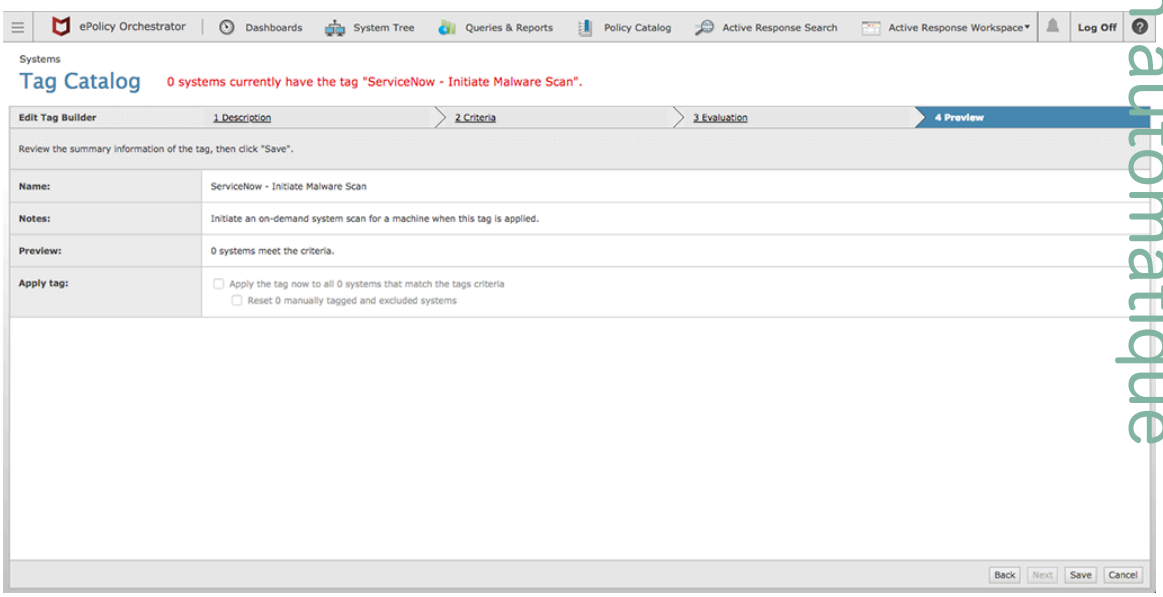
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Cliquez sur **Évaluation** dans la barre de progression pour continuer.



f. Une fois la page Catalogue de balises de l'étape d'évaluation affichée, laissez les paramètres de cette page par défaut et, dans la barre de progression, cliquez sur **Aperçu**.

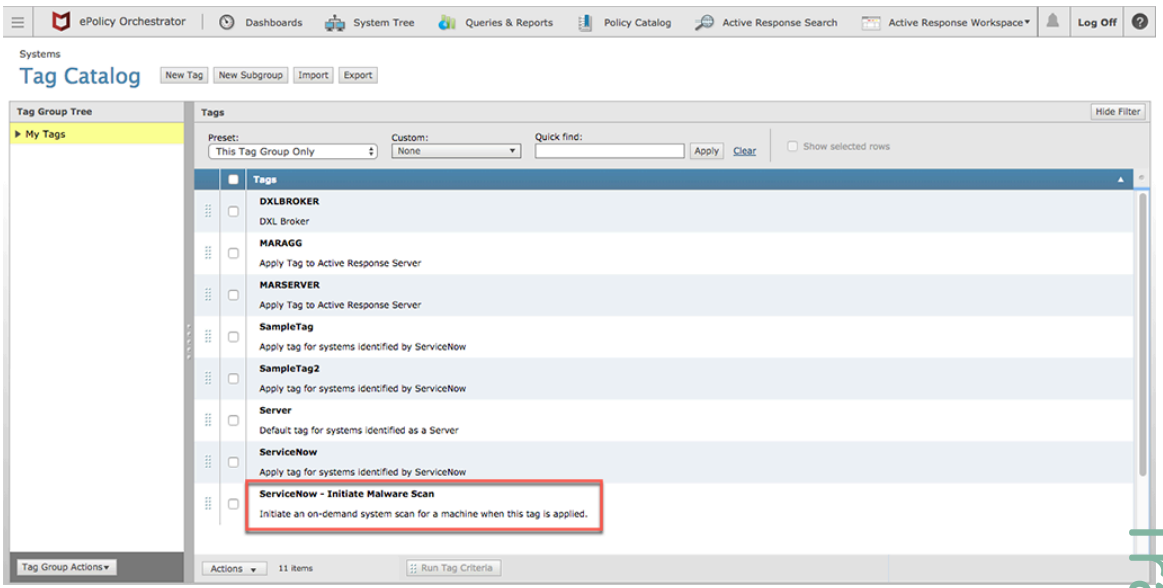


g. Une fois la page Aperçu affichée, en bas à droite de la page, cliquez sur **Enregistrer** pour enregistrer l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

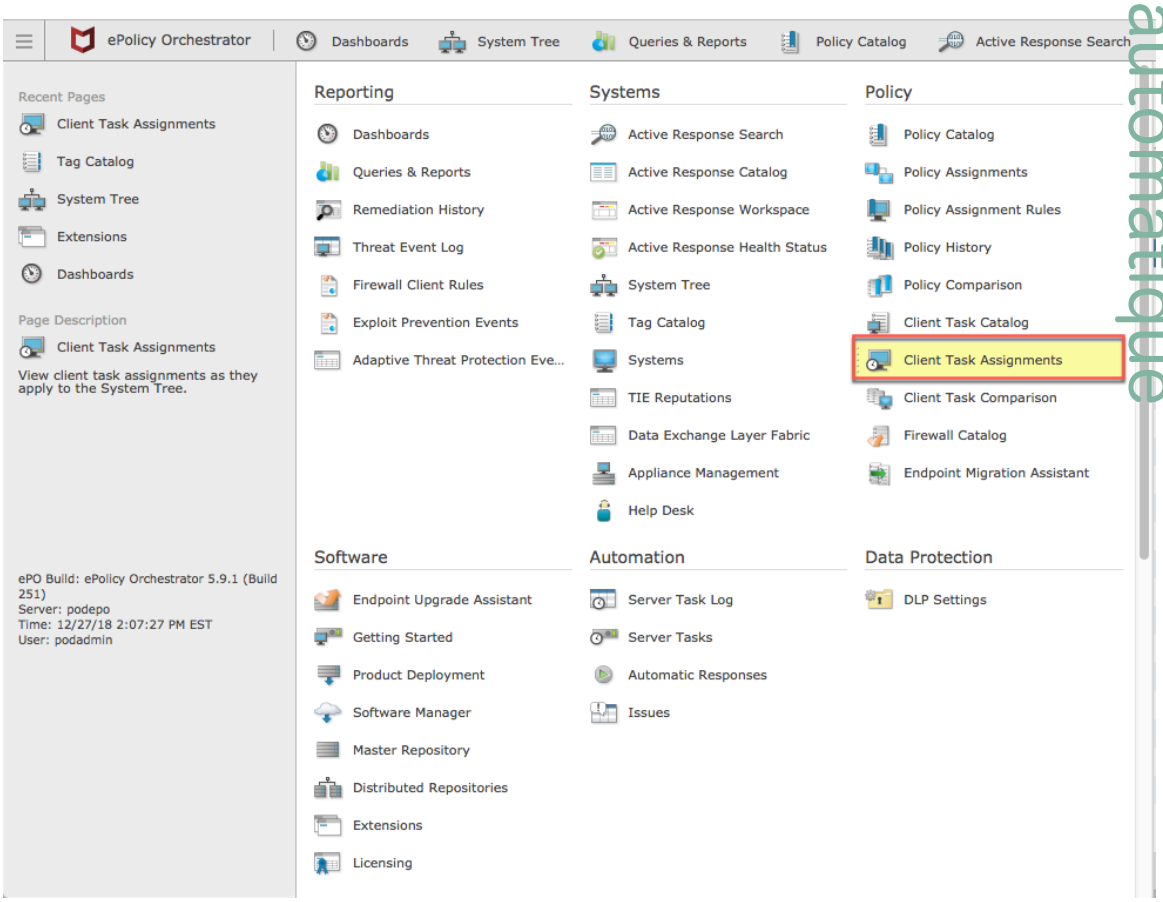
La nouvelle balise s’affiche dans le catalogue de balises, comme illustré dans la figure suivante.



7. Créez une balise de sécurité pour l’action d’isolement de l’hôte en répétant les étapes précédentes.
Une fois que vous avez créé les deux balises, vous êtes prêt à affecter des actions aux nouvelles balises.

8. Pour ajouter une action à votre nouvelle balise, procédez comme suit.

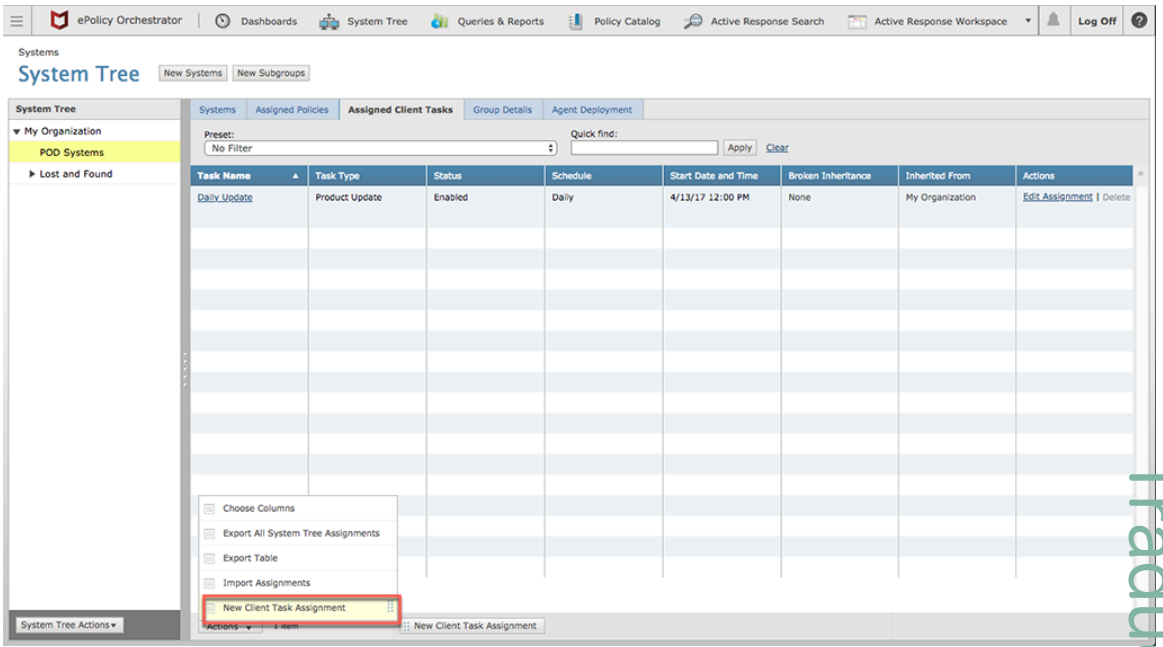
a. Accédez à la page d’accueil et, dans la section Politique, cliquez sur le lien **Affectations de tâches client** .



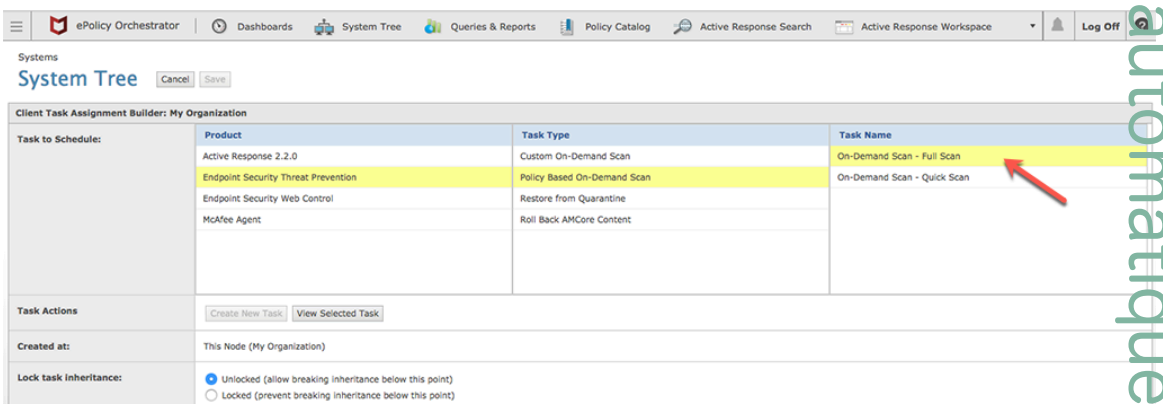
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

b. Dans la page System Tree qui s'affiche, en bas de la page, développez le menu **Actions** et sélectionnez **Nouvelle affectation de tâche client**.



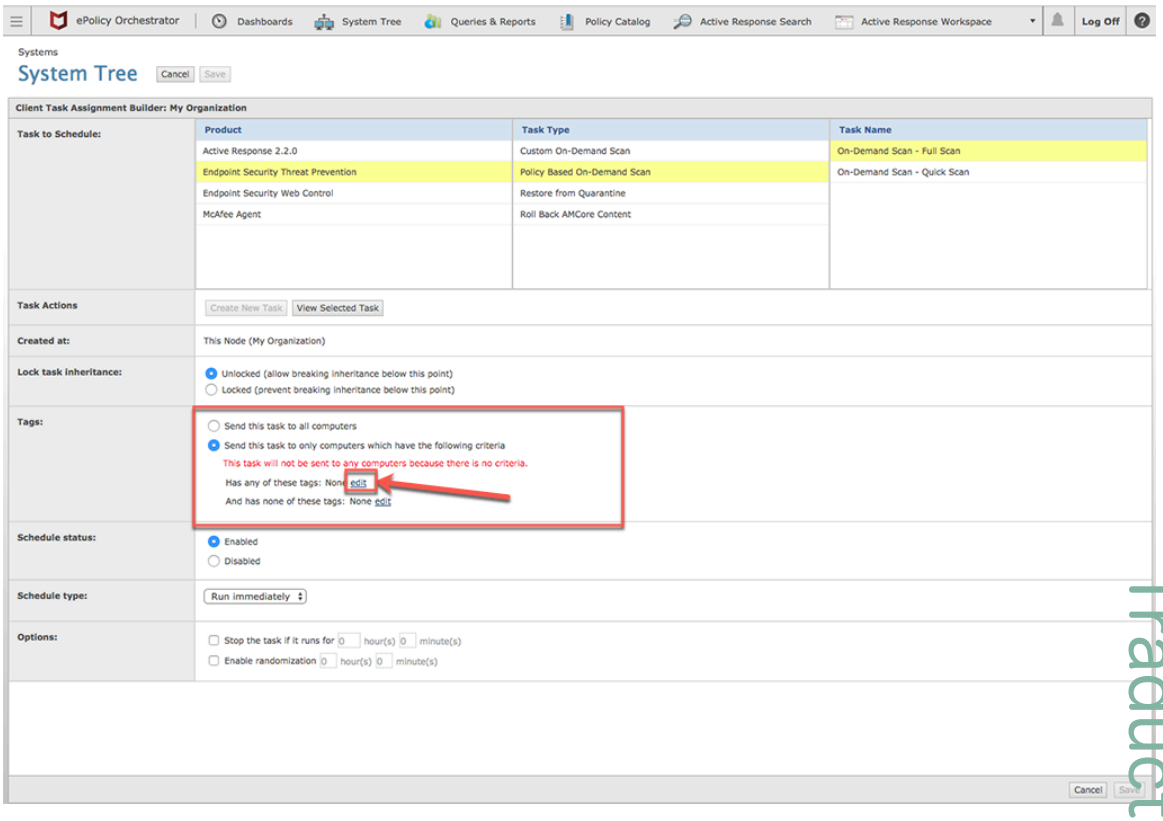
c. Sur la page qui s'affiche, accédez à **Prévention des menaces de sécurité du point de terminaison** > **Analyse sur demande basée sur une politique** > **Analyse à la demande : analyse complète** en sélectionnant le chemin comme illustré dans la figure suivante.



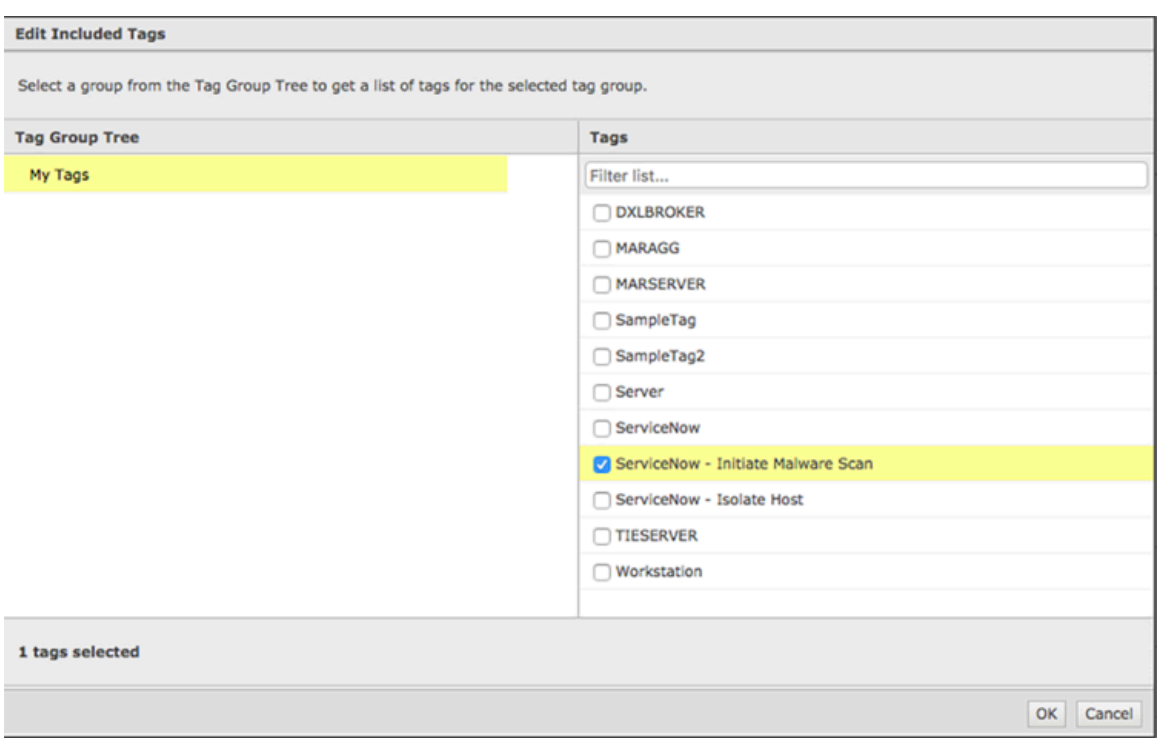
d. Dans la section Balises, sous la case d'option et à côté de A l'une de ces balises :, cliquez **sur le lien** Modifier pour modifier les critères de la balise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Dans la boîte de dialogue qui s'affiche, sélectionnez la balise Lancer l'analyse ServiceNow anti-programme malveillant que vous avez créée lors des étapes précédentes, puis cliquez sur **OK**.



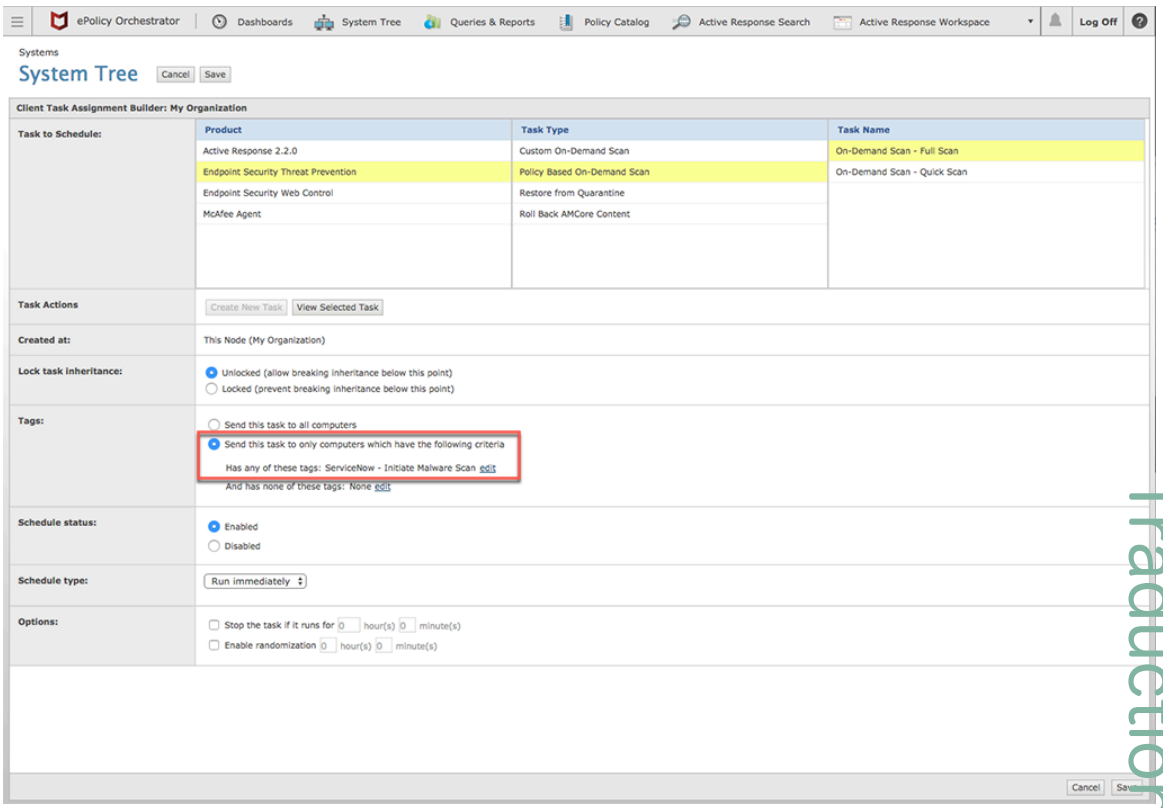
La balise ServiceNow Initiate Malware Scan que vous avez créée est affectée à l'action d'analyse à la demande.

f. Cliquez sur **OK**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

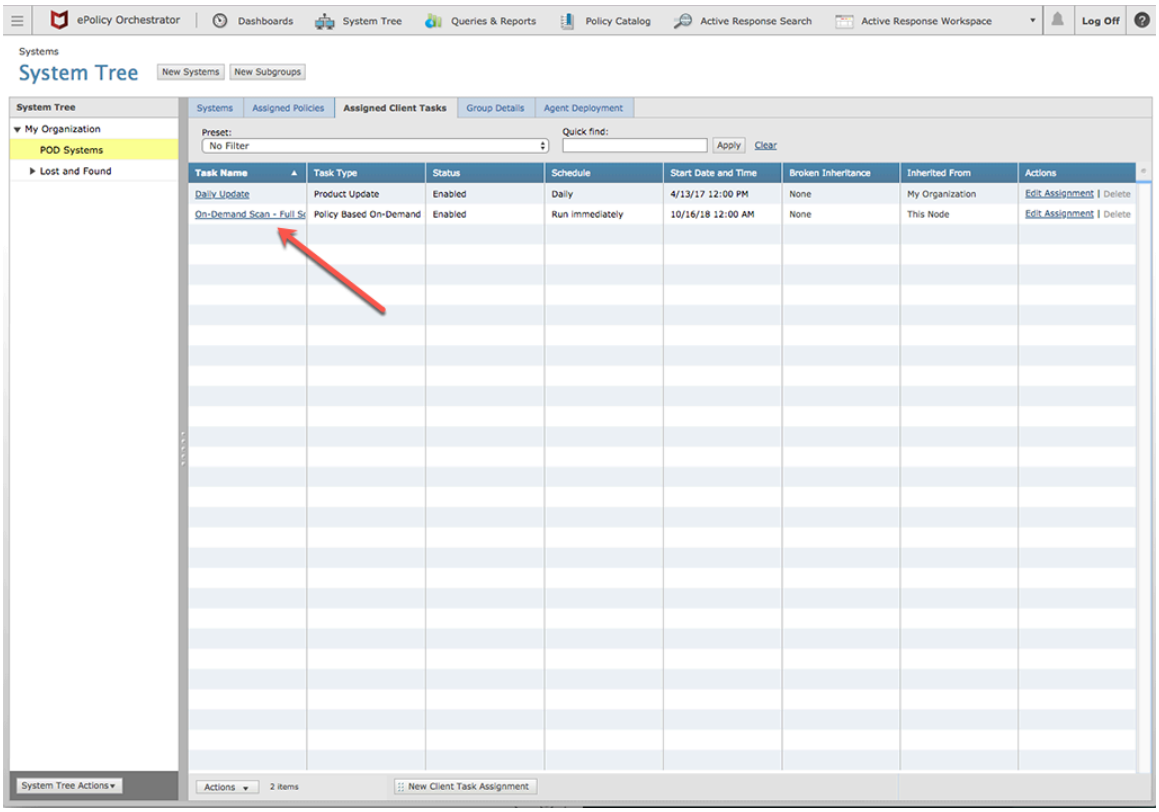
Dans la section Balises, sous la case d'option et à côté de A l'une de ces balises :, la balise Lancer l'analyse anti-programme malveillant s'affiche.



g. Cliquez sur **Enregistrer**.
Sur la page de l'arborescence des systèmes, la tâche s'affiche dans la liste Tâches du client affectées (onglet).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



h. Si vous n'avez pas affecté d'action à l'action Isoler l'hôte, répétez les étapes précédentes pour l'affecter.

Vous avez correctement installé le module d'extension d'extension, créé des balises de sécurité et affecté des tâches à vos balises. Vous avez terminé la configuration de l'intégration dans votre McAfee ePO console. L'étape suivante consiste à configurer un serveur dans votre ServiceNow AI Platform instance.

Installez l'application et configurez un serveur pour l'intégration McAfee ePO

Avant d'appeler les workflows pour l'intégration, installez et configurez l'application McAfee ePO sur ServiceNow Store votre ServiceNow AI Platform instance. La configuration est requise pour se connecter à la McAfee ePO console.

Avant de commencer

Rôle requis : ServiceNow AI Platform administrateur (admin)

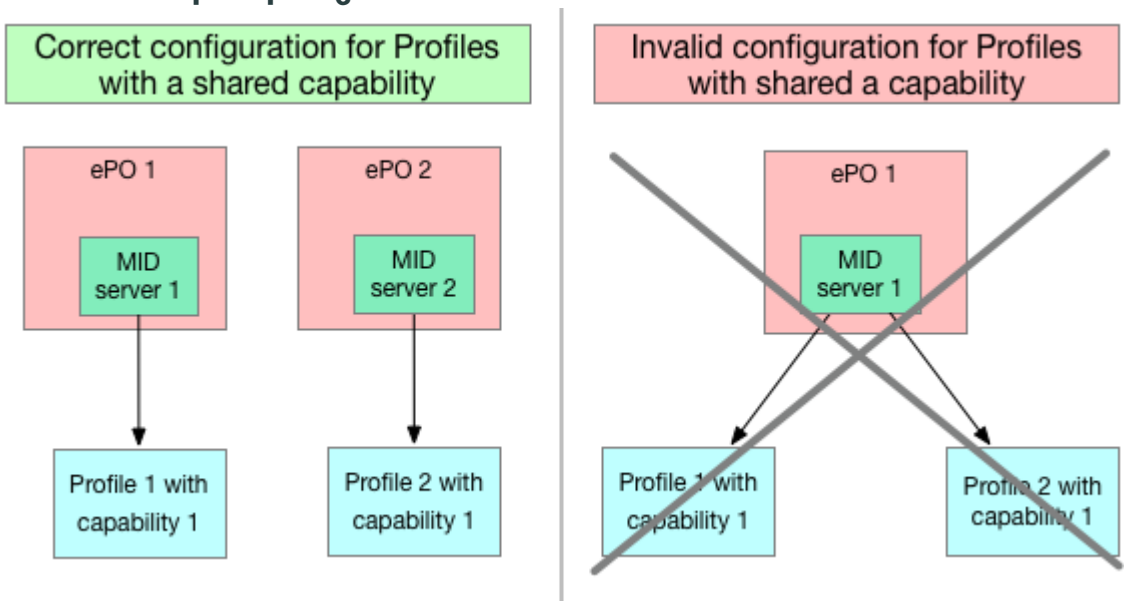
Pourquoi et quand exécuter cette tâche

L'intégration prend en charge plusieurs serveurs, cependant, pour éviter les conflits dans les profils qui partagent les mêmes conditions de déclenchement, vous ne pouvez pas partager une McAfee ePO option avec plusieurs profils qui utilisent le même McAfee ePO serveur. Par exemple, comme le montre la figure suivante, vous pouvez avoir l'option 1 dans plusieurs profils tant que chaque McAfee ePO serveur est mappé à un profil unique ayant l'option 1.

Traduction automatique

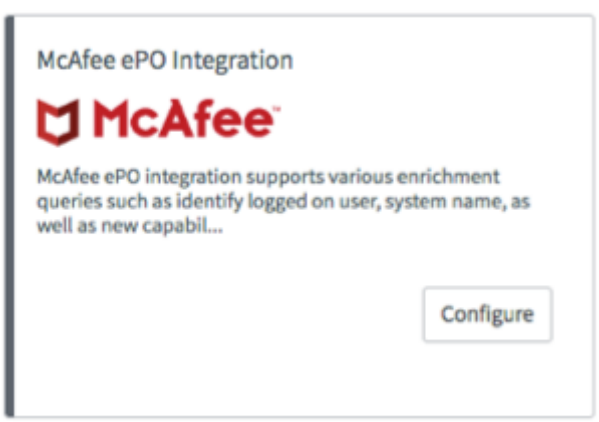
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Limitations du profil partagé McAfee



Procédure

1. Téléchargez le McAfee ePO pour Opérations de sécurité à partir de et ServiceNow Store installez-le.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette d'intégration McAfee ePOOpérations de sécurité , puis cliquez sur **Configurer**.



4. Remplissez les champs du formulaire.

Configuration de l'intégration de McAfee ePO

Champ	Description
Nom	Nom de l'intégration, par exemple `demo-1`.
Nom du serveur ePO	Nom du McAfee ePO serveur. Si vous utilisez un serveur, par exemple, `McAfee HQ` (`McAfee` Head Headquarterss). Ce nom est la façon dont le serveur et les informations d'identification associées sont reconnus.

Traduction automatique

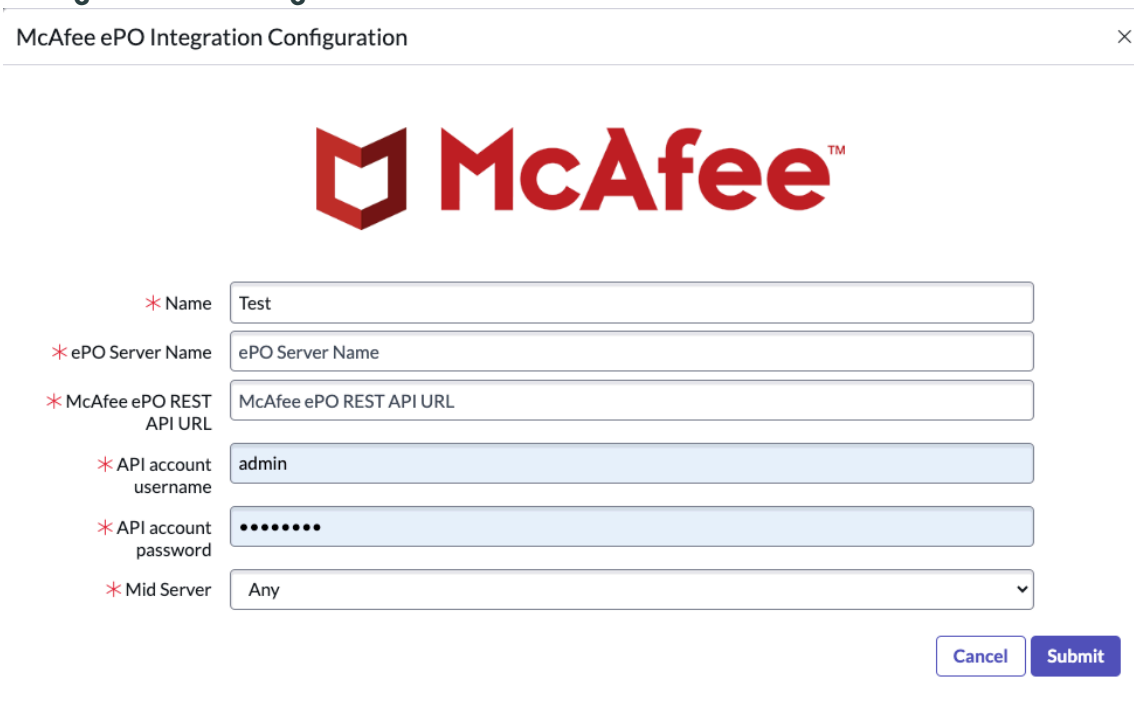
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si votre organisation a besoin de prendre en charge plusieurs serveurs, saisissez le nom de chaque serveur et répétez le processus.
URL REST API McAfee ePO	URL de base hébergeant l'API McAfee ePO REST. Entrez l'URL avec le protocole https://, par exemple, `https ://corp.epo_server :8443`.
Nom d'utilisateur du compte API	Nom d'utilisateur de compte unique, par exemple, `API ServiceNow`.
Mot de passe du compte API	Mot de passe unique pour le compte API.
Serveur MID	Sélectionnez le nom du Serveur MID que vous avez configuré lors de la configuration de votre ServiceNow AI Platform instance. Vous pouvez sélectionner un serveur MID spécifique dans la liste ou sélectionner **N'importe lequel** pour permettre la sélection automatique d'un serveur MID valide dans la liste pour cette intégration. **Remarque :** ○ Le serveur MID sélectionné pendant ce temps de configuration s'applique tout au long de cette intégration. ○ Seuls les serveurs MID actifs et validés sont affichés dans cette liste. Par défaut, la valeur est définie sur **Quelconque**. Un exemple de nom est `secops_local_midserver`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de l'intégration de McAfee ePO



5. Cliquez sur **Envoyer**.
   La liste des configurations de McAfee ePO s'affiche avec votre nouvel enregistrement de configuration. Vous avez terminé la configuration d'un McAfee ePO serveur.

   Remarque : Si votre organisation a besoin d'une prise en charge de plusieurs serveurs, répétez les étapes.

Modifier les balises de sécurité dans le ServiceNow AI Platform pour l'intégration McAfee ePO

Dans le cadre de la configuration de l'intégration, modifiez les noms de balises de sécurité que vous avez créés dans votre McAfee ePO console dans votre ServiceNow AI Platform instance. Modifiez les noms de balises dans votre ServiceNow AI Platform instance afin qu'ils correspondent aux noms des balises de votre McAfee ePO console.

Avant de commencer

Rôle requis : ServiceNow AI Platform administrateur d'incident de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Les noms de balises de sécurité dans votre McAfee ePO console pour les actions de lancement d'analyse anti-programme malveillant et d'isolement de l'hôte doivent correspondre aux noms de balises de sécurité dans les enregistrements pour ces options de votre ServiceNow AI Platform instance.

Avant de créer un profil d'aptitude pour exécuter vos options, affichez la liste des options disponibles McAfee ePO et modifiez les balises de sécurité dans votre ServiceNow AI Platform instance afin qu'elles correspondent aux noms de balises de sécurité de votre McAfee ePO console.

Pour plus d'informations sur la création des noms de balises de sécurité dans votre McAfee ePO console, reportez-vous à la section Configurer votre McAfee ePO console à intégrer Réponse aux incidents de sécurité à (SIR).

Traduction automatique

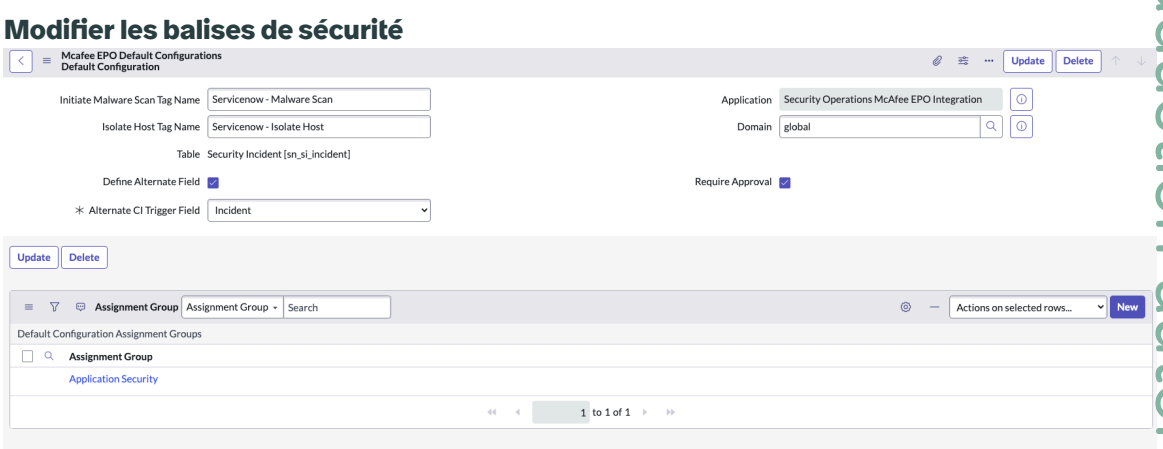
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intégration de McAfee ePO** > **Paramètres par défaut**.
2. Pour modifier le nom de la balise de sécurité de l'intégration McAfee ePO , cliquez sur **Configuration par défaut**.

   Remarque : Veillez à effectuer cette configuration après avoir installé l'intégration McAfee ePO .

3. Dans le champ Nom de balise Lancer l'analyse anti-programme malveillant, entrez le nom de la balise de sécurité que vous avez créée dans votre McAfee ePO console pour l'action Lancer l'analyse.
   Par exemple, ServiceNow - Analyse des programmes malveillants
4. Dans le champ Nom de la balise Isoler l'hôte, entrez le nom de la balise de sécurité que vous avez créée dans votre McAfee ePO console pour l'action Isoler l'hôte.
   Par exemple, ServiceNow - Isoler l'hôte
5. Si vous ne souhaitez pas utiliser le champ de déclenchement CI lors de la création de l'incident, cochez la case **Définir un autre champ** .
   Lorsque cette option est activée, la liste de choix du champ Déclenchement CI alternatif s'affiche.



6. Choisissez un autre champ dans la liste de choix pour vérifier vos critères de recherche de CI.
   Pour cet exemple, en tant qu'utilisateur disposant du rôle sn_si.admin, vous pensez que le champ CI ne sera pas renseigné sur l'incident de sécurité lors de la création de l'incident. Sinon, vous pensez que les informations CI pour un FQDN, un nom d'hôte ou une adresse IP seront renseignées dans le champ CI identifié de l'incident de sécurité, et vous sélectionnez le champ CI identifié comme alternative. Le CI identifié est sélectionné pour cet exemple, mais vous pouvez utiliser n'importe quel champ de l'incident de sécurité pour l'autre CI.
7. Dans le champ Domaine, sélectionnez un domaine ou un groupe pour cette configuration à l'aide de l'option de recherche.
   Par exemple, global.
8. Dans le champ Exiger l'approbation, cochez la case **Exiger l'approbation** si vous utilisez les options Isoler l'hôte et Supprimer l'isolement.

   Remarque : Les fonctionnalités Lancer l'analyse anti-programme malveillant, Répertorier les événements de menace et Obtenir les détails du système n'ont pas besoin d'approbation.

9. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le nom de la balise ePO est mis à jour et affiché dans la liste des configurations par défaut de McAfee ePO. Le nom de la balise de sécurité de l'action d'analyse des programmes malveillants dans votre ServiceNow AI Platform instance correspond au nom de l'analyse dans votre McAfee ePO console.

Vous avez modifié avec succès les noms de balises ePO pour l'analyse anti-programme malveillant et les options d'isolement de l'hôte dans votre ServiceNow AI Platform instance. L'étape suivante consiste à créer un profil pour vos capacités.

Information associée

Documentation produit McAfee

Créer un groupe d'approbation

Créez un groupe d'approbation pour l'intégration qui peut approuver les demandes d'isolement McAfee ePOOpérations de sécurité des ordinateurs hôtes et de restauration sur le réseau.

Avant de commencer

Vous ne pouvez pas réaffecter l'autorisation d'approbation à un groupe, sauf si un groupe d'approbation est disponible dans votre instance.

Remarque : L'option d'approbation dans le s'affiche uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte Configurer les paramètres .

Rôle requis : ServiceNow AI Platform® administrateur d'incidents de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Les demandes d'approbation soumises par l'analyste des incidents de sécurité pour isoler les ordinateurs hôtes et supprimer l'isolement sont affectées par défaut à l'utilisateur disposant du rôle sn_si.admin. En tant qu'utilisateur disposant de ce rôle, vous pouvez réaffecter cette autorisation d'approbation au cours de l'étape de configuration d'un profil. Avant de pouvoir réaffecter une autorité à un groupe d'approbation, un groupe d'approbation doit être disponible sur la liste Groupes de votre ServiceNow AI Platform instance.

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Groupes**.
2. Dans la liste des groupes, cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Groupe d'approbation

Champ	Description
Nom	Nom du groupe qui s'affiche lorsqu'une demande d'approbation est soumise, par exemple, Approbateurs Isolement de l'hôte McAfee.
E-mail de groupe	Liste de distribution d'e-mails de groupe ou l'adresse e-mail du point de contact, par exemple le gestionnaire de groupe, McAfeeapproval@servicenow.com
Responsable	Nom du gestionnaire de groupe. Cliquez sur l'icône de recherche pour afficher la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Parent	(Facultatif) Autre groupe dont ce groupe est membre, si ce groupe a un parent.
Description	Informations supplémentaires sur ce groupe.
Inclut des membres	Option permettant d'inclure des membres dans ce groupe.
Délégataire par défaut	Option permettant de choisir un utilisateur comme délégataire par défaut pour ce groupe. Utilisez l'option Rechercher pour ouvrir la liste des utilisateurs.
Rôles	Option permettant de sélectionner les rôles de ce groupe. Utilisez l'option Ajouter et supprimer pour ajouter et supprimer des rôles.
Type	Option permettant de choisir une catégorie pour ce groupe. Utilisez l'option Rechercher pour ouvrir la liste des types de groupes.
Fournisseurs	Option permettant de choisir un fournisseur pour ce groupe. Utilisez l'option de recherche pour ouvrir la liste des fournisseurs.

4. Cliquez sur **Envoyer**.
   Le nouveau groupe s'affiche dans la liste Groupes.

   Ce groupe est disponible pour traiter les demandes lorsque vous activez l'option **Exiger l'approbation** pendant la configuration de ce profil.

   Pour surveiller et traiter les demandes soumises par les utilisateurs disposant du rôle sn_si.analyst, chaque membre du groupe d'approbation accède à l'onglet **Mes approbations** dans le ServiceNow AI Platform.

McAfee ePO Profils d'aptitude d'intégration

En tant qu'utilisateur disposant du rôle d'administrateur d'incident de sécurité (sn_si.admin), vous créez des profils pour les options de McAfee ePO votre ServiceNow AI Platform® instance. Vous regroupez les requêtes ou les actions dans des profils et déterminez les McAfee ePO options que vous souhaitez exécuter lorsqu'un nouvel incident de sécurité est créé.

Profils d'aptitude

Vous créez des profils™ afin de pouvoir regrouper McAfee ePO des options et configurer les paramètres de ces options à partir de votre ServiceNow AI Platform® instance. Vous avez la possibilité de créer plusieurs profils pour ces options, ce qui vous permet de déterminer quelles actions ou requêtes sont invoquées lorsqu'un Réponse aux incidents de sécurité incident (SIR) est créé. Pour répondre aux besoins de votre organisation, vous pouvez créer un profil unique qui exécute des requêtes pour les détails du système, lance des analyses de programmes malveillants et isole les machines hôtes, par exemple, ou vous pouvez créer plusieurs profils, chacun avec sa propre McAfee ePO capacité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types de profils et capacités requises McAfee ePO

Objectif primaire de votre profil	Configurer les besoins	Fonctionnalités de McAfee ePO requises pour ce type de profil
Collecter les détails du système	Aucun	**Obtenir les détails de l'hôte**
Isoler un hôte	Vérifiez auprès de votre McAfee ePO administrateur que vous avez créé les balises de sécurité pour l'action Isoler l'hôte dans votre McAfee ePO console. Pour plus d'informations, consultez Configurer votre McAfee ePO console à intégrer Réponse aux incidents de sécurité à (SIR).	**Isoler l'hôte**
Analyser et rechercher les menaces sur votre hôte	Vérifiez auprès de votre McAfee ePO administrateur que vous avez créé les balises de sécurité pour l'action Lancer l'analyse anti-programme malveillant dans votre McAfee ePO console. Pour plus d'informations, consultez Configurer votre McAfee ePO console à intégrer Réponse aux incidents de sécurité à (SIR).	**Lancer l'analyse anti-programme malveillant** **Remarque :** Dans le cadre de l'analyse anti-programme malveillant, l'aptitude Répertorier les McAfee ePO événements de menace est invoquée automatiquement. Toutefois, vous n'êtes pas tenu d'ajouter l'option Répertorier les événements de menace au profil avec l'option d'analyse anti-programme malveillant. Les résultats de l'analyse anti-programme malveillant sont affichés dans l'onglet Détails de l'événement de menace de l'incident de sécurité.
Supprimer l'isolement d'un hôte	Vérifiez auprès de votre McAfee ePO administrateur que vous avez créé les balises de sécurité pour l'action Isoler l'hôte dans votre McAfee ePO console. Pour plus d'informations, consultez Configurer votre McAfee ePO console à intégrer Réponse aux incidents de sécurité à (SIR).	**Supprimer l'isolement**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types de profils et capacités requises McAfee ePO (suite)

Objectif primaire de votre profil	Configurer les besoins	Fonctionnalités de McAfee ePO requises pour ce type de profil
Collecter les données d'enrichissement des menaces.	Aucun	**Répertorier les événements de menace**

Créer un profil d'aptitude

Créez un profil et sélectionnez les McAfee ePO options que vous souhaitez que le profil exécute.

Avant de commencer

Rôle requis : ServiceNow AI Platform® administrateur d'incidents de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Pour cette étape de la configuration, vous devez créer un profil pour les McAfee ePO options. Lorsque vous créez des profils, tenez compte de l'intention du profil avant d'y ajouter McAfee ePO des options. Reportez-vous à la table suivante lorsque vous créez des profils.

Le tableau suivant répertorie les options que vous devez ajouter à un profil si vous souhaitez que celui-ci effectue certaines requêtes ou actions. Créez un profil unique qui exécute des requêtes de détails sur l'hôte, lance des analyses anti-programmes malveillants, supprime l'isolement et isole les ordinateurs hôtes, ou crée plusieurs profils, chacun ayant sa propre capacité unique.

Procédure

1. Accédez à la **Intégration de McAfee ePO** > **Profils de fonctionnalités de McAfee ePO**.
   La liste des profils d'aptitude McAfee ePO s'affiche.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom du profil d'aptitude McAfee ePO . Ce nom vous permet d'identifier le type de profil et de le décrire. Un exemple pour un profil qui exécute des requêtes est les détails de l'hôte et de la menace. Ce nom est également le nom de la balise de sécurité pour ce profil par défaut.
Description	Informations supplémentaires sur le profil qui décrivent plus en détail les activités du profil. Un exemple de description pour un profil qui exécute des requêtes est Enrichissement des menaces pour les détails du système et une liste des événements de menace. Voici un exemple de description d'un profil qui exécute des actions : Isoler l'ordinateur hôte.
Source	Nom du McAfee ePO serveur. Seuls les serveurs configurés sont disponibles dans la liste de choix.
Aptitude de McAfee ePO	Aptitudes du McAfee ePO profil. McAfee ePO prend en charge les fonctionnalités suivantes :

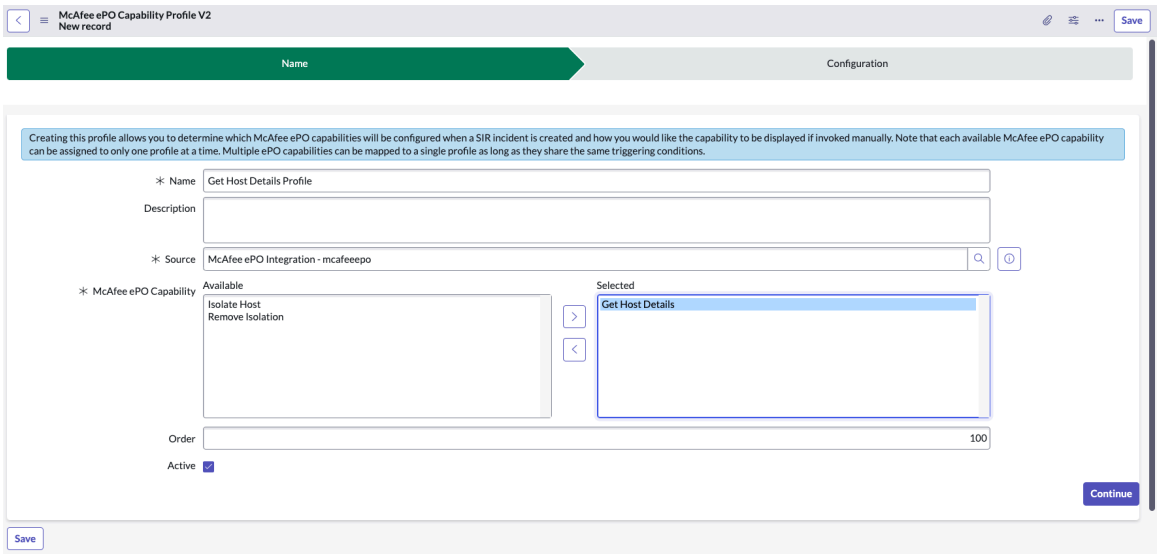
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Obtenir les détails de l'hôte ○ Isoler le profil de l'hôte ○ Lancer l'analyse anti-programme mal–veillant ○ Supprimer l'isolement ○ Répertorier les événements de menace Sélectionnez les options souhaitées pour ce profil dans la colonne **Disponible** et déplacez-les vers la colonne **Sélectionné** . Vous ne pouvez pas ajouter Obtenir les détails de l'hôte, Lancer une analyse anti-programme malveillant et Répertorier les événements de menace dans le même profil, et vous ne pouvez pas ajouter Supprimer l'isolement et Isoler l'hôte sur le même profil.
Ordre	Priorité du workflow. La valeur par défaut est 100. La valeur de ce champ indique l'ordre dans lequel les workflows sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400.
Actif	La case à cocher est sélectionnée par défaut pour indiquer que le profil est actif. Lorsque cette option est sélectionnée, le profil est actif et se déclenche automatiquement lorsqu'un incident de sécurité correspondant aux conditions de filtrage que vous spécifiez au cours de l'étape de configuration est créé. Lorsqu'il est inactif, le profil ne s'exécute pas et il n'est pas disponible pour être appelé à partir d'une liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Pour enregistrer et valider le profil, cliquez sur **Continuer**.
   Si la validation réussit, la page se recharge et le formulaire **de configuration** s'affiche.

Que faire ensuite

L'étape suivante consiste à configurer votre profil. Avant de configurer les paramètres du profil, vous pouvez passer en revue les concepts de configuration des profils et des conditions de déclenchement. Voir Configurer votre McAfee ePO console à intégrer Réponse aux incidents de sécurité à (SIR) et Définir des conditions de déclenchement avec un champ d'élément de configuration (CI) pour plus d'informations.

Définir des conditions de déclenchement avec un champ d'élément de configuration (CI)

Après avoir créé un profil et sélectionné les McAfee ePO options que vous souhaitez que le profil exécute, vous configurez les paramètres du profil afin qu'il ne s'exécute que lorsqu'un ensemble de conditions spécifiques est rempli.

Vous pouvez définir ces conditions de déclenchement afin que le profil s'exécute automatiquement en fonction des valeurs de champ par défaut qui sont mises en correspondance sur un ServiceNow AI Platform® Réponse aux incidents de sécurité incident de sécurité. Vous pouvez également configurer un profil pour qu'il recherche des correspondances avec les valeurs de champ que vous identifiez spécifiquement sur l'incident de sécurité.

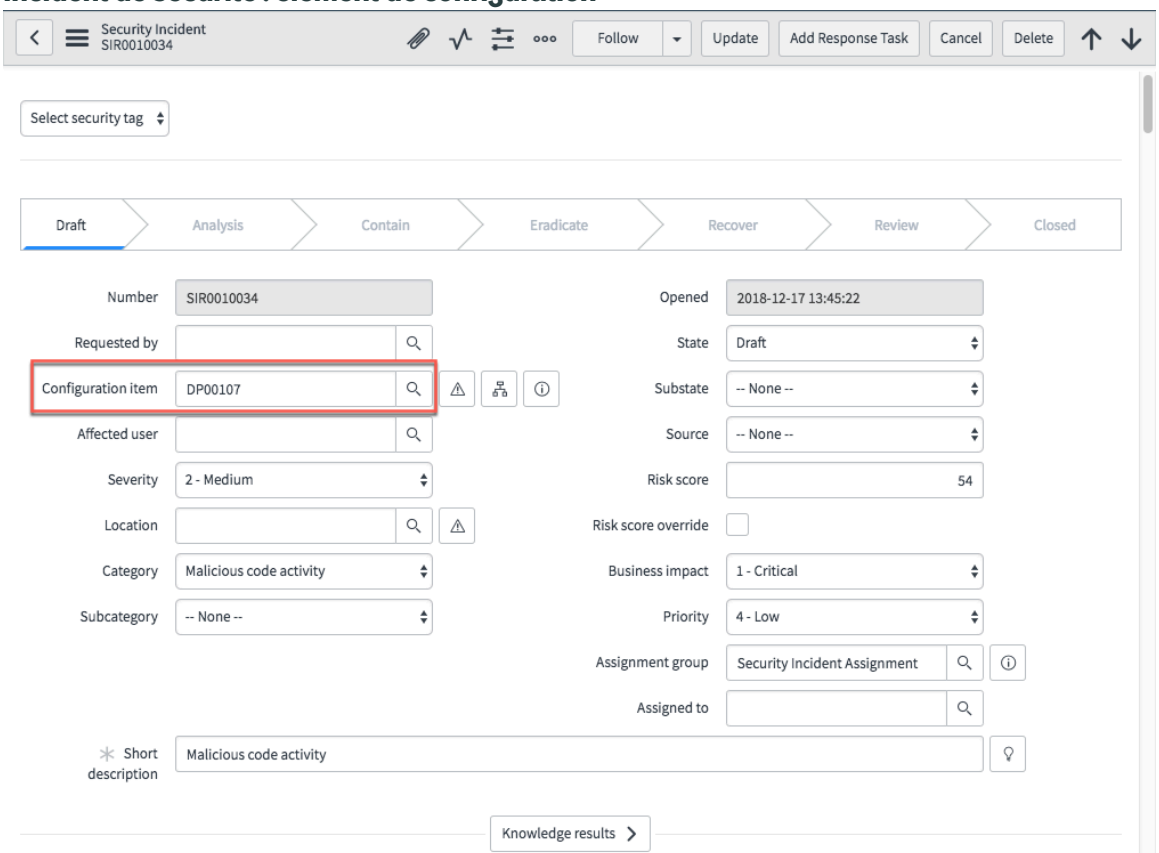
L'une des clés de la fonctionnalité de l'intégration et du fonctionnement d'un profil est le champ Élément de configuration (CI) sur l'incident ServiceNow AI Platform® Réponse aux incidents de sécurité de sécurité (SIR). La valeur de ce champ est la valeur principale pour un incident de sécurité. Cette valeur est utilisée pour faire correspondre les ID de vos actifs avec les informations stockées dans la ServiceNow AI Platform® base de données. Lorsqu'un SIR incident de sécurité est créé par un événement de sécurité et qu'un profil est activé, vos actifs sont analysés à la recherche d'une valeur correspondante pour un nom de domaine complet (FQDN), un nom d'hôte ou une adresse IP en fonction de la valeur du champ Élément de configuration.

Dans l'idéal, une valeur correspondante est trouvée dans la base de données, et les données peuvent être collectées à partir de la McAfee ePO console pour l'actif correspondant, extraites dans votre ServiceNow AI Platform® instance et affichées dans les listes connexes d'un incident de sécurité. La figure suivante illustre un exemple de champ Élément de configuration renseigné avec un nom d'hôte sur un SIR incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incident de sécurité : élément de configuration



Si le champ Élément de configuration (CI) de l'incident de sécurité n'est pas renseigné, ou si une correspondance ne peut être trouvée pour un nom de domaine complet, un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour afficher toutes les données d'enrichissement de CI correspondantes trouvées lors de l'analyse de vos actifs.

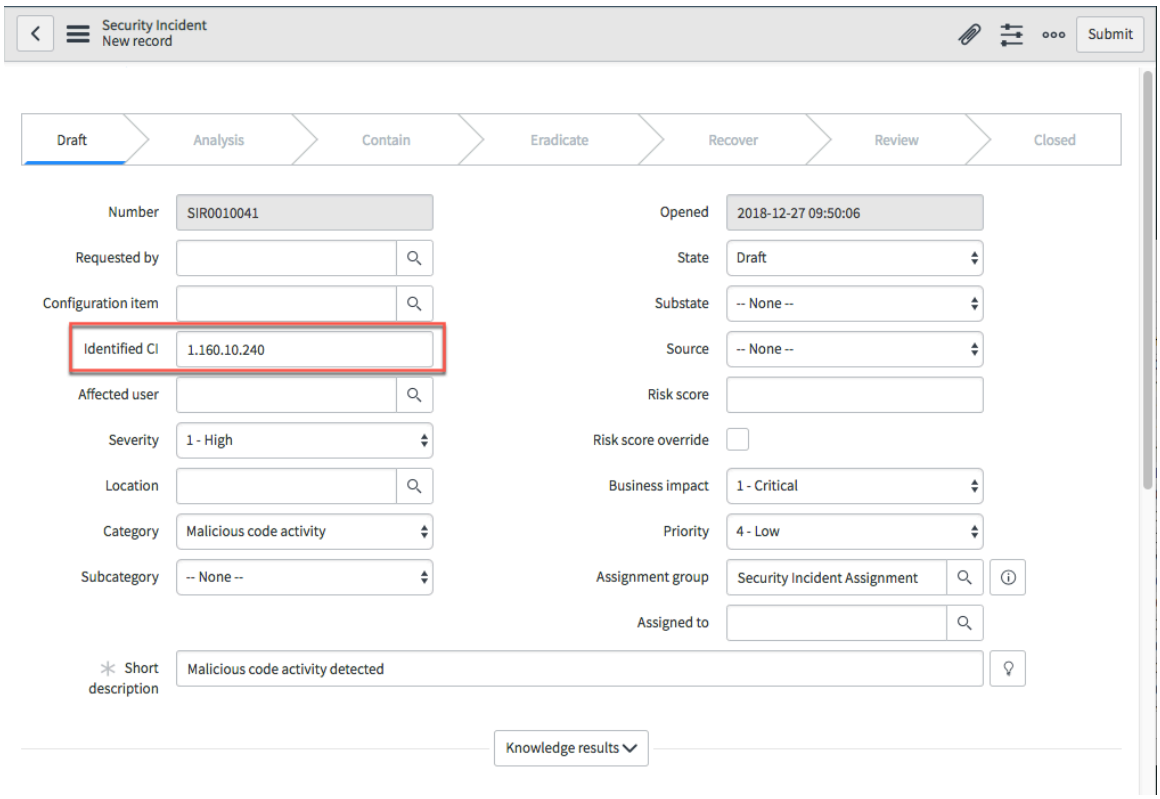
Au cours de l'étape de configuration du profil, vous pouvez sélectionner un autre champ de déclenchement CI pour l'identification du point de terminaison afin de vous assurer que les données d'enrichissement CI de la McAfee ePO recherche sont renseignées sur l'incident de sécurité associé. Vous pouvez sélectionner n'importe quel champ de l'incident de sécurité comme champ de déclenchement CI alternatif, y compris les champs personnalisés que vous créez. En sélectionnant cet autre champ CI comme sauvegarde, vous vous assurez que vos profils s'exécutent même si le champ CI n'est pas renseigné sur l'incident de sécurité associé lors de la création de l'incident.

Par exemple, en tant qu'analyste du centre des opérations de sécurité (SOC), vous créez un champ personnalisé pour un incident de sécurité appelé Adresse IP sur mon incident de sécurité. Si vous pensez que la valeur de ce champ personnalisé ne sera pas affichée dans le champ Élément de configuration de l'incident de sécurité lors de la création de l'incident, vous pouvez configurer le profil pour qu'il recherche cette adresse IP. En cas de correspondance, l'adresse IP est affichée sur l'incident de sécurité dans le champ de votre choix. Dans la figure suivante, le champ CI identifié est sélectionné comme champ alternatif pour l'adresse IP pour cet exemple.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incident de sécurité : CI identifié

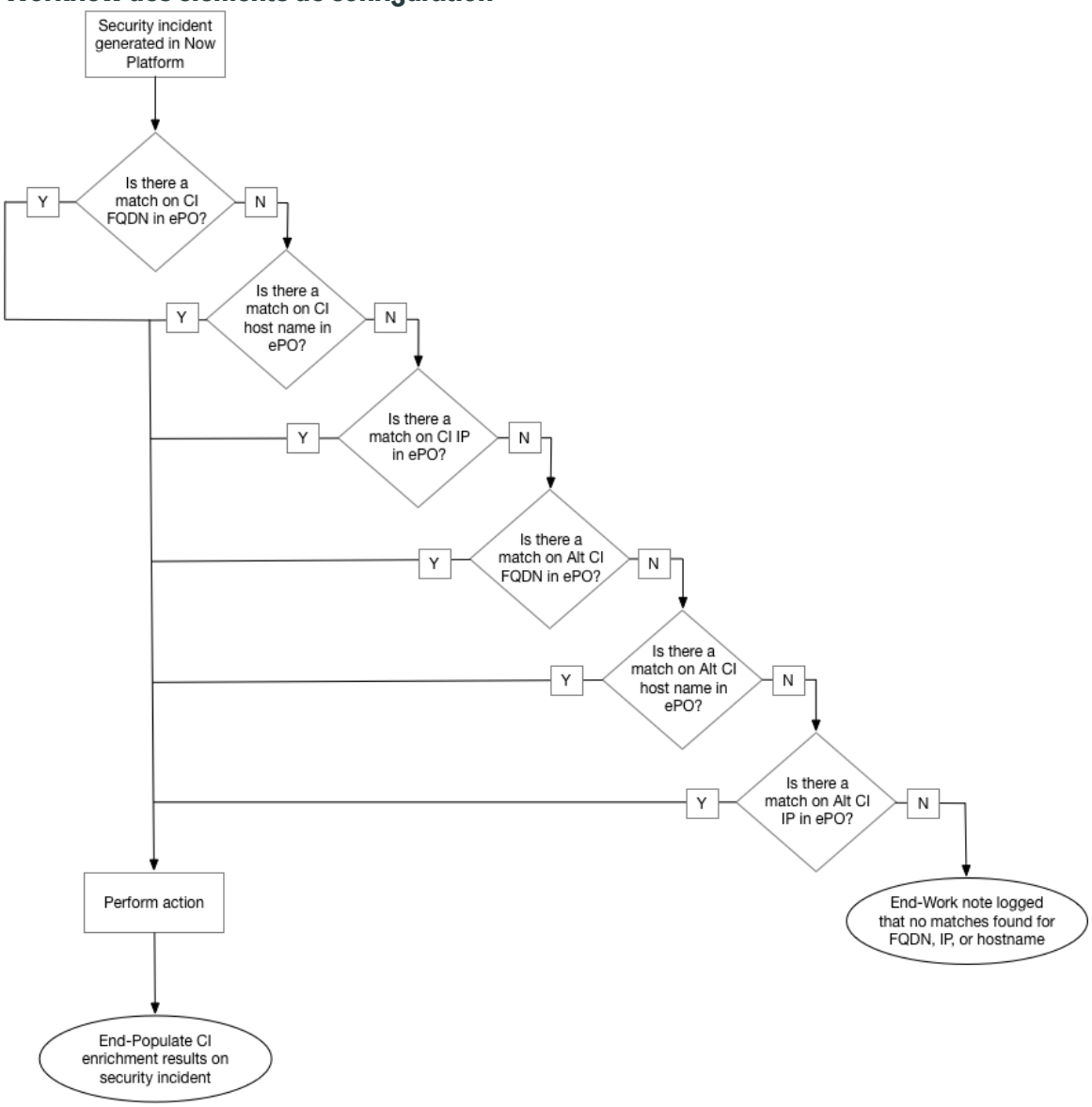


La figure suivante illustre comment la première recherche du workflow recherche des correspondances pour les éléments de configuration. Si le champ de déclenchement CI alternatif est activé, la deuxième recherche recherche les correspondances entre les valeurs alternatives.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow des éléments de configuration



Si aucun ID correspondant n'est trouvé pour le champ CI ou l'autre champ CI, une note de travail est journalisée et un message s'affiche sur l'incident de sécurité. Lorsqu'aucune correspondance n'est trouvée, aucune donnée d'enrichissement n'est renseignée sur les incidents de sécurité liés à l'événement.

Vous activez le champ de déclenchement CI alternatif et sélectionnez le champ pour lequel vous souhaitez afficher l'ID correspondant pendant l'étape de configuration d'un profil. Cette étape d'activation du champ CI alternatif est décrite ainsi que les autres exigences de configuration de profil dans Configurer les paramètres.

Configurer les paramètres

Une fois que vous avez créé un profil et sélectionné les McAfee ePO options que vous souhaitez que le profil exécute, configurez les paramètres afin que le profil ne soit appelé que dans les conditions spécifiques que vous définissez.

Configuration d'un profil

Dans cette étape, vous configurez un profil d'aptitude afin qu'il ne s'exécute que lorsque les conditions que vous spécifiez sont remplies. Vous définissez les conditions des incidents

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de sécurité qui déclenchent automatiquement les McAfee ePO options que vous avez sélectionnées pour le profil. Vous pouvez également sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI) et définir des conditions de filtrage afin que seuls les incidents de sécurité liés à votre événement déclencheur lancent automatiquement le profil. L'étape de configuration inclut les paramètres suivants sur le formulaire de configuration du profil.

Champ de déclenchement d'un autre élément de configuration (CI)

Si le champ Élément de configuration (CI) de l'incident de sécurité (SIR) n'est ServiceNow AI Platform® Réponse aux incidents de sécurité pas renseigné avec une valeur, ou si une correspondance est introuvable dans la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour afficher toutes les données d'enrichissement de CI correspondantes trouvées lors de l'analyse de vos actifs. Pour plus d'informations sur les champs Élément de configuration et Autre élément de configuration d'un incident de sécurité, reportez-vous à la section Définir des conditions de déclenchement avec un champ d'élément de configuration (CI).

Balises de sécurité

Pour vous aider à suivre l'état des machines hôtes isolées et le lancement des analyses de logiciels malveillants, une fonction de balisage facultative est disponible. Par défaut, cette option est désactivée dans le formulaire de configuration des profils. Si cette option est activée pendant l'étape de configuration, les noms des balises de sécurité s'affichent dans le formulaire de configuration. Il s'agit des noms des balises affichées sur les incidents de sécurité associés. Ces balises vous informent lorsqu'une action d'isolement d'hôte est lancée avec succès et lorsqu'elle est approuvée. Une fois qu'un hôte est renvoyé avec succès sur le réseau, la balise de sécurité est automatiquement supprimée de l'incident de sécurité. Pour les analyses de programmes malveillants, une balise est affichée sur l'incident de sécurité connexe lorsqu'une analyse est planifiée. Une fois l'analyse terminée, la balise planifiée est automatiquement remplacée par une balise qui indique que l'analyse est terminée avec succès.

Déclenchement automatique basé sur l'incident

Lorsque l'option Déclenchement automatique basé sur l'incident est activée, le générateur de conditions de filtre est disponible et vous devez définir des conditions de filtrage qui spécifient quand le profil s'exécute automatiquement. Un filtre commun est Catégorie est Activité de code malveillant™ et L'impact sur l'activité est 1 - Critique™. Avec ces filtres, seuls les incidents de sécurité liés à un code malveillant et ayant un impact critique sur l'entreprise lancent le profil. L'utilisation de l'option de déclenchement automatique peut réduire le nombre d'incidents de sécurité qui appellent automatiquement le profil.

Approbations

Si votre organisation souhaite un niveau de contrôle supplémentaire sur des actions telles que l'isolement des ordinateurs hôtes et le lancement d'analyses anti-programmes malveillants, vous pouvez activer l'option Exiger l'approbation pendant l'étape de configuration d'un profil.

Par exemple, si les fonctionnalités d'approbation et de balisage sont activées pour un profil, après qu'une demande d'isolement d'un ordinateur hôte ou de renvoi au réseau est soumise pour approbation, l'incident de sécurité associé est balisé automatiquement pour que l'action soit lancée. Les demandes sont envoyées pour approbation à un utilisateur disposant du rôle sn_si.admin par défaut, mais cette approbation peut être réaffectée à une autre personne ou à un groupe d'approbation pour répondre aux besoins de votre

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

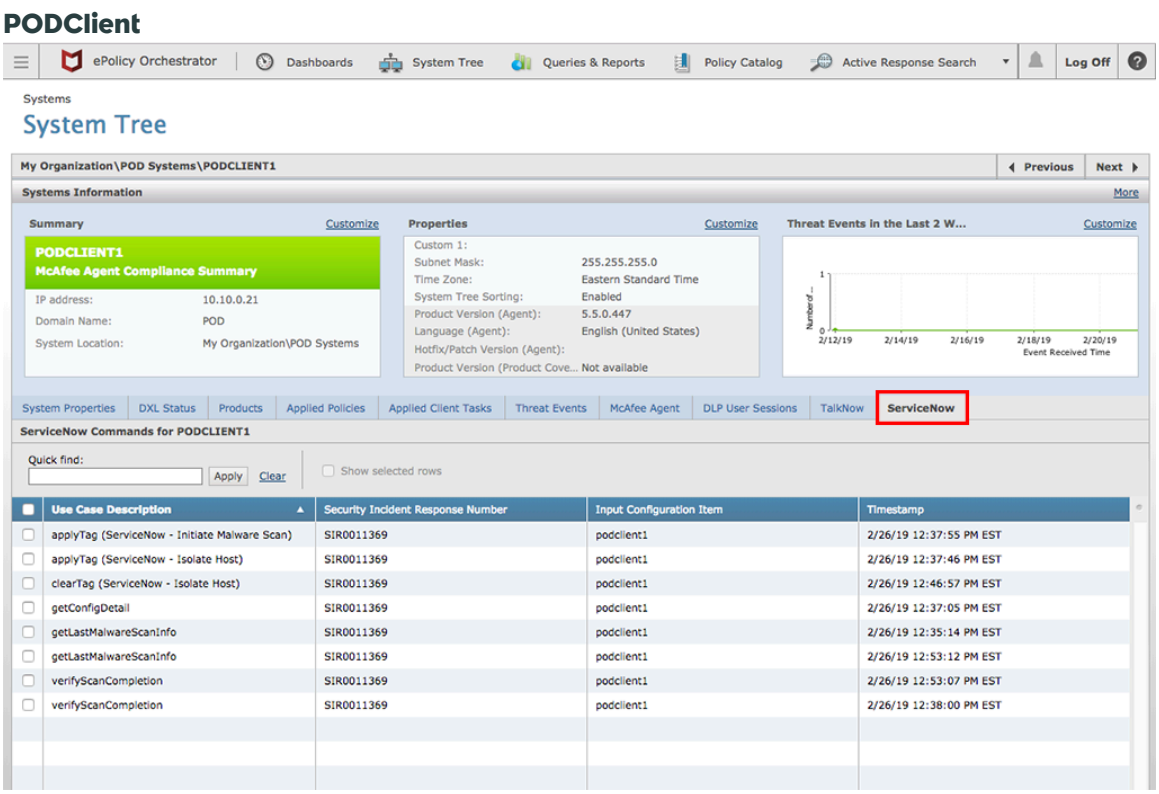
organisation. Les approbateurs traitent les demandes dans **Mes approbations** dans leurs ServiceNow AI Platform® instances. Les balises de sécurité sont affichées sur les incidents de sécurité associés. Toutes les activités du workflow sont également enregistrées dans des notes de travail pour créer une piste d'audit.

ServiceNow Journal d'audit dans la McAfee ePO console

Dans la version 5.10.0 de McAfee ePO, un ServiceNow onglet s'affiche avec un journal des commandes lancées à partir de votre ServiceNow AI Platform® instance. Une fois qu'une action ou une requête est invoquée à partir d'un profil de votre ServiceNow AI Platform® instance sur un ordinateur hôte (point de terminaison) dans la McAfee ePO console, un journal d'audit des ServiceNow commandes est créé dans la McAfee ePO console. Ce journal s'affiche dans l'arborescence système de la McAfee ePO console et vous aide à auditer les heures des commandes envoyées à des points de terminaison spécifiques. Pour afficher les événements consignés ServiceNow sur des ordinateurs spécifiques dans une McAfee ePO console, procédez comme suit.

1. Accédez à l'arborescence système dans votre McAfee ePO console et localisez l'onglet ServiceNow .
2. Cliquez sur l'onglet pour ouvrir une liste d'ordinateurs hôtes.
3. Dans la colonne Nom, cliquez sur un nom d'hôte pour ouvrir le journal d'audit.

Dans l'image suivante, un exemple de journal pour un hôte (PODCLIENT1) s'affiche.



Les événements initiés à partir des profils de votre ServiceNow AI Platform® instance sont enregistrés et affichés dans le journal. Vérifiez en vérifiant l'état de l'ordinateur hôte que les événements répertoriés dans le journal sont exécutés avec succès sur l'hôte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemples de profils

Les rubriques suivantes comprennent des exemples sur la façon de configurer des profils et de tester des incidents de sécurité. Ces exemples incluent des profils pour toutes les McAfee ePO options disponibles pour cette intégration.

Configurer les profils et les incidents de sécurité pour les requêtes d'enrichissement du système

Configurez les paramètres de votre profil de sorte que le profil ne se déclenche que dans les conditions que vous définissez.

Avant de commencer

Rôle requis : ServiceNow AI Platform® administrateur d'incident de sécurité (sn_si.admin)

Pourquoi et quand exécuter cette tâche

Définissez les conditions qui déclenchent automatiquement les McAfee ePO options que vous avez sélectionnées pour le profil. Vous pouvez également sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI). Dans cet autre champ, vous pouvez définir des conditions de filtrage afin que seuls les incidents de sécurité liés à votre événement déclencheur déclenchent automatiquement le profil.

Procédure

1. Si la page Configuration ne s'affiche pas, cliquez sur **Configuration** dans la barre de progression.
2. Renseignez les champs du formulaire

Option	Description
Activer un champ de déclenchement CI alternatif	Champ de déclenchement d'autre élément de configuration (CI). La valeur par défaut est effacée. Lorsque cette case n'est pas cochée et que l'option de champ de déclenchement CI alternatif est désactivée, aucun autre champ pour le CI n'est identifié. Si elle est désactivée, une valeur du champ CI doit être renseignée sur un SIR incident de sécurité, et la valeur du champ doit être reconnue par la McAfee ePO console avant que le profil ne collecte les données d'enrichissement. Cochez cette case si vous pensez que le champ CI ne sera pas renseigné lors de la création de l'incident, mais que les informations CI seront renseignées dans un autre champ de l'incident de sécurité. Lorsque cette option est activée, la liste de choix du champ Déclenchement CI alternatif s'affiche. Choisissez un autre champ dans la liste de choix pour vérifier vos critères de recherche de CI. Pour plus d'informations sur le champ de déclenchement CI alternatif, reportez-vous à la section Définir des conditions de déclenche-

Traduction automatique

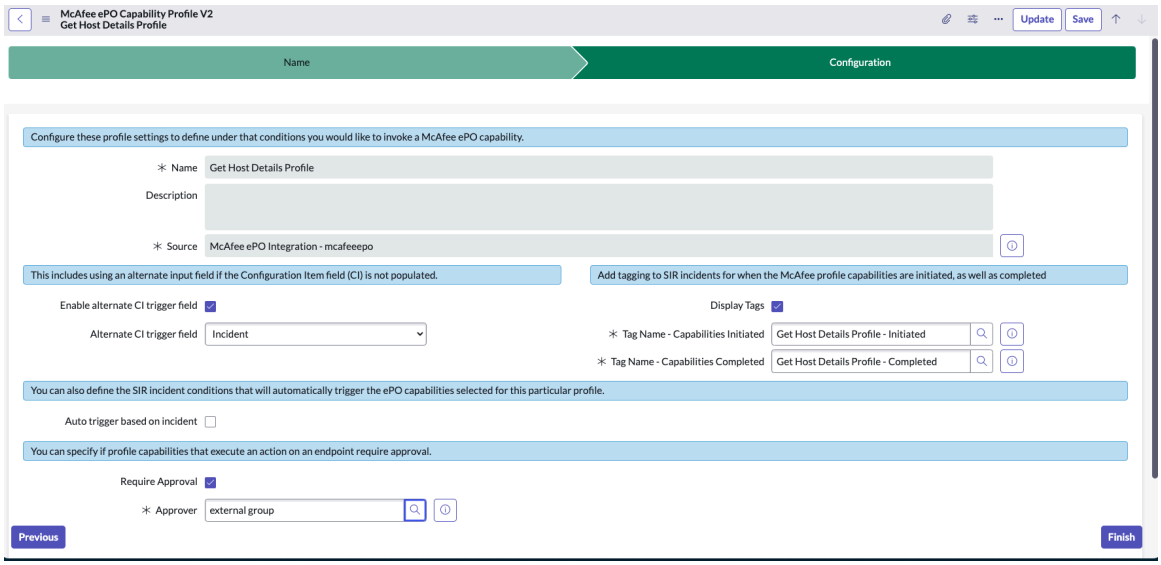
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	ment avec un champ d'élément de configuration (CI).
Balises d'affichage	Des balises de sécurité sont affichées sur les incidents de sécurité. La valeur par défaut est effacée. Lorsque cette case est décochée et que l'option de balisage est désactivée, aucun nom de balise de sécurité n'est affiché sur le formulaire de configuration et les balises ne sont pas affichées sur les incidents de sécurité associés. Pour cet exemple, l'option des balises de sécurité est désactivée.
Déclenchement automatique basé sur l'incident	Conditions de filtre. La valeur par défaut est effacée. Lorsque la case est décochée et que l'option est désactivée, le profil doit être invoqué manuellement à partir d'un incident de sécurité. Lorsque cette option est activée, le générateur de conditions de filtre s'affiche. Vous devez définir les conditions de filtrage pour spécifier quand le profil s'exécute automatiquement lors de la création de l'incident. Un exemple courant de filtre pour un profil qui exécute des requêtes d'enrichissement est la catégorie est Activité de code malveillant et Impact sur l'activité est 1-Critique. Ces conditions de filtre vous aident à localiser les incidents liés à des types spécifiques d'événements de sécurité et vous aident à limiter le nombre d'incidents de sécurité que vous devez examiner. Ces paramètres de filtre restent enregistrés jusqu'à ce que vous les modifiiez et vous pouvez les modifier pendant l'étape d'aperçu et de test de l'incident de la configuration.
Exiger l'approbation	Option d'approbation de demande. La valeur par défaut est effacée. Cette option d'approbation est disponible pour tous les profils. Habituellement, les approbations sont utilisées pour les options qui appellent des actions telles que l'isolement de l'hôte et les analyses de programmes malveillants. Lorsque la case est décochée et que cette option est désactivée, aucune demande d'approbation n'est soumise. Pour cet exemple, aucune autorisation préalable

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	n’est requise pour les requêtes d’enrichis–sement du système.



3. Pour activer l’option de champ CI alternatif et définir les conditions de filtrage qui appellent automatiquement ce profil, procédez comme suit.

a. Cochez la **case du champ Activer un autre déclencheur de CI** .
Le champ Autre déclencheur CI s’affiche. Pour cet exemple, en tant qu’utilisateur disposant du rôle sn_si.admin, vous pensez que le champ CI ne sera pas renseigné sur l’incident de sécurité lors de la création de l’incident. Sinon, vous pensez que les informations CI pour un FQDN, un nom d’hôte ou une adresse IP seront renseignées dans le champ CI identifié de l’incident de sécurité, et vous sélectionnez le champ CI identifié comme alternative. Le CI identifié est sélectionné pour cet exemple, mais vous pouvez utiliser n’importe quel champ de l’incident de sécurité pour l’autre CI.

b. Dans la liste de choix du champ **Autre déclencheur CI** qui s’affiche, sélectionnez le champ **CI identifié** .

Tous les champs disponibles sur l’incident de sécurité sont affichés dans la liste, y compris les champs personnalisés. Dans le champ Déclenchement CI alternatif, CI identifié s’affiche.

Lorsque ce profil est invoqué et que le champ CI n’est pas renseigné sur l’incident de sécurité associé lors du déclenchement de l’événement initial, le profil utilise alternativement la valeur du champ CI identifié dans la recherche.

c. Cochez la case **Déclencher automatiquement en fonction de l’incident** .
Le générateur de conditions de filtre s’affiche. Cette option permet de définir les conditions de filtrage et de spécifier quand le profil est appelé automatiquement lors de la création d’un incident de sécurité.

d. Définissez les conditions d’incident SIR qui déclencheront automatiquement les options ePO sélectionnées pour ce profil particulier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Si les options du profil qui exécutent une action sur un point de terminaison nécessitent une approbation, cochez la case **Exiger l'approbation** .

f. Sélectionnez une approbation à l'aide de l'icône de recherche.

4. Cliquez sur **Terminer**.
   Vous avez correctement configuré le profil afin qu'il se déclenche automatiquement lors de la création de l'incident, et un autre champ est utilisé pour renseigner les résultats CI correspondants.

Configurer un profil pour lancer l'analyse anti-programme malveillant

Après avoir créé un profil avec l'aptitude Lancer l'analyse anti-programme malveillant et toutes les autres McAfee ePO options que vous souhaitez que le profil exécute, configurez les paramètres du profil afin qu'il soit appelé dans les conditions spécifiques que vous définissez.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
En tant qu'utilisateur disposant du rôle sn_si.admin, configurez le profil afin qu'il planifie une analyse uniquement lorsque les conditions que vous spécifiez sont remplies pour ServiceNow AI Platform Réponse aux incidents de sécurité les incidents de sécurité (SIR). Vous définissez les conditions des incidents de sécurité qui déclenchent l'analyse. Toutes les autres McAfee ePO options que vous sélectionnez pour le profil partagent les conditions de déclenchement. Vous pouvez sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI) et définir des conditions de filtrage. Vous préférez peut-être définir un filtrage afin que seuls les SIR incidents de sécurité liés à votre événement déclencheur invoquent automatiquement le profil.

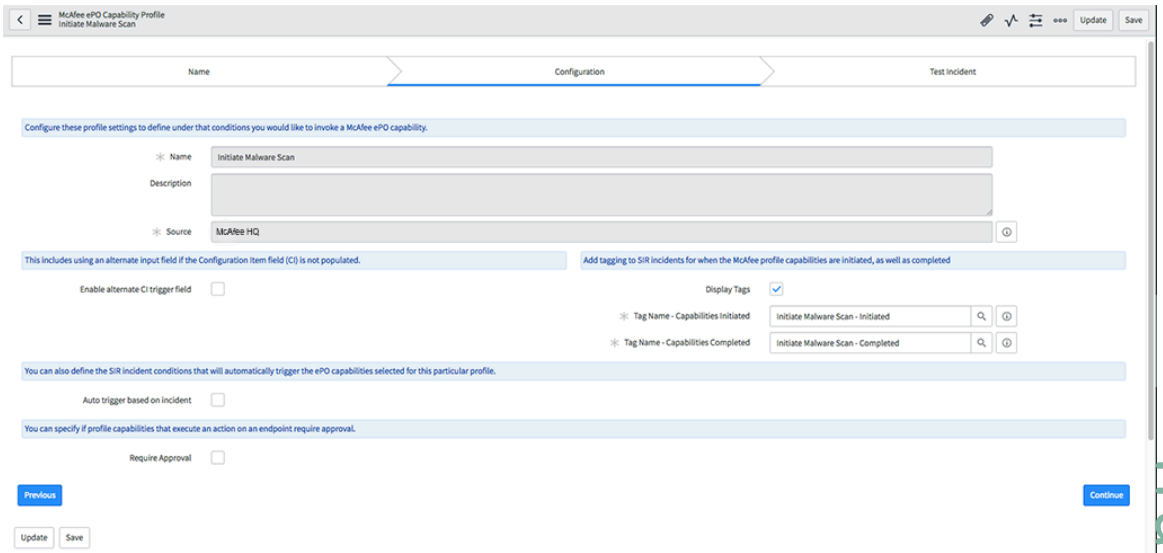
Comme pour l'action Isoler l'hôte, vous pouvez lancer une analyse à la demande directement à partir d'un SIR incident de sécurité. Pour plus d'informations sur le lancement manuel d'une analyse, reportez-vous à la section Déclencher McAfee ePO manuellement le profil à partir d'un incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si la page Configuration ne s’affiche pas, cliquez sur **Configuration** dans la barre de progression.



Le formulaire Configuration s’affiche.

2. Remplissez le formulaire.

Option	Description
Activer un champ de déclenchement CI alternatif	Champ de déclenchement d’autre élément de configuration (CI). Désactivé par défaut. Pour cet exemple, la case n’est pas cochée. Lorsque cette case n’est pas cochée et que l’option de champ de déclenchement CI alternatif est désactivée, aucun autre champ pour le CI n’est identifié. Si elle est désactivée, une valeur du champ CI doit être renseignée sur un SIR incident de sécurité, et la valeur du champ doit être reconnue par la McAfee ePO console avant l’exécution du profil. Lorsque cette case est cochée et que cette option est activée, la liste de choix du champ Autre déclencheur CI s’affiche. Choisissez n’importe quel champ de cette liste comme champ alternatif pour le CI. Pour plus d’informations sur le champ de déclenchement CI alternatif, reportez-vous aux sections Définir des conditions de déclenchement avec un champ d’élément de configuration (CI) et Créer un profil d’aptitude.
Balises d'affichage	Balises de sécurité sur les incidents de sécurité. Désactivé par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Lorsque cette case est décochée et que l'option de balisage est désactivée, aucun nom de balise de sécurité n'est affiché sur l'incident de sécurité. Laissez cette case décochée si vous ne souhaitez pas que des balises de sécurité s'affichent sur les incidents de sécurité associés. Lorsque la case est cochée et que l'option de balisage est activée, les noms des balises de sécurité s'affichent sur le formulaire de configuration. Il s'agit des noms de balises affichés sur les incidents de sécurité associés. Les analyses anti-programmes malveillants peuvent être programmées en dehors des heures de travail et prendre du temps. Au-dessus de l'incident de sécurité, lorsque le balisage est activé, une balise de sécurité s'affiche pour indiquer que l'analyse est planifiée. Une fois l'analyse terminée, la balise programmée est automatiquement remplacée par une balise qui indique que l'analyse est terminée avec succès. Les noms et les couleurs des balises peuvent être modifiés. Pour plus d'informations, consultez Modifier les balises de sécurité dans le ServiceNow AI Platform pour l'intégration McAfee ePO.
Déclenchement automatique basé sur l'incident	Conditions de filtre. Désactivé par défaut. Lorsque la case est décochée et que l'option est désactivée, le profil ne lance pas automatiquement une analyse anti-programmes malveillants. Le profil doit être lancé manuellement à partir d'un incident de sécurité. Lorsque la case à cocher est sélectionnée et que l'option de déclenchement automatique est activée, le générateur de conditions de filtre s'affiche sur le formulaire. Vous devez définir les conditions de filtrage pour spécifier quand le profil s'exécute automatiquement lors de la création de l'incident. Pour cet exemple, les filtres pour `la catégorie est Activité du code malveillant` et `Impact sur l'activité est 1 - Critique` sont utilisés. Pour plus d'informations sur le créa-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	teur de conditions de filtre, reportez-vous à la section Créer un profil d'aptitude.
Exiger l'approbation	Requiert une approbation avant de lancer l'analyse. Désactivé par défaut. Lorsque la case est décochée et que l'option d'approbation est désactivée, un utilisateur disposant du rôle sn_si.analyst lance une analyse anti-programme malveillant sans demander d'approbation préalable. Cochez cette case et activez cette option si vous souhaitez qu'un utilisateur disposant du rôle sn_si.analyst demande l'approbation avant de lancer une analyse anti-programme malveillant.

Pour cet exemple, les options d'approbation et de balisage sont activées pour le profil. Pour plus d'informations sur la configuration du champ Activer un autre champ de déclenchement CI et des options Déclenchement automatique en fonction de l'incident , reportez-vous à la section Configurer les profils et les incidents de sécurité pour les requêtes d'enrichissement du système.

3. Choisissez une option pour continuer.

Option	Description
Précédent	Revenez à l'étape Nom si vous souhaitez modifier le profil.
Enregistrer	Enregistrez vos changements et restez sur cette page. Pour enregistrer vos modifications, dans la bannière grise en haut de l'écran, cliquez avec le bouton droit de la souris. Dans le menu qui s'affiche, cliquez sur **Enregistrer**.
Continuer ou sélectionner Tester l'incident dans la barre de progression	Passez à l'étape Tester l'incident et l'étape d'aperçu. Si vous quittez la page sans enregistrer au préalable vos modifications, vos modifications ne sont pas enregistrées.
Supprimer	Supprimez ce profil de la liste des profils d'aptitude McAfee ePO .

Vous avez correctement configuré le profil afin qu'une analyse anti-programme malveillant se déclenche automatiquement lors de la création de l'incident. Un autre champ CI est utilisé pour renseigner les résultats CI correspondants de l'analyse. L'étape suivante consiste à prévisualiser et tester les incidents de sécurité pour ce profil.

Déclencher McAfee ePO manuellement le profil à partir d'un incident de sécurité

Déclenchez manuellement un profil d'aptitude à partir d'un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Avant de commencer

Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : L'option d'approbation dans le s'affiche uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte Configurer les paramètres .

Pourquoi et quand exécuter cette tâche

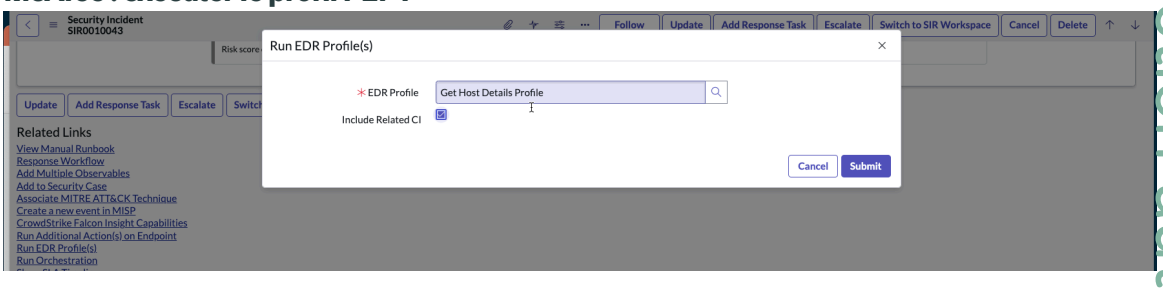
Vous pouvez appeler automatiquement une demande pour obtenir les détails de l'hôte, isoler l'ordinateur hôte ou supprimer l'isolement d'un ordinateur si les conditions de déclenchement que vous spécifiez dans le profil correspondent aux conditions des incidents de sécurité. Si vous souhaitez soumettre une demande manuellement, vous pouvez également la soumettre directement à partir d'un incident de sécurité.

Une fois que vous avez activé le profil, en fonction des conditions de déclenchement configurées, vous pouvez afficher les résultats de la requête dans les ServiceNow AI Platform incidents de sécurité. McAfee ePO Les intégrations vous permettent également d'exécuter des options individuelles sur des éléments de configuration (CI) sans utiliser de profil.

Procédure

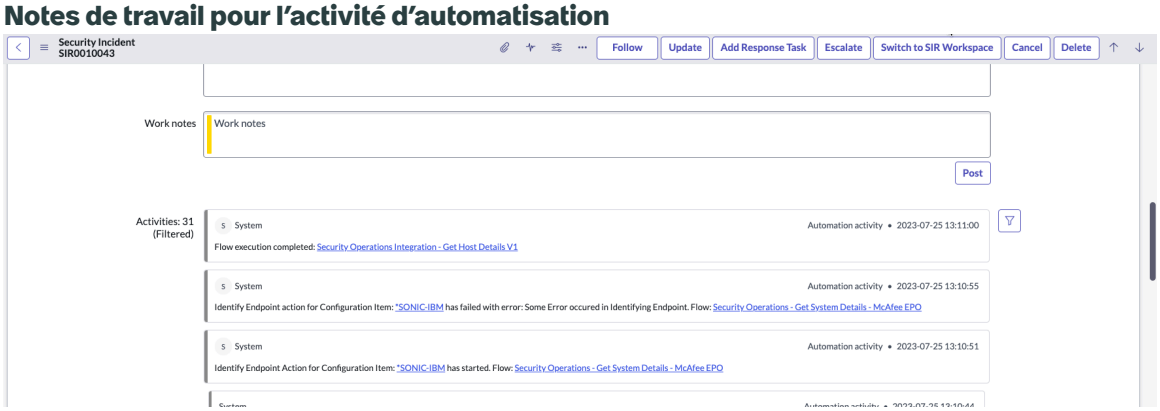
1. Accédez à la **Tous** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les McAfee ePO informations.
3. Dans la section des listes connexes, sélectionnez **Exécuter le(s) profil(s) EDR**.

McAfee : exécuter le profil PEPT



4. Parcourez et sélectionnez un profil dans la liste des profils disponibles.
   Les profils disponibles sont les suivants : Obtenir les détails de l'hôte, Isoler l'ordinateur hôte et Supprimer l'isolement. Par exemple, nous allons sélectionner Obtenir les détails de l'hôte.
5. Sélectionnez **Inclure le CI connexe** pour exécuter ce profil sur tous les CI associés du profil.
   Par exemple, si cinq CI sont associés à l'incident de sécurité, le profil sélectionné s'exécute sur les cinq CI.
6. Cliquez sur **Envoyer**.
   Le profil sélectionné est déclenché manuellement. Vous pouvez consulter la section Notes de travail et activités ainsi que les balises initiées et terminées par le profil dans la section Notes de travail.

Notes de travail pour l'activité d'automatisation

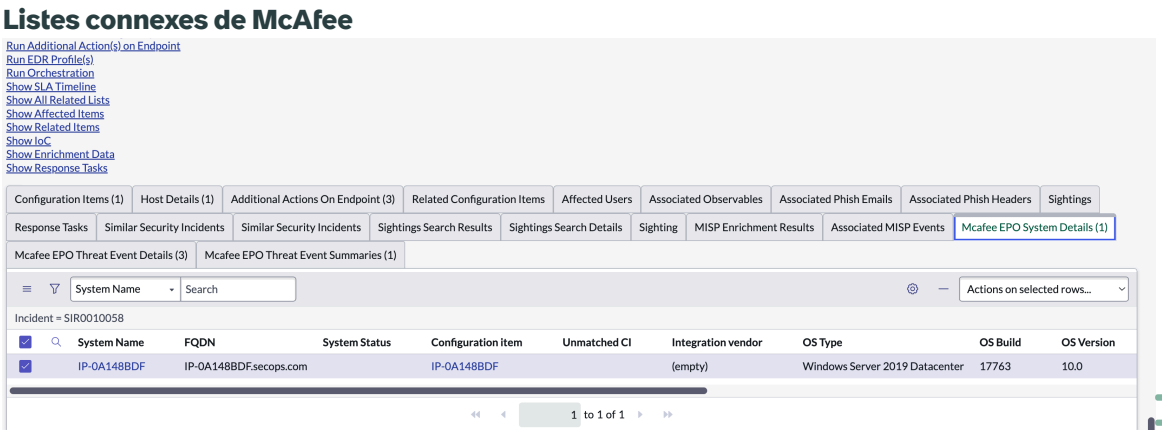


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les résultats s'affichent sous la forme de listes connexes telles que Obtenir les détails de l'hôte, Isoler l'ordinateur hôte ou Supprimer l'isolement.

Remarque : Toutes les tables de listes connexes étendent les tables de base. Dans cet exemple, les détails du système McAfee ePO sont une table étendue de la table de base Détails de l'hôte.



7. Pour exécuter des options individuelles sur un élément de configuration (CI), procédez comme suit :

   a. Dans la liste connexe Éléments de configuration, sélectionnez le CI requis.

   b. Cliquez sur la liste déroulante **Actions sur les lignes sélectionnées...** et sélectionnez l'option requise que vous souhaitez exécuter pour le CI sélectionné.
   Par exemple, Isoler l'hôte.

   c. Cliquez sur **Isoler l'hôte** pour l'exécuter sur le CI sélectionné.
   Le CI sélectionné est isolé du réseau.

Déclencher des actions supplémentaires dans l'intégration McAfee ePO

La liste des événements de menace et les options Lancer une analyse anti-programme malveillant peuvent être déclenchées à partir d'actions supplémentaires.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer et déclencher des actions supplémentaires dans les autorisations d'intégration à l'aide des options **Exécuter des actions supplémentaires sur le**McAfee ePO point de terminaison, qui incluent les options Répertorier les événements de menace et McAfee ePO Lancer une McAfee ePO analyse anti-programme malveillant.

Procédure

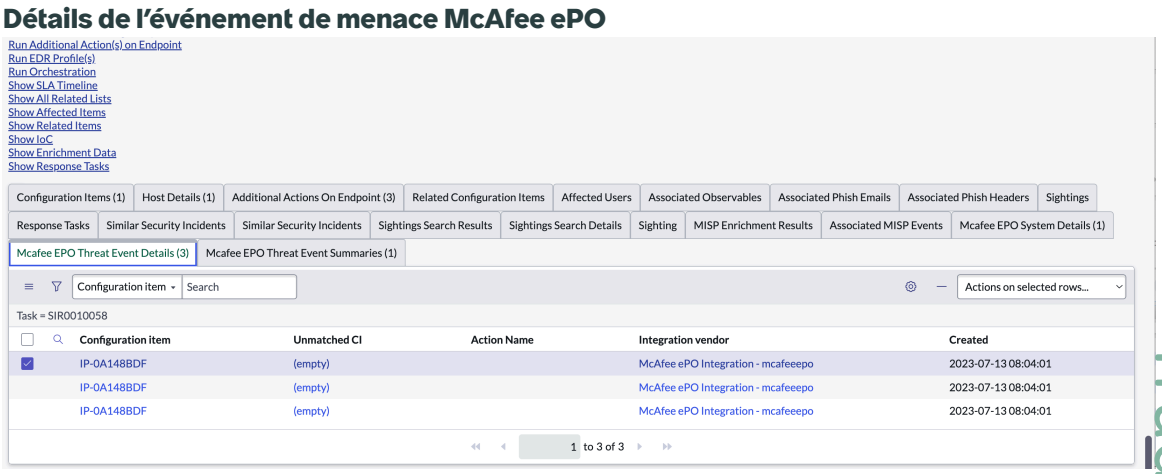
1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité sur lequel vous souhaitez exécuter les actions supplémentaires.
3. Dans la section Liens connexes, cliquez sur **Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison**.
4. Parcourez et sélectionnez l'implémentation de l'aptitude que vous souhaitez déclencher dans la liste des actions supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, McAfee ePO répertorier les événements de menace.

5. Sélectionnez **Inclure le CI connexe** pour exécuter cette action supplémentaire sur tous les CI connexes du profil.
   Par exemple, si cinq CI sont associés à l'incident de sécurité, le profil sélectionné s'exécute sur les cinq CI.
6. Cliquez sur **Exécuter des actions supplémentaires**.



Remarque : Toutes les tables de listes connexes étendent les tables de base. Dans cet exemple, la table Détails de l'événement de menace McAfee ePO est une table étendue de la table de base Actions supplémentaires sur le point de terminaison.

7. Affichez et validez les détails de l'événement de menace McAfee ePO dans les listes connexes.

Utilisation de l'intégration McAfee ePO dans Analyst Workspace

Utilisez l'intégration McAfee ePO pour tirer parti des McAfee ePO options de l'espace de travail d'analyste SIR.

Avant de commencer

Rôle requis : sn_si.admin

Avant d'utiliser McAfee ePO l'intégration dans l'espace de travail de Réponse aux incidents de sécurité, vous devez la télécharger à partir de et la ServiceNow Store configurer. Pour plus d'informations, consultez Configurer votre ServiceNow AI Platform instance pour l'intégration McAfee ePO.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'intégration McAfee ePO pour effectuer des actions de rattrapage sur les points de terminaison en temps réel, utiliser des profils pour recueillir des détails sur l'hôte et effectuer des requêtes ou des actions spécifiques sur le point de terminaison à l'aide de l'espace de Réponse aux incidents de sécurité travail.

L'intégration McAfee ePO permet aux analystes d'utiliser les options suivantes McAfee ePO sur Analyst Réponse aux incidents de sécurité Workspace :

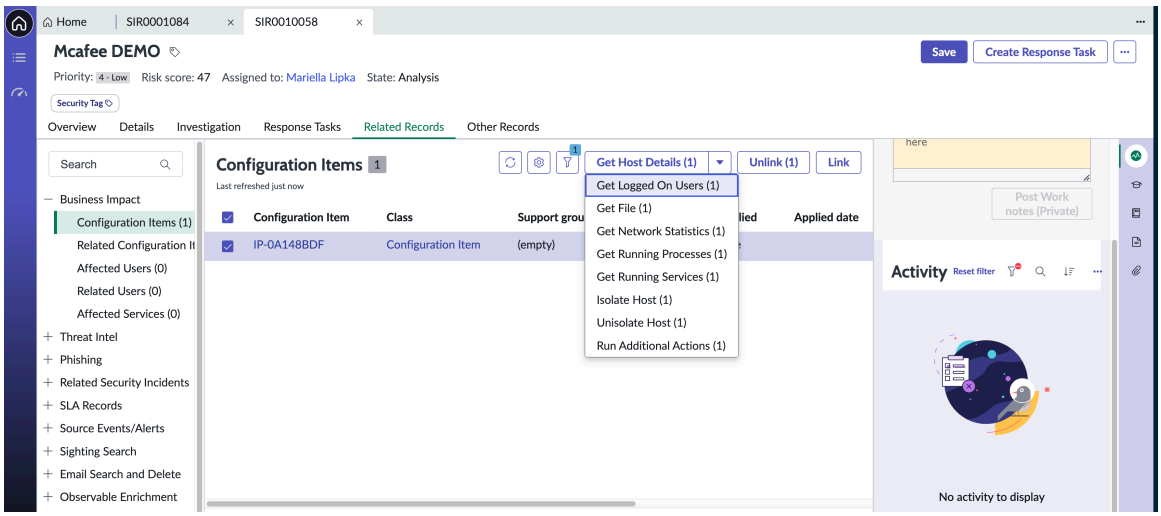
- **Obtenir les détails de l'hôte**
- **Isoler l'hôte**
- **Supprimer l'isolement**
- **Exécuter une ou plusieurs actions supplémentaires sur le point de terminaison**

Traduction automatique

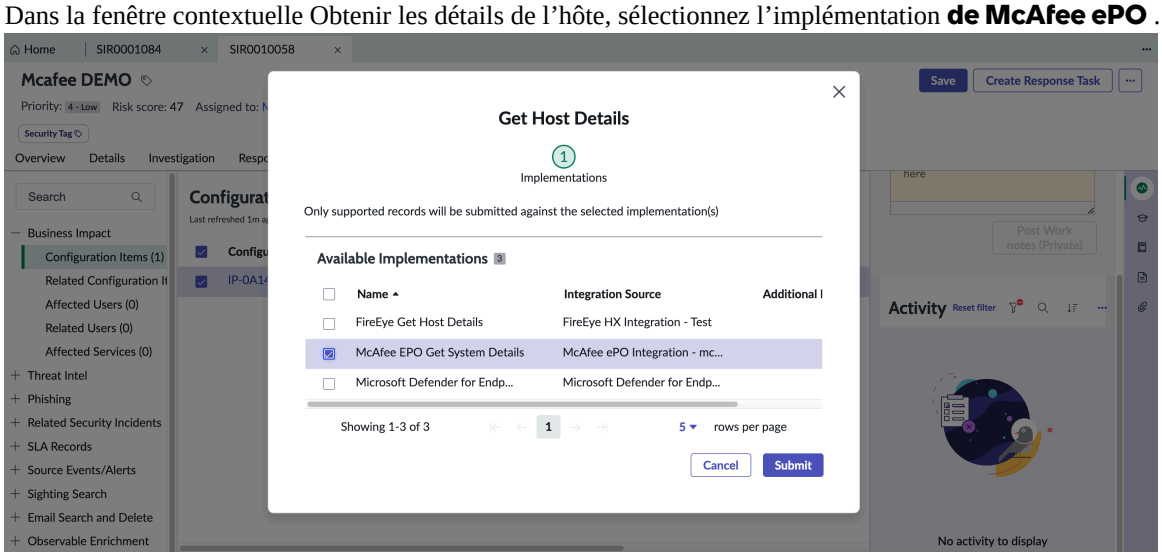
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour ouvrir l'incident de sécurité dans l'espace de travail SIR, cliquez sur **Basculer vers l'espace de travail SIR** sur l'incident de sécurité.
2. Dans l'espace de travail SIR, sélectionnez l'onglet **Enregistrements connexes** .
3. Sélectionnez un **élément de configuration**, puis choisissez une aptitude McAfee ePO à déclencher à partir de l'action déroulante de la liste connexe.
   Par exemple, Obtenir les détails de l'hôte.



4. Dans la fenêtre contextuelle Obtenir les détails de l'hôte, sélectionnez l'implémentation **de McAfee ePO** .

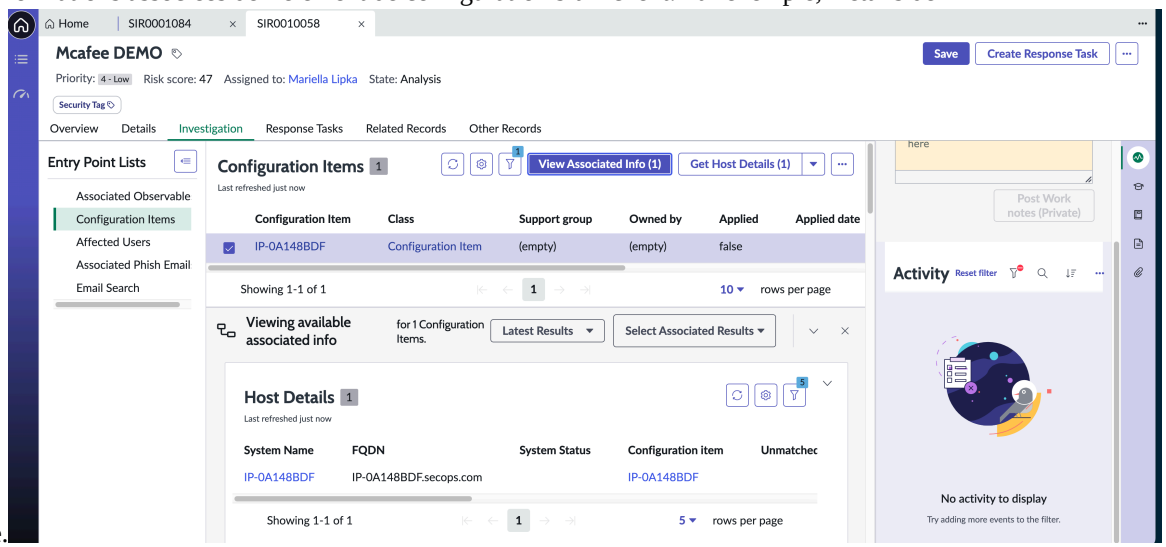


5. Cliquez sur **Envoyer**.
   L'aptitude Obtenir les détails de l'hôte est invoquée sur le CI. Vous pouvez consulter les notes de travail pour connaître les résultats et les conclusions.
6. Pour afficher les données de l'option déclenchée, sélectionnez l'onglet **Examen** .
7. Sélectionnez **l'élément de configuration**, puis cliquez sur l'action **Afficher les informations associées** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les informations associées de l'élément de configuration s'affichent. Par exemple, Détails de l'hôte.



8. Cliquez sur **l'élément de configuration** pour afficher les détails de l'hôte.
   De même, vous pouvez essayer d'utiliser les autres fonctionnalités de McAfee ePO pour vos incidents de sécurité dans SIR Analyst Workspace.
9. Vous pouvez utiliser les fonctionnalités de McAfee ePO sur la liste connexe **Détection et réponse des points de terminaison (EDR)** à des fins d'analyse.
10. Parcourez et sélectionnez un profil dans la liste des profils disponibles.
    Les profils disponibles sont les suivants : Obtenir les détails de l'hôte, Isoler l'ordinateur hôte et Supprimer l'isolement. Par exemple, nous allons sélectionner Obtenir les détails de l'hôte.
11. Sélectionnez l'implémentation **de McAfee ePO** , puis cliquez sur **Soumettre**.

Tester les incidents de sécurité pour lancer l'analyse anti-programme malveillant

Après avoir configuré un profil pour l'analyse anti-programme malveillant, testez-le et affichez les incidents de sécurité qui correspondent aux paramètres de votre profil. Prévisualisez les résultats de l'analyse sur les listes connexes d'un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

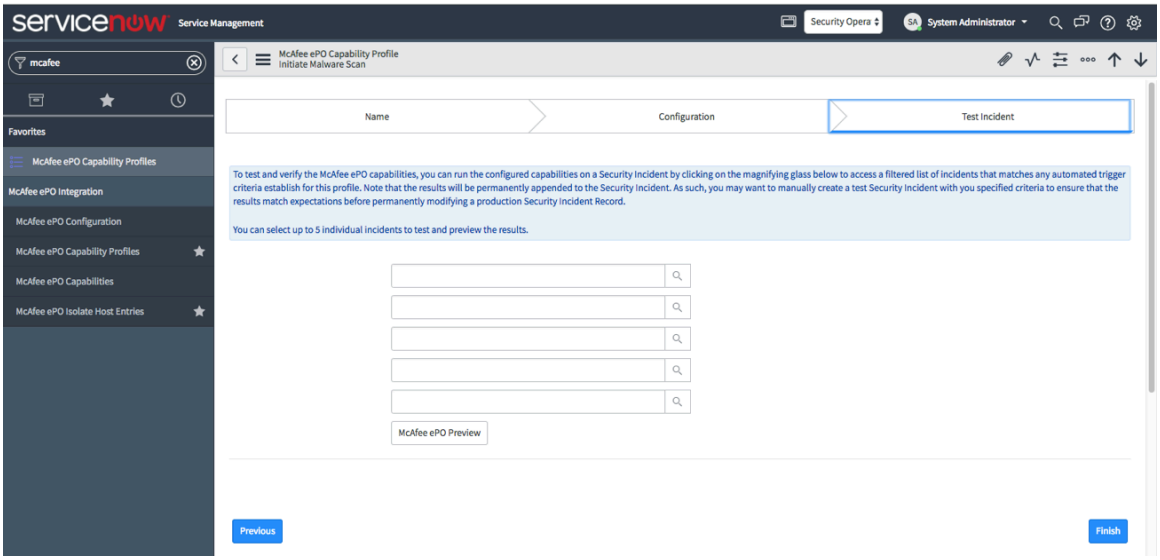
En tant qu'utilisateur disposant du rôle sn_si.admin, vérifiez que le profil avec l'option d'analyse anti-programme malveillant est invoqué et que les résultats de la recherche d'analyse correspondent à ce qui est attendu avec un aperçu des listes connexes sur un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR). L'aperçu vous permet de valider le fait que les résultats de l'analyse sont renvoyés comme prévu pour le profil.

Procédure

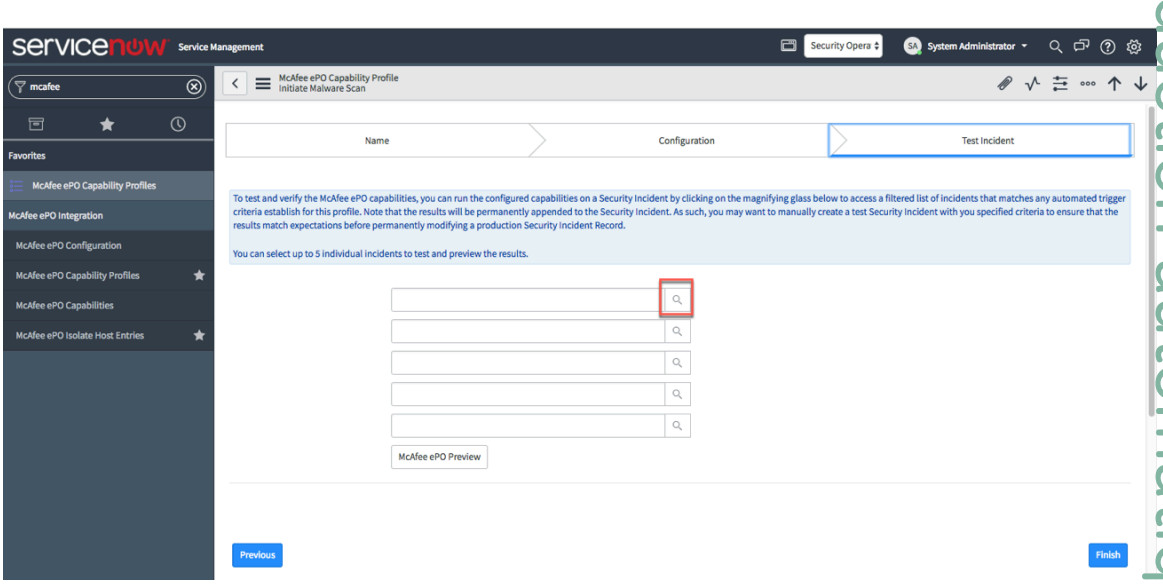
1. Si la page Tester l'incident n'est pas affichée, cliquez sur **Tester l'incident** dans la barre de progression.
   La page Tester l'incident s'affiche pour votre profil. Pour cet exemple, le profil Lancer l'analyse anti-programme malveillant que vous avez créé et configuré dans les sections précédentes s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. À droite du champ supérieur, cliquez sur l'icône de recherche pour sélectionner un incident de sécurité à afficher dans l'aperçu.

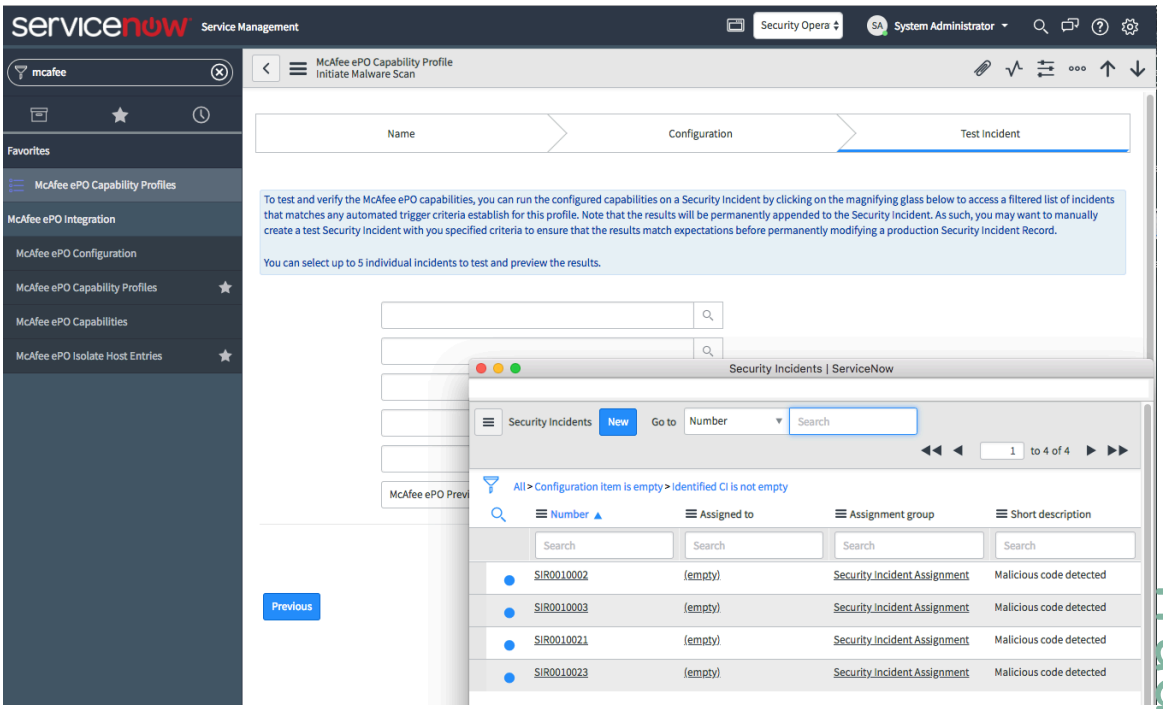


Seuls les incidents de sécurité qui correspondent aux critères de profil sont affichés.

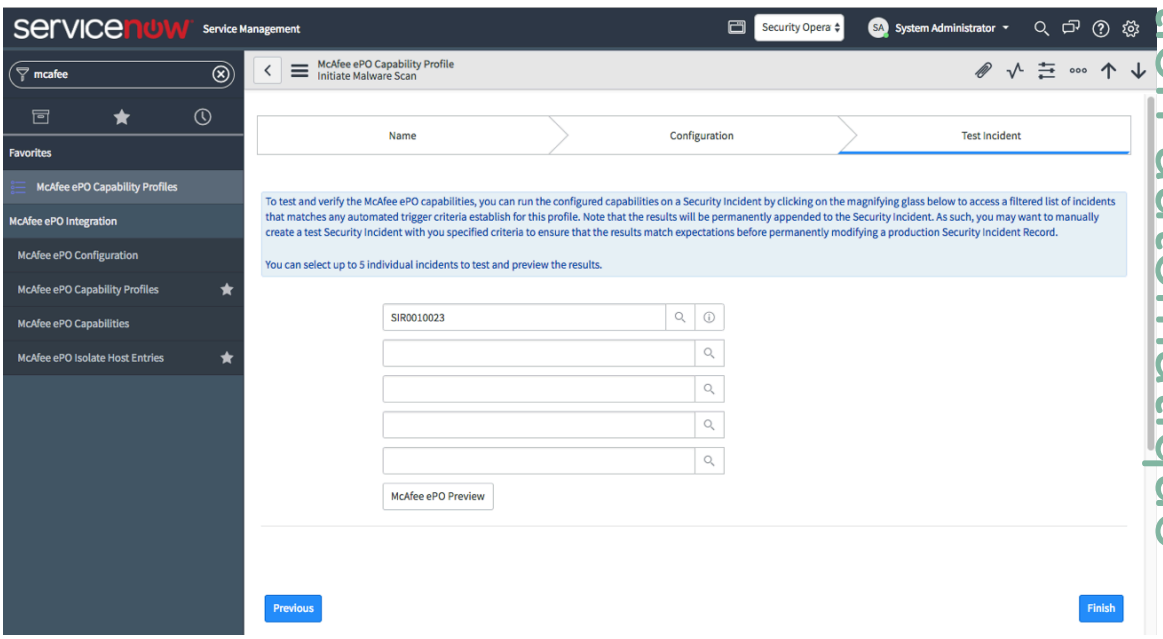
3. Dans la colonne Nombre de la liste qui s'affiche, sélectionnez un élément que vous souhaitez afficher dans l'aperçu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



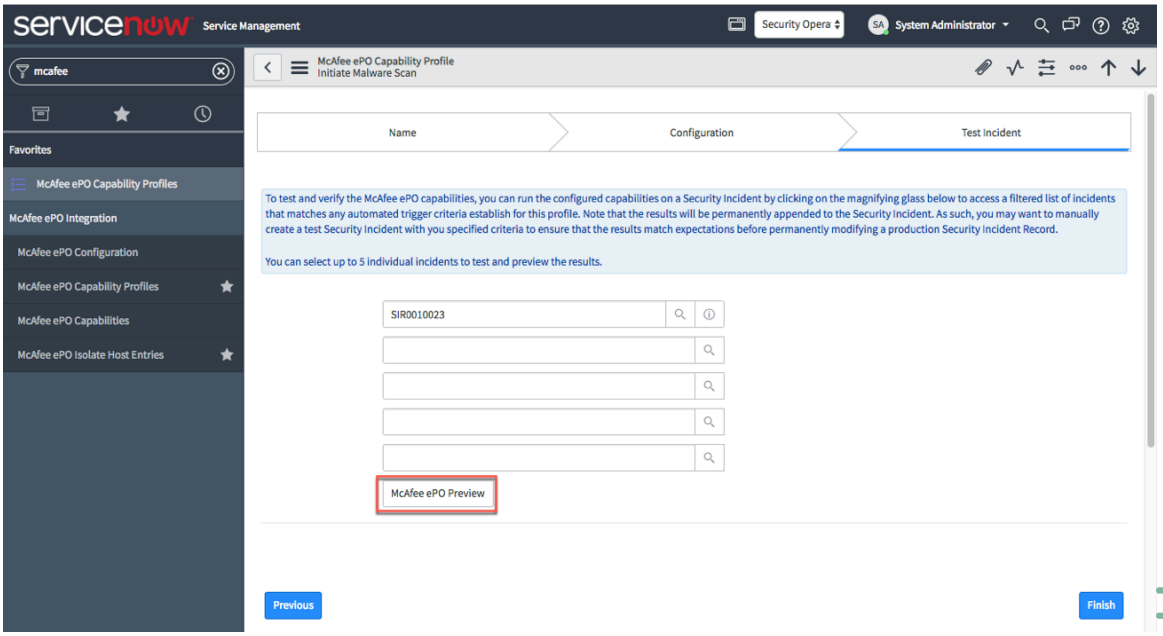
Le numéro de l'incident de sécurité est affiché dans le champ.



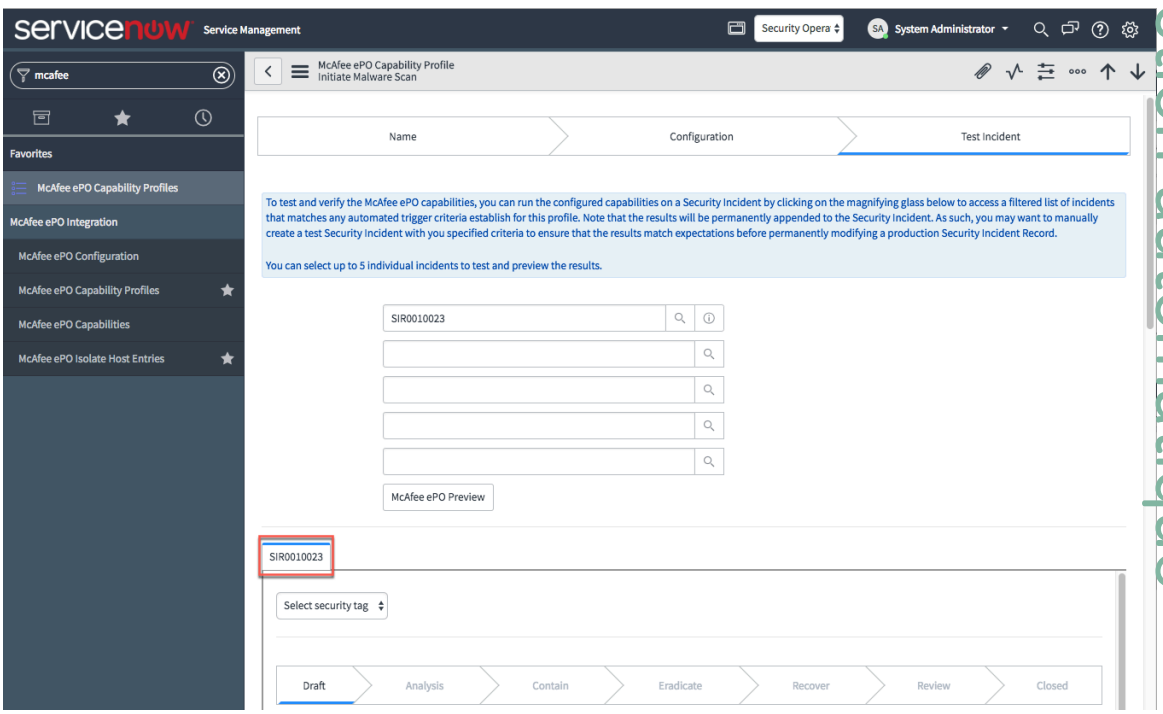
4. Répétez les étapes 2 et 3 jusqu'à ce que tous les incidents que vous souhaitez prévisualiser s'affichent dans les champs.
   Sélectionnez jusqu'à cinq incidents de sécurité pour l'aperçu.
5. Cliquez sur **Aperçu de McAfee ePO**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les incidents de sécurité qui correspondent aux conditions d'événement de votre profil s'affichent. Une fois la page chargée, en bas de la page, des onglets sont affichés pour chaque incident de sécurité.

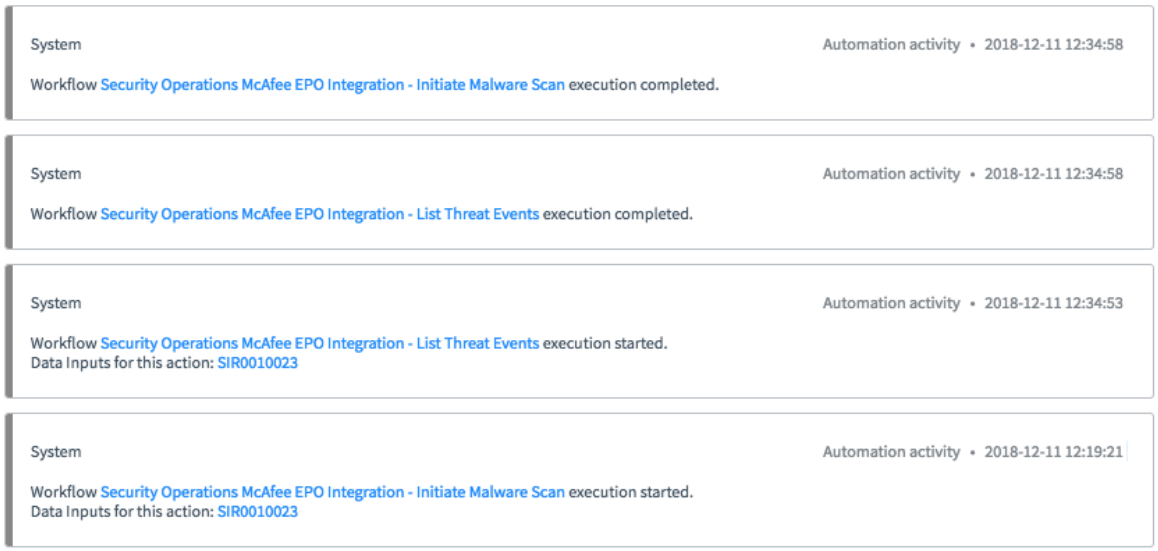


6. Faites défiler pour afficher les notes de travail.

Remarque : Le workflow de la liste des événements de menace fait partie de l'analyse. Pour en savoir plus sur la création d'un profil avec l'option d'analyse anti-programme malveillant, reportez-vous à la section Créer un profil d'aptitude.

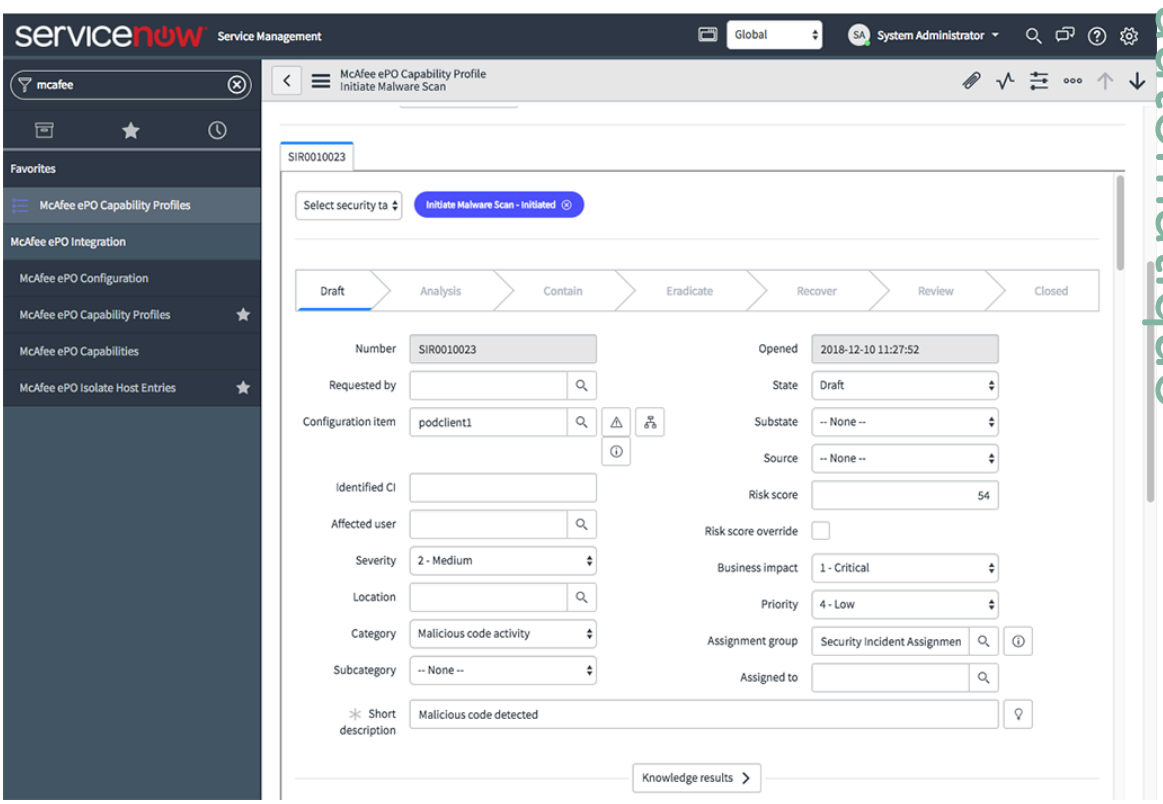
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les analyses sont parfois programmées pour s'exécuter après les heures de pointe afin de minimiser leur impact sur les utilisateurs du réseau. L'analyse peut ne pas se terminer immédiatement. Dans ce cas, en haut de l'incident de sécurité, une balise de sécurité est affichée indiquant que l'analyse est planifiée. Reportez-vous aux notes de travail pour connaître l'état du workflow. Les notes de travail indiquent une fois les workflows démarrés et terminés. Pour cet exemple, les notes de travail de la figure suivante montrent que l'analyse a démarré et qu'elle s'est terminée avec succès. L'aptitude Répertorier les événements de menace a également été démarrée et terminée avec succès dans le cadre de l'analyse.

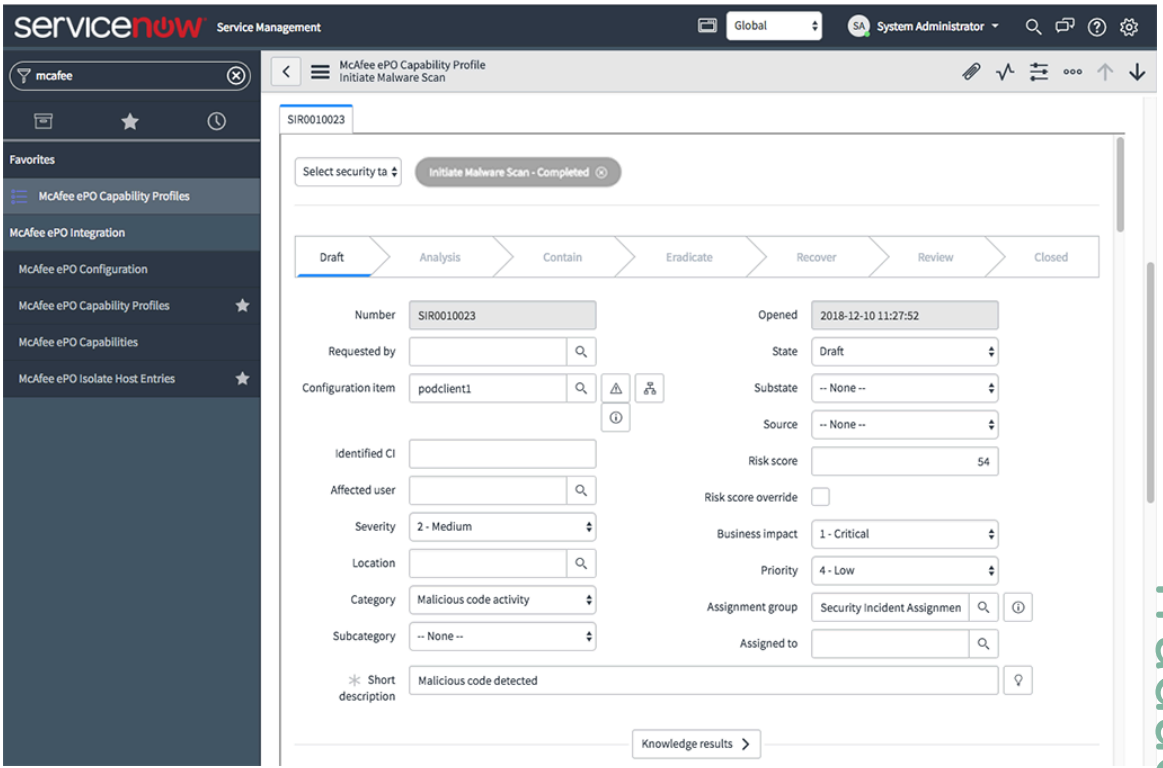
La figure suivante montre un exemple de balise de sécurité sur l'incident de sécurité connexe.



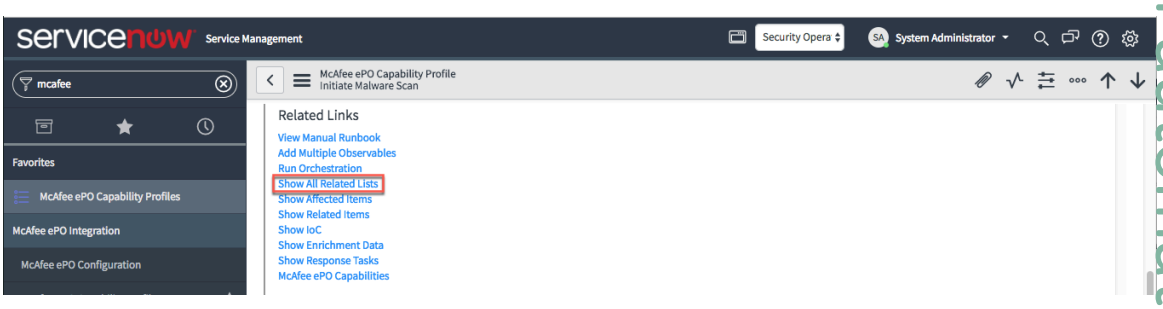
Lors de l'incident de sécurité, une fois l'analyse terminée, la balise planifiée est automatiquement remplacée par la balise terminée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

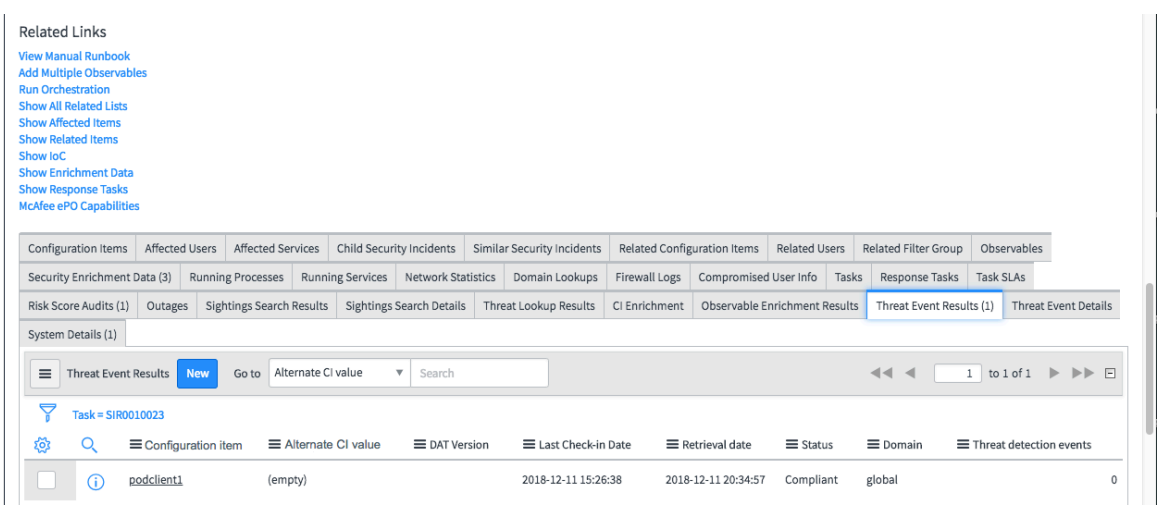


7. Après avoir vérifié que l'analyse est terminée avec succès, sur l'incident de sécurité, faites défiler pour afficher les liens connexes et cliquez sur **Afficher toutes les listes connexes**.



Les résultats de l'événement de menace et les détails de l'événement de menace s'affichent sous forme d'onglets.

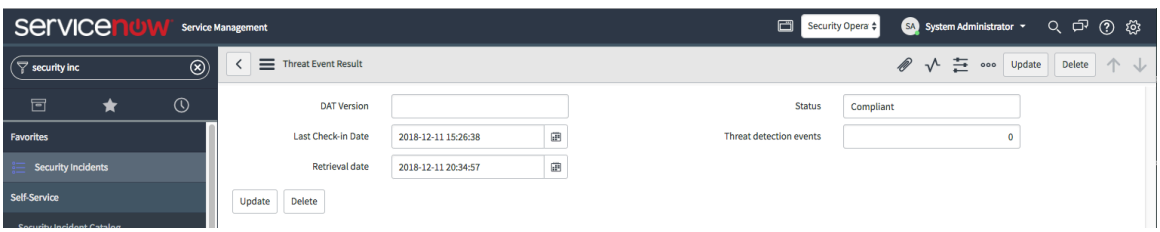
8. Si la liste Détails de l'événement de menace n'est pas sélectionnée, sélectionnez-la pour afficher les résultats.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Cliquez sur un élément dans la colonne Source pour ouvrir un enregistrement et afficher les données d'enrichissement.



Les données d'enrichissement incluent les informations suivantes.

- Valeur du champ CI qui a été mise en correspondance pendant l'analyse.
- Dernière date d'enregistrement avec le fuseau horaire. Ces données font référence au moment où, en heure locale, les données les plus récentes ont été extraites de la McAfee ePO console.
- Données brutes

Vous avez vérifié avec succès que le workflow d'analyse s'est terminé correctement pour les incidents de sécurité qui correspondent aux critères de déclenchement automatique que vous avez définis pour ce profil.

10. Choisissez-en un pour continuer.

Option	Description
Précédent	Revenez à l'étape de configuration du profil. Si vous n'êtes pas satisfait des résultats du test et de l'aperçu, continuez à configurer les paramètres de profil.
Terminer	Terminez la configuration. Vous êtes invité à confirmer l'activation.

Tester les incidents de sécurité et approuver les demandes pour l'hôte isolé

L'étape de test et d'aperçu vous permet de valider que les résultats du workflow d'isolation de l'hôte et de suppression de l'isolement de l'hôte sont renvoyés comme prévu pour le profil.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Au cours de cette étape de la configuration, en tant qu'utilisateur disposant du rôle sn_si.admin, vérifiez que le profil que vous avez configuré avec l'aptitude Isoler l'hôte renvoie les incidents de sécurité et les ID d'actifs correspondants comme prévu. Affichez les incidents de sécurité réels ServiceNow AI Platform Réponse aux incidents de sécurité (SIR) qui sont créés lorsque des conditions d'événement de sécurité correspondant aux paramètres de votre profil se produisent.

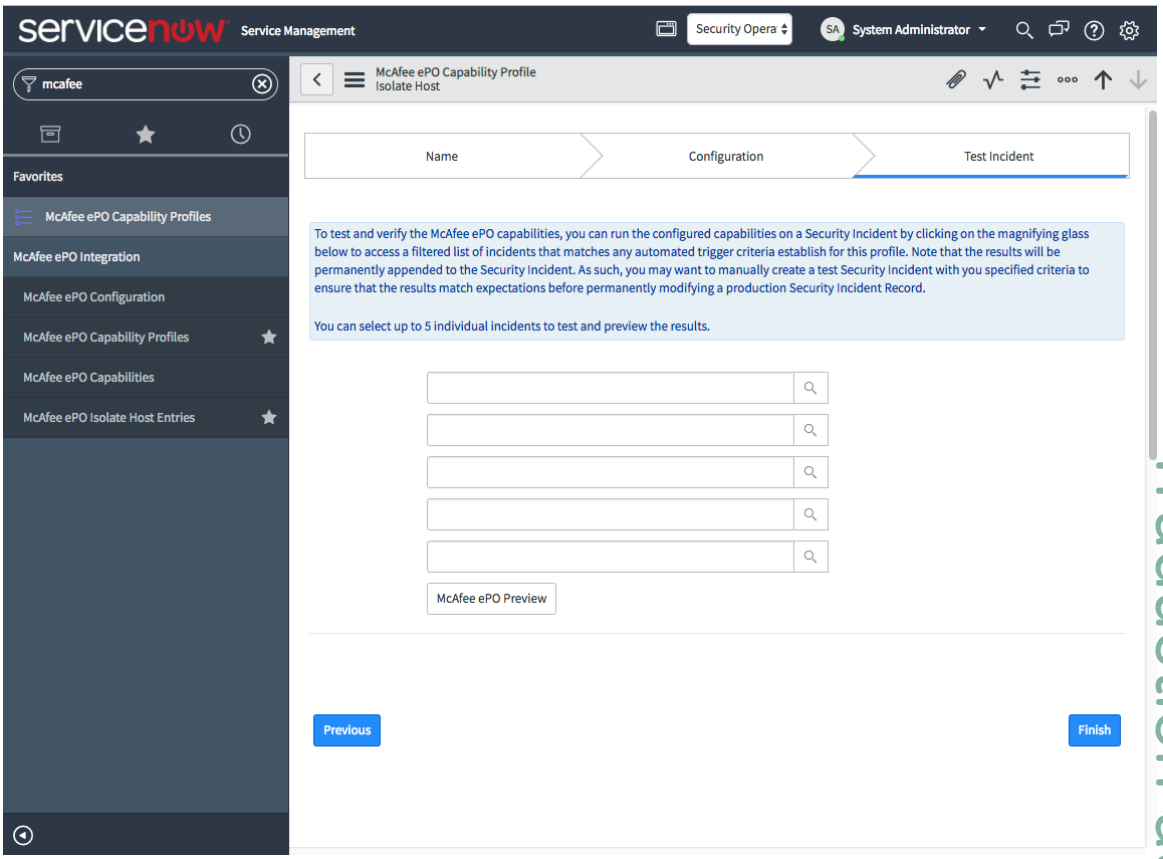
Après l'envoi d'une demande d'isolement d'un ordinateur hôte, traitez-la en tant qu'utilisateur disposant d'un rôle d'approbateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si la page Tester l'incident n'est pas affichée, cliquez sur **Tester l'incident** dans la barre de progression.

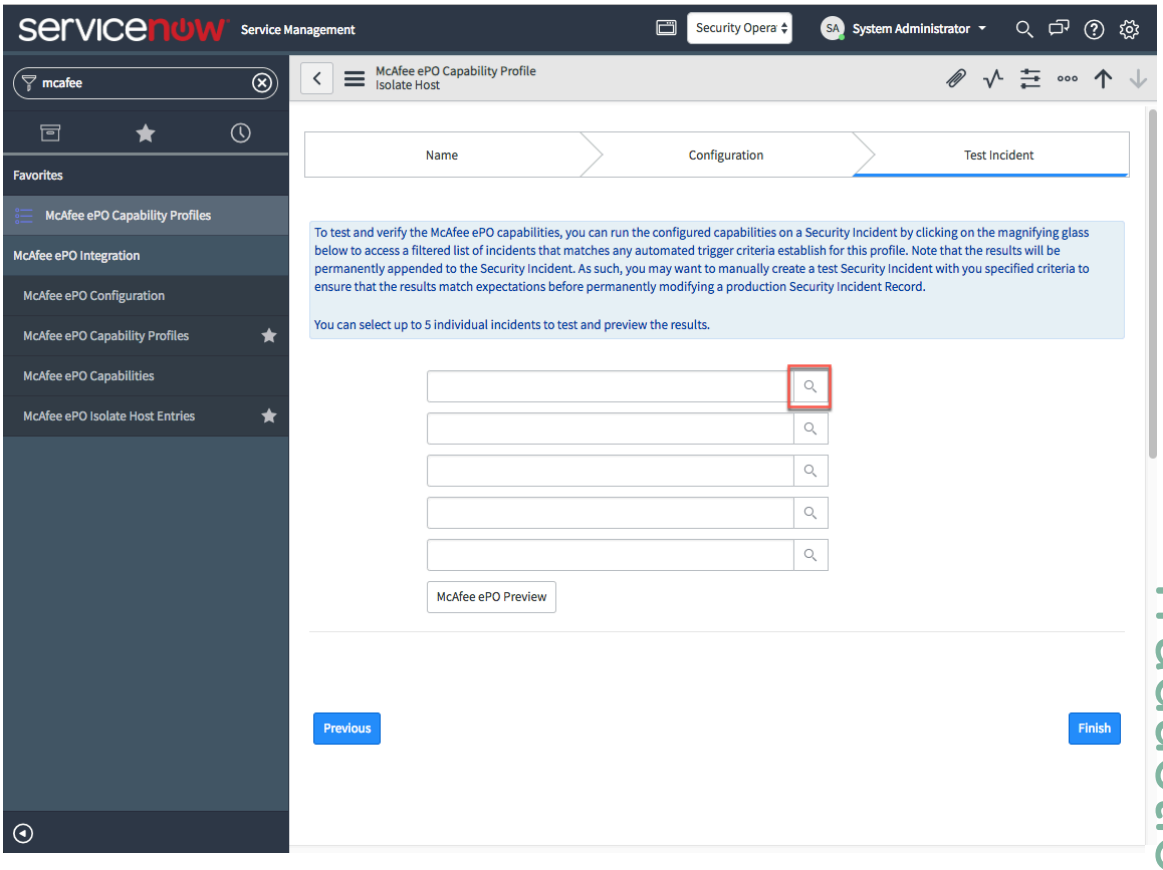


La page Tester l'incident s'affiche pour votre profil. Pour cet exemple, le profil Isoler l'hôte™ que vous avez créé et configuré dans les sections précédentes s'affiche.

2. À droite du champ supérieur, cliquez sur l'icône de recherche pour sélectionner l'incident de sécurité à prévisualiser.

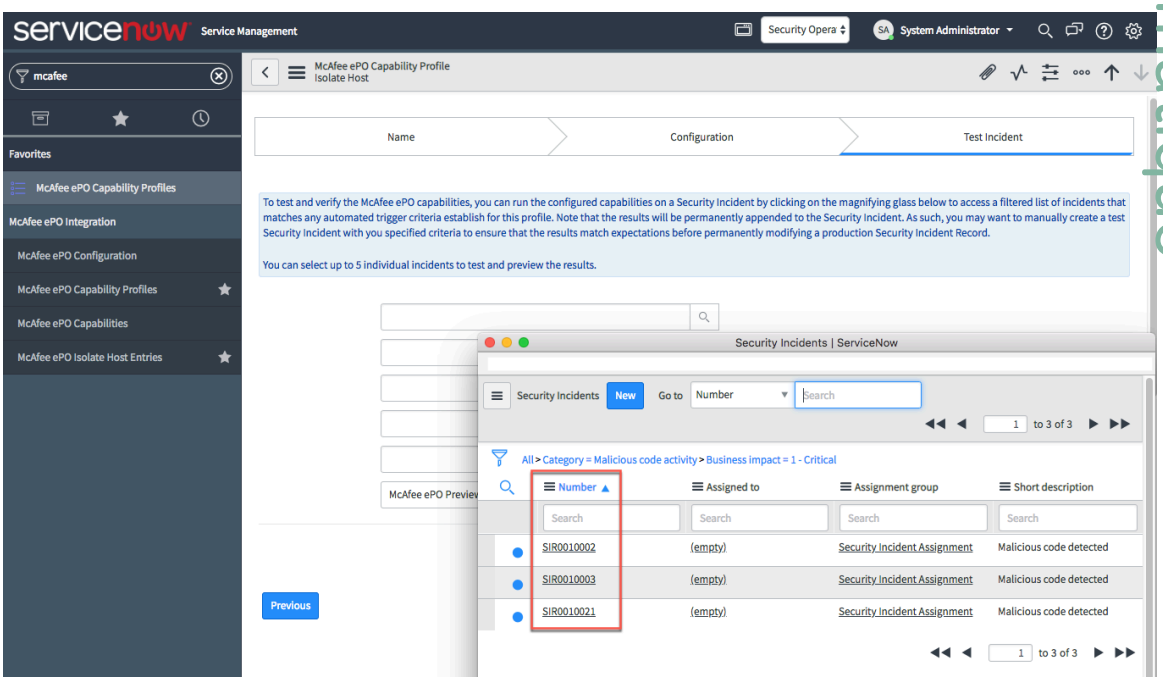
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans la colonne Nombre de la liste qui s'affiche, sélectionnez un élément que vous souhaitez afficher dans l'aperçu.

Seuls les incidents de sécurité qui correspondent aux critères que vous avez définis pour le profil sont affichés.

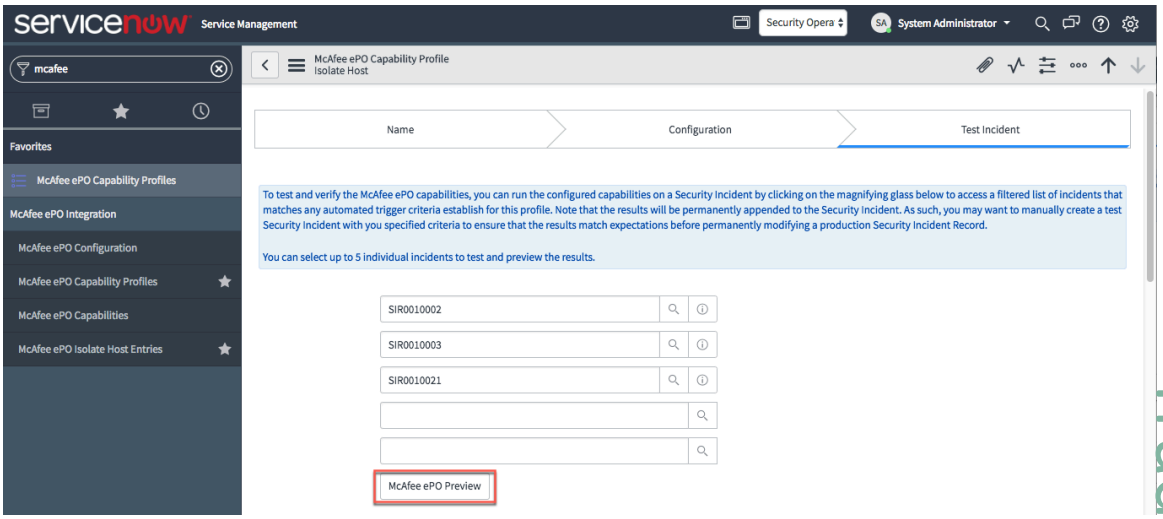


Les incidents de sécurité sont affichés sur la page.

Traduction automatique

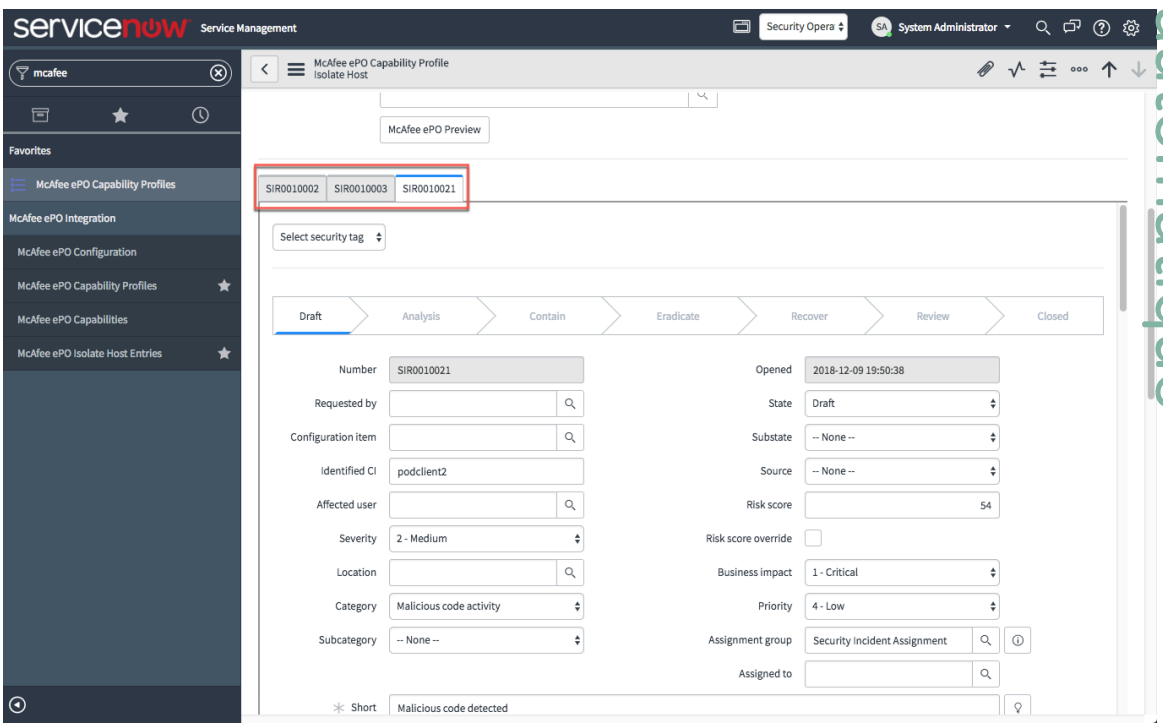
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Répétez les étapes 2 et 3 jusqu'à ce que tous les incidents que vous souhaitez prévisualiser s'affichent dans les champs.
   Sélectionnez jusqu'à cinq incidents de sécurité pour l'aperçu.
5. Cliquez sur **McAfee ePO Preview** pour afficher les incidents de sécurité.



Les incidents créés pour les conditions d'événement de sécurité qui correspondent à votre profil sont affichés dans des onglets.

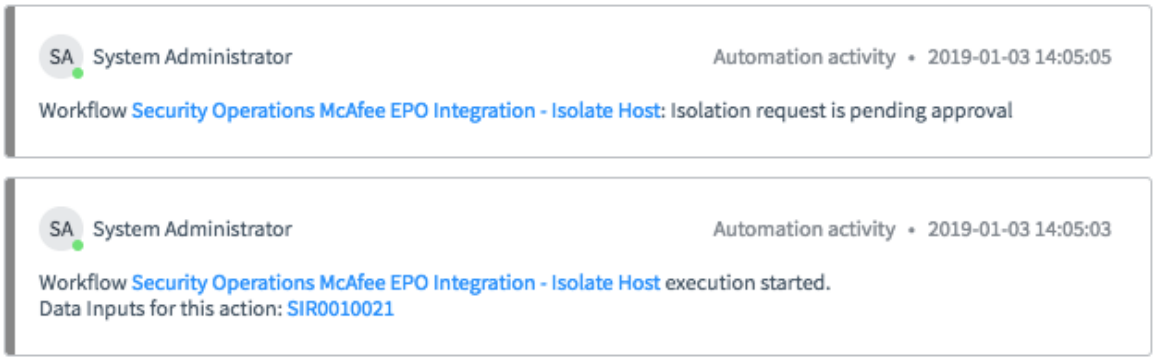
Remarque : Si vous quittez la page Incident de test à ce stade, vos incidents de sécurité sont effacés de ces champs.



6. Sélectionnez un onglet et, sur l'incident de sécurité, faites défiler pour afficher les notes de travail.

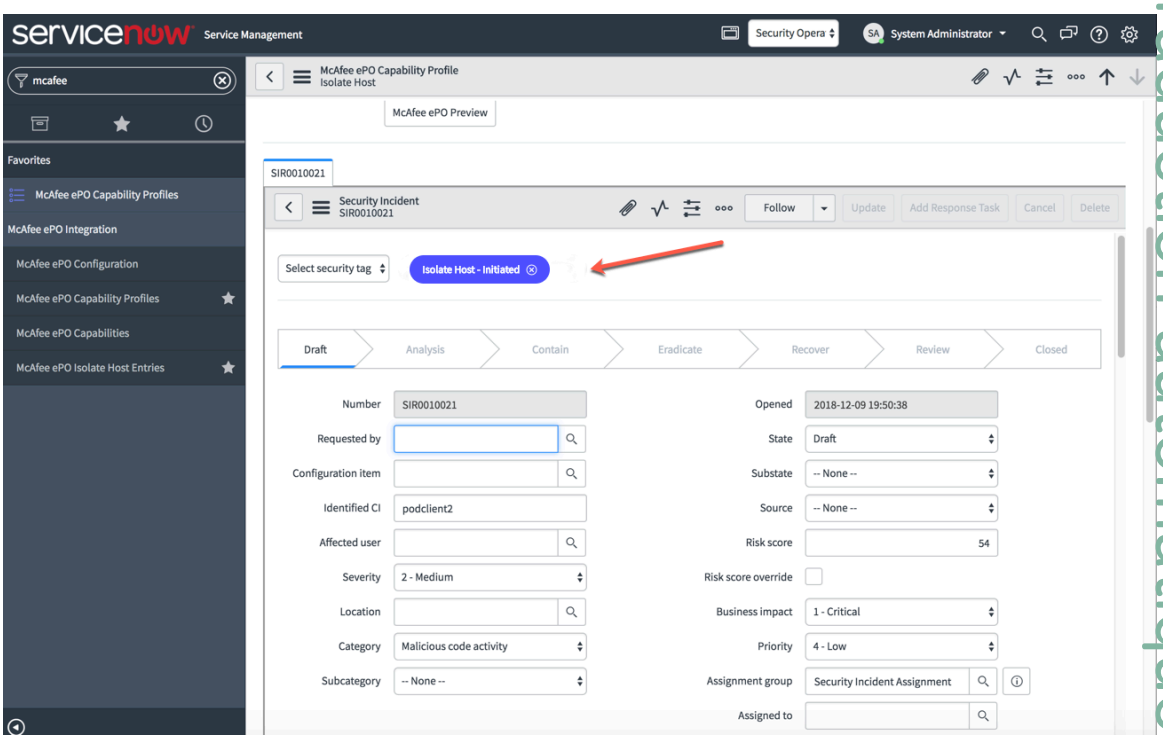
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pour cet exemple, SIR0010021 de l'image précédente est sélectionnée. La liste des notes de travail indiquant que le workflow d'isolement de l'hôte est lancé. Étant donné que l'option **Exiger l'approbation** est activée pour ce profil, les notes de travail indiquent que la demande est en attente d'approbation.

Au-dessus de l'incident, la balise de sécurité indiquant que la demande est lancée (Isoler l'hôte - Initiée) est affichée.



Traduction automatique

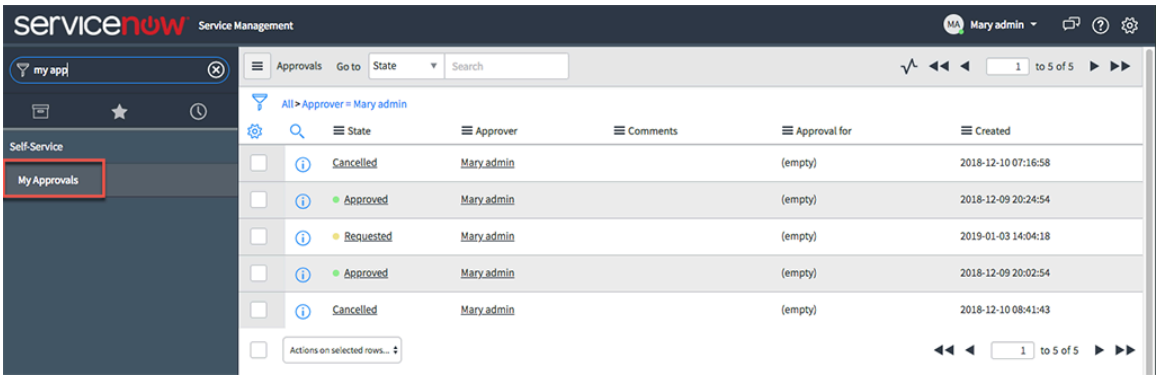
Vous avez localisé avec succès les incidents de sécurité qui correspondent à votre profil pour l'aptitude Isoler l'hôte et visualisé un incident de sécurité.

7. Si vous êtes un utilisateur d'un groupe d'approbation, procédez comme suit pour traiter une demande.

   a. Accédez à **Mes approbations** dans votre instance.

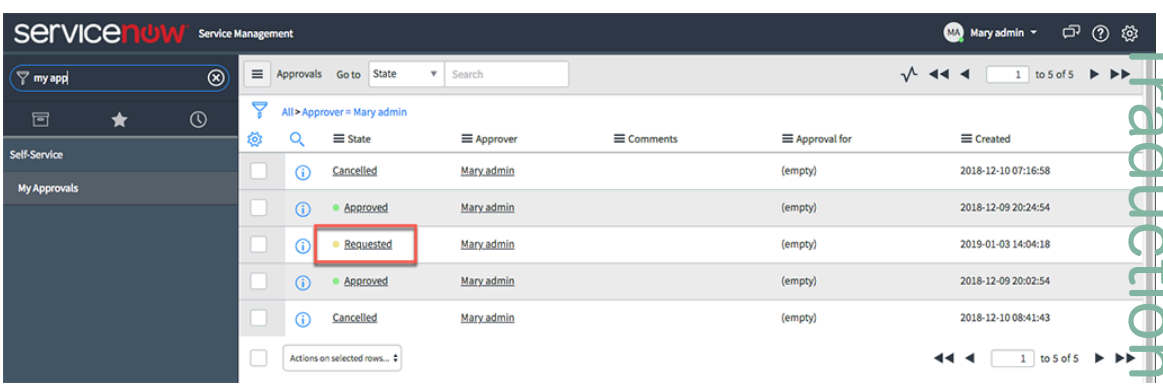
      Pour cet exemple, le nom d'utilisateur de l'approbateur est Mary admin™.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

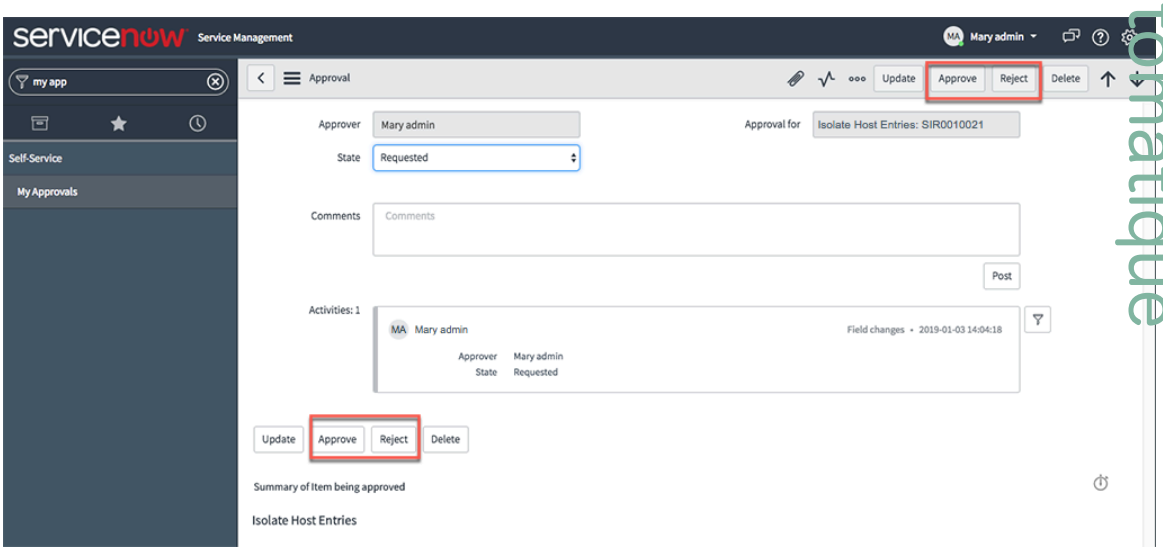


La liste des approbations s’affiche.

b. Dans la colonne État, cliquez sur un élément pour ouvrir l’enregistrement d’approbation.



c. Dans l’enregistrement d’approbation qui s’affiche, cliquez sur **Approuver** ou **Rejeter**.



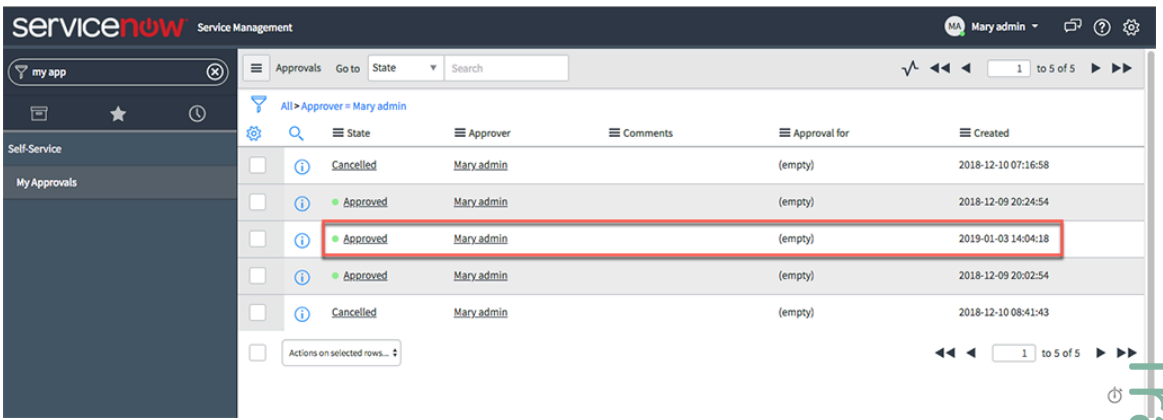
Une fois la demande traitée, l’exécution du workflow peut prendre quelques instants. Sur l’enregistrement en haut, un message s’affiche comme illustré dans la figure suivante si la transaction dure plus de quelques secondes.



Traduction automatique

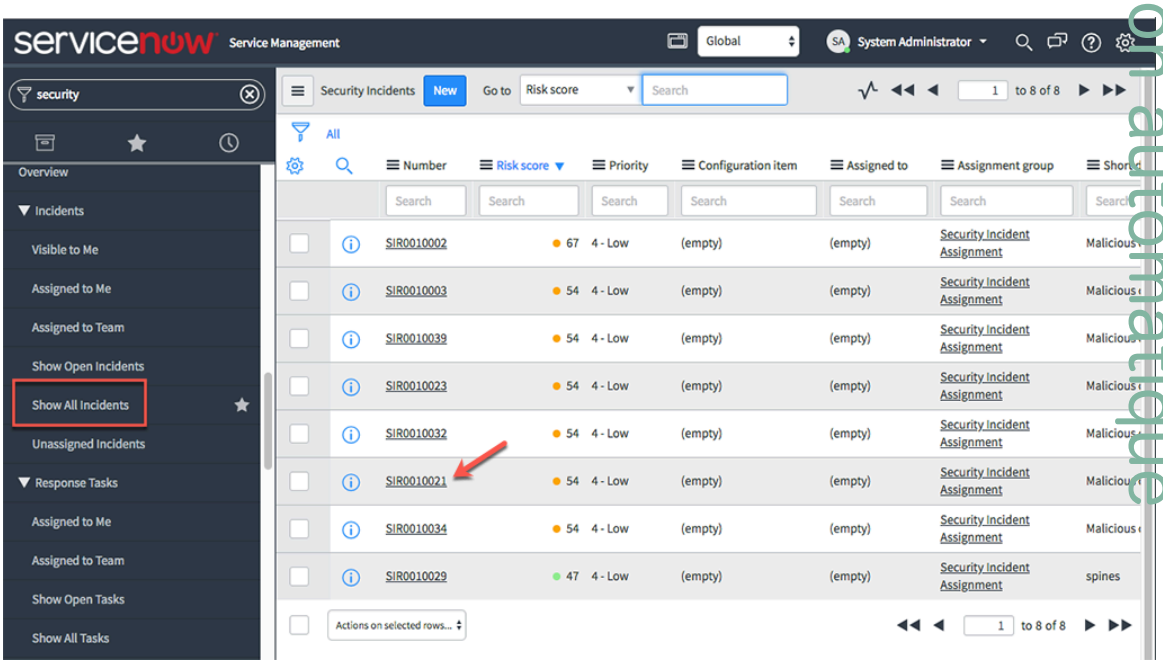
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après quelques instants, dans l'enregistrement d'approbation qui s'affiche, la colonne État passe de Demandé à Approuvé. Aucune approbation supplémentaire n'est requise pour isoler l'ordinateur hôte pour cette demande. Si la demande est rejetée, l'hôte n'est pas isolé et la demande reste en attente. En tant qu'utilisateur disposant du rôle sn_si.analyst, si la demande est rejetée, vous devez envoyer une nouvelle demande si vous souhaitez toujours isoler le point de terminaison.



La demande d'isolement de l'ordinateur hôte dans la figure précédente est approuvée.

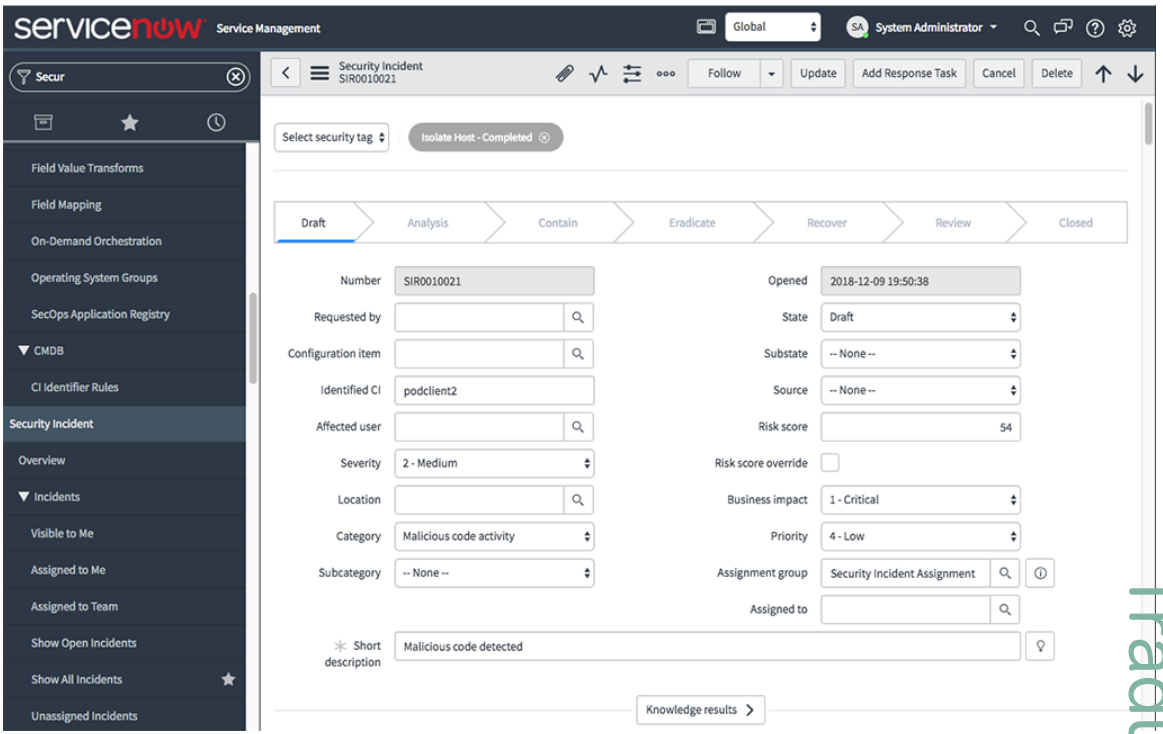
d. Accédez à la **Incident de sécurité** > **Incidents** > **Afficher les incidents** et, dans la colonne Numéro, cliquez sur une entrée pour ouvrir l'incident de sécurité avec lequel vous travaillez.



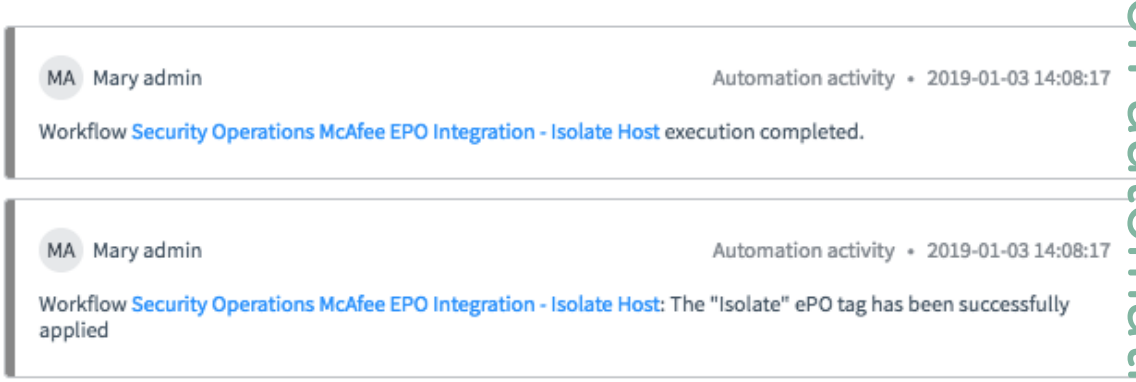
Sur l'incident de sécurité qui s'affiche, la balise Isoler l'hôte - Terminé™ remplace la balise Isoler l'hôte - Initié™ . Le workflow d'isolation de l'hôte pour cet exemple est réussi.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les notes de travail sur l'incident de sécurité indiquent également que l'isolement de l'hôte est terminé et que l'approbateur, Mary admin™, est répertorié.



Important : Bien que la balise de sécurité et les notes de travail sur l'incident de sécurité indiquent qu'un workflow d'isolement de l'hôte est réussi, retournez à votre McAfee ePO console et vérifiez que la machine hôte est isolée de votre réseau.

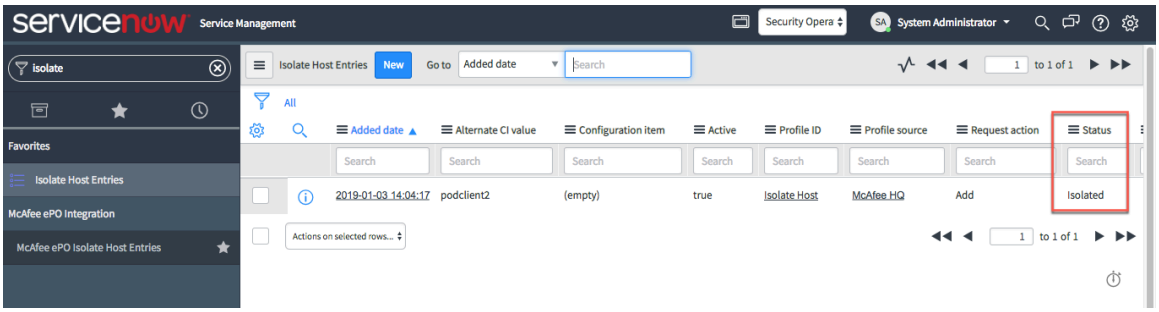
Une fois que vous avez terminé votre enquête sur l'actif, lancez le workflow Supprimer l'isolement à partir de la table Entrées d'isolement de l'hôte™ dans votre ServiceNow AI Platform® instance pour renvoyer l'hôte au réseau.

8. Pour retirer l'hôte de la quarantaine et le renvoyer sur le réseau, procédez comme suit.

Traduction automatique

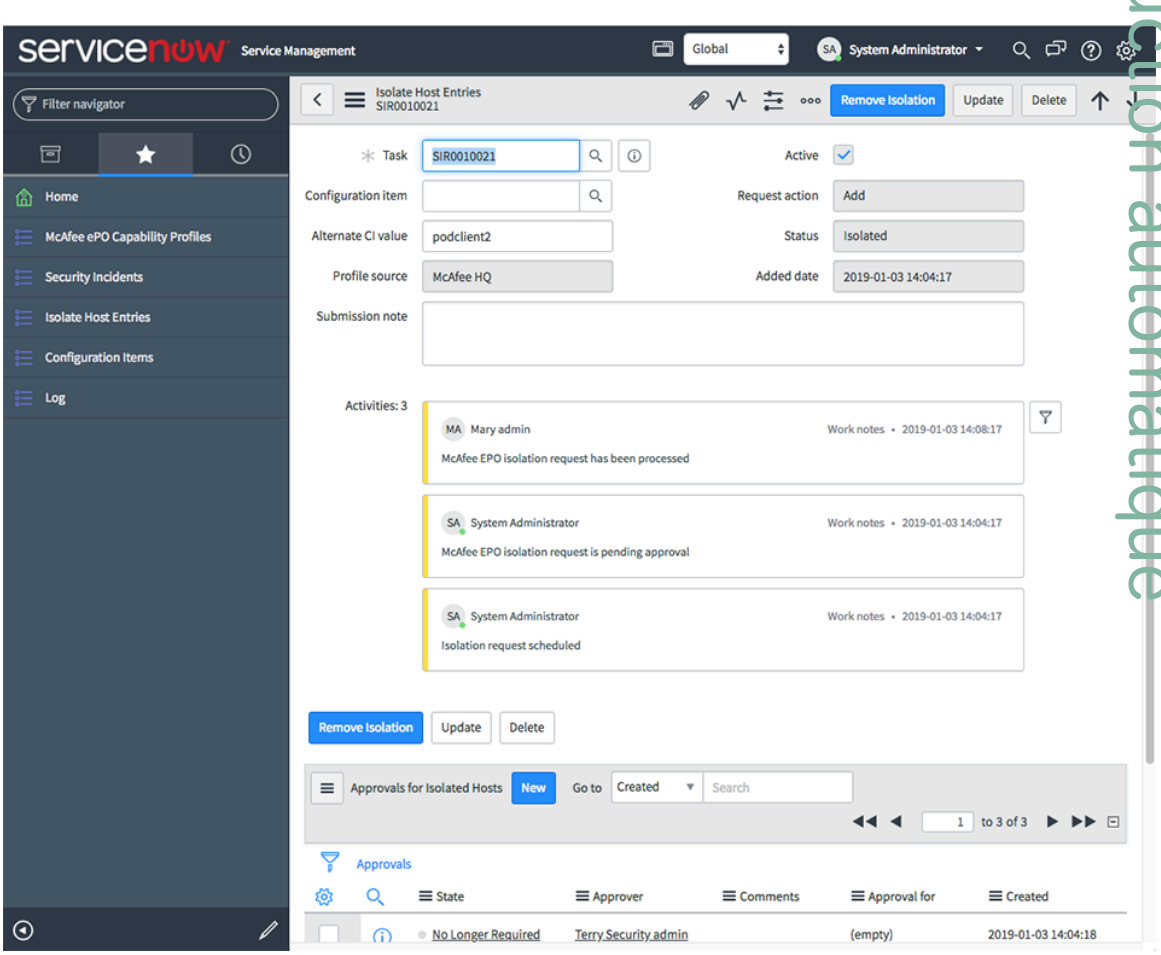
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Si la table Isoler les entrées de l'hôte n'est McAfee ePO pas affichée, accédez à **Intégration McAfee epO** > **Intégration McAfee epO Isoler les entrées de l'hôte**.



La liste Isoler les entrées de l'hôte s'affiche. En haut de la liste, dans la colonne État, recherchez l'actif que vous avez isolé.

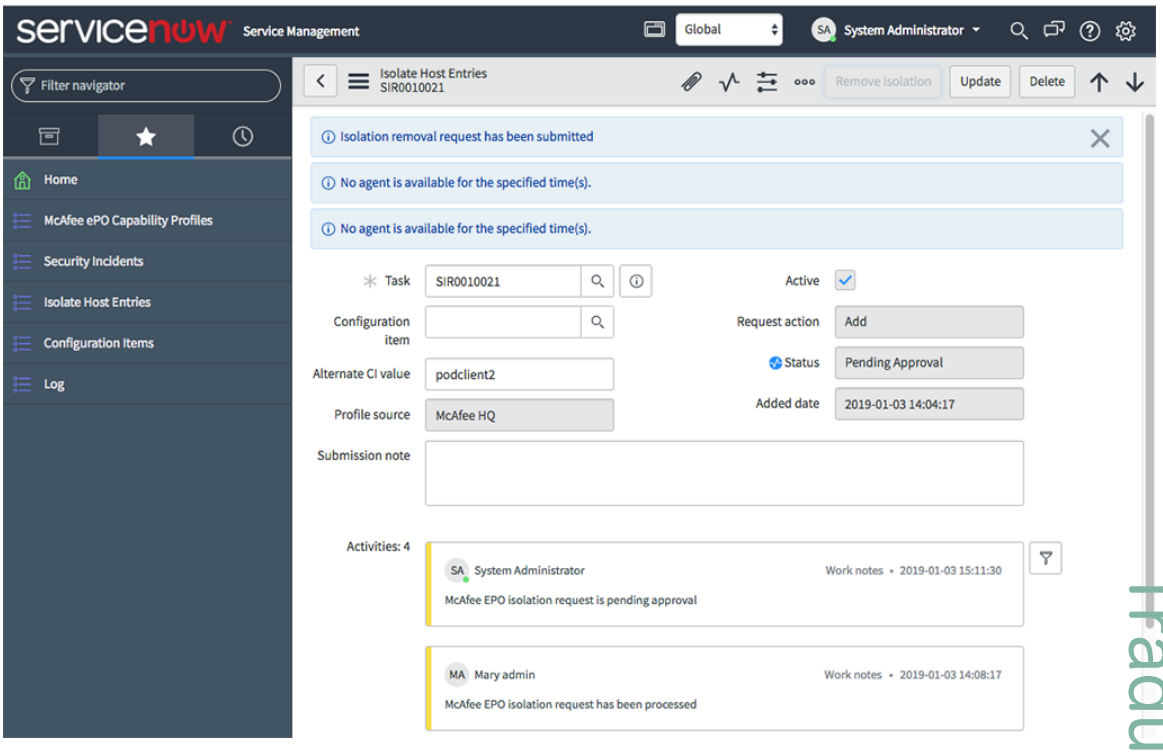
b. Dans la colonne Date d'ajout, cliquez sur l'élément pour ouvrir l'enregistrement.
L'enregistrement Isoler les entrées de l'hôte s'affiche. Une piste d'audit pour toutes les actions associées à l'incident de sécurité est affichée dans les notes de travail. Dans la figure suivante, la dernière entrée des notes de travail est une isolation réussie de l'hôte. La date de fin de la quarantaine est affichée dans le champ **Date d'ajout** (03/01/2019 14:04:17).



c. Cliquez sur **Supprimer l'isolation** pour lancer le workflow de restauration de la machine sur le réseau. L'enregistrement Isoler l'entrée de l'hôte s'affiche. En haut de l'enregistrement, un message indique que la demande a été envoyée. L'état passe **d'Isolé** à **En attente d'approbation**, et une note de travail est consignée. Dans ce cas, l'administrateur système a demandé que la machine soit restaurée sur le réseau.

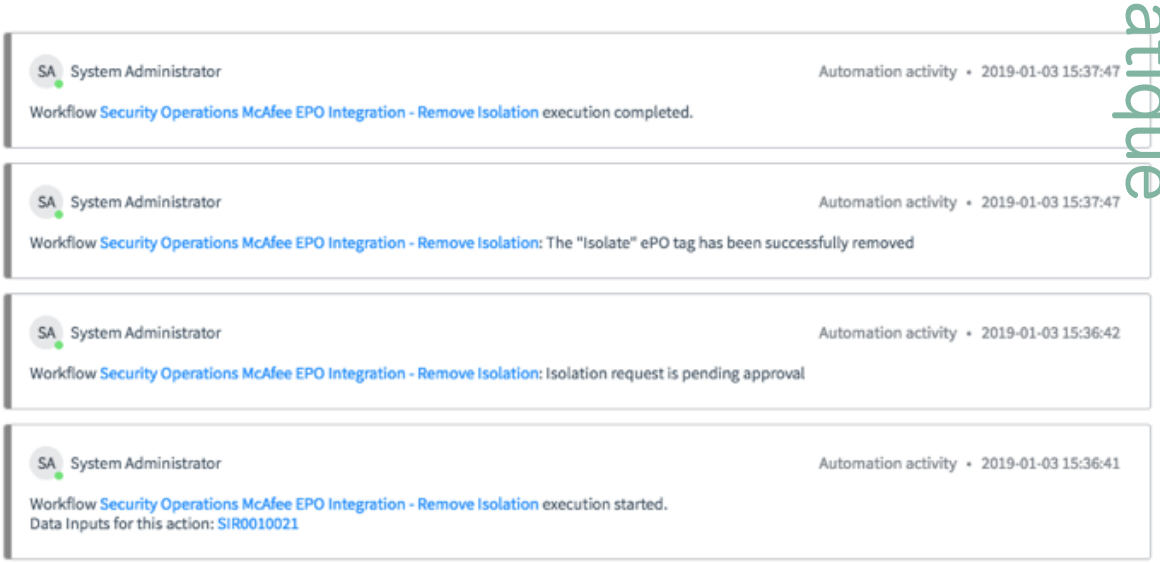
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Après avoir été notifié de la demande, en tant qu'utilisateur avec l'autorisation d'approbation pour l'isolement de l'hôte, accédez à **Mes approbations** dans votre instance et ouvrez l'enregistrement pour la demande de suppression d'isolement.

e. Cliquez sur **Approuver** pour approuver la demande et renvoyer l'actif sur le réseau.
Vous pouvez également cliquer sur **Rejeter** pour maintenir la demande dans l'état En attente d'approbation. Si une demande est rejetée, une nouvelle demande doit être soumise pour isoler l'hôte. Une fois que vous avez approuvé la demande de suppression de l'isolement de l'hôte, la balise de l'incident de sécurité est supprimée. Notes de travail Créez une piste d'audit pour la demande de suppression d'isolement. Pour cet exemple, l'administrateur système a initié et approuvé la demande.



La balise de sécurité et les notes de travail sur l'incident de sécurité indiquent que le workflow de suppression d'isolement de l'hôte est terminé avec succès. Pour vérifier que l'hôte est de retour sur le réseau, retournez à votre McAfee ePO console et vérifiez que l'ordinateur hôte est maintenant actif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Choisissez-en un pour continuer.

Option	Description
Précédent	Revenez à l'étape de configuration du profil. Si vous n'êtes pas satisfait des résultats du test et de l'aperçu, continuez à configurer les paramètres de profil.
Terminer	Terminez la configuration. Vous êtes invité à confirmer l'activation.

Modifier les noms et les couleurs des balises de début et de fin

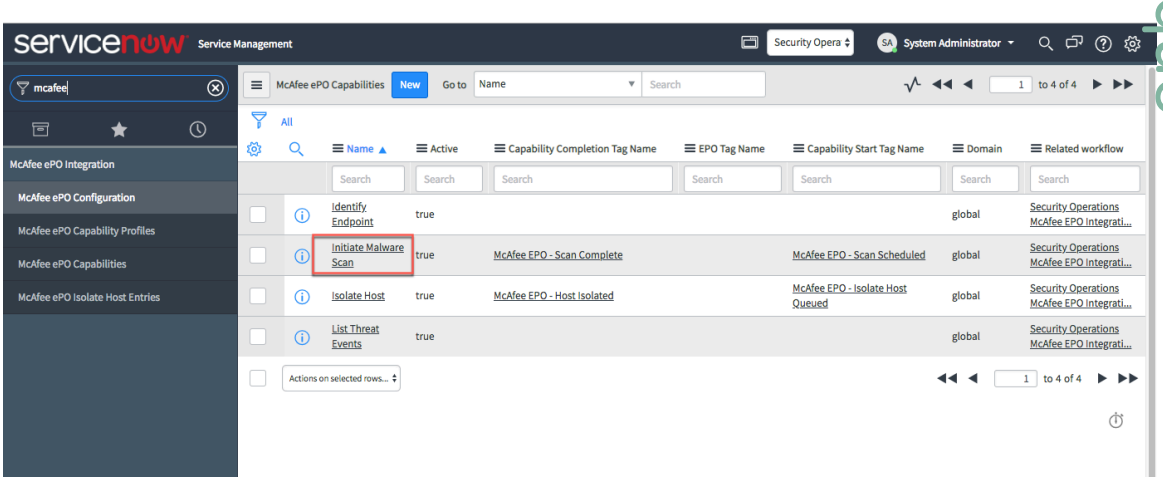
Vous préférez peut-être modifier les noms et les couleurs des balises de démarrage et de fin pour les capacités de lancement d'analyse anti-programme malveillant et d'isolement de l'hôte. Les balises de début et de fin vous aident à identifier rapidement les options invoquées à partir des incidents de ServiceNow AI Platform Réponse aux incidents de sécurité sécurité (SIR).

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
En tant qu'utilisateur disposant du rôle sn_si.admin, vous préférerez peut-être modifier les couleurs et les noms des balises de sécurité affichées sur SIR les incidents de sécurité. Vous pouvez également affecter des balises à des groupes de balises de sécurité pour vous aider à les organiser dans votre ServiceNow AI Platform® instance. Par exemple, vous pouvez modifier les couleurs des balises de sorte que la balise de début d'une option soit d'une couleur et que la balise de complétion soit d'une autre couleur. Ces différentes couleurs peuvent vous aider à identifier rapidement quand les analyses commencent et sont terminées. Pour plus d'informations sur la configuration des groupes de balises et des balises de sécurité, consultez Configurer les groupes de balises et les balises de sécurité.

Procédure

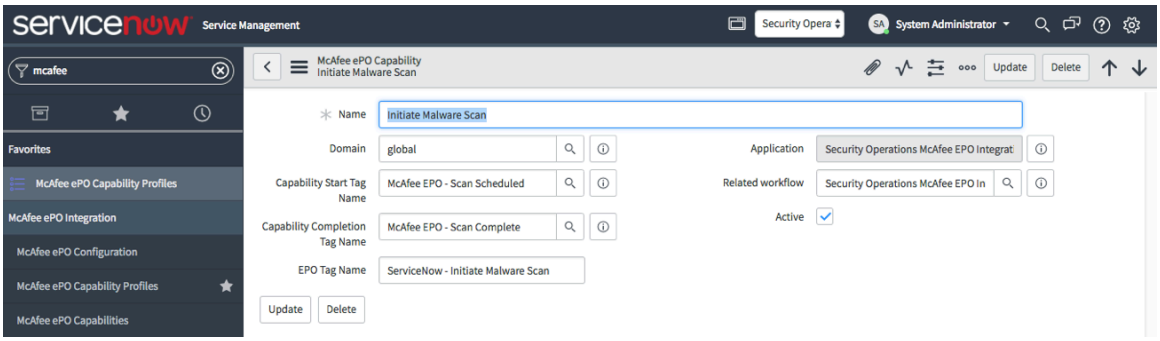
1. Pour modifier les noms et les couleurs des balises de sécurité, accédez à **Capacités McAfee ePO** et, dans la colonne Nom, cliquez sur un élément de la liste.



L'enregistrement de l'option s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. Pour modifier une balise, à droite d'un nom de balise, cliquez sur l'icône d'informations et ouvrez l'enregistrement de la balise.

Dans l'enregistrement qui s'affiche, modifiez les champs.

Champ	Description
Nom	Entrez un nom pour la balise de sécurité.
Couleur	Couleur de la balise de sécurité. Sélectionnez une couleur dans la liste de choix.
Groupe de balises de sécurité	Entrez un nom du groupe de balises de sécurité. Cliquez sur l'icône d'informations pour afficher les groupes disponibles. La valeur par défaut est le groupe de balises META.
Appliquer l'accès restreint	Cochez cette case pour affecter les rôles de lecture et d'écriture requis par les utilisateurs pour lire ou écrire dans des enregistrements qui ont cette balise de sécurité. La valeur par défaut est effacée.
Ordre	Indiquez l'ordre dans lequel la balise apparaît sur les formulaires ou dans une liste. La valeur par défaut est 100. Pour définir l'ordre dans la liste, saisissez une valeur. Par exemple, 100, 200, 300, 400. La balise avec le numéro le plus bas s'affiche en premier sur la liste. Le pro–fil avec le numéro le plus élevé s'affiche en dernier.
Actif	Activer ou désactiver la balise.
Description	Description de la balise.

3. Choisissez-en un pour continuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Mettre à jour	Mettez à jour la page avec les nouveaux changements.
Supprimer	Supprimez cet enregistrement de balise de la fonctionnalité McAfee ePO.

McAfee ESM : intégration de l'analyseur d'e-mails

L'intégration ESM - Analyseur d'e-mails est prise en charge par un analyseur d'e-mails qui utilise les notifications par e-mail d'ESM pour créer des incidents de sécurité.

Configurer McAfee ESM : intégration de l'analyseur d'e-mails

L'intégration de McAfee ESM à l'analyseur d'e-mails utilise les notifications par e-mail d'ESM pour gérer les workflows d'enrichissement et de réponse.

Avant de commencer

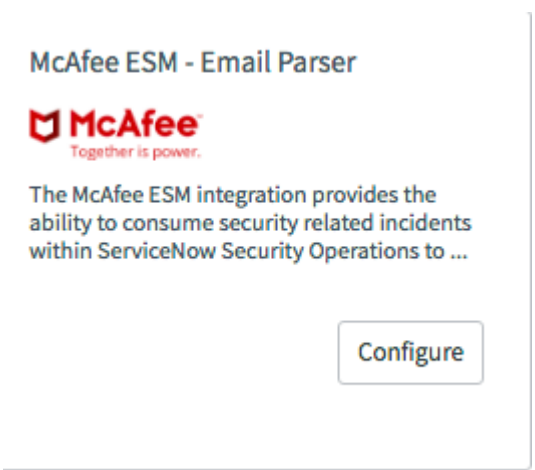
Rôle requis : sn_si_admin

Pourquoi et quand exécuter cette tâche

Un modèle d'analyseur d'e-mails McAfee ESM est fourni pour l'intégration. Il doit être configuré et activé avant l'intégration. La mise à jour de l'analyseur l'active.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.



2. Dans la carte McAfee ESM - Analyseur d'e-mails, cliquez sur **Configurer**.
3. Dans la boîte de dialogue **McAfee ESM - Configuration de l'analyseur d'e-mails** , cliquez sur le lien **Configurer l'analyseur d'e-mails** .
4. Cliquez sur le lien **McAfee ESM** pour modifier les paramètres dans le modèle d'analyseur d'e-mail fourni. Renseignez au minimum le champ L'e-mail provient de . Pour créer votre propre analyseur d'e-mails, reportez-vous à la section Créer des analyseurs d'e-mails dans Security Operations.
5. Cochez la case **Actif** .
6. Cliquez sur **Mettre à jour** dans le formulaire **Analyseur d'e-mails** .
   L'analyseur d'e-mails est actif. Vous n'avez pas besoin de revenir aux **configurations d'intégration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

McAfee ESM : intégration de l'enrichissement des incidents

McAfee ESM - L'intégration de l'enrichissement des incidents recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

- Introduction à l'intégration McAfee ESM - Enrichissement des incidents
- Créer des enregistrements de configuration de recherche de perceptions

Utiliser

- Exécuter une recherche de perceptions
- Security Operations Integration - Flux de recherche de perceptions
- Opérations de sécurité - Flux de recherche d'observations McAfee ESM
- Afficher les détails de la recherche de perceptions
- Afficher les résultats de recherche de perceptions

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Introduction à l'intégration McAfee ESM - Enrichissement des incidents

McAfee ESM protège les terminaux contre les virus, les logiciels espions, les chevaux de Troie et autres menaces de logiciels malveillants et s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration d'enrichissement McAfee ESM des incidents, vous devez la télécharger à partir de et ServiceNow Store ajouter l'URL de base de l'API et les informations d'identification de connexion appropriées.

Avant de commencer

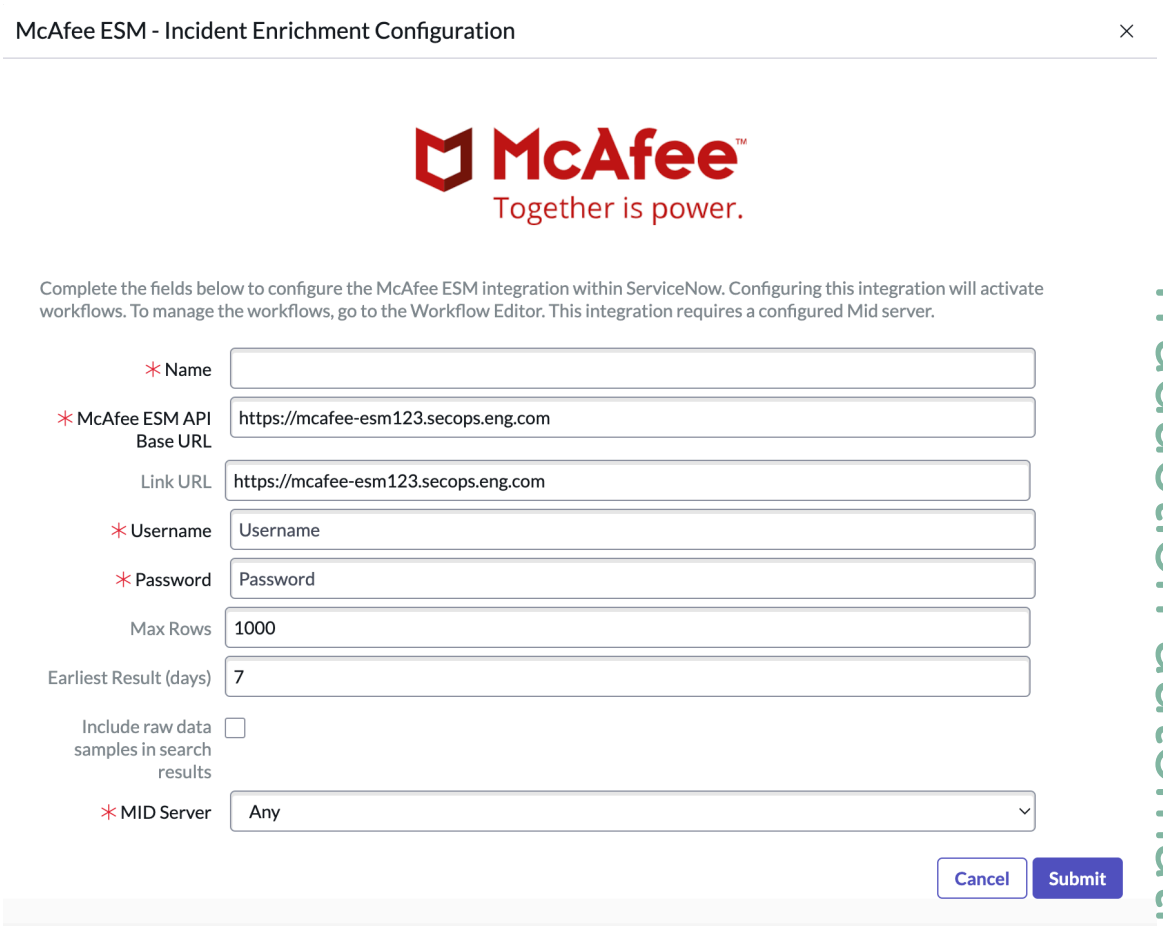
Rôle requis : sn_si_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Intégrations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la carte - Enrichissement de l'incident McAfee ESM , cliquez sur **Nouveau**.



4. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
URL de base de l'API McAfee ESM	URL de base que vous avez acquise sur le site McAfee ESM.
URL de lien	[Facultatif] L'URL de lien qui renvoie à une instance McAfee ESM, lorsqu'elle est disponible. **Remarque :** Si vous obtenez une erreur, veuillez utiliser l'URL de base de l'API McAfee ESM.
Nom d'utilisateur	Votre nom d'utilisateur McAfee ESM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mot de passe	Votre mot de passe McAfee ESM.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend de votre paramètre dans la propriété **nombre de lignes de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	**Sélectionnez N'importe lequel** pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

5. Cliquez sur **Envoyer**.
   La carte de configuration d'intégration s'affiche.
6. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
7. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Intégration Microsoft Azure Sentinel

Microsoft Azure Sentinel est une solution SIEM (Security Information Event Management) et Security Orchestration Automated Response (SOAR) basée sur le cloud. Vous pouvez utiliser l'intégration Microsoft Azure Sentinel pour ingérer des incidents Azure Sentinel et créer automatiquement des incidents de sécurité dans Réponse aux incidents de sécurité.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

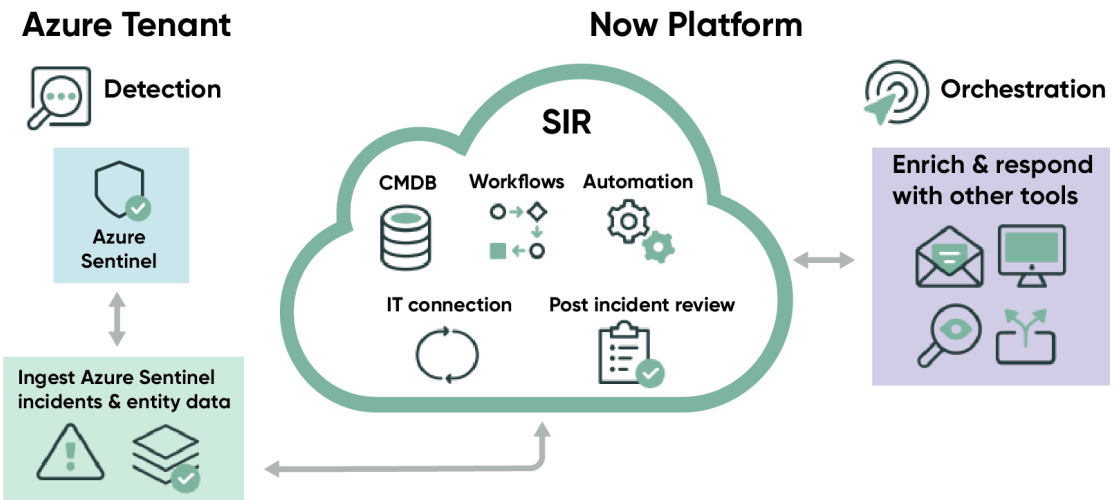
Vue d'ensemble

Consultez le diagramme suivant pour découvrir comment Microsoft Azure Sentinel s'intègre aux ServiceNow AI Platform Opérations de sécurité applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Now Platform - Azure Sentinel integration overview



Fonctionnalités principales

Utilisez les fonctionnalités clés de cette intégration pour effectuer les actions suivantes :

- Découvrez Microsoft Azure Sentinel les incidents qui sont candidats aux incidents de sécurité et automatisez la création de ces incidents de sécurité.
- Mappez Microsoft Azure Sentinel les champs d'incident et d'entité aux champs d'incident SIR de sécurité.
- Filtrer les Microsoft Azure Sentinel incidents.
- Regroupez les incidents aux incidents de sécurité ouverts existants afin de ne pas avoir à créer des incidents de sécurité en double.
- Automatisez Microsoft Azure Sentinel les mises à jour de l'état des incidents pour Réponse aux incidents de sécurité afin de pouvoir créer et fermer les incidents de sécurité.

  Remarque : ServiceNow Met à jour l'état des incidents en fonction de la création ou de la fermeture de Microsoft Azure Sentinel l'incident de sécurité. Cette mise à jour inclut également des commentaires sur les incidents agrégés et les nouveaux incidents.

- Planifiez l'ingestion d'incidents pour créer des incidents de sécurité périodiquement.
- Synchroniser les commentaires sur l'incident avec SIR les Microsoft Azure Sentinel notes de travail.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Microsoft Site web de la documentation produit	Site web de la documentation produit Microsoft
ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise en route de l'intégration Microsoft Azure Sentinel

Activez et configurez le module d'extension pour Security Operation afin qu'il s'interface Microsoft Azure Sentinel - Ingestion des incidents avec votre instance et Réponse aux incidents de sécurité votre ServiceNow AI Platform produit.

Avant de pouvoir utiliser l'intégration Microsoft Azure Sentinel , vous devez la télécharger à partir du ServiceNow Store.

Rôle requis : Microsoft Azure développeur d'application, Microsoft Azure administrateur locataire.

Passez en revue la liste de vérification de configuration suivante et vérifiez que vous avez terminé toutes les tâches pour une intégration fluide.

Liste de vérification

Tâche de configuration	Description
Affectez et vérifiez les rôles et Réponse aux incidents de sécurité requisServiceNow AI Platform.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • Le rôle administrateur installe l'intégration à partir de et ServiceNow Store attribue le rôle sn_si.ingestion_profile_admin. • Le rôle sn_si.ingestion_profile_admin effectue les tâches suivantes : ◦ Configure l'intégration. ◦ Crée des profils d'incident. ◦ Mappe les champs de données d'incident Microsoft Azure Sentinel avec les champs d'incident de sécurité. ◦ Planifie l'ingestion d'incidents en cours. ◦ Active les mises à jour d'incident lorsqu'un Réponse aux incidents de sécurité incident est créé ou fermé. ◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst).
Affectez les Microsoft Azure rôles requis.	Les rôles suivants sont requis pour enregistrer Microsoft Azure et configurer votre application : • Développeur d'application pour l'enregistrement de l'application. • Administrateur du locataire pour donner des autorisations à l'application en appelant le point de terminaison de consentement de l'administrateur.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.	Le ServiceNow Centre d'intégration module d'extension Programme

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	d'installation du pack de démarrage [com.glide.hub.integrations] est requis. Le Réponse aux incidents de sécurité module d'extension (com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ces applications ne sont pas déjà installées, vous devez installer et activer chaque application une par une dans l'ordre suivant pour garantir une installation fluide : **1.** Réponse aux incidents de sécurité **2.** Interface utilisateur Réponse aux incidents de sécurité **3.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **4.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Enregistrez et configurez votre application dans le Microsoft Azure portail.	Enregistrez votre application dans le Microsoft Azure portail et accordez à vos utilisateurs un accès en lecture et en écriture à l'application.

Traduction automatique

Inscrire et configurer le Microsoft Azure portail

Enregistrez votre application dans le Microsoft Azure portail et accordez à vos utilisateurs un accès en lecture et en écriture à l'application.

Avant de commencer

Rôle requis : Microsoft Azure développeur d'application, Microsoft Azure administrateur de locataire

Procédure

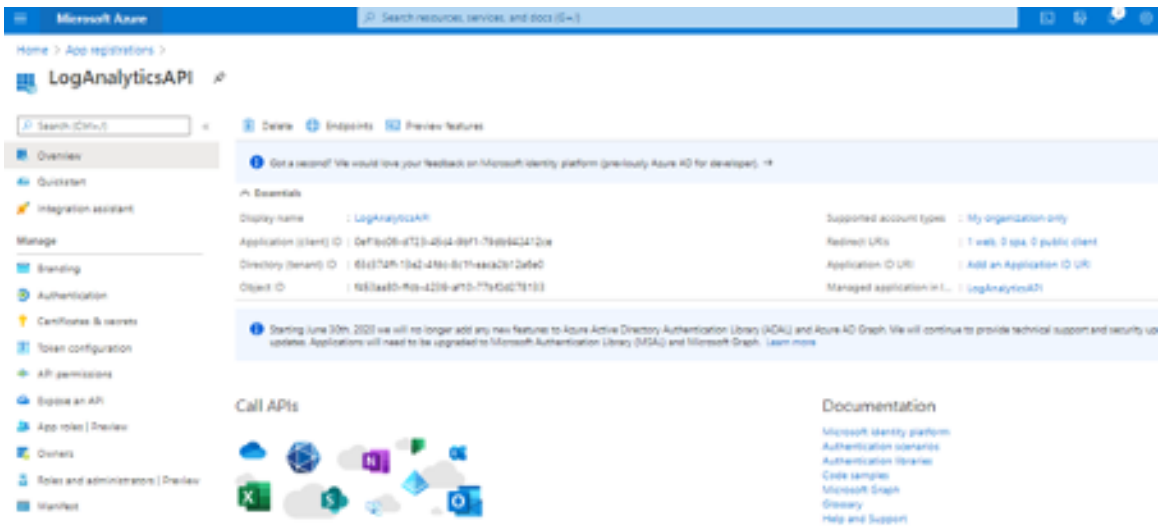
1. Connectez-vous au Microsoft Azure portail.
2. Recherchez et sélectionnez **les inscriptions d'application**.
3. Cliquez sur **Nouvelle inscription**.
4. Remplissez les champs du formulaire.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrer un formulaire d'application

Champ	Description
Nom	Nom d'affichage orienté utilisateur de l'application. Par exemple, LogAnalyticsAPI.
Types de compte pris en charge	Type de compte qui peut utiliser cette application ou accéder à l'API.
URI de redirection	URI de redirection. La réponse d'authentification est dirigée vers cet URI après l'authentification réussie d'un utilisateur.

5. Cliquez sur **Inscrire**.
   Une fois que vous avez enregistré l'application, la page Vue d'ensemble s'affiche.



6. Accédez à la **Gérer** > **Certificats et secrets**.
7. Dans la section Clés secrètes client, cliquez sur **Nouvelle clé secrète client**.
   Vous ne pouvez pas afficher le secret client ultérieurement, assurez-vous donc de copier et d'enregistrer le secret client maintenant à cette étape. Si vous oubliez le secret client, vous pouvez en générer un nouveau en suivant les instructions des étapes 4 et 5.
8. Accédez à la **Gérer** > **Autorisations d'API**.
9. Cliquez sur **Ajouter une autorisation**.
10. Dans la fenêtre Autorisations de l'API de demande, cliquez sur l'onglet **API utilisées par mon organisation** .
11. Recherchez et sélectionnez le nom de l'application **de l'API d'analyse de journaux** .
12. Dans Autorisations de l'API Analyse de journaux, sélectionnez **Autorisations d'application**.
    L'activation de cette autorisation garantit que l'application s'exécute en tant que service d'arrière-plan ou démon sans utilisateur connecté.
13. Dans la section Données, sélectionnez **Data.Read**
14. Cliquez sur **Ajouter des autorisations**.
    Les autorisations sont mises à jour.
15. Activez l'option **Accorder le consentement de l'administrateur pour le répertoire par défaut** pour l'autorisation d'API Data.Read que vous avez activée à l'étape 13.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

16. Recherchez et sélectionnez **des espaces de travail d'analyse de journaux**.
17. Sélectionnez votre espace de travail Sentinel Log Analytics.
    La page Vue d'ensemble de l'espace de travail Sentinel Log Analytics s'affiche.
18. Accédez à la **Contrôle d'accès (IAM)** > **Affectations de rôles**.
19. Cliquez sur **Ajouter**, puis sélectionnez **Ajouter une affectation de rôle**.
20. Remplissez les champs du formulaire.

Formulaire Ajouter affectation de rôle

Champ	Description
Rôle	Type de compte pouvant utiliser cette application. Sélectionnez **Azure Sentinel Responder**.
Affecter l'accès à	Périmètre des autorisations que vous définissez. Sélectionnez **l'utilisateur**, **le groupe** ou **le principal du service**.
Sélectionner	Application que vous avez créée précédemment à l'étape 4. Par exemple, LogAnalyticsAPI.

21. Cliquez sur **Enregistrer**.

Installer et configurer l'intégration Microsoft Azure Sentinel

Installez et configurez l'intégration Microsoft Azure Sentinel à partir de sur ServiceNow Store votre ServiceNow AI Platform instance pour commencer à ingérer des incidents Azure Sentinel.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Téléchargez l'intégration Microsoft Azure Sentinel à partir de et ServiceNow Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la Microsoft Azure Sentinel tuile et cliquez sur **Configurer**.
4. Remplissez les champs du formulaire.

Microsoft Azure Sentinel - Formulaire Configuration de l'ingestion d'incident

Champ	Description
Nom	Nom de la configuration d'instance Microsoft Azure Cloud .
URL d'identité	URL d'identité pour le Microsoft Azure Cloud locataire. Par exemple, login.microsoftonline.com. Pour plus d'informations, consultez la documentation Microsoft Azure .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Gestionnaire de ressources Azure	Point de terminaison Azure Resource Manager pour Microsoft Azure Cloud locataire. Par exemple, management.azure.com. Pour plus d'informations, consultez la documentation Microsoft Azure .
ID de locataire	Microsoft Azure Sentinel ID de locataire. Il s'agit de l'instance Microsoft Azure à partir de laquelle tous les incidents du portail sont récupérés.
ID client	ID client de l'application que vous avez enregistrée dans le Microsoft Azure portail.
Secret client	Secret client pour votre application enregistrée.
ID d'abonnement	ID d'abonnement pour votre application enregistrée.
Nom du groupe de ressources	Nom du groupe de ressources pour votre application enregistrée.
Nom de l'espace de travail	Nom de l'espace de travail de votre application enregistrée.

5. Cliquez sur **Envoyer**.

Résultats
Une fois que vous avez validé et soumis la configuration, chaque configuration du serveur d'ingestion d'incidents est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

Créer un profil pour Microsoft Azure Sentinel

Créez un profil d'incident dans votre ServiceNow AI Platform instance et déterminez les Microsoft Azure Sentinel incidents qui se prêtent à la création d'incidents de sécurité.

Avant de commencer
Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche
L'intégration vous permet de créer différents types d'incidents, tels que des tentatives d'accès non autorisé et des programmes malveillants. Ces incidents sont créés en fonction des profils que vous configurez dans l'instance ServiceNow AI Platform . Tous les incidents sont initialement créés pour un type d'incident configuré dans un profil. Les incidents créés peuvent ensuite être filtrés davantage pour spécifier quels incidents créent des incidents de sécurité.

Tous les incidents qui répondent aux critères de sélection dans votre Microsoft Azure locataire et qui sont disponibles via l'API Microsoft Azure Sentinel sont initialement ingérés dans votre ServiceNow AI Platform instance.

Procédure

1. Accédez à la **Tous** > **Intégration de Microsoft Azure Sentinel** > **Profil d'incident Azure Sentinel**.
2. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Remplissez les champs du formulaire.

Microsoft Azure Sentinel - Formulaire Configuration de l'ingestion d'incident

Champ	Description
Nom	Nom du profil. Ce nom vous permet d'identifier le type de profil et constitue également le nom par défaut de la balise de sécurité associée à ce profil.
Actif	Indique que le profil est actif. Lorsque le profil est actif, cela implique que l'interroge ServiceNow AI Platform activement les incidents Azure Sentinel et que les incidents de sécurité correspondants sont créés lorsque SIR les conditions de filtrage sont vérifiées.
Source	Microsoft Azure locataire que vous avez configuré pour ingérer des incidents. Si vous avez configuré plusieurs locataires, sélectionnez le locataire approprié pour les types d'incidents que vous prévoyez d'ingérer pour le profil.
Ordre	Priorité du flux. La valeur de ce champ indique l'ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400. La valeur par défaut est 100.
Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

4. Pour passer à la section Mappage, cliquez sur **Continuer**.

Que faire ensuite

Mappez les champs d'incident individuels Microsoft Azure Sentinel aux champs de l'incident ServiceNow AI Platform SIR de sécurité.

Mapper les champs d'incident Microsoft Azure Sentinel

Mappez les champs d'incident individuels Microsoft Azure Sentinel aux champs de l'incident SIR de sécurité afin de pouvoir créer des incidents avec les données mappées.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Sur la page de mappage, dans la section Mappage de champ Azure Sentinel, sélectionnez l'une des méthodes d'intégration d'échantillons.

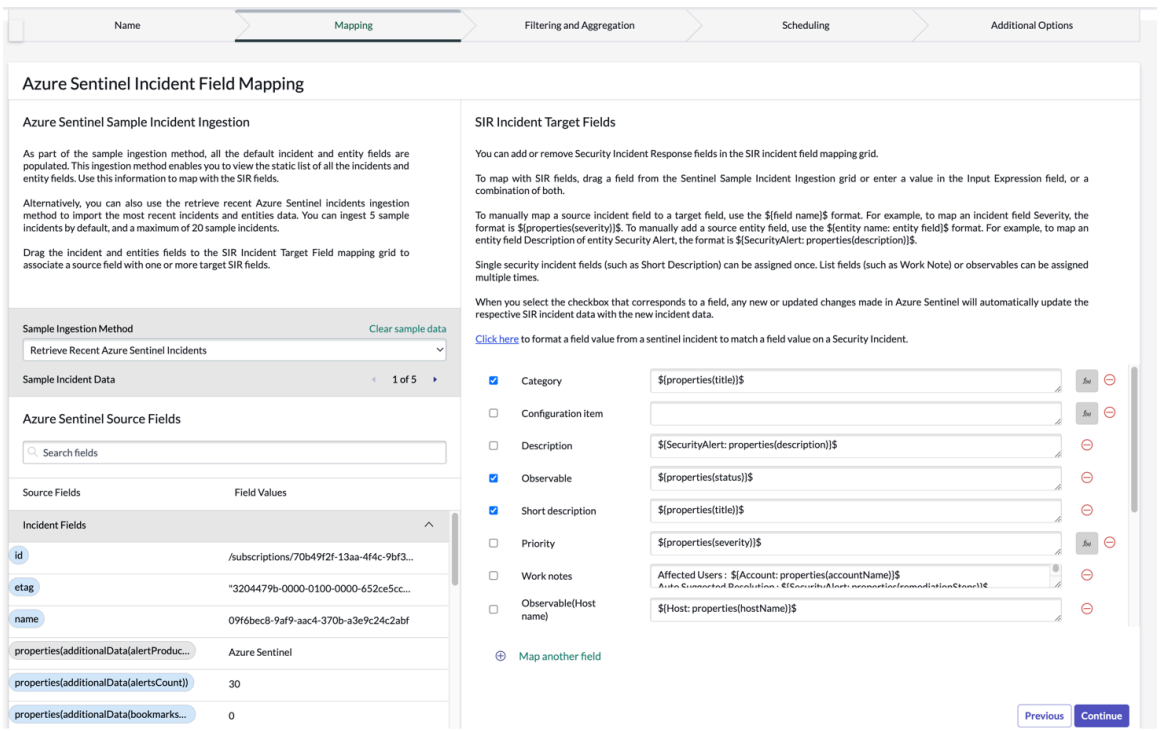
Méthodes d'intégration des exemples

Champ	Description
Tous les champs d'incident et d'entité par défaut	Utilisez cette méthode d'ingestion pour afficher la liste statique de tous les champs d'incidents et d'entités. Cette méthode contient uniquement des noms de champs par défaut sans valeur. Vous pouvez utiliser ces informations pour mapper avec les SIR champs.
Récupérer les incidents Azure Sentinel récents	Utilisez cette méthode d'ingestion pour importer les données d'incidents et d'entités les plus récentes. Si l'incident Azure Sentinel contient les données de l'entité, les données de l'entité sont récupérées et disponibles pour le mappage dans la section Champs sources Azure Sentinel. Parfois, l'incident Azure Sentinel peut ne pas contenir les données d'entité, et par conséquent, les champs d'entité ne sont pas disponibles pour le mappage dans un tel scénario. Si l'incident Azure Sentinel contient plusieurs alertes, la première alerte faisant partie de l'incident s'affiche dans la section de mappage. Lors de l'ingestion également, les premières valeurs de champ d'alerte de sécurité seront utilisées. Vous pouvez ingérer 5 échantillons d'incidents par défaut et un maximum de 20 échantillons d'incidents. Les valeurs de champ d'échantillon d'incident sont renseignées lorsque le profil ingère les exemples d'incidents. Vous pouvez mapper ces incidents aux **champs cibles d'incidents SIR**. Les champs et les valeurs d'incident s'affichent sous forme d'onglets individuels.
Importer un échantillon de données	Cliquez sur **Importer des données témoins** pour importer des exemples d'incidents à partir d'Azure Sentinel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Ce bouton s’affiche lorsque vous sélectionnez la méthode d’ingestion Récupérer les incidents Azure Sentinel récents. La récupération d’échantillons d’incidents à partir du Microsoft Azure Sentinel serveur peut prendre un moment. Mappez ces incidents récupérés aux **champs cibles d’incidents SIR**. Les champs et les valeurs d’incident s’affichent sous forme d’onglets individuels.



2. Pour ajouter des champs aux champs par défaut affichés dans l’incident de sécurité, procédez comme suit :

a. Dans la section Champs cibles d’incidents SIR, cliquez sur le Map another field Bouton Mapper un autre champ.
Il affiche une liste de champs, à partir desquels SIR vous pouvez sélectionner un champ pour un nouveau champ à afficher.

b. Dans la colonne Incident de sécurité, développez la liste qui s’affiche, puis sélectionnez un champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Plusieurs observables peuvent être affichés sur le même incident de sécurité. Par exemple, le champ **Observable** peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs **Élément de configuration** et **Notes de travail** prennent en charge plusieurs valeurs. Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, vous voyez un message d'erreur indiquant que ce champ ne prend pas en charge plusieurs valeurs. De même, si un champ d'un incident de sécurité comporte une liste dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste, le champ n'est pas renseigné sur l'incident de sécurité.

c. Dans la section Champs sources Azure Sentinel, faites glisser et déplacez votre champ pour le mapper à votre nouveau champ.

d. Lorsque vous cochez la case correspondant à un champ, toutes les modifications nouvelles ou mises à jour apportées dans Azure Sentinel mettent automatiquement à jour les données d'incident SIR respectives avec les nouvelles données d'incident.

Remarque : Dans le système de base, la propriété système sn_sec_sentinel.incident_updates est définie par défaut sur Vrai pour recevoir les Microsoft Azure Sentinel mises à jour relatives aux nouvelles alertes liées à SIR.

- Par défaut, les champs Utilisateurs affectés, Éléments de configuration et Observables sont cochés. Cela signifie que chaque fois que de nouveaux observables ou éléments de configuration associés, ou des utilisateurs affectés sont ajoutés à l'incident, ces informations sont automatiquement extraites et renseignées dans les listes connexes respectives dans Security Incident Response (SIR) au cours de cet intervalle d'interrogation.
- Pour tous les autres champs, vous devez cocher la case correspondant à un champ pour tous les changements nouveaux ou mis à jour apportés à l'enregistrement d'incident Azure Sentinel dans Azure Sentinel. Cela met automatiquement à jour les données d'incident SIR respectives avec les nouvelles données d'incident.

Important : Une diligence raisonnable doit être effectuée avant de sélectionner cette fonctionnalité, car le remplacement des données existantes peut entraîner des données instables pour l'analyste et toute autre automatisation définie même par les valeurs de champ de l'incident de sécurité peut également être affectée. Il est donc très important de faire preuve de diligence raisonnable avant de sélectionner une fonctionnalité de remplacement.

3. Pour supprimer un champ, utilisez le ⊖ en regard du champ d'expression d'entrée dans la section Champs cibles de l'incident SIR.

4. Pour mapper une valeur de champ de la section Champs sources Azure Sentinel à un champ de la section Champs cibles de l'incident SIR, utilisez l'une des actions suivantes :

a. Faites glisser le nom du champ (par exemple, l'ID) et déposez-le à côté d'un nom de champ dans la colonne Champs cibles de l'incident SIR.

Vous pouvez faire correspondre n'importe quelle valeur de la section Champs sources Azure Sentinel à un champ de la section Champs cibles des incidents SIR. Les champs sont codés par couleur afin que vous ne négligez pas ou ne dupliquiez pas les champs d'incident dans le processus de mappage. Les champs bleu clair indiquent qu'un champ d'incident n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ d'incident entrant à plusieurs champs d'un incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

mappé à un champ de l'incident de sécurité. De cette façon, vous pouvez visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations d'incident importantes restantes restent non mappées.

b. Vous pouvez ajouter une combinaison de texte et de champ.
Par exemple, le nom de l'incident est ${name}$. Ici, le nom de l'incident peut être saisi manuellement tandis que ${name}$ est mappé à partir de la section Champs sources Azure Sentinel.

c. Vous pouvez saisir manuellement un champ d'incident source ou d'entité et le mapper à un champ cible.

- Pour mapper manuellement un champ d'incident source, utilisez le format ${nom de champ}$. Par exemple, pour mapper la gravité d'un champ d'incident, le format est ${properties(severity)}$.
- Pour ajouter manuellement un champ d'entité source, utilisez le format ${nom de l'entité : champ d'entité}$. Par exemple, pour mapper un champ d'entité Description de l'entité Alerte de sécurité, le format est ${SecurityAlert : properties(description)}$.

Cette intégration classe certains sous-types d'observables. Lorsque vous mappez un champ Azure Sentinel avec le champ observable SIR, l'observable ServiceNow AI Platform classifie automatiquement l'observable. Si vous souhaitez mapper de manière générique l'observable Azure Sentinel entrant au type d'observable dans SIR, faites glisser et déplacez le champ Azure Sentinel dans le champ Observable. Toutefois, si vous connaissez le type d'observable pour l'observable Azure Sentinel entrant dans SIR, effectuez un mappage spécifique au champ Type d'observable SIR . Voici quelques exemples de types SIR d'observables spécifiques dans : Observable (nom de domaine), Observable (adresse e-mail), Observable (adresse IP (V4)) et Observable (nom d'hôte).

Si vos champs Azure Sentinel entrants contiennent des MITRE-ATT&CK informations, mappez-les MITRE-ATT&CK au champ Technique. Assurez-vous que le champ Azure Sentinel entrant contient l'ID ou le nom de la MITRE-ATT&CK technique.

Parfois, les valeurs des champs d'incident ne Microsoft Azure Sentinel se traduisent pas directement dans les champs de l'incident de sécurité SIR. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques.

5. Pour formater la traduction d'un nouveau champ à partir d'un incident Azure Sentinel afin qu'il corresponde à une valeur de champ d'un incident de sécurité, cliquez sur le lien **Cliquez ici** dans l'en-tête des **champs cibles de l'incident SIR** .

6. Pour modifier les champs qui prennent en charge la traduction de champ, cliquez sur l'icône Traduction de champ du  de champ.
Les champs qui prennent en charge la traduction des champs sont **Catégorie**, **Élément de configuration** et **Priorité**. Par exemple, cliquez sur l'icône du  à côté de la catégorie. L'éditeur de script de traduction de champ Azure Sentinel s'ouvre.

7. Entrez les modifications apportées au script, cliquez sur **Mettre à jour** pour enregistrer les modifications et revenir à la page Mappage.
Par exemple, pour Catégorie, définissez les éléments suivants dans l'éditeur de script :

```
"<Incoming Sentinel Incident Field Value>" : "<Category to assign to the Security Incident>".
```

Ce mappage garantit qu'un profil n'utilise que des catégories configurées.

8. Poursuivez votre mappage en ajoutant ou en supprimant des valeurs de champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir des critères supplémentaires qu'un incident entrant doit satisfaire pour créer un incident de sécurité.

9. Pour passer à la section Filtrage et agrégation, cliquez sur **Continuer**.

Que faire ensuite

Définissez et définissez des conditions de filtre afin de pouvoir spécifier quels incidents doivent créer des incidents de sécurité. Vous pouvez utiliser les mêmes valeurs de champ (définies dans la section Mappage) dans le générateur de conditions de génération d'incident (dans la section Filtrage et agrégation) pour définir des critères supplémentaires qu'un incident entrant doit satisfaire pour créer un incident de sécurité.

Définition des critères de filtre et d'agrégation

Vous pouvez définir et définir des conditions de filtre afin de spécifier quels incidents entrants Microsoft Azure Sentinel doivent provoquer des incidents de sécurité. Vous pouvez également définir des critères de champ d'incident supplémentaires qui permettent d'ajouter un incident entrant à un incident de sécurité ouvert au lieu de créer un incident.

Définir les conditions de filtrage pour les incidents de sécurité

Définissez les conditions de filtrage afin que les incidents de sécurité ne soient créés que lorsque les conditions de filtrage correspondent.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Ce type de filtrage vous aide à isoler les incidents de sécurité et limite le nombre d'incidents de sécurité que vous créez. Si vous définissez des critères de filtrage supplémentaires, seuls les incidents requis sont ingérés sans avoir à modifier la requête ou la configuration de l'incident déclenché.

Procédure

1. Pour définir les critères qu'un incident entrant Microsoft Azure Sentinel doit satisfaire pour qu'un incident de sécurité soit créé, sélectionnez **Filtre basé sur les conditions**.

   Les options du premier champ des Conditions de filtre correspondent aux champs affichés dans la section d'ingestion d'incidents d'exemple Azure Sentinel pour l'incident que vous avez ingéré. Ces champs sont dynamiques et changent en fonction de l'incident que vous ingérez. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.

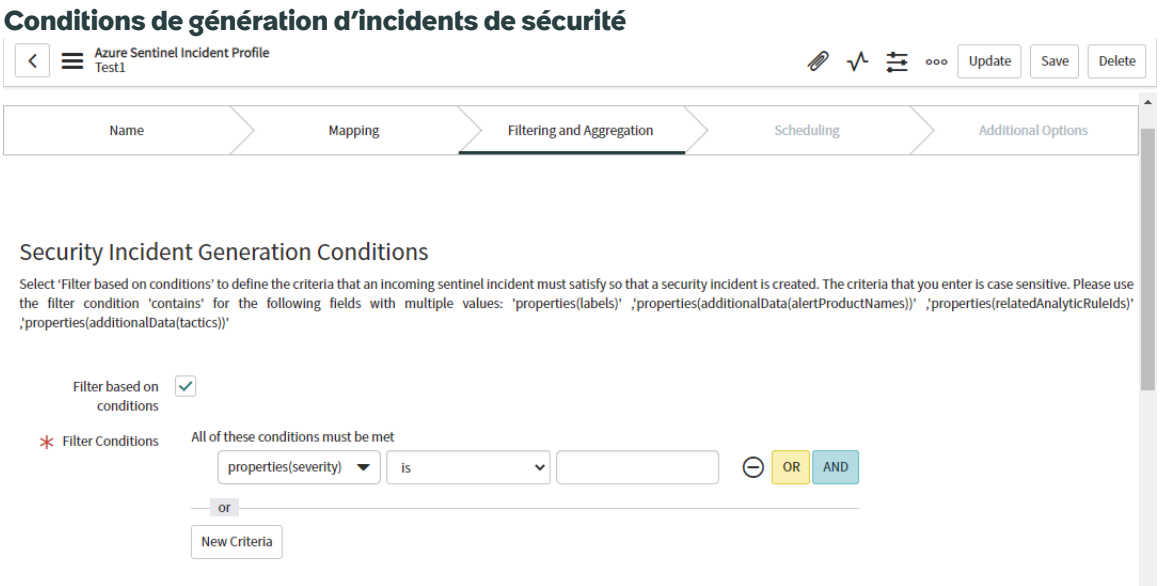
   Utilisez la condition *`de filtre contenue`* pour les champs suivants à valeurs multiples :

   - properties(labels)
   - properties(additionalData(alertProductNames))
   - properties(relatedAnalyticRuleIds)
   - properties(additionalData(tactics))

   Étant donné que la condition de filtre ne peut récupérer que des chaînes, vous devez utiliser la condition de filtre *`contient`* pour les champs ci-dessus afin de vous assurer que les données sont filtrées correctement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres pour la première ligne.
3. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.

Définir les conditions d'agrégation

Définissez des critères d'agrégation d'incidents supplémentaires qui regroupent un incident entrant à un incident de sécurité SIR existant au lieu de créer des incidents similaires, potentiellement en double. Lorsque vous utilisez des critères de valeur de correspondance de champ pour chaque profil, cette agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'incidents connexes sur un seul incident de sécurité.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Si un nouvel incident correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation de l'étape de mappage, l'incident est automatiquement ajouté à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher tous les incidents agrégés ajoutés sur une liste connexe sur un incident de sécurité.

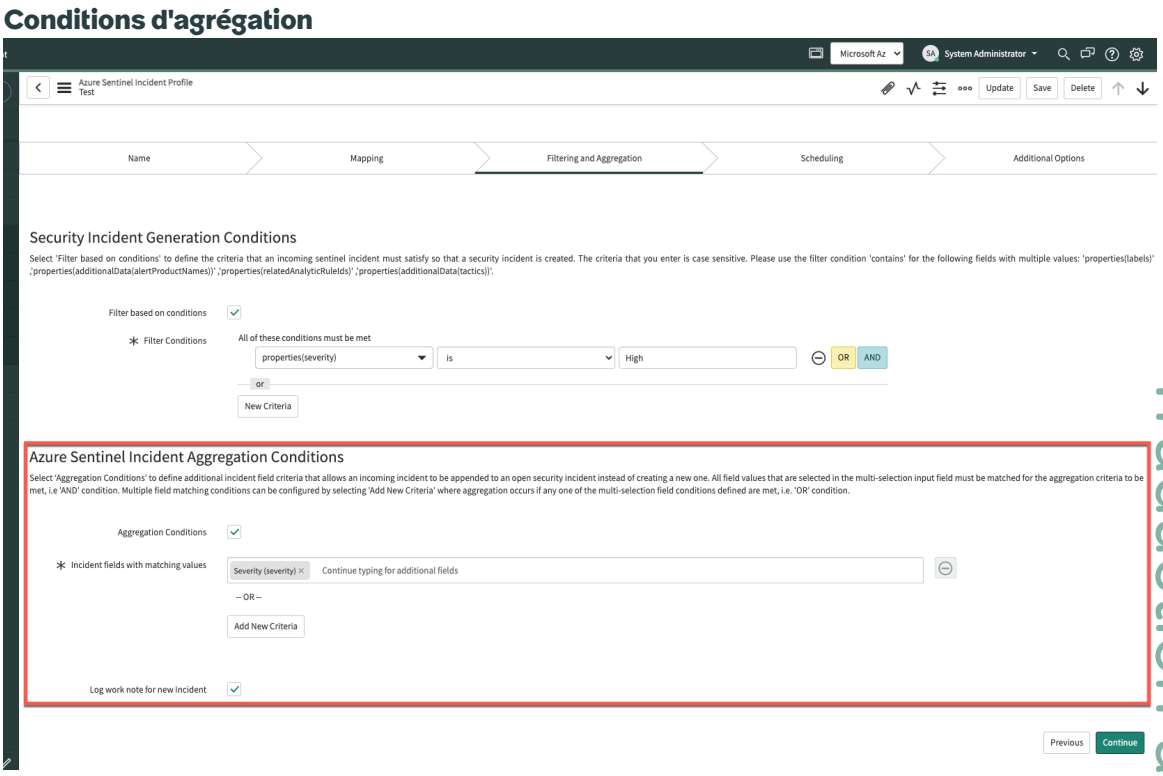
Tous les incidents regroupés sur un incident de sécurité sont affichés dans la liste connexe des incidents regroupés Azure Sentinel. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi des incidents s'ajoutent aux incidents de sécurité existants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour définir des critères de champ d'incident supplémentaires qui permettent d'ajouter un incident entrant Microsoft Azure Sentinel à un incident de sécurité ouvert au lieu de créer un nouvel incident, sélectionnez l'option **Conditions d'agrégation** , comme illustré dans la figure suivante.



2. Dans le champ **Champs d'incidents avec valeurs correspondantes** , saisissez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre ServiceNow AI Platform instance.
   Toutes les valeurs de champ que vous avez sélectionnées dans le champ d'entrée de sélection multiple doivent correspondre afin que les critères d'agrégation soient remplis et que cet incident entrant puisse être ajouté à un incident de sécurité existant. Cette sélection implique qu'il s'agit d'une condition *ET* dans laquelle des champs, tels que des observables et des éléments de configuration qui peuvent avoir plusieurs valeurs de champ, leur sont mappés. Si seul un sous-ensemble de valeurs correspond, les conditions d'agrégation d'incidents Azure Sentinel ne sont pas remplies et un nouvel incident de sécurité est créé.
3. Pour ajouter plusieurs conditions de correspondance de champ, cliquez sur **Ajouter un nouveau critère**
   L'agrégation se produit si l'une ou l'autre des conditions de champ de sélection multiple que vous définissez est remplie. Cette sélection implique la condition *OU* .
4. Pour mettre à jour la note de travail d'un nouvel incident lorsqu'elle est ajoutée à un incident de sécurité, sélectionnez **Enregistrer la note de travail pour le nouvel incident**.

   La note de travail indique qu'un nouvel incident est ajouté et comprend un lien vers les détails de l'incident. La note de travail du journal met également à jour d'autres détails que vous ajoutez au champ note de travail dans votre section de mappage.
5. Pour configurer le calendrier, cliquez sur **Continuer**.

Que faire ensuite

Définissez un calendrier pour récupérer les données d'incident et les incidents ingérés qui correspondent aux critères du profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Planifier la récupération de l'incident Microsoft Azure Sentinel

Définissez un calendrier pour récupérer les données d'incident et ingérer les Microsoft Azure Sentinel incidents qui correspondent aux critères du profil.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier la fréquence à laquelle vous souhaitez interroger les incidents futurs Microsoft Azure Sentinel qui correspondent à la configuration de profil d'incident.

Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Pour définir une date et une heure spécifiques pour l'ingestion initiale, activez l'option **Définir le délai d'ingestion des incidents**. L'ingestion suivante est basée sur la période de l'intervalle d'interrogation.

L'intervalle d'interrogation est configuré individuellement pour chaque profil. Les différents intervalles d'interrogation peuvent avoir un impact sur les performances de l'intégration Microsoft Azure Sentinel des incidents. Lors de la planification, prévoyez d'équilibrer la charge du système par rapport à l'urgence d'un incident. Une valeur par défaut d'une minute est définie pour tous les profils. Vous pouvez modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

Toutes les alertes qui sont ajoutées à l'incident dans un intervalle d'interrogation particulier sont exécutées par un processus, puis ajoutées aux listes connexes d'alertes Azure Sentinel et une note de travail est également publiée.

Procédure

1. Renseignez les champs du formulaire de planification.

   Configurez le calendrier pour définir comment et quand extraire les Microsoft Azure incidents du locataire.

   Formulaire de planification

Champ	Description
Intégration de l'incident en cours	Ingestion d'incident en cours que l'instance ServiceNow AI Platform extrait du Microsoft Azure locataire pour les nouveaux incidents. Les incidents de sécurité sont créés si des incidents déclenchés sont détectés et que les critères de filtrage de génération d'incidents correspondent.
Incrémentation du sondage (minutes)	Fréquence d'interrogation définie en minutes.
Définir le délai d'intégration de l'incident	Ingestion d'incident basée sur la date et l'heure configurées. Vous pouvez utiliser cette option pour définir une date et une heure spécifiques pour l'ingestion initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Délai d'intégration de l'incident d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.
Récupération ponctuelle	Cochez cette case pour permettre la récupération unique des incidents Azure Sentinel historiques, puis procédez au rapprochement des données. Lorsque vous sélectionnez ce point de cochage, l'application extrait tous les incidents Azure Sentinel ouverts et fermés pour la période allant jusqu'à 6 mois environ. Lors du traitement des données, les incidents en cours et les données historiques sont tous deux extraits, mais le traitement des incidents en cours prime sur l'extraction historique et, dans le cas contraire, l'extraction historique peut prendre un certain temps en fonction de la durée et du nombre d'incidents que vous ingérez. **Remarque :** Les incidents Azure Sentinel historiques récupérés sont soumis à des contrôles de déduplication afin d'éviter tout doublon dans l'application Réponse aux incidents de sécurité.
Depuis date	Date depuis laquelle les incidents historiques sont ingérés à partir d'Azure Sentinel. **Remarque :** Les données d'incident sont extraites approximativement des 6 derniers mois.

La page de planification vous permet de définir comment et quand les incidents sont extraits du Microsoft Azure locataire.

2. Pour accéder à la page Options supplémentaires, cliquez sur **Continuer**.

Automatiser les mises à jour et les fermetures d'incidents en fonction de l'état de l'incident SIR

Automatisez les mises à jour et les fermetures d'incidents en fonction de l'état de l'incident SIR . L'intégration Microsoft Azure Sentinel dispose d'une interface bidirectionnelle qui permet aux incidents de créer des incidents de sécurité et de mettre à jour les incidents après la création ou la fermeture de l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Renseignez les champs du formulaire.
   Suivez les instructions pour terminer la configuration de la mise à jour des incidents lorsque vous créez ou fermez un incident de sécurité dans SIR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Automatisation du formulaire de mise à jour des incidents

Catégorie	Champ	Description
Mises à jour de création d'incident	Mettre à jour l'état des incidents Azure Sentinel lors de la création de l'incident SIR	Option qui vous permet d'utiliser la fonctionnalité de mise à jour automatisée des incidents. L'état Microsoft Azure Sentinel de l'incident est mis à jour dans Microsoft Azure l'incident avec les commentaires après la création de l'incident SIR dans le ServiceNow AI Platform.
	Mise à jour du statut de l'incident initial	État de l'incident initial mis à jour dans l'environnement Microsoft Azure Sentinel . Vous pouvez sélectionner **Nouveau** ou **Actif** comme état.
	Commentaires initiaux renvoyés à l'incident	Commentaires initiaux publiés sur l'incident dans l'environnement Microsoft Azure Sentinel . Modifiez le texte par défaut qui s'affiche dans la section Commentaires en ajoutant ou en modifiant les variables de substitution à l'aide du format ${nom de champ}$ pour n'importe quel champ du formulaire d'incident SIR .
Mises à jour de la clôture de l'incident	Fermer les incidents Azure Sentinel lors de la fermeture de l'incident SIR	Option qui vous permet d'utiliser la fonctionnalité de mise à jour automatique de l'état des incidents. Microsoft Azure Sentinel Les incidents sont fermés dans l'incident Microsoft Azure avec les commentaires donnés après la fermeture de l'incident SIR dans le ServiceNow AI Platform.
	Mise à jour du statut de l'incident de fermeture	Mise à jour de l'état de l'incident lorsque l'incident Microsoft Azure Sentinel est fermé en SIR.
	Commentaires de fermeture renvoyés à l'incident	Commentaires qui sont publiés sur l'incident dans l'incident Microsoft Azure Sentinel lorsque l'incident est fermé dans SIR. Modifiez le texte par défaut qui s'affiche dans la section Commentaires en ajoutant ou en modifiant les variables de substitution à l'aide du format ${nom de champ}$ pour n'importe quel champ du formulaire d'incident SIR .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

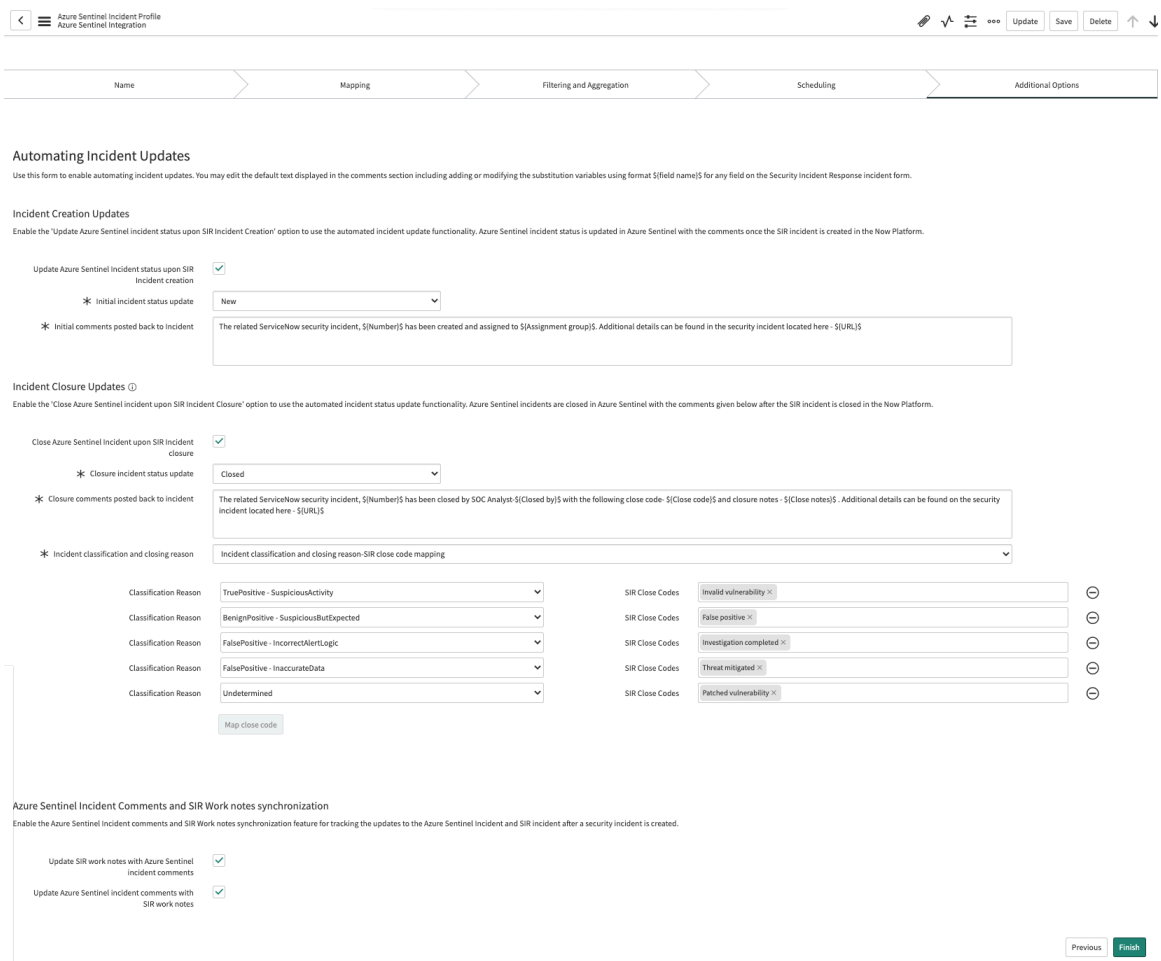
Catégorie	Champ	Description
	Classification des incidents et motif de fermeture	Méthode de classification des incidents et de motif de fermeture utilisée pour fermer l'incident dans l'environnement Microsoft Azure Sentinel . Sélectionnez la **méthode de classification et de motif de fermeture des incidents par défaut** pour fermer l'incident dans l'environnement Microsoft Azure Sentinel . Lorsque vous sélectionnez cette méthode, vous devez définir la **classification des incidents et le motif de fermeture par défaut**. Lorsque vous fermez un incident dans SIR, l'état de l'incident dans Azure Sentinel est également fermé avec la **classification des incidents par défaut et le motif de fermeture** spécifiés. Sélectionnez la méthode de **mappage Classification des incidents et code de fermeture du SIR** pour fermer les incidents et mapper les motifs de classification avec les SIR codes de fermeture. Vous pouvez mapper plusieurs SIR codes de fermeture à un seul motif de classification. Une fois que vous avez fermé un incident à SIR l'aide du code de fermeture, l'état de l'incident dans Azure Sentinel est également fermé avec la classification des incidents et le motif de fermeture mappés. Si le motif de classification et SIR les codes de fermeture ne sont pas mappés, ou si aucune correspondance n'est trouvée, l'incident est fermé en utilisant le motif de classification par défaut « indéterminé » dans l'environnement Microsoft Azure Sentinel .
Synchronisation des commentaires d'incidents Azure Sentinel et des notes de travail SIR	Mettre à jour les notes de travail SIR avec les commentaires sur l'incident Azure Sentinel	Option que vous pouvez sélectionner pour mettre à jour vos Microsoft Azure Sentinel commentaires dans les notes de SIR travail. Le commentaire dans les SIR notes de travail apparaît avec le préfixe `Commentaire de Sentinel`. Le commentaire contient également

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catégorie	Champ	Description
		l’ID Sentinel, les détails de l’analyste et l’horodatage.
	Mettre à jour les commentaires sur l'incident Azure Sentinel avec les notes de travail SIR	Option que vous pouvez sélectionner pour mettre à jour vos SIR notes de travail dans les commentaires sur l’incident Microsoft Azure Sentinel . Le commentaire apparaît Microsoft Azure Sentinel avec le préfixe `Commentaire de ServiceNow`.

L’exemple suivant montre les options de configuration disponibles pour automatiser les mises à jour des incidents.



Traduction automatique

2. Cliquez sur **Terminer**.

Que faire ensuite

Le profil passe à l’état En attente. Lorsque le message de confirmation indique que l’installation et la configuration sont terminées, vous pouvez activer le profil.

Copier un Microsoft Azure Sentinel profil

Copiez un profil existant et ses paramètres associés au lieu de créer un profil. Lorsque vous créez plusieurs profils, vous pouvez réutiliser les paramètres d’un profil existant en copiant ces profils.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

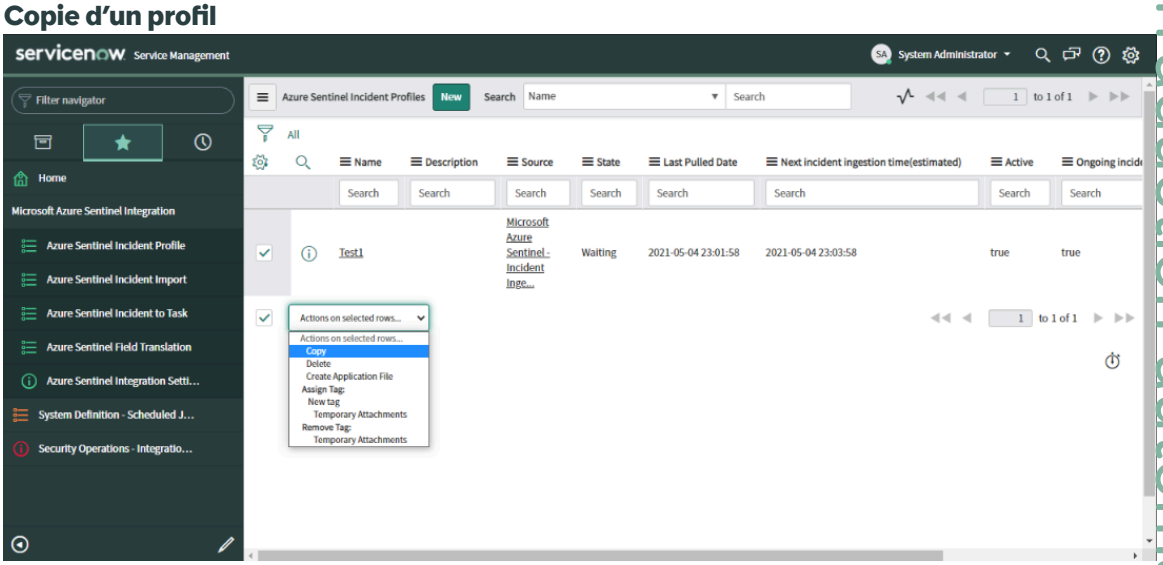
Pourquoi et quand exécuter cette tâche

Lorsque vous copiez un profil, le nom du profil est initialement modifié pour éviter de créer des profils en double. Le profil copié est également désactivé (défini sur faux) pour vous assurer que vous ne l'activez pas accidentellement avant de terminer la configuration. Vous pouvez copier les profils et utiliser les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

1. Accédez à la **Tous** > **Intégration de Microsoft Azure Sentinel** > **Profil Azure Sentinel**.
2. Dans la liste des profils Azure Sentinel, sélectionnez un profil que vous souhaitez copier, puis dans la liste Actions sur les lignes sélectionnées, cliquez sur **Copier** comme illustré dans l'exemple suivant.

Copie d'un profil

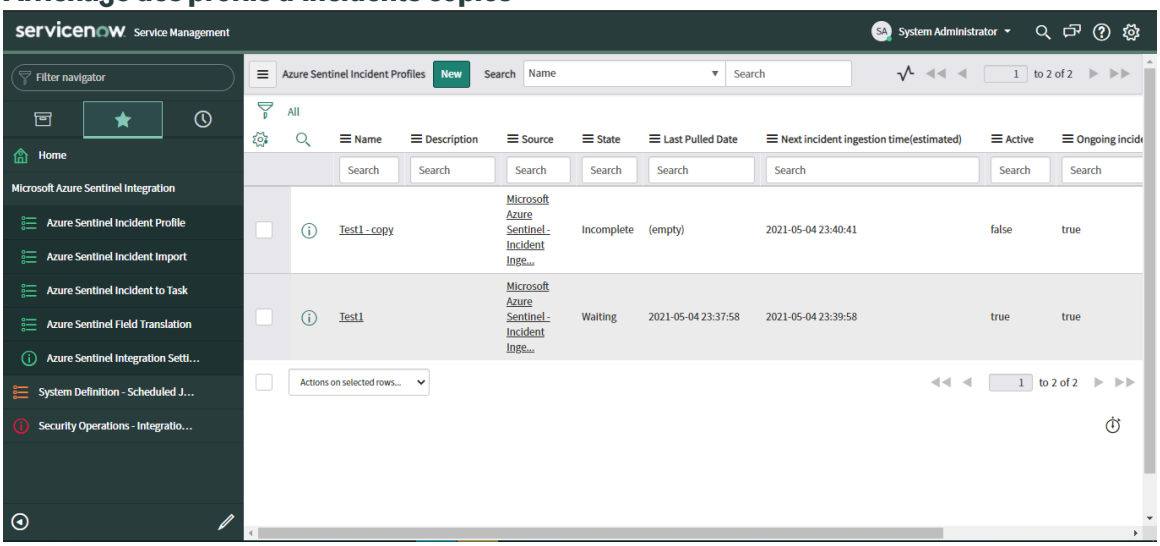


Le profil est copié et affiché dans la liste, comme illustré dans l'exemple suivant. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient le mot « copier ». Bien que le profil d'origine soit activé (vrai), la copie est désactivée à ce stade (faux). Vous préférez peut-être modifier les valeurs du profil copié et les renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des profils d'incidents copiés



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. L'état de la colonne Actif est défini sur faux, ce qui signifie que le profil doit être activé.

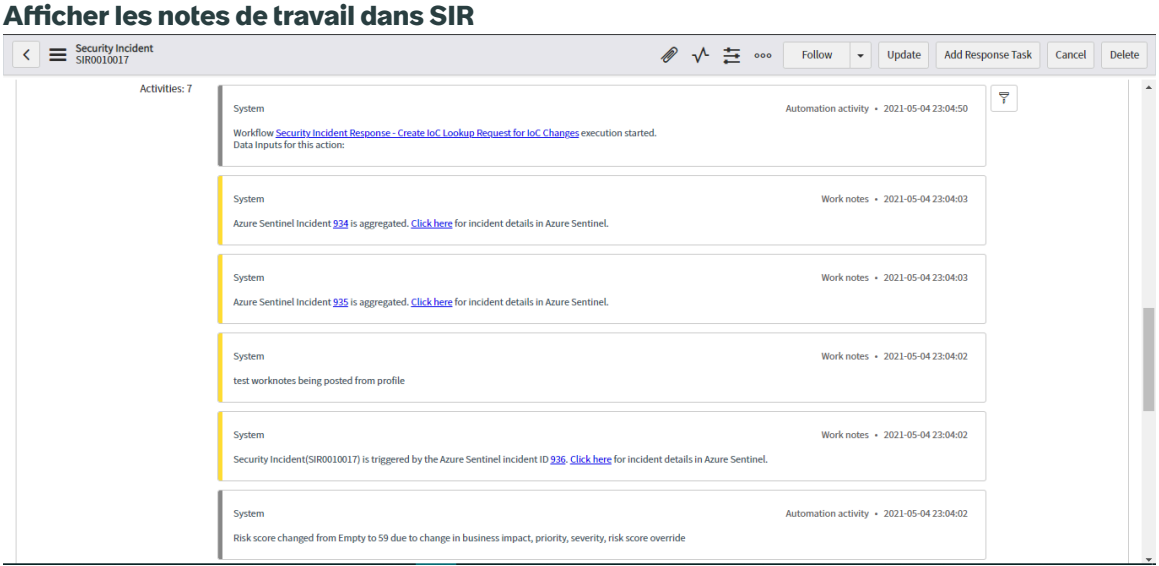
SIR formulaire après une ingestion d'incident

Une fois l'incident ServiceNow AI Platform ingéré, un incident de Microsoft Azure Sentinel sécurité est créé et des mises à jour sont apportées à cet enregistrement d'incident de sécurité.

Notes de travail

Une note de travail est publiée lorsqu'un incident est regroupé et si vous avez configuré l'option **Consigner la note de travail pour le nouvel incident** dans les critères d'agrégation d'incidents. L'exemple suivant montre les notes de travail dans SIR.

Afficher les notes de travail dans SIR



Lorsque vous cliquez sur le numéro d'incident, vous pouvez afficher l'enregistrement d'importation d'incident interne qui contient les données brutes de l'incident. L'exemple suivant montre les données brutes d'incident dans SIR.

Traduction automatique

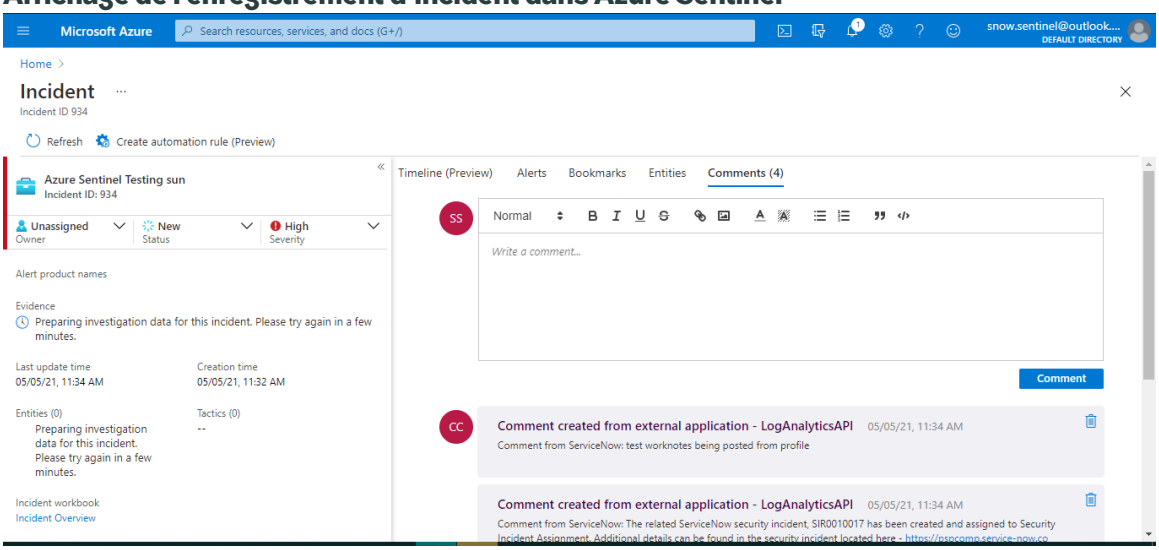
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les données brutes de l'incident dans SIR



Lorsque vous cliquez sur le lien **Cliquer ici** , vous pouvez afficher l'enregistrement dans l'environnement Microsoft Azure Sentinel . L'exemple suivant montre l'enregistrement dans l'environnement Microsoft Azure Sentinel .

Affichage de l'enregistrement d'incident dans Azure Sentinel

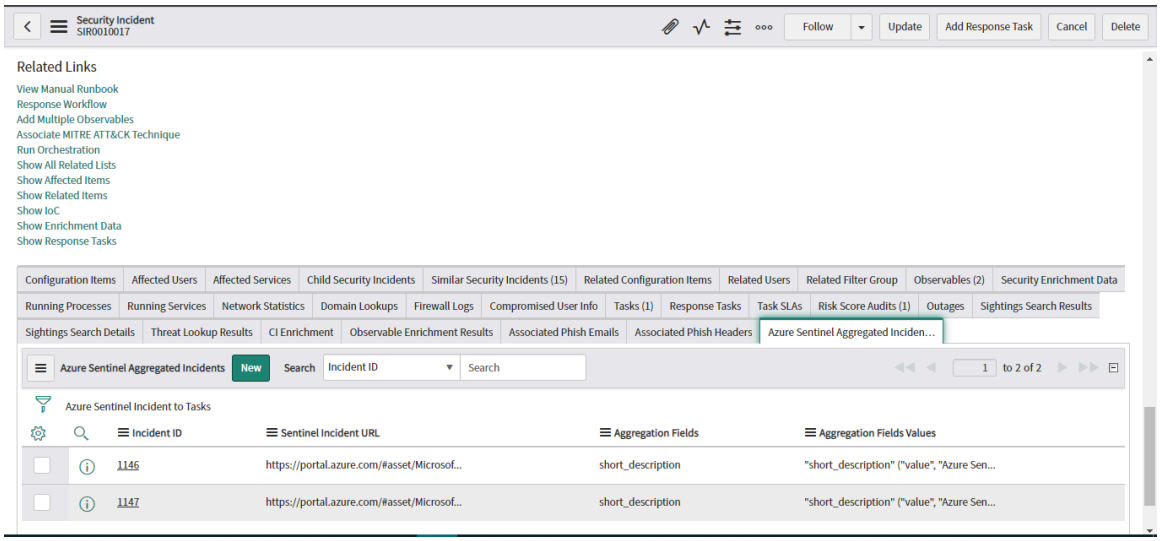


Incidents Sentinel regroupés

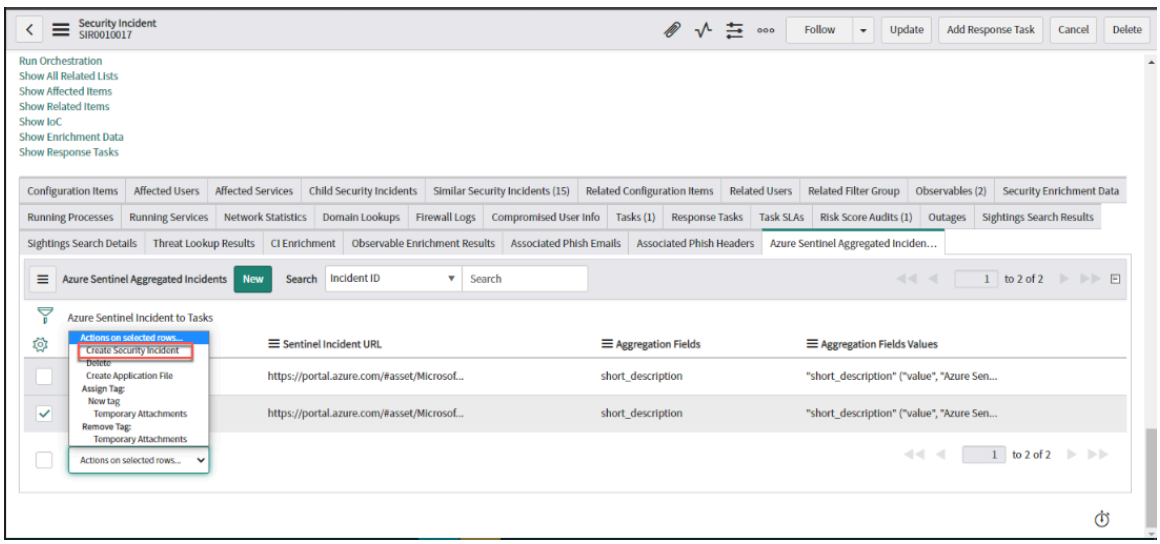
Affichez les incidents Sentinel agrégés : Affichez les incidents qui sont regroupés à l'incident de sécurité. Accédez à la **Afficher toutes les listes connexes** > **Incidents Microsoft Azure Sentinel regroupés**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Créer un incident de sécurité : Sélectionnez un incident dans la liste, cliquez sur le menu **Actions** , puis sur **Créer un incident de sécurité**. Cette option crée un nouvel incident de sécurité pour l'incident et cet incident est désagrégé de l'incident de sécurité parent.



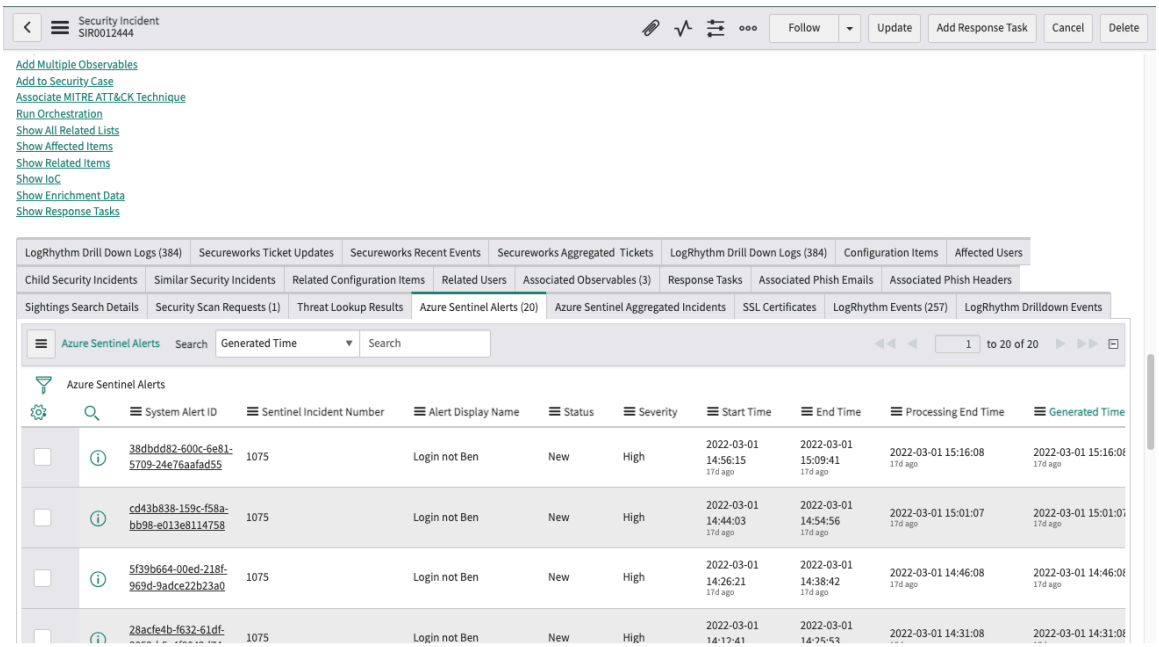
Alertes Azure Sentinel

Pour afficher les alertes associées à l'incident Sentinel qui a déclenché l'incident de sécurité, accédez à **Afficher toutes les listes connexes** > **Alertes Azure Sentinel**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Alertes Azure Sentinel



Passer en revue les paramètres d'intégration Microsoft Azure Sentinel

Examinez les paramètres d'intégration Microsoft Azure Sentinel afin de pouvoir modifier les propriétés système en fonction de votre environnement.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Accédez à la **Tous** > **Intégration de Microsoft Azure Sentinel** > **Paramètres de l'intégration d'Azure Sentinel**.
2. Modifiez les paramètres suivants selon vos besoins.

Microsoft Azure Sentinel Paramètres d'intégration

Nom de la propriété	Description
Appliquer une limite au nombre de jours pour lesquels des données d'échantillon peuvent être extraites. sn_sec_sentinel.max_nombre_de_jours_pour_données_de_l'échantillon	Nombre maximal de jours pendant lesquels vous pouvez extraire des exemples de données de l'environnement Microsoft Azure Sentinel . Type : entier Valeur par défaut : 7
Recevez des mises à jour relatives aux nouvelles alertes liées à SIR. sn_sec_sentinel.incident_updates	Activez l'option pour recevoir les mises à jour des incidents. Type : booléen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété	Description
	Valeur par défaut : true
Le caractère du délimiteur pour diviser les valeurs dans Microsoft Azure Sentinel les mappages de champs. sn_sec_sentinel.delimiter	Le caractère du délimiteur pour diviser les valeurs dans Microsoft Azure Sentinel les mappages de champs. Type : chaîne Valeur par défaut : ', ' (virgule avec espace)
Appliquer une limite au nombre d'échantillons d'incidents pouvant être extraits. sn_sec_sentinel.max_num_of_sample_incident_per_call	Nombre maximal d'échantillons d'incidents que vous extrayez de l'environnement pour l'ingestion Microsoft Azure Sentinel . Type : nombre entier Valeur par défaut : 5 Valeur maximale de l'échantillon : 20
Appliquez une limite au nombre d'incidents sentinel qui peuvent être regroupés en un seul incident. sn_sec_sentinel.max_agrégations_per_si	Limite d'agrégation d'incidents pour un incident de sécurité. Par exemple, s'il y a 102 incidents, les 100 premiers sont regroupés en incident_1 de sécurité et les 2 autres en incident_2 de sécurité. Type : nombre entier Valeur par défaut : 100
Appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés dans une période de 24 heures. sn_sec_sentinel.max_si_per_day	Nombre maximal d'incidents de sécurité pouvant être créés dans un délai de 24 heures dans le ServiceNow AI Platform. Type : nombre entier Valeur par défaut : 1 000
Limite maximale de pagination pour l'extraction des données d'incident dans un appel REST. sn_sec_sentinel.max_taille_page_	Limite de pagination pour l'extraction des données d'incident dans un appel REST à partir de l'environnement Microsoft Azure Sentinel . Type : nombre entier Valeur par défaut : 100
Valeur de version de l'API pour les incidents. sn_sec_sentinel.sentinel_security_incident_api_version	Version de l'API Microsoft pour la récupération des incidents Sentinel. Valeur par défaut : 01/10/2021
Valeur de version de l'API pour les alertes. sn_sec_sentinel.sentinel_security_alert_api_version	Version de l'API Microsoft pour la récupération des alertes Sentinel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété	Description
	Valeur par défaut : 01/10/2021
Valeur de version de l'API pour les entités. sn_sec_sentinel.sentinel_security_entities_api_version	Version de l'API Microsoft pour la récupération des entités Sentinel. Valeur par défaut : 01/10/2021
sn_sec_sentinel.logging.verbosité	Niveau de verbosité du journal de l'application, c'est-à-dire le nom du type d'information. Vous pouvez également mettre à jour la valeur dans les options suivantes : ○ **erreur** ○ **avertir** ○ **info** ○ **debug** Valeur par défaut : **info**.

3. Cliquez sur **Enregistrer**.
   Vos paramètres d'intégration modifiés sont appliqués dans l'intervalle d'interrogation suivant, tel que défini dans le profil.

Séparation de domaine

L'application Séparation de domaine est prise en charge. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : basique

- Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de service de l'application.
- L'application prend en charge Séparation de domaine lors de l'exécution. Séparation de domaine inclut la séparation à partir de l'interface utilisateur, des clés de cache, du reporting, des déploiements et des agrégations.
- Le propriétaire de l'instance doit configurer l'application de sorte qu'elle fonctionne sur plusieurs locataires.

Exemple de cas d'utilisation : lorsqu'un fournisseur de service (SP) utilise la messagerie instantanée pour répondre au message d'un locataire-client, le client doit pouvoir afficher la réponse du SP.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnement de Séparation de domaine dans l'intégration Microsoft Azure Sentinel

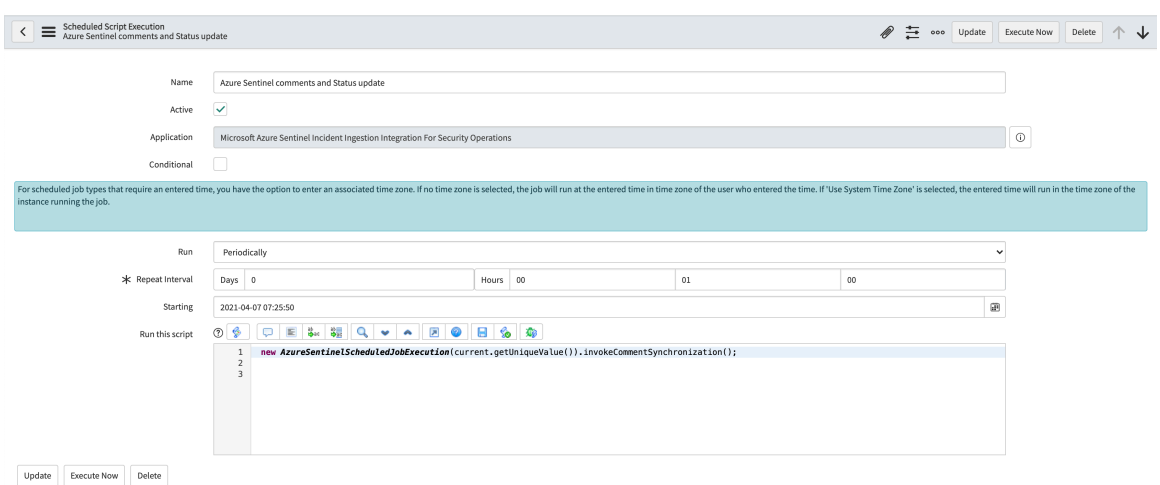
Pour procéder à la séparation en domaines, procédez comme suit :

- Créer un utilisateur avec le rôle sn_si.admin dans le domaine respectif.

  Remarque : Lorsque vous créez le profil, utilisez le sélecteur de domaine pour sélectionner un domaine. Ne créez pas l'utilisateur dans le domaine parent et ne changez pas ultérieurement le domaine du profil. Vous devez avoir un utilisateur pour chaque domaine de votre profil avec le rôle sn_si.admin. Utilisez cet utilisateur pour créer ou modifier des paramètres dans le profil.

- Désactiver les travaux planifiés existants.
- Répliquez les travaux planifiés suivants pour chaque domaine :
  - Azure Sentinel : extraction des alertes et des entités
  - Synchronisation des commentaires Azure Sentinel
  - Mise à jour de l'état d'Azure Sentinel
  - Processus du profil Azure Sentinel
  - Données brutes du processus Azure Sentinel
  - Nettoyage des données Azure Sentinel
  - Extraire le commentaire historique Azure Sentinel
- Changez **l'option Exécuter en tant que de** l'utilisateur système à l'utilisateur disposant du rôle sn_si.admin dans le domaine respectif, puis exécutez la tâche planifiée.

L'exemple suivant montre comment répliquer la tâche de commentaires et de mise à jour d'état Azure Sentinel et exécuter la tâche en tant qu'utilisateur système.



Information associée

Séparation de domaine pour les fournisseurs de services

Comparaison Microsoft Azure Sentinel et API de sécurité Microsoft Graph intégrations avec SIR

Vous pouvez afficher les différences entre Microsoft Azure Sentinel les intégrations et API de sécurité Microsoft Graph choisir celle qui convient à votre ServiceNow AI Platform instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble de Microsoft Azure Sentinel - Ingestion des incidents

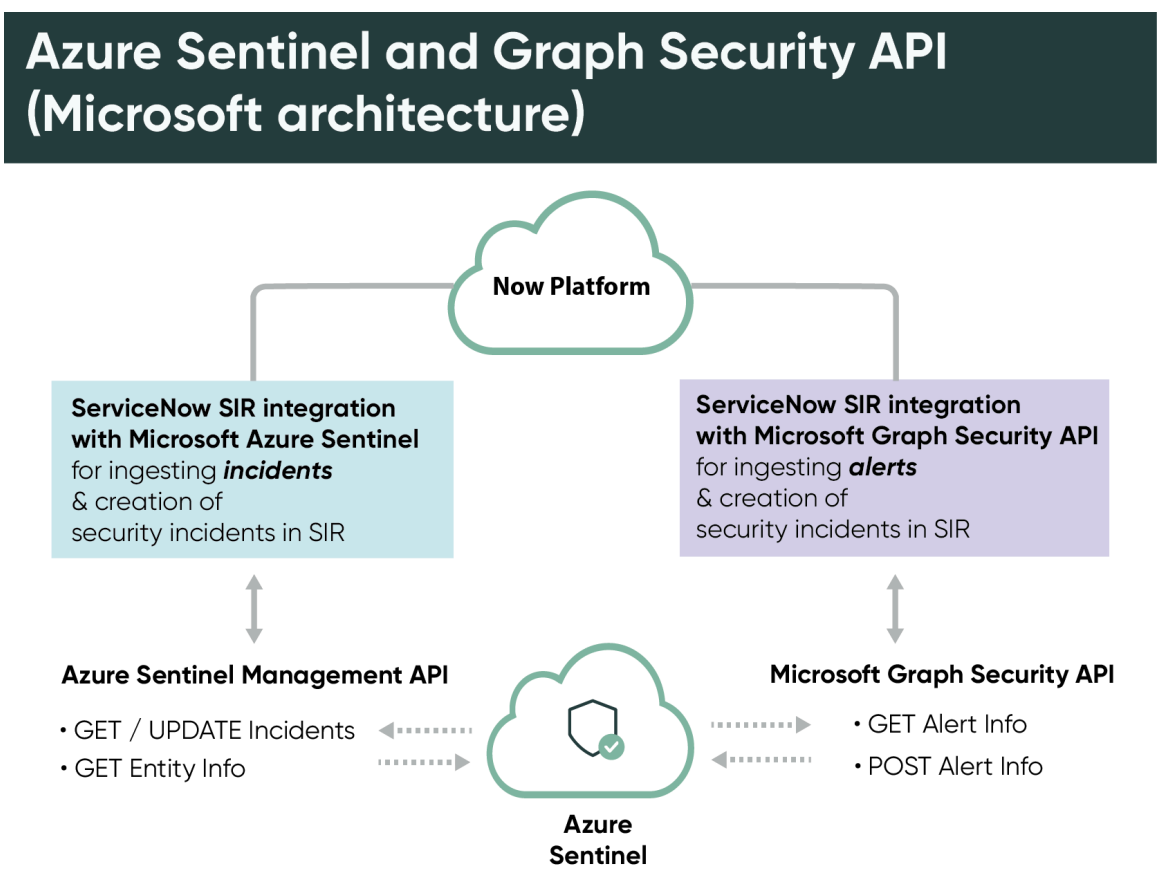
Microsoft Azure Sentinel est une solution SIEM (Security Information Event Management) et Security Orchestration Automated Response (SOAR) basée sur le cloud. Microsoft Azure Sentinel fournit des analyses de sécurité intelligentes et des renseignements sur les menaces dans toute l'entreprise. Il fournit une solution unique pour la détection des alertes, la visibilité des menaces, la chasse proactive et la réponse aux menaces.

Vue d'ensemble de API de sécurité Microsoft Graph

Il s'agit API de sécurité Microsoft Graph d'un service intermédiaire (ou courtier) qui fournit une interface de programmation unique pour connecter plusieurs fournisseurs de sécurité (natifs de Microsoft ainsi que ServiceNow des partenaires).

L'intégration API de sécurité Microsoft Graph résout ces problèmes en utilisant le pour se connecter à différentes technologies de sécurité Microsoft telles qu'Azure API de sécurité Microsoft Graph Sentinel, Microsoft Defender Advanced Threat Protection et Azure Advanced Threat Protection. Les alertes des fournisseurs de sécurité Microsoft sont ingérées et les incidents de sécurité sont automatiquement créés dans Réponse aux incidents de sécurité.

Résumé des différences de fonctionnalités



Microsoft Azure Sentinel Vs API de sécurité Microsoft Graph

Microsoft Azure Sentinel	API de sécurité Microsoft Graph
Ingère les incidents ainsi que les Microsoft Azure Sentinel informations sur les entités (le cas échéant)	Ingère les alertes de plusieurs fournisseurs de sécurité (y compris Azure Sentinel) dans un schéma standard

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Microsoft Azure Sentinel Vs API de sécurité Microsoft Graph (suite)

Microsoft Azure Sentinel	API de sécurité Microsoft Graph
et automatise la création d'incidents de sécurité dans SIR.	et automatise la création d'incidents de sécurité dans SIR.
Automatise les mises à jour de l'état des Microsoft Azure Sentinel incidents pour Réponse aux incidents de sécurité afin que vous puissiez créer et fermer des incidents de sécurité. **Remarque :** ServiceNow Met à jour l'état des incidents en fonction de la création ou de la fermeture de Microsoft Azure Sentinel l'incident de sécurité.	Prend en charge les mises à jour des alertes (changement de l'état de l'alerte et fermeture de l'alerte) pour les fournisseurs de sécurité sélectionnés. **Remarque :** Pour plus d'informations sur les fournisseurs de API de sécurité Microsoft Graph sécurité pris en charge, consultez la documentation Microsoft .
Utilisez cette intégration si votre scénario inclut les conditions suivantes : • L'enquête préliminaire sur l'incident est en cours Microsoft Azure Sentinel et l'enquête ultérieure est en cours SIR • Ingérer des Microsoft Azure Sentinel incidents dans SIR	Utilisez cette intégration si votre scénario inclut les conditions suivantes : • Effectuer une enquête sur les incidents dans SIR. • Ingérer des Microsoft Azure Sentinel alertes dans SIR. • Les incidents ne sont pas créés dans Microsoft Azure Sentinel.
L'alerte est une entité dans Microsoft Azure Sentinel. Vous ne pouvez pas récupérer des alertes autonomes ou spécifiques à l'aide de l'API Microsoft Azure Sentinel de gestion. Vous pouvez uniquement récupérer les données d'alerte associées à un incident. Les données d'alerte disponibles à l'aide de cette intégration sont plus riches que les données d'alerte disponibles à l'aide de .API de sécurité Microsoft Graph	Les Microsoft Azure Sentinel données d'alerte normalisées sont disponibles. Les Microsoft Azure Sentinel champs d'alerte mappés en interne dans API de sécurité Microsoft Graph et disponibles dans API de sécurité Microsoft Graph, peuvent être utilisés dans cette intégration.
	Vous ne pouvez pas mettre à jour les alertes dans cette Microsoft Azure Sentinel intégration.

Intégration Microsoft Defender pour point de terminaison

Cela Microsoft Defender pour point de terminaison vous permet d'inspecter, d'analyser et de contenir de manière proactive les menaces connues et inconnues sur n'importe quel point de terminaison.

L'intégration Microsoft Defender pour point de terminaison aide les analystes de sécurité à enquêter efficacement sur les incidents de sécurité et à les corriger sans avoir à naviguer entre les outils.

Vous pouvez utiliser cette intégration pour créer des configurations permettant de récupérer les détails de l'hôte, les détails des utilisateurs connectés, les détails des machines connexes et d'autres options d'enrichissement. Vous pouvez demander à ce qu'une machine n'accède pas aux réseaux ou qu'elle soit retirée de l'isolement. Les demandes peuvent être acceptées ou rejetées par les approbateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Fonctionnalités principales

Microsoft Defender pour point de terminaison possède les fonctionnalités principales suivantes :

- Réalisation d'une recherche de sécurité d'entreprise pour identifier les observables potentiellement malveillants sur les points de terminaison et application de mesures correctives.
- Réalisation d'actions de réponse telles que Isoler l'hôte, Supprimer l'isolation, Limiter l'exécution des applications, Effectuer une analyse antivirus, Limiter la restriction d'application et Arrêter et mettre en quarantaine le fichier.
- Créer ou mettre à jour des indicateurs.
- Effectuer l'enrichissement des observables et récupérer les données relatives aux indicateurs.

Microsoft Defender pour point de terminaison

Explorer Démarrer avec Microsoft Defender pour point de terminaison	**Installer** Installez l'application et configurez une source pour l'intégration	**Configurer** Configurer les profils et les incidents de sécurité pour Microsoft Defender pour point de terminaison
Profil d'aptitude Créez un profil d'aptitude pour l'intégration de Microsoft Defender pour point de terminaison.	**Configurations supplémentaires** Configurations supplémentaires que vous pouvez effectuer dans Microsoft Defender pour point de terminaison	**Divers** Créez et configurez un profil pour la recherche d'observations et les indicateurs avec Microsoft Defender pour point de terminaison.

Enregistrer et configurer l'dans Microsoft Defender pour point de terminaison le Microsoft Azure portail

Enregistrez l'application Microsoft Defender pour point de terminaison dans le portail Microsoft Azure et accordez l'accès en lecture et en écriture à l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : développeur d'application, administrateur de locataire.

Procédure

1. Connectez-vous au portail Microsoft Azure.
2. Entrez les inscriptions d'applications dans la zone de recherche, puis cliquez **sur Cliquez sur Nouvelle inscription**.
3. Saisissez un nom pour votre application et l'URI de redirection, puis cliquez sur **Enregistrer**.
   Un exemple de nom est Microsoft Defender pour point de terminaison. L'URI de redirection est utilisé lors de la fourniture du consentement de l'administrateur pour l'application.
4. Sur la page **Inscriptions d'applications** , sélectionnez l'application que vous avez enregistrée à l'étape 3.
5. Sous Gérer, sélectionnez **Certificats et secrets**.
6. Pour créer un secret client, sélectionnez **Nouveau secret client**.
7. Copiez le secret client et enregistrez-le.

   Si vous avez oublié le secret client, vous pouvez générer un nouveau secret client.
8. Accédez à la **Gérer** > **Autorisations d'API**.
9. Cliquez sur **Ajouter une autorisation**.
10. Dans la fenêtre Autorisations de l'API de demande, cliquez sur l'onglet **API utilisées par mon organisation** .
11. Recherchez et sélectionnez **WindowsDefenderATP**.
12. Dans les autorisations WindowsDefenderATP, sélectionnez **Autorisations d'application**.
    L'activation de cette autorisation garantit que l'application s'exécute en tant que service d'arrière-plan ou démon sans utilisateur connecté.
13. Ajoutez les autorisations au niveau de l'application suivantes et accordez un consentement administrateur pour les autorisations d'API nouvellement ajoutées.

Autorisation	Nom d'affichage de l'autorisation
Machine.Read.All	Lire tous les profils d'ordinateur
Utilisateur.Lecture.Tout	Lire les profils d'utilisateurs
Machine.Isoler	Isoler la machine
Machine.RestrictExecution	Restreindre l'exécution de code
Machine.Scan	Machine d'analyse
Machine.StopAndQuarantine	Arrêter et mettre en quarantaine
URL. Lecture.Tout	URL de lecture
Fichier.Lecture.Tout	Lire les profils de fichiers
Adresse IP.Lecture.Tout	Lire les profils d'adresses IP
Ti.ReadWrite.All	Indicateurs de lecture et d'écriture

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise en route de l'intégration Microsoft Defender pour point de terminaison

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre ServiceNow AI Platform® instance avant d'installer l'application Microsoft Defender pour point de terminaison à partir du ServiceNow Store.

Avant de commencer

Rôle requis : admin

Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application afin de garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform et Réponse aux incidents de sécurité (SIR).	Les rôles suivants sont requis : **1.** Vous devez disposer du rôle d'administrateur système (admin) pour installer l'application pour l'intégration. **2.** Vous devez disposer du rôle d'administrateur d'incident de sécurité (sn_si.admin) pour configurer l'intégration, créer, activer et supprimer des profils. **3.** vous devez disposer du rôle d'analyste des incidents de sécurité (sn_si.analyst) pour travailler avec des incidents de sécurité. Un utilisateur disposant de ce rôle peut initier n'importe quelle option disponible dans l'intégration.
Vérifiez que les applications principales ServiceNow nécessaires à la prise en charge de l'intégration sont installées et activées avant d'installer l'application.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ces applications ne sont pas déjà installées, vous devez installer et activer chaque application une par une dans l'ordre suivant pour assurer une installation fluide : **1.** Réponse aux incidents de sécurité **2.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **3.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Avant d'activer l'option d'approbation des profils, vérifiez que vous avez créé un groupe d'approbation.	Un workflow d'approbation facultatif est disponible pour isoler les machines hôtes, les restaurer sur le réseau et exécuter des actions supplémentaires sur le point de terminaison. Si votre organisation souhaite un niveau de contrôle supplémentaire sur ces actions, activez l'option Exiger l'approbation lors de la configuration des profils.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	Dans les cas où le profil est disponible, la configuration du profil pour approbation est prioritaire. Dans un scénario où le profil n'est pas disponible, les approbations sont traitées en fonction des paramètres par défaut. En tant qu'administrateur de sécurité, vous pouvez configurer l'approbation tout en configurant les profils et les paramètres par défaut. Un groupe d'approbation doit être disponible sur la liste des groupes de votre instance. Pour surveiller et traiter les demandes soumises par les utilisateurs disposant du rôle sn_si.analyst, chaque membre du groupe d'approbation doit accéder à Mes approbations dans le ServiceNow AI Platform®. Les approbateurs peuvent également trouver les demandes soumises exclusivement pour Microsoft Defender pour point de terminaison intégration dans le module Approbations. Pour plus d'informations sur la création d'un groupe d'utilisateurs, consultez Créer un groupe d'utilisateurs .

Que faire ensuite

Vous avez correctement configuré votre ServiceNow AI Platform® instance pour l'intégration Microsoft Defender pour point de terminaison . L'étape suivante consiste à installer l'application Microsoft Defender pour point de terminaison à partir du ServiceNow Store pour l'intégration.

Installer l'application et configurer Microsoft Defender pour point de terminaison l'intégration

Installez et configurez l'intégration Microsoft Defender pour point de terminaison à partir de sur ServiceNow Store votre ServiceNow AI Platform instance. Commencez à créer des profils d'option à l'aide des configurations.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Téléchargez l'intégration de Microsoft Defender pour point de terminaison à partir de et ServiceNow Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette Microsoft Defender pour point de terminaison, puis cliquez sur **Configurer**.
4. Renseignez les champs suivants du formulaire.

Configurer Microsoft Defender pour point de terminaison

Nom	Nom de la configuration d'instance Microsoft Defender pour point de terminaison .

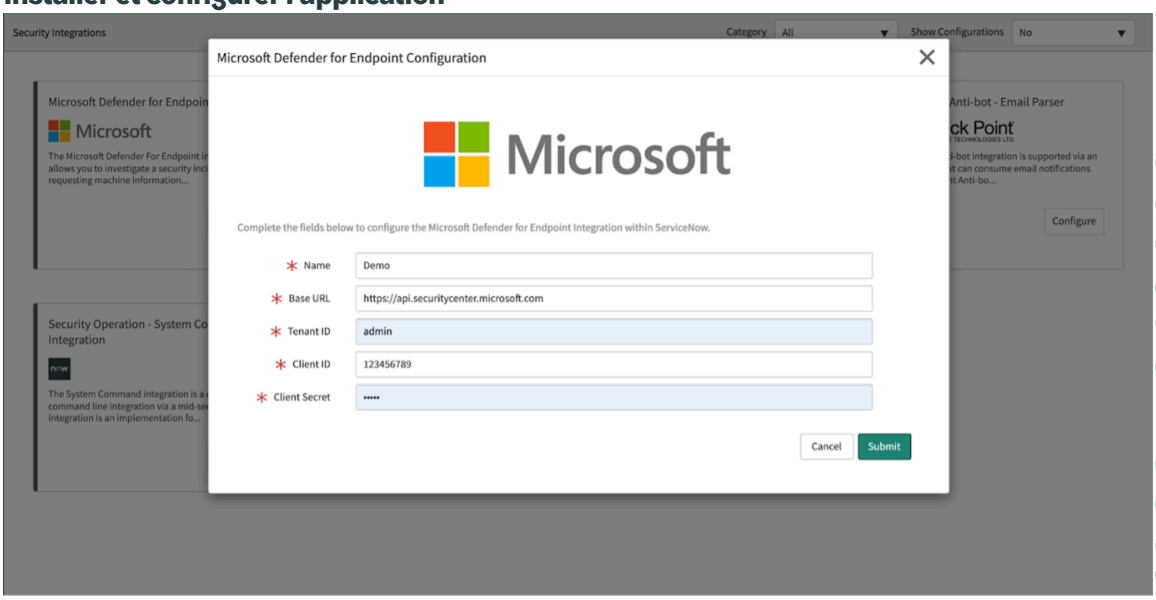
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

URL de base	URL de base de service pour Microsoft Defender pour point de terminaison
ID de locataire	L'ID Microsoft Defender pour point de terminaison du locataire. Toutes les actions seront effectuées sur cette instance.
ID client	ID client pour l'application que vous avez enregistrée dans le portail Microsoft Azure.
Secret client	Secret client pour votre application enregistrée.

5. Cliquez sur **Envoyer**.

Installer et configurer l'application



Traduction automatique

Résultats

La liste des Microsoft Defender pour point de terminaison configurations s'affiche avec votre nouvel enregistrement de configuration. Vous avez terminé la configuration pour le Microsoft Defender pour point de terminaison.

Microsoft Defender pour point de terminaison Paramètres par défaut

Vous devez effectuer des paramètres de configuration supplémentaires une fois l'installation terminée.

Une fois l'installation terminée, vous pouvez trouver le module Paramètres par défaut sous l'application dans le Microsoft Defender pour point de terminaison volet de navigation de gauche. Il contient les paramètres par défaut pour différentes Microsoft Defender pour point de terminaison fonctionnalités.

Rôles requis : sn_si.admin, sn_si.analyst (lecture seule).

Configurations supplémentaires

Les paramètres de configuration supplémentaires sont les suivants :

- **Approbation** : cette approbation est spécifiquement destinée à l'action Isoler l'hôte, Supprimer l'isolement de l'hôte et aux actions supplémentaires telles que Restreindre l'exécution des applications, Supprimer la restriction d'application et Exécuter une analyse

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

antivirus. Vous pouvez utiliser cette approbation uniquement lorsque les actions sont déclenchées directement à partir de la liste connexe et s'il n'existe aucun profil existant. S'il existe des profils pour ces options, la configuration de l'approbation dans le profil est prioritaire.

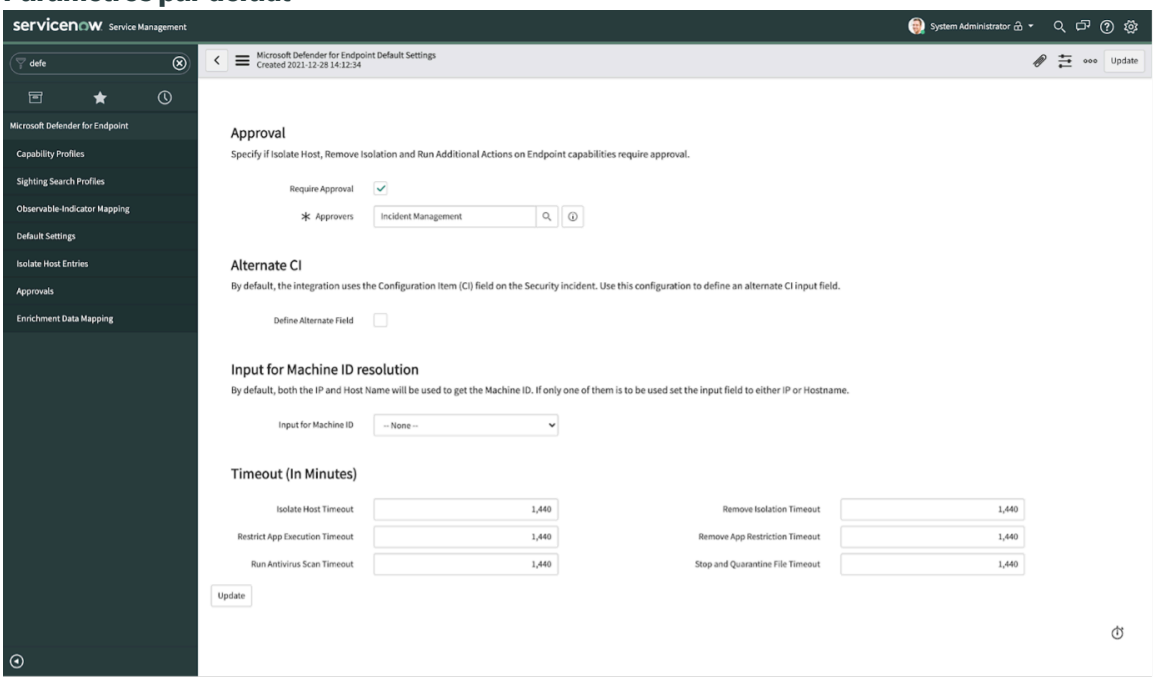
  - **Exiger l'approbation** : lorsque vous activez **Exiger l'approbation**, le champ Approbateurs est disponible sur le formulaire.
  - **Approbateurs** : liste des groupes d'approbateurs. Après avoir soumis une demande, l'approbation du groupe est requise pour terminer la demande.

- **CI alternatif** : cochez cette case pour afficher la liste des champs disponibles pour transmettre un CI alternatif à la capacité. Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité. Cette configuration est applicable uniquement pour l'aptitude Exécuter des actions supplémentaires sur le point de terminaison. Utilisez cette configuration pour définir un champ d'entrée CI alternatif pour la seule aptitude Exécuter des actions supplémentaires sur le point de terminaison. Pour les autres options, utilisez la configuration dans la section de profil. Si les profils ne définissent pas de CI alternatif, les options prendront le champ CI du formulaire d'incident de sécurité.
- **Entrée pour la résolution de l'ID de l'agent** : par défaut, l'adresse IP et le nom d'hôte sont utilisés pour obtenir l'ID de l'agent. Si vous n'utilisez qu'un seul d'entre eux, définissez le champ d'entrée sur IP ou Nom d'hôte.
- **Délai d'expiration** :
  - **Isoler le délai d'expiration de l'hôte (en minutes) :** Indique le seuil d'exécution pour les options Isoler l'hôte.
  - **Supprimer le délai d'isolement (en minutes) :** Indique le seuil d'exécution de l'aptitude Supprimer le délai d'isolement.
  - **Restreindre le délai d'expiration d'exécution de l'application (en minutes) :** Indique le seuil d'exécution de l'aptitude Restreindre l'exécution de l'application.
  - **Supprimer le délai de restriction d'application (en minutes) :** Indique le seuil d'exécution de l'aptitude Supprimer la restriction d'application.
  - **Délai d'expiration de l'analyse antivirus (en minutes) :** Indique le seuil d'exécution de l'aptitude Exécuter l'analyse antivirus.
  - **Arrêter et mettre en quarantaine le délai d'expiration du fichier (en minutes) :** Indique le seuil d'exécution de l'option Arrêter et mettre en quarantaine le fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres par défaut



Mapper les types d'indicateurs Microsoft Defender pour point de terminaison

Mappez le type d'observable ServiceNow avec le type d'indicateur Microsoft Defender pour point de terminaison . Ce mappage sera utilisé dans les actions Enrichissement des observables et Créer un indicateur dans Microsoft Defender.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst (lecture seule)

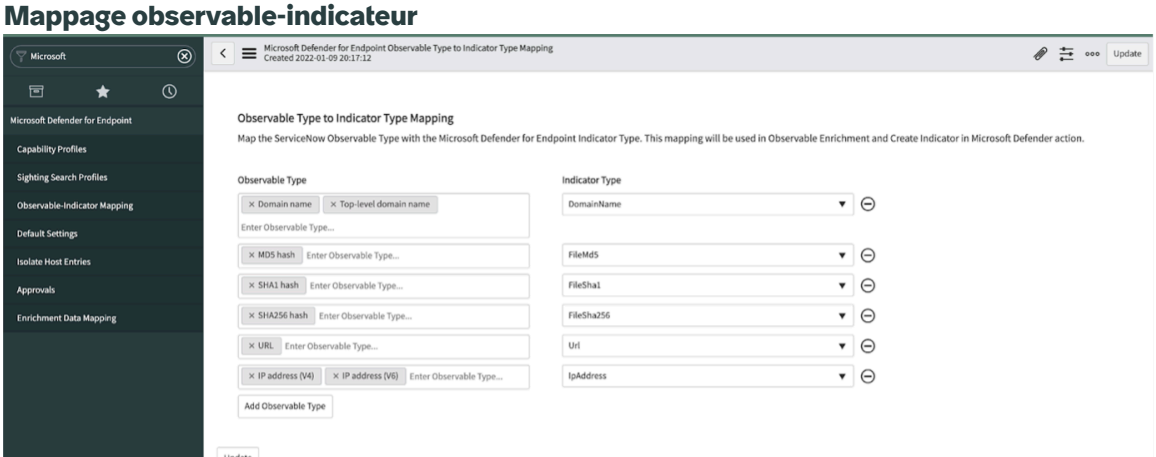
Pourquoi et quand exécuter cette tâche

Dans un scénario où le type d'observable n'est pas mappé à un type d'indicateur, ces observables ne sont pas éligibles à l'enrichissement des observables et à la création d'indicateurs dans Microsoft Defender pour point de terminaison.

Procédure

1. Accédez à la **Microsoft Defender pour point de terminaison** > **Mappage observable-indicateur**.

Mappage observable-indicateur



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Ajoutez ou mettez à jour un type d'observable de l'une des façons suivantes :
   - Pour ajouter un nouveau mappage, cliquez sur **Ajouter un type d'observable**.
   - Pour mettre à jour l'observable sur le mappage du type d'indicateur, cliquez sur une ligne existante.
3. Pour enregistrer le mappage, cliquez sur **Mettre à jour**.

Créer un profil d'aptitude pour l'intégration Microsoft Defender pour point de terminaison

Créez un profil et sélectionnez les Microsoft Defender pour point de terminaison options que vous souhaitez que le profil exécute.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Les profils sont créés pour regrouper ou regrouper les options, ce qui aiderait les analystes à effectuer facilement l'enquête ou la correction. Vous pouvez ajouter les fonctionnalités suivantes au profil :

- Obtenir les détails de l'hôte
- Obtenir les utilisateurs connectés
- Isoler l'hôte
- Supprimer l'isolement

Vous ne pouvez pas associer les options Isoler l'hôte et Supprimer l'isolement de l'hôte avec d'autres options tout en créant un profil. Les profils de ces capacités doivent être créés individuellement. D'autre part, les fonctionnalités Obtenir les détails de l'hôte et Obtenir les utilisateurs connectés peuvent être regroupées. Vous pouvez créer des profils individuellement ou en les matraquant en entier ou en partie selon vos besoins.

Remarque : Une fois qu'une option est incluse dans un profil, elle ne peut être incluse dans aucun autre profil provenant de la même source.

Procédure

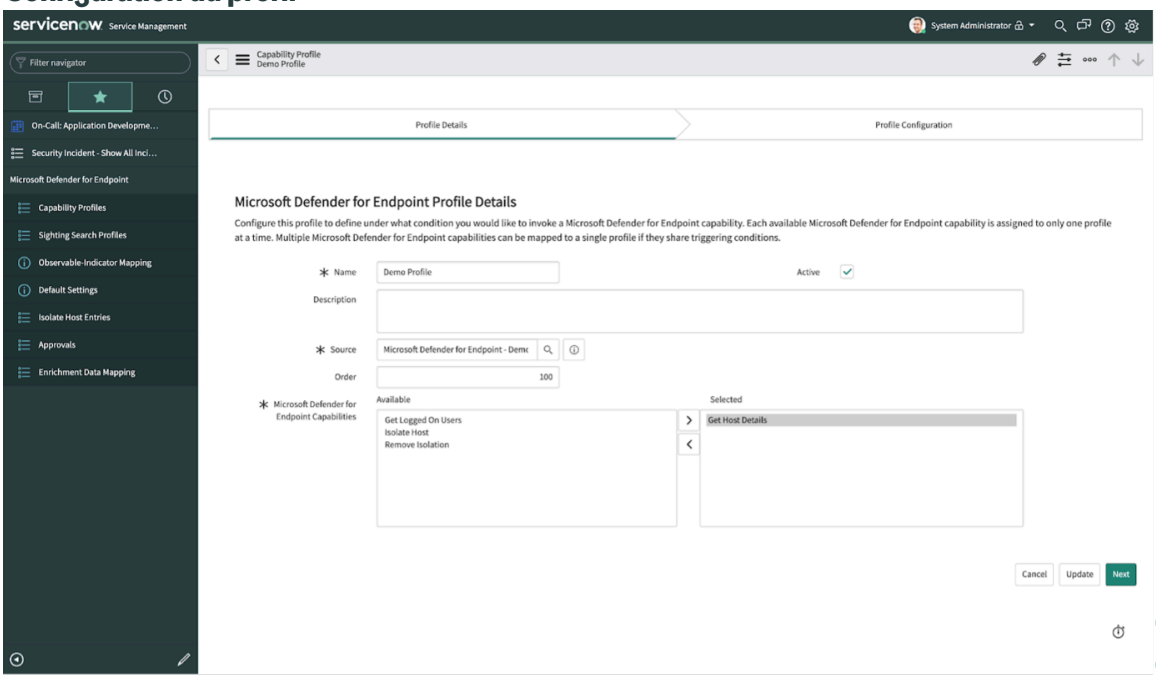
1. Accédez à la **Microsoft Defender pour point de terminaison** > **Profils d'aptitude**.

   La liste des profils d'aptitude de Microsoft Defender pour point de terminaison s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration du profil



2. Cliquer sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de profil d'aptitude

Champ	Description
Nom	Nom du profil d'aptitude Microsoft Defender pour point de terminaison . Ce nom vous permet d'identifier le type de profil et de le décrire.
Description	Informations supplémentaires sur le profil qui décrit plus en détail le profil.
Source	Nom de la Microsoft Defender pour point de terminaison source. Seules les sources configurées sont disponibles dans la liste.
Options de Microsoft Defender pour point de terminaison	Aptitudes du Microsoft Defender pour point de terminaison profil. Sélectionnez les options souhaitées pour ce profil dans la colonne Disponible et déplacez-les vers la colonne Sélectionné.
Ordre	Priorité du flux. La valeur par défaut est 100. La valeur de ce champ indique l'ordre dans lequel les flux sont exécutés lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Option permettant d'indiquer que le profil est actif. Une fois le profil actif, il est automatiquement déclenché lorsqu'un incident de sécurité correspondant aux conditions de filtrage que vous avez spécifiées dans la configuration est créé.

4. Pour passer à la configuration du profil, cliquez sur **Suivant**.

Que faire ensuite

L'étape suivante consiste à configurer votre profil. Avant de configurer les paramètres du profil, vous préférez peut-être passer en revue les profils de processus et les conditions de configuration et de déclenchement. Pour plus d'informations, consultez Conditions de déclenchement dans un élément de configuration.

Conditions de déclenchement dans un élément de configuration

Une fois que vous avez créé un profil et sélectionné les Microsoft Defender pour point de terminaison options que vous souhaitez que le profil exécute, configurez les paramètres du profil de sorte que le profil s'exécute uniquement lorsqu'un ensemble de conditions spécifiques est rempli.

Comment déclencher des conditions dans un élément de configuration

Vous pouvez définir des conditions de déclenchement afin que le profil s'exécute automatiquement chaque fois qu'un incident de sécurité correspondant à la condition de déclenchement est créé. Si la condition de déclenchement n'est pas définie, ces profils peuvent être exécutés manuellement en cliquant sur le formulaire Exécuter le(s) profil(s) EDR sur l'incident de sécurité et en sélectionnant le profil.

Par défaut, l'intégration utilise le champ Élément de configuration (CI) sur l'incident de sécurité. Cette valeur est utilisée pour faire correspondre les ID de vos actifs avec les informations stockées dans le ServiceNow AI Platform Base de données de gestion des configurations (CMDB). Lorsqu'un incident de sécurité est créé et qu'un profil est exécuté automatiquement ou manuellement, une recherche est effectuée pour récupérer le nom d'hôte ou l'adresse CMDB IP en fonction de la valeur du champ CI. Le nom d'hôte ou l'adresse IP est utilisé pour résoudre l'ID de l'agent Microsoft Defender pour point de terminaison afin d'identifier le point de terminaison.

Dans un scénario idéal, une valeur correspondante est trouvée dans la base de données et les données sont collectées à partir de la Microsoft Defender pour point de terminaison console pour l'actif correspondant. Les données des différentes options sont extraites dans votre ServiceNow AI Platform Base de données de gestion des configurations (CMDB) instance et affichées dans les listes connexes d'un incident de sécurité. Lorsque le champ Élément de configuration (CI) de l'incident de sécurité n'est pas renseigné avec un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ de l'incident de sécurité qui contient le nom d'hôte ou l'adresse IP pour effectuer la résolution de l'ID d'agent.

Au cours de l'étape de configuration de la configuration du profil, vous pouvez sélectionner un autre champ CI pour l'identification du point de terminaison afin de vous assurer que vous êtes en mesure d'identifier le point de terminaison sur Microsoft Defender pour point de terminaison. Vous pouvez sélectionner n'importe quel champ de l'incident de sécurité comme champ de déclenchement CI alternatif, y compris les champs personnalisés que vous créez. En sélectionnant cet autre champ CI comme copie de sauvegarde, vous vous assurez que

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vos profils s'exécutent même si le champ CI n'est pas renseigné sur l'incident de sécurité associé lors de la création de l'incident.

Remarque : Les champs CI alternatifs ne sont pris en compte que pour les options qui peuvent être ajoutées à un profil. Ces fonctionnalités incluent Obtenir les détails de l'hôte, Obtenir les utilisateurs connectés, Isoler l'hôte et Supprimer l'isolement. Pour toutes les actions supplémentaires, l'autre CI doit être configuré dans le module Paramètres par défaut.

Configurer les profils et les incidents de sécurité pour l'intégration Microsoft Defender pour point de terminaison

Créez un profil et sélectionnez les Microsoft Defender pour point de terminaison options que vous souhaitez que le profil exécute. Vous devez configurer les paramètres afin que le profil ne puisse être déclenché que dans les conditions définies.

Avant de commencer
Rôle requis : sn_si.admin, sn_si.analyst (lecture seule)

Pourquoi et quand exécuter cette tâche
Configurez le profil de sorte qu'il s'exécute uniquement lorsque les conditions spécifiées sont remplies. Si nécessaire, vous pouvez sélectionner un autre champ d'entrée pour le champ Élément de configuration (CI) et définir des conditions de filtrage afin que le profil puisse être déclenché automatiquement lorsqu'un incident de sécurité répondant aux conditions de déclenchement est créé.

Remarque : Vous pouvez accéder à la page Configuration du profil uniquement après avoir saisi la page Détails du profil.

Procédure

1. Accédez à la **Microsoft Defender pour point de terminaison** > **Profils d'aptitude**.
2. Après avoir rempli la section Détails du profil, cliquez sur **Suivant**.
   Examinez et configurez les sections.
3. Dans la section Définir des critères d'incident (automatisation), sélectionnez l'option **Définir des critères d'incident** pour déclencher Microsoft Defender pour point de terminaison automatiquement les options du profil.
   Définir des critères d'incident (automatisation) : définissez les conditions d'incident de sécurité qui déclenchent automatiquement les options de Microsoft Defender pour point de terminaison pour le profil. Si vous ne sélectionnez pas l'option **Définir des critères d'incident** , le profil et les options sous-jacentes peuvent être invoqués manuellement à partir de l'incident de sécurité.

   Remarque : Les options Isoler l'hôte et Supprimer l'isolement de l'hôte ne peuvent pas être déclenchées automatiquement.

   a. Dans les **Conditions de filtre**, sélectionnez le champ requis.
   b. Ajoutez **de nouveaux critères** et définissez également **la conditionOU** ou ET.
4. Dans la section Approbations, cochez la case **Exiger l'approbation** pour fournir un niveau de contrôle supplémentaire.

   Si vous sélectionnez cette option, vous avez plus de contrôle lors de l'utilisation des fonctionnalités de Microsoft Defender for Endpoint pour isoler les machines hôtes, les restaurer sur le réseau, obtenir des fichiers.

   L'option Approbations de la configuration du profil s'affiche uniquement pour les options Isoler l'hôte et Supprimer l'isolement de l'hôte respectivement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Dans la section Configuration supplémentaire, sélectionnez l'option **Définir un champ alternatif** pour définir un champ d'entrée alternatif.
   Configuration supplémentaire : lorsque le champ Élément de configuration (CI) n'est pas renseigné sur l'incident de sécurité avec un nom d'hôte ou une adresse IP qui correspond à la base de données, vous pouvez sélectionner un autre champ sur l'incident de sécurité pour interroger les API Microsoft Defender for Endpoint.

   Remarque : Pour plus d'informations, consultez Conditions de déclenchement dans un élément de configuration.

   a. Sélectionnez l'option **Définir un autre champ** .

   b. Sélectionner le champ d'entrée dans le **Champ de déclenchement CI alternatif**.

6. Dans la section Balises, cochez la case **Afficher la balise** pour activer le balisage des incidents de sécurité, le nom du profil est précédé de l'activation de la balise.

   Vous pouvez éventuellement baliser les incidents de sécurité avec des balises pour les balises de profil initié, de profil terminé et de profil échoué. Par défaut, cette option est désactivée pour tous les profils.

7. Cliquer sur **Terminé**.

Vérifier les filtres des conditions de déclenchement

Validez le profil et vérifiez que les filtres de condition de déclenchement que vous avez configurés fonctionnent comme prévu.

Avant de commencer
Rôle requis : sn_si.admin ou sn_si.analyst

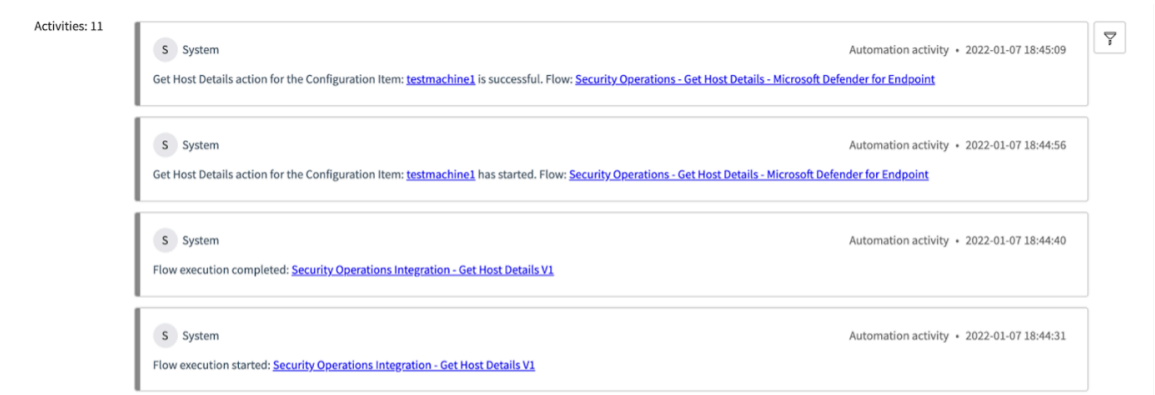
Pourquoi et quand exécuter cette tâche
Après avoir activé le profil, en fonction des conditions de déclenchement configurées, vous pouvez afficher les résultats de la requête dans les ServiceNow AI Platform® incidents de sécurité.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Pour créer un nouvel incident de sécurité, sélectionnez **Nouveau**.
3. Pour déclencher le profil respectif, fournissez les conditions de filtre telles qu'indiquées dans le profil d'aptitude.
4. Cliquer sur **Enregistrer**.
5. Pour valider les notes de travail et la section activités, affichez et vérifiez les enregistrements étiquetés avec les balises profil initié, profil terminé ou profil échoué.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Pour valider toutes les données des listes connexes, cliquez sur **Afficher toutes les listes connexes**.
7. Cliquez sur un onglet de **liste connexe** pour valider les détails.
   Par exemple, Détails de l'hôte.

Déclencher les Microsoft Defender pour point de terminaison options à partir des liens connexes

Déclenchez manuellement un profil d'aptitude après avoir examiné un incident de sécurité à partir des liens connexes.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Pourquoi et quand exécuter cette tâche

En plus d'exécuter le profil pour le CI ou le CI alternatif de l'incident de sécurité, vous pouvez également exécuter le profil pour les valeurs CI présentes dans la liste connexe Élément de configuration en sélectionnant **Inclure le CI connexe** dans la boîte de dialogue. Cela récupère également les données des valeurs CI présentes dans la liste connexe. Vous pouvez également exécuter le profil uniquement pour les valeurs de CI présentes dans la liste connexe.

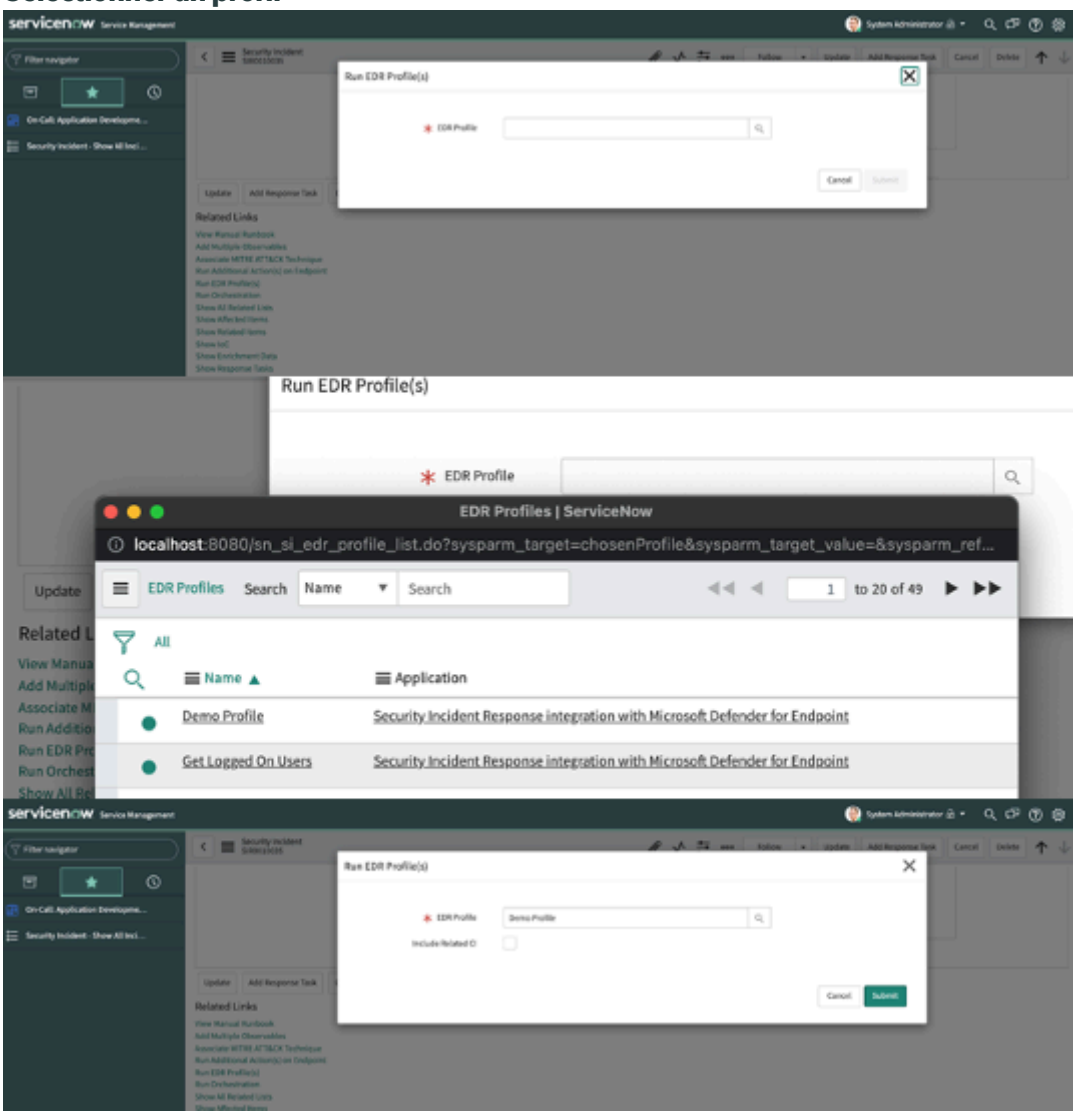
Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les Microsoft Defender pour point de terminaison informations.
3. Dans la section Liens connexes, cliquez sur **Exécuter le(s) profil(s) EDR**.
4. Parcourez et sélectionnez un profil dans la liste des profils disponibles, puis cliquez sur **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sélectionner un profil



Le profil sélectionné est déclenché manuellement.

5. Validez la section Notes de travail et activités.
6. Affichez les balises et validez les données dans les listes connexes.

Déclencher la liste connexe à partir d'un Microsoft Defender pour point de terminaison élément de configuration

Déclenchez manuellement un profil d'aptitude à partir de la liste connexe des éléments de configuration.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les Microsoft Defender pour point de terminaison informations.
3. Cliquer sur **Afficher toutes les listes connexes**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur la liste connexe Élément de configuration.
5. Sélectionnez les éléments de configuration ajoutés.
6. Dans **Actions sur** les lignes sélectionnées, sélectionnez une option.
   L'aptitude sélectionnée est déclenchée manuellement.
7. Validez la section Notes de travail et activités.
8. Affichez les balises et validez les données dans les listes connexes.

Configurations supplémentaires dans Microsoft Defender pour point de terminaison

L'intégration Microsoft Defender pour point de terminaison prend en charge l'exécution d'actions supplémentaires au-delà des actions standard.

Le prend Microsoft Defender pour point de terminaison en charge les configurations supplémentaires suivantes :

Configurer l'option Isoler l'hôte dans Microsoft Defender pour point de terminaison

Isolez l'hôte de l'accès au réseau en Microsoft Defender pour point de terminaison fonction de la gravité de l'attaque. L'isolation de l'hôte du réseau vous permet d'empêcher toute autre activité malveillante ou attaque potentielle sur d'autres hôtes.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Exigences relatives à l'aptitude Isoler l'hôte

Option	Obligatoire	Description
Isoler l'hôte	Type d'isolement	(Obligatoire) Type d'isolement (complet ou sélectif).
	Commentaire	(Obligatoire) Commentaire à associer à l'action.

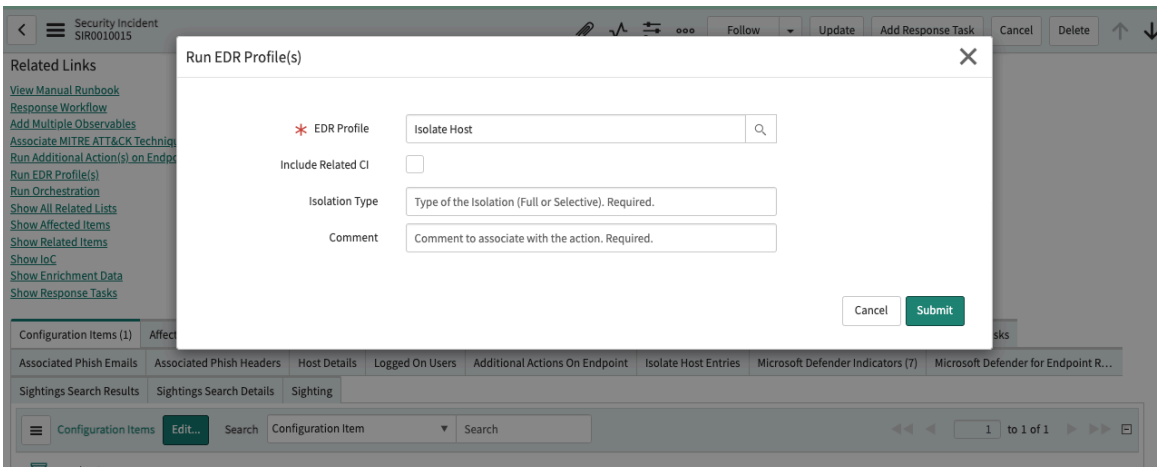
Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.
3. Dans la section Liens connexes, cliquez sur **Exécuter le(s) profil(s) EDR**.
4. Parcourez et sélectionnez un profil avec **l'option Isoler l'hôte** sélectionné dans la liste des profils disponibles, puis cliquez sur **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Isoler l'hôte



Vous pouvez également effectuer les étapes suivantes :

a. Dans la section Listes connexes, cliquez sur **Afficher toutes les listes connexes**.

b. Cliquez sur la liste connexe **Élément de configuration** .

c. Sélectionnez **Isoler l'hôte** et sélectionnez les options correspondantes.

5. Validez l'activité et la section activités d'automatisation, puis assurez-vous que les données sont conformes aux attentes.
6. Affichez les données et validez les détails d'isolement de l'hôte sur les listes connexes.

Configurer l'option Supprimer l'isolement de l'hôte dans Microsoft Defender pour point de terminaison

Si nécessaire, supprimez l'isolement d'un hôte précédemment isolé du réseau dans Microsoft Defender pour point de terminaison. Vous pouvez empêcher toute autre activité malveillante ou attaque potentielle sur d'autres hôtes.

Avant de commencer

Exigences relatives à l'aptitude de suppression de l'isolement

Option	Entrée requise	Description
Supprimer l'isolement	Commentaire	(Obligatoire) Commentaire à associer à l'action.

Rôle requis : sn_si.admin ou sn_si.analyst

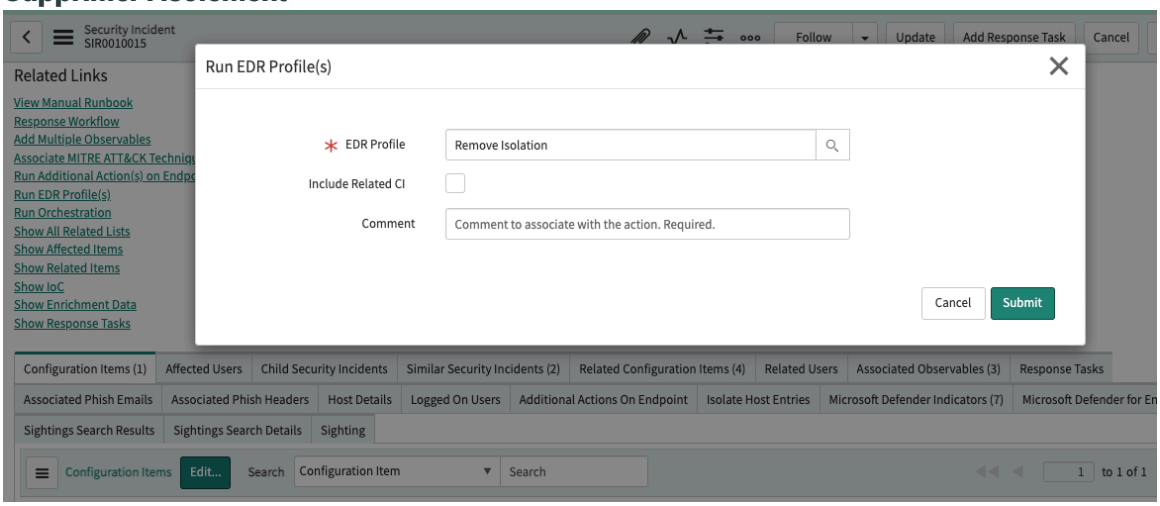
Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.
3. Dans la section Liens connexes, cliquez sur **Exécuter le(s) profil(s) EDR**.
4. Parcourez et sélectionnez un profil avec **l'option Supprimer l'isolement** sélectionnée dans la liste des profils disponibles, puis cliquez sur **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supprimer l'isolement



Vous pouvez également effectuer les étapes suivantes :

a. Cliquez sur **Afficher toutes les listes connexes** dans la section Listes connexes.

b. Cliquez sur la liste connexe **Élément de configuration** .

c. Sélectionnez **Supprimer l'isolement** et sélectionnez les options correspondantes.

5. Validez l'activité d'automatisation et la section activités.
6. Affichez les données et validez les détails d'isolement de l'hôte sur les listes connexes.
7. Validez les activités d'automatisation de l'exécution.

Configurer l'option Exécuter l'analyse antivirus dans Microsoft Defender pour point de terminaison

Lancez à distance une analyse antivirus pour identifier et corriger les programmes malveillants susceptibles d'être présents sur un appareil compromis. Exécutez l'analyse dans le cadre du processus d'enquête ou de réponse.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

Conditions requises pour l'aptitude Exécuter l'analyse antivirus

Entrée	Description
Type d'analyse	(Obligatoire) Type d'analyse (complète ou rapide).
Commentaire	(Obligatoire) Commentaire à associer à l'action.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.

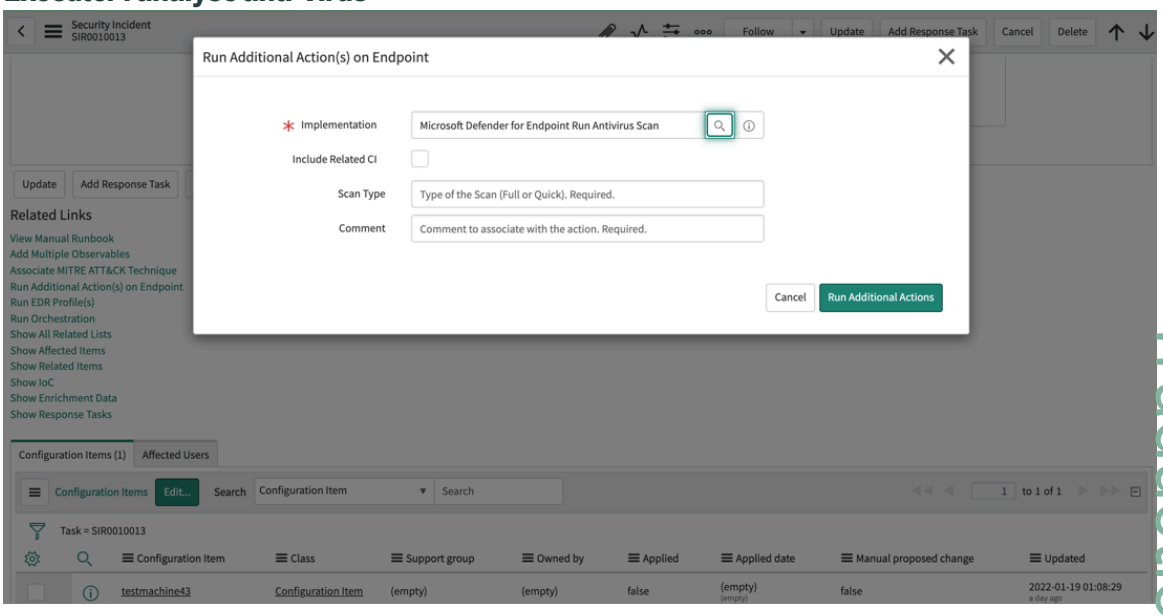
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans la section Liens connexes, cliquez sur **Exécuter des actions supplémentaires sur le point de terminaison**.

b. Parcourez et sélectionnez l'option requise.
Par exemple, cliquez sur **Exécuter l'aptitude Analyse antivirus** .

Exécuter l'analyse anti-virus



Vous pouvez également effectuer les étapes suivantes :

a. Dans la section Listes connexes, cliquez sur **Afficher toutes les listes connexes**.

b. Cliquez sur la liste connexe **Élément de configuration** .

c. Sélectionnez les éléments de configuration ajoutés, puis dans Actions sur les lignes sélectionnées, sélectionnez **Exécuter des actions supplémentaires sur le point de terminaison**.

Une fois que vous avez sélectionné l'implémentation de l'aptitude **Exécuter l'analyse antivirus**, les champs **d'entréeType d'analyse supplémentaire** et Commentaire s'affichent.

3. Sélectionnez le **type d'analyse** que vous souhaitez exécuter (rapide ou complet) et ajoutez un commentaire avant d'exécuter l'analyse.
4. Pour lancer l'analyse antivirus, cliquez sur **Exécuter une action supplémentaire**.
5. Affichez les activités d'automatisation de l'exécution et validez-les.
6. Validez l'état de l'action dans les listes connexes Actions supplémentaires sur le point de terminaison.

Configurer l'option Restreindre l'exécution d'applications dans Microsoft Defender pour point de terminaison

Pour contenir une attaque, limitez ou verrouillez un appareil et empêchez l'exécution de tentatives ultérieures de programmes potentiellement malveillants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Conditions requises pour l'aptitude Restreindre l'exécution de l'application

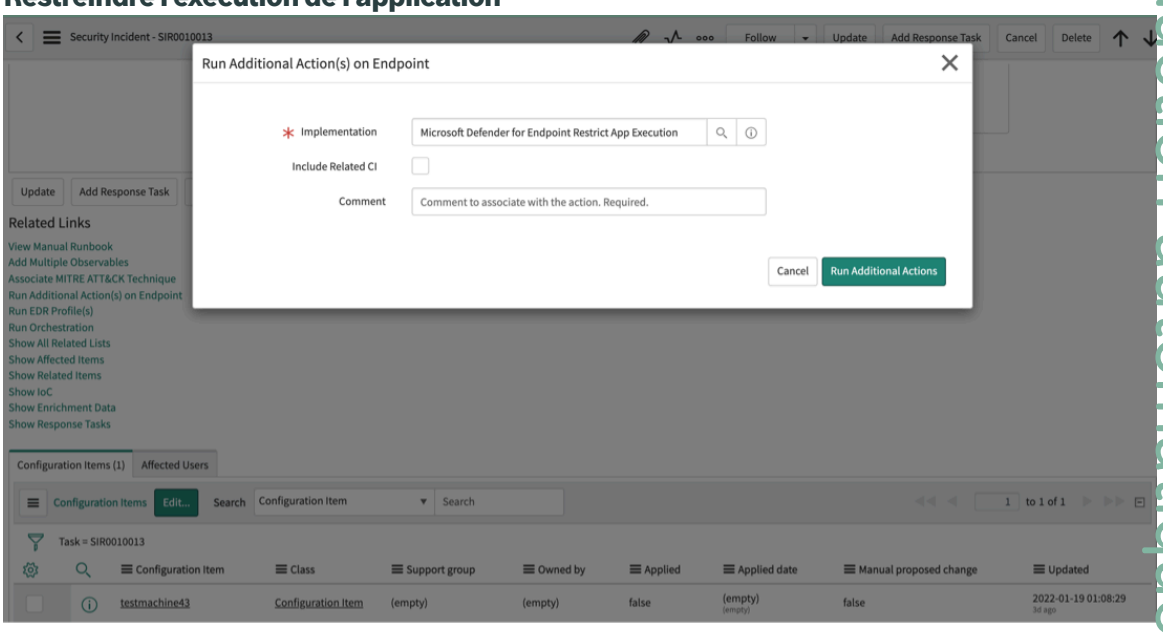
Entrée	Description
Commentaire	(Obligatoire) Commentaire à associer à l'action)

Rôle requis : sn_si.admin ou sn_si.analyst

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.
   a. Dans la section Liens connexes, cliquez sur **Exécuter des actions supplémentaires sur le point de terminaison**.
   b. Parcourez et sélectionnez l'aptitude **Restreindre l'exécution des applications** .

Restreindre l'exécution de l'application



Vous pouvez également effectuer les étapes suivantes :

   a. Dans la section Listes connexes, cliquez sur **Afficher toutes les listes connexes**.
   b. Cliquez sur la liste connexe **Élément de configuration** .
   c. Sélectionnez les éléments de configuration ajoutés.
   d. Dans Actions sur les lignes sélectionnées, sélectionnez **Exécuter des actions supplémentaires sur le point de terminaison**.

3. Pour activer Restreindre l'exécution de l'application sur l'ordinateur, cliquez sur **Exécuter une action supplémentaire**.
4. Affichez les activités d'automatisation de l'exécution et validez-les.
5. Validez l'état de l'action dans les listes connexes Actions supplémentaires sur le point de terminaison.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'option Supprimer la restriction d'application dans Microsoft Defender pour point de terminaison

Si nécessaire, supprimez les restrictions de toute application sur l'appareil.

Avant de commencer

Rôle requis : sn_si.admin ou sn_si.analyst

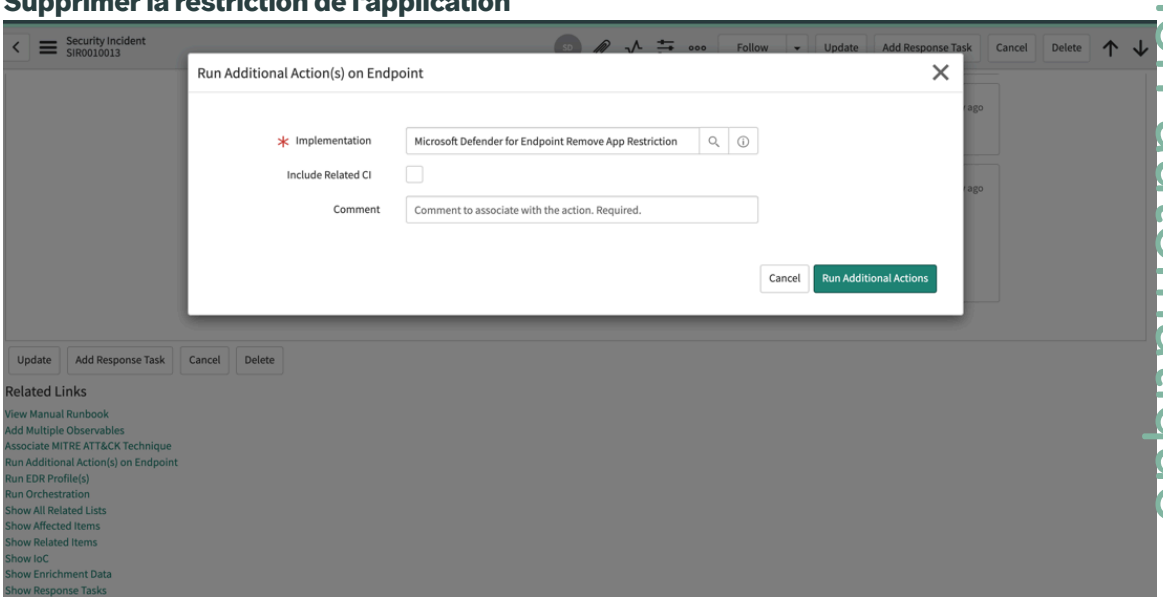
Conditions requises pour l'aptitude de suppression de la restriction d'application

Entrée	Description
Commentaire	(Obligatoire) Commentaire à associer à l'action)

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.
   a. Dans la section Liens connexes, cliquez sur **Exécuter des actions supplémentaires sur le point de terminaison**.
   b. Parcourez et sélectionnez l'option **Supprimer la restriction d'application** .

Supprimer la restriction de l'application



Vous pouvez également effectuer les étapes suivantes :

a. Dans la section Listes connexes, cliquez sur **Afficher toutes les listes connexes**.
b. Cliquez sur la liste connexe **Élément de configuration** .
c. Sélectionnez les éléments de configuration ajoutés.
d. Sélectionnez **Exécuter des actions supplémentaires sur le point de terminaison**.
Le champ d'entrée Commentaire supplémentaire s'affiche.

3. Pour supprimer la restriction d'application, cliquez sur **Exécuter une action supplémentaire**.
4. Affichez les activités d'automatisation de l'exécution et validez-les.
5. Validez l'état de l'action dans les listes connexes Actions supplémentaires sur le point de terminaison.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'option Obtenir les ordinateurs associés à partir de Defender dans Microsoft Defender pour point de terminaison

Obtenez la liste des machines connexes d'observables spécifiques.

Avant de commencer

Remarque : Les types observables pris en charge sont le nom de domaine, le hachage SHA1 et le nom d'utilisateur.

Rôle requis : sn_si.admin ou sn_si.analyst

Pourquoi et quand exécuter cette tâche

Vous pouvez récupérer la liste des machines qui ont accédé aux observables particuliers. Vous pouvez stocker la liste dans la table Détails des ordinateurs connexes de Microsoft Defender for Endpoint. Vous pouvez déclencher la fonctionnalité Obtenir les ordinateurs associés à partir de Defender à partir de la liste connexe Observables associés.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.



3. Dans la section Liens connexes, cliquez sur **Afficher IoC**.
4. Cliquez sur la liste connexe Observables associés.
5. Sélectionner les observables associés.
6. Dans la liste Actions, sélectionnez l'aptitude **Obtenir les ordinateurs associés à partir de Defender** .
7. Validez l'activité d'automatisation et la section activités.
8. Affichez les données et validez les détails des ordinateurs associés à Microsoft Defender for Endpoint sur les listes connexes.
9. Affichez les activités d'automatisation de l'exécution et validez-les.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'option Arrêter et mettre en quarantaine un fichier dans Microsoft Defender pour point de terminaison

Arrêtez et mettez en quarantaine les fichiers à partir de la plateforme Microsoft Defender.

Avant de commencer

Types d'observables pris en charge : hachage SHA1.

Exigences relatives à l'aptitude d'arrêt et de mise en quarantaine des fichiers

Entrée	Description
Commentaire	(Obligatoire) Commentaire à associer à l'action)

Rôle requis : sn_si.admin ou sn_si.analyst

Pourquoi et quand exécuter cette tâche

Vous pouvez exécuter l'action Arrêter et mettre en quarantaine le fichier sur les observables particuliers de type SHA1 uniquement. Stockez les détails dans la table Actions supplémentaires sur le point de terminaison. Vous pouvez déclencher l'aptitude Arrêter et mettre en quarantaine le fichier à partir de la liste connexe des détails des machines associées à Microsoft Defender for Endpoint.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.
3. Dans la section Liens connexes, cliquez sur **Afficher toutes les listes connexes**.
4. Cliquez sur la liste connexe Détails des ordinateurs associés à Microsoft Defender pour point de terminaison.
5. Sélectionnez un ou plusieurs enregistrements.
6. Dans **Actions sur** les lignes sélectionnées, sélectionnez l'option **Arrêter et mettre en quarantaine le fichier** .
7. Validez l'activité d'automatisation et la section activités.
8. Affichez les données et validez les données sur les listes connexes.
9. Affichez les activités d'automatisation de l'exécution et validez-les.

Créer et configurer un profil pour la recherche de perceptions avec l'intégration Microsoft Defender pour point de terminaison

Créez et configurez automatiquement le profil de recherche de perceptions à l'aide du Microsoft Defender pour point de terminaison.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le workflow Recherche de perceptions pour effectuer les recherches de perception. Ce workflow accepte une liste d'observables, recherche toutes les options d'implémentation, crée les requêtes basées sur les configurations de recherche de perceptions et exécute les recherches basées sur le workflow configuré.

Le Microsoft Defender pour point de terminaison fournit un profil de recherche de perception du système de base qui vous permet de configurer les recherches automatiques de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

perception. Avec ce profil, vous pouvez accéder aux informations observables connexes d'une organisation et également voir les observations d'autres organisations.

Procédure

1. Accédez à la **Intégrations** > **Configuration de la recherche de détections**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs suivants du formulaire.

Formulaire Configuration de la recherche de perceptions

Champ	Description
Nom	Nom du profil de recherche de perceptions.
Est une recherche enregistrée	Option permettant d'enregistrer la configuration de la recherche. Les requêtes de configuration de recherche enregistrées sont des exemples de requêtes. Vous pouvez les remplacer par les paramètres de votre environnement et créer des configurations de recherche enregistrées supplémentaires, au besoin.
Source de recherche de perceptions	La source configurée pour la recherche de perceptions dans Microsoft Defender pour point de terminaison l'intégration.
Rechercher	Chaîne de recherche native qui forme une requête.
Actif	Option permettant d'activer la configuration de recherche enregistrée. Seules les configurations de recherche actives peuvent effectuer une recherche de perceptions.
Type d'observable	Type de catégorie d'observable. Par exemple, adresse IP, valeur de hachage, URL et nom de domaine.
Nombre maximum d'observables par recherche	Nombre maximal d'observables que vous pouvez afficher à partir d'une requête de recherche. Définissez cette valeur sur 1 pour cette intégration.
Paramètres de la recherche de perceptions	Paramètres pour définir des requêtes plus complexes qui incluent la logique et d'autres opérateurs pris en charge par le magasin de journaux spécifié.

4. Cliquez sur **Envoyer**.

Effectuer une recherche de perception manuelle dans Microsoft Defender pour point de terminaison

Sélectionnez un ou plusieurs observables et effectuez une recherche de perception manuelle pour Microsoft Defender pour point de terminaison déterminer la prévalence d'une menace au fil du temps.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Les types d'observables pris en charge sont les suivants :

- Nom du domaine
- Adresse IP (V4)
- Adresse IP (V6)
- Hachage MD5
- Hachage SHA1
- Hachage SHA256

Procédure

1. Accédez aux **incidents de sécurité**.
2. Ouvrez un SIR existant ou créez-en un nouveau.
3. Dans les liens connexes, cliquez sur **Afficher l'IoC**.
4. Cliquez sur les listes connexes Observables associés.
5. Sélectionnez les observables.
6. Dans la liste Actions, cliquez sur **Exécuter l'enrichissement de l'élément observable**.
7. Sélectionnez les observables sous **Action** sur les lignes sélectionnées, puis cliquez sur **Exécuter la recherche de perceptions**.

   Remarque : La recherche de perception est prise en charge pour les types d'observables de nom de domaine, d'adresse IP (V4), d'adresse IP (V6), de hachage MD5, de hachage SHA1 et de hachage SHA256.

8. Indiquez la période de la recherche, puis cliquez sur **Rechercher**.

   Remarque : Microsoft Defender pour point de terminaison ne prend en charge la recherche de perception que pour les 30 derniers jours. Si votre requête de plage est antérieure aux 30 derniers jours, la recherche de perception ne récupère aucune donnée. Si votre requête de plage chevauche les 30 derniers jours, les observations des 30 derniers jours uniquement sont récupérées. Si votre requête de plage se rapporte aux 30 derniers jours, les observations comprises entre l'heure de début définie et l'heure actuelle sont récupérées.

9. Une fois la recherche terminée, validez les résultats et les détails dans les listes connexes.
10. Cliquez sur **Détails de recherche de perceptions** pour afficher les détails de la recherche de perceptions.
11. Cliquez sur l'onglet Perception pour plus **d'informations** et sur l'onglet **Résultats de recherche de perceptions** pour les résultats de recherche.

    Vous pouvez afficher des informations supplémentaires relatives à l'observation particulière dans le champ **Résumé** .

Réalisation d'un enrichissement automatique de l'observable dans Microsoft Defender pour point de terminaison

Procédez à un enrichissement automatique des observables dans Microsoft Defender pour point de terminaison pour enrichir les observables avec des informations supplémentaires tirées de diverses sources.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Vérifiez que vous avez activé la propriété système **Réponse aux incidents de sécurité** . Cette option déclenche la fonctionnalité d'enrichissement des observables dans SIR, chaque fois qu'un observable est associé à un incident de sécurité.

Rôle requis : sn_si.admin, sn_si.analyst

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser cette fonctionnalité pendant les enquêtes de réponse aux incidents pour contenir une menace identifiée. Lorsque de nouveaux observables sont associés à l'incident de sécurité, vous pouvez activer l'exécution automatique de la fonctionnalité d'enrichissement des observables dans Microsoft Defender pour point de terminaison.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.
3. Validez l'activité d'automatisation une fois que les nouveaux observables ont été associés à l'incident de sécurité.
4. Affichez les résultats de l'enrichissement dans la liste connexe Indicateurs de l'incident de sécurité. Vous pouvez utiliser la table suivante pour plus d'informations sur l'enrichissement des observables.

Indicateur Microsoft Defender

Champ	Description
ID de l'indicateur	Identité de l'entité de l'indicateur. Cliquez sur **Ouvrir** pour afficher l'enregistrement en détail dans l'instance ServiceNow AI Platform
Observable	L'observable associé au résultat.
Titre	Titre de l'indicateur.
Type d'indicateur	Type de l'indicateur.
Action	Action effectuée par l'indicateur.
Action recommandée	Actions recommandées pour l'indicateur.
Fournisseur de l'intégration	Intégration de la source Defender à partir de laquelle les données sont récupérées.
Date d'expiration	Délai d'expiration de l'indicateur.
Date de récupération	Date de création de l'enregistrement d'enrichissement.

Effectuer un enrichissement manuel de l'observable dans Microsoft Defender pour point de terminaison

Sélectionner un ou plusieurs observables et effectuer un enrichissement manuel des observables pour enrichir les observables avec des informations supplémentaires à partir de Microsoft Defender pour point de terminaison.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

L'intégration Microsoft Defender pour point de terminaison permet l'enrichissement des observables pour tous les types d'observables mappés dans le module Mappage observable-indicateur.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez examiner avec les informations Microsoft Defender pour point de terminaison.
3. Cliquez sur **Afficher toutes les listes connexes**.
4. Cliquez sur l'onglet **Observables associés** .
5. Sélectionnez les observables.
6. Dans la liste Actions, cliquez sur **Exécuter l'enrichissement de l'élément observable**.
7. Sélectionnez une **source** Microsoft Defender pour point de terminaison et déplacez-la dans la colonne **Sélectionné** pour spécifier l'implémentation que vous souhaitez utiliser pour enrichir les observables sélectionnés.
8. Cliquez sur **Envoyer**.
9. Pour valider l'état de l'exécution, consultez les notes de travail.
10. Pour afficher les résultats, cliquez sur l'onglet **Indicateur Microsoft Defender** .
    Vous pouvez utiliser la table suivante pour plus d'informations sur l'enrichissement des observables.

Indicateur Microsoft Defender

Champ	Description
ID de l'indicateur	Identité de l'entité de l'indicateur. Cliquez sur **Ouvrir** pour afficher l'enregistrement en détail dans l'instance ServiceNow AI Platform
Observable	L'observable associé au résultat.
Titre	Titre de l'indicateur.
Type d'indicateur	Type de l'indicateur.
Action	Action effectuée par l'indicateur.
Action recommandée	Actions recommandées pour l'indicateur.
Fournisseur de l'intégration	Intégration de la source Defender à partir de laquelle les données sont récupérées.
Date d'expiration	Délai d'expiration de l'indicateur.
Date de récupération	Date de création de l'enregistrement d'enrichissement.

Créer des indicateurs dans Microsoft Defender pour point de terminaison

Créez des indicateurs à partir des observables associés de l'incident de sécurité à l'aide du Microsoft Defender pour point de terminaison.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

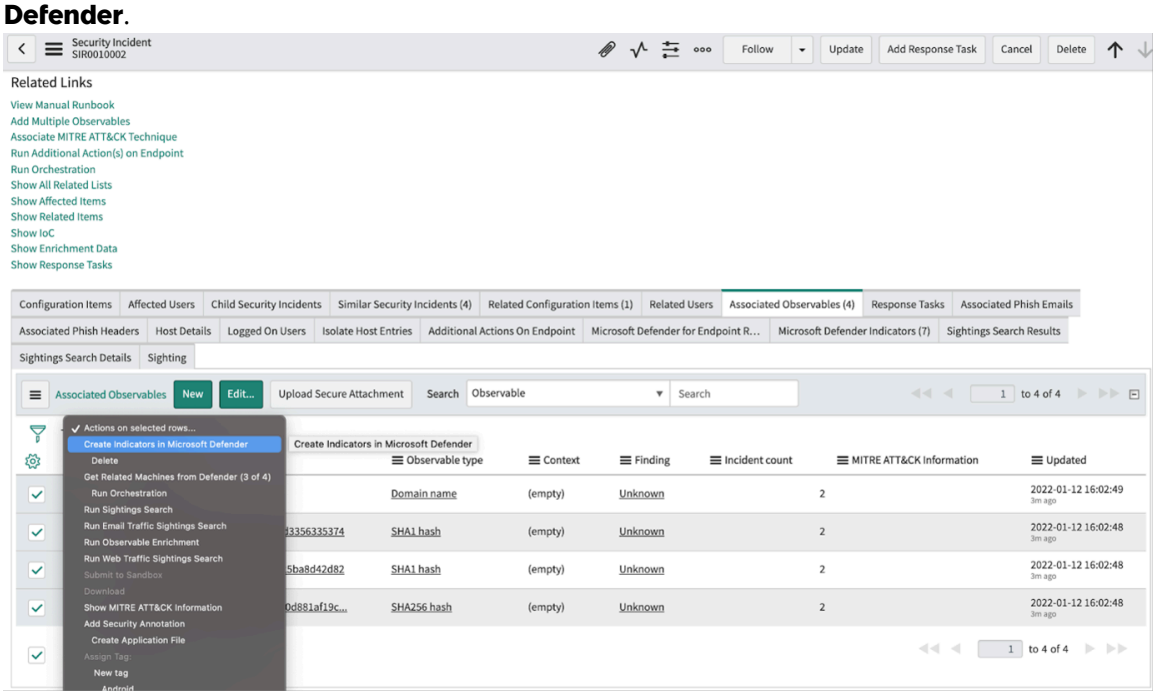
Pourquoi et quand exécuter cette tâche

L'intégration Microsoft Defender pour point de terminaison permet l'enrichissement des observables pour tous les types d'observables mappés dans le module de mappage Observable-Indicateur.

Créer des indicateurs vous permettent de définir une liste d'indicateurs pour la détection, ainsi que pour la prévention et les réponses en matière de blocage. Vous pouvez créer les indicateurs à partir d'un observable associé de l'incident de sécurité.

Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour lesquels vous souhaitez créer des indicateurs dans Microsoft Defender pour point de terminaison.
3. Cliquez sur les listes connexes Observables associés.
4. Ajoutez des observables existants ou créez-en de nouveaux.
5. Sélectionnez les observables.
6. Dans les **actions** sur les lignes sélectionnées, cliquez sur **Créer un indicateur dans Microsoft Defender**.



7. Remplissez les champs du formulaire.

Champ	Description
Observables sélectionnés	Observables qui sont affectés. Cette action peut être utilisée pour créer des indicateurs pour plusieurs observables. Si vous souhaitez désélectionner un observable, vous pouvez le faire en désélectionnant les observables dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si les types d'observables pris en charge ne sont pas mappés, les indicateurs ne sont pas créés dans Microsoft Defender pour ces observables.
Titre	Titre de l'indicateur.
Description	Description de l'indicateur.
Délai d'expiration	Délai d'expiration de l'indicateur.
Actions recommandées	Actions recommandées qui doivent être effectuées pour l'indicateur.
Source	Configuration d'intégration pour créer l'indicateur.
Action	Actions qui seront effectuées si l'indicateur est détecté dans l'organisation. Les valeurs possibles sont les suivantes : ○ **Avertissement** ○ **Bloc** ○ **Audit** ○ **'BlockAndRemediate** ○ **Autorisé**
Application	L'application Microsoft Defender pour point de terminaison associée à l'indicateur. Ce champ ne s'applique qu'à un nouvel indicateur et ne peut pas être utilisé pour un indicateur existant.
Gravité	Gravité de l'indicateur. Les valeurs possibles sont les suivantes : ○ **Faible** ○ **Moyen** ○ **Élevé**
Noms de groupes RBAC	Noms de groupes RBAC auxquels l'indicateur sera appliqué. Les noms sont dans une liste séparée par des virgules.

8. **Cliquer sur Créer un indicateur**
9. Validez l'activité et les messages d'interface utilisateur.
10. Cliquez sur l'onglet **Indicateur Microsoft Defender** pour afficher les résultats.

Mettre à jour les indicateurs dans Microsoft Defender pour point de terminaison

Mettez à jour les indicateurs existants à Microsoft Defender pour point de terminaison partir du menu contextuel de liste ou de la vue de formulaire de l'indicateur Microsoft Defender respectivement.

Avant de commencer
Rôle requis : sn_si.admin, sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

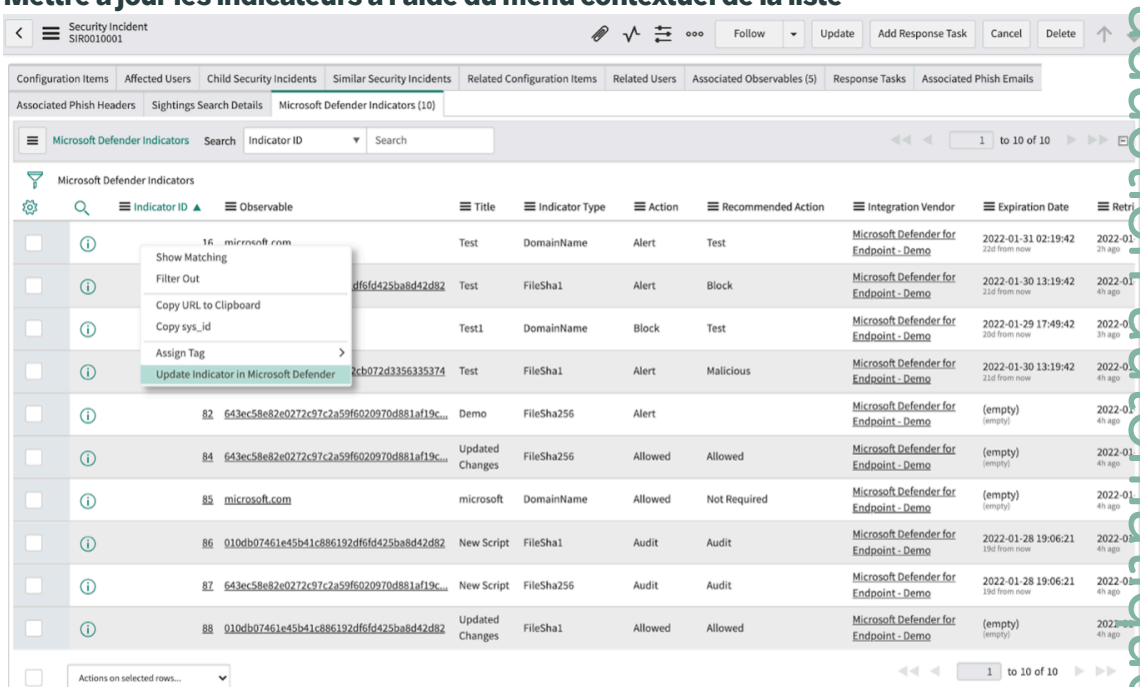
Procédure

1. Accédez à la **Incidents de sécurité** > **Afficher les incidents**.
2. Cliquez sur **Afficher toutes les listes connexes** , puis sur l'onglet **Indicateurs Microsoft Defender** .

> **Remarque :**
>
> Vous devez configurer la liste connexe pour les indicateurs Microsoft Defender, qui apparaissent dans les listes connexes des incidents de sécurité. Pour plus d'informations, voir Actions d'interface utilisateur du formulaire.

3. Mettez à jour les indicateurs Microsoft Defender pour point de terminaison de l'une des façons suivantes :
   - Pour mettre à jour les indicateurs à partir du menu contextuel de la liste, sélectionnez la ligne de l'indicateur que vous souhaitez mettre à jour et cliquez sur **Mettre à jour l'indicateur dans l'option Microsoft Defender** .

Mettre à jour les indicateurs à l'aide du menu contextuel de la liste

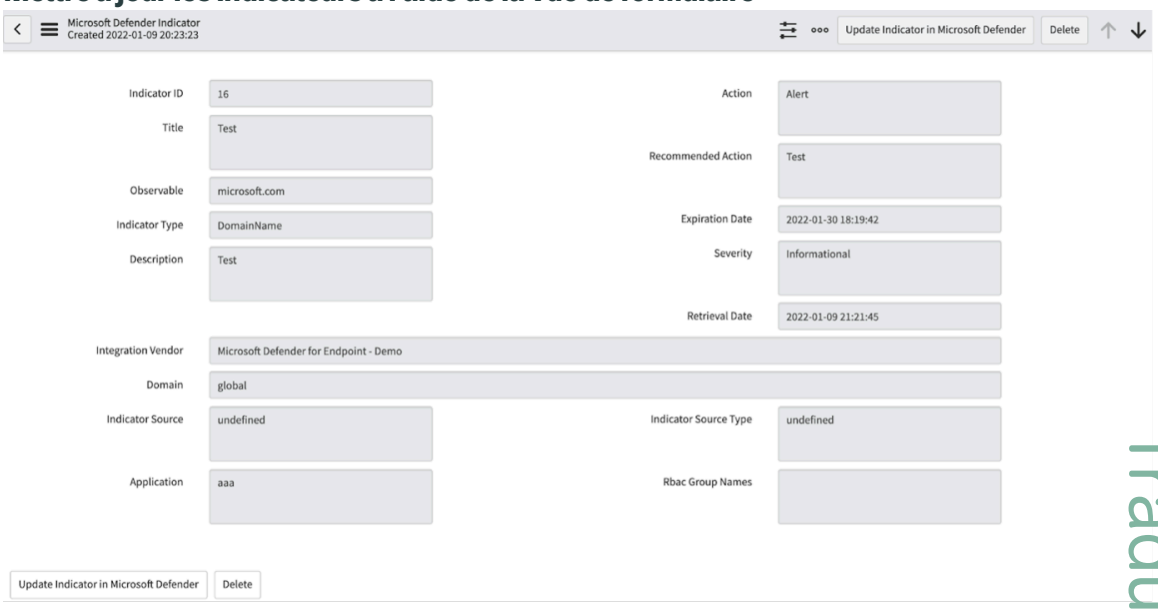


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Pour mettre à jour les indicateurs à partir de la vue de formulaire, cliquez sur **Mettre à jour l'indicateur dans Microsoft Defender** dans la vue de formulaire.

Mettre à jour les indicateurs à l'aide de la vue de formulaire



4. Remplissez les champs du formulaire.

Formulaire d'indicateur Microsoft Defender

Champ	Description
Titre	Titre de l'indicateur.
Description	Description de l'indicateur.
Délai d'expiration	Délai d'expiration de l'indicateur.
Actions recommandées	Actions recommandées à effectuer pour l'indicateur.
Source	Configuration d'intégration pour créer l'indicateur.
Action	Actions effectuées si l'indicateur est détecté dans l'organisation. Les valeurs possibles sont les suivantes : ○ **Avertissement** ○ **Bloc** ○ **Audit** ○ **Bloquer et corriger** ○ **Autorisé**
Application	L'application Microsoft Defender pour point de terminaison associée à l'indicateur. Ce champ ne s'applique qu'à un nouvel indicateur et ne peut pas être utilisé pour un indicateur existant.
Gravité	Gravité de l'indicateur. Les valeurs possibles sont les suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **Faible** ○ **Moyen** ○ **Élevé**
Noms de groupes RBAC	Noms de groupes RBAC auxquels l'indicateur est appliqué. Les noms sont dans une liste séparée par des virgules.

5. Cliquez sur **Mettre à jour l'indicateur**.
6. Validez l'activité et les messages d'interface utilisateur.

Séparation de domaine dans l'intégration Microsoft Defender pour point de terminaison

L'intégration prend en charge Séparation Microsoft Defender pour point de terminaison de domaine. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Prise en charge : basique

Pour la séparation en domaines, procédez comme suit :

1. Créer un utilisateur avec le rôle sn_si.admin dans le domaine respectif.
2. Effectuez les procédures d'intégration Microsoft Defender pour point de terminaison dans le domaine approprié.

Configuration de la limite de débit dans l'intégration Microsoft Defender pour point de terminaison

Configurez la limite de taux de l'API et le délai d'expiration de la limite de taux pour Microsoft Defender pour point de terminaison l'intégration.

Avant de commencer

Rôle requis : sn_si.admin, sn_si.analyst (lecture seule)

Procédure

1. Dans le filtre de navigation, entrez `sys.properties.list`.
   La liste exhaustive des propriétés de la table Propriétés système [sys_properties] s'affiche.
2. Recherchez et modifiez les propriétés suivantes selon vos besoins.

Nom de la propriété	Description
sn_sec_defender_ep.rate_limit_timeout_in_minutes	Si une demande ne s'exécute pas dans le délai spécifié, l'exécution est interrompue et un message d'erreur approprié s'affiche. Valeur par défaut : 75.
sn_sec_defender_ep.request_per_hour_limit	Si l'appel d'API configuré est effectué sur le même point de terminaison dans l'heure, la demande est

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété	Description
	mise en file d'attente jusqu'à ce que le seuil soit atteint ou que le délai d'expiration configuré soit atteint. Valeur par défaut : 1 500.
sn_sec_defender_ep.request_per_minute_limit	Si l'appel d'API configuré est effectué sur le même point de terminaison dans la minute, la demande est mise en file d'attente jusqu'à ce que le seuil soit atteint ou que le délai d'expiration configuré soit atteint. Valeur par défaut : 100.
sn_sec_defender_ep.import_indicator_request_per_minute_limit	Si l'appel d'API configurée est effectué sur le point de terminaison dans la minute, la demande est mise en file d'attente jusqu'à ce que le seuil soit atteint ou que le délai d'expiration configuré soit atteint. Valeur par défaut : 30.

Intégration Microsoft Exchange Online

Pour l'application d'intégration Microsoft Exchange Online par ServiceNow, le ServiceNow AI Platform® Réponse aux incidents de sécurité produit (SIR) est intégré au Microsoft Exchange Online service, l'un des services basés sur le cloud de la Microsoft suite de produits Office 365. L'analyste SOC (Security Operation Center) peut rechercher les menaces liées à la sécurité dans l'environnement de messagerie de votre entreprise et supprimer et corriger les e-mails d'hameçonnage grâce aux fonctions de recherche et de suppression d'e-mails.

Vue d'ensemble de l'intégration Microsoft Exchange Online

En tant qu'analyste des incidents de sécurité, vous exécutez l'intégration à partir de l'interface de l'analyste de sécurité, et le workflow renvoie les détails des e-mails qui correspondent aux critères de recherche. Les recherches d'e-mails sont basées sur des critères qui incluent les lignes d'objet ainsi que les adresses e-mail de l'expéditeur et du destinataire. Une fois la recherche d'e-mails terminée, vous pouvez supprimer les Microsoft Exchange Online e-mails suspects du service, et un processus d'approbation facultatif peut être configuré pour demander l'approbation avant de supprimer les e-mails.

Cette intégration de recherche et de suppression d'e-mails peut être utilisée avec un workflow d'incident ou un runbook de réponse d'hameçonnage plus large. Une fois qu'un utilisateur ou un employé d'entreprise reçoit un e-mail suspect et le signale à l'équipe d'intervention ou à la boîte de réception de l'entreprise, l'e-mail signalé est transféré ServiceNow AI Platform et classé comme un incident de sécurité. Après avoir vérifié qu'un e-mail est une attaque d'hameçonnage, en tant qu'analyste responsable de l'enquête sur les incidents d'hameçonnage, vous pouvez lancer une recherche d'e-mails pour déterminer si d'autres utilisateurs d'entreprise ont reçu cet e-mail d'hameçonnage. La recherche vous permet de localiser les e-mails associés à la même campagne de phishing et d'identifier d'autres victimes potentielles qui ont pu recevoir l'e-mail, l'avoir lu et potentiellement cliquer sur une URL malveillante ou ouvrir une pièce jointe.

Fonctionnalités principales

L'intégration comprend les fonctionnalités clés suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurez les critères de recherche des menaces d'hameçonnage dans Réponse aux incidents de sécurité en fonction des combinaisons des champs expéditeur, destinataire et objet des messages électroniques.
- Pour les recherches par e-mail volumineuses et longues, l'analyste des incidents de sécurité est informé par e-mail lorsque la recherche est terminée avec succès, ainsi que le nombre de messages correspondants.
- L'état des messages individuels vous informe si les destinataires ont lu ou supprimé des e-mails suspects.
- S'ils sont configurés, les processus d'approbation facultatifs garantissent que les e-mails suspects ne sont pas supprimés sans approbation préalable.
- Une piste d'audit complète pour les demandes de suppression, qui inclut le nombre d'e-mails supprimés, est enregistrée dans les notes de travail des incidents de sécurité.
- Si le balisage est configuré, les balises de sécurité enregistrent le lancement et l'exécution réussie des workflows de recherche et de suppression d'e-mails sur les incidents de sécurité.

Versions prises en charge Microsoft Exchange Online

Cette intégration prend en charge Microsoft Exchange Online les services, qui font partie de la Microsoft suite Office 365. L'intégration ne prend pas en charge les environnements Exchange hébergés Microsoft . Microsoft exécute Microsoft Exchange Online les services sur la version Exchange 2016.

Prérequis

Le module d'extension com.snc.si_dep est requis pour toute ServiceNow AI Platform version. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications.

Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour assurer une installation fluide :

1. Cadre de travail d'intégration de sécurité
2. Security Support Common
3. Orchestration du support de sécurité
4. Security Incident Response

Configurer votre Microsoft compte Azure

Effectuez les tâches de configuration suivantes dans votre Microsoft portail Azure avant d'installer l'application ServiceNow pour cette intégration. Ce compte permet au locataire d'accéder aux détails de l'e-mail Microsoft Exchange Online .

Avant de commencer

Rôle requis : Microsoft administrateur du portail Azure

Ce compte est nécessaire pour accéder Microsoft Exchange Online au locataire afin de collecter des détails supplémentaires des e-mails et de supprimer des e-mails. Ce compte est configuré dans le Microsoft portail Azure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les images présentées dans les tâches suivantes sont protégées par des privilèges et sont propriétaires et sont utilisées avec l'autorisation de Microsoft. Ce contenu est sujet à des mises à jour d'ici le Microsoft. Pour vérifier que vous avez accès au contenu le plus récent, consultez le site web de la documentation Microsoft .

Dans les images suivantes, ServiceNow Inc. s'affiche pour le nom de compte dans les exemples du portail Azure. Dans votre compte du portail Azure, le nom de la société de votre compte dans le portail Azure s'affiche.

Procédure

Si vous n'avez pas créé d'ID d'application pour l'authentification OAuth dans le Microsoft portail Azure, procédez comme suit.

a. Connectez-vous au portail Azure à l'aide Microsoft de vos informations d'identification d'administrateur du portail Azure.

b. Saisissez **les inscriptions d'applications** dans la zone **de recherche** .

c. Sélectionnez **Nouvelle inscription**.

d. Remplissez le formulaire Enregistrer une demande qui s'affiche.

Champ	Description
Nom	Nom de l'application. Dans cet exemple, l'intégration de ServiceNow Exchange Online est saisie.
Types de compte pris en charge	Pour ce compte, dans Types de comptes pris en charge, sélectionnez **Comptes dans ce répertoire organisationnel uniquement (nom de votre organisation).** Ce domaine est utilisé pour les recherches d'e-mails.
URL de redirection (facultatif)	Si vous saisissez une valeur pour ce champ, elle n'est pas utilisée par l'intégration.

e. Sélectionnez **Enregistrer**.
Un ID d'application est créé. Cet ID est similaire à un nom d'utilisateur. Vous saisissez cette valeur sur la page de configuration dans le champ **ID de l'application OAuth** au cours de l'étape de configuration dans votre ServiceNow AI Platform instance décrite dans Configurer l'intégration Microsoft Exchange Online.

f. Sous **Gérer**, sélectionnez **Manifest.**

g. Recherchez l'entrée **requiredResourceAccess** (à la ligne 52 ou vers cette date).

h. Modifiez **les valeurs resourceAppId**, **resourceAccess id** et **type resourceAccess** avec l'extrait de code suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
"requiredResourceAccess": [
        {
                "resourceAppId": "00000003-0000-0000-c000-000000000000",
                "resourceAccess": [
                        {
                                "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
                                "type": "Role"
                        },
                        {
                                "id": "dd98c7f5-2d42-42d3-a0e4-633161547251",
                                "type": "Role"
                        }
                ]
        }
 ],
```

i. Sélectionnez **Enregistrer**.

j. Sous **Gérer** , sélectionnez **les autorisations d'API**.

k. Sélectionnez **Ajouter une autorisation**.

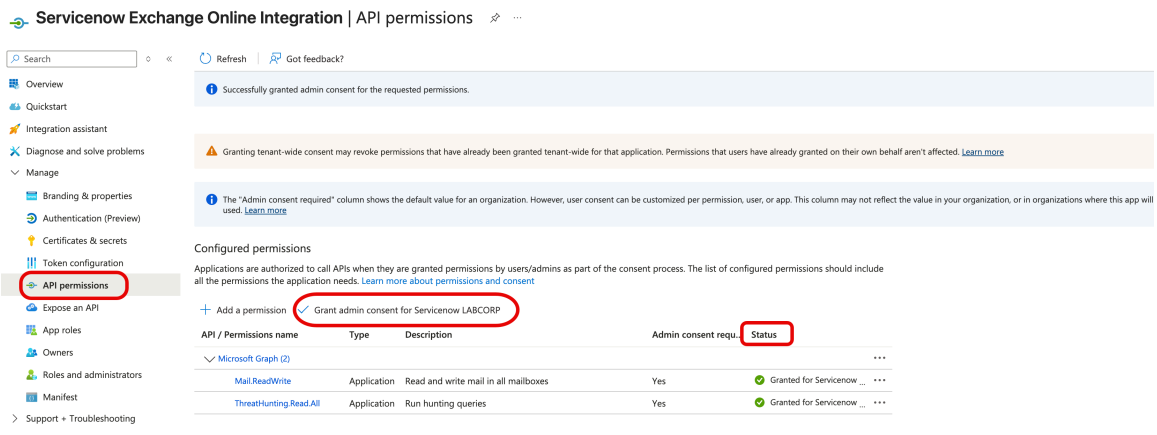
l. Dans le volet Autorisations de l'API de demande qui s'affiche, sélectionnez **Microsoft Graph**.

m. Dans le volet Autorisations de l'API de demande qui s'affiche, sélectionnez **Autorisations d'application**.

n. Dans le champ Sélectionner les autorisations qui s'affiche, saisissez **Menace** et cochez la case **ThreatHunting.Read.All** .

o. Sélectionnez **Accorder le consentement de l'administrateur pour <Organisation>**.

p. Sélectionnez **Oui**.
La valeur **d'état** devrait maintenant être **Accordé pour < Organisation**



>.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

Que faire ensuite
Vous êtes prêt à configurer votre ServiceNow AI Platform® instance pour l'intégration.

Installer Microsoft Exchange Online l'application

Avant d'exécuter l'intégration sur votre instance, installez l'application Microsoft Exchange Online pour l'intégration à partir de .ServiceNow Store

Avant de commencer
Avant d'installer l'application à partir de sur votre ServiceNow AI Platform instance, effectuez toutes les tâches répertoriées dans les listes de ServiceNow Store vérification prérequises.

Rôle requis : admin

Procédure

1. Si vous n'avez pas installé l'application pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes d'installation.
2. Après avoir installé l'application à partir du ServiceNow Store, configurez-la pour qu'elle se connecte à votre ServiceNow AI Platform instance.

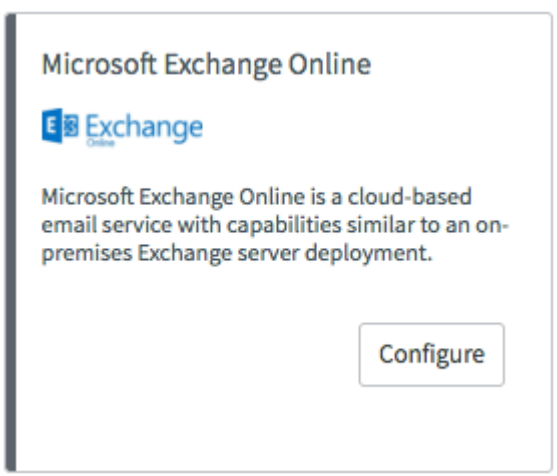
Configurer l'intégration Microsoft Exchange Online

Après avoir installé l'application à partir du ServiceNow Store, configurez-la pour qu'elle se connecte à votre ServiceNow AI Platform instance. Cette activation active les workflows de recherche et de suppression.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Dans votre ServiceNow AI Platform instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**.
2. Localisez la Microsoft Exchange Online tuile.
3. Cliquez sur **Configurer**.



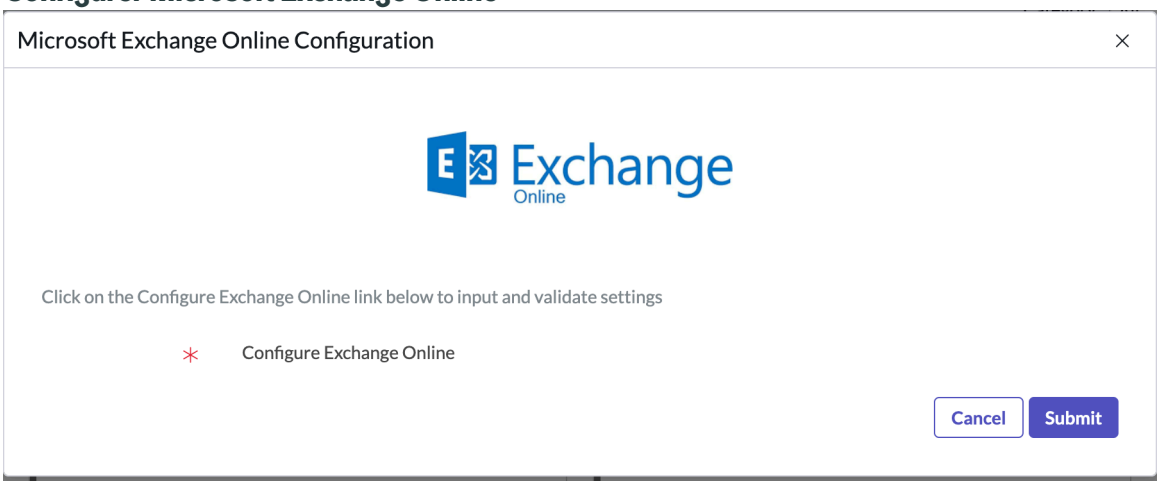
4. Dans la boîte de dialogue Configuration qui s'affiche Microsoft Exchange Online , cliquez sur **Configurer Exchange Online**.

   Un exemple de formulaire complété et validé suit la table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Microsoft Exchange Online



Option	Description
Onglet Paramètres de connexion	
Locataire	Le Microsoft Exchange Online locataire sur lequel vous souhaitez effectuer des recherches. Ce texte est le nom unique qui apparaît après @ pour les adresses e-mail de votre organisation. Dans cet exemple, snowsecops.onmicrosoft.com est le locataire (domaine).
Empreinte du certificat	Une empreinte de certificat est un hachage d'un certificat, calculé sur toutes les données du certificat et sa signature. Les empreintes sont utilisées comme identificateurs uniques pour les certificats, dans les applications lors de la prise de décisions de confiance, dans les fichiers de configuration et affichées dans les interfaces.
ID de l'application OAuth	ID (client) de l'application qui a été généré pour le compte que vous avez créé dans le Microsoft portail Azure. Pour plus d'informations, consultez Configurer votre Microsoft compte Azure.
Secret client OAuth	Mot de passe (secret client) du compte que vous avez créé dans le Microsoft portail Azure. Pour plus d'informations, consultez Configurer votre Microsoft compte Azure.
Onglet Paramètres supplémentaires	
Fenêtre de recherche d'e-mails (jours)	L'historique de recherche d'e-mails varie en nombre de jours. L'intégration recherche les e-mails qui ont été envoyés ou reçus dans le serveur pour le Microsoft Exchange Online nombre de jours calendaires que vous saisissez. Vous devez saisir une valeur comprise entre 1 et 30. 30 jours est le nombre maximal et par défaut que vous pouvez saisir pour une recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	La saisie d'un nombre faible de jours dans la plage de la fenêtre de recherche améliore le délai de réponse, mais vous risquez de ne pas capturer tous les messages correspondants. Ce paramètre global s'applique à toutes les recherches. Avant d'exécuter la recherche d'e-mails, il n'existe aucun paramètre vous permettant de modifier cette valeur pour des recherches individuelles.
Durée de recherche maximale	Utilisez cette option pour définir le seuil du délai d'expiration de la recherche. Si le seuil du délai d'expiration est atteint, la recherche se termine et aucun résultat n'est affiché. Vous pouvez spécifier une valeur par défaut de 90 minutes et une valeur maximale de 240 minutes. En définissant ce seuil, vous pouvez éviter les boucles de recherche interminables qui pourraient causer des problèmes de performances sur le locataire et l'instance Microsoft Exchange OnlineServiceNow .
Balisage	Balise de sécurité. Sélectionné par défaut. Lorsqu'elles sont activées, les balises de sécurité sont automatiquement appliquées aux incidents de sécurité associés lorsque les fonctionnalités de recherche et de suppression sont lancées et terminées avec succès. Les noms de balises par défaut sont affichés, mais les noms et les couleurs des balises peuvent être modifiés. Pour plus d'informations, consultez Modifier les balises de sécurité pour l'intégration Microsoft Exchange Online.
Récupérer les e-mails supprimés	Sélectionné par défaut. Cet élément s'applique uniquement aux e-mails que vous avez supprimés à l'aide de cette intégration. Si vous ne souhaitez pas que les utilisateurs de votre organisation aient accès aux e-mails que vous avez supprimés, vérifiez que la case à cocher est désactivée. Si la case est décochée, les e-mails que vous supprimez à l'aide du workflow de cette intégration sont définitivement supprimés et placés dans le dossier Purges. Ce dossier est un sous-dossier dans le dossier Microsoft Exchange Online Éléments

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

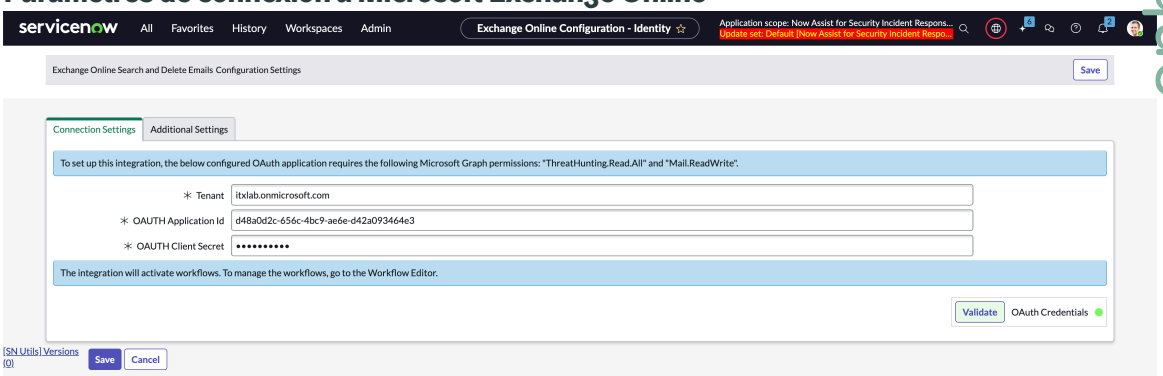
Option	Description
	récupérables auquel un utilisateur ne peut normalement pas accéder. Si vous souhaitez que les utilisateurs récupèrent les e-mails que vous supprimez, cochez cette case. Si cette case est cochée, selon la configuration du compte utilisateur dans Microsoft Exchange Online, les e-mails que vous supprimez à l'aide du workflow de cette intégration sont placés dans le dossier Éléments supprimés de la boîte aux lettres de l'utilisateur. Si un compte est configuré de manière à ce que l'utilisateur puisse afficher le dossier Éléments supprimés dans sa boîte aux lettres, l'utilisateur peut récupérer les e-mails que vous supprimez de son compte Microsoft Exchange Online. Pour plus d'informations, voir Récupérer des éléments ou des e-mails supprimés dans Outlook Web App .
Notification d'achèvement de la recherche	Sélectionnez cette option pour activer les notifications lorsque la recherche est terminée. Si la case **Activer** est cochée, vous recevrez des notifications si des e-mails correspondants sont trouvés. Si la case n'est pas cochée, les notifications d'achèvement de la recherche ne sont pas envoyées.
Approbations	Demander l'approbation pour supprimer des e-mails. La valeur par défaut est effacée. Lorsque la case est décochée, le processus d'approbation facultatif permettant de demander une autorisation préalable avant de Microsoft Exchange Online supprimer des e-mails du service est désactivé. Vérifiez que cette case est décochée si vous souhaitez autoriser votre analyste des incidents de sécurité à supprimer des e-mails sans demander d'autorisation préalable. Si cette option est activée, une demande est envoyée par e-mail à chaque membre d'un groupe d'approbation. Dans la liste, sélectionnez-y un groupe d'approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

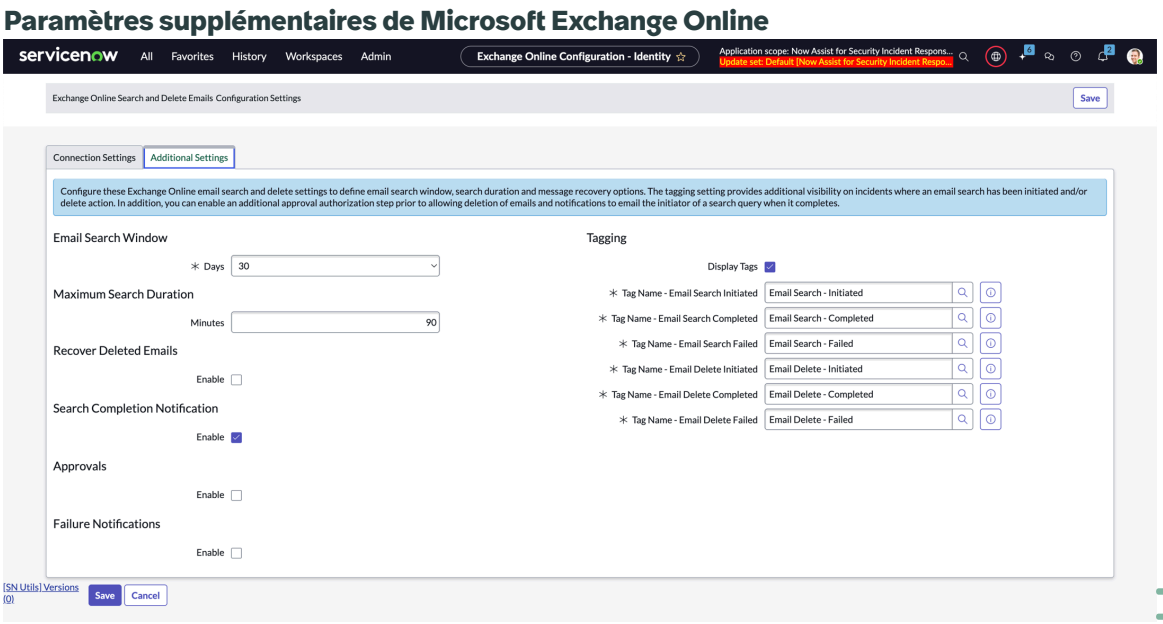
Option	Description
	Lorsqu'une demande est soumise à un groupe d'approbation, une seule approbation du groupe est nécessaire pour terminer la demande. Tout membre du groupe d'approbation dispose d'un pouvoir d'approbation. Le fait d'avoir un groupe de plus d'une personne avec une autorisation d'approbation garantit que ces demandes sont traitées dans les délais.
Notifications de défaillance	Cochez cette case pour activer les notifications d'échec lorsque l'action de recherche ou de suppression échoue en raison d'informations d'identification OAuth non valides. Si cette option est activée, les notifications de défaillance sont envoyées par e-mail à chaque membre du groupe de notifications de défaillance lorsque les informations d'identification OAuth ne sont pas valides. Si la case n'est pas cochée, aucune notification d'échec n'est envoyée.
Seuil de résultat d'e-mail	À partir de la version 10.3 ou ultérieure, vous pouvez spécifier un seuil de suppression d'e-mail pour les approbations. Si le nombre d'e-mails en cours de suppression est supérieur ou égal à la valeur spécifiée ici, la demande de suppression doit être approuvée avant que l'action de suppression ne soit invoquée. Si la valeur de seuil est définie sur 1, chaque demande de suppression doit être approuvée.

Paramètres de connexion à Microsoft Exchange Online



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Choisissez-en un pour continuer.

Option	Description
Enregistrer	Enregistrez vos modifications. Cette action ne vérifie pas votre connexion.
Dans l'onglet Paramètres de connexion, cliquez sur Valider.	Cette action valide votre authentification de certificat, votre connexion au serveur MID et vos informations d'identification OAuth. Si vos informations d'identification sont valides, le bouton **Valider** et les deux indicateurs sont verts.

Trouble?
Si un message d'erreur s'affiche ou si un ou plusieurs des indicateurs à droite du bouton Valider sont rouges, vérifiez que les informations d'identification du compte utilisateur que vous avez saisies sont valides. Entrez vos informations d'identification et cliquez à nouveau sur **Enregistrer** .

Échec de la validation

Reportez-vous au tableau suivant pour en savoir plus sur le bouton **Valider** et les icônes colorées.

État du bouton et des indicateurs Valider	Description
Le bouton Valider est vert et tous les petits indicateurs colorés sont verts.	Indique que la connexion au serveur MID et les informations d'identification sont valides.
Le bouton Valider est rouge clair avec une bordure bleue et un ou tous les petits indicateurs colorés sont orange.	La validation est en cours de traitement. La validation peut prendre quelques instants de plus.
Le bouton Valider est rouge clair et un ou tous les petits indicateurs colorés sont rouges.	• Le bouton d'authentification basée sur certificat Exchange Online ou d'informations d'identification OAuth

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État du bouton et des indicateurs Valider	Description
	est rouge : indique que les informations d'identification Exchange Online ne sont pas valides. • L'authentification basée sur certificat Exchange Online et les boutons Prêt pour le serveur MID sont rouges : indique que le serveur MID n'est pas accessible et que, par conséquent, l'authentification basée sur certificat Exchange Online via le serveur MID a échoué. • L'indicateur d'authentification basée sur certificat Exchange Online est rouge, mais le bouton Serveur MID Prêt est vert : indique que le serveur MID est actif et configuré correctement, mais que l'authentification basée sur certificat Exchange Online est incorrecte.

Définir des critères de recherche d'e-mails et demander une recherche dans le Microsoft Exchange Online service

En tant qu'utilisateur disposant du rôle sn_si.analyst, définissez les critères de recherche et soumettez une demande de recherche d'e-mails basée sur les détails d'incident d'un enregistrement d'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Les figures de cette procédure sont affichées avec **les formulaires à onglets** sélectionnés dans les paramètres système. Pour plus d'informations sur la sélection et l'effacement des formulaires à onglets, consultez la section intitulée Afficher les formulaires à onglets dans Configuration de la mise en page du formulaire sur le site Web de la documentation du produit ServiceNow .

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

L'état des messages individuels qui correspondent à la requête de recherche et les résultats de la recherche sont consignés dans l'enregistrement d'incident de sécurité. Si les notifications par e-mail sont activées, vous pouvez afficher les résultats de la recherche dans un e-mail.

Les critères de recherche peuvent inclure les adresses d'expéditeur de message, les adresses de destinataire ou les noms de sujets. Les combinaisons suivantes de paramètres de recherche d'objet, d'expéditeur et de destinataire sont souvent utilisées pour trouver des e-mails liés au phishing qui peuvent faire partie d'une seule campagne d'hameçonnage :

- Retrouvez tous les e-mails originaux envoyés par un compte de phishing : Recherche par expéditeur.
- Trouvez tous les e-mails originaux pour une seule campagne de phishing : Recherche par sujet et par expéditeur.
- Retrouvez tous les e-mails reçus pour une seule campagne de phishing (originale et transférée, n'importe quel expéditeur) : Recherche par sujet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Trouvez tous les e-mails transférés pour un seul e-mail d'hameçonnage d'un seul utilisateur : Recherche par destinataire + objet.
- Trouvez tous les e-mails liés au phishing envoyés à un seul utilisateur : Recherche par expéditeur + destinataire.

Remarque : Les recherches sont effectuées sur les e-mails envoyés ou reçus au cours des 30 derniers jours calendaires, sauf si une fenêtre de recherche plus courte est configurée lors de la configuration initiale. Une recherche d'e-mails réussie est requise avant de pouvoir supprimer des e-mails.

L'exemple suivant vous montre comment lancer une recherche à partir d'un ServiceNow AI Platform incident de sécurité. Un incident de sécurité est créé en fonction de l'e-mail d'origine d'une attaque de phishing suspectée sur le Microsoft Exchange Online serveur de votre organisation. Pour cet exemple, les critères de recherche sont Expéditeur (De) plus Objet, où De est phisher@cbazyx.com et Objet est Connexion à votre compte.

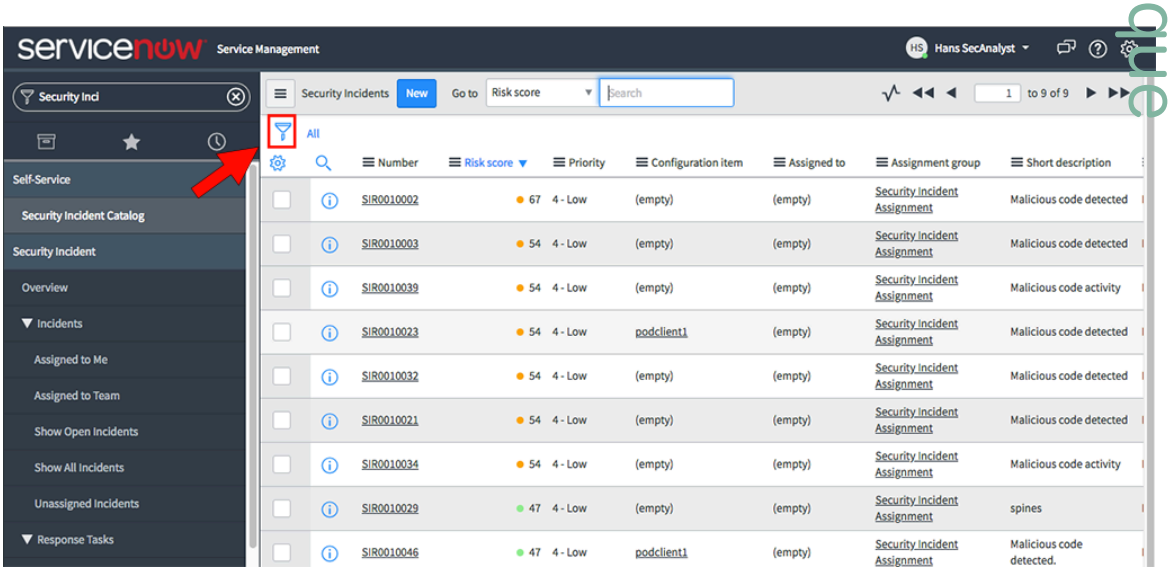
Les résultats des recherches sur les sujets sont renvoyés lorsque la recherche trouve des chaînes de texte contenant des mots clés qui correspondent aux critères de recherche entrés. Dans cet exemple, l'objet est la connexion à votre compte. Utilisez l'opérateur **ET** pour séparer les conditions de recherche De et Objet afin de retourner des résultats pour tous les e-mails contenant ces critères de recherche donnés. Les étapes suivantes décrivent comment configurer une recherche qui trouve uniquement les e-mails contenant du texte de ligne d'objet envoyés par un compte de hameçonnage spécifique.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents** et localisez l'incident de sécurité avec lequel vous travaillez.
2. Vous pouvez également procéder comme suit pour définir et exécuter un filtre afin que seuls les incidents de sécurité créés par des événements de phishing soient affichés.

   a. Accédez à la **Incident de sécurité** > **Afficher les incidents** pour ouvrir la liste des incidents de sécurité.

   b. Dans le coin supérieur gauche de la liste qui s'affiche, cliquez sur l'icône de filtre.

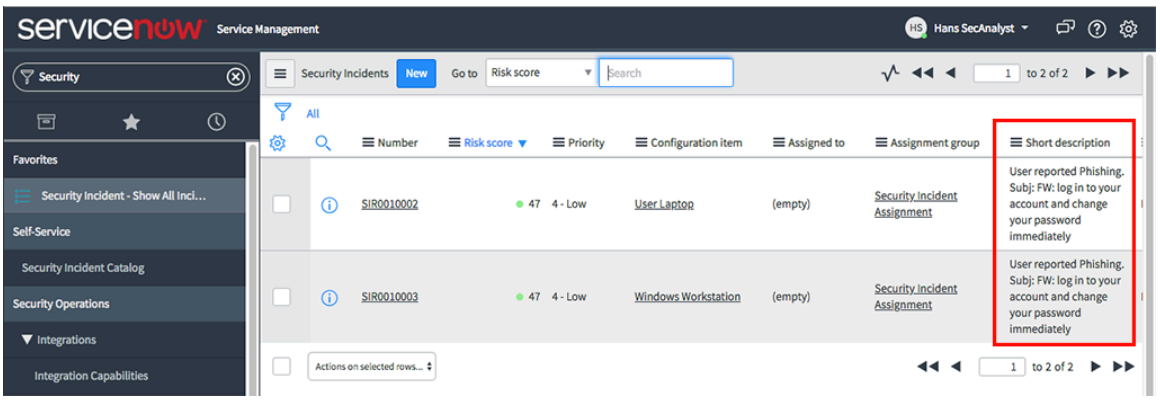


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Dans les champs qui s'affichent, sélectionnez **Description brève** > **contient** Dans les listes de choix, saisissez **Hameçonnage signalé par l'utilisateur** et cliquez sur **Exécuter**.

Les incidents de sécurité liés au phishing s'affichent.

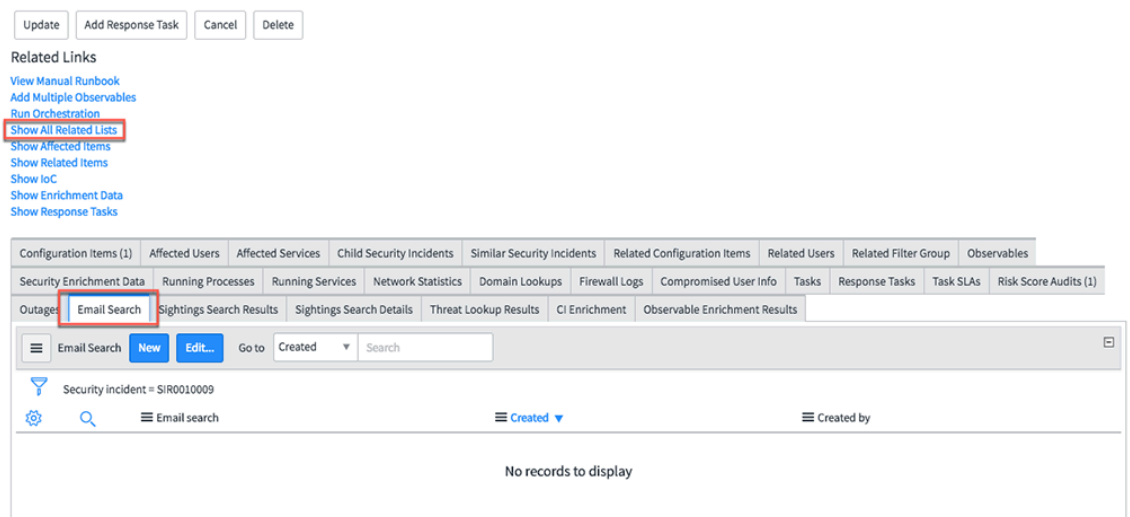


d. Utilisez le texte de la colonne Brève description pour vous aider à localiser l'incident de sécurité avec lequel vous travaillez.

e. Dans la colonne Numéro, cliquez sur un incident de sécurité pour ouvrir un enregistrement.

3. Faites défiler l'enregistrement d'incident de sécurité jusqu'au bas et cliquez sur la liste connexe Recherche d'e-mails.

Si la liste connexe Recherche d'e-mails n'est pas affichée, cliquez sur le lien connexe **Afficher toutes les listes connexes** pour afficher cette liste connexe.



4. Dans la liste connexe Recherche d'e-mails, cliquez sur **Nouveau** pour créer un enregistrement de recherche d'e-mails.
Le formulaire Recherche d'e-mail s'affiche. Si vous souhaitez réexécuter cette requête de recherche pour le même incident lié à l'hameçonnage avec des modifications mineures, vous pouvez réutiliser cet enregistrement de requête de recherche. Cependant, il est peu probable que vous utilisiez cette recherche pour un autre incident lié au phishing, car les campagnes de phishing sont dynamiques et les champs Expéditeur et Message changent souvent.

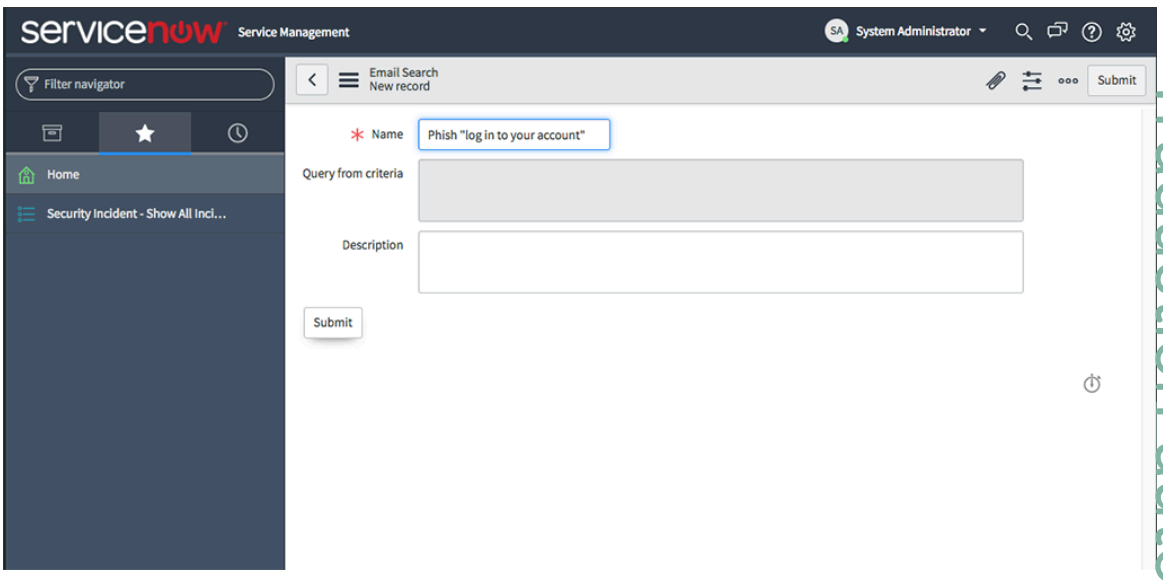
5. Facultatif : Pour modifier un enregistrement de requête de recherche existant, cliquez sur **Modifier**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Renseignez les champs du formulaire Recherche d’e-mails.

Champ	Description
Nom	Informations permettant de décrire le type de recherche. Pour cet exemple, un nom pour une recherche De + Objet est Phish « connectez-vous à votre compte ».
Description	Informations relatives à la recherche dans le serveur de messagerie. Un exemple pour cette recherche est From=phisher@cbazyx.com + Objet=connectez-vous à votre compte.

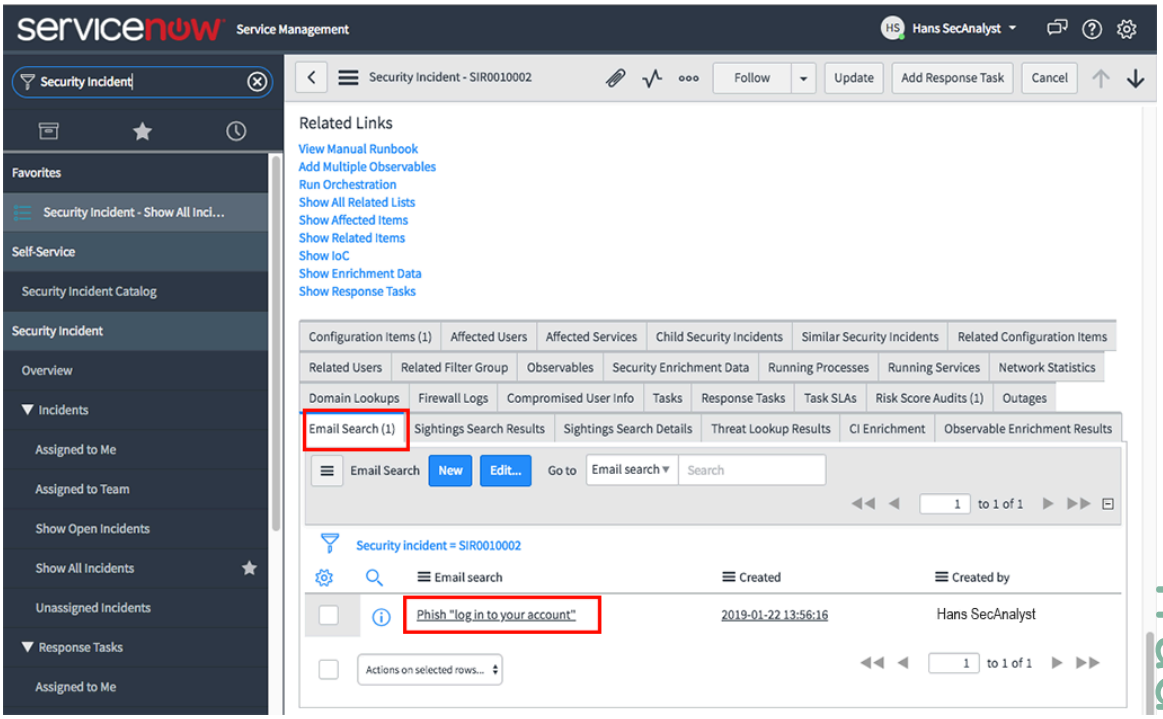


7. Cliquez sur **Envoyer**.
   L’incident de sécurité s’affiche et le nom de la recherche d’e-mail s’affiche dans la colonne Recherche d’e-mails de la liste connexe Recherche d’e-mails. Avant de pouvoir utiliser cette nouvelle requête de recherche, des critères de recherche doivent être définis pour l’enregistrement de recherche.

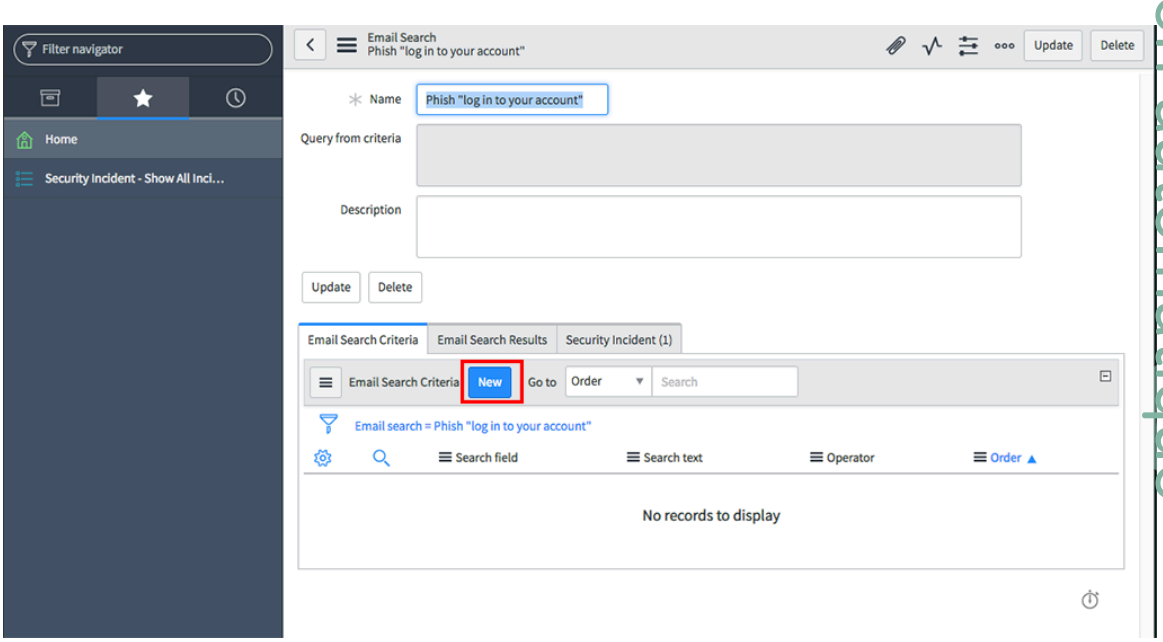
8. Pour définir des critères de recherche, une fois la liste connexe Recherche d’e-mails sélectionnée, dans la colonne Recherche d’e-mails, cliquez sur **Phish « se connecter à votre compte ».**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Dans l'enregistrement de recherche d'e-mails qui s'affiche, cliquez sur la liste connexe Critères de recherche d'e-mails et cliquez sur **Nouveau**.



10. Renseignez les champs du formulaire Critères de recherche d'e-mails.

Un exemple de formulaire rempli suit la table.

Champ	Description
Recherche d'e-mail	Le champ est renseigné automatiquement avec le nom que vous avez saisi pour l'enregistrement de recherche d'e-mail.

Traduction automatique

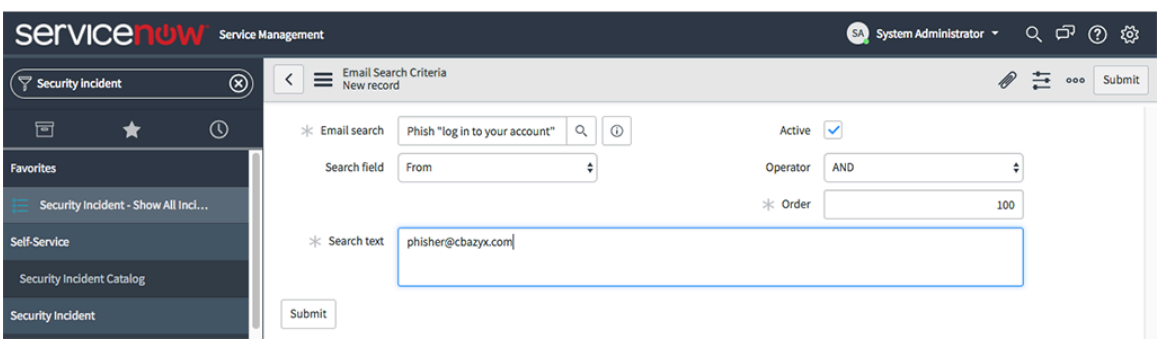
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Icône de recherche	Chercher dans une liste. Une liste des recherches enregistrées. Cliquez sur l'icône pour ouvrir une liste des recherches d'e-mails enregistrées. Cliquez sur un élément de cette liste pour supprimer la recherche actuelle et sélectionner une recherche d'e-mail précédemment enregistrée.
Icône d'informations	Icône utilisée pour afficher l'enregistrement de recherche d'e-mail. Cliquez sur l'icône pour afficher l'enregistrement de recherche d'e-mail.
Champ de recherche	Critère de recherche (**Objet**, **De** ou **Destinataire**). Sélectionnez le critère de recherche dans la liste de choix et définissez une valeur que vous souhaitez rechercher dans le champ de texte. Pour cet exemple, commencez par De phisher@cbazyx.com (l'adresse e-mail de l'expéditeur de l'e-mail d'hameçonnage).
Actif	Option permettant d'activer la recherche. La recherche est activée par défaut. Si vous décochez cette option, cet enregistrement n'est pas inclus dans une recherche.
Opérateur	Opérateurs (**ET, OU**) pour affiner votre recherche. **ET** : le système recherche les conditions séparées par **ET** et ne renvoie les résultats que si toutes les conditions sont remplies. Pour la recherche expéditeur plus objet, utilisez l'opérateur **ET** afin que les deux conditions de recherche soient remplies lors de la recherche d'e-mail. Pour cet exemple, utilisez l'opérateur **ET** pour que la requête soit De (Expéditeur) = phisher@cbazyx.com **ET Objet** = Connectez-vous à votre compte. **OU** : le système recherche et renvoie des résultats si l'une des conditions séparées par **OU** est remplie. Par exemple, From (Sender) = phisher@cbazyx.com **OR** From (Sender) = phisher-2@cbazyx.com.
Ordre	Si vous entrez plus de deux conditions de recherche, utilisez l'ordre pour classer les conditions par ordre de priorité. 100 est la valeur par défaut. Saisissez une valeur comprise entre 1 et 100 pour chaque

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

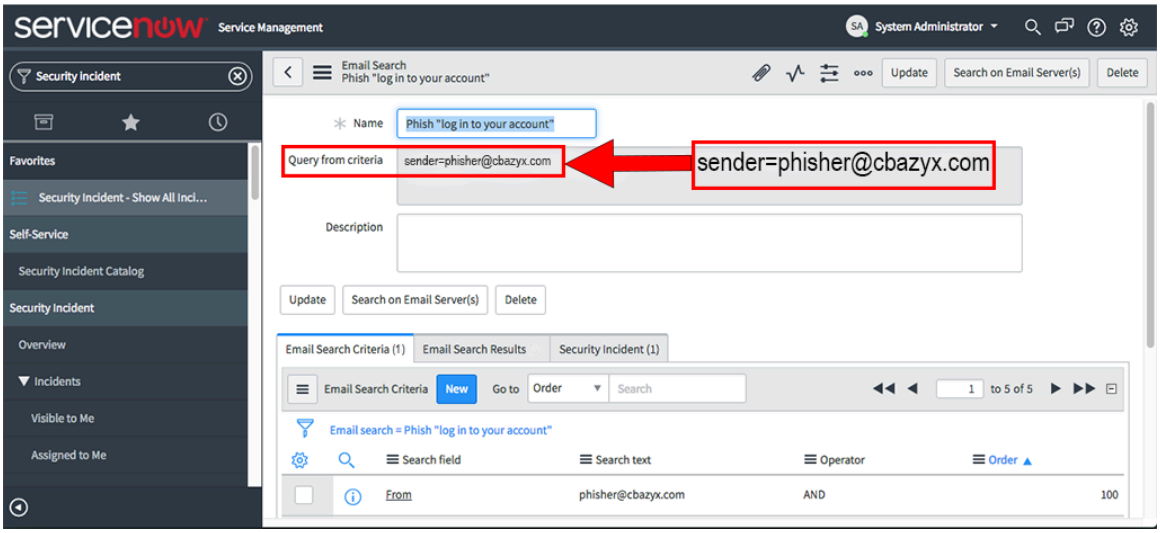
Champ	Description
	condition, par exemple 100, 95, 90, 80. La condition avec le numéro le plus bas affecté a la priorité de recherche la plus élevée au sein d'un groupe de conditions.
Texte de recherche	Les valeurs de texte (mots clés) pour la recherche (adresses e-mail ou lignes d'objet). Le champ de recherche contient le texte utilisé dans la recherche, par exemple, phisher@cbazyx.com. Pour que la recherche renvoie des résultats précis pour les recherches de l'expéditeur (De) et du destinataire, les chaînes de recherche doivent correspondre exactement. Pour les recherches par sujet, la chaîne de recherche peut contenir des mots clés qui font partie d'une chaîne plus large. Par exemple, un objet peut contenir la chaîne de recherche exacte qui correspond à un en-tête de message transféré ou de réponse tel que FW : connectez-vous à votre compte et changez votre mot de passe immédiatement. Par exemple, Connectez-vous à votre compte sont des mots-clés exacts dans la chaîne connectez-vous à votre compte et changez votre mot de passe immédiatement. Aucune désignation de caractère générique (*) n'est requise pour prendre en charge un type de recherche *contain*. Actuellement, il n'existe aucune méthode de filtrage pour faire correspondre une chaîne de recherche exacte qui ne fait pas partie d'une chaîne de texte plus grande.



11. Cliquez sur **Envoyer**.
L'enregistrement de recherche d'e-mail s'affiche. Dans le champ **Critères de requête d'origine** , les critères de recherche que vous avez ajoutés pour l'expéditeur (De) s'affichent.

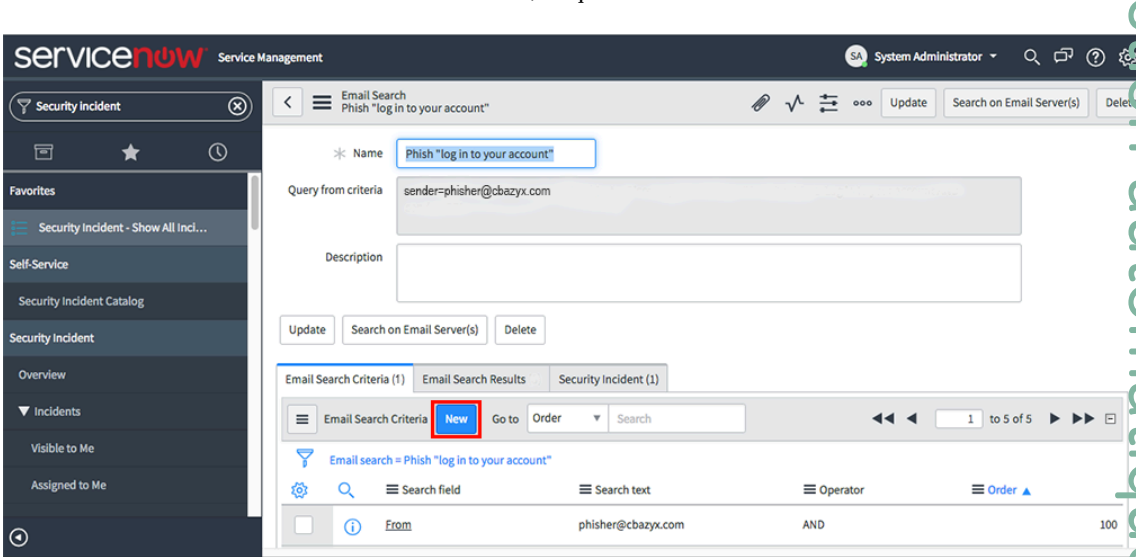
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



12. Pour mettre à jour ces critères de recherche d'e-mails avec plus d'informations afin que la requête inclue la condition objet-plus-expéditeur que vous souhaitez, suivez les étapes pour ajouter une autre condition de recherche.

a. Dans la liste connexe aux critères de recherche d'e-mails, cliquez sur **Nouveau**.



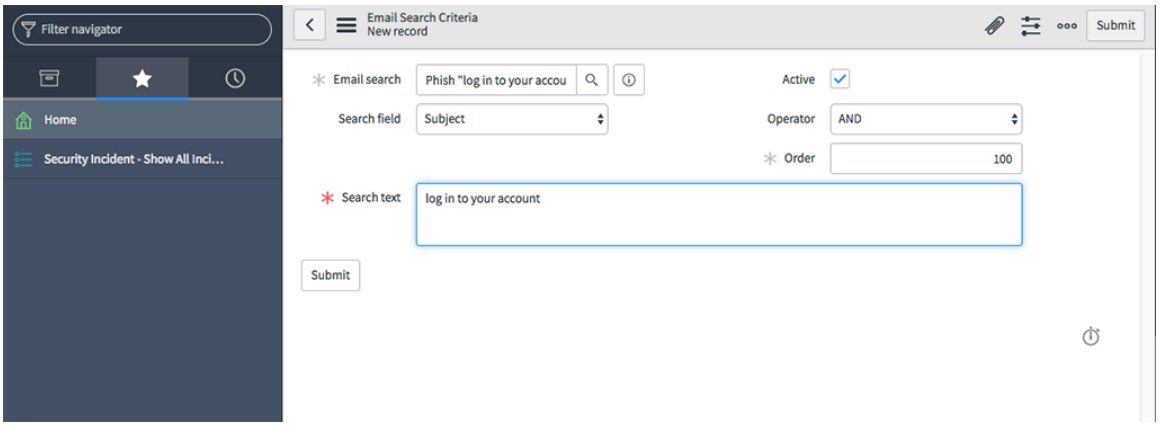
b. Dans la liste **des champs Rechercher**de l'enregistrement Critères de recherche d'e-mails qui s'affiche, sélectionnez **Objet**.

c. Dans la liste Opérateur, sélectionnez**ET** ou **OU**.
Si vous sélectionnez **OU**, la recherche renvoie des résultats si les mots clés de la chaîne de texte de la ligne d'objet correspondent, ou si la condition d'adresse e-mail est vérifiée. **ET** est sélectionné pour cet exemple afin que la recherche ne renvoie des résultats que pour les e-mails qui contiennent les mots clés de la chaîne de texte de l'objet et qui correspondent à l'adresse e-mail de l'expéditeur.

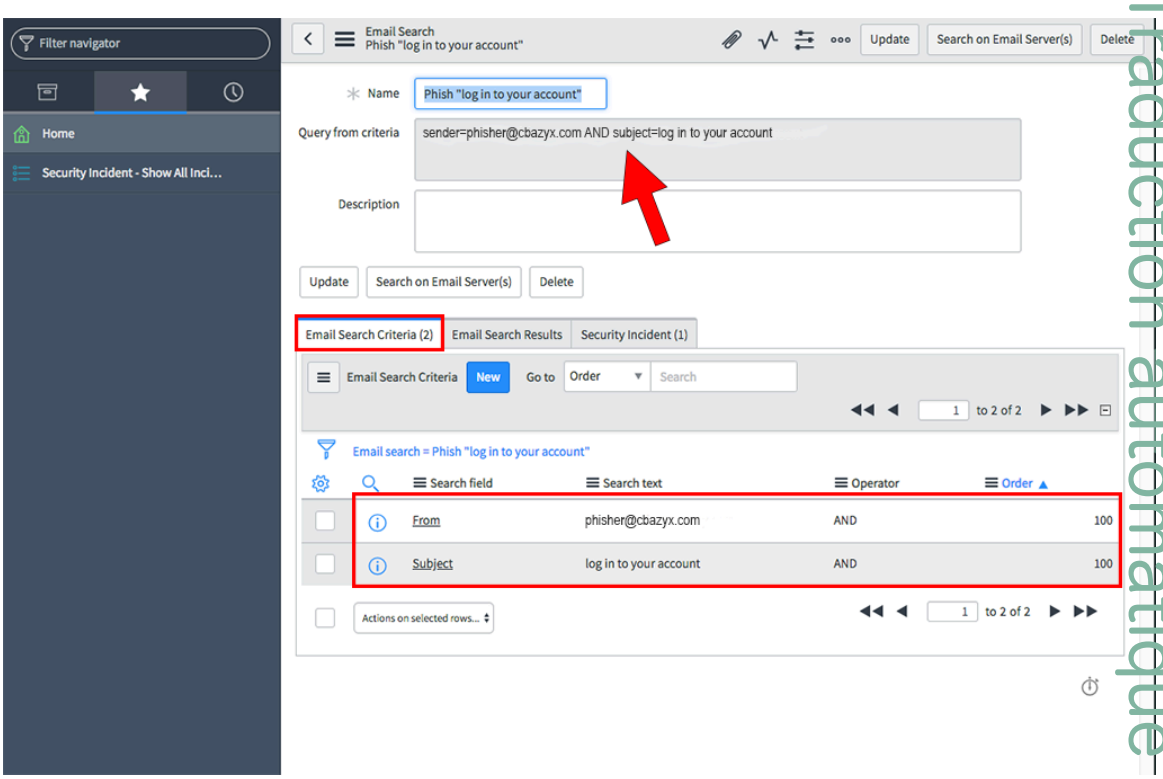
d. Dans le champ **Texte de recherche** , saisissez la valeur du texte de la ligne d'objet, connectez-vous à votre compte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Cliquez sur **Envoyer**.
La nouvelle condition s'affiche dans la liste connexe Critères de recherche d'e-mails, et les deux conditions sont affichées dans le champ **Interroger à partir de critères** , séparés par l'opérateur **ET** .



Traduction automatique

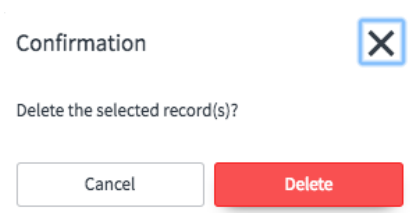
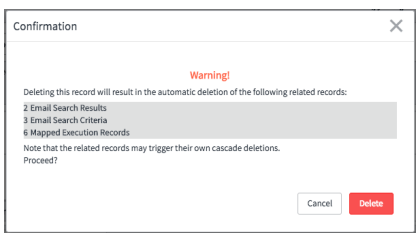
f. Facultatif : Si vous avez plus de deux conditions de recherche et que vous sélectionnez **ET** pour séparer chaque condition, définissez la valeur d'ordre pour les classer par ordre de priorité.

g. Continuez à ajouter, modifier ou supprimer des critères de recherche comme vous le souhaitez, puis cliquez sur **Mettre à jour** pour enregistrer vos changements dans l'enregistrement.

13. Choisissez une option pour continuer.

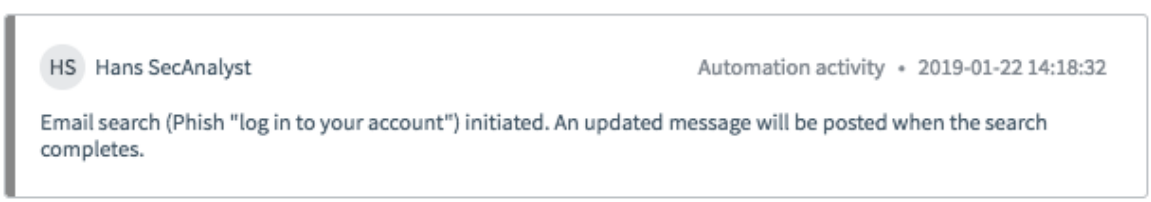
Option	Description
Mettre à jour	Mettez à jour et enregistrez vos changements dans l'enregistrement.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Rechercher sur les serveurs de messagerie	Lancez une recherche sur les serveurs avec les critères que vous avez enregistrés dans l'enregistrement des critères de recherche d'e-mails.
Supprimer	Supprimez cet enregistrement de recherche d'e-mails de votre ServiceNow AI Platform instance. Cette action ne supprime pas les e-mails réels. Elle supprime uniquement l'enregistrement de recherche utilisé pour trouver des messages. Une boîte de dialogue s'affiche. Si vous cliquez sur **Supprimer**, les résultats de la recherche d'e-mails et les critères de recherche d'e-mails de cet enregistrement de recherche sont supprimés.  Si un enregistrement possède des résultats de recherche, l'avertissement suivant s'affiche. 

14. Pour lancer une recherche d'e-mail, sur l'enregistrement de recherche d'e-mail, cliquez sur **Rechercher sur le(s) serveur(s) de messagerie**.
Un message s'affiche pour indiquer que la demande de recherche a été envoyée.

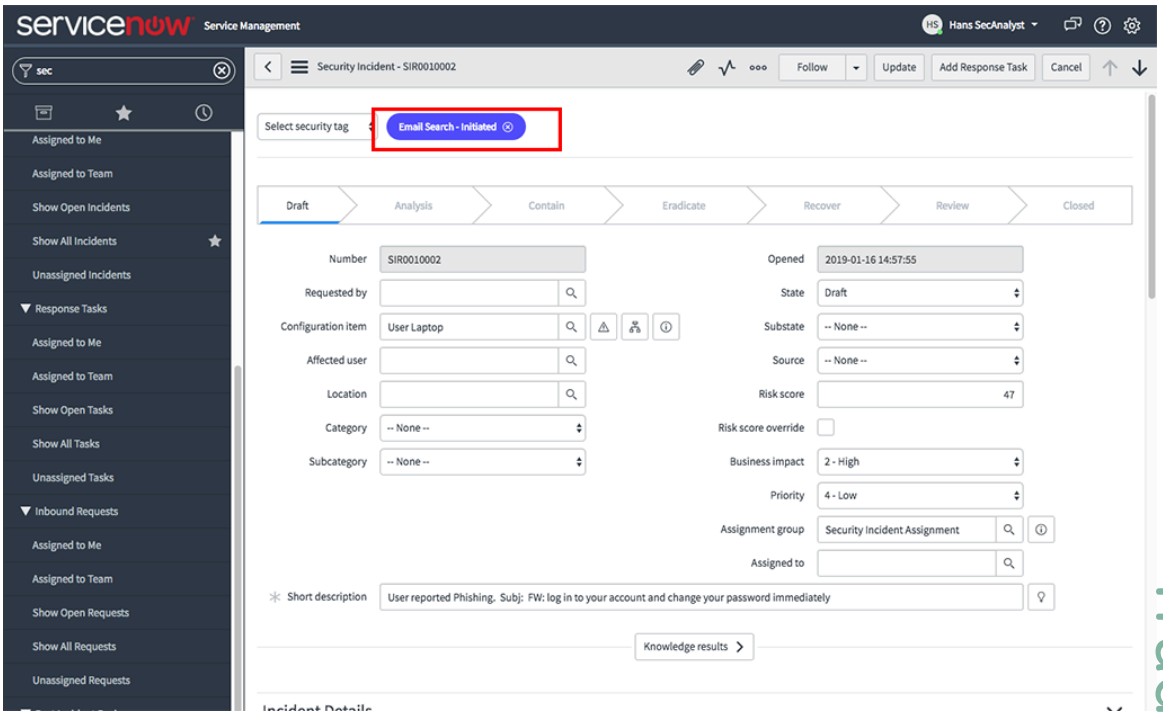
    Sur l'enregistrement d'incident de sécurité, une note de travail s'affiche indiquant qu'une recherche a été lancée.

    Si le balisage est activé, en haut de l'enregistrement d'incident de sécurité, la balise de sécurité Recherche d'e-mail - Initiée s'affiche.

Traduction automatique

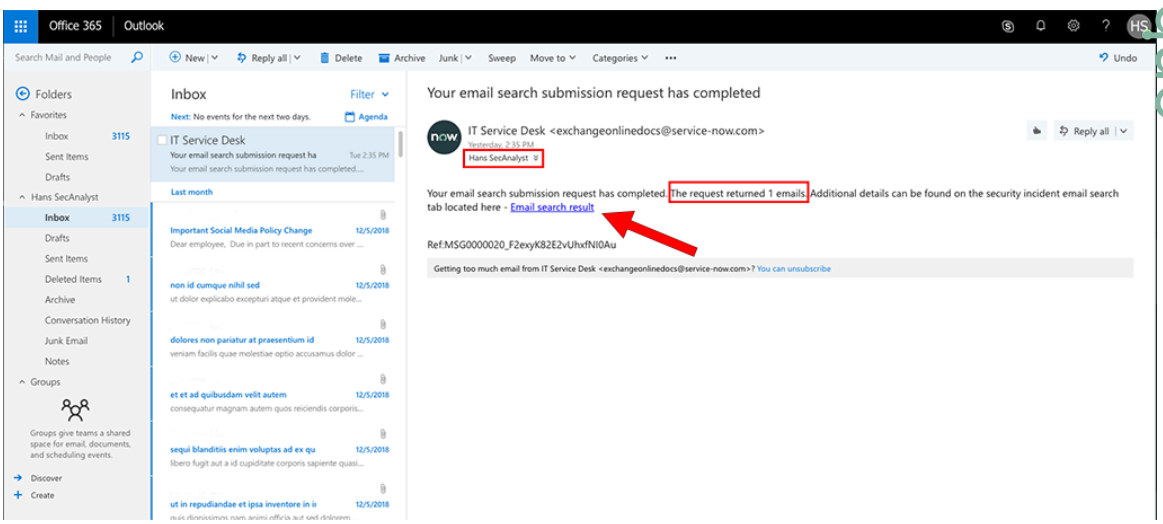
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois la recherche terminée, si les notifications par e-mail sont activées, un e-mail est envoyé à l'adresse e-mail de la personne qui a initié la recherche.

Dans cet exemple, l'utilisateur ayant le rôle sn_si.analyst, Hans SecAnalyst, a soumis cette recherche. L'image suivante montre que cette notification est envoyée à un compte dans Microsoft Exchange Online. Toutefois, ces notifications peuvent être envoyées à un autre service de messagerie, selon les besoins.

Cette notification vous permet d'afficher tous les résultats correspondants qui nécessitent un suivi et une suppression. L'exemple suivant montre qu'il existe un e-mail qui correspond aux critères de recherche. Un lien de résultat de recherche d'e-mail vers l'enregistrement de résultat de recherche d'e-mail dans votre ServiceNow AI Platform instance est également fourni. Si vous souhaitez afficher l'enregistrement de recherche, cliquez sur ce lien.



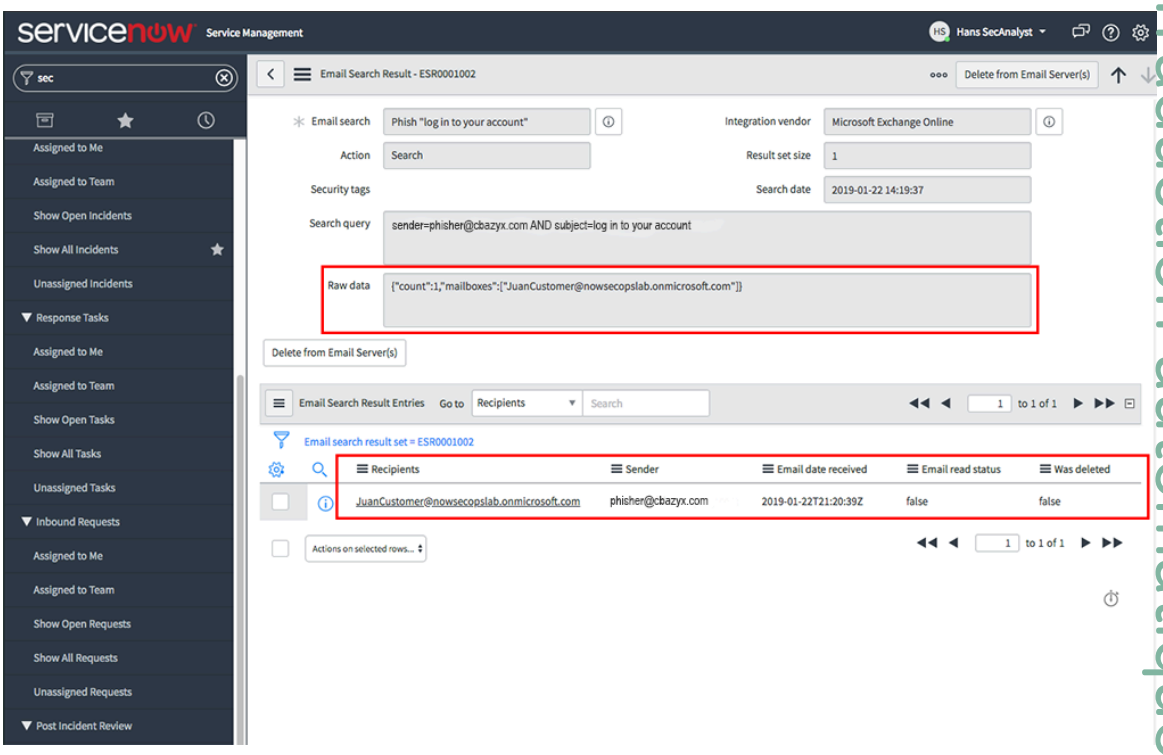
15. À partir de cet e-mail, pour afficher les résultats de la recherche, cliquez sur le lien **Résultat de recherche d'e-mail** .

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

L’enregistrement du résultat de la recherche d’e-mail s’affiche. Sur cet enregistrement, vous pouvez vérifier et examiner les données suivantes.

- Dans le champ **Données brutes** , le nombre d’e-mails correspondant aux critères de recherche {"count » :1}, et les adresses de boîte aux lettres où les e-mails ont été trouvés sont affichés ["JuanCustomer@nowsecopslab.onmicrosoft.com"].
- Dans la colonne Destinataires, le destinataire est (JuanCustomer@nowsecopslab.onmicrosoft.com).
- Dans la colonne Expéditeur , la source de l’e-mail s’affiche.
- Dans la colonne Date de réception de l’e-mail , la date et l’heure de réception de l’e-mail s’affichent pour vous aider à suivre les chronologies des campagnes d’hameçonnage.
- Dans la colonne État de lecture de l’e-mail , l’e-mail dans cet exemple n’a pas été lu (faux). Si un e-mail a été lu, la valeur Vrai s’affiche.
- Dans la colonne A été supprimé , l’e-mail de cet exemple n’a pas été supprimé. Si un e-mail a été supprimé, la valeur Vrai s’affiche.

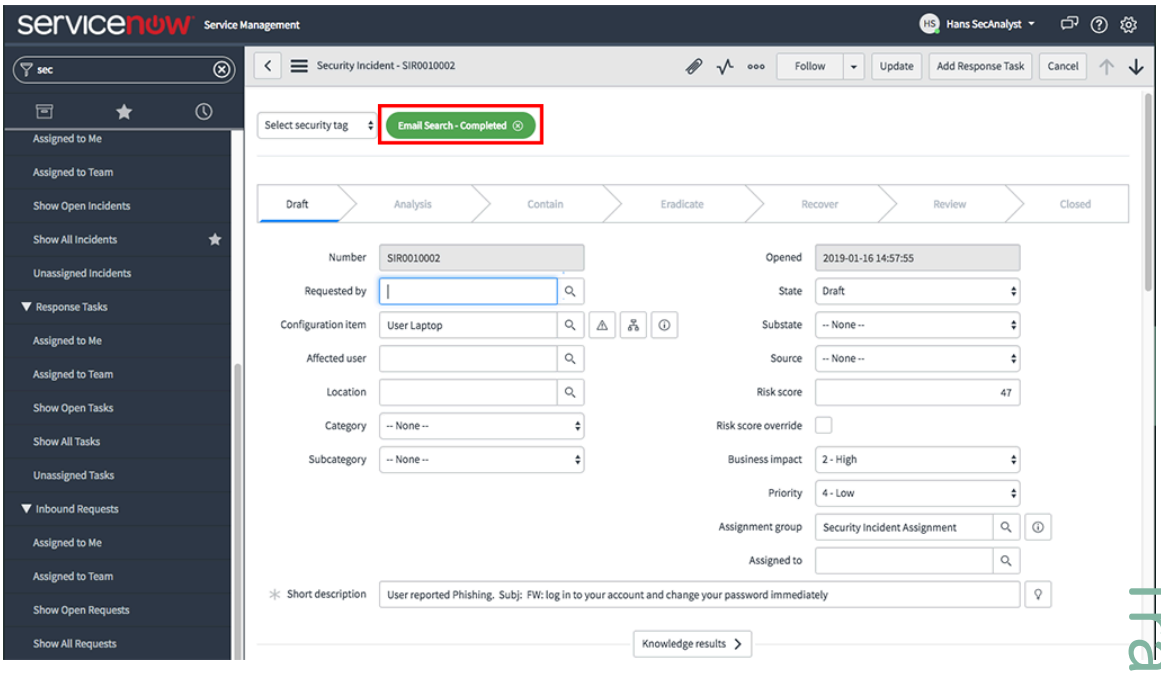


Traduction automatique

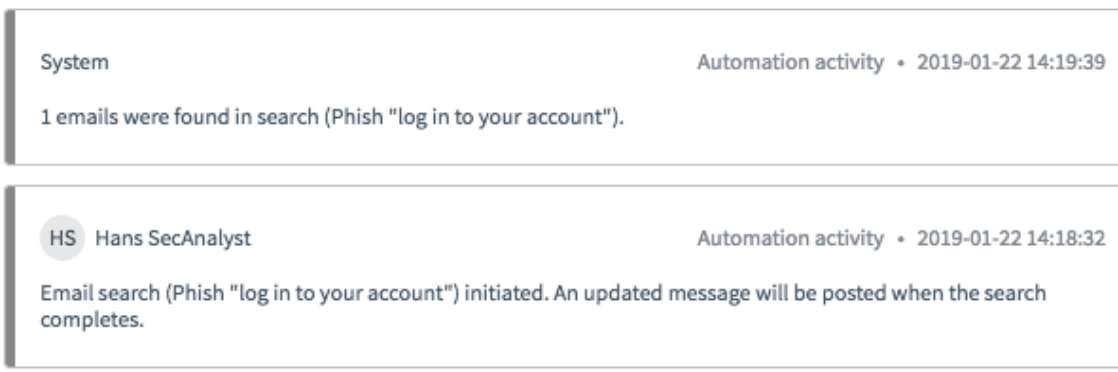
16. Pour afficher les résultats de recherche de l’incident de sécurité, procédez comme suit.

a. Accédez à la **Incident de sécurité** > **Incidents** et ouvrez l’incident de sécurité avec lequel vous travaillez.
En haut de l’enregistrement, lorsque la recherche est terminée avec succès, la balise de sécurité Recherche d’e-mail - Terminée remplace la balise de sécurité Recherche d’e-mail - Initiée .

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Des notes de travail s'affichent indiquant que la recherche a été effectuée avec succès et qu'un e-mail correspondant a été trouvé.

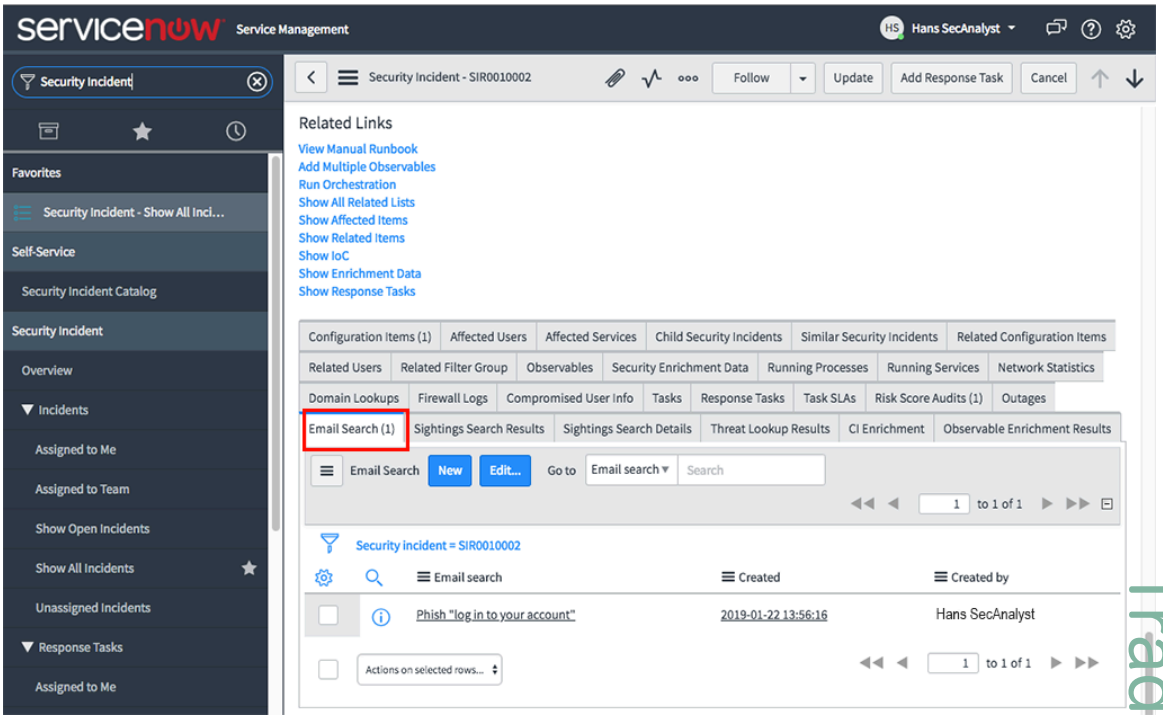


b. Faites défiler l'enregistrement d'incident de sécurité jusqu'au bas et cliquez sur la liste connexe Recherche d'e-mails.

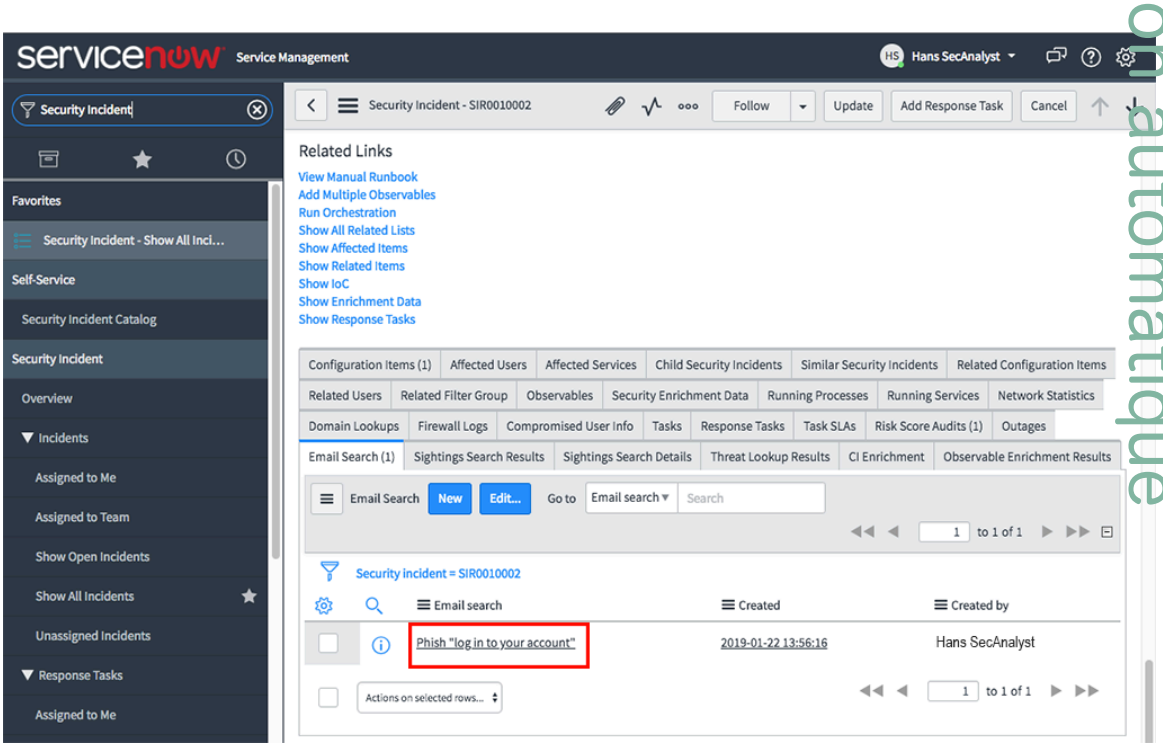
Si la liste connexe Recherche d'e-mails n'est pas affichée, cliquez sur le lien connexe**Afficher toutes les listes connexes** pour afficher cette liste connexe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Une fois la liste connexe Recherche d'e-mails sélectionnée, dans la colonne Recherche d'e-mails, cliquez sur le nom de votre recherche.



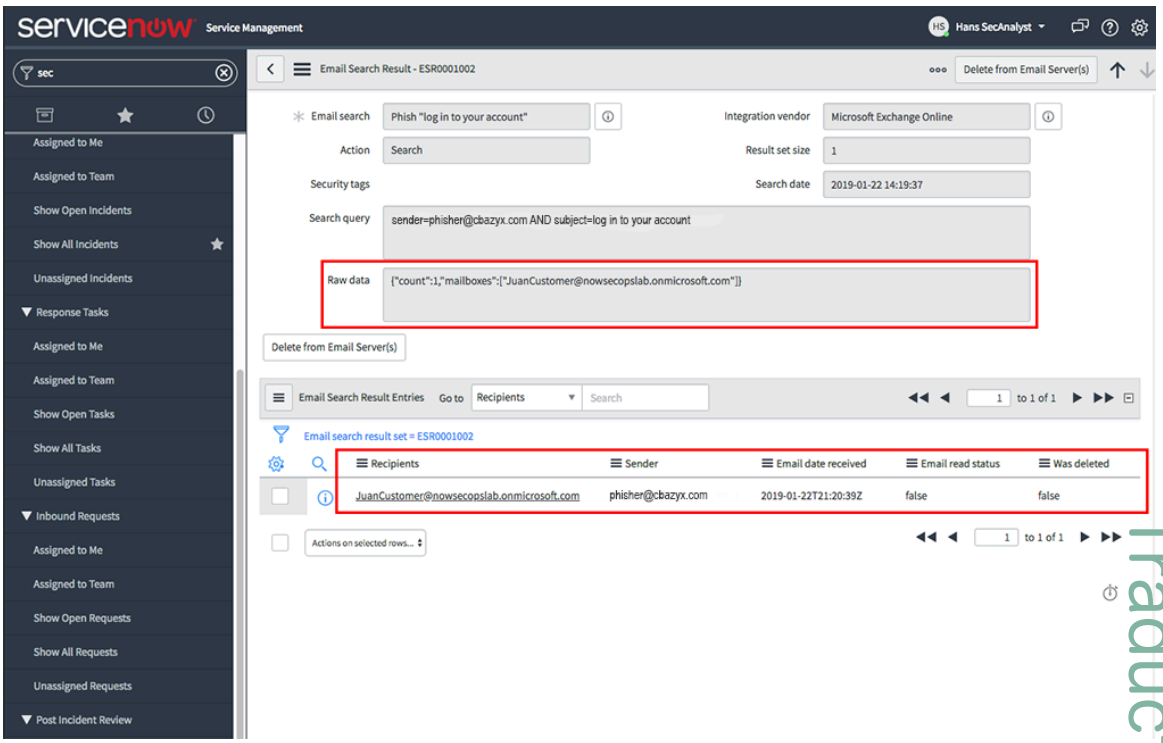
d. Dans l'enregistrement de recherche d'e-mail, cliquez sur la liste connexe Résultats de recherche d'e-mail.

e. Dans la colonne Date de recherche, cliquez sur la date de votre recherche pour afficher les données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’enregistrement du résultat de la recherche d’e-mail s’affiche.



Une fois qu’une recherche d’e-mails est terminée avec succès, évaluez les résultats. Si vous déterminez que les e-mails doivent être corrigés, vous pouvez maintenant supprimer des e-mails ou demander l’approbation de suppression.

Demander l’approbation de suppression pour les e-mails sur le service Microsoft Exchange Online

Une fois qu’une recherche d’e-mails est terminée avec succès et que les messages correspondants sont identifiés, vous pouvez supprimer définitivement tous les e-mails suspects du service Microsoft Exchange Online liés à l’incident de sécurité et à la campagne d’hameçonnage.

Avant de commencer

Rôle requis : sn_si.analyst

Le système effectue des suppressions sur vos derniers résultats de recherche réussis.

Pourquoi et quand exécuter cette tâche

Si les approbations et les notifications par e-mail sont activées, envoyez une demande de suppression des e-mails à un groupe d’approbation avant de les supprimer.

Les résultats de la recherche d’e-mails sont affichés avec tous les messages qui ont été reçus. Pour vous assurer que les e-mails d’hameçonnage sont supprimés, les résultats de la suppression sont publiés dans les notes de travail de l’incident de sécurité associé. Si le balisage est activé, une balise de sécurité s’affiche également sur l’incident de sécurité associé. Si l’e-mail n’est pas supprimé, vous en êtes également informé dans les notes de travail.

En fonction des politiques de votre organisation, vous devrez peut-être demander une approbation avant de supprimer les e-mails d’hameçonnage. Le processus d’approbation de suppression nécessite des informations sur le nombre d’e-mails à supprimer et, éventuellement, l’accès à d’autres détails de message. Pour le traitement de la demande de suppression, dans une notification par e-mail, un approbateur reçoit le nombre de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

messages électroniques correspondants, le lien de l'incident de sécurité pour accéder aux détails complets du message et les liens d'approbation ou de rejet. Les liens contenus dans cet e-mail permettent à un approbateur d'accepter ou de rejeter la demande de suppression à partir de la notification par e-mail. Une piste d'audit complète avec horodatage est également disponible pour suivre le moment où l'état d'approbation a changé dans les notes de travail. Si un groupe d'approbation est affecté, un utilisateur du groupe peut traiter la demande pour l'ensemble du groupe. Chaque membre du groupe d'approbation reçoit une notification par e-mail pour la demande.

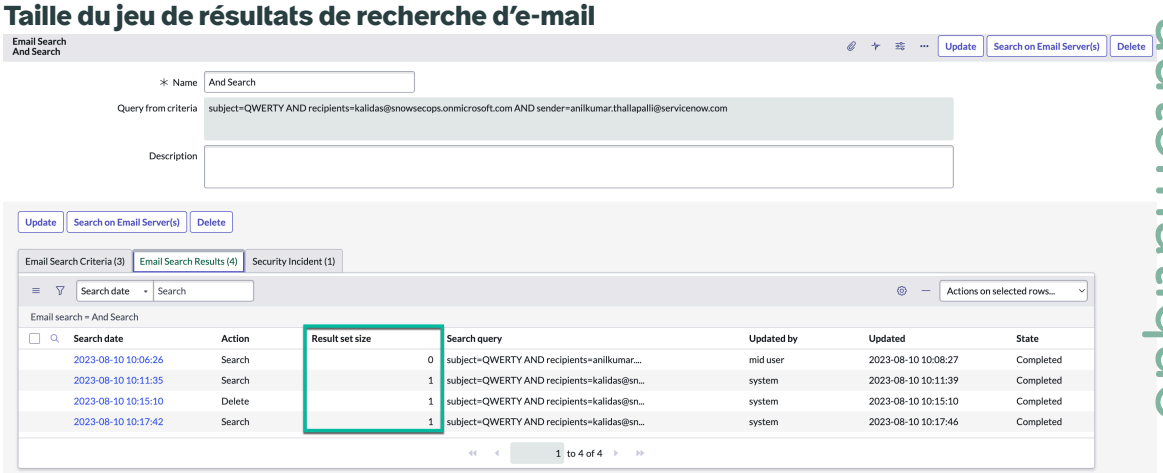
En tant qu'utilisateur disposant du rôle sn_si.analyst, si vous déterminez que les e-mails doivent être corrigés, suivez les étapes requises pour supprimer des e-mails. Si les approbations sont activées, demandez l'approbation pour supprimer des e-mails du Microsoft Exchange Online service.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité > Afficher tous les incidents**.
2. Cliquez sur la liste connexe **Recherche d'e-mails** .
3. Une fois la liste connexe Recherche d'e-mails sélectionnée, dans la colonne Recherche d'e-mails, cliquez sur le nom de votre recherche.
   Les résultats de la recherche sont affichés dans la liste connexe Résultats de recherche d'e-mails.

   Pour cet exemple, cette recherche a trouvé des e-mails qui correspondent à vos critères de recherche. Deux actions de recherche sont répertoriées dans l'enregistrement. Une recherche n'a aucune correspondance (0) et l'autre recherche a un e-mail correspondant (1).

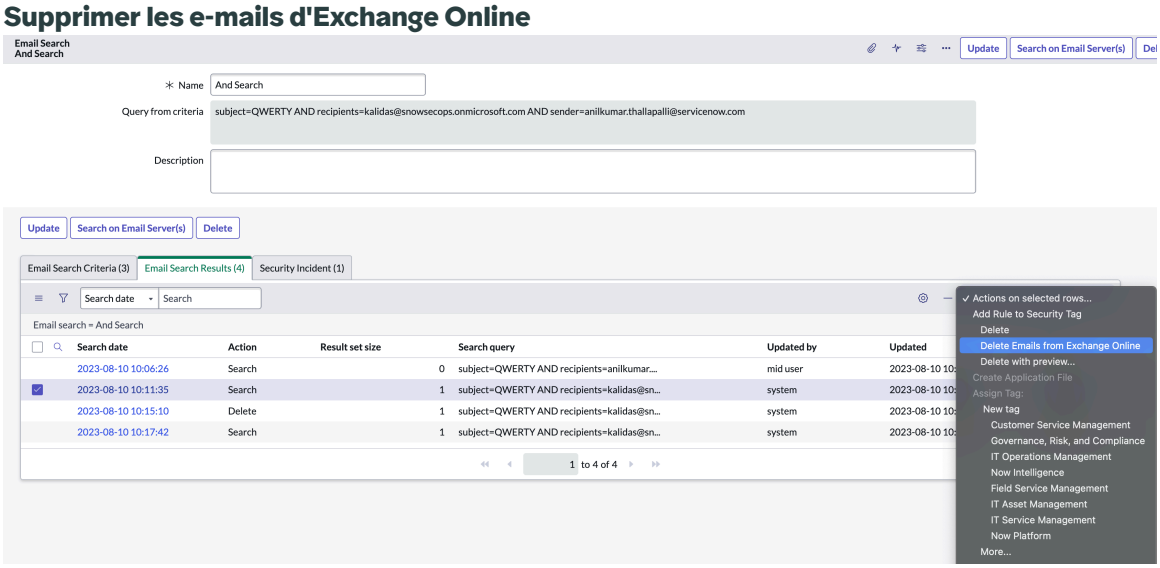
Taille du jeu de résultats de recherche d'e-mail



4. Pour supprimer des éléments d'e-mail associés à une recherche, cochez la case d'un ensemble de résultats de recherche à gauche de la colonne Date de recherche.
   Vous pouvez sélectionner un jeu de résultats unique ou plusieurs jeux de résultats dans la liste.
5. Sélectionnez les jeux de résultats que vous souhaitez supprimer.

Traduction automatique

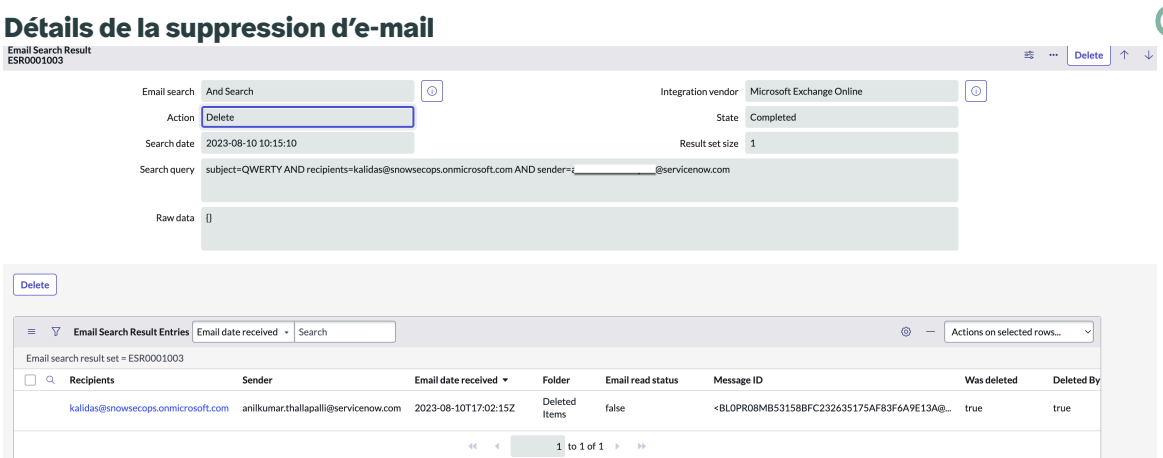
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. En bas de la liste connexe Résultats de recherche d'e-mails, dans la liste Actions sur les lignes sélectionnées, sélectionnez **Supprimer les e-mails d'Exchange Online pour supprimer tous les éléments d'e-mail** associés à un ou plusieurs ensembles de résultats du serveur Exchange Online.
Si un ensemble de résultats contient plusieurs e-mails, vous n'avez pas besoin d'ouvrir l'enregistrement des résultats de recherche d'e-mails et de sélectionner des e-mails individuels pour les supprimer. Tous les éléments d'e-mails avec un statut faux dans la colonne A été supprimé dans l'enregistrement des résultats de recherche d'e-mails sont supprimés une fois que vous avez sélectionné **Supprimer les e-mails d'Exchange Online**.

   Si un élément d'e-mail d'un jeu de résultats a déjà été supprimé, l'état de la colonne A été supprimé de l'enregistrement des résultats de recherche d'e-mails est vrai. Ces éléments ne sont pas supprimés à nouveau.

   Si l'option d'approbation est désactivée pendant l'étape de configuration, une fois que vous avez sélectionné **Supprimer les e-mails d'Exchange Online**, les e-mails associés à l'ensemble de résultats sont supprimés. Le jeu de résultats lui-même n'est pas supprimé. Toutefois, l'état de tous les éléments d'e-mail supprimés de l'ensemble de résultats est mis à jour sur vrai dans la colonne A été supprimé de l'enregistrement du résultat de recherche d'e-mail. Pour plus d'informations sur la fonction d'approbation, reportez-vous à Configurer l'intégration Microsoft Exchange Online.



   Ces e-mails sont supprimés du Microsoft Exchange Online locataire sur lequel vous avez effectué les recherches. Une note de travail s'affiche si les e-mails sont supprimés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sur l'enregistrement d'incident de sécurité, la balise de sécurité Suppression d'e-mail - Terminé s'affiche.

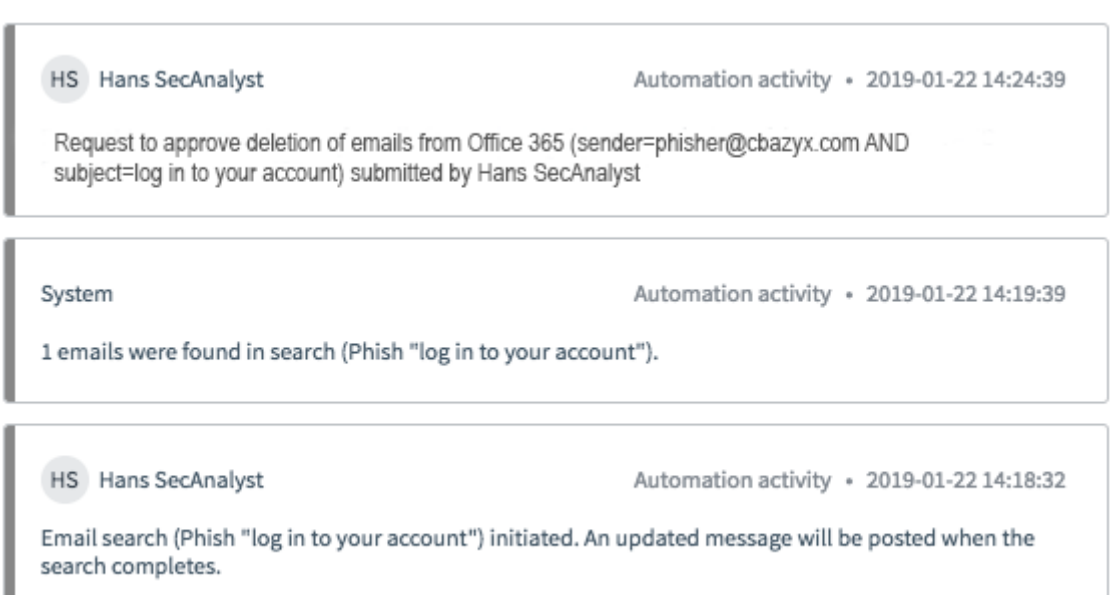


Si les approbations sont désactivées pour les demandes de suppression, vous avez correctement supprimé les Microsoft Exchange Online e-mails du locataire.

Si les approbations sont activées pour les demandes de suppression au cours de l'étape de configuration, une notification par e-mail est envoyée à chaque membre du groupe d'approbation que vous avez sélectionné lors de l'étape de configuration, une notification par e-mail est envoyée à chaque membre du groupe d'approbation que vous avez sélectionné lors de l'étape **de** configuration.

Si le balisage est activé pendant l'étape de configuration, la balise de sécurité Suppression d'e-mail : initiée s'affiche sur l'enregistrement d'incident de sécurité connexe. Pour plus d'informations sur le balisage, reportez-vous à la section Configurer l'intégration Microsoft Exchange Online.

Des notes de travail indiquent qu'une demande de suppression d'e-mails est soumise par l'utilisateur disposant du rôle sn_si.analyst (Hans SecAnalyst).



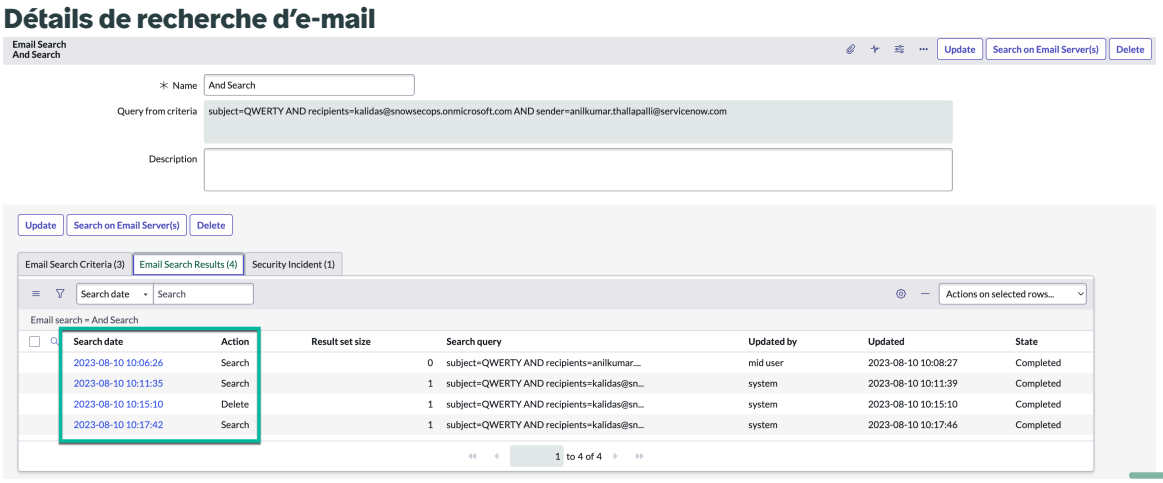
Si les approbations sont activées, l'étape suivante consiste à traiter la demande de suppression.

7. Sinon, si vous souhaitez afficher les détails et les éléments d'e-mail individuels d'un enregistrement de recherche avant de le supprimer ou de soumettre une demande de suppression, procédez comme suit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Une fois la liste connexe Résultats de recherche d'e-mails sélectionnée, dans la colonne Date de recherche, cliquez sur la date d'une recherche que vous souhaitez vérifier.



Les informations suivantes sur les e-mails s'affichent :

- Destinataires
- Expéditeur
- Date de réception de l'e-mail
- État de lecture de l'e-mail (vrai ou faux)
- A été supprimé (vrai ou faux)
- Supprimé par l'intégration (vrai ou faux)

> **Remarque :**
>
> La valeur est définie sur vrai lorsque l'e-mail est supprimé lorsque l'analyste lance l'opération Supprimer du ou des serveurs de messagerie.
>
> Les notes de travail sont mises à jour avec le nombre total d'enregistrements supprimés, qui inclut les enregistrements supprimés par intégration et utilisateur.

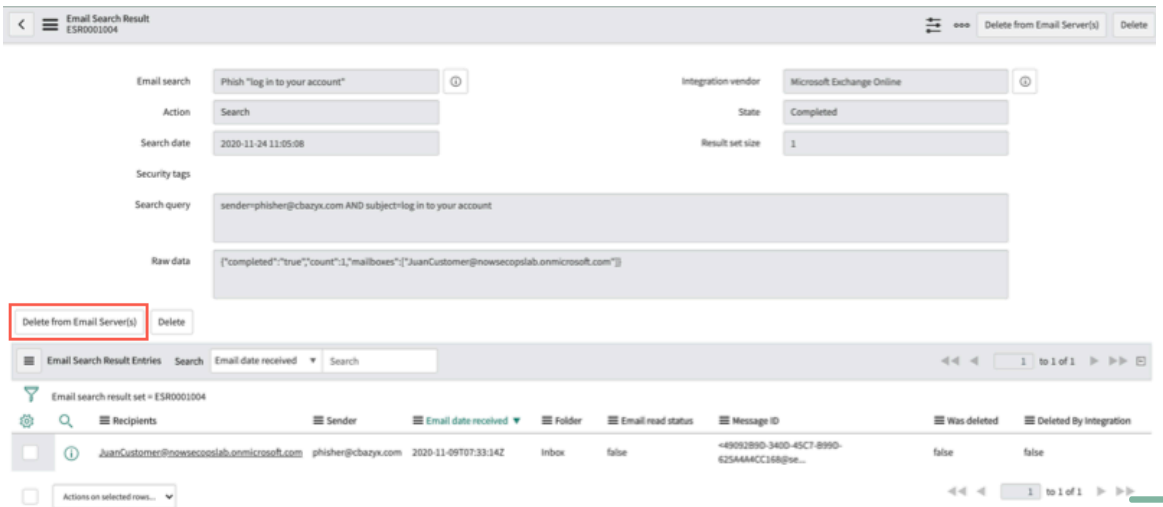
b. Une fois que vous avez examiné les données, pour supprimer tous les e-mails ou envoyer une demande de suppression de tous les e-mails, cliquez sur **Supprimer des serveurs de messagerie.**

Comme décrit dans l'exemple précédent, s'il y a plusieurs e-mails répertoriés sur l'enregistrement des résultats de recherche, vous n'avez pas besoin de sélectionner les e-mails individuels pour les supprimer. La demande de suppression supprime tous les e-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

mails associés à la recherche lorsque la valeur « faux » s'affiche dans la colonne A été supprimé des derniers résultats de recherche.



Si les approbations sont activées, vous avez correctement soumis une demande de suppression d'e-mails. Les balises de sécurité et les notes de travail sont affichées sur l'enregistrement d'incident de sécurité connexe, comme décrit dans l'exemple précédent. En tant qu'approbateur, l'étape suivante consiste à traiter la demande de suppression.

Approuver les demandes de suppression d'e-mail pour l'intégration Microsoft Exchange Online

Si l'option d'approbation est activée dans votre ServiceNow AI Platform instance, les demandes de suppression d'e-mails sont envoyées par e-mail à chaque membre du groupe d'approbation. Vous sélectionnez le groupe d'approbation au cours de l'étape de configuration. Les approbations fournissent à votre organisation un niveau de contrôle supplémentaire sur la suppression des e-mails.

Avant de commencer

Vérifiez que l'option **Approbations** est sélectionnée dans l'onglet Paramètres supplémentaires du formulaire Paramètres de configuration de recherche et de suppression d'e-mails Exchange Online.

Vérifiez que vous avez activé les options **d'envoi d'e-mail et**de **réception d'e-mail activées** dans votre ServiceNow AI Platform instance pour les demandes d'approbation.

Lorsque l'utilisateur disposant du rôle sn_si.analyst soumet des demandes de suppression d'e-mail, par défaut, ces demandes sont envoyées par e-mail à sn_si.admin. Si vous avez créé un groupe d'approbation, chaque membre du groupe reçoit une notification. Les approbateurs peuvent traiter les demandes de suppression d'e-mails directement à partir de la notification par e-mail. Les demandes peuvent également être traitées à partir des enregistrements de résultats de recherche d'e-mails dans ServiceNow AI Platform les instances. Cette rubrique affiche les deux méthodes d'approbation.

Les informations suivantes décrivent la demande dans la notification par e-mail :

Numéro d'enregistrement du résultat de recherche d'e-mail

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Numéro unique affecté à l'enregistrement de recherche par dans ServiceNow AI Platform le cadre de la piste d'audit.

Nom de l'analyste ayant soumis la demande

Nom de la personne qui a soumis la demande dans le cadre de la piste d'audit.

Lien vers l'incident de sécurité

Un lien vers l'incident de sécurité lié à l'événement de hameçonnage. Affichez l'incident de sécurité avec les notes de travail, les recherches par e-mail et les résultats de recherche d'e-mails directement à partir de l'e-mail.

Approuver ou rejeter les liens

Liens permettant d'approuver ou de rejeter la demande à partir de la notification par e-mail. Une fois que vous avez cliqué sur l'un des liens, le système lance automatiquement le workflow connexe et une note de travail est publiée dans l'enregistrement d'incident de sécurité.

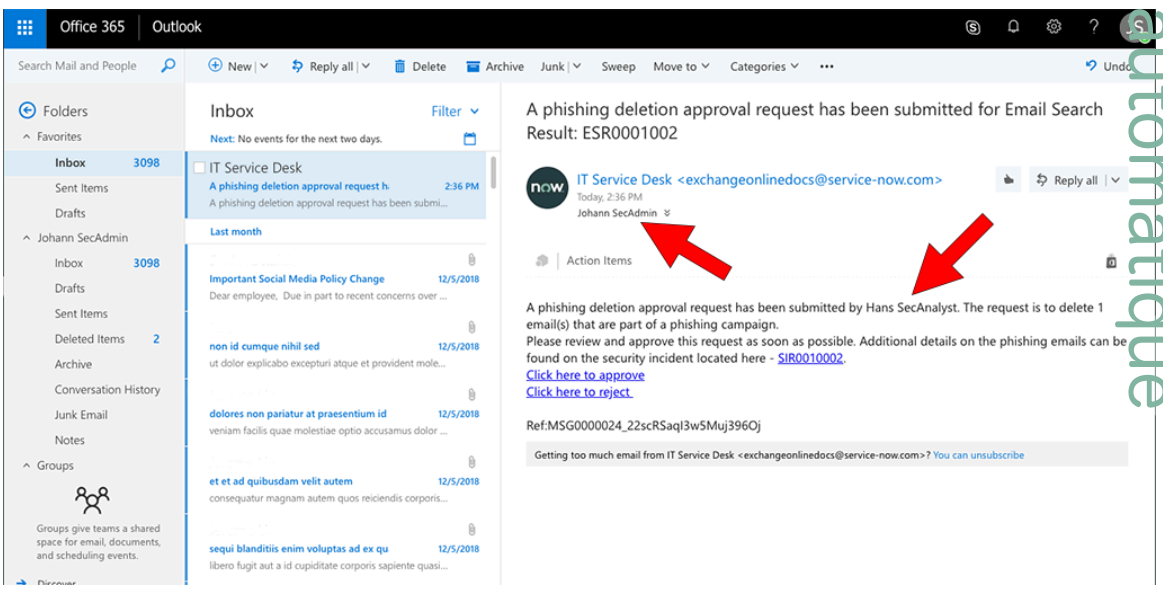
Rôle requis : sn_si.admin ou tous les membres d'un groupe d'approbation affecté.

Procédure

1. Pour traiter la demande de suppression de la notification par e-mail, procédez comme suit.

a. En tant qu'approbateur, localisez l'e-mail de notification dans le compte de messagerie que vous avez configuré dans votre ServiceNow AI Platform compte d'utilisateur.

Dans cet exemple, l'utilisateur disposant du rôle sn_si.analyst (Hans SecAnalyst) soumet une demande pour supprimer un e-mail. Johann SecAdmin est membre du groupe d'approbation.



b. Dans la notification par e-mail, choisissez une option pour continuer.

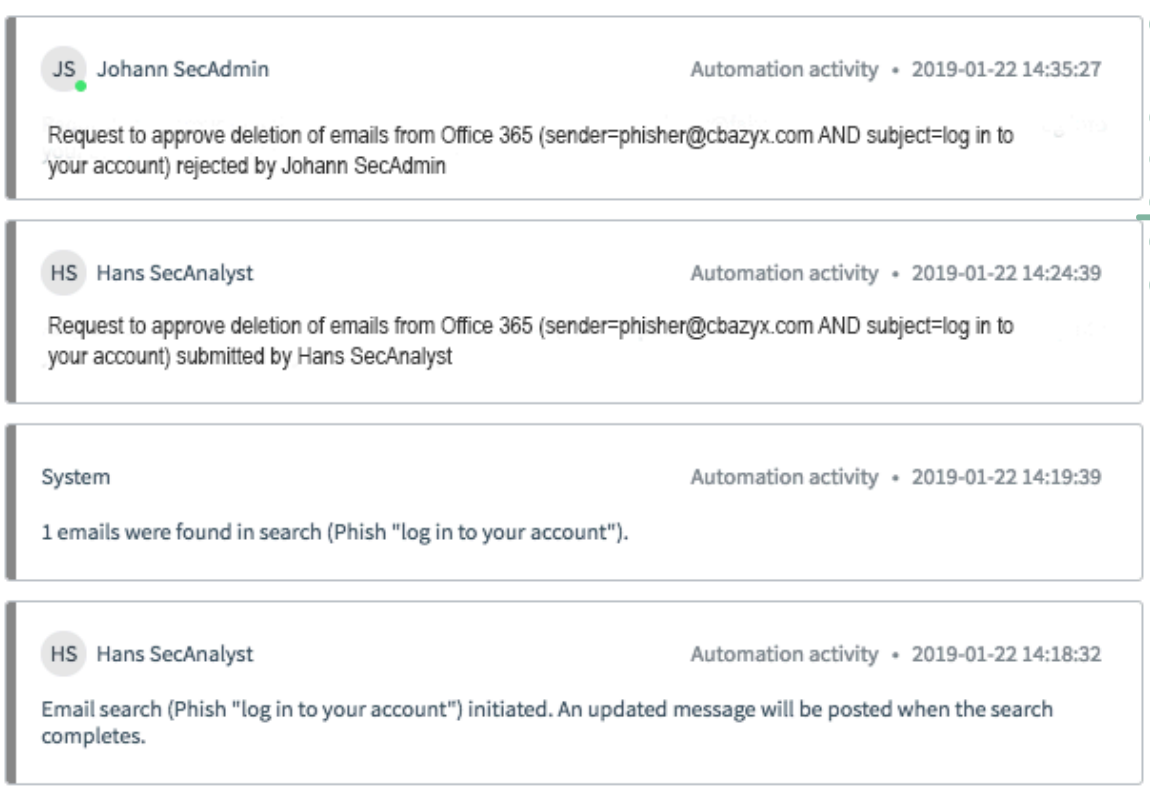
Option	Description
Cliquez sur Cliquez ici pour approuver le lien Approuver	Approuver la demande de suppression. Tous les éléments d'e-mail ayant un statut faux dans la colonne A été supprimé et qui sont associés à l'enregistrement de résultat de recherche sont automatiquement supprimés du Microsoft Exchange Online locataire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	L'état de tous les éléments d'e-mail du jeu de résultats est mis à jour sur vrai dans la colonne A été supprimé de l'enregistrement du résultat de recherche d'e-mail. Une note de travail est publiée dans l'enregistrement d'incident de sécurité avec le nombre d'e-mails supprimés avec succès. Si le balisage est activé, la balise Suppression d'e-mail - Terminée remplace la balise Suppression d'e-mail - Initiée .
Cliquez ici pour rejeter le lien	Refusez la demande de suppression. Une note de travail est publiée avec le nom de la personne qui a rejeté la demande. Après le rejet d'une demande, en tant qu'utilisateur disposant du rôle sn_si.analyst, vous devez soumettre une nouvelle demande de suppression si vous déterminez que les e-mails doivent être supprimés.
Cliquez sur le lien vers l'enregistrement de l'incident de sécurité (SIR0010002)	Examinez l'incident de sécurité associé et toutes les données de recherche connexes avant de traiter la demande.

L'image suivante montre un exemple de piste d'audit créée par les notes de travail sur l'enregistrement d'incident de sécurité connexe pour cet exemple. Lorsque la demande est rejetée à partir de la notification par e-mail par un approbateur, une note de travail est publiée avec la personne qui a rejeté la demande. Johann SecAdmin rejette cette demande.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans le ServiceNow AI Platform cas de la personne qui a rejeté la demande (Johann SecAdmin), dans **Libre-service > mes approbations**, Rejeté s'affiche dans la colonne État.

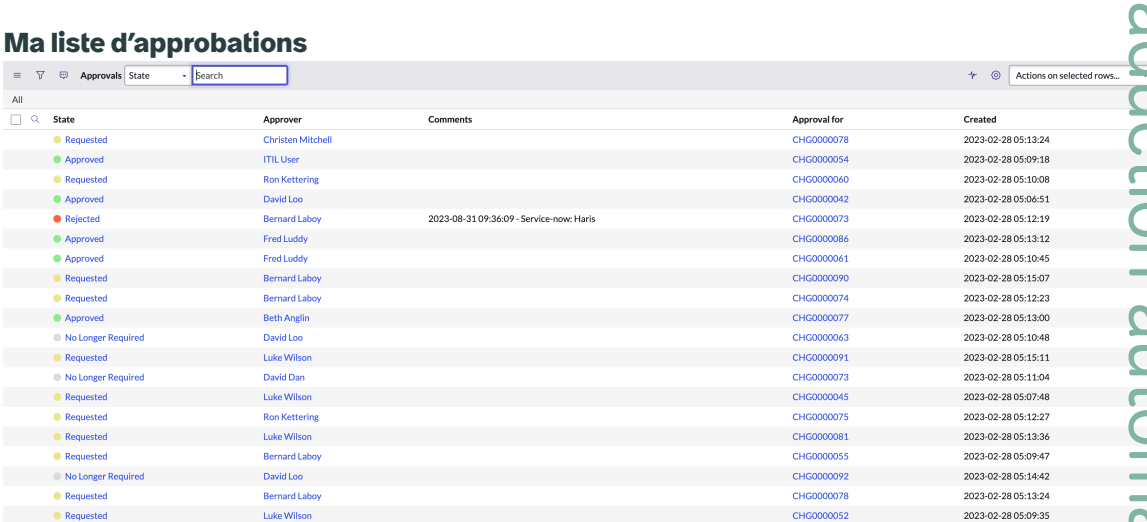
Après qu'une demande a été rejetée par un seul membre du groupe d'approbation, en tant qu'utilisateur disposant du rôle sn_si.analyst, vous devez soumettre une nouvelle demande de suppression de ces e-mails si vous déterminez qu'ils doivent être supprimés.

Pour cet exemple, une fois la demande rejetée, l'utilisateur disposant du rôle sn_si.analyst soumet une nouvelle demande.

Un autre membre du groupe d'approbation, John Approver, reçoit un e-mail similaire à celui illustré dans l'exemple précédent. John Approver peut également traiter cette demande.

2. Les approbateurs peuvent également accéder à **Libre-service > mes approbations** dans leurs ServiceNow AI Platform instances pour afficher et traiter les demandes de suppression.
Pour traiter une demande à partir de **Mes approbations**, procédez comme suit.

   a. Accédez à la **Libre-service > mes approbations**.

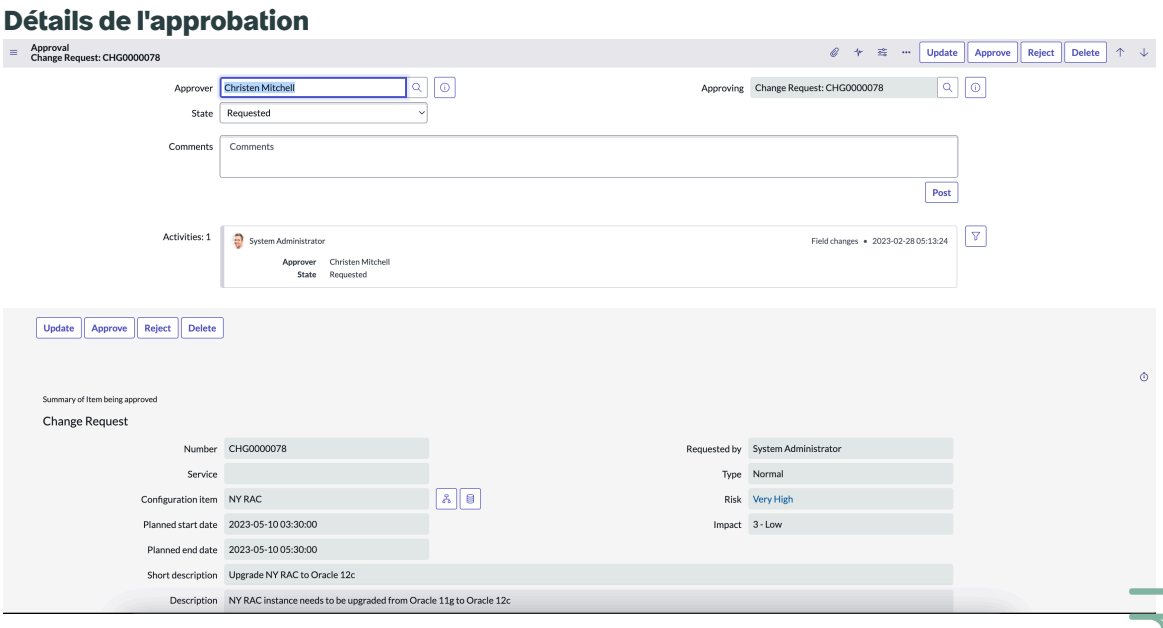


   b. Dans la colonne État, cliquez sur l'élément demandé.

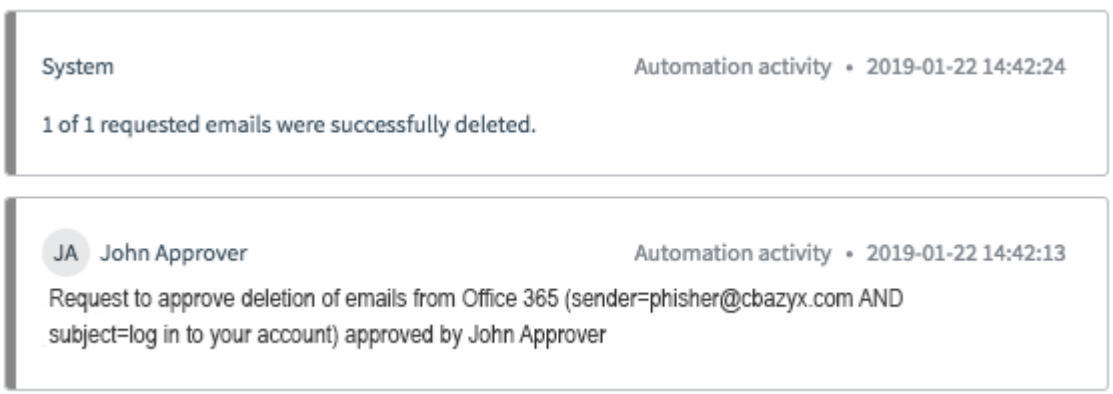
      L'enregistrement d'approbation qui s'affiche répertorie les données relatives à la recherche, à la demande de recherche et aux résultats de la recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Sur cet enregistrement, cliquez sur **Approuver** pour approuver la demande.
Une fois la demande approuvée, le système lance le workflow de suppression pour supprimer les e-mails. L'image suivante montre un exemple de piste d'audit créée par les notes de travail sur l'enregistrement d'incident de sécurité connexe pour cet exemple. Une fois que cette demande de suppression est soumise à nouveau, elle est approuvée. Quelle que soit la méthode utilisée pour approuver une demande, le nombre d'e-mails supprimés avec succès est publié dans une note de travail.



Une fois les e-mails supprimés, sur l'enregistrement d'incident de sécurité connexe, si le balisage est activé, la balise Suppression d'e-mail - Terminée remplace la balise Suppression d'e-mail - initiée .

Entrante **Libre-service > mes approbations** pour l'approbateur (John Approver), l'état passe de Demandé à Approuvé.

Entrante **Libre-service > mes approbations** pour les autres membres du groupe d'approbation, par exemple, Johann SecAdmin, l'état devient N'est plus nécessaire une fois la demande approuvée.

3. Pour confirmer que les e-mails sont supprimés des résultats de recherche d'e-mails sur l'enregistrement d'incident de sécurité connexe, procédez comme suit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

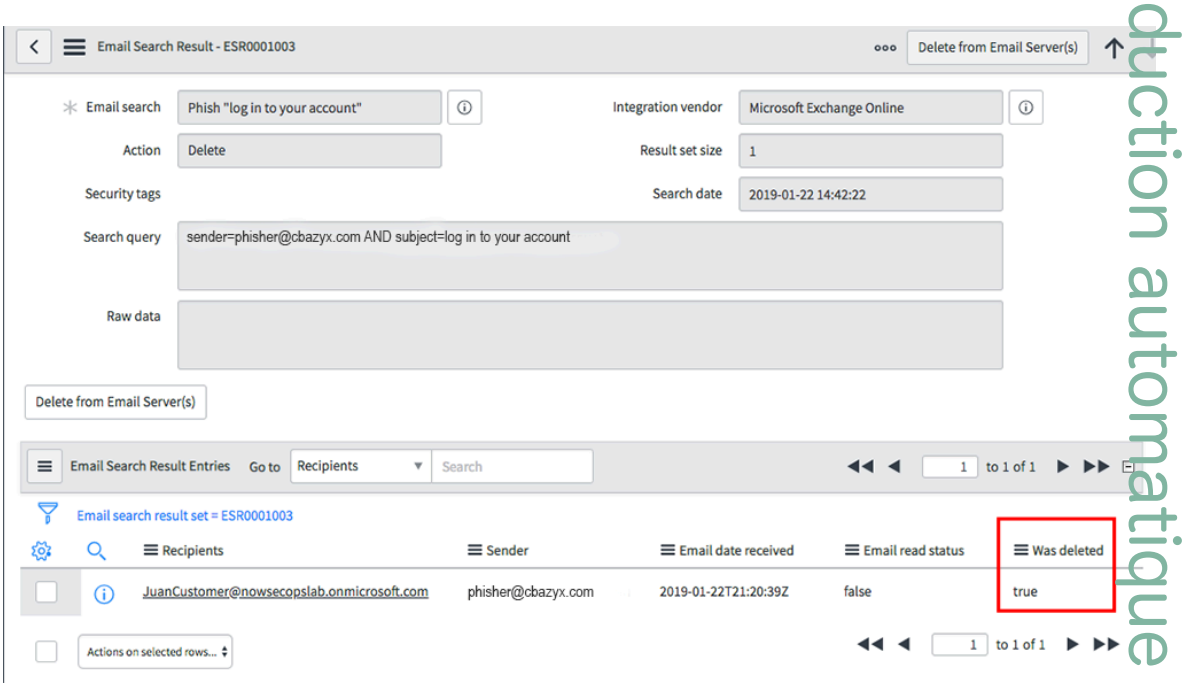
a. Accédez à la **Incidents de sécurité > Afficher tous les incidents** et localiser l'incident de sécurité lié au phishing.
Les listes connexes s'affichent au bas de l'enregistrement.

b. Cliquez sur la liste connexe **Recherche d'e-mails** .

c. Cliquez sur le nom de la recherche dans la colonne Recherche d'e-mails (Phish « connectez-vous à votre compte »).
L'enregistrement de recherche d'e-mail s'affiche. Si la liste connexe Recherche d'e-mails n'est pas visible, cliquez sur le lien **Afficher toutes les listes connexes**.

d. Cliquez sur la liste connexe **Résultats de recherche d'e-mail** .
Dans la colonne Date de recherche, les actions de recherche et de suppression d'e-mails sont affichées avec les dates correspondantes.

e. Dans la colonne Date de recherche, cliquez sur l'élément qui correspond à l'action de suppression.
Dans l'enregistrement des résultats de recherche d'e-mails qui s'affiche, l'état de la colonne A été supprimé indique que l'e-mail est supprimé (vrai).



Vous avez approuvé avec succès les demandes de suppression d'e-mails d'une notification par e-mail et d'un enregistrement d'approbation, et confirmé que les e-mails sont supprimés. Pour plus d'informations sur la localisation de l'enregistrement des résultats de recherche d'e-mails, reportez-vous à la section Définir des critères de recherche d'e-mails et demander une recherche dans le Microsoft Exchange Online service.

Récupérer les e-mails supprimés sur le Microsoft Exchange Online service

(Facultatif) En tant qu'administrateur Microsoft Exchange, vous pouvez récupérer les e-mails supprimés si votre rattrapage d'incident nécessite que vous récupériez les e-mails supprimés par le workflow de cette intégration.

Avant de commencer

Pour en savoir plus sur la façon dont cette intégration supprime les e-mails, reportez-vous à la section Configurer l'intégration Microsoft Exchange Online.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur le rôle d'administration dans le Microsoft produit Office 365, y compris des informations sur la récupération d'éléments supprimés dans une boîte aux lettres utilisateur, voir À propos du rôle d'administrateur Exchange Online .

Rôle requis : admin, administrateur Microsoft Exchange

Pourquoi et quand exécuter cette tâche

Si vous sélectionnez l'option **Récupérer les e-mails supprimés** dans l'onglet Paramètres supplémentaires pendant l'étape de configuration, vous activez la récupération des e-mails supprimés dans votre Microsoft Exchange Online locataire. Les e-mails supprimés à l'aide du workflow de suppression de cette intégration sont placés dans le sous-dossier Éléments supprimés du dossier Éléments récupérables dans la boîte aux lettres de l'utilisateur sur le Microsoft Exchange Online service. Si le compte de l'utilisateur est configuré dans Microsoft Exchange Online le locataire de manière à ce que l'utilisateur puisse afficher le dossier Éléments supprimés, l'utilisateur peut récupérer ces e-mails à l'aide du Microsoft service Outlook sur le web. L'administrateur peut également récupérer les Microsoft Exchange Online e-mails supprimés d'un dossier Éléments supprimés d'un utilisateur. Pour plus d'informations, voir Récupérer des éléments ou des e-mails supprimés dans Outlook Web App .

Rôle requis : Microsoft Exchange Online administrateur ou Microsoft administrateur général pour récupérer les e-mails supprimés.

Rôle requis : sn_si.admin dans pour ServiceNow AI Platform activer l'option Récupérer les e-mails supprimés.

Rôle requis : sn_si.analyst pour effectuer une recherche réussie d'e-mails ServiceNow AI Platform et vérifier que les e-mails sont supprimés avec succès avant leur récupération.

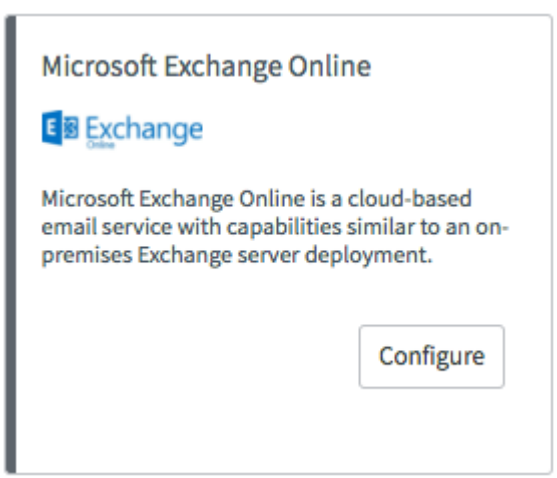
Procédure

Pour activer l'option de récupération d'e-mail, procédez comme suit.

a. Accédez à la **Security Operations** > **Intégrations** > **Configurations**.

b. Localisez la Microsoft Exchange Online tuile.

c. Cliquez sur **Configurer**.

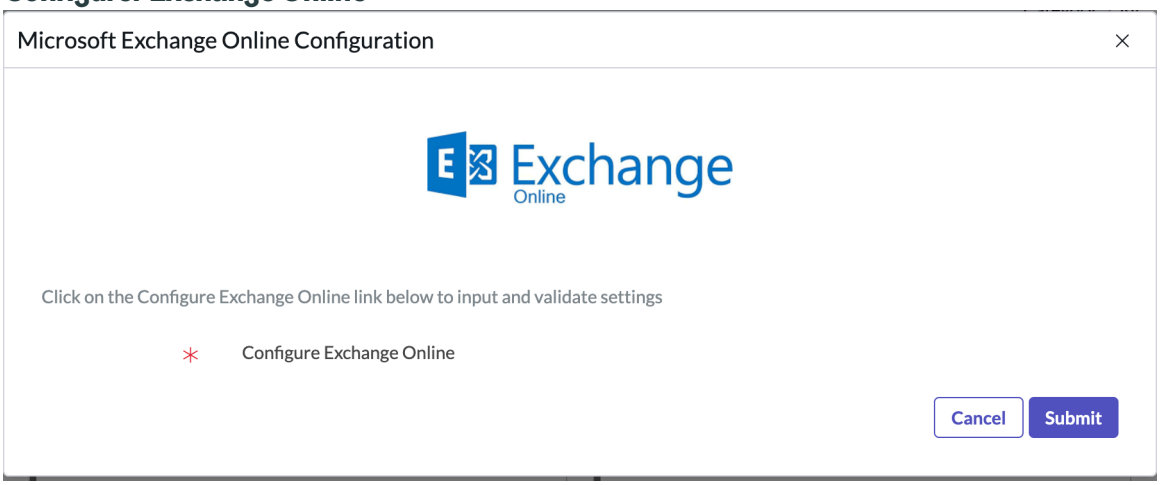


d. Dans la boîte de dialogue Configuration qui s'affiche Microsoft Exchange Online , cliquez sur **Configurer Exchange Online**.

Traduction automatique

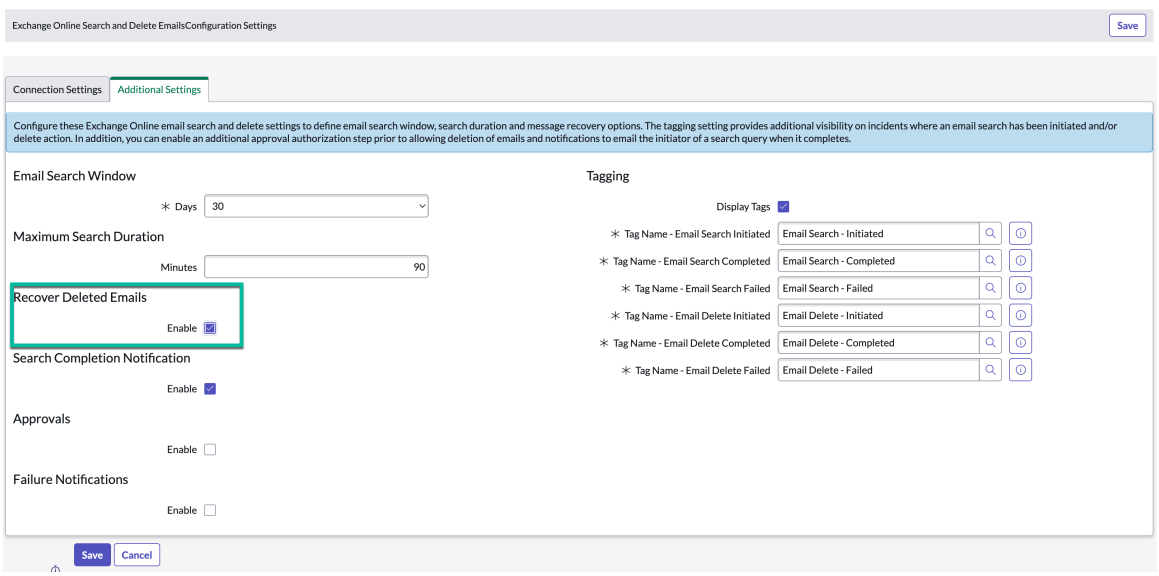
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Exchange Online



e. Dans l'onglet Paramètres supplémentaires sous Récupérer les e-mails supprimés, cochez la case **Activer** .

Récupérer les e-mails supprimés



f. Vérifiez tous les autres paramètres et cliquez sur **Soumettre**.

g. Pour vérifier que la recherche et la suppression des e-mails sont effectuées avec succès pour les e-mails que vous souhaitez récupérer, accédez à l'incident de sécurité qui a journalisé les workflows de recherche et de suppression d'e-mails.

h. Localisez les notes de travail et vérifiez que le système a bien supprimé les messages.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. En tant qu'administrateur Microsoft Exchange Online ou administrateur global, connectez-vous à votre Microsoft compte Office 365.

j. Suivez les étapes décrites dans Récupérer des éléments ou des e-mails supprimés dans Outlook Web App sur le site Web de la Microsoft documentation.

Modifier les balises de sécurité pour l'intégration Microsoft Exchange Online

Vous pouvez modifier les noms et les couleurs des balises de sécurité dans votre ServiceNow AI Platform® instance pour l'intégration Microsoft Exchange Online . Ces balises de sécurité vous aident à identifier rapidement quand la recherche d'e-mails se termine ou échoue. Ils identifient également le moment où des demandes de suppression d'e-mails sont lancées et le moment où les éléments d'e-mail sont supprimés avec succès.

Avant de commencer

Par défaut, les balises de sécurité sont activées dans votre ServiceNow AI Platform® instance si vous sélectionnez l'option **Afficher les balises** pendant l'étape de configuration. Vous pouvez modifier les couleurs et les noms des balises et affecter des balises à des groupes de balises de sécurité pour vous aider à les organiser dans votre ServiceNow AI Platform® instance. Par exemple, vous pouvez modifier les couleurs des balises de sorte que la balise de début d'une option soit d'une couleur et que la balise de complétion soit d'une autre couleur pour correspondre aux autres balises de sécurité activées dans votre ServiceNow AI Platform® instance. Ces différentes couleurs peuvent vous aider à identifier rapidement quand les workflows démarrent et sont terminés. Si vous décidez que vous n'avez pas besoin d'une balise spécifique, vous pouvez également désactiver une balise unique de l'enregistrement de balise sans la désactiver pour l'intégration. Si elle est désactivée, cette balise n'est plus affichée sur les incidents de sécurité associés. Pour plus d'informations sur la configuration des groupes de balises et des balises de sécurité, voir Configurer les groupes de balises et les balises de sécurité sur le site Web de la documentation produit ServiceNow .

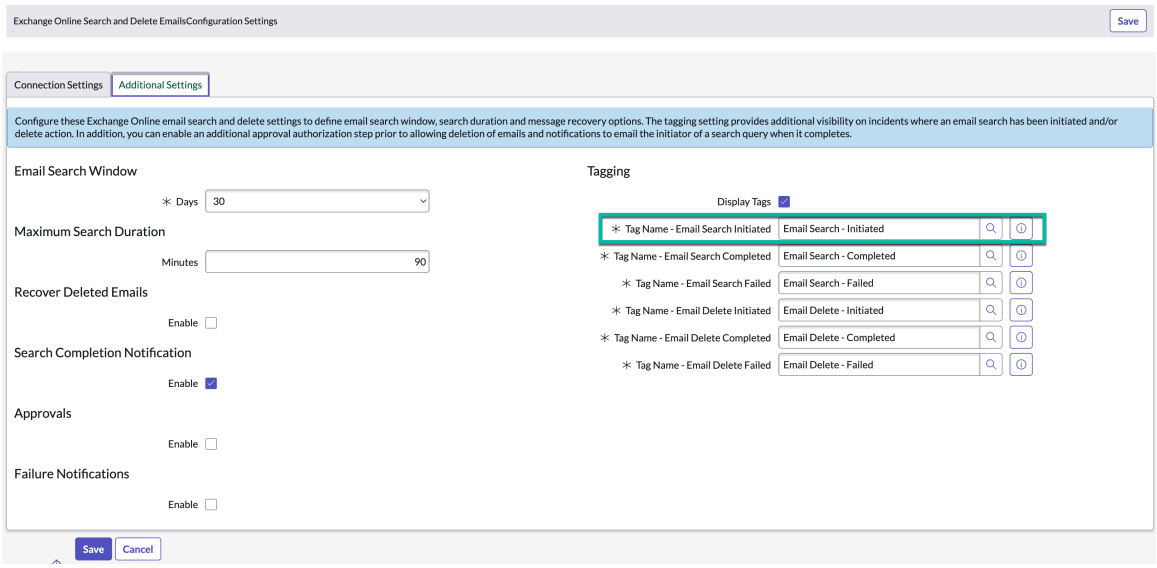
Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Intégrations** > **Paramètres Exchange Online**.
2. Cliquez sur l'onglet **Paramètres supplémentaires** pour le sélectionner.
3. Dans l'onglet qui s'affiche, si l'option **Afficher les balises** est désactivée, sélectionnez-la pour afficher les noms des balises.
4. Une fois les noms de balises affichés, cliquez sur l'icône d'informations à droite d'une balise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



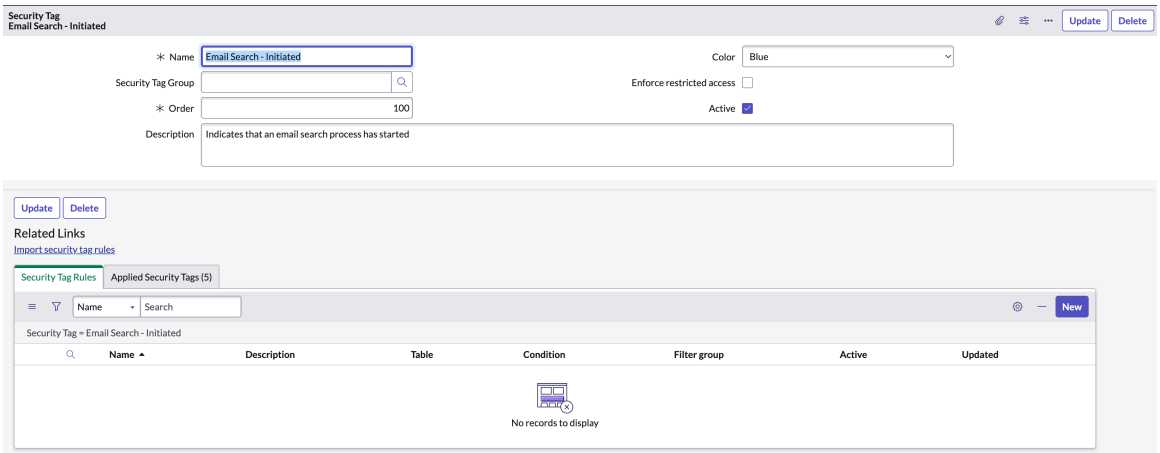
5. Dans la boîte de dialogue Balise de sécurité qui s'affiche, cliquez sur **Ouvrir l'enregistrement**.
6. Dans l'enregistrement qui s'affiche, modifiez les champs.

Option	Description
Nom	Nom unique de la balise de sécurité.
Couleur	Couleur de la balise de sécurité. Sélectionnez une couleur dans la liste de choix.
Groupe de balises de sécurité	Nom du groupe de balises de sécurité. Cliquez sur l'icône d'informations pour afficher les groupes disponibles. La valeur par défaut est le groupe de balises META.
Appliquer l'accès restreint	Sélectionnez cette option pour affecter des rôles de lecture et d'écriture requis par les utilisateurs pour lire ou écrire sur des enregistrements qui ont cette balise de sécurité. La valeur par défaut est effacée.
Ordre	Indiquez l'ordre dans lequel la balise apparaît sur les formulaires ou dans une liste. La valeur par défaut est 100. Pour définir l'ordre dans la liste, saisissez une valeur. Par exemple, 100, 200, 300, 400. La balise avec le numéro le plus bas s'affiche en premier sur la liste. Le profil avec le numéro le plus élevé s'affiche en dernier.
Actif	Activer ou désactiver cette balise. Est sélectionné par défaut (actif)
Description	Description de la balise.

7. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous avez désormais modifié l'enregistrement de balise pour une balise de sécurité.

Intégration de Microsoft Exchange sur site

L'intégration Microsoft Exchange sur site fournit aux analystes de sécurité des outils pour contenir et éradiquer les menaces d'hameçonnage et d'e-mails d'hameçonnage dans les instances locales.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

Introduction à l'intégration de Microsoft Exchange On-Premises

Utiliser

Rechercher et supprimer des e-mails d'hameçonnage

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Introduction à l'intégration de Microsoft Exchange On-Premises

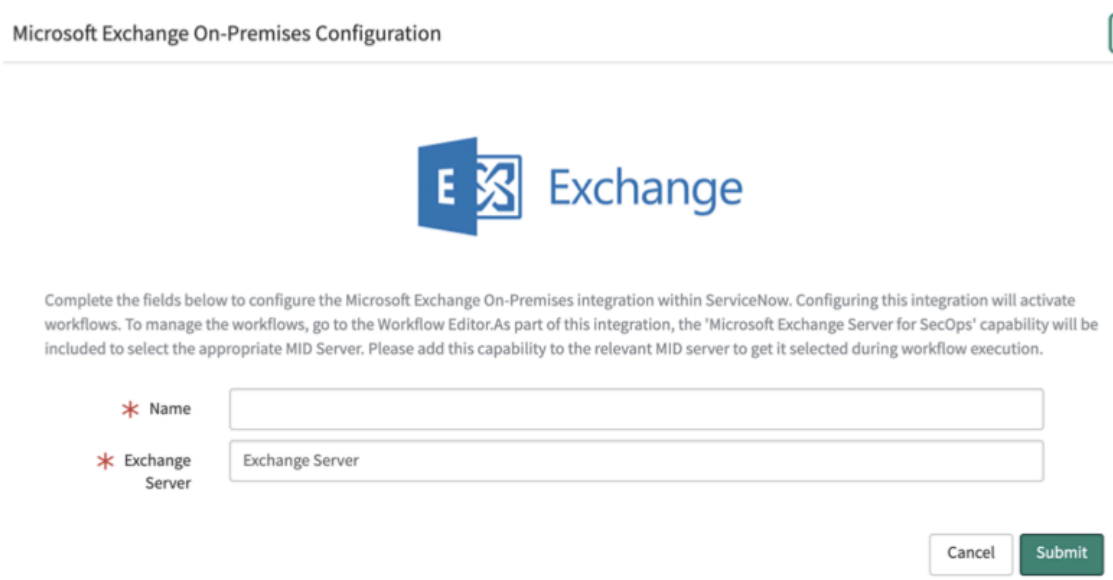
L'intégration Microsoft Exchange sur site fournit aux analystes de sécurité des outils pour contenir et corriger les menaces d'hameçonnage et d'e-mails d'hameçonnage dans les instances locales. Avant de pouvoir utiliser l'intégration Microsoft Exchange sur site, vous devez la télécharger à partir de et ServiceNow Store identifier les serveurs Exchange et MID appropriés.

Avant de commencer

Rôle requis : sn_si_admin

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois le système d'exploitation d'installation terminé, accédez à **Security Operations** > **Intégrations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la Microsoft Exchange carte Sur site, cliquez sur **Nouveau**.



4. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
Serveur Exchange	Indiquez le serveur Exchange à utiliser.

> **Remarque :** La configuration de cette intégration active les flux. Pour gérer les flux, accédez au **Studio de workflow/Concepteur de flux**.

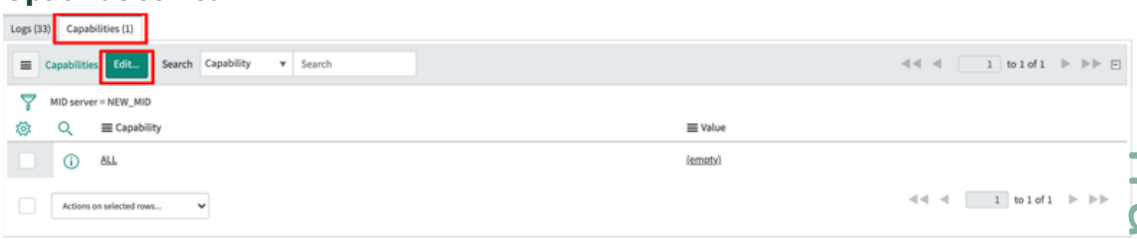
5. Cliquez sur **Envoyer**.
   La carte de configuration d'intégration s'affiche.
6. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.

Traduction automatique

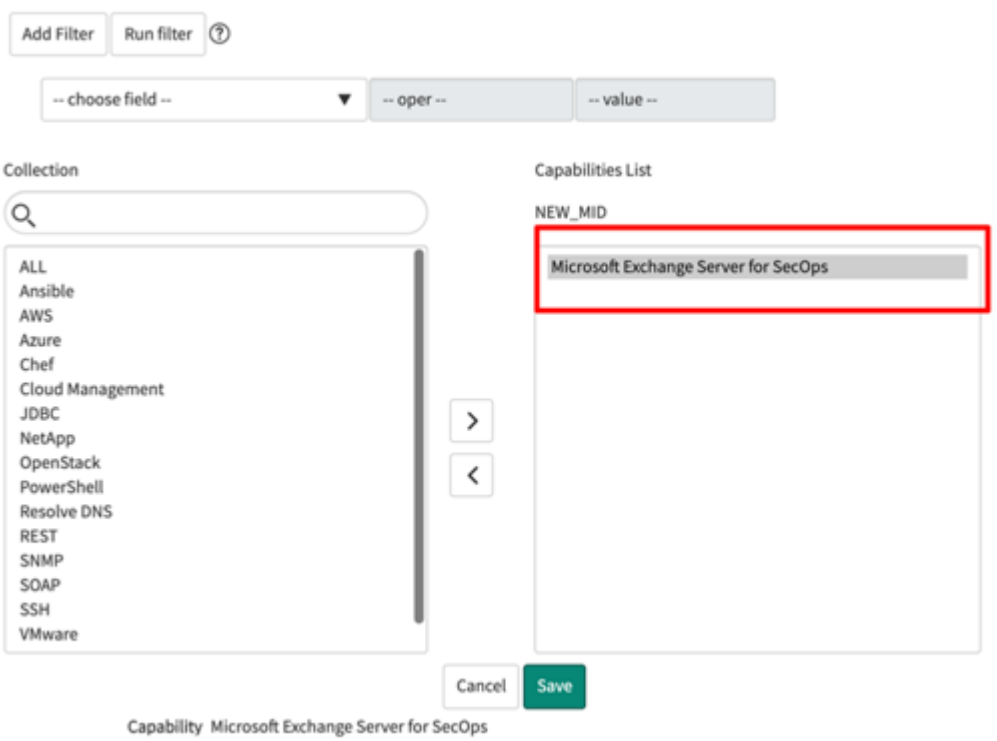
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .
8. Accédez à la **Orchestration** > **Serveurs MID**.
9. Ouvrez l'enregistrement et vérifiez l'état du serveur MID qui est accessible au serveur Exchange et son option **d'état** est définie sur **Oui**.
10. Ajouter l'aptitude Serveur MID :
    - Sélectionnez le serveur MID respectif pour ajouter l'option.
    - Cliquez sur la liste connexe **Options** , puis sur **Modifier**.

Option de serveur MID



    - Supprimer **tout** et ajouter **Microsoft Exchange Server pour SecOps**.



    - Sélectionnez les **plages** IP dans la section **Listes connexes** et définissez la valeur sur **TOUTES** ou sur la valeur souhaitée.
    - Sélectionnez les **applications prises en charge** dans la section **Listes connexes** et définissez la valeur sur TOUT ou Orchestration.
    - **Enregistrez** l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Validez les connexions et les informations d'identification.
12. Une fois les informations d'identification validées, la configuration sur l'instance ServiceNow est terminée et prête à effectuer des opérations de recherche et de suppression d'e-mails à l'aide de cette intégration.

Microsoft Exchange : effectuer un flux de recherche et de suppression d'e-mails

Lorsque le flux **Microsoft Exchange : effectuer une recherche et une suppression d'e-mails** est exécuté, il recherche le serveur Exchange à l'aide de la requête de recherche fournie et renvoie les détails à l'instance locale.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Le flux **Microsoft Exchange : effectuer une recherche et une suppression d'e-mails** est exécuté lorsque des recherches d'e-mails sont configurées et que vous appuyez sur le bouton **Supprimer des serveurs de messagerie** ou **Rechercher sur les serveurs de messagerie.**

Les actions spécifiques à cette intégration sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Les actions de flux comprennent :

- Créer une action de recherche de conformité
- Vérifier la conformité Action d'état de recherche

Créer une action de prévisualisation de recherche de conformité

L'action Créer un aperçu de recherche de conformité crée une nouvelle action de recherche de conformité de type aperçu sur le serveur Exchange pour la recherche de conformité créée.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variable	Description
targetId	Champ d'identificateur obligatoire de l'hôte cible où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Conditions de sortie

Les conditions de sortie possibles pour cette action sont les suivantes :

Conditions de sortie

Variable	Description
Terminé	Lorsque l'action de recherche de conformité est créée avec succès.
Erreur lors de la création de l'action	Lorsque la création d'une action de recherche de conformité échoue en raison d'une exception dans le serveur Exchange.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions de sortie (suite)

Variable	Description
Erreur	Lorsqu'une exception se produit dans l'action de flux.

Vérifier le statut de l'action d'aperçu

L'aperçu de l'action Statut de l'action vérifie l'état de l'action de recherche de conformité de type aperçu et renvoie les informations d'aperçu des e-mails trouvés comme le destinataire, l'expéditeur, l'objet, la date de réception de l'e-mail.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
targetId	Champ d'identificateur obligatoire de l'hôte cible où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
réponse	Contient l'état de l'action de recherche de conformité et les informations d'aperçu de l'e-mail trouvé dans le cadre de la recherche de conformité.

Conditions de sortie

Les conditions de sortie possibles pour cette action sont les suivantes :

Conditions de sortie

Variable	Description
Aperçu en cours	Lorsque l'état de l'action de recherche de conformité est en cours.
Aucun e-mail trouvé	Lorsque l'état de l'action de recherche de conformité est terminé et qu'aucun e-mail n'est trouvé dans le cadre de la recherche de conformité.
Aperçu terminé	Lorsque l'état de l'action de recherche de conformité est terminé et que les e-mails sont trouvés dans le cadre de la recherche de conformité.
Erreur lors de la vérification de l'état	Lorsque la vérification de l'état échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'activité du workflow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une action de suppression de recherche de conformité

L'action Créer une recherche de conformité et supprimer crée une nouvelle action de recherche de conformité de type purge sur le serveur Exchange pour la recherche de conformité créée.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variable	Description
targetId	Champ d'identificateur obligatoire de l'hôte cible où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Conditions de sortie

Les conditions de sortie possibles pour cette action sont les suivantes :

Conditions de sortie

Variable	Description
Terminé	Lorsque l'action de recherche de conformité est créée avec succès.
Erreur lors de la création de l'action	Lorsque la création d'une action de recherche de conformité échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'action de flux.

Vérifier le statut de l'action Supprimer

L'action Vérifier l'état de l'action Supprimer vérifie l'état de l'action de recherche de conformité de type purge et effectue une opération de suppression réversible sur le serveur Exchange pour les e-mails trouvés dans le cadre de la recherche de conformité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variable	Description
targetId	Champ d'identificateur obligatoire de l'hôte cible où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
réponse	Contient l'état de l'action de recherche de conformité et le nombre d'e-mails supprimés qui ont été trouvés dans le cadre de la recherche de conformité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions de sortie

Les conditions de sortie possibles pour cette action sont les suivantes :

Conditions de sortie

Variable	Description
Suppression en cours	Lorsque l'état de l'action de recherche de conformité est en cours.
Aucun e-mail trouvé	Lorsque l'état de l'action de recherche de conformité est terminé et qu'aucun e-mail n'est supprimé dans le cadre de la recherche de conformité.
Suppression terminée	Lorsque l'état de l'action de recherche de conformité est terminé et que les e-mails sont supprimés dans le cadre de la recherche de conformité.
Erreur lors de la vérification de l'état	Lorsque la vérification de l'état échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'action de flux.

Supprimer l'action de recherche de conformité

L'action Supprimer la recherche de conformité supprime la recherche de conformité créée du serveur Exchange.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variable	Description
targetId	Champ d'identificateur obligatoire de l'hôte cible où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Intégration de l'ingestion d'alertes de l'API Microsoft Graph Security

Utilisez l'intégration API de sécurité Microsoft Graph pour ingérer des alertes des fournisseurs de sécurité Microsoft Graph et créer automatiquement des incidents de sécurité.

Vue d'ensemble

Il s'agit API de sécurité Microsoft Graph d'un service intermédiaire (ou courtier) qui fournit une interface de programmation unique pour connecter plusieurs fournisseurs de sécurité (natifs de Microsoft ainsi que les partenaires ServiceNow).

L'intégration API de sécurité Microsoft Graph résout ces problèmes en utilisant le pour se connecter à différentes technologies de sécurité Microsoft telles qu'Azure API de sécurité Microsoft Graph Sentinel, Microsoft Defender Advanced Threat Protection et Azure Advanced Threat Protection. Les alertes des fournisseurs de sécurité Microsoft sont ingérées et les incidents de sécurité sont automatiquement créés dans Réponse aux incidents de sécurité.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Détection des API de sécurité Microsoft Graph alertes qui sont candidates aux incidents de sécurité et automatisation de la création d'incidents de sécurité.
- Mappage des champs d'alerte aux champs d'incident de sécurité.
- Agrégation d'alertes similaires à des incidents de sécurité ouverts existants au lieu de créer des incidents de sécurité en double.
- Prévisualisez les valeurs des champs d'alerte et validez leurs mappages dans l'incident de sécurité.
- Mise à jour automatique de l'état de l'alerte pour la création et la fermeture d'un incident de sécurité.
- Configurez l'ingestion planifiée d'alertes pour créer périodiquement des incidents de sécurité.

Configurer votre instance Now Platform pour l'intégration de l'API Microsoft Graph Security

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre ServiceNow AI Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application afin de garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles et requis ServiceNow AI Platform®Réponse aux incidents de sécurité .	Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre ServiceNow AI Platform® instance. • Un utilisateur disposant du rôle d'administrateur ServiceNow AI Platform® (admin) installe l'application à partir de et ServiceNow Store lui affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans le ServiceNow AI Platform®: ◦ Nomme, crée et modifie les profils d'alerte. ◦ Sélectionne et mappe les champs de données d'alerte de l'API Microsoft Graph Security aux champs d'incident de sécurité. ◦ Prévisualise les détails de l'incident de sécurité pour plus d'exactitude avant de finaliser la configuration. ◦ Planifie l'ingestion d'alerte en cours. ◦ Active la mise à jour des alertes lorsqu'un Réponse aux incidents de sécurité incident est créé et fermé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Les utilisateurs disposant du sn_si.analyst travaillent sur des incidents de sécurité. Pour plus d'informations sur les rôles et l'attribution de rôles aux utilisateurs, voir Rôles sur le site Web de la documentation produit ServiceNow .
Enregistrez votre application dans le Microsoft Azure portail.	Avant de pouvoir ingérer des alertes, vous devez configurer votre application dans le Microsoft Azure portail. Consultez Configurer le portail Microsoft Azure pour en savoir plus.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Ingestion d'événements et d'alertes pour Security Operations : Cette application nécessite : ◦ com.glide.hub.integration.runtime => Exécution du Centre d'intégration ServiceNow ◦ com.glide.hub.action_step.rest => Étape d'action du Centre d'intégration ServiceNow : REST **Remarque :** Les composants du concentrateur d'intégration sont installés avec le module d'extension d'ingestion d'événements et d'alertes. Si ceux-ci ne sont pas installés, contactez le support client pour obtenir de l'aide. Pour plus d'informations sur l'installation Opérations de sécurité des applications principales, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Configurer le portail Microsoft Azure

Pour récupérer les alertes de sécurité d'une application disponible dans le locataire Microsoft Azure à l'aide du API de sécurité Microsoft Graph, vous devez enregistrer l'application dans le Microsoft Azure portail et accorder l'accès en lecture et en écriture aux événements de sécurité à l'application.

Avant de commencer

Rôle requis :

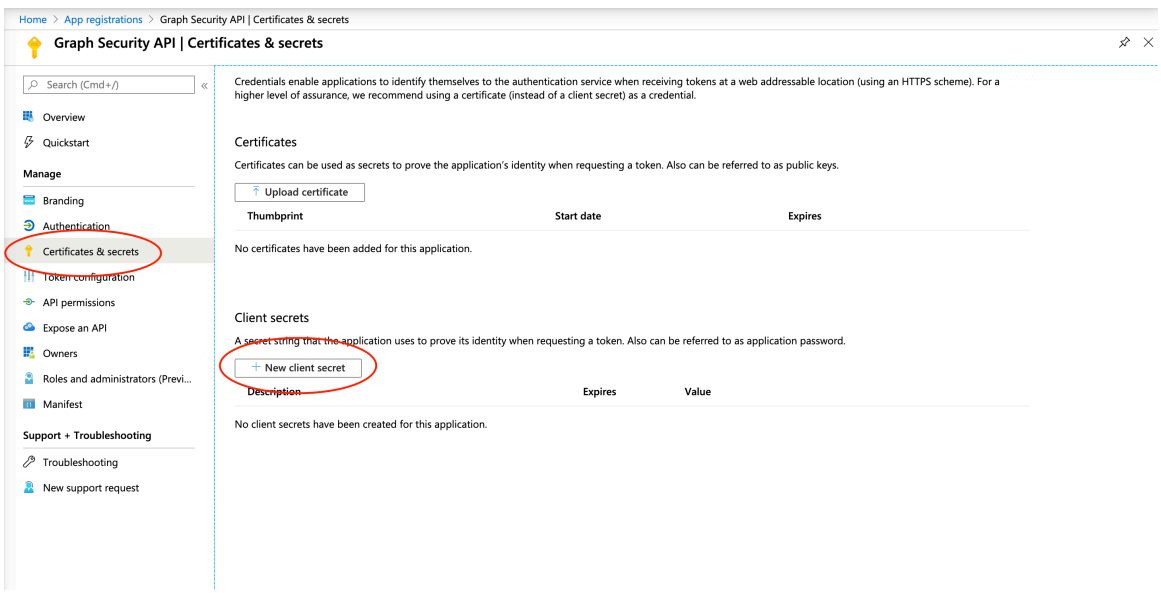
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Développeur d’application : requis pour enregistrer l’application.
- Administrateur de locataire : l’administrateur Microsoft Azure de locataire doit accorder des autorisations à l’application en appelant le point de terminaison de consentement de l’administrateur.

Procédure

1. Connectez-vous au Microsoft Azure portail.
2. Saisissez **les inscriptions d’applications** dans la zone **de recherche** .
3. Cliquez sur **Nouvelle inscription**.
4. Saisissez un nom pour votre application et l’URI de redirection, par exemple http://localhost et cliquez sur **Enregistrer**.
   L’URI de redirection est utilisé lors de la fourniture du consentement de l’administrateur pour l’application.
5. Sur la page Inscriptions d’applications, sélectionnez l’application que vous avez enregistrée, par exemple Graph Security Demo.
6. Sous **Gérer**, sélectionnez **Certificats et secrets**.



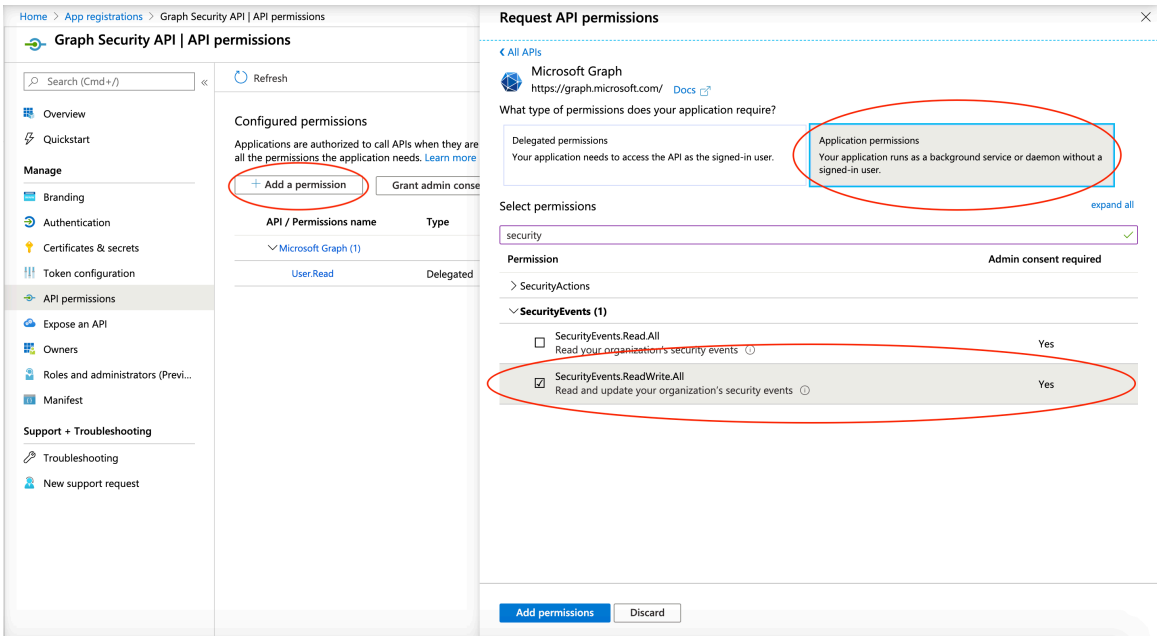
7. Sélectionnez **Nouveau secret client** pour créer un secret client.
   Copiez le secret client et enregistrez-le, car il ne sera plus visible ultérieurement. Si vous avez oublié le secret client, vous pouvez générer un nouveau secret client.

   Remarque : Si vous oubliez le secret client, vous pouvez en générer un nouveau en suivant les instructions des étapes 4 et 5.

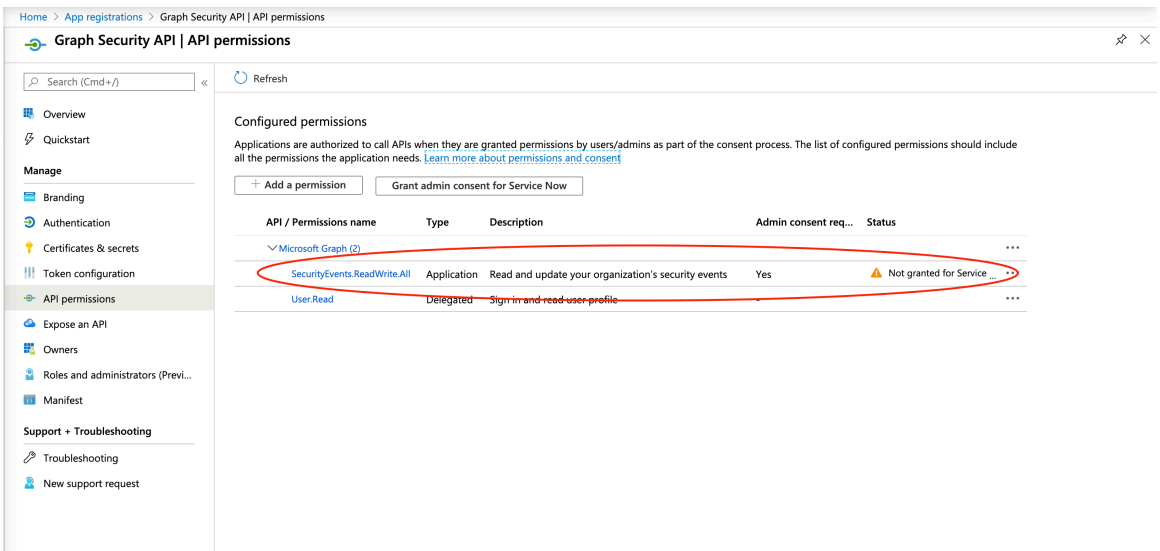
8. Cliquez sur **Afficher les autorisations d’API** dans la page Vue d’ensemble.
9. Ajoutez de nouvelles autorisations d’API au niveau de l’application pour les événements de sécurité SecurityEvents.ReadWrite.All.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Accordez le consentement de l'administrateur pour les autorisations d'API nouvellement ajoutées. Pour plus d'informations, consultez le modèle d'autorisation Microsoft Graph de référence des autorisations Microsoft Graph.



11. Connectez-vous en tant qu'administrateur de locataire et donnez votre consentement pour l'application. Les étapes sont indiquées ci-dessous :

a. Accédez à l'URL suivante : https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

Entrez le APPLICATION_ID de l'application que vous avez enregistrée.

12. Cliquez sur **Accepter** pour accepter les autorisations demandées par l'application créée ci-dessus. Vous pouvez ensuite utiliser l'application pour lire les événements de sécurité. Consultez la documentation sur l'autorisation de sécurité Microsoft Graph pour plus de détails.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer et configurer l'application ServiceNow pour l'intégration de l'ingestion d'alertes de l'API Microsoft Graph Security

Avant d'exécuter l'intégration sur votre ServiceNow AI Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre correctement aux Réponse aux incidents de sécurité produits sur Opérations de sécurité votre ServiceNow AI Platform instance.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si vous n'avez pas installé l'application API de sécurité Microsoft Graph à partir de pour ServiceNow Store l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette API Microsoft Graph Security : ingestion d'alerte.



3. Pour configurer l'application, cliquez sur **Configurer**.
4. Renseignez les champs de la boîte de dialogue Configuration de l'ingestion d'alerte qui s'affiche.

Champ	Description
Nom	Nom de l'instance dans le Microsoft Azure cloud. Vous ne pouvez saisir que des valeurs alphanumériques et des traits d'union (-) dans ce champ.
ID de locataire	L'ID Microsoft Azure du locataire. Il s'agit de l'instance à partir de laquelle toutes les alertes du Microsoft Azure portail sont récupérées.
ID client	ID client de l'application que vous avez enregistrée dans le Microsoft Azure portail. Consultez Configurer le portail Microsoft Azure pour en savoir plus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Secret client	Mot de passe de votre application enregistrée.

5. Cliquez sur **Envoyer**.
   Une fois validée et soumise, chaque configuration de serveur d'ingestions d'alerte est enregistrée sur la page Intégrations de sécurité sous forme de tuile. Si les tuiles de configuration que vous avez enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste de choix Afficher les configurations, cliquez sur **Oui**.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer un profil d'alerte.

Créer un profil pour l'intégration de l'ingestion d'alertes d'API Microsoft Graph Security

En tant qu'utilisateur disposant du rôle sn_si.admin, vous créez un profil d'alerte dans votre ServiceNow AI Platform instance et déterminez quelles alertes génèrent des incidents de sécurité. Avant que des incidents de sécurité ne soient créés à partir d'alertes ingérées, les valeurs de champ des alertes sont affichées sur une mise en page d'un ServiceNow AI Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera affiché.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

L'intégration vous permet d'ingérer différents types d'alertes, telles que des tentatives d'accès non autorisé et des logiciels malveillants, par exemple. Ces alertes sont ingérées en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance. Toutes les alertes sont initialement ingérées pour un type d'alerte configuré dans un profil. Les alertes ingérées peuvent ensuite être filtrées davantage pour spécifier quelles alertes créent des incidents de sécurité.

Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les alertes identifiées comme à haut risque. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir des alertes ingérées, les valeurs de champ individuelles des alertes filtrées sont mappées aux champs correspondants sur une mise en page d'incident de sécurité pour un aperçu. Toutes les alertes qui répondent aux critères de sélection dans votre Microsoft Azure locataire et qui sont disponibles au cours de la API de sécurité Microsoft Graph sont initialement ingérées dans votre ServiceNow AI Platform instance.

Identifier la source pour le profil

Indiquez le nom et la source du profil.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Pour créer un profil pour une alerte dans votre ServiceNow AI Platform instance, accédez à **Intégration de l'API Microsoft Graph Security** > **Profil de l'API Microsoft Graph Security**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs.

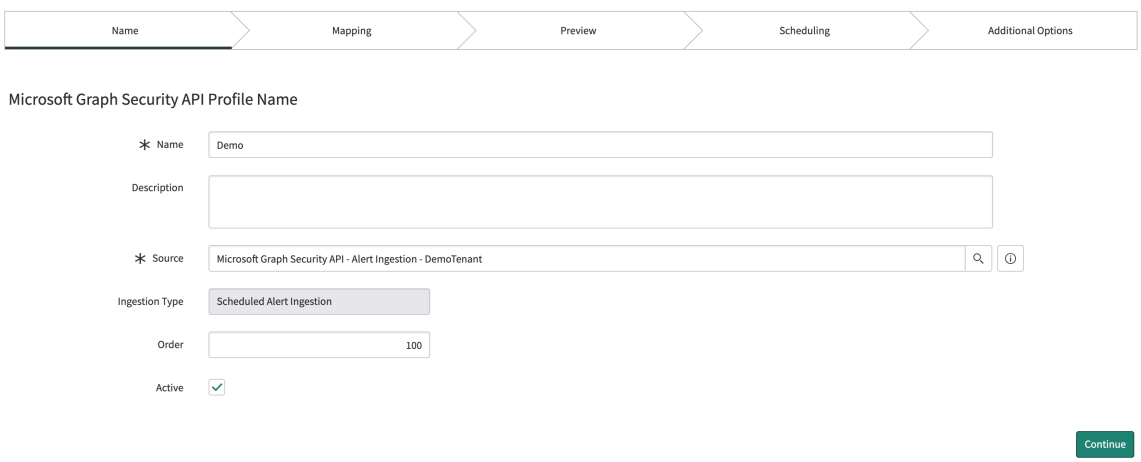
   Un exemple de formulaire rempli suit la table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre ServiceNow AI Platform instance doivent être uniques.
Actif	La case à cocher est désactivée par défaut. Si cette option est désactivée, le profil n'est pas actif. **Remarque :** Vous devez remplir toutes les sections du profil avant de l'activer.
Source	Le Microsoft Azure locataire que vous avez configuré pour ingérer des alertes. Si vous avez configuré plusieurs locataires, sélectionnez le locataire approprié pour les types d'alertes que vous prévoyez d'ingérer pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Plus la valeur de commande est faible, plus la priorité est élevée.
(Facultatif) Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli.



Que faire ensuite

L'étape suivante consiste à mapper les champs d'alerte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage des champs d'alerte pour l'intégration de l'ingestion d'alertes d'API Microsoft Graph Security

Après avoir identifié les sources pour l'ingestion d'alerte planifiée, l'étape suivante consiste à mapper les champs d'alerte individuels aux champs d'un ServiceNow AI Platform SIR incident de sécurité.

Pour l'étape de mappage, vous devez d'abord ingérer des échantillons d'alertes Microsoft Azure du locataire. Ensuite, vous devez vous assurer que toutes les données de champ d'alerte pertinentes sont mappées à l'endroit approprié sur le formulaire d'incident SIR , puis visualiser l'incident dans la SIR section d'aperçu.

Le mappage des exemples de champs d'alerte implique les éléments suivants :

- Ingérer des échantillons d'alertes d'API Microsoft Graph Security
- Mapper les alertes aux champs de réponse aux incidents de sécurité

Ingérer des échantillons d'alertes d'API Microsoft Graph Security

Ingérer des échantillons d'alertes de votre Microsoft Azure locataire.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

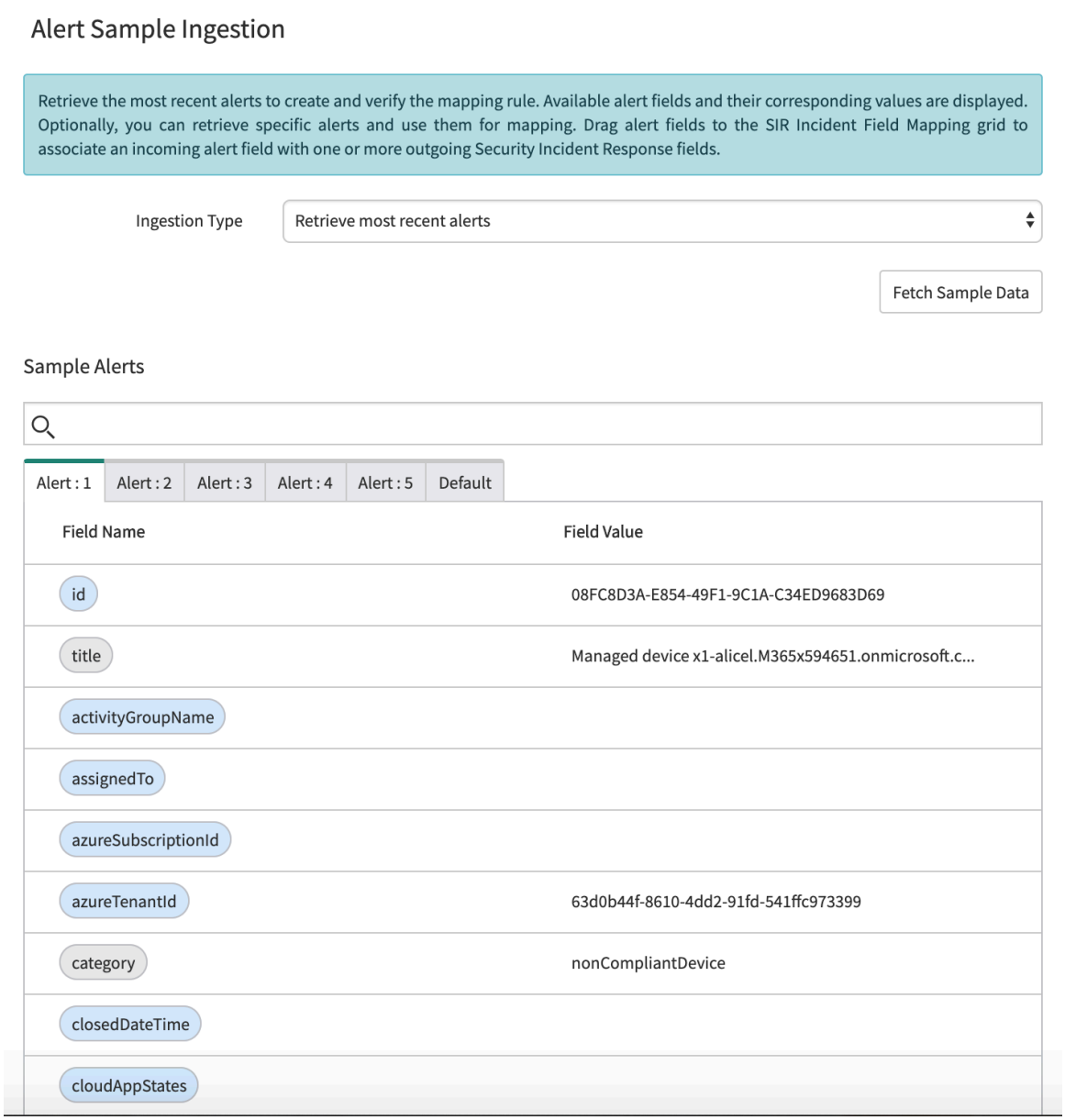
1. Vous pouvez soit extraire les 5 échantillons d'alertes les plus récents, soit fournir les ID d'alerte uniques pour les alertes spécifiques que vous souhaitez utiliser pour votre expérience de mappage.
   Dans la liste de choix **Préférence d'ingestion** , sélectionnez l'une des options suivantes :
   - Récupérer les alertes les plus récentes : les 5 alertes les plus récentes sont récupérées.
   - Sélectionner les alertes en fonction de l'ID des alertes : spécifiez l'ID d'alerte pour les alertes à récupérer. Vous pouvez spécifier un maximum de 5 ID d'alertes séparés par des virgules.
2. Cliquez sur **Extraire un échantillon de données** pour extraire les dernières données d'alerte d'échantillon Microsoft Azure du locataire.
   L'extraction des échantillons d'alertes peut prendre quelques instants.

   Les valeurs des champs d'échantillons d'alerte sont renseignées sur le côté gauche du formulaire lorsque des échantillons d'alertes sont ingérés par le profil. Il s'agit des alertes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que vous mappez aux champs d'incident SIR de sécurité. Les résultats des champs et des valeurs d'alerte sont affichés sous forme d'onglets individuels.



Que faire ensuite

Une fois que vous avez extrait les exemples de données, l'étape suivante consiste à mapper les champs d'alerte à l'incident de sécurité.

Mapper les alertes aux champs de réponse aux incidents de sécurité

Mappez les champs d'alerte individuels des alertes déclenchées aux champs d'un ServiceNow AI Platform incident de sécurité.

Mappage de champs d'alerte

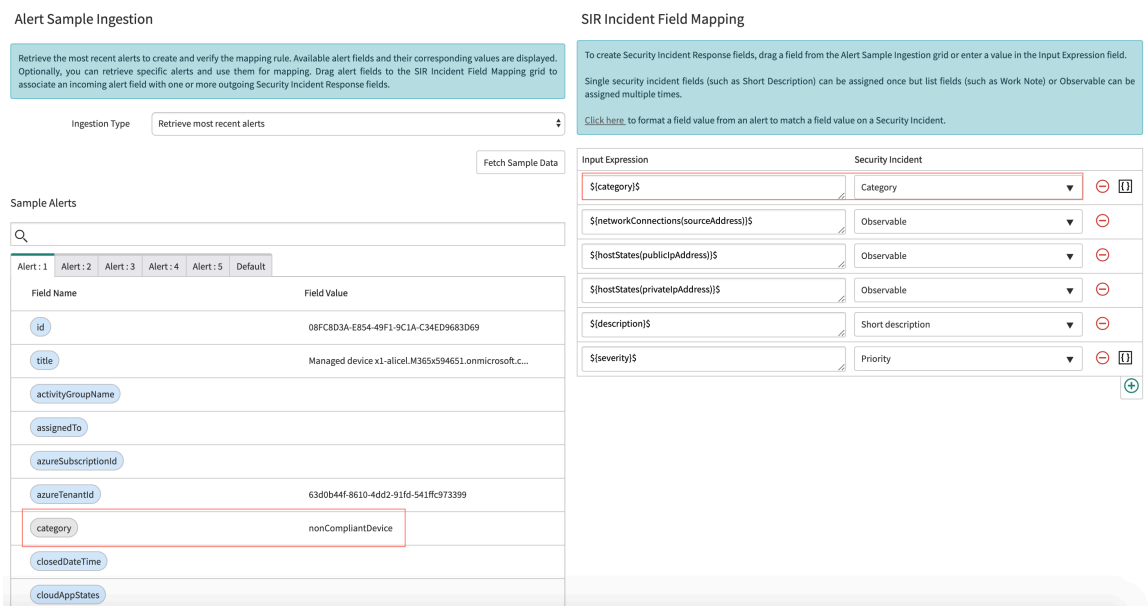
En tant qu'utilisateur disposant du rôle sn_si.admin, utilisez les champs de la section Exemples d'alertes à gauche et mappez-les aux champs d'incident de sécurité de la colonne Mappage de champ d'incident SIR sur le panneau de droite. Modifiez la configuration de mappage en faisant glisser les champs d'alerte du côté gauche et en les déposant dans la section de mappage d'incident SIR sur la droite. Le mappage sur la droite associe le champ d'alerte entrante à un champ d'incident de sécurité sortant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Une fois que vous avez extrait les exemples de données, l'étape suivante consiste à mapper les champs d'alerte à l'incident de sécurité. Pour faire correspondre une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez tout en maintenant enfoncé le nom d'un champ bleu sur le côté gauche du formulaire.
2. Faites glisser le nom du champ, par exemple la catégorie, et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

   La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, la catégorie est mappée au champ Catégorie de l'incident de sécurité.



Toutefois, vous pouvez faire correspondre n'importe quelle valeur du côté gauche à un champ sur la droite. Vérifiez que la valeur est correctement mappée sur l'incident de sécurité pendant l'étape d'aperçu.

Pour vous assurer qu'aucun champ d'alerte n'est négligé ou dupliqué dans le processus de mappage, des champs sont codés par couleur. Le code couleur des champs d'alerte vous aide à suivre les valeurs d'alerte que vous avez déjà mappées à mesure qu'elles deviennent grisées, tandis que tous les champs non mappés restants apparaissent en bleu. Cela vous aide à mieux visualiser quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations d'alerte importantes restantes restent non mappées.

Les champs bleu clair sur la gauche indiquent qu'un champ d'alerte n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ d'alerte entrante à plusieurs champs sur un incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et mappé à un champ de l'incident de sécurité. Ce code couleur vous aide à suivre le mappage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

a. Pour saisir manuellement une valeur dans le champ expression d'entrée, saisissez-la au format ${fieldname}$. Le champ d'alerte sera mappé au champ d'incident de sécurité.

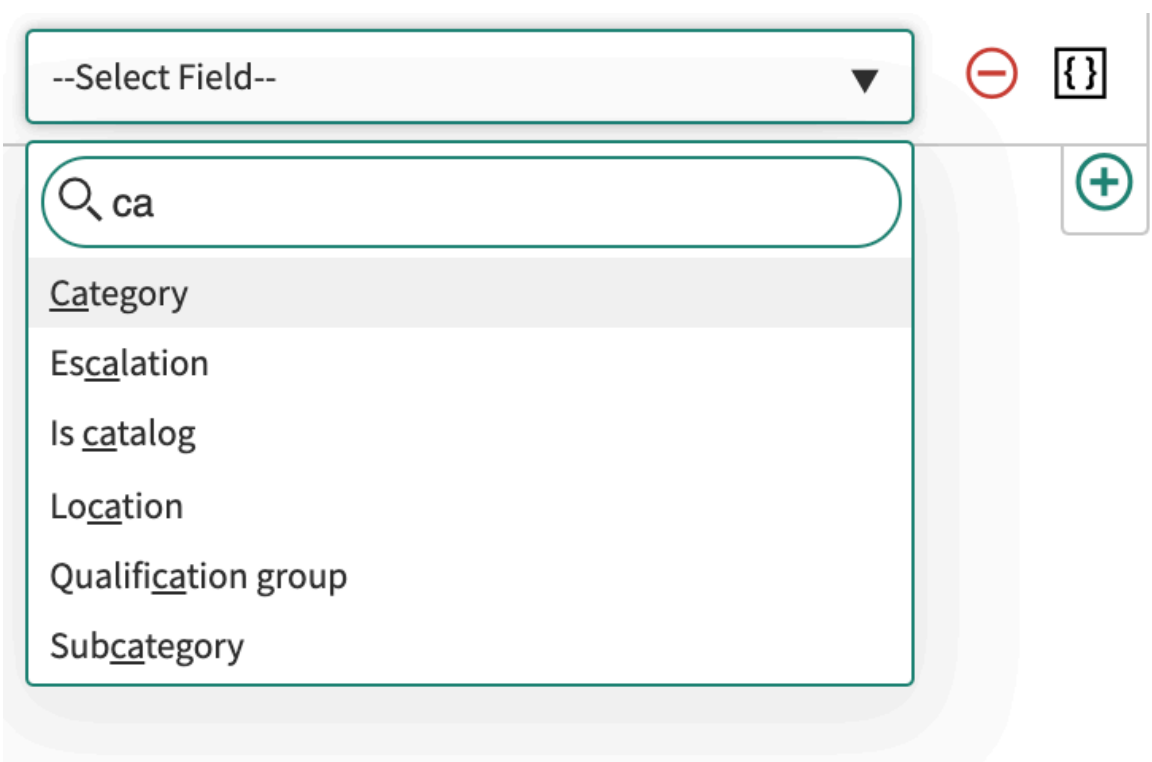
b. Vous ne pouvez pas mapper les alertes ingérées aux champs Cadre de travail de la MITRE-ATT&CK section de mappage des incidents de sécurité. Si vous mappez toujours les champs, les informations ne seront pas disponibles dans le cadre de la MITRE-ATT&CK carte dans la MITRE-ATT&CK section cadre de travail du formulaire d'incident de sécurité. Pour associer les MITRE-ATT&CK techniques, utilisez la fonction d'extraction automatique disponible dans le cadre de travail MITRE-ATT&CK du Renseignements sur les menaces module.

3. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit.

a. À droite du formulaire, dans la section Mappage du champ d'incident SIR , en bas de la grille, cliquez sur l'icône plus (+). Un nouveau champ s'affiche.

b. Dans la colonne Incident de sécurité, développez la liste de choix qui s'affiche, puis sélectionnez un champ.

Dans la liste de choix développée pour le nouveau champ, certains champs sont ombrés. Dans la figure suivante, la catégorie a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. Semblable au code couleur pour les champs d'alerte sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident déjà mappés SIR .



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

> **Remarque :** Comme plusieurs observables peuvent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs.
> Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité possède une liste de choix dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste de choix, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher de la nouvelle ligne.

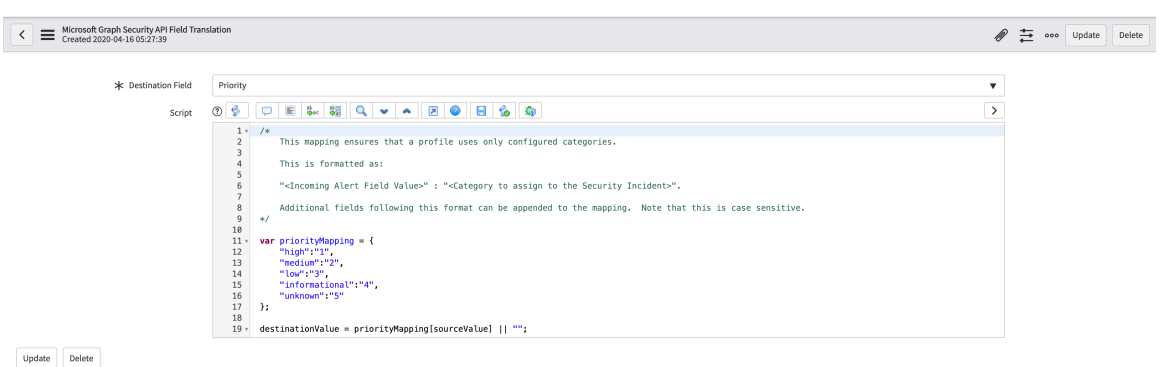
d. Sur le côté gauche du formulaire, cliquez avec le bouton gauche pour sélectionner l'ID d'alerte souhaité dans le champ expression d'entrée. Avec la fonction glisser-déposer, mappez-le à côté de votre nouveau champ.

4. Poursuivez le mappage en ajoutant ou en supprimant des valeurs de champ au mappage.
5. Une fois que vous avez terminé les étapes de mappage de champ précédentes, vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir des critères supplémentaires qu'une alerte entrante doit satisfaire pour créer un incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

Formater la traduction du champ

Dans certains cas, les valeurs des champs d'alerte peuvent API de sécurité Microsoft Graph ne pas être traduites directement dans les champs de l'incident de sécurité SIR. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident de sécurité SIR à l'aide de la fonctionnalité Formater la traduction du champ.

Pour utiliser l'éditeur de script, cliquez sur l'icône {}. L'éditeur de script s'affiche.



Conditions de génération d'incidents

Une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de pouvoir spécifier quelles alertes doivent créer des incidents de sécurité et quelles alertes doivent être filtrées (par exemple, les alertes de priorité faible). Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incidents pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

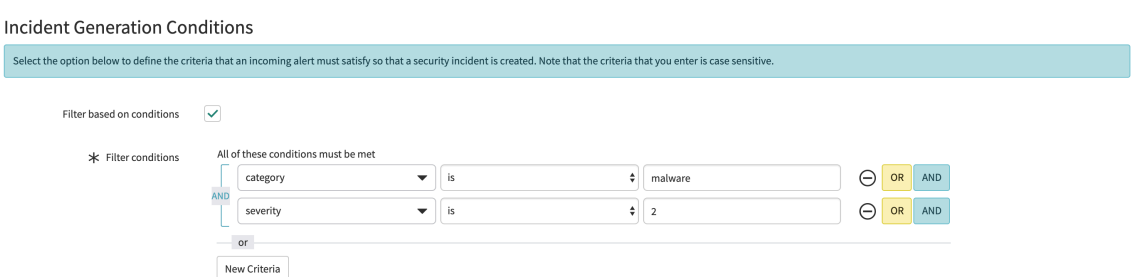
définir des critères supplémentaires qu'une alerte entrante doit satisfaire pour créer un incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

1. Faites défiler jusqu'à la section Conditions de génération d'incidents sur le formulaire et sélectionnez l'option Filtrer en fonction des conditions. Le générateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

   Les options des listes de choix pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'alerte pour l'alerte que vous avez ingérée. Ces champs sont dynamiques et changent en fonction de l'alerte que vous ingérez. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'alerte. Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférerez peut-être retourner à votre locataire Microsoft Azure et examiner vos alertes pour les mots clés.

2. À l'aide des listes de choix et des champs du générateur de conditions, définissez des filtres pour la première ligne.
3. Pour ajouter plus de conditions, à droite des champs, cliquez sur **ET** ou **OU**.
   - Si **ET**est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU**est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Sur la deuxième ligne, définissez une deuxième condition de filtre

   L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création d'incidents de sécurité.



   Vous avez défini les conditions de déclenchement afin que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

   Ce type de filtrage vous aide à isoler les alertes de sécurité et limite le nombre d'incidents de sécurité que vous créez. Si des critères de filtrage supplémentaires sont définis, seules les alertes requises sont ingérées sans qu'il soit nécessaire de modifier la requête ou la configuration des alertes déclenchées.

Critères d'agrégation d'alertes pour gérer des alertes similaires et empêcher les incidents en double

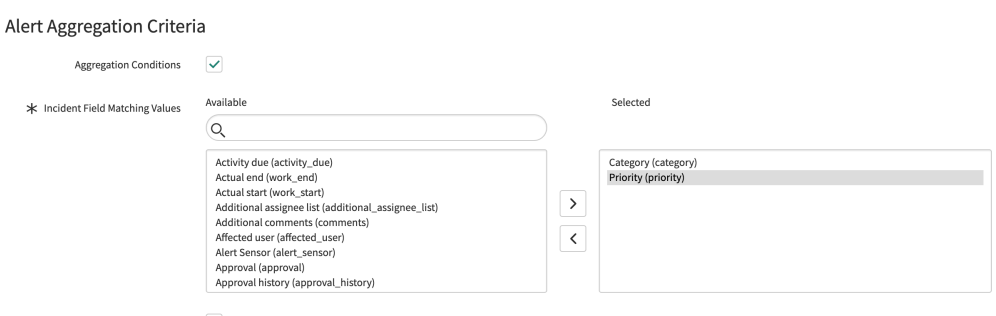
Définissez des critères d'agrégation d'alertes supplémentaires qui regroupent une alerte entrante à un incident de sécurité existant SIR au lieu de créer des incidents similaires, potentiellement en double. En utilisant des critères de valeur de correspondance de champ pour chaque profil, cette option d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'alerte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

connexes sur un seul incident de sécurité. Pour définir les critères, procédez comme suit ci-dessous :

1. Faites défiler jusqu'à la section Critères d'agrégation d'alertes sur le formulaire et sélectionnez l'option Conditions d'agrégation. Les colonnes Valeurs correspondantes au champ Incident s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés sur l'incident SIR de sécurité.
2. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans ServiceNow AI Platform votre et déplacez-les vers la liste Sélectionné. Toutes les valeurs de champ que vous sélectionnez doivent être mises en correspondance pour ajouter cette alerte entrante à un incident de sécurité existant. Cela inclut les champs, tels que les observables et les éléments de configuration, auxquels plusieurs valeurs de champ d'alerte peuvent être mappées. Toutes les valeurs doivent correspondre. Si seul un sous-ensemble de valeurs correspond, les conditions d'agrégation d'alertes ne seront pas remplies et un nouvel incident de sécurité sera créé. Voir la capture d'écran ci-dessous pour le mappage de champs à valeurs multiples.



Si une nouvelle alerte correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation à l'étape de mappage, l'alerte est automatiquement ajoutée à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher toutes les alertes agrégées ajoutées sur une liste connexe sur un incident de sécurité. Toutes les alertes agrégées sur un incident de sécurité sont affichées dans la liste connexe Alertes Microsoft Graph agrégées. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi des alertes sont ajoutées aux incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous Liens connexes et cliquez sur le lien **Afficher toutes les listes connexes** .

3. (Facultatif) Pour enregistrer une note de travail pour une nouvelle alerte récemment ajoutée à l'incident de sécurité, cochez la case pour activer cette option. La note de travail indique qu'une nouvelle alerte a été ajoutée, ainsi qu'un lien vers les détails de l'alerte et tout autre détail qui a pu être ajouté au champ Note de travail dans votre section de mappage.

   Vous avez correctement mappé les valeurs d'une alerte aux champs d'un SIR incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage. Vous avez également ajouté des alertes ou des événements aux incidents de sécurité existants SIR .

4. Cliquez sur **Continuer** pour poursuivre la configuration du profil. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un incident de sécurité SIR

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prévisualiser l'incident de sécurité pour l'intégration de l'API Microsoft Graph Security

Une fois l'étape de mappage terminée, affichez un aperçu des valeurs que vous avez mappées dans un ServiceNow AI Platform SIR incident de sécurité. Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs d'alerte que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer

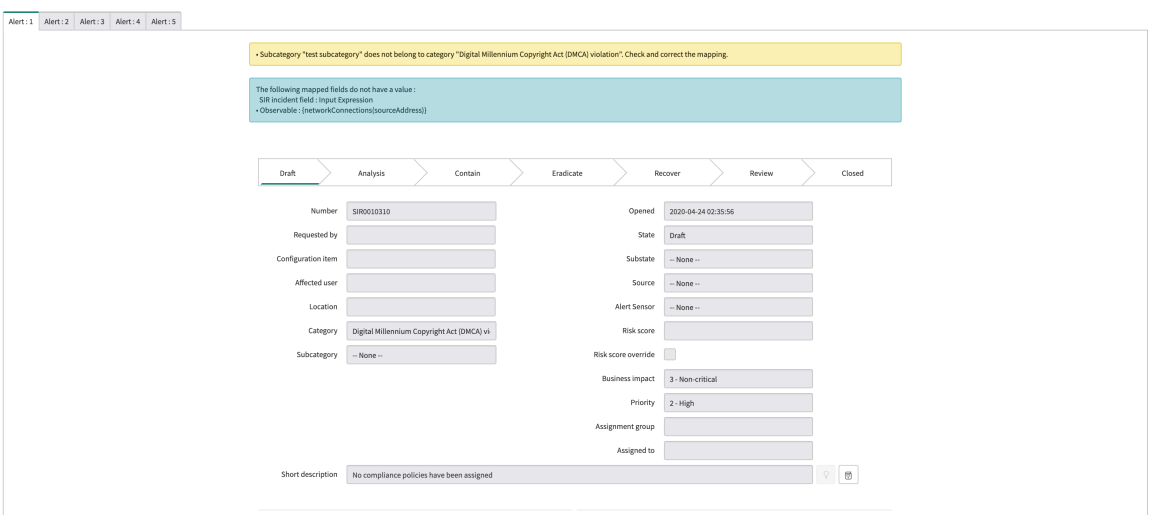
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

En tant qu'utilisateur disposant du rôle sn_si.admin, prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs erronés ou pour renseigner les données manquantes. Si l'aperçu n'est pas effectué avec succès, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le Réponse aux incidents de sécurité produit.

Procédure

1. Si l'aperçu de l'incident de sécurité ne s'affiche pas, cliquez sur **Aperçu** dans la barre de progression.
   Toutes les alertes ingérées et les mappages de champs définis dans la page Mappage s'affichent.
2. Cliquez sur un ID d'alerte pour afficher un aperçu de l'incident de sécurité.
   Cette vue est en lecture seule et aucun enregistrement de cet incident de sécurité n'est enregistré.
3. Examinez le mappage de champs des valeurs d'alerte sur l'incident de sécurité.



L'image précédente est un exemple d'aperçu avec une erreur de mappage des échantillons qui ont été ingérés.

4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

Que faire ensuite

Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à définir le calendrier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir le calendrier pour l'intégration de l'API Microsoft Graph Security

Vérifiez les paramètres par défaut pour la récupération des alertes ou modifiez la planification si nécessaire. Cette étape vous permet de filtrer la récupération de vos alertes en fonction d'une plage de dates.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez également choisir la fréquence à laquelle vous interrogerez les alertes futures qui correspondent à la configuration du profil d'alerte. Pour les profils d'ingestion d'alerte automatisée, avant que le profil ne soit activé, vous vérifiez et modifiez la planification et la récupération des alertes. Cette étape est nécessaire pour les profils d'alerte planifiée.

En tant qu'utilisateur disposant du rôle sn_si.admin, vous configurez ces intervalles d'interrogation pour chaque profil. Les performances de l'intégration de l'ingestion API de sécurité Microsoft Graph d'alerte sont impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférez peut-être équilibrer la charge du système par rapport à l'urgence de l'incident. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférez peut-être modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

Procédure

1. Si la page Planification de la barre de progression ne s'affiche pas, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les alertes sont extraites du Microsoft Azure locataire.

Option	Description
Ingestion d'alerte en cours sélectionnée	En fonction du paramètre par défaut, l'instance ServiceNow AI Platform extrait du Microsoft Azure locataire de nouvelles alertes toutes les cinq minutes. Les incidents de sécurité sont créés si des alertes déclenchées sont trouvées et si les critères de filtrage de génération d'incidents sont vérifiés. Pour équilibrer l'ingestion d'alertes par rapport à la charge du serveur et pour extraire les données les plus récentes, vous préférez utiliser cinq minutes. Toutefois, cette valeur peut être modifiée si nécessaire.
○ Ingestion d'alerte en cours sélectionnée ○ Définir le délai d'ingestion de l'alerte initiale	Délai d'ingestion initial Si vous souhaitez planifier l'ingestion initiale à une heure précise, procédez comme suit : ○ Sélectionnez les champs Ingestion d'alerte en cours et Définir la durée d'ingestion de l'alerte initiale. ○ Spécifiez la durée dans le champ Entrer le délai d'ingestion de l'alerte initiale. L'ingestion initiale aura lieu à l'heure spécifiée ici. Les ingestions suivantes seront basées sur le calendrier défini dans le champ Incrémentation de l'interrogation (minutes). Par exemple, si vous avez une tâche d'alerte quotidienne qui s'exécute une fois

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	par jour à 4 h (heure locale), vous pouvez configurer le profil d'alerte correspondant dans votre ServiceNow AI Platform instance pour qu'il s'exécute à 4 h 05, heure locale, afin de capturer immédiatement l'alerte et de créer un incident de sécurité. Saisissez 04 05 00 dans le champ Inges–tion d'alerte initiale. Dans le champ Incré–mentation (minutes), saisissez 1 440 (24 heures) pour planifier la prochaine inges–tion d'alerte pendant 24 heures à compter de l'ingestion d'alerte initiale. Le délai d'in–gestion de l'alerte initiale et l'heure d'in–gestion de l'alerte suivante sont affichés dans les champs. Pour configurer les paramètres de cet exemple, procédez comme suit : ○ Sélectionnez l'option **Ingestion d'alerte en cours** . ○ Dans le champ Incrémentation de l'inter–rogation (minutes), saisissez 1440 (24 heures). ○ Cliquez sur l'option **Définir la durée d'in gestion de l'alerte initiale** pour activer la modification des champs Délai d'inges–tion de l'alerte initiale et Délai (estimé) d'ingestion de l'alerte suivante. ○ Dans le champ Délai d'ingestion de l'alerte initiale, saisissez 04 05 00. Dans le champ Heure (estimée) de la prochaine ingestion d'alerte, l'heure de la prochaine ingestion d'alerte s'affiche.
Champ de récupération unique sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhai–tez une extraction ponctuelle pour ingérer des alertes historiques. Lorsque ce paramètre est configuré, un profil est utilisé une fois pour récupérer les alertes des événements historiques basés sur une plage de dates. À droite du champ Depuis la date, cliquez sur l'icône Calen–drier. Dans le calendrier qui s'affiche, sé–lectionnez la date à laquelle vous souhaitez commencer à extraire des alertes. À partir de la valeur Depuis la date, les alertes sont récupérées jusqu'à la date actuelle. No–tez que vous pouvez revenir jusqu'à sept jours en arrière à partir de la date actuelle. Cette fonctionnalité n'est pas destinée à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	récupérer un nombre important d'alertes historiques, mais plutôt un nombre mini–mal d'alertes en cours de traitement actif au moment de l'activation du profil. Une fois les alertes extraites, ce paramètre ne récupère plus d'alertes pour ce profil à partir de la date actuelle. Ce paramètre renseigne l'incident de sécurité avec toutes les alertes trouvées pour la plage que vous saisissez.

3. Cliquez sur **Continuer** pour accéder à la page Options supplémentaires.

Automatiser les mises à jour et la fermeture des alertes en fonction de l'état de l'incident SIR

L'intégration API de sécurité Microsoft Graph d'ingestion d'alertes dispose d'une interface bidirectionnelle qui permet aux deux alertes de créer des incidents de sécurité, ainsi qu'une mise à jour des alertes une fois l'incident de sécurité créé et/ou fermé avec les détails pertinents de l'incident tels que le numéro d'incident, le SIR groupe d'affectation, SIR l'URL de l'incident, etc. T

Avant de commencer

Rôle requis : sn_si.admin

Remarque : Les états d'alerte initiale et de fermeture ne sont mis à jour que si cette fonctionnalité est prise en charge par le fournisseur de service. Pour en savoir plus, consultez la documentation et la API de sécurité Microsoft Graph documentation du fournisseur de sécurité.

Procédure

1. Si la page Options supplémentaires de la barre de progression ne s'affiche pas, sélectionnez **Options supplémentaires**.
2. Suivez les instructions ci-dessous pour terminer la configuration de la mise à jour des alertes lors de la création de l'incident de sécurité.

Option ou champ	Description
Mettre à jour les alertes lors de la création de l'incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour le statut de l'alerte et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'alerte. Cela peut se produire à la fois pour les alertes de déclenchement initiales qui créent l'incident de sécurité et pour les alertes agrégées.
Mise à jour de l'état de l'alerte initiale	Sélectionnez un état d'alerte initial dans la liste. Cet état est défini pour toutes les alertes lorsqu'un incident de sécurité est créé pour une alerte ingérée. Cela inclut les alertes qui créent de nouveaux incidents et les alertes qui sont ingérées et agrégées à un incident ouvert existant. **Remarque :** En fonction de l'état d'alerte sélectionné ici, l'état d'alerte utilisé par les fournisseurs de sécurité est mis à jour en conséquence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
Commentaires initiaux renvoyés à l'alerte	En fonction de l'étape que vous avez sélectionnée, les commentaires par défaut s'affichent. Vous pouvez modifier le texte par défaut et utiliser le format ${nom de champ}$ pour ajouter ou modifier les champs disponibles dans le formulaire d'incident de sécurité.
Fermer les alertes lors de la fermeture de l'incident SIR	Sélectionnez cette option si vous souhaitez utiliser l'option de fermeture automatique des alertes. Cela peut se produire à la fois pour les alertes de déclenchement initiales qui créent l'incident de sécurité et pour les alertes agrégées. L'état de l'alerte est mis à jour dans le fournisseur de sécurité avec les commentaires d'état et de fermeture après SIR la fermeture de l'incident dans le ServiceNow AI Platform.
Mise à jour de l'état de l'alerte de fermeture	Sélectionnez un état d'alerte dans la liste. Sélectionnez la valeur d'état à définir pour toutes les alertes lorsqu'un incident de sécurité est fermé pour une alerte ingérée.
Commentaires de fermeture renvoyés à l'alerte	Les commentaires de fermeture par défaut sont affichés ici. Vous pouvez modifier le texte par défaut et utiliser le format ${nom de champ}$ pour ajouter ou modifier tous les champs disponibles dans le formulaire d'incident de sécurité.

3. Cliquez sur **Terminer** pour terminer la configuration et faire passer le profil à l'état **En attente** .
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Activez ce profil pour extraire des alertes du Microsoft Azure locataire en fonction de votre planification. Un maximum de 1 000 incidents de sécurité peut être créé dans un délai de 24 heures.

Paramètres de configuration de l'intégration de l'API Microsoft Graph Security

Utilisez cette option pour modifier les propriétés système par défaut de l'intégration d'ingestion API de sécurité Microsoft Graph .

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

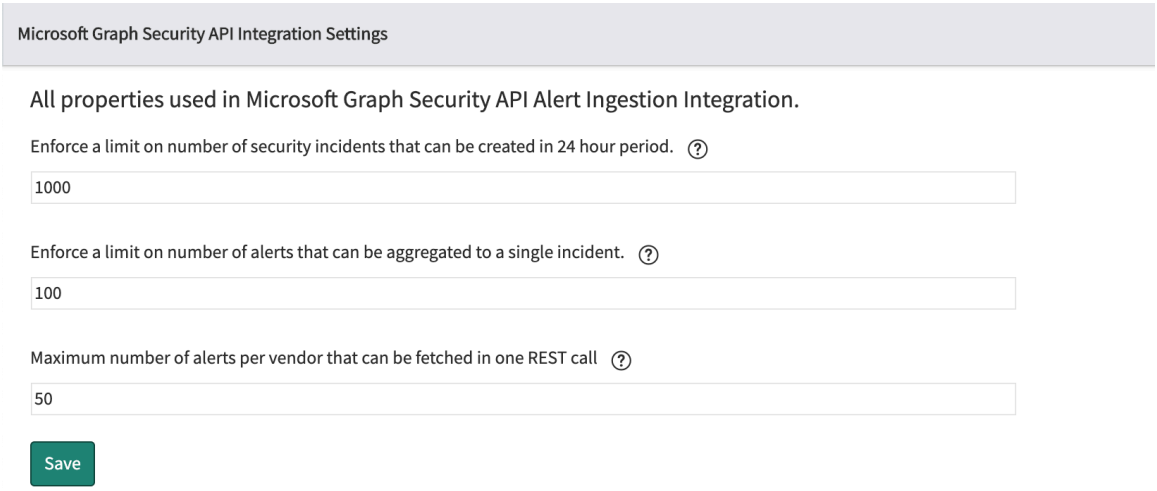
Modifiez les propriétés de configuration par défaut pour limiter le nombre d'incidents de sécurité qui peuvent être créés sur une période de 24 heures ou le nombre d'alertes qui peuvent être regroupées en un seul incident de sécurité.

Pour modifier les propriétés système, connectez-vous en tant qu'utilisateur disposant du rôle *sn_si.admin* et accédez à **Intégration de l'API Microsoft Graph Security** > **Paramètres de l'API de sécurité Microsoft Graph**.

Les paramètres de configuration par défaut s'affichent. Vous pouvez modifier ces paramètres si nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



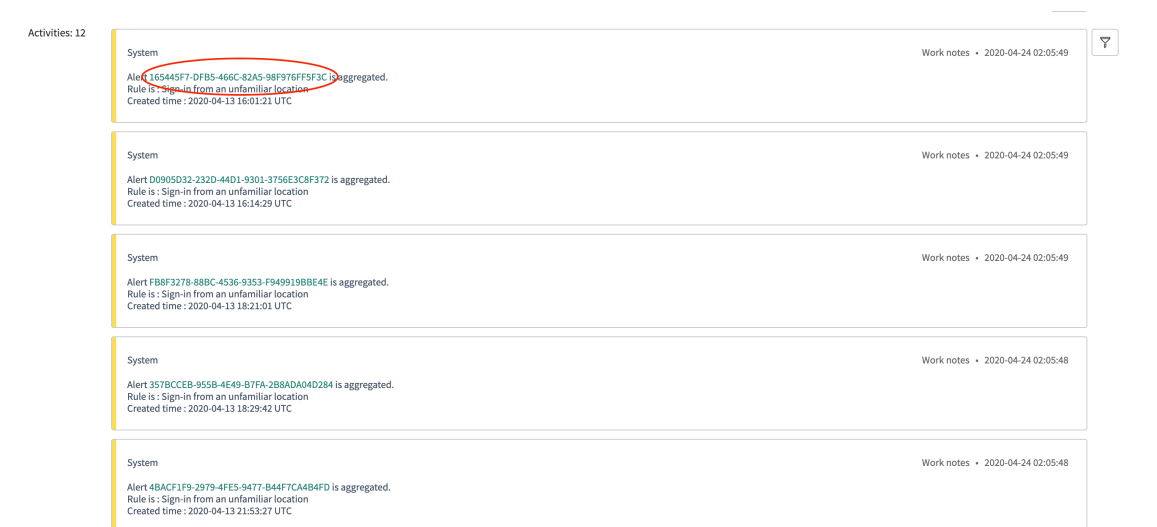
Tous les paramètres d'intégration modifiés seront appliqués au cours de l'intervalle d'interrogation suivant, tel que défini dans le profil.

Formulaire Réponse aux incidents de sécurité après l'ingestion d'alerte

Une fois qu'une API de sécurité Microsoft Graph alerte a été ingérée, un incident de sécurité est créé et les mises à jour correspondantes sont apportées à l'enregistrement d'incident de sécurité.

Notes de travail

Si vous aviez sélectionné l'option **Consigner la note de travail pour la nouvelle alerte** dans les critères d'agrégation d'alertes, comme décrit dans le Mapper les alertes aux champs de réponse aux incidents de sécurité, une note de travail est publiée lorsque l'alerte est agrégée.



Cliquez sur le lien de l'alerte pour accéder à l'enregistrement d'importation d'alerte interne qui contient des données d'alerte brutes.

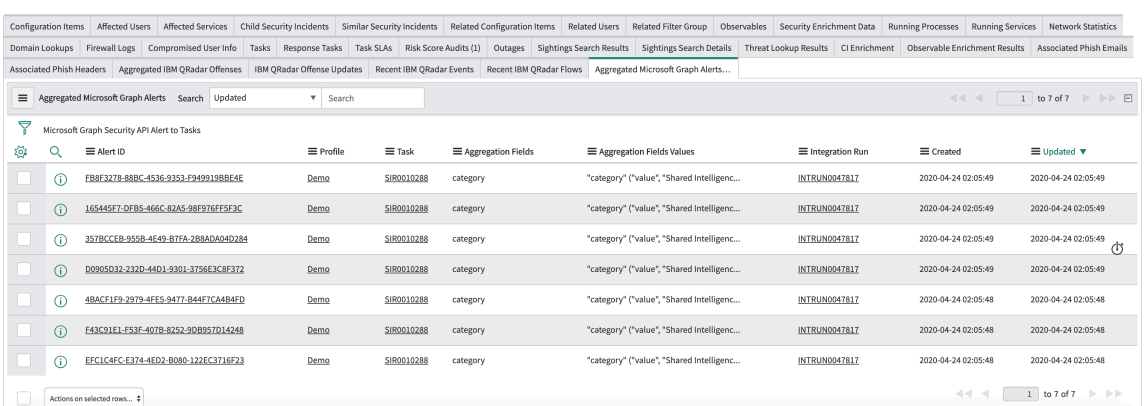
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Alertes agrégées

Cliquer sur **Listes connexes** > **Alertes de sécurité Microsoft Graph agrégées** pour afficher les alertes agrégées à l'incident de sécurité.



- **Créer un incident de sécurité** : sélectionnez une alerte dans la liste, cliquez sur le menu **Actions** , puis sur **Créer un incident de sécurité**. Cette option crée un nouvel incident de sécurité pour l'alerte et cette alerte est désagrégée de l'incident de sécurité parent.
- **Supprimer l'enregistrement d'alerte** : sélectionnez une alerte dans la liste, cliquez sur le menu **Actions** , puis sur **Supprimer**. Cette option supprime l'enregistrement d'alerte.

Facultatif : copier un profil d'API Microsoft Graph Security

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils pour gagner du temps.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

En tant qu'utilisateur disposant du rôle sn_si.admin, si vous copiez un profil, le nom du profil est initialement modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) et n'est donc pas activé accidentellement avant de terminer la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intégration de l'API Microsoft Graph Security** > **Profil de l'API Microsoft Graph Security**.
2. Dans la liste Profils qui s'affiche API de sécurité Microsoft Graph , sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.
   Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (vrai), la copie est désactivée à ce stade (faux). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.

   Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. Notez que l'état de la colonne **Actif** est défini sur faux, car le profil doit être activé.

Que faire ensuite

Vous êtes invité à activer le nouveau profil une fois que vous avez terminé les étapes de configuration.

Séparation de domaine et API de sécurité Microsoft Graph ingestion d'alerte

L'application Séparation de domaine est prise en charge. L'intégration API de sécurité Microsoft Graph ingère les alertes des fournisseurs de sécurité Microsoft Graph et crée automatiquement des incidents de sécurité. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : basique

- Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de service de l'application.
- L'application prend en charge Séparation de domaine lors de l'exécution. Séparation de domaine inclut la séparation à partir de l'interface utilisateur, des clés de cache, du reporting, des déploiements et des agrégations.
- Le propriétaire de l'instance doit configurer l'application de sorte qu'elle fonctionne sur plusieurs locataires.

Exemple de cas d'utilisation : lorsqu'un fournisseur de service (SP) utilise la messagerie instantanée pour répondre au message d'un locataire-client, le client doit pouvoir afficher la réponse du SP.

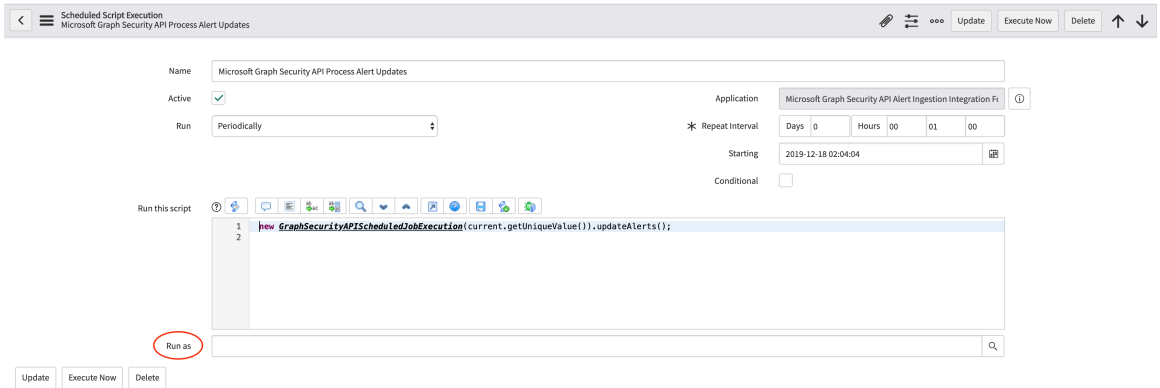
Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

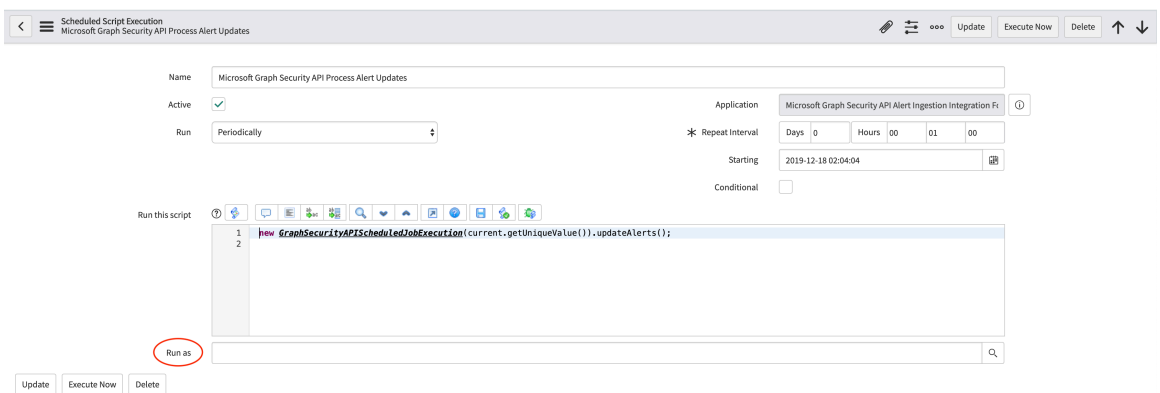
Comment fonctionne Séparation de domaine dans API de sécurité Microsoft Graph

Pour réaliser la séparation de domaine, répliquez les API de sécurité Microsoft Graph travaux planifiés Processus de profil et SIR Mises à jour des alertes de processus et changez les travaux **Exécuter en tant qu'utilisateurs** . Par défaut, les utilisateurs système exécutent ces travaux planifiés. Changez **l'exécution en tant qu'utilisateur** ayant le rôle sn_si.admin dans le domaine respectif et exécutez la tâche planifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





Information associée

Séparation de domaine pour les fournisseurs de services

Utilisation de Concepteur de flux et du concentrateur d'intégration dans l'intégration de l'API Microsoft Graph Security

À l'aide de Concepteur de flux et de la fonctionnalité IntegrationHub, plusieurs flux secondaires et actions ont été créés dans le cadre de l'intégration API de sécurité Microsoft Graph .

Les flux secondaires suivants sont disponibles :

- API de sécurité Microsoft Graph Validation de la configuration : cette option est utilisée dans la tuile de configuration pour valider les informations d'identification de la configuration initiale.
- Appel REST pour API de sécurité Microsoft Graph: ceci est utilisé pour toutes les interactions avec l'API de sécurité Microsoft Graph à l'aide d'appels REST.
- Récupérer des échantillons d'alertes : ceci est utilisé dans la section Mappage de la configuration du profil pour extraire des données d'échantillon. Ce flux secondaire est déclenché de façon asynchrone.

Dépannage de l'intégration de l'API Microsoft Graph Security

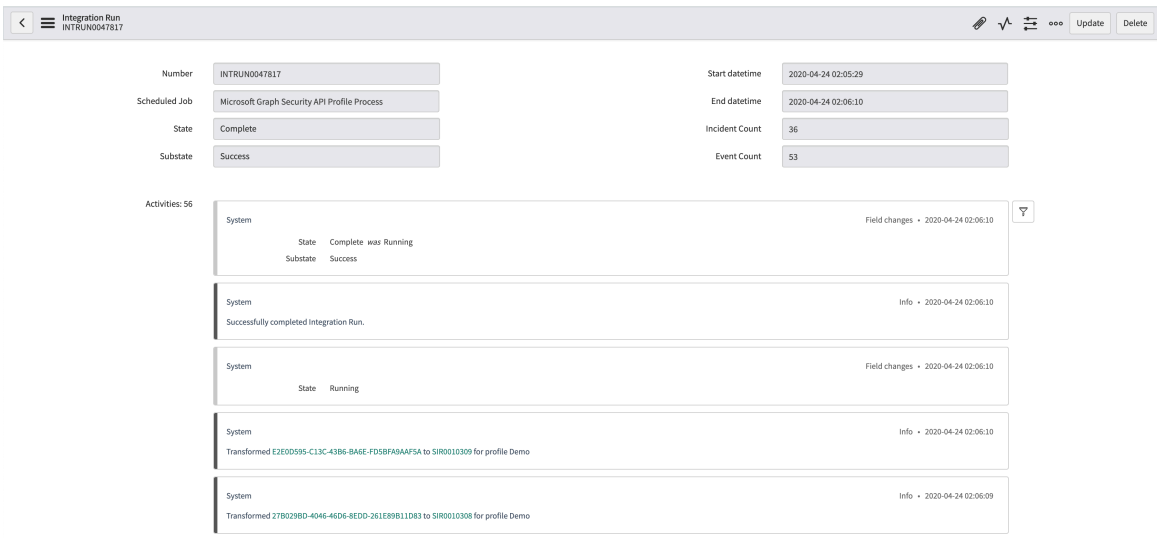
Cette section présente des conseils de dépannage importants et les questions fréquemment posées relatives à l'intégration de l'ingestion d'alertes API de sécurité Microsoft Graph .

- **Exécution de l'intégration** : lorsqu'une tâche planifiée commence à s'exécuter, un enregistrement d'exécution de l'intégration avec des journaux, des erreurs et des avertissements s'affiche. Le nombre d'alertes extraites et le nombre d'incidents créés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

lors d'une exécution de tâche planifiée sont également affichés. Les utilisateurs disposant du rôle sn_si.analyst peuvent voir si des erreurs/profils ont échoué lors de l'extraction pendant l'exécution de l'intégration. Les utilisateurs disposant du rôle sn_si.analyst peuvent rechercher des erreurs dans la table sn_event_ingestion_integration_run .
Pour résoudre les problèmes d'intégration, vous devez d'abord vérifier l'exécution de l'intégration. Les erreurs sont enregistrées sous forme de notes de travail dans les enregistrements d'exécution de l'intégration pour chaque exécution de tâche planifiée.



- **Profil incomplet** : lors de la configuration du profil, dans la section Options supplémentaires (Automatiser les mises à jour et la fermeture des alertes en fonction de l'état de l'incident SIR), vous devez cliquer sur le bouton **Terminer** pour vous assurer que le profil est déplacé vers l'état En attente indiquant qu'il est en attente d'ingestion.
- **Valider le profil** : pour valider si l'intégration fonctionne correctement, vérifiez les états du profil, la date de la dernière opération Pull du profil, la table d'importation d'alertes, les enregistrements de la table des alertes à la tâche.
- **Problèmes SSL** : lors de la connexion via le , assurez-vous que l'instance dispose d'un certificat CA valide qui n'a API de sécurité Microsoft Graph pas expiré. Vous pouvez importer RSA ou vos propres certificats dans la plateforme et vous assurer que le nom commun du certificat correspond au nom d'hôte. Voir KB0778285 pour plus de détails.

Intégration Palo Alto Networks - AutoFocus

Le Palo Alto Networks - AutoFocus système de base d'intégration comprend un workflow et une série d'activités de workflow que vous pouvez utiliser pour intégrer Palo Alto Networks - AutoFocus votre instance.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

Activer et configurer l'intégration Palo Alto Networks - AutoFocus

---

Utiliser

Développer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

- Security Operations Palo Alto Networks : workflow de vérification et de blocage des valeurs
- Obtenir des informations sur la session AutoFocus Flux d'enrichissement
- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Traduction automatique

Activer et configurer l'intégration Palo Alto Networks - AutoFocus

La fonction Configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, notamment Palo Alto Networks - AutoFocus. Avant de pouvoir utiliser le Palo Alto Networks - AutoFocus, vous devez le télécharger à partir ServiceNow Store du .

Avant de commencer

Rôle requis : sn_si_admin

Procédure

1. Télécharger une application à partir de ServiceNow Store pour la première fois.
2. Une fois l'installation terminée, accédez au site d'assistance de Palo Alto Networks et obtenez la clé API.
3. Dans votre instance, accédez à **Security Operations** > **Configuration de l'intégration**.
4. Sur la carte Palo Alto Networks AutoFocus, cliquez sur **Configurer**.
5. Entrez (ou collez) la **clé API** que vous avez acquise sur le site d'assistance de Palo Alto Networks.
6. Cliquez sur **Envoyer**.

Obtenir des informations sur la session AutoFocus Flux d'enrichissement

Lorsque le flux **d'enrichissement des informations de session Security Operations Palo Alto Networks - Get AutoFocus** est exécuté, il met en file d'attente une requête de recherche avec AutoFocus pour recueillir des informations sur une adresse IP source spécifiée. Si AutoFocus a connaissance des sessions précédentes provenant de cette adresse IP, un rapport au format JSON est renvoyé.

Avant de commencer

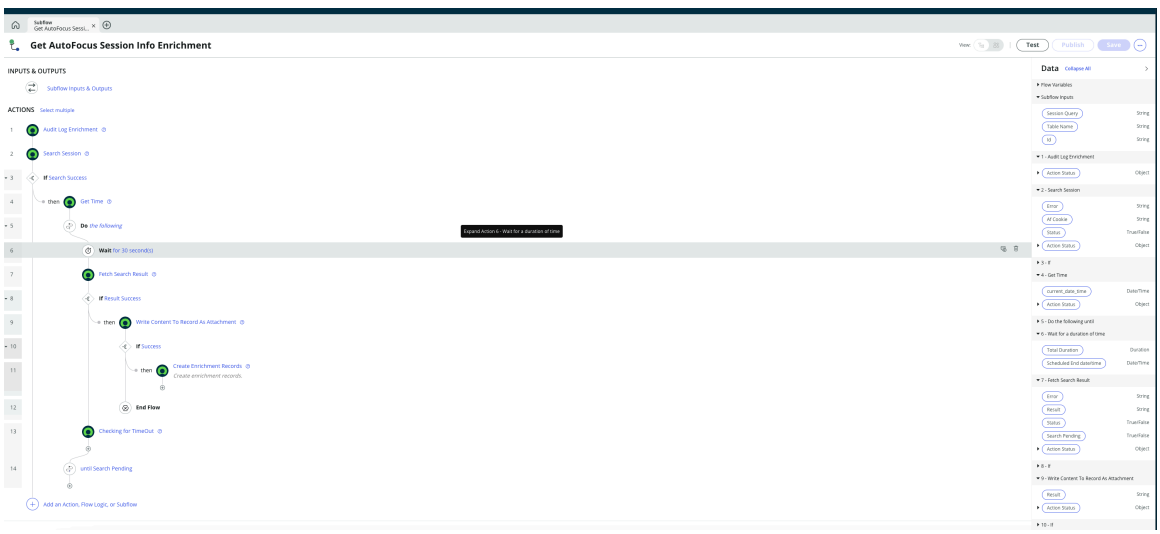
Rôle requis : sn_si.analyst

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Le flux **d'enrichissement Security Operations Palo Alto Networks - Obtenir des informations de session AutoFocus** est exécuté lorsque le champ **IP source** d'un incident de sécurité est modifié et que l'enregistrement est mis à jour. Le flux récupère l'adresse IP et envoie une requête à AutoFocus. Si AutoFocus a précédemment identifié des sessions provenant de l'adresse IP, un rapport au format JSON est renvoyé.

Security Operations Palo Alto Networks : obtenir le flux d'enrichissement des données WildFire



Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. Cliquez sur **l'onglet Indicateurs de compromission** et renseignez le champ **Adresse IP source** .
3. Cliquez sur **Mettre à jour**.
   AutoFocus analyse les informations à partir de l'adresse IP et un fichier texte au format JSON est joint à l'incident de sécurité.

   Les actions spécifiques à cette intégration sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Action de session de recherche AutoFocus

L'action de flux **de session de recherche AutoFocus** télécharge les informations d'une adresse IP affectée à un incident de sécurité vers AutoFocus et les met en file d'attente pour une requête de recherche.

Variables d'entrée

Remarque :

Lorsque l'action s'exécute, elle met en file d'attente une requête de recherche avec AutoFocus pour collecter des informations pour une adresse IP source spécifiée. Si AutoFocus a précédemment identifié des sessions provenant de cette adresse IP, un rapport au format JSON est renvoyé.

Les variables d'entrée déterminent le comportement initial de l'action.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Variable	Description
searchSessionQuery [chaîne]	Requête de recherche d'informations sur la session.

Action Récupérer les résultats de la recherche

L'action **de flux Récupérer les résultats de recherche** récupère les résultats de recherche identifiés par un cookie sur la requête de recherche initiée par l'action de **session de recherche AutoFocus** .

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variables d'entrée

Variable	Description
afcookie [chaîne]	Le cookie AutoFocus pour la demande de recherche générée par le Action de session de recherche AutoFocus.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
searchPending [booléen]	Vrai si la demande de recherche est toujours en cours de traitement dans AutoFocus.
Résultat [chaîne]	Données des résultats de la recherche.
état [booléen]	Vrai si la recherche est terminée et que les résultats ont été générés avec succès.
Erreur [chaîne]	L'erreur, le cas échéant, qui s'est produite dans l'action.

Intégration Palo Alto Networks - Firewall

Pour effectuer Palo Alto Networks - Firewall l'intégration, assurez-vous d'avoir une Serveur MID configuration avec des informations d'identification SSH. Si aucun pare-feu n'est déjà installé, ajoutez-en un.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

- Activer et configurer l'intégration du pare-feu Palo Alto Networks
- Configurer les informations d'identification SSH vers le serveur MID

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

Utiliser

Palo Alto Networks Workflow du lanceur de pare-feu

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Configurer les informations d'identification SSH vers le serveur MID

Le pare-feu Palo Alto Networks envoie des appels d'API au serveur MID. Dans ce contexte, assurez-vous que les informations d'identification SSH ont été créées pour Serveur MID.

Avant de commencer

- Le module d'extension Orchestration doit être activé.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Orchestration** > **Informations d'identification et connexions** > **Informations d'identification**.
2. Cliquez sur **Nouveau**.
3. Dans l'écran Intercepteur, cliquez sur **Informations d'identification SSH**.
4. Renseignez les champs nécessaires.

Informations d'identification SSH

Champ	Description
Nom	Entrez un nom pour les informations d'identification.
Actif	Cochez cette case pour activer ces informations d'identification.
Concerne	**Sélectionnez Tous les serveurs MID** ou **Serveurs MID spécifiques**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Serveurs MID	Si vous avez sélectionné **Serveurs MID spécifiques**, cliquez sur l'icône de verrou et sélectionnez les serveurs MID auxquels vous souhaitez appliquer ces informations d'identification.
Ordre	Sélectionnez l'ordre dans lequel les informations d'identification sont essayées par le serveur. Les plus petits nombres sont essayés en premier.
Nom d'utilisateur	Entrez le nom d'utilisateur de l'utilisateur associé à ces informations d'identification, le cas échéant.
Mot de passe	Si vous avez saisi un **nom d'utilisateur**, entrez le mot de passe de l'utilisateur.
Balise	Entrez une balise à utiliser pour les critères de recherche. Le champ **Balise** doit contenir la même valeur que le **nom**.

Activer et configurer l'intégration du pare-feu Palo Alto Networks

La fonction Configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, notamment Palo Alto Networks - Firewall. Avant de pouvoir utiliser le Palo Alto Networks - Firewall, vous devez le télécharger à partir ServiceNow Store du .

Avant de commencer

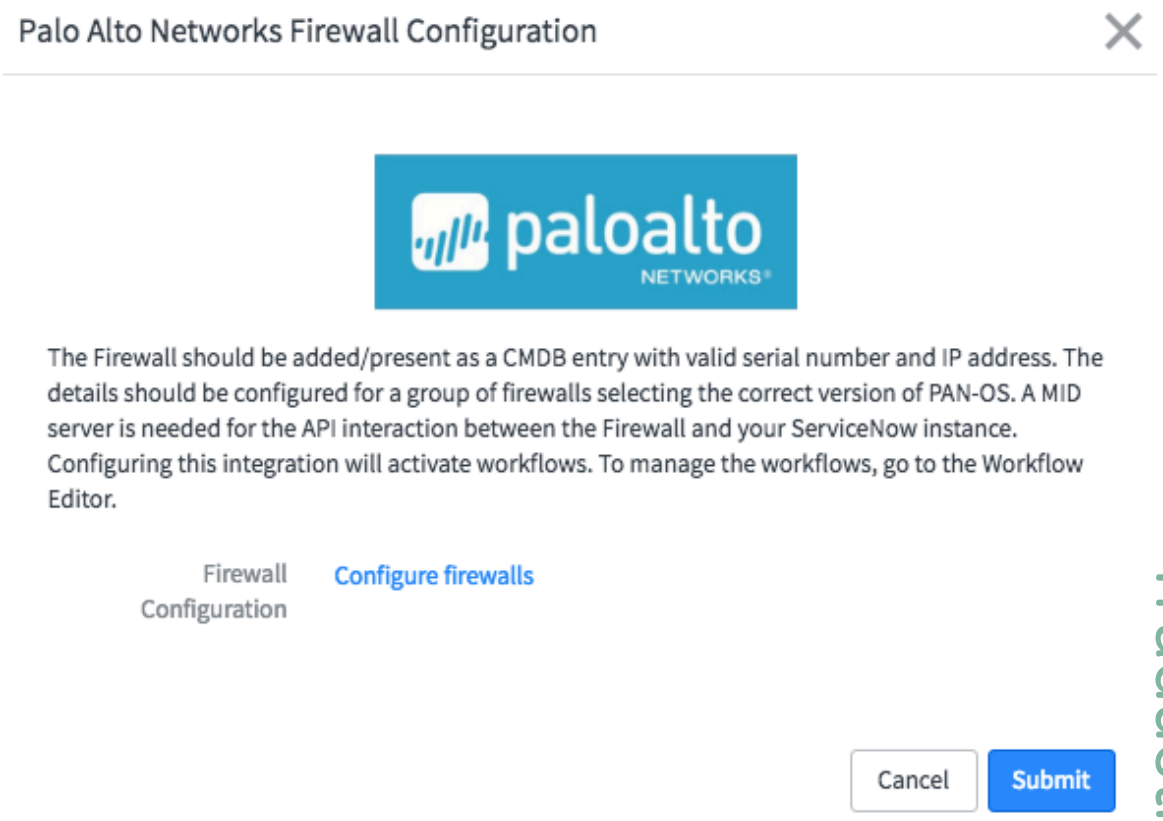
Rôle requis : sn_si_admin

Procédure

1. Avant d'activer et de configurer l'intégration, accédez au tableau de bord du pare-feu Palo Alto Networks. Notez les noms de la liste dynamique d'adresses IP, d'URL ou de domaine que vous utilisez pour le blocage du pare-feu.
2. Télécharger l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Security Operations** > **Configuration de l'intégration**. Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte Palo Alto Networks Firewall, cliquez sur **Configurer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

5. Cliquez sur **Configurer les pare-feu**.
6. Dans l'écran Configurations du pare-feu, cliquez sur **Nouveau**.
7. Renseignez les champs du formulaire comme il convient.

Champ	Description
Pare-feu	Cliquez sur l'icône de verrou et sélectionnez le pare-feu à configurer.
Version du pare-feu	Sélectionnez la version du pare-feu Palo Alto Networks.**PAN-OS-7.1** est la version recommandée. La sélection de versions antérieures peut renvoyer des résultats incohérents.
Nom d'utilisateur	Entrez le nom d'utilisateur à utiliser lors de la connexion au pare-feu via les points de terminaison REST.
Mot de passe	Entrez le mot de passe de l'utilisateur qui se connecte.
Liste dynamique d'adresses IP	Entrez le nom de la liste dynamique externe ou de la liste de blocs dynamiques que vous utilisez pour les adresses IP.
Liste dynamique d'URL	Entrez le nom de la liste dynamique externe ou de la liste de blocs dynamiques que vous utilisez pour les URL.
Liste dynamique de domaine	Saisissez le nom de la liste dynamique externe ou de la liste de blocs dynamiques que vous utilisez pour les domaines.

8. Cliquez sur **Envoyer**.

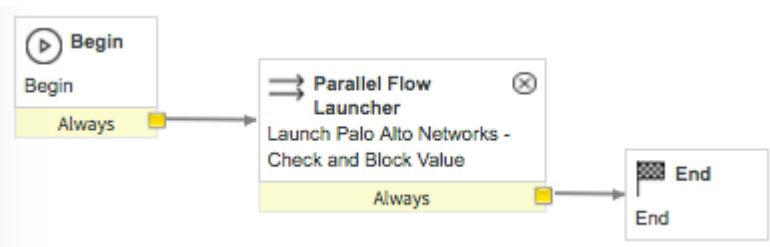
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Palo Alto Networks Workflow du lanceur de pare-feu

Le workflow du **lanceur de pare-feu Palo Alto Networks** de Security Operations est l'implémentation du pare-feu Palo Alto Networks lancée par le workflow de l'aptitude **Security Operations Integration - Demande de bloc**.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Les activités du processus de workflow comprennent :Security Operations Palo Alto Networks : workflow de vérification et de blocage des valeurs



Security Operations Palo Alto Networks : workflow de vérification et de blocage des valeurs

Au fur et à mesure que des incidents de sécurité sont créés et triés pour identifier les menaces potentielles, vous pouvez utiliser le workflow **Security Operations Palo Alto Networks - Check and Block Value** pour vérifier et mettre à jour automatiquement les adresses IP, les URL et les domaines à l'aide de listes dynamiques externes définies dans Palo Alto Networks - Firewall.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Le workflow **Security Operations Palo Alto Networks - Vérifier et bloquer la valeur** est exécuté lorsque les demandes de blocage de pare-feu sont soumises. La demande de bloc spécifie le pare-feu à utiliser, le type d'observable à vérifier et à bloquer (si nécessaire) et la valeur du bloc. C'est-à-dire l'adresse IP, l'URL ou le domaine en question.

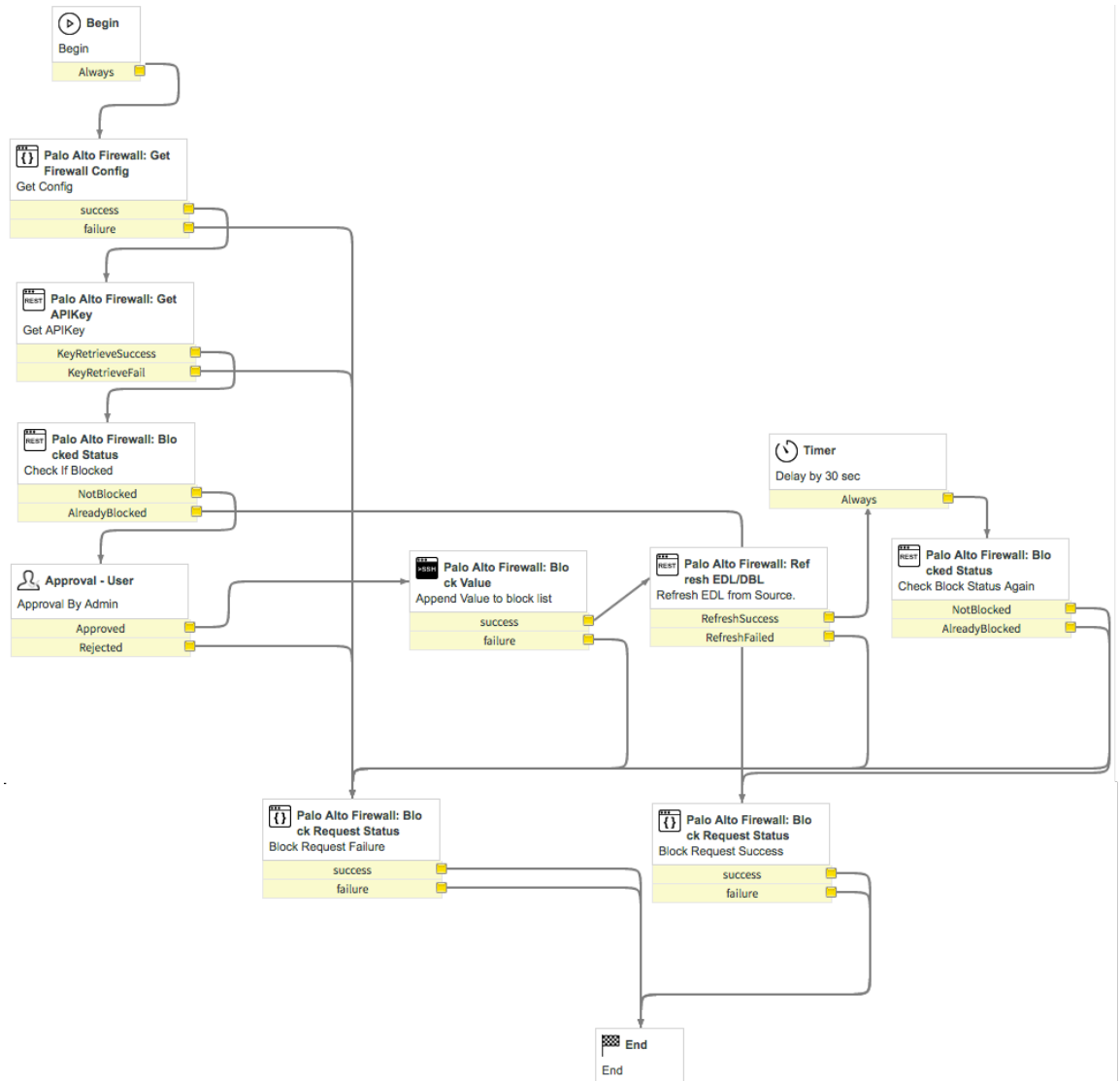
Pendant l'exécution du workflow, les commandes définies sous **Intégration de Palo Alto Networks** > **Pare-feu** > **Commandes** sont exécutés. Les commandes de type Show (par exemple, Show-IP-ExternalDynamicList) déterminent si la valeur existe sur le pare-feu. Les commandes de type Refresh (par exemple, Refresh-IP-ExternalDynamicList) ajoutent de la valeur qui n'existe pas sur le pare-feu à la liste de blocs.

Après l'exécution de l'activité État bloqué, l'approbation d'un administrateur système est requise pour que le workflow puisse se poursuivre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Palo Alto Networks : workflow de vérification et de blocage de valeur



Procédure

1. Accédez à la **Intégration de Palo Alto Networks** > **Pare-feu** > **Demandes de blocs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Pare-feu	Sélectionnez le pare-feu à utiliser.
Type de bloc	Sélectionnez le type de valeur à vérifier : ○ IP ○ URL ○ DOMAINE

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Valeur du bloc	Saisissez la valeur du type sélectionné à vérifier sur le pare-feu.

4. Cliquez sur **Envoyer**.

Pare-feu Palo Alto : bloquer l'activité de l'état de la demande

Cette activité est appelée par d'autres activités pour définir l'état de la demande de bloc de pare-feu sur réussite ou échec.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
firewallBlockRequestSysid [chaîne]	L'ID système de la demande de bloc de pare-feu. Cette variable d'entrée est obligatoire.
État [chaîne]	Indique si la tâche d'actualisation a été exécutée : réussite ou échec.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures. La sortie se compose de données provenant de la configuration du pare-feu ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
Résultat [chaîne]	Indique si la tâche d'actualisation a réussi ou échoué.

Pare-feu Palo Alto : activité de valeur de bloc

Une fois que le workflow a identifié une valeur qui n'est pas sur le pare-feu, l'enregistrement est acheminé pour approbation. Après approbation, cette activité se connecte au serveur MID via vos informations d'identification SSH et invoque un script qui ajoute la valeur à la liste de blocs externes du pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Remarque : Vous devez entrer manuellement les variables d'entrée pour cette activité, puis publier le workflow . Si le workflow n'est pas publié, les variables d'entrée ne sont pas enregistrées pour les utilisateurs non-administrateurs.

Variables d'entrée

Variable	Description
toBeBlockedValue [chaîne]	Valeur à ajouter à l'EDL si elle n'est pas déjà présente. Cette variable d'entrée est obligatoire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée (suite)

Variable	Description
typeToBeBlocked [chaîne]	Type de valeur à bloquer : IP, URL ou Domaine. Cette variable d'entrée est obligatoire.
targetHost [chaîne]	Serveur MID sur lequel le script est exécuté.
SSHCredentialTag [chaîne]	La balise d'informations d'identification SSH définie sur le Serveur MID.
scriptCommand [chaîne]	Script AppendValueToList.sh utilisé pour ajouter la valeur à l'EDL. Le chemin d'accès complet au serveur MID est nécessaire.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Résultat [chaîne]	Le résultat a été transmis à l'EDL.

Pare-feu Palo Alto : activité d'état bloqué

Cette activité vérifie si la valeur (IP, URL ou domaine) est incluse dans sa liste dynamique externe/liste de blocs dynamiques (EDL/DBL) respective sur le pare-feu. Les détails EDL/DBL sont obtenus à partir du pare-feu à l'aide d'une commande opérationnelle, et une routine est exécutée pour vérifier si la valeur est bloquée sur le pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité. Toutes les entrées de variables d'entrée répertoriées sont obligatoires.

Variables d'entrée

Variable	Description
valueToBeChecked [chaîne]	La valeur de la demande de bloc.
showEDLDetailsCommand [chaîne]	La commande Liste dynamique externe utilisée pour déterminer si la valeur existe sur le pare-feu.
FirewallIpAddress [chaîne]	L'adresse IP du pare-feu utilisé.
FirewallApiKey [chaîne]	Clé API du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures. La sortie se compose de données provenant de la configuration du pare-feu, ainsi que de données générées dynamiquement à l'aide du message API de commande opérationnelle du pare-feu Palo Alto.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
commandResult [chaîne]	Résultats du pare-feu pour la commande Afficher les détails de l'EDL.
blockedStatus [booléen]	Vrai indique bloqué. Faux indique non bloqué.
commandResponse [chaîne]	État de la réponse obtenu à partir du pare-feu pour la commande Afficher les détails de l'EDL.

Pare-feu Palo Alto : obtenir l'action de clé API

Cette action récupère la clé API à partir du pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action. Toutes les entrées de variables d'entrée répertoriées sont obligatoires.

Variables d'entrée

Variable	Description
Nom d'utilisateur [chaîne]	Le nom d'utilisateur de l'administrateur du pare-feu.
Mot de passe [chaîne]	Mot de passe administrateur du pare-feu.
FirewallIpAddress [chaîne]	Adresse IP du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes. La sortie se compose de données provenant de la configuration du pare-feu ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
APIKey [chaîne]	Clé API du pare-feu.

Pare-feu Palo Alto : action Obtenir la configuration du pare-feu

L'action de flux **Pare-feu Palo Alto : obtenir la configuration du pare-feu** accède à toutes les informations de configuration du pare-feu connexes à partir de la base de données et les rend disponibles pour utilisation par l'action suivante.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variables d'entrée

Variable	Description
firewallSysid [chaîne]	ID système du pare-feu. Cette variable d'entrée est obligatoire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée (suite)

Variable	Description
typeOfValueToBeBlocked [chaîne]	Type de valeur à bloquer sur le pare-feu : IP, URL ou Domaine.
firewallIPAddress [chaîne]	Adresse IP du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes. La sortie se compose de données provenant de la configuration du pare-feu ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
ipEDLName [chaîne]	Nom de la liste dynamique externe pour les adresses IP.
urlEDLName [chaîne]	Nom de la liste dynamique externe pour les URL.
domainEDLName [chaîne]	Nom de la liste dynamique externe des domaines.
firewallVersionSysId [chaîne]	ID système pour la version du pare-feu.
refreshEDLCommand [chaîne]	Commande à utiliser pour actualiser l'EDL à partir de la source.
ShowEDLDetailsCommand [chaîne]	Commande à utiliser pour obtenir les détails de l'EDL.
état [booléen]	Vrai indique la réussite. Faux indique un échec.
Erreur [chaîne]	L'erreur, le cas échéant, qui s'est produite dans l'action.
point de terminaison [chiffré]	Point de terminaison chiffré à partir de la base de données.

Pare-feu Palo Alto : actualiser l'activité EDL/DBL

Cette activité exécute une commande opérationnelle sur le pare-feu pour actualiser la liste dynamique externe à partir de la source configurée sur le pare-feu. La sortie de cette activité indique si la tâche d'actualisation a été mise en file d'attente.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité. Toutes les entrées de variables d'entrée répertoriées sont obligatoires.

Variables d'entrée

Variable	Description
FirewallIpAddress [chaîne]	Adresse IP du pare-feu en cours d'actualisation.
FirewallApiKey [chaîne]	Clé API de pare-feu actualisée.
FirewallCommand [chaîne]	Commande opérationnelle à exécuter pour mettre en file d'attente la tâche d'actualisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures. La sortie se compose de données provenant de la configuration du pare-feu ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
activité. Sortie.résultat [chaîne]	Chaîne de texte indiquant si la tâche d'actualisation a été mise en file d'attente pour s'exécuter : réussite ou échec.

Obtenir le flux de données du journal

Si Réponse aux incidents de sécurité, Renseignements sur les menaces et sont Palo Alto Networks - Firewall activés, le flux **Security Operations Palo Alto Networks - Obtenir les données du journal** s'exécute automatiquement lorsque l'adresse IP source des observables dans un incident de sécurité est modifiée.

Avant de commencer

Rôle requis : sn_si.analyst

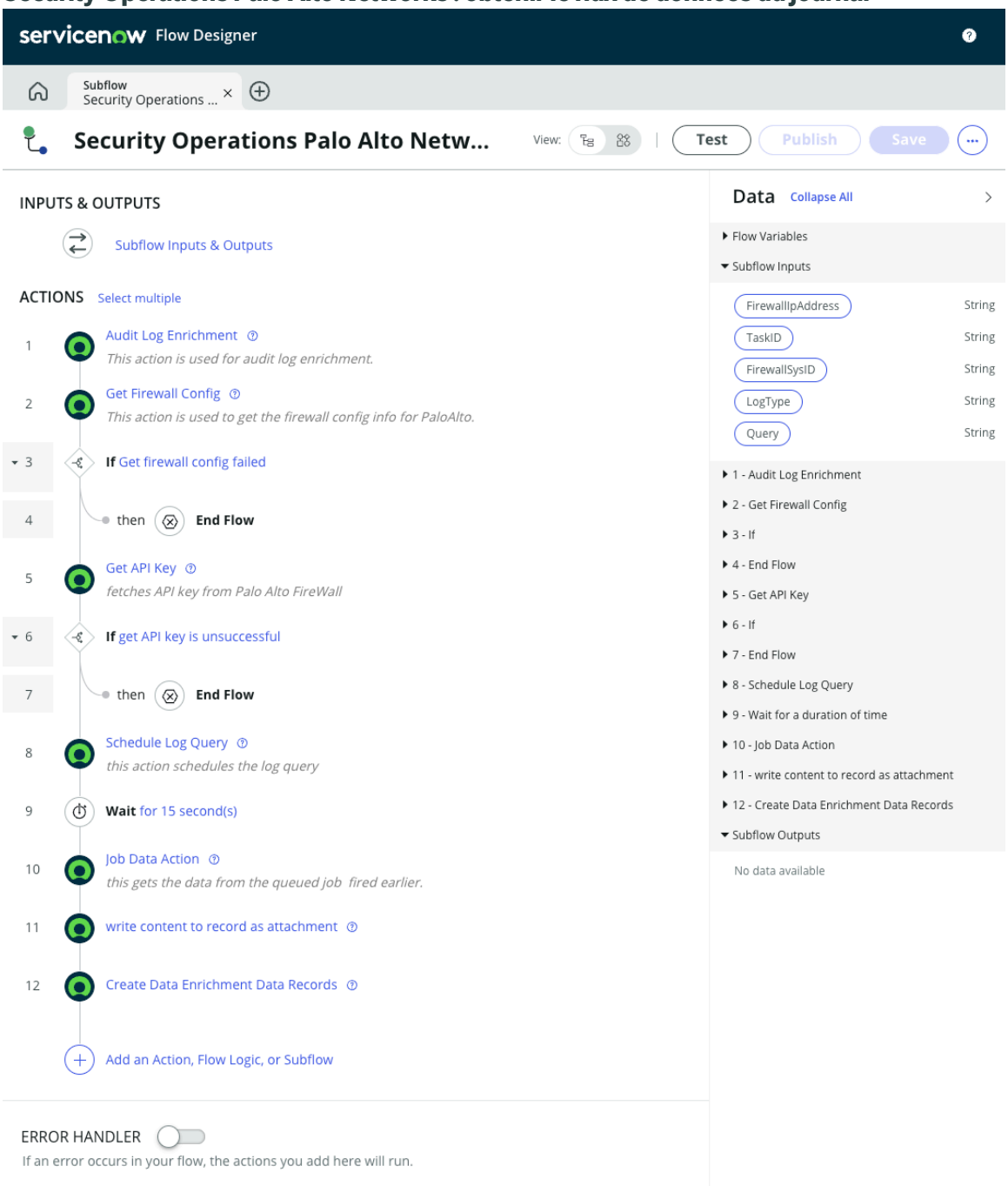
Pourquoi et quand exécuter cette tâche

Pendant l'exécution du flux, les informations de configuration du pare-feu sont récupérées à partir de la base de données et la clé API est récupérée à partir du pare-feu. L'action Obtenir le journal met en file d'attente une requête de recherche sur le pare-feu. Lorsque la requête s'exécute, elle renvoie un ID de tâche qui est utilisé pour récupérer les données des journaux de menaces à partir du pare-feu. Il joint les données du journal sous forme de fichier XML à l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Palo Alto Networks : obtenir le flux de données du journal



Traduction automatique

Procédure

1. Accédez à un incident de sécurité qui contient des observables.
2. Cliquez sur l'onglet **Observables de l'incident de sécurité** .
3. Dans **Adresse IP source**, ajoutez ou modifiez l'adresse IP.
4. Cliquez sur **Mettre à jour**.
   Le flux **Security Operations Palo Alto Networks : obtenir les données du journal** s'exécute et les données enrichies du journal des menaces sont jointes à l'incident de sécurité. Les informations sont également analysées et affichées dans la section **Journaux du pare-feu** sous **l'onglet Données d'enrichissement** .

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pare-feu Palo Alto : obtenir l'action de clé API

Cette action récupère la clé API à partir du pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action. Toutes les entrées de variables d'entrée répertoriées sont obligatoires.

Variables d'entrée

Variable	Description
Nom d'utilisateur [chaîne]	Le nom d'utilisateur de l'administrateur du pare-feu.
Mot de passe [chaîne]	Mot de passe administrateur du pare-feu.
FirewallIpAddress [chaîne]	Adresse IP du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes. La sortie se compose de données provenant de la configuration du pare-feu ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
APIKey [chaîne]	Clé API du pare-feu.

Pare-feu Palo Alto : action Obtenir la configuration du pare-feu

L'action de flux **Pare-feu Palo Alto : obtenir la configuration du pare-feu** accède à toutes les informations de configuration du pare-feu connexes à partir de la base de données et les rend disponibles pour utilisation par l'action suivante.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variables d'entrée

Variable	Description
firewallSysid [chaîne]	ID système du pare-feu. Cette variable d'entrée est obligatoire.
typeOfValueToBeBlocked [chaîne]	Type de valeur à bloquer sur le pare-feu : IP, URL ou Domaine.
firewallIPAddress [chaîne]	Adresse IP du pare-feu.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes. La sortie se compose de données provenant de la configuration du pare-feu ainsi que de données générées dynamiquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
ipEDLName [chaîne]	Nom de la liste dynamique externe pour les adresses IP.
urlEDLName [chaîne]	Nom de la liste dynamique externe pour les URL.
domainEDLName [chaîne]	Nom de la liste dynamique externe des domaines.
firewallVersionSysId [chaîne]	ID système pour la version du pare-feu.
refreshEDLCommand [chaîne]	Commande à utiliser pour actualiser l'EDL à partir de la source.
ShowEDLDetailsCommand [chaîne]	Commande à utiliser pour obtenir les détails de l'EDL.
état [booléen]	Vrai indique la réussite. Faux indique un échec.
Erreur [chaîne]	L'erreur, le cas échéant, qui s'est produite dans l'action.
point de terminaison [chiffré]	Point de terminaison chiffré à partir de la base de données.

Pare-feu Palo Alto : action d'obtention du journal

L'action Pare-feu Palo Alto : obtenir le flux de journal planifie une requête sur le pare-feu pour récupérer les journaux et renvoie un JobID utilisé pour récupérer les données du journal.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variables d'entrée

Variable	Description
FirewallIpAddress [chaîne]	Adresse IP du pare-feu. Cette variable d'entrée est obligatoire.
FirewallApiKey [chaîne]	Clé d'accès API du pare-feu. Cette variable d'entrée est obligatoire.
FirewallLogType [chaîne]	Type de données de journal à récupérer (défini sur menace). Cette variable d'entrée est obligatoire.
FirewallLogFilterQuery [chaîne]	Requête à exécuter pour rechercher des journaux sur le pare-feu. Cette variable d'entrée est obligatoire.
LogDirection [chaîne]	Spécifie si les journaux sont affichés dans l'ordre du plus ancien (en arrière) ou du plus récent en premier (en avant).
LogNumber [chaîne]	Spécifie le nombre de journaux à récupérer.
LogSkipCount [chaîne]	Spécifie le nombre de journaux à ignorer lors de la récupération d'un journal.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes. La sortie se compose de données provenant de la configuration du pare-feu ainsi que de données générées dynamiquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
QueuedJobID [chaîne]	ID de la tâche renvoyé par le pare-feu.
JobScheduled [chaîne]	Spécifie (réussite ou échec) si la tâche a été envoyée au pare-feu.
Erreur [chaîne]	Toute erreur renvoyée.

Pare-feu Palo Alto : action sur les données de la tâche

Une fois que l'action **Palo Alto Firewall : Obtenir le journal** a mis en file d'attente la requête de recherche vers le pare-feu et que la tâche s'exécute, l'action **Palo Alto Firewall : action** Données de tâche récupère les données du journal des menaces à partir du pare-feu.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action. Tous les champs d'entrée sont obligatoires.

Variables d'entrée

Variable	Description
FirewallIpAddress [chaîne]	Adresse IP du pare-feu.
FirewallApiKey [chaîne]	Clé d'accès API du pare-feu.
JobID [chaîne]	ID de la tâche en file d'attente.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes. La sortie se compose de données provenant de la configuration du pare-feu ainsi que de données générées dynamiquement.

Variables de sortie

Variable	Description
commandStatus [chaîne]	Spécifie (réussite ou échec) si les données ont été récupérées à partir du pare-feu.
JobData [chaîne]	Les données collectées à partir du pare-feu.
Erreur [chaîne]	Toute erreur renvoyée.

Intégration Palo Alto Networks - WildFire

Palo Alto Networks - WildFire est une application basée sur le cloud qui interagit avec le pare-feu de votre système.

Traduction automatique

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

Activer Palo Alto Networks - WildFire

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

Utiliser

Obtenir le flux d’enrichissement des données WildFire

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l’écriture d’intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l’intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Activer Palo Alto Networks - WildFire

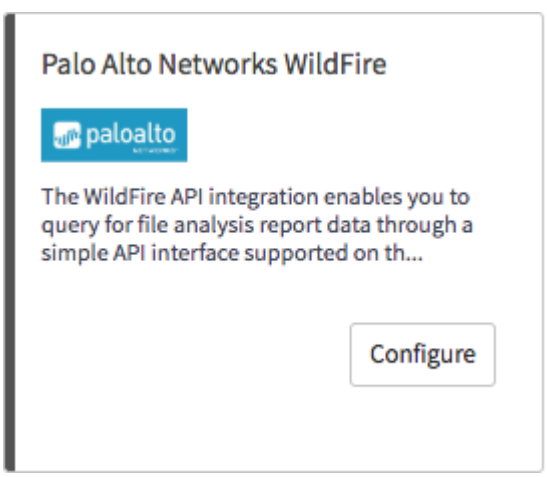
Avant de pouvoir utiliser l’intégration Security Operations Palo Alto Networks - WildFire, vous devez télécharger l’intégration à partir du ServiceNow Store.

Avant de commencer

Rôle requis : admin

Procédure

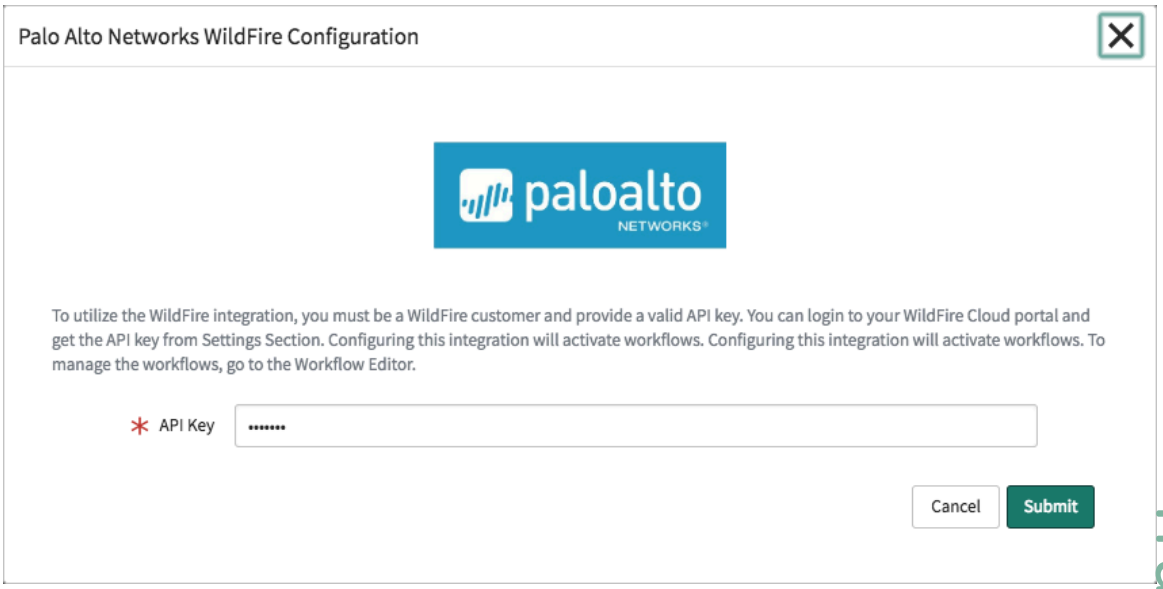
1. Télécharger l’intégration à partir de ServiceNow Store.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d’une série de cartes.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la Carbon Black carte, cliquez sur **Configurer**.



4. Entrez la clé API, puis cliquez sur **Soumettre**.
   La carte de configuration d'intégration s'affiche.
5. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Obtenir le flux d'enrichissement des données WildFire

Lorsque le flux **Security Operations Palo Alto Networks - Get WildFire Data Enrichment** est exécuté, un fichier de hachage est téléchargé dans WildFire. Les données sont enrichies et les rapports sont téléchargés vers l'instance pour faciliter le traitement des attaques potentielles de logiciels malveillants.

Avant de commencer

Rôle requis : sn_si.analyst

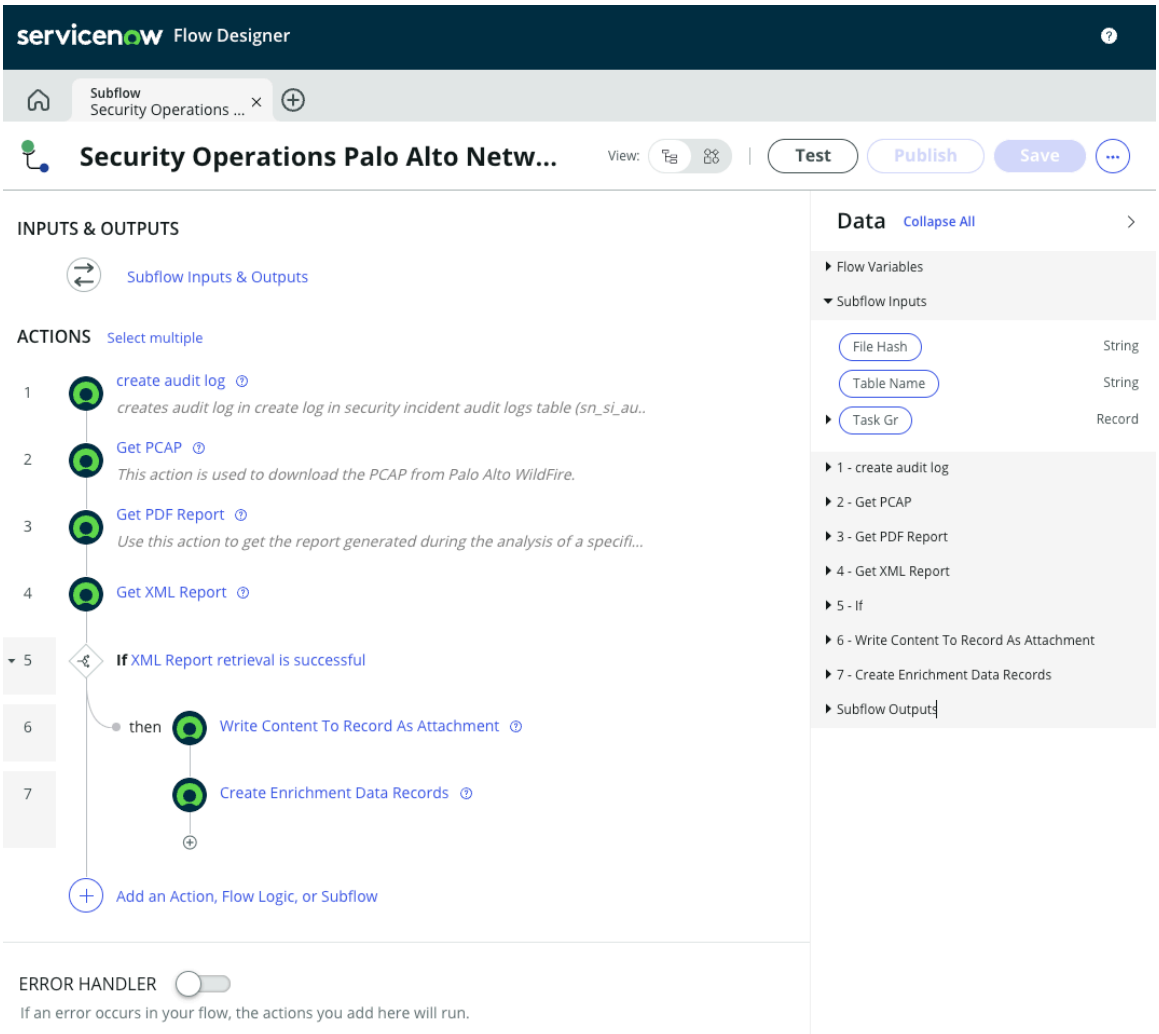
Pourquoi et quand exécuter cette tâche

Le flux **Security Operations Palo Alto Networks - Get WildFire Data Enrichment** est exécuté lorsqu'un incident de sécurité est créé à partir d'une alerte reçue de l'application Palo Alto Network Firewall. Un hachage de programme malveillant à partir de la notification par e-mail reçue du pare-feu est saisi dans l'onglet **IoC** de l'incident de sécurité et l'enregistrement est mis à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Operations Palo Alto Networks : obtenir le flux d'enrichissement des données WildFire



Procédure

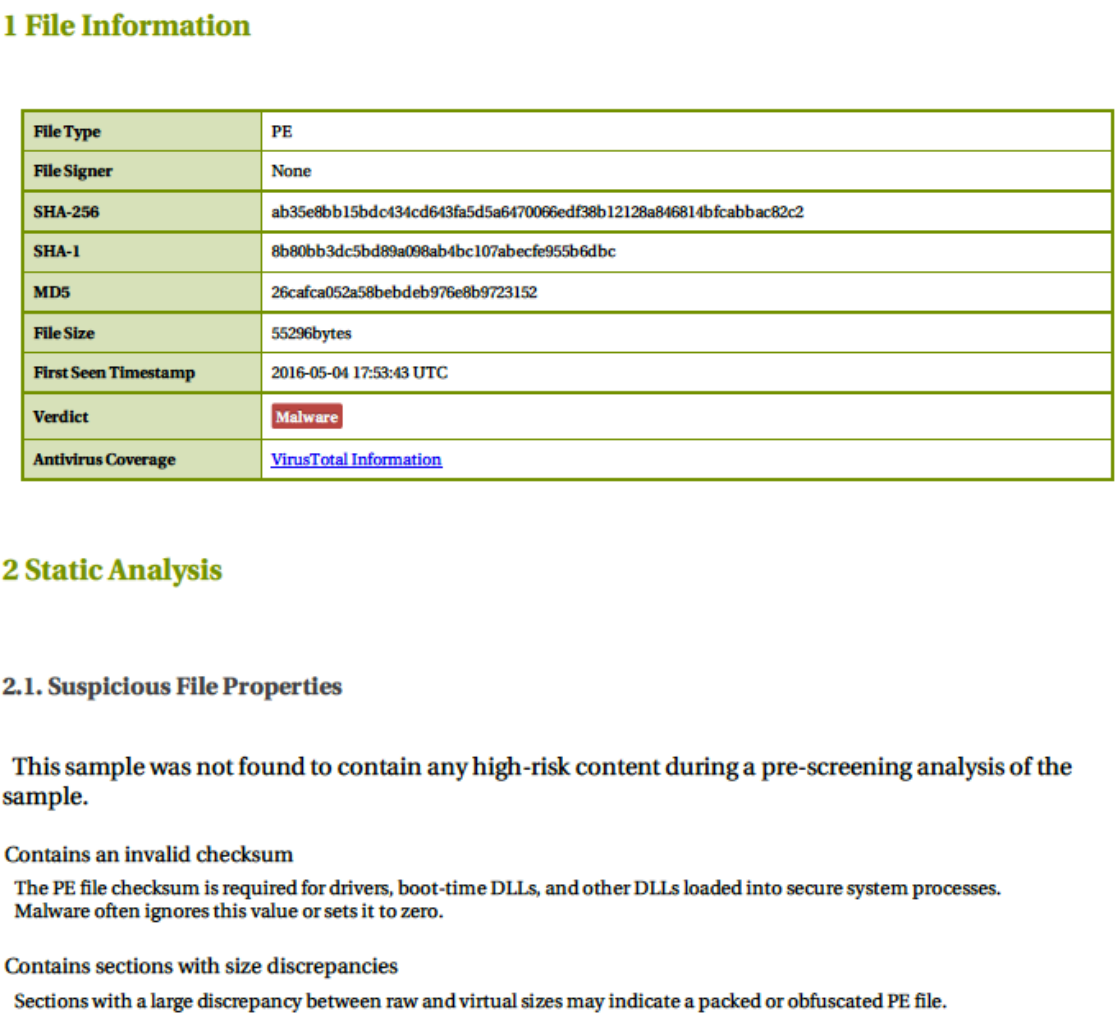
1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents ouverts**.
2. En fonction de la notification par e-mail reçue du pare-feu, localisez et ouvrez l'incident de sécurité qui a été créé.
3. Cliquez sur **l'onglet Indicateurs de compromission** et renseignez le **hachage** de programme malveillant avec le hachage que vous avez reçu dans l'alerte.
4. Cliquez sur **Mettre à jour**.
   Le flux entraîne le chargement du fichier de hachage vers WildFire où les données sont enrichies. Les rapports aux formats PDF et XML sont joints à l'enregistrement (incident de sécurité ou IoC) dans votre instance pour faciliter le traitement des attaques potentielles de programmes malveillants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si les données enrichies incluent des informations de capture de paquets, les informations PCAP sont également téléchargées. Les données PCAP capturent les actions effectuées par le fichier. Par exemple, il peut signaler les serveurs contactés par le fichier. Pour afficher les fichiers PCAP, vous avez besoin d'un analyseur de paquets, tel que Wireshark .

Exemple de PDF généré par Wildfire



1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

WildFire : obtenir l'action PCAP

L'action **WildFire : Obtenir le flux PCAP** récupère les informations de capture de paquets (PCAP) générées lors de l'analyse d'un hachage de fichier spécifié sur WildFire. Le résultat de cette action est attaché à un enregistrement spécifique tel qu'identifié par le **TableName** et le **RecordId**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variables d'entrée

Variable	Description
FileSHA256Hash [chaîne]	Hachage du fichier reçu de l'application Palo Alto Network Firewall.
Nom de table [chaîne]	La table affectée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée (suite)

Variable	Description
RecordId [chaîne]	L'incident de sécurité ou l'IoC en cours de mise à jour.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
commandStatus [booléen]	Vrai si un résultat est obtenu et joint avec succès.
errorMessage	L'erreur, le cas échéant, qui s'est produite dans l'action.

WildFire : action de rapport PDF

L'action **de flux WildFire : obtenir un rapport PDF** obtient le rapport généré lors de l'analyse d'un hachage de fichier spécifié sur WildFire au format PDF. Le résultat de cette action est attaché à un enregistrement spécifique tel qu'identifié par le **TableName** et le **RecordId**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variables d'entrée

Variable	Description
Nom de table [chaîne]	La table affectée.
FileSHA256Hash [chaîne]	Hachage du fichier reçu de l'application Palo Alto Network Firewall.
RecordId [chaîne]	L'incident de sécurité ou l'IoC en cours de mise à jour.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
commandStatus [booléen]	Vrai si un résultat est obtenu et joint avec succès.
errorMessage	L'erreur, le cas échéant, qui s'est produite dans l'action.

WildFire : action de rapport XML d'obtention

L'action **de flux WildFire : obtenir un rapport XML** obtient le rapport généré lors de l'analyse d'un hachage de fichier spécifié sur WildFire au format XML. Le résultat de cette action est attaché à un enregistrement spécifique tel qu'identifié par le **TableName** et le **RecordId**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d’entrée déterminent le comportement initial de l’action.

Variables d'entrée

Variable	Description
Nom de table [chaîne]	La table affectée.
FileSHA256Hash [chaîne]	Hachage du fichier reçu de l’application Palo Alto Network Firewall.
RecordId [chaîne]	L’incident de sécurité ou l’IoC en cours de mise à jour.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
commandStatus [booléen]	Vrai si un résultat est obtenu et joint avec succès.
errorMessage	L’erreur, le cas échéant, qui s’est produite dans l’action.

Intégration Palo Alto Networks - Next-Generation Firewall

Une fois installé et configuré, l’analyste d’incident de sécurité utilise cette intégration pour bloquer les adresses IP, les URL et les domaines malveillants à l’aide des options de liste dynamique externe (EDL) avec les ServiceNow Réponse aux incidents de sécurité produits (SIR). L’analyste des incidents de sécurité crée des entrées pour une EDL à partir d’observables déterminés comme malveillants lors ServiceNow SIR d’incidents de sécurité.

Une EDL est un fichier texte hébergé sur un serveur Web externe. Pour cette intégration, ce serveur Web est votre ServiceNow AI Platform instance, qui vous permet d’importer Palo Alto Networks - Next-Generation Firewall des objets inclus dans la liste, les adresses IP, les URL et les domaines, et d’appliquer la politique.

Pour appliquer la politique sur les entrées EDL, la liste est référencée dans une règle ou un profil de politique. Au fur et à mesure que les entrées EDL sont modifiées, le pare-feu importe dynamiquement la liste à l’intervalle configuré et applique la politique sans changement de configuration ni validation sur le pare-feu. Pour cette intégration, ServiceNow AI Platform a créé une table contenant les entrées EDL qui sont récupérées par les personnes autorisées Palo Alto Networks - Next-Generation Firewall aux intervalles de récupération configurés.

L’intégration comprend les fonctionnalités suivantes :

- Flexibilité de création de plusieurs EDL qui s’appliquent à différentes politiques de pare-feu, de refus ou d’autorisation.
- Rapports détaillés sur les types de sites bloqués (hameçonnage, programmes malveillants et sites sur liste d’autorisation).
- Balisage des incidents de sécurité avec des entrées EDL par type d’observable ServiceNow AI Platform (URL, domaine, adresse IP).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurer les périodes d'expiration des EDL pour conserver la taille de leur liste en faisant automatiquement expirer ou en supprimant les entrées les plus anciennes.
- Recherche, suppression ou migration d'entrées EDL entre des listes EDL.
- Liaison des entrées EDL aux enregistrements d'observables et aux incidents de sécurité qui incluent des résultats de Threat Intelligence et des détails sur les raisons pour lesquelles une entrée est bloquée.

L'intégration nécessite que les modules d'extension (com.snc.security_incident) et (com.snc.secops.orchestration) du Réponse aux incidents de sécurité produit soient activés.

Cette intégration ne prend en charge Palo Alto Networks que (PAN-OS 8.x). Les versions antérieures ne sont pas prises en charge.

Cette intégration est compatible avec les versions Kingston, Londres, Madrid et New York du ServiceNow AI Platform®.

Remarque : Les rubriques suivantes sont numérotées. Pour une installation, une configuration et une vérification fluides des résultats attendus, suivez les rubriques dans l'ordre dans lequel elles sont présentées.

Créer un profil de certificat pour le Palo Alto Networks - Next-Generation Firewall

L'intégration nécessite un profil de certificat pour valider et authentifier la connexion sécurisée entre le ServiceNow AI Platform® serveur et le Palo Alto Networks - Next-Generation Firewall serveur.

Rôle requis : Palo Alto Networks - Next-Generation Firewall administrateur.

A Palo Alto Networks - Next-Generation Firewall s'authentifie à une ServiceNow AI Platform® instance, récupère les entrées EDL à partir de la table de base de données et intègre les entrées dans les règles de politique de pare-feu correspondantes. Cette récupération nécessite le rôle de compte utilisateur de l'API dans l'instance ServiceNow AI Platform® , qui est utilisé par l'administrateur du pare-feu PAN pour accéder à l'API ServiceNow AI Platform® .

Suivez les étapes ci-dessous pour télécharger les DigiCertificates et configurer le profil de certificat.

1. Téléchargez le certificat DigiCert ou Entrust CA Gateway en fonction du cas d'utilisation. Pour plus d'informations, reportez-vous à l'article KB1702083 dans le Now Support Base de connaissances.
2. Configurez le profil de certificat. Pour plus d'informations, consultez la documentation de Palo Alto Networks .

Information associée

« Configurer un profil de certificat » dans le Guide de l'administrateur PAN-OS 10.0

Configurer et installer Palo Alto Networks - Next-Generation Firewall

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches de configuration sont nécessaires pour une installation sans faille.

Avant de commencer

Rôle requis : (admin)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
Vérifiez que les rôles requis ServiceNow AI Platform et Réponse aux incidents de sécurité sont affectés.	Les rôles suivants sont requis : • L’administrateur système (administrateur) installe l’application et affecte le rôle d’administrateur d’incident de sécurité (sn_si.admin). • L’administrateur d’incident de sécurité (sn_si.admin) supervise la configuration et crée, active et supprime des EDL. Ce rôle affecte également le rôle sn_si.analyst. • L'(admin) attribue le rôle de compte API (sn_sec_panfw.api_account_access), qui est utilisé exclusivement pour saisir les ServiceNow AI Platform® informations d’identification requises pour l’authentification Palo Alto Networks afin que les pare-feu puissent récupérer les EDL à partir ServiceNow AI Platform® du . • (sn_si.analyst) ou analyste du Centre des opérations de sécurité (SOC), crée des entrées EDL et travaille sur les incidents de sécurité.
Vérifiez que vous utilisez Palo Alto Networks - Next-Generation Firewall la version 9.x et 10.x.	Cette intégration ne prend en charge Palo Alto Networks - Next-Generation Firewall que OS 9.0 et versions ultérieures.
Configurez tous les profils EDL, les règles de politique de sécurité et les profils de certificat comme Palo Alto Networks recommandé dans la Palo Alto Networks documentation.	Reportez-vous à la documentation générale et aux Palo Alto Networks exigences sur le site Web de la documentation de Paloalto Networks .
Vérifiez que vous avez téléchargé et configuré le certificat d’autorité racine DigiCert.	L’intégration nécessite ce certificat pour valider et authentifier la connexion sécurisée entre le ServiceNow AI Platform serveur et le Palo Alto Networks - Next-Generation Firewall serveur. Pour plus d’informations sur la configuration du certificat, consultez « Configurer un profil de certificat » dans le Guide de l’administrateur PAN-OS 10.0 . Pour le téléchargement, consultez Créer un profil de certificat pour le Palo Alto Networks - Next-Generation Firewallet Certificats DigiCert Trusted Root Authority .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l’intégration sont installées et activées avant d’installer l’application pour l’intégration.	Conditions requises pour la version Madrid et ultérieures Pour la version Madrid et les versions familiales ultérieures, le module d’extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d’extension installe automatiquement toutes les dépendances requises pour prendre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Orchestration du support de sécurité Pour en savoir plus sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.
Si votre organisation dispose ServiceNow AI Platform® de processus de gestion des changements et d'approbation pour la suppression d'e-mails, vérifiez que l'option d'envoi/réception d'e-mails est activée.	Pour vérifier que l'option d'envoi/réception d'e-mail est activée dans votre ServiceNow AI Platform® instance, accédez à **Propriétés d'e-mail** > **Administration** > **Propriétés d'e-mail**. Dans Configuration des e-mails sortants, vérifiez que les **options Envoi etRéception d'e-mail** sont sélectionnées.

Procédure

Si vous n'avez pas installé l'application pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes d'installation.

Créer le rôle du compte d'API pour Palo Alto Networks - Next-Generation Firewall

Un rôle de compte API est requis dans votre ServiceNow AI Platform® instance pour cette intégration. Le nom d'utilisateur et le mot de passe associés à ce compte sont créés dans le ServiceNow AI Platform® et saisis afin Palo Alto Networks qu'ils s'authentifient Palo Alto Networks - Next-Generation Firewall lors de la ServiceNow AI Platform® récupération des entrées EDL.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

L'administrateur ServiceNow AI Platform® crée un rôle de compte API (sn_sec_panfw.api_account_access). Ce compte est utilisé exclusivement pour saisir les informations d'identification requises pour l'authentification Palo Alto Networks afin que les pare-feu puissent récupérer les EDL à partir ServiceNow AI Platform® du . Ce

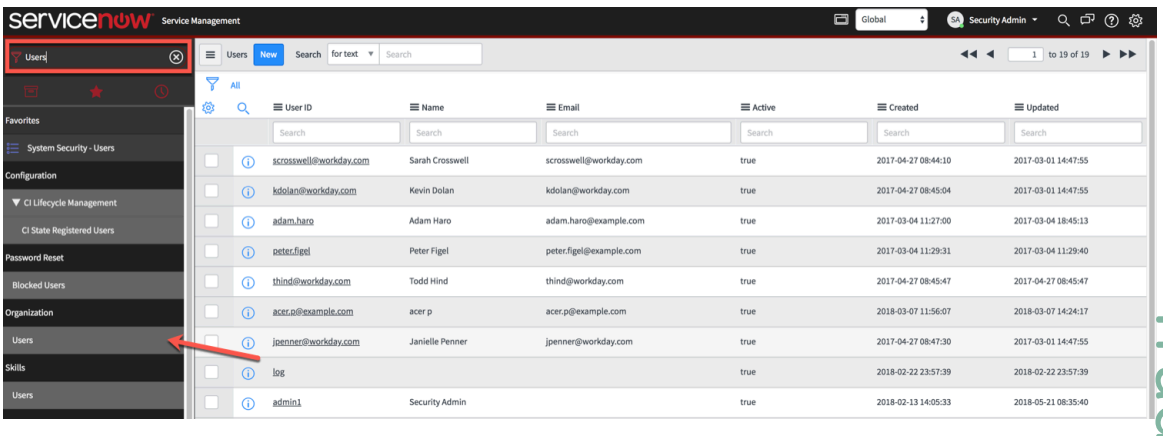
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

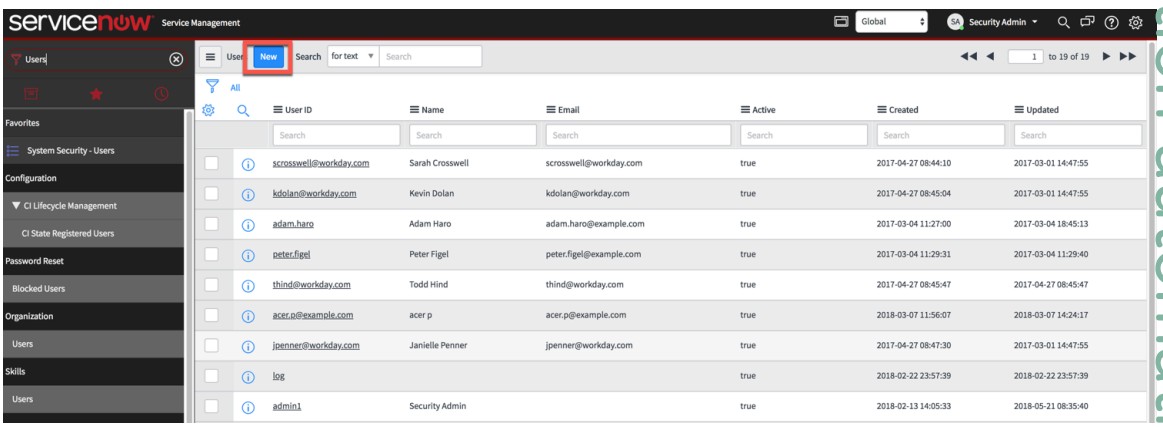
compte est un compte d’utilisateur d’API distinct et unique dans l’instance ServiceNow AI Platform® et affecté à l’administrateur Palo Alto Networks - Next-Generation Firewall .

Procédure

1. Accédez à la **Tous** > **Organisation** > **Utilisateurs**.
2. Cliquez sur le module **Utilisateurs** .



3. Cliquez sur **Nouveau** dans la liste Utilisateurs qui s’affiche.



Un nouveau formulaire d’utilisateur s’affiche.

4. Remplissez le formulaire.

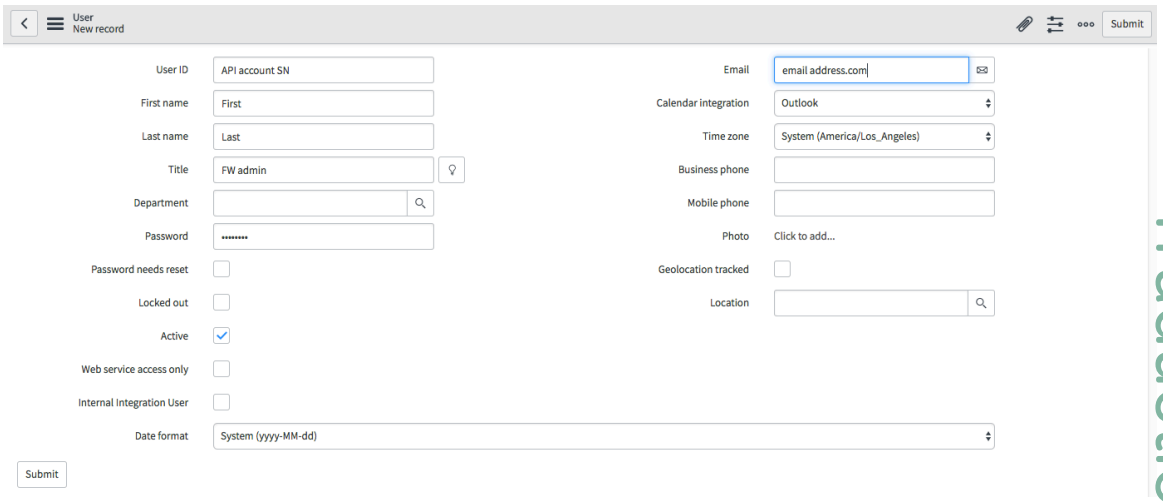
Remarque : Les valeurs d’ID d’utilisateur, de titre et d’adresse e-mail indiquées dans la table et la figure suivantes sont des exemples de valeurs.

Champ	Description
ID d'utilisateur	ID d’utilisateur unique pour le rôle dans votre ServiceNow AI Platform® instance. Cet ID utilisateur est entré dans le champ **Nom d’utilisateur** de la section **Authentification client** de la boîte de dialogue Listes dynamiques externes du Palo Alto Networks site. Par exemple, le compte API SN.
Prénom	Personne que vous affectez.
Nom de famille	Personne que vous affectez.

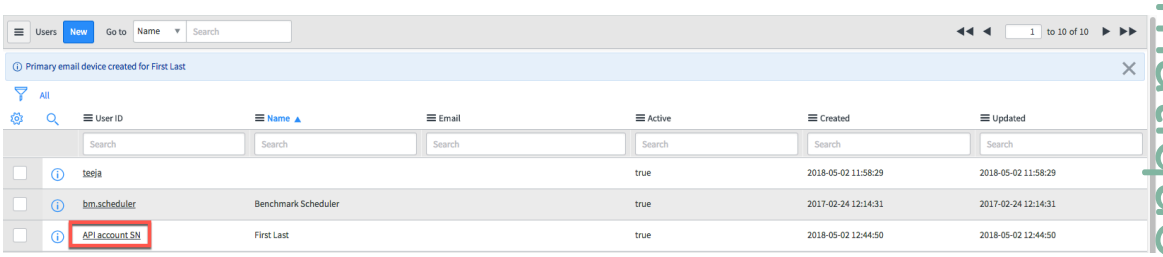
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Titre	Fonction, par exemple, `Administrateur FW`.
Mot de passe	Mot de passe unique créé pour ce rôle. Ce mot de passe est entré dans le champ **Mot de passe** de la section **Authentification client** de la boîte de dialogue Listes dynamiques externes du Palo Alto Networks site.
E-mail	Adresse e-mail unique.



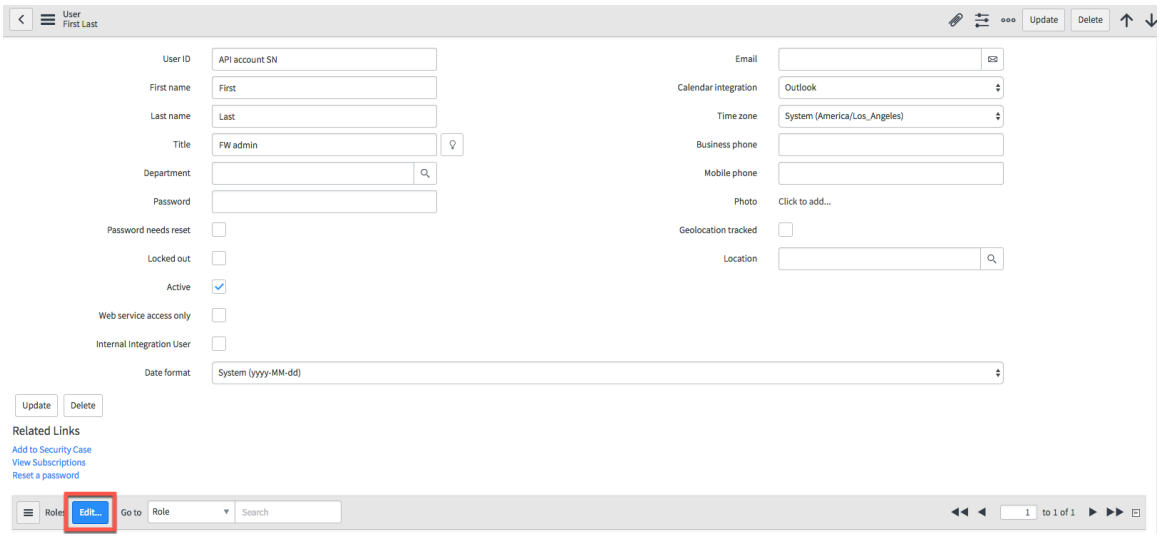
5. Cliquez sur **Envoyer**.
   Une fois le rôle soumis, vous pouvez l'affecter.
6. Dans la liste des utilisateurs dans la colonne **ID d'utilisateur** , cliquez sur le nom de l'ID d'utilisateur que vous avez saisi, le `compte API SN`, par exemple.



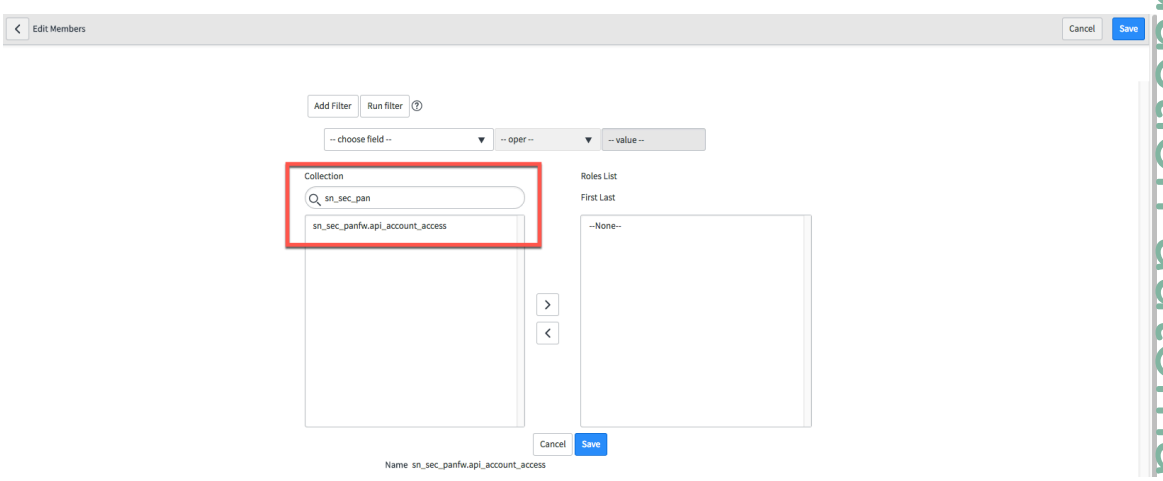
7. Dans l'enregistrement ouvert dans la section Rôles, cliquez sur **Modifier**.

Traduction automatique

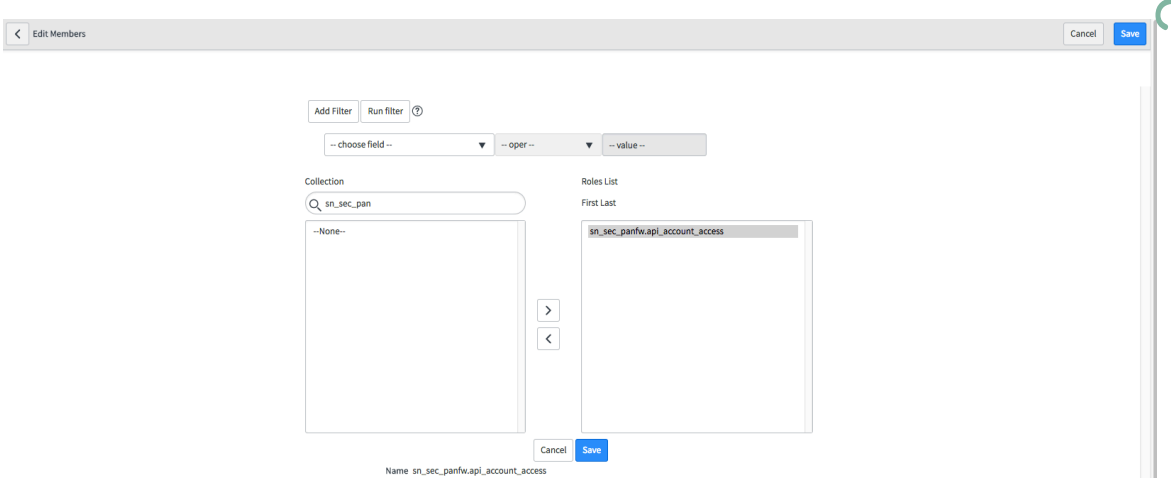
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Dans le formulaire **Modifier les membres**qui s'affiche, saisissez `sn_sec_panfw.api_account_access` dans le champ **Collecte** .
   Sous le champ **Collecte** , le rôle s'affiche dans la colonne.



9. Dans la colonne **Collection** , sélectionnez puis déplacez `sn_sec_panfw.api_account_access` vers la **liste Rôles**.

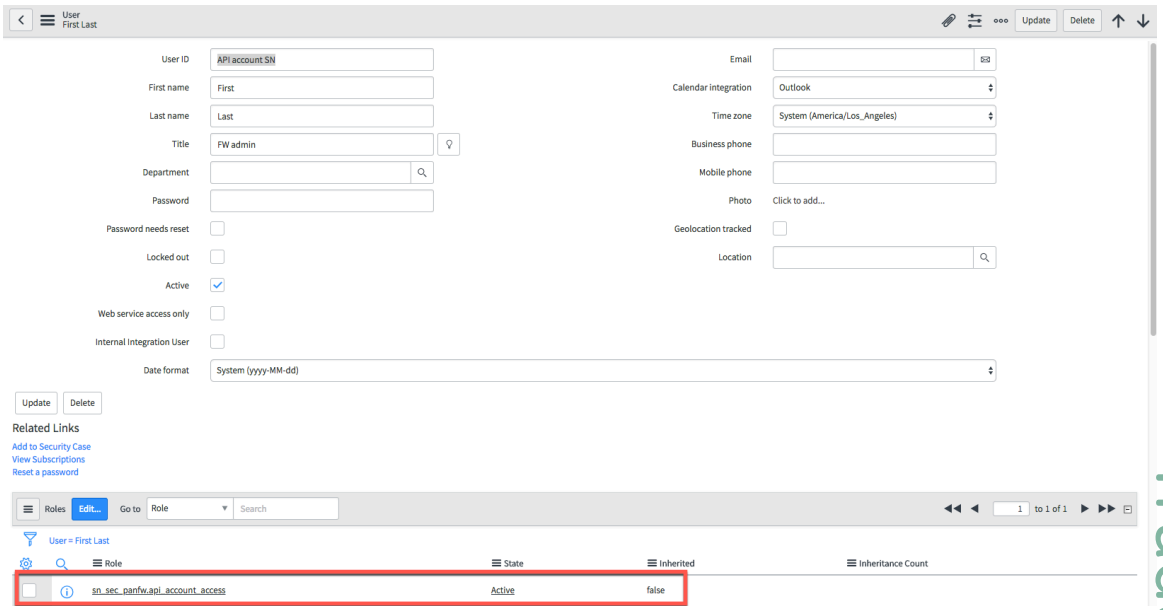


10. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Naviguez jusqu'aux **utilisateurs** et, dans la colonne **Utilisateur** de la liste, cliquez sur le nom d'ID que vous avez créé pour le rôle (compte API SN).



L'enregistrement utilisateur s'affiche. Cet enregistrement vérifie que le compte d'utilisateur a été affecté. **L'État** est actif et le rôle n'est pas hérité.

Listes dynamiques externes prises en charge pour Palo Alto Networks - Next-Generation Firewall

L'intégration ServiceNow Palo Alto Networks - Next-Generation Firewall prend en charge les listes dynamiques externes (EDL) qui acceptent les observables d'adresse IP, d'URL et de domaine.

EDL et observables pris en charge

Une *liste dynamique externe* est un fichier texte hébergé sur un *serveur Web* externe, qui est l'instance ServiceNow AI Platform pour cette intégration. Ils Palo Alto Networks - Next-Generation Firewall peuvent ensuite importer des objets (adresses IP, URL, domaines) inclus dans la liste et appliquer la politique. Pour appliquer la politique sur les entrées EDL, la liste est référencée dans une règle ou un profil de politique.

Cette intégration prend en charge trois types d'EDL :

- IP (cela inclut une adresse IP unique, ainsi que des blocs CIDR (plages) d'adresses).
- URL
- Domaine

Le tableau suivant répertorie les descriptions des observables pris en charge par cette intégration et des exemples de formats pour chaque type.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Observables pris en charge et exemples de formats

Observable	Exemples de formats	Description
Adresse IP	• 95.153.103.54 (IPv4) • (IPv6) : 2001:00B8:130F :FE03:0000:09C0:080F:130B	Représente une adresse d'interface unique et distincte. L'intégration prend en charge les formats IPv4, IPv6 et CIDR. La prise en charge des observables d'adresse IP inclut les plages CIDR (Classless Inter-Domain Routing), par exemple, 95.153.100.0/22. Remarque : un message d'erreur s'affiche lorsque vous essayez de joindre une seule adresse IP à une EDL que vous avez déjà bloquée dans le cadre d'une plage CIDR. Par exemple, l'adresse unique 95.153.103.54 fait partie de la plage CIDR représentée par 95.153.100.0/22 (95.153.100.0-95.153.103.255).
URL	• www.example.com • www.example.com/article.html • example.com • *.example.com	Les caractères génériques sont pris en charge. Le ServiceNow AI Platform reformatage des entrées d'URL pour se Palo Alto Networks conformer aux exigences du format EDL.
Domaine	• www.example.com • example.com • mail.example.com	Les caractères génériques ne sont pas pris en charge.

Pour plus d'informations sur les directives de formatage et les EDL, consultez « Directives de formatage pour une liste dynamique externe » dans le Guide de l'administrateur PAN-OS 10.0 sur le Palo Alto Networks site Web.

Créer une EDL pour le pare-feu de nouvelle génération Palo Alto Networks

Créez une liste dynamique externe (EDL) dans votre ServiceNow AI Platform instance. Une fois approuvées et activées, vous pouvez créer des entrées pour les EDL à partir d'observables identifiés comme malveillants sur ServiceNow AI Platform Réponse aux incidents de sécurité des incidents (SIR) et demander l'approbation pour les bloquer.

Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Créez l'EDL sur votre ServiceNow AI Platform instance afin que le pare-feu puisse importer des objets (adresses IP, URL, domaines) inclus dans la liste et appliquer la politique. Pour appliquer la politique sur les entrées EDL, la liste est référencée dans une règle ou un profil de politique.

Les chiffres de la section suivante sont affichés avec **les formulaires à onglets** effacés dans Paramètres système. Pour plus d'informations sur la sélection et l'effacement des formulaires à onglets, reportez-vous à la section « Afficher les formulaires à onglets » dans Configurer la mise en page du formulaire .

Procédure

1. Une fois l'installation de l'application terminée, accédez à **Intégrations** > **Configurations d'intégration**.
2. Localisez la Palo Alto Networks - Next-Generation Firewall tuile et cliquez sur **Configurer**.



3. Cliquez sur **Créer une nouvelle liste EDL**.



4. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Palo Alto Networks Formulaire de liste dynamique externe de pare-feu

Champ	Description
Nom	Palo Alto Networks Nom de la liste dynamique du pare-feu. Incluez le type d'observable (URL, adresse IP, domaine) dans ce champ afin que l'analyste de sécurité puisse facilement reconnaître l'intention de l'EDL par son nom. Le nom doit également indiquer clairement à quelle stratégie de pare-feu ces objets EDL sont mappés. Voici quelques exemples de noms EDL : IP de programme malveillant sortant ou URL d'hameçonnage sortant.
Actifs	Cette case est décochée par défaut pour indiquer que l'EDL est inactive. Lorsqu'elle est inactive, l'EDL ne peut pas recevoir d'entrées supplémentaires. Lorsque la case est cochée, l'EDL est activée et disponible pour les entrées EDL.
Balise d'affichage	La case à cocher est sélectionnée par défaut pour baliser automatiquement l'observable et l'enregistrement d'incident de sécurité associé si l'observable est bloqué sur une EDL. Lorsque cette option est sélectionnée, les champs Type de balise et Balise EDL pour les observables sont disponibles sur le formulaire. **Remarque :** Un nom de balise est créé par défaut à partir de la valeur que vous entrez dans le champ **Nom** avec un préfixe *EDL*, par exemple, EDL-Malware OutBound IP. Vous pouvez modifier le nom et la couleur de la balise. Voir : (Facultatif) Modifier le nom de la balise de sécurité pour Palo Alto Networks - Next-Generation Firewall. Le nom de la balise est affiché dans le champ Balise EDL pour les observables une fois que l'EDL est enregistrée. Lorsque la case est décochée, aucune balise n'est créée et les champs Type de balise et Balise EDL pour les observables ne sont pas disponibles sur le formulaire.
Type d'observable	Sélectionnez un type d'observable que cette EDL accepte dans la liste de choix : adresse IP (y compris CIDR), URL ou domaine.
Type de balise	Balises disponibles dans la liste de choix.

Traduction automatique

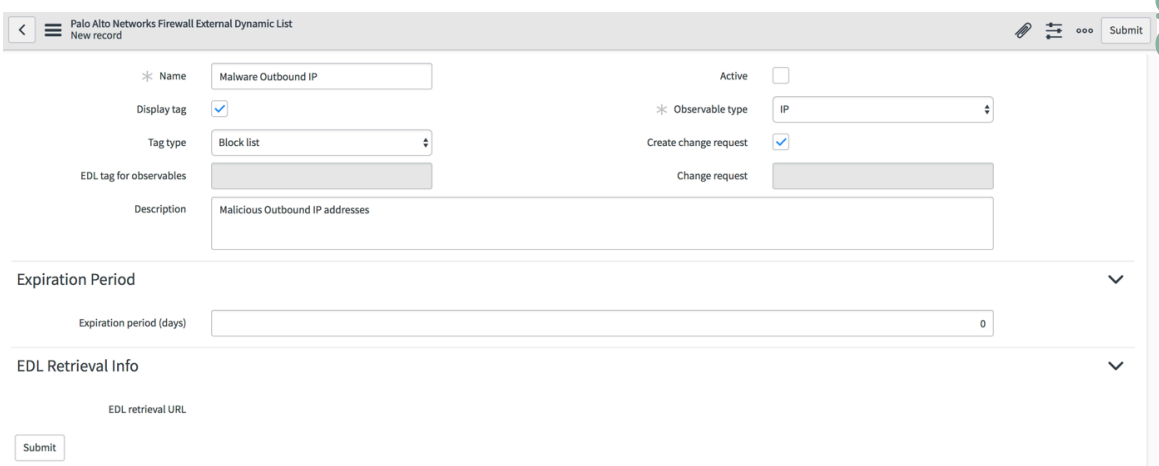
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Une liste de blocs est une liste d'observables Palo Alto Networks - Next-Generation Firewall que vous souhaitez bloquer. Une liste d'autorisation est une liste d'observables Palo Alto Networks - Next-Generation Firewall que vous souhaitez autoriser. Par défaut, la couleur de la balise de la liste de blocs est noire et la couleur de la balise de la liste d'autorisation est grise. Vous pouvez changer la couleur. Voir : (Facultatif) Modifier le nom de la balise de sécurité pour Palo Alto Networks - Next-Generation Firewall.
Création d'une demande de changement	Cette case à cocher est sélectionnée par défaut pour créer automatiquement une demande de changement et des tâches de changement dans votre ServiceNow AI Platform instance, qui sont jointes à l'enregistrement EDL. La demande de changement est utilisée pour configurer l'URL de récupération de liste des EDL dans le Palo Alto Networks - Next-Generation Firewall serveur. Cette option est recommandée si votre administrateur de pare-feu utilise également le pour modifier la politique ou les règles du ServiceNow AI Platform pare-feu. Si vous créez une demande, une fois qu'elle est fermée, la liste EDL est automatiquement activée. Décochez la case pour activer manuellement l'EDL après avoir reçu une notification par e-mail de l'administrateur du pare-feu indiquant que la configuration Palo Alto Networks est terminée. Lorsque la case Créer une demande de changement est décochée, le champ Demande de changement n'est pas disponible.
Balise d'EDL pour les observables	ce champ n'est affiché que si la case Afficher la balise est cochée. Le champ est automatiquement renseigné une fois l'EDL enregistrée avec une valeur par défaut du champ Nom. Pour plus d'informations sur la modification du nom et de la couleur de la balise par défaut, consultez (Facultatif)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Modifier le nom de la balise de sécurité pour Palo Alto Networks - Next-Generation Firewall
Demande de changement	Lorsque la case Créer une demande de changement est cochée, le numéro de la demande de changement s'affiche sur l'instance ServiceNow AI Platform une fois l'EDL enregistrée. Lorsque la case à cocher Créer une demande de changement est désactivée, ce champ n'apparaît pas.
Description	Description de la liste dynamique du pare-feu Palo Alto Networks. Le nom contient généralement les types de sites et d'observables que vous vous attendez à trouver sur cette EDL, et vous pouvez utiliser ce champ pour plus de détails.
Période d'expiration (jours)	Période d'expiration de l'EDL. 0 (valeur par défaut) indique que l'entrée EDL n'expire jamais. Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous saisissez. Vous pouvez entrer une valeur minimale de 1, mais il n'y a pas de valeur maximale. Par exemple, si vous saisissez 30 jours à 14h01 le 1er mai, l'EDL expirera à 14h01 le 31 mai. Toutes les entrées de cette EDL héritent alors de cette valeur par défaut, sauf si vous remplacez la valeur sur une base individuelle.

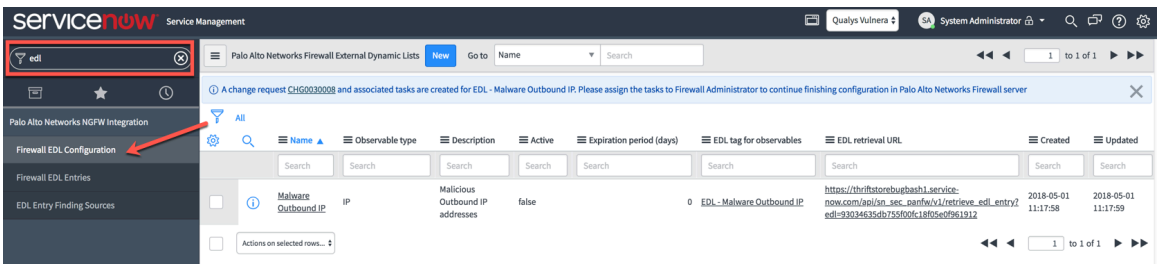


5. Cliquez sur **Envoyer**.

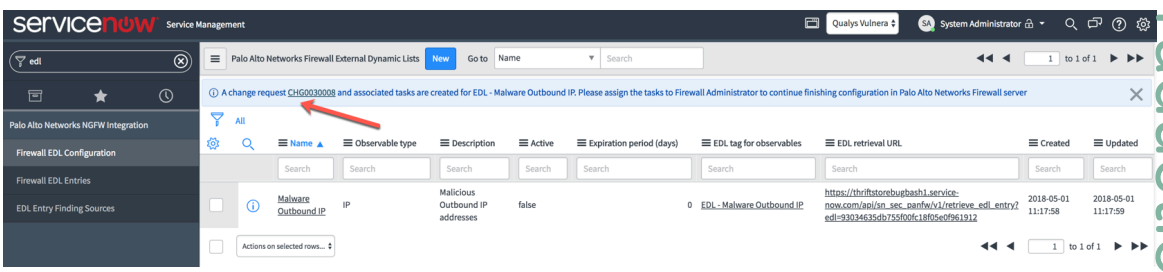
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

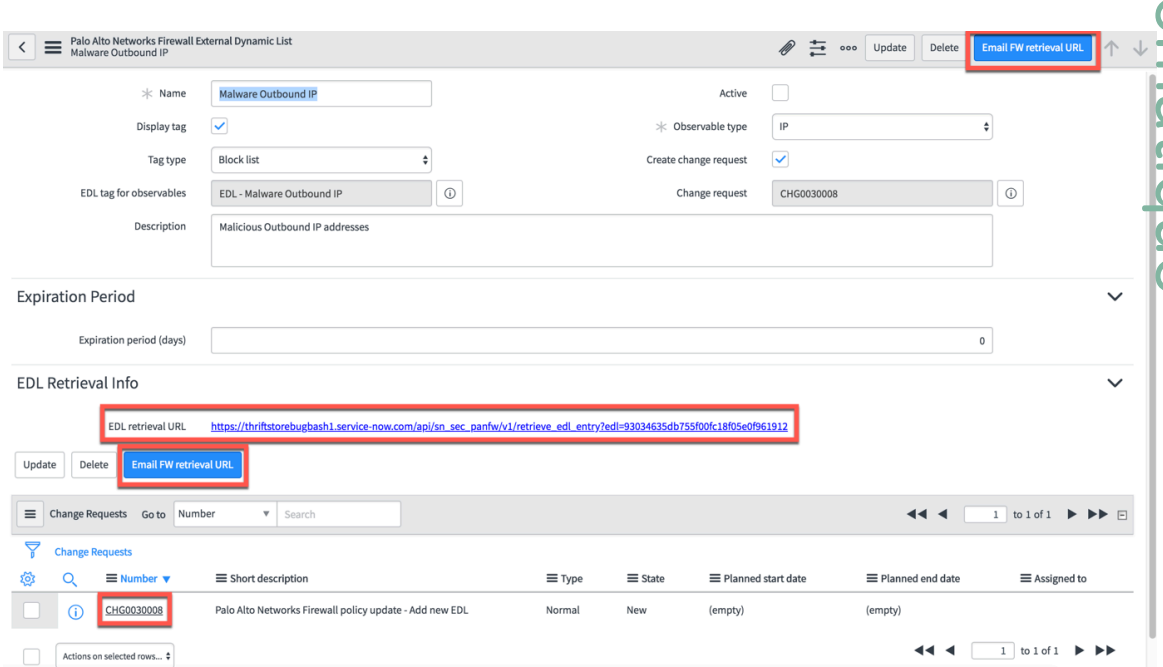
6. Si la liste des listes dynamiques externes du pare-feu Palo Alto Networks n'est pas affichée, accédez à **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu** et cliquez sur **Configuration de l'EDL du pare-feu**.



La nouvelle EDL s'affiche. L'état de l'EDL est toujours inactif (faux), ce qui signifie que l'EDL n'est pas disponible pour accepter des entrées. Si **la création** d'une demande de changement a été configurée, un message s'affiche indiquant qu'une demande de changement et des tâches ont été créées dans votre ServiceNow AI Platform instance.



7. Dans la colonne **Nom** , cliquez sur un élément pour ouvrir l'enregistrement.
L'enregistrement EDL s'affiche. Cet exemple montre une EDL IP sortante de programme malveillant. Les champs, options et liens suivants sont affichés dans le nouvel enregistrement après soumission et décrits dans le tableau suivant.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

URL de récupération et liens de demande de changement sur l'enregistrement EDL

Option	Description
Envoyer par e-mail l'URL de récupération de transfert	Envoie par e-mail un avis indiquant que le lien EDL est disponible pour configuration à l'administrateur du Palo Alto Networks pare-feu.
URL de récupération de l'EDL	Cette URL est placée dans le champ **Source** de la boîte de dialogue d'authentification des listes dynamiques externes de l'onglet **Créer une liste** sur le Palo Alto Networks site Web. Le lien URL que l'administrateur Palo Alto Networks de pare-feu utilise pour la configuration dans le Palo Alto Networks pare-feu est automatiquement généré et affiché. **Remarque :** Si vos paramètres système sont définis sur **Formulaires à onglets**, ce lien s'affiche dans l'onglet **Informations de récupération de l'EDL** au bas de l'enregistrement.
ServiceNow AI Platform Demande de changement	Un lien vers l'enregistrement de la demande de changement s'affiche dans la section Demandes de changement lorsqu'elle est configurée, et le numéro de la demande s'affiche dans le champ Demande de changement.
Mettre à jour	Modifiez les données et mettez à jour les champs modifiables.
Supprimer	Supprimez l'enregistrement.

8. Créez et ajoutez d'autres EDL selon vos besoins.
   Les EDL sont affichées dans la Palo Alto Networks liste Listes dynamiques externes.

Que faire ensuite

Activer une EDL manuellement ou avec une demande de ServiceNow AI Platform changement.

Activer un EDL

Une fois que la liste dynamique externe (EDL) a été créée dans Ur ServiceNow AI Platform® et que l'URL est disponible, l'administrateur Palo Alto Networks du pare-feu configure l'EDL dans le Palo Alto Networks - Next-Generation Firewall. L'URL de récupération est utilisée par l'administrateur du Palo Alto Networks pare-feu pour configurer l'EDL dans le Palo Alto Networks - Next-Generation Firewall serveur. Avant de pouvoir accepter des entrées EDL, l'EDL doit être configurée Palo Alto Networks et activée dans le ServiceNow AI Platform®.

Avant de commencer

Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

Une fois l'EDL configurée, en tant qu'administrateur d'incident de sécurité, vous pouvez l'activer manuellement ou, l'EDL est automatiquement activée à l'achèvement d'une ServiceNow AI Platform®

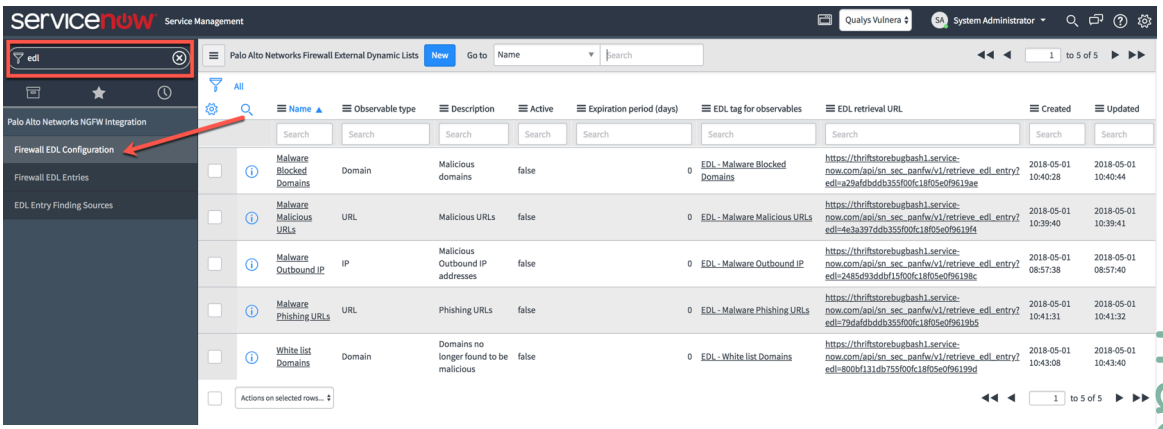
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

demande de changement. L'EDL doit être approuvée et passée de l'état inactif à l'état actif avant de pouvoir accepter des entrées EDL.

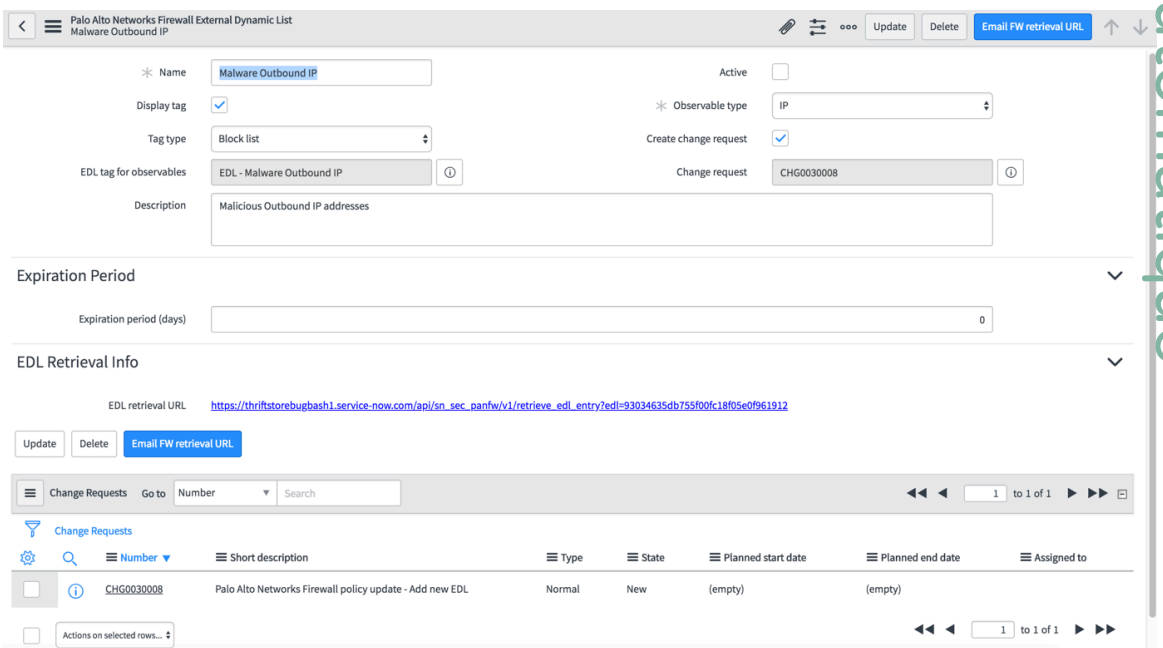
Procédure

1. Accédez à la **Tous** > **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu** et sélectionnez le module **Configuration de l'EDL du pare-feu** .



2. Dans la liste Palo Alto Networks Firewall Dynamic Lists qui s'affiche, sélectionnez votre nouvel EDL dans la colonne Nom.

3. Sur l'enregistrement qui s'affiche, notez les boutons **Envoyer par e-mail l'URL de récupération de transfert par e-mail** , le lien URL de récupération de l'EDL actif et, le cas échéant, la demande de ServiceNow AI Platform® changement dans la section Demandes de changement.
Assurez-vous que la case **Actif** est décochée.



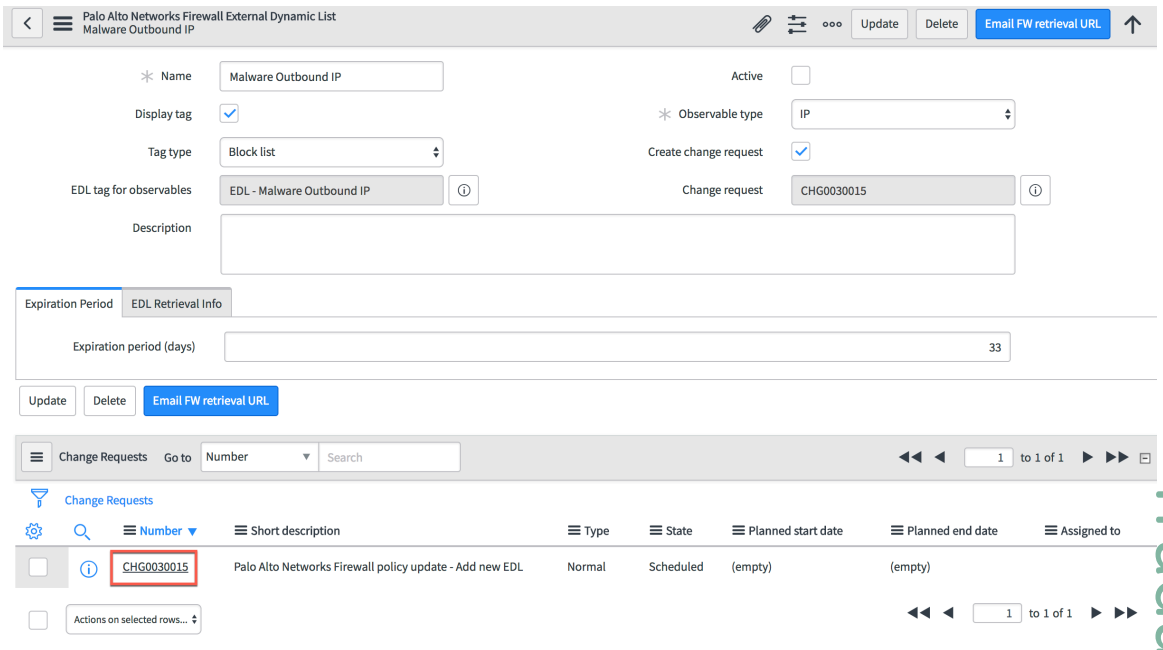
Remarque : Lorsque les **formulaires à onglets** sont effacés dans vos paramètres système, l'URL de récupération EDL apparaît dans la section **Informations de récupération EDL** , comme illustré dans la figure précédente.

La figure suivante montre les **informations de récupération EDL** affichées sous forme d'onglet avec **des formulaires à onglets** sélectionnés dans vos paramètres système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cliquez sur l'onglet **Informations de récupération de l'EDL** pour afficher l'URL de récupération. Le lien vers la demande de changement (**CH0030015**) s'affiche également.



4. Pour terminer la configuration et faire passer l'EDL d'inactive à active, vous devez choisir l'une des options suivantes pour informer l'administrateur du pare-feu que l'URL de récupération est disponible.

Option	Description
Cliquez sur Envoyer par e-mail l'URL de récupération de transfert par e-mail.	Envoyez par e-mail l'URL de récupération de l'EDL directement à l'administrateur du pare-feu. Cette option permet à l'administrateur du pare-feu de terminer la configuration sur la Palo Alto Networks plateforme. Choisissez cette option si l'administrateur du pare-feu n'utilise pas le ServiceNow AI Platform® . **Remarque :** L'administrateur d'incident de sécurité active manuellement l'EDL après avoir reçu l'avis ServiceNow AI Platform® que la Palo Alto Networks - Next-Generation Firewall configuration est terminée. Voir : Activer une EDL manuellement.
Complétez la ServiceNow AI Platform® demande de changement et affectez les tâches de configuration à l'administrateur du pare-feu.	Cette option n'est disponible que si l'administrateur de pare-feu pour Palo Alto Networks utilise également le ServiceNow AI Platform®, et si les ServiceNow AI Platform® processus de gestion des changements et d'approbation sont configurés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent approuver la demande de ServiceNow AI Platform® changement. Une fois les tâches de configuration terminées et la demande de changement fermée, l'EDL est activée automatiquement. Voir : Activer une EDL pour Palo Alto Networks - Next-Generation Firewall avec une demande de changement.

Après avoir informé l'administrateur du pare-feu que l'URL de récupération est disponible et confirmé que l'EDL a été configurée dans , en Palo Alto Networks tant qu'administrateur d'incident de sécurité, l'étape suivante consiste à activer l'EDL. Soit vous activez l'EDL manuellement, soit, s'il est configuré, vous utilisez le ServiceNow AI Platform formulaire de demande de changement pour activer l'EDL.

Information associée

Configurer une EDL

Activer une EDL manuellement

Si l'administrateur du pare-feu Palo Alto Networks n'utilise pas le ServiceNow AI Platform, et que vous êtes directement informé de la Palo Alto Networks - Next-Generation Firewall configuration, vous pouvez activer la liste dynamique externe (EDL) manuellement.

Avant de commencer

Dans Palo Alto Networks, affectez un objet EDL, une stratégie et l'URL source à l'EDL que vous avez créée. Pour en savoir plus sur la configuration de l'EDL dans , reportez-vous à Palo Alto Networks la Palo Alto Networks - Next-Generation Firewall section Configurer une EDL.

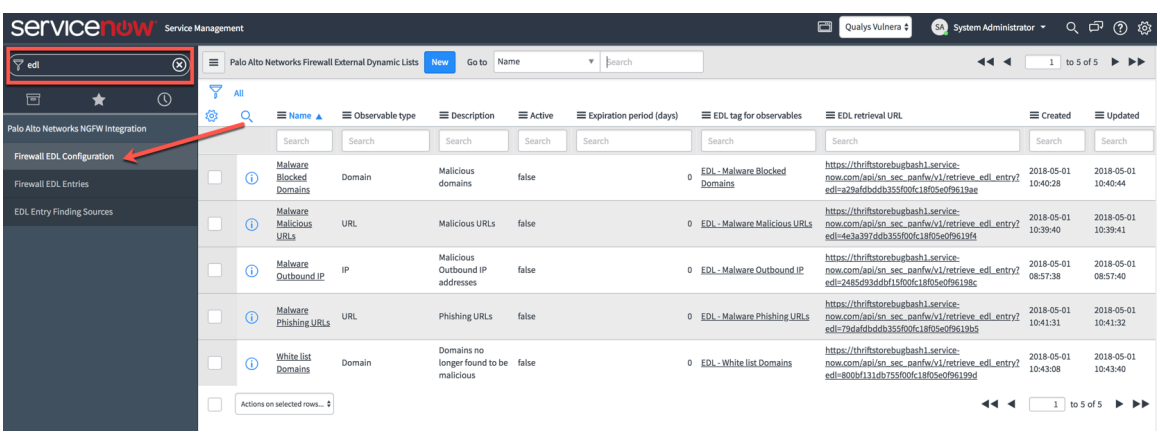
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche

En tant qu'administrateur d'incident ServiceNow AI Platform de sécurité, vous êtes averti par l'administrateur du Palo Alto Networks pare-feu lorsque la configuration de l'EDL est terminée dans le Palo Alto Networks - Next-Generation Firewall.

Procédure

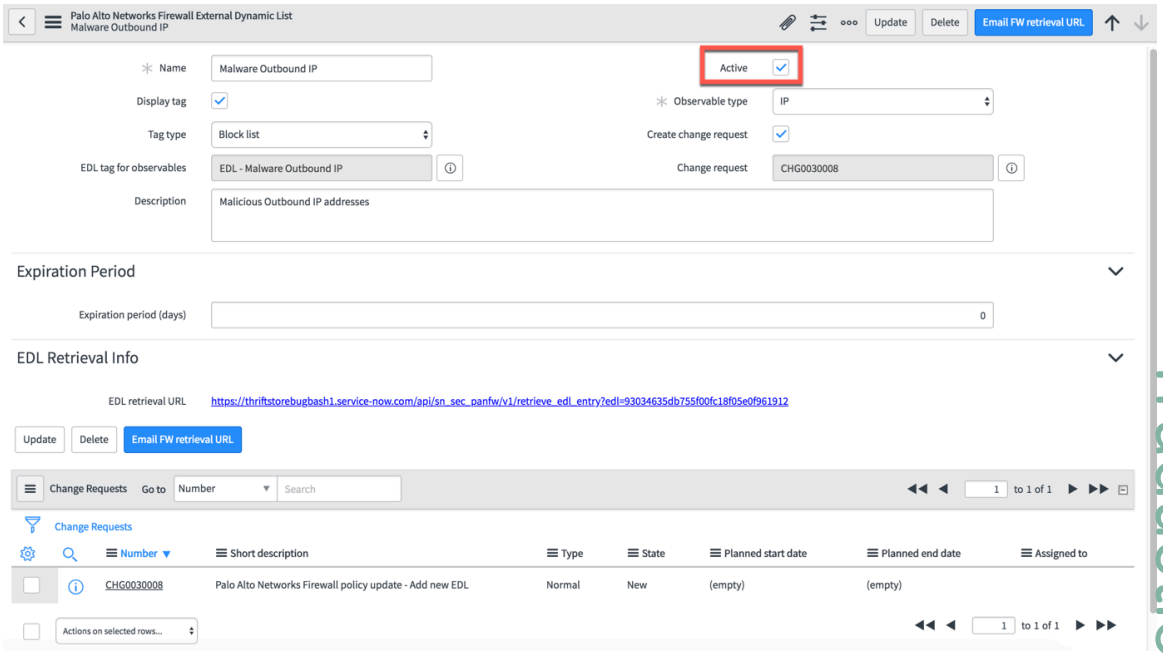
1. Accédez à la **Tous** > **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu**.



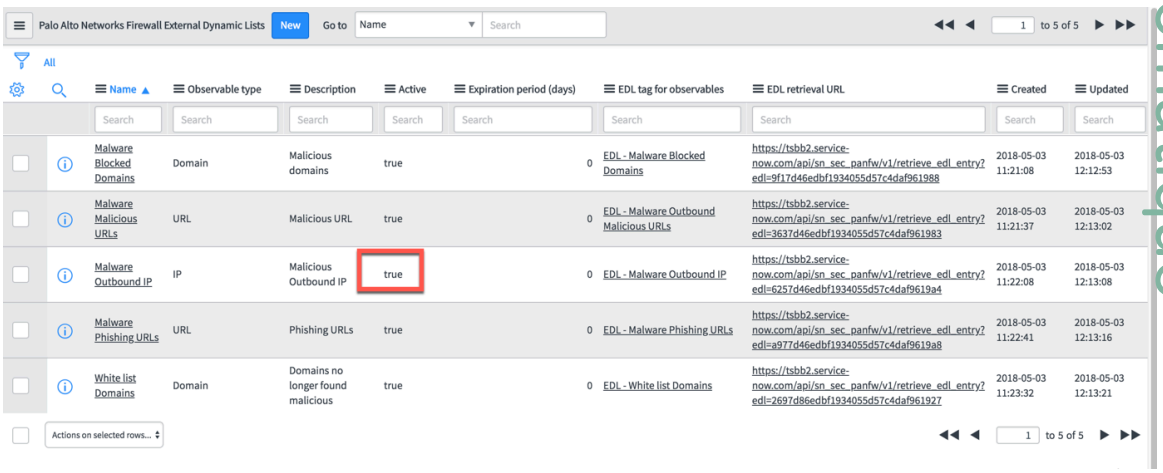
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Sélectionnez le module **Configuration de l'EDL de pare-feu** .
3. Dans la liste des listes dynamiques externes du pare-feu Palo Alto Networks, cliquez sur un élément dans la colonne **Nom** pour l'ouvrir.
4. Dans l'enregistrement qui s'ouvre, cochez la case **Actif** .



5. Cliquez sur **Mettre à jour**.
   Dans la colonne **Actif** de la liste Listes dynamiques externes du pare-feu Palo Alto Networks, vrai s'affiche pour l'état de l'EDL.



Résultats

L'EDL est activée et prête à recevoir des entrées EDL

Que faire ensuite

Soumettez des entrées EDL à partir d'un incident de sécurité ou de la liste de blocage.

Configurer une EDL

L'administrateur Palo Alto Networks du pare-feu configure une EDL sur le Palo Alto Networks - Next-Generation Firewall Une fois informé, l'URL de récupération est disponible à partir

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

du ServiceNow AI Platform. Pour que l'EDL puisse accepter des entrées EDL, elle doit être configurée dans Palo Alto Networks, puis activée dans le ServiceNow AI Platform®.

Avant de commencer

Rôle requis : Palo Alto Networks administrateur de pare-feu

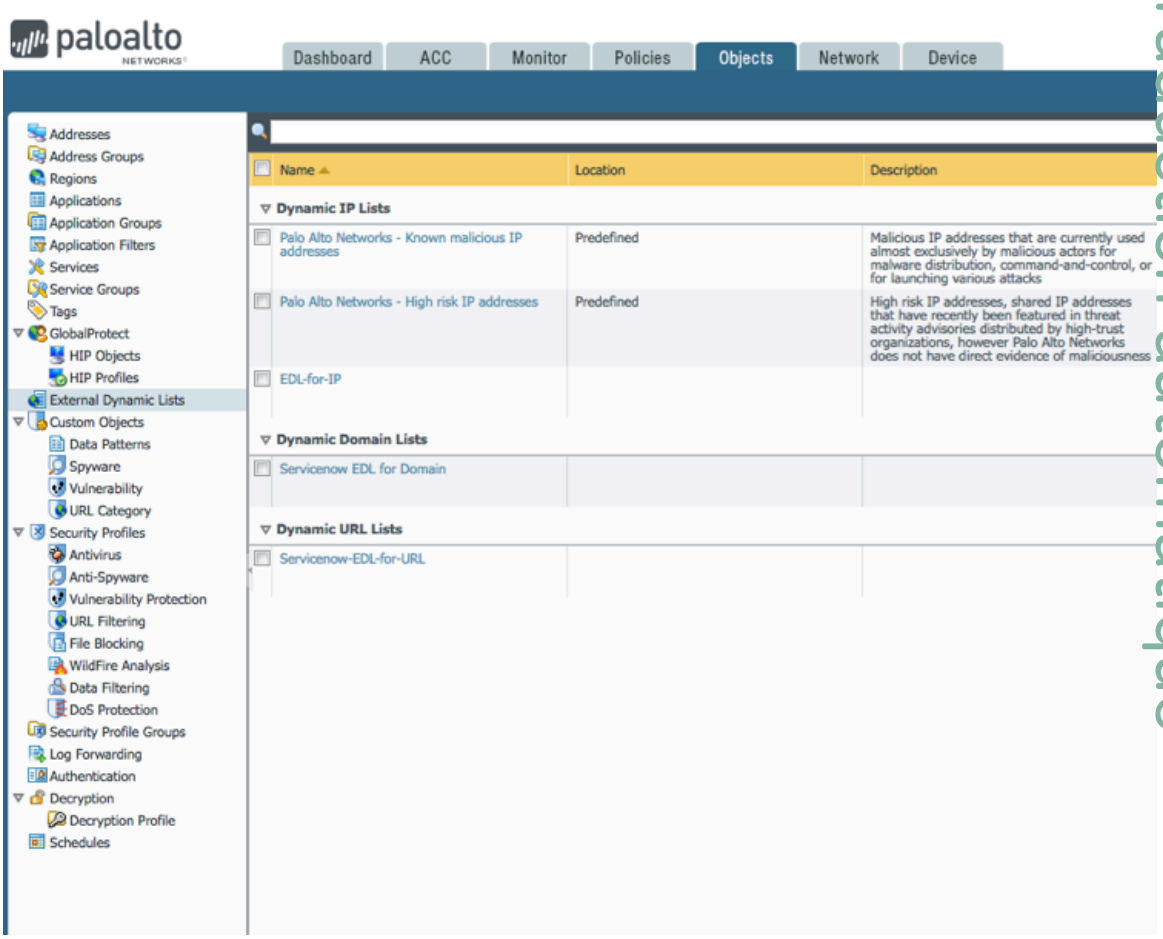
Pourquoi et quand exécuter cette tâche

L'administrateur Palo Alto Networks - Next-Generation Firewall crée un objet EDL et affecte l'URL source (récupération) et la politique à l'EDL. Ces tâches sont effectuées avant Palo Alto Networks l'activation de l'EDL dans le ServiceNow AI Platform.

Les images de la section suivante sont utilisées avec permission et sont PRIVILÉGIÉES et PROPRIÉTAIRES.

Procédure

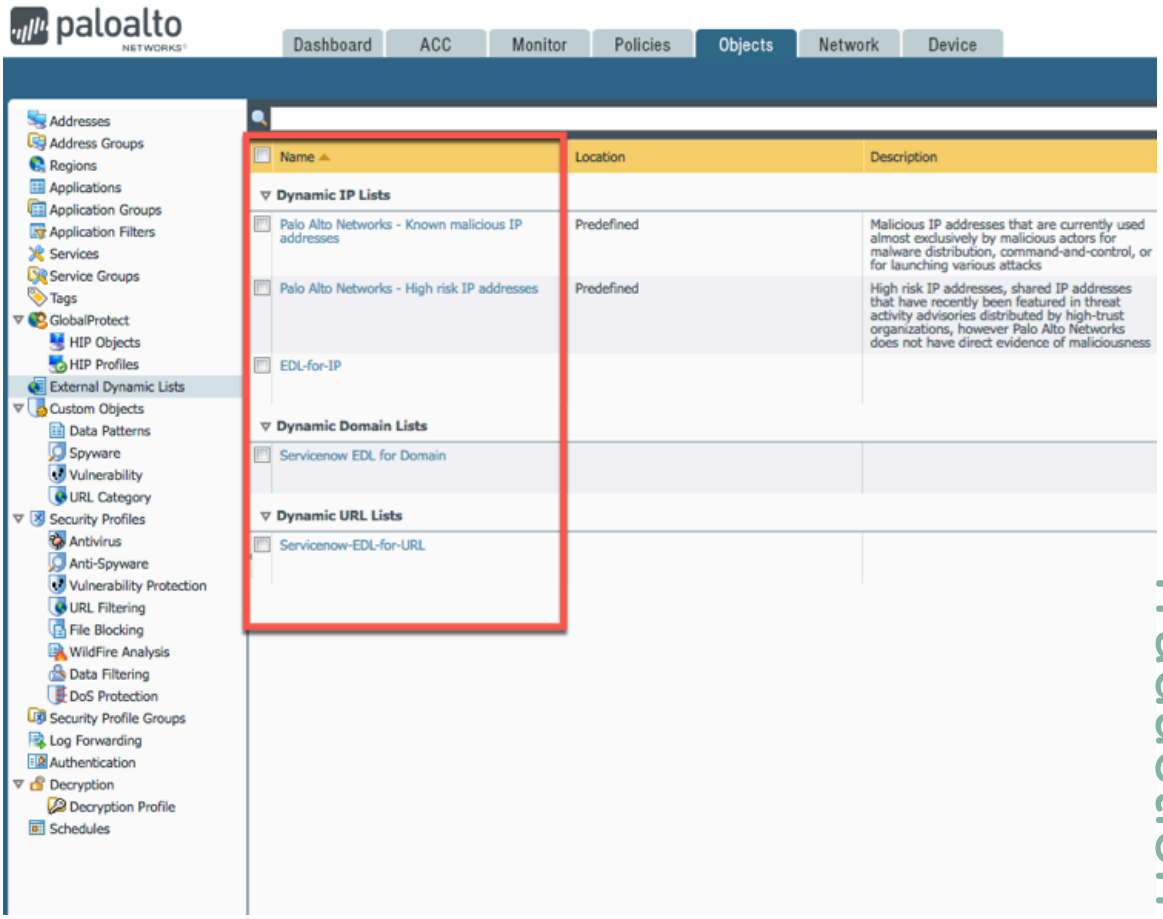
1. Si vous n'avez pas configuré l'EDL sur le pare-feu, accédez à **Listes dynamiques externes** > **Objets** in Palo Alto Networks.



2. Dans la colonne **Nom**, sélectionnez l'EDL ServiceNow que vous souhaitez configurer dans la liste, par exemple, **EDL ServiceNow pour URL.**

Traduction automatique

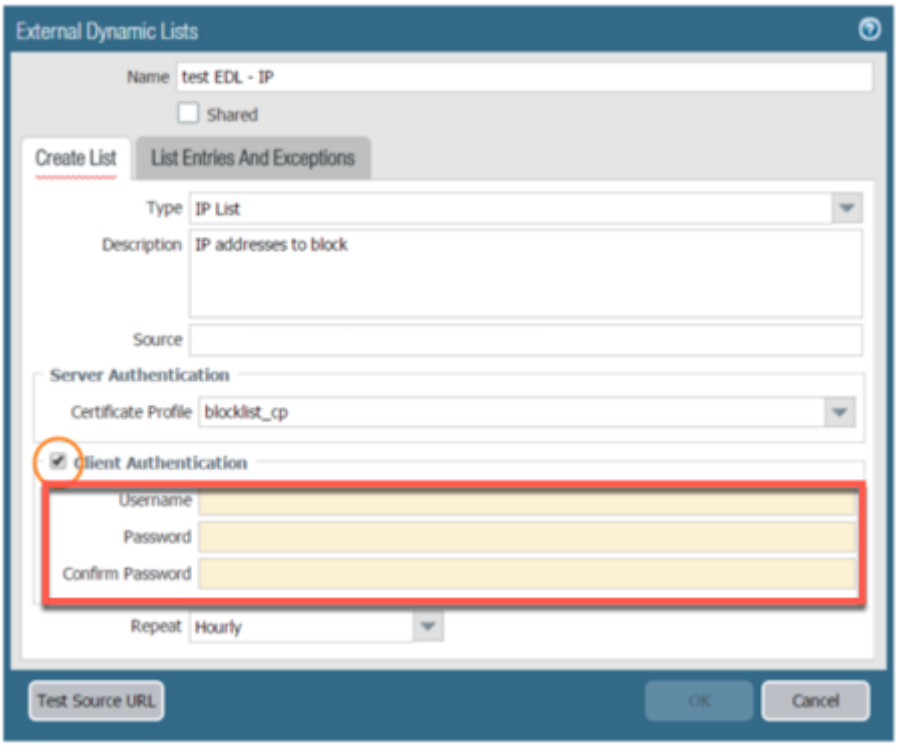
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



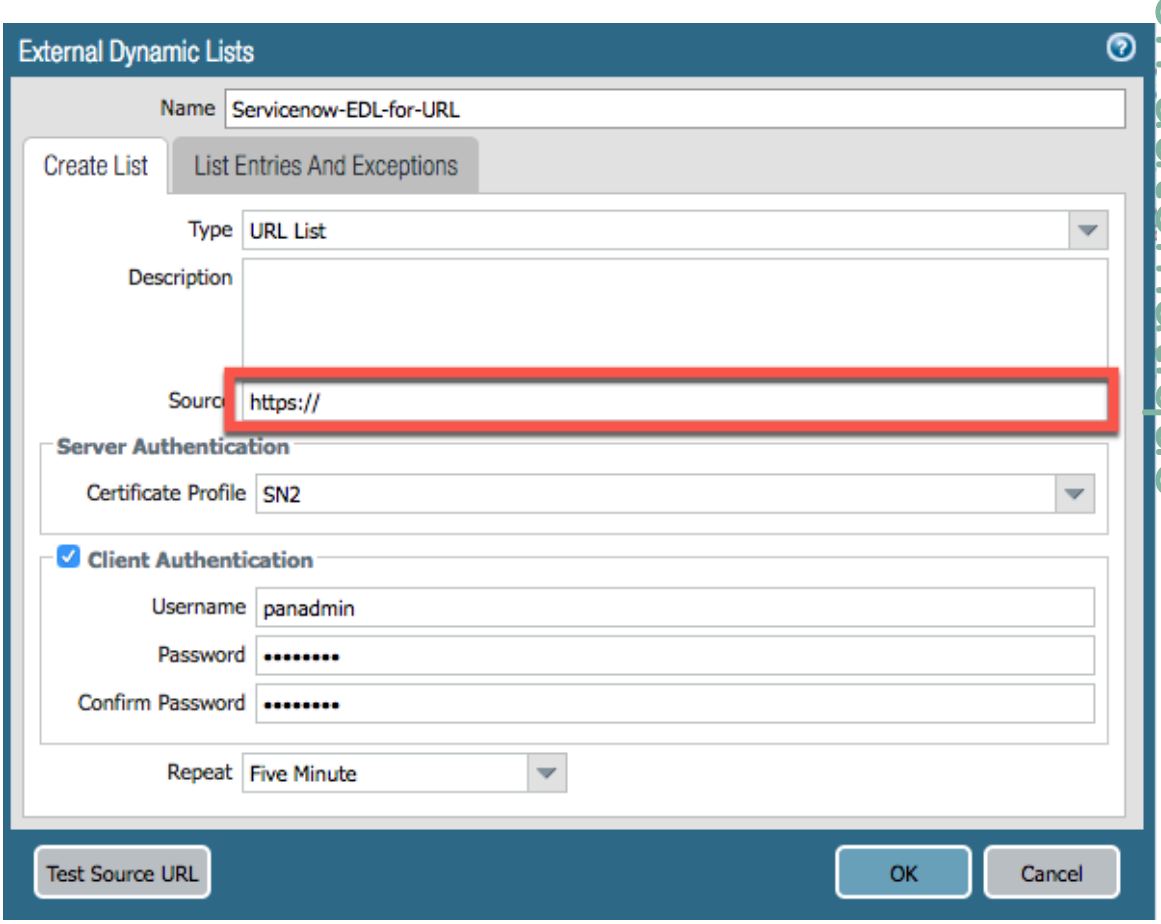
3. Dans la boîte de dialogue Listes dynamiques externes, entrez le nom d'utilisateur et le mot de passe à authentifier avec le ServiceNow AI Platform®.
Ces informations d'identification correspondent au nom d'utilisateur et au mot de passe que vous avez créés pour le rôle de compte API (sn_sec_panfw.api_account_access) dans votre ServiceNow instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans le champ Source, saisissez l'URL qui a été générée dans la liste EDL de votre ServiceNow instance.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez un profil de certificat dans la liste de choix, SN2, par exemple.
6. Cliquez sur OK.

Activer une EDL pour Palo Alto Networks - Next-Generation Firewall avec une demande de changement

S'il est configuré, le ServiceNow formulaire de demande de changement est utilisé pour activer la liste dynamique externe (EDL). Cette option est recommandée si votre administrateur de pare-feu utilise également le pour modifier la politique ou les règles du ServiceNow AI Platform pare-feu. L'EDL est activée automatiquement et prête à recevoir des entrées EDL lors de la fermeture de la ServiceNow AI Platform demande de changement.

Avant de commencer

Remarque : Les figures de la section suivante sont affichées avec **les formulaires à onglets** sélectionnés dans les paramètres système. Pour plus d'informations sur la sélection et l'effacement des formulaires à onglets, consultez la section intitulée Afficher les formulaires à onglets dans Configuration de la mise en page du formulaire sur le site Web de la documentation produit ServiceNow .

Rôle requis : sn_si.admin pour approuver la demande de changement et les tâches de changement

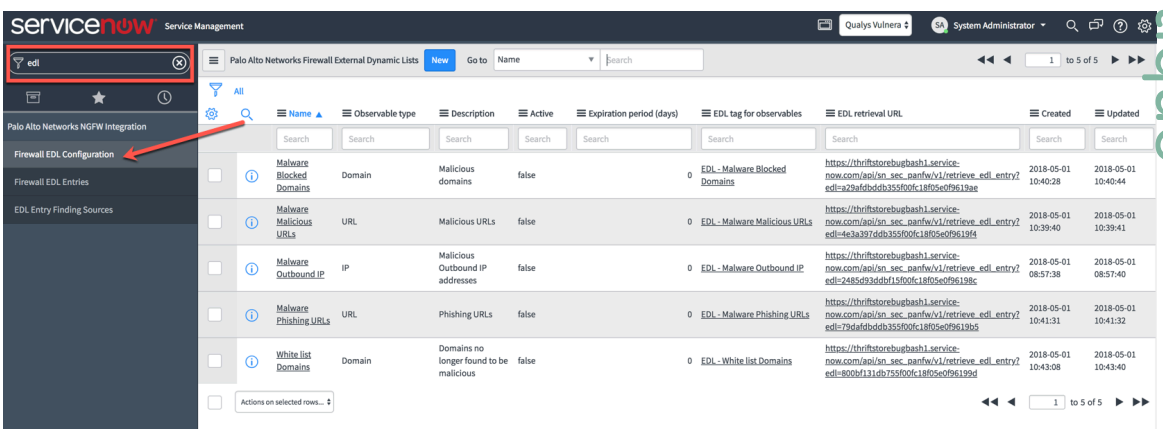
Palo Alto Networks administrateur de pare-feu pour terminer les tâches de configuration dans Palo Alto Networks

Pourquoi et quand exécuter cette tâche

Une fois configurée, surveillez votre ServiceNow AI Platform demande de changement et affectez-lui toutes les tâches nécessaires pour configurer le Palo Alto Networks - Next-Generation Firewall. Une fois ces tâches terminées, fermez la ServiceNow AI Platform demande de changement pour activer automatiquement l'EDL.

Procédure

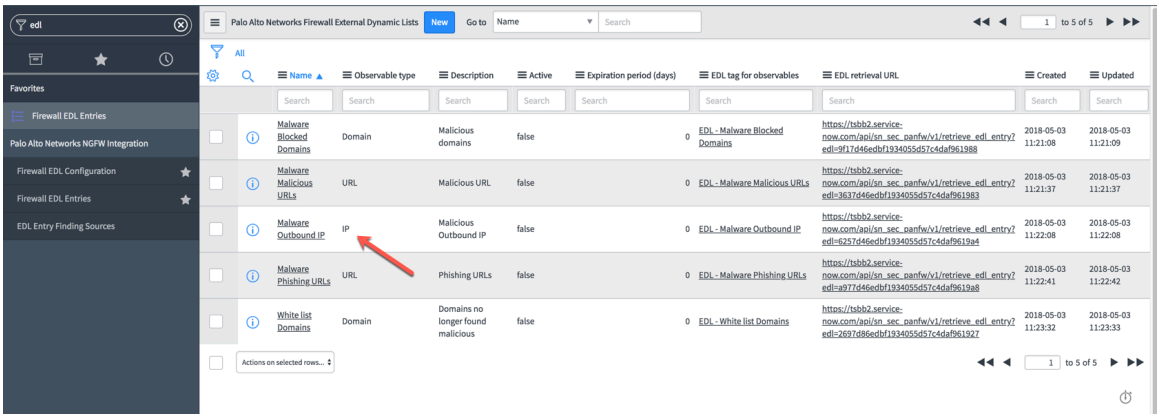
1. Accédez à la **Tous** > **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu**.



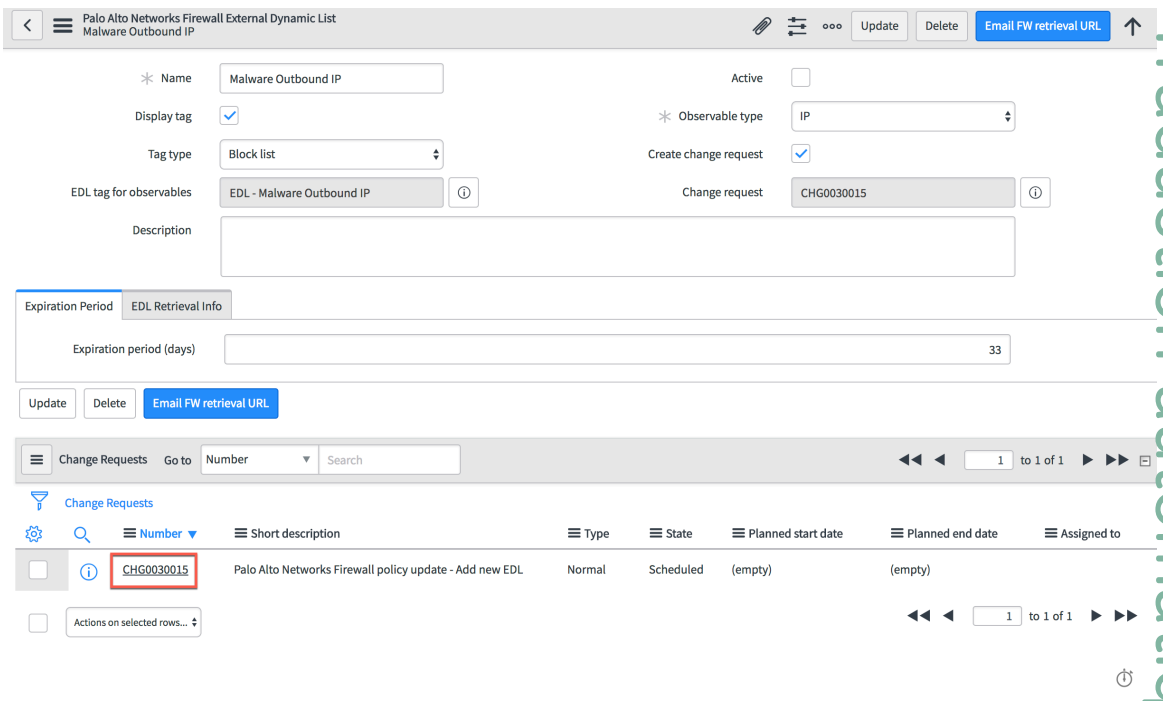
2. Sélectionnez le module EDL et cliquez sur un EDL dans la colonne **Nom** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



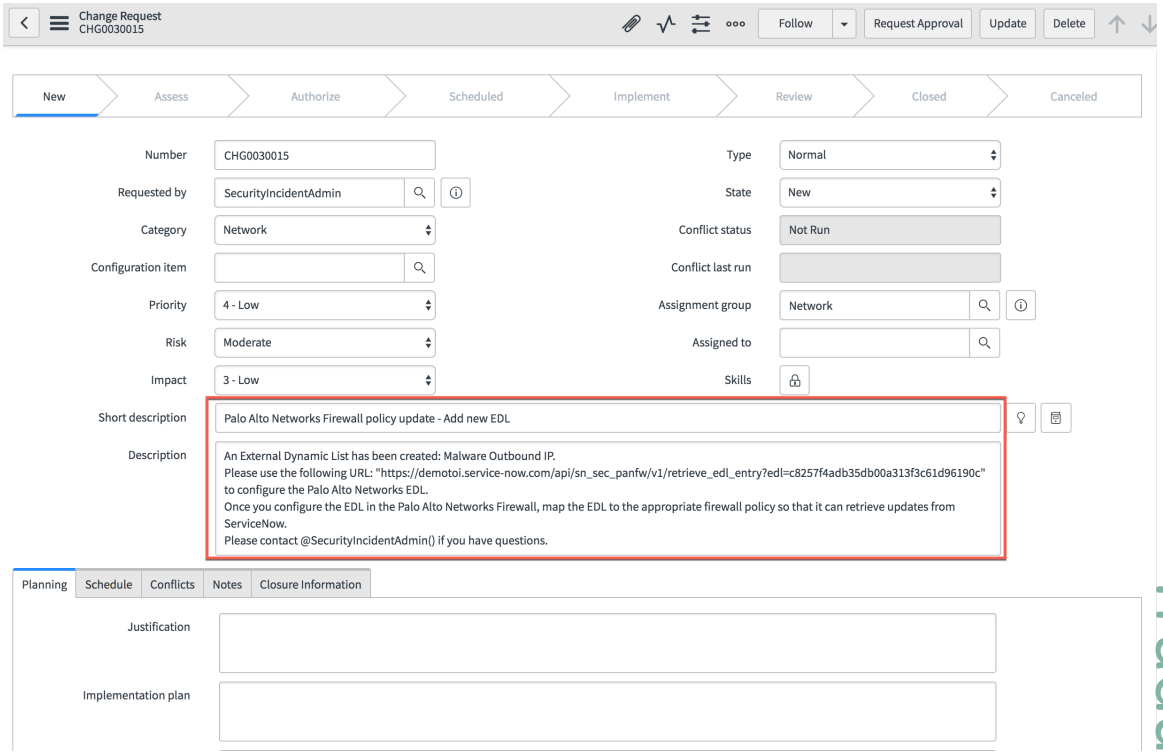
3. Dans l'enregistrement EDL ouvert, cliquez sur le numéro de la demande de changement dans la liste connexe Demandes de changement.



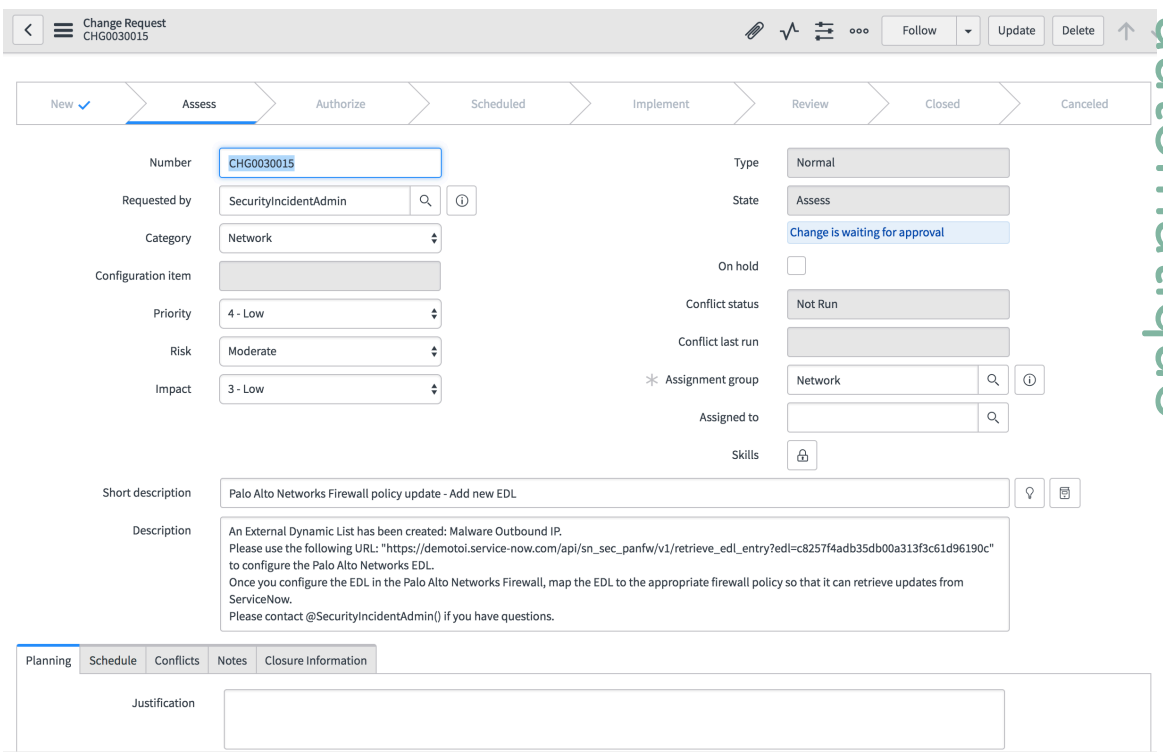
L'enregistrement de la demande de changement s'affiche. Le champ **Description** répertorie l'URL de récupération utilisée pour configurer l'EDL Palo Alto Networks . Des détails sur le mappage de l'EDL à la stratégie appropriée Palo Alto Networks - Next-Generation Firewall sont également inclus. Dans le champ **Brève description**, un commentaire indique qu'il existe une demande d'ajout d'une nouvelle EDL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans le coin supérieur droit de l'enregistrement, cliquez sur **Demander l'approbation**.
L'état passe à Évaluer, et un message s'affiche indiquant que la demande de changement est en attente d'approbation.

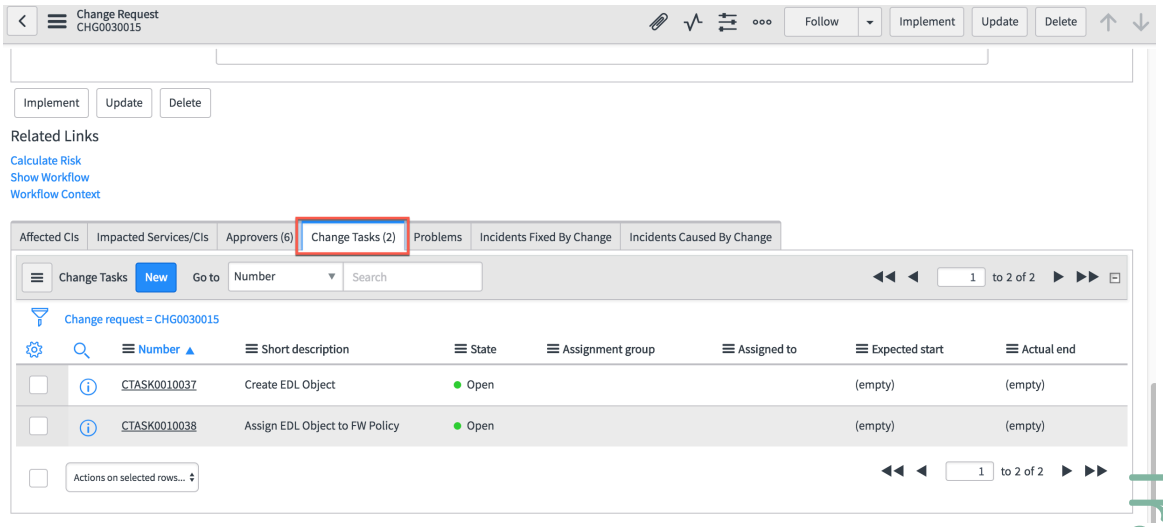


5. Pour terminer la demande de changement et activer l'EDL, suivez les étapes pour affecter les tâches et fermer la demande de changement.

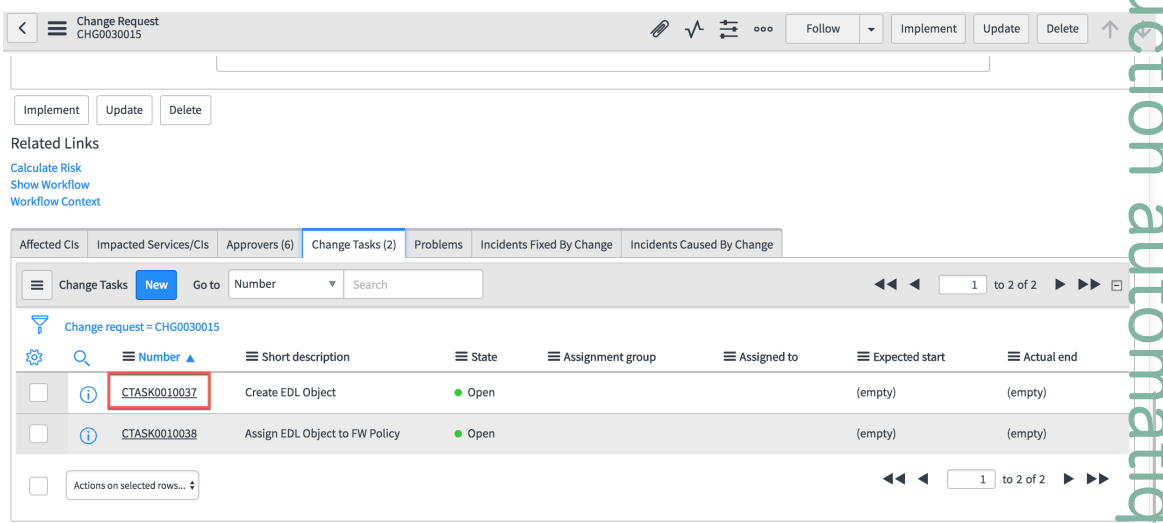
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. S’il n’est pas affiché, ouvrez la demande de changement et sélectionnez l’onglet **Tâches de changement** .



b. Cliquez sur la tâche associée à la création de l’objet EDL pour l’ouvrir.

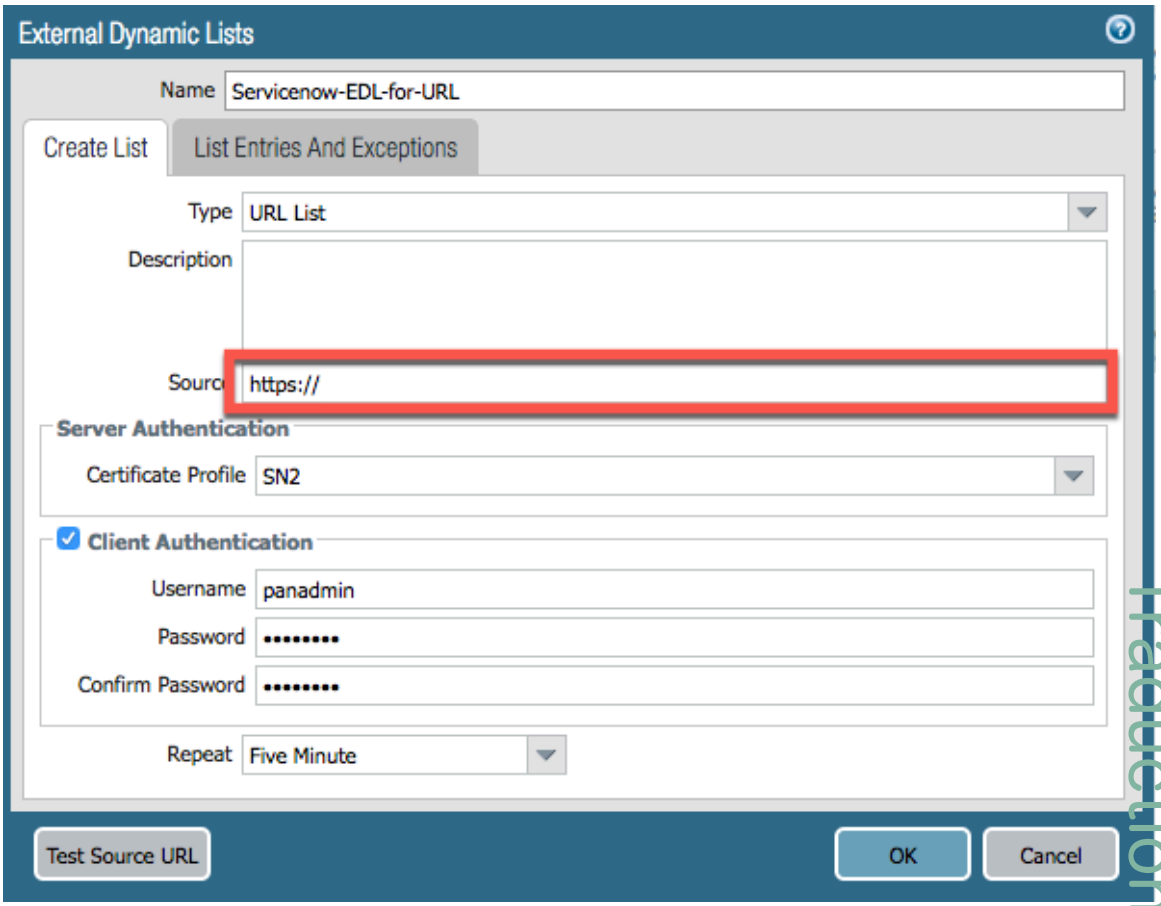


c. Sur l’enregistrement qui s’affiche, affectez la tâche à l’administrateur du Palo Alto Networks pare-feu, puis cliquez sur **Mettre à jour**.
L’administrateur du pare-feu est informé et crée l’objet EDL dans le Palo Alto Networks - Next-Generation Firewall.

Pour créer l’objet EDL, l’URL de récupération est copiée dans Palo Alto Networks à ServiceNow AI Platform **Listes dynamiques externes** > **Créer des listes** > **Source**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

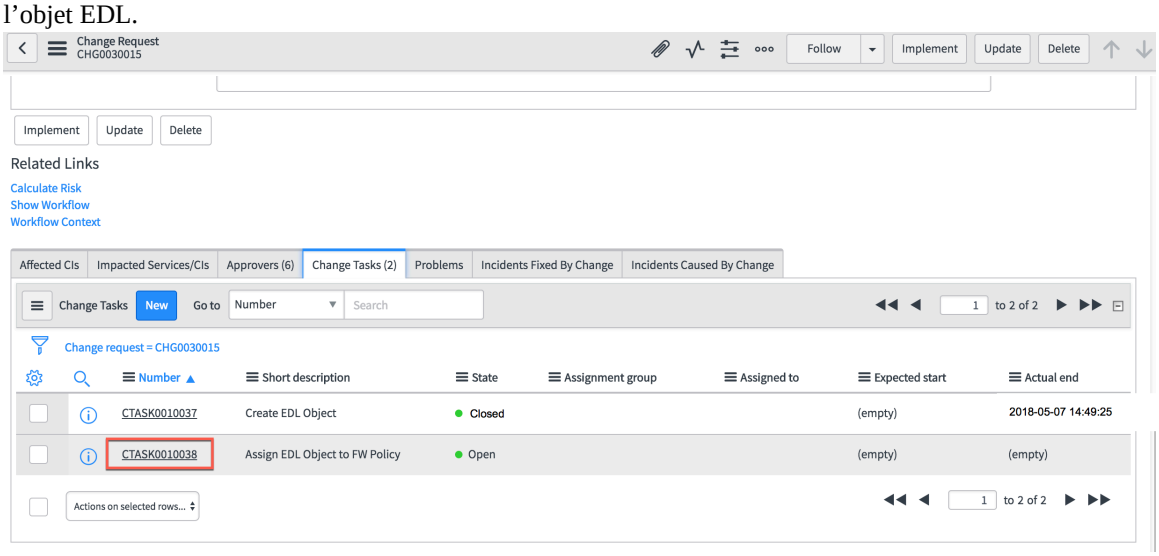


L'image est utilisée avec permission et est PRIVILÉGIÉE et PROPRIÉTAIRE.

d. Après avoir vérifié que l'objet EDL a été créé dans Palo Alto Networks, dans le ServiceNow AI Platform, accédez à la demande de changement associée à la création de l'objet EDL et cliquez sur **Fermer la tâche**.

Sur l'enregistrement de tâche de cet exemple, CTASK0010037 a été fermée pour cette tâche.

e. Accédez à l'onglet Tâches de changement et cliquez sur la tâche d'affectation d'une politique de pare-feu à l'objet EDL.



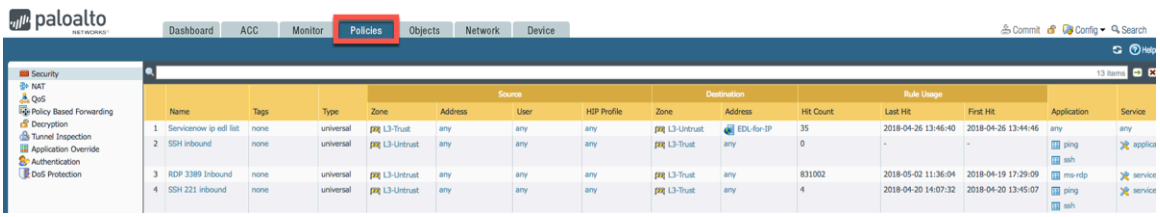
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'état de CTASK0010037 est Fermé.

f. Ouvrez l'enregistrement et affectez la tâche suivante.

Une fois la tâche affectée, dans Palo Alto Networks, l'administrateur du pare-feu accède à l'onglet **Politiques** pour affecter la politique.



L'image est utilisée avec permission et est PRIVILÉGIÉE et PROPRIÉTAIRE.

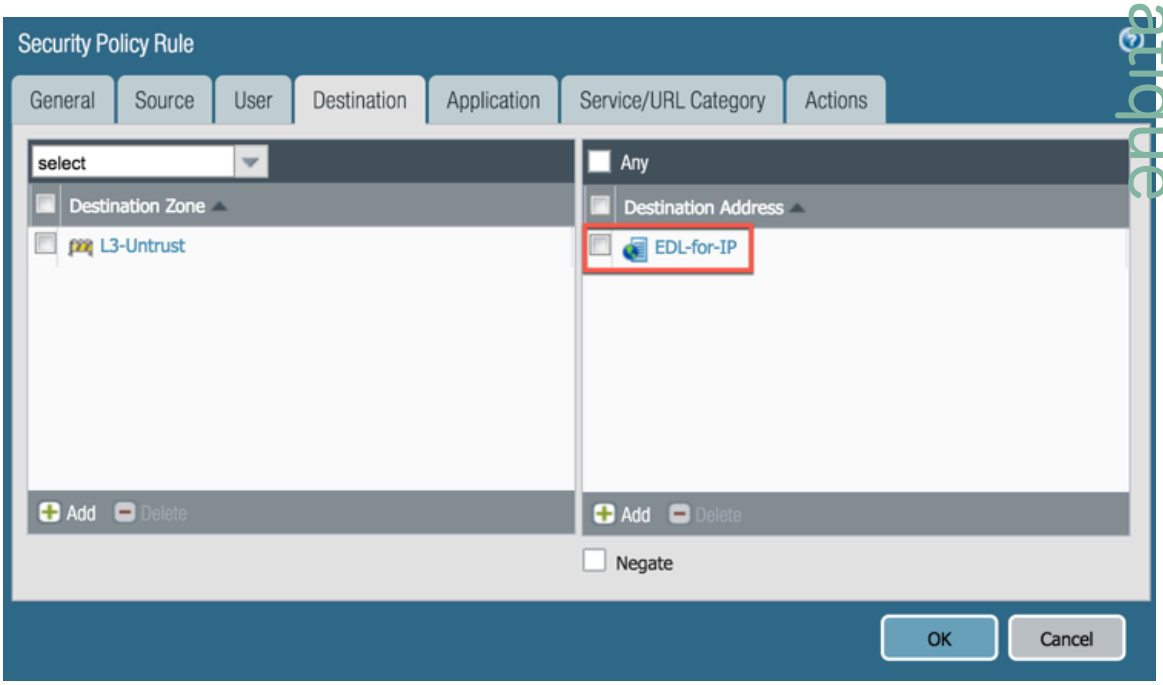
g. Dans la colonne **Nom** , recherchez et cliquez sur la règle de politique de sécurité à laquelle vous souhaitez ajouter l'EDL, par exemple, la **liste des EDL IP de ServiceNow**.



L'image est utilisée avec permission et est PRIVILÉGIÉE et PROPRIÉTAIRE.

h. Dans la boîte de dialogue Règle de politique de sécurité, sélectionnez l'onglet **Destination** pour ajouter une EDL dans le champ **Adresse de destination** .

i. Pour afficher toutes les EDL disponibles, cliquez sur l'icône **Ajouter** .



L'image est utilisée avec permission et est PRIVILÉGIÉE et PROPRIÉTAIRE.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

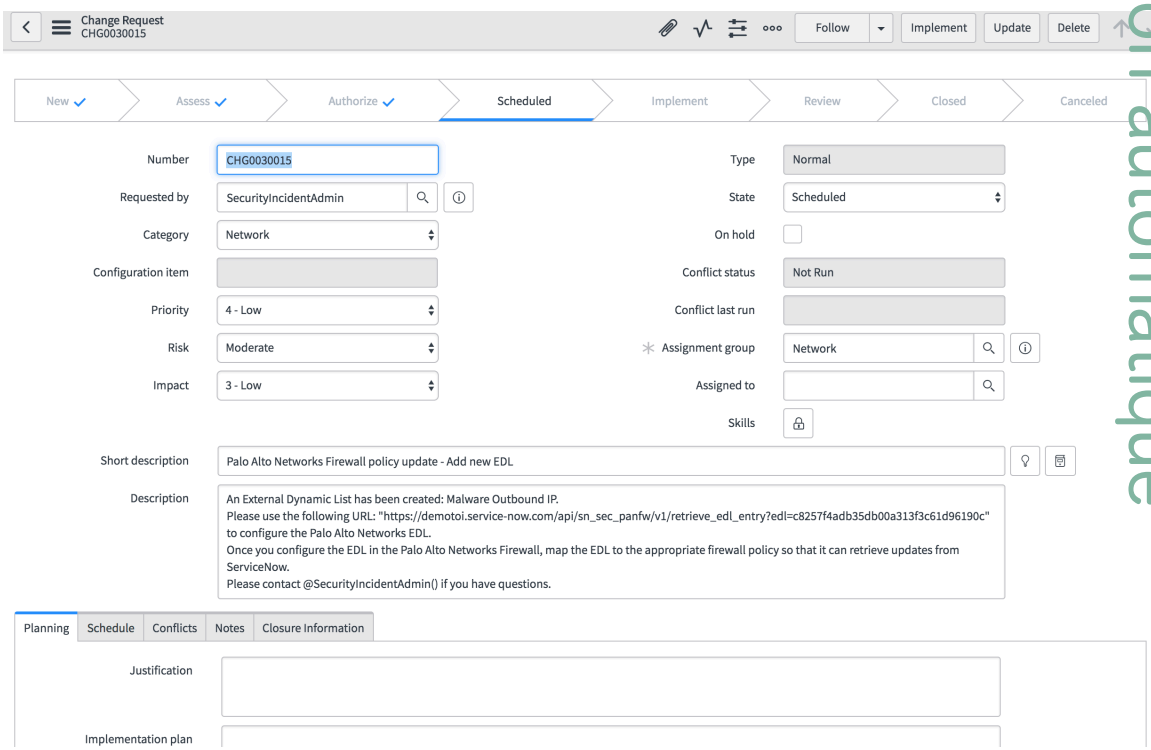
j. Cliquez sur **OK**.

k. Après avoir vérifié que l'objet EDL a été affecté à une politique de sécurité, accédez à la demande de changement, ouvrez la tâche associée à l'affectation de l'objet EDL, puis cliquez ServiceNow AI Platform sur **Fermer la tâche**.
Une fois les deux tâches fermées, la demande de changement est prête à être approuvée.

l. Dans l'enregistrement de demande de changement, cliquez sur la liste connexe **des approbateurs** et sélectionnez un élément dans la colonne **État** pour ouvrir la demande utilisée pour créer l'EDL.



m. Sur le formulaire de demande d'approbation ouvert, cliquez sur **Approuver**.
L'état de la demande de changement passe à Planifié.



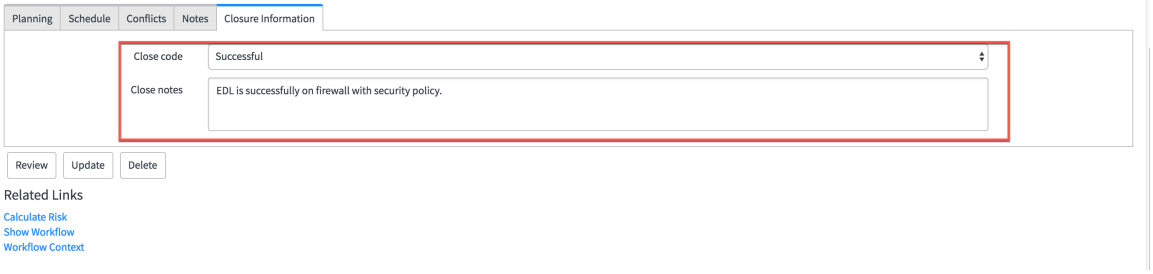
n. Cliquez **sur Implémenter**.

o. Cliquez sur l'onglet **Informations sur la fermeture** et saisissez des notes pour fermer la demande.

Une saisie dans ce champ est obligatoire pour fermer la demande de changement.

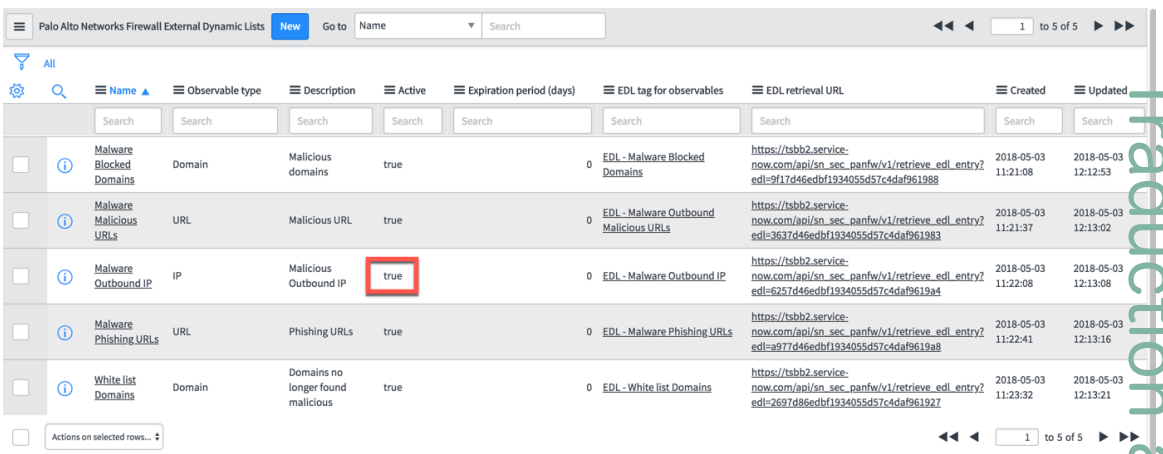
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

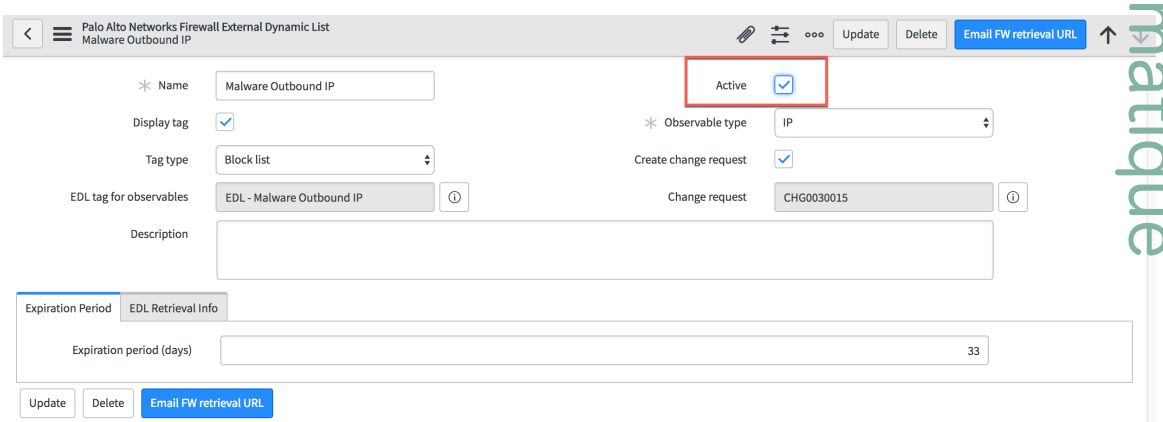


Une fois la demande de changement fermée, l'EDL est activée automatiquement. Si vous n'avez pas vérifié que l'EDL est activée, accédez à **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu**.

Dans la colonne Actif de la liste, notez que l'état de l'EDL est (vrai).



Dans la colonne Nom, cliquez sur le nom de l'EDL et, dans l'enregistrement ouvert, notez que la case **Actif** est également cochée.



L'EDL est maintenant prête à accepter les entrées EDL.

Que faire ensuite

Soumettez des entrées EDL à partir d'un incident de sécurité ou de la liste de blocage.

Soumettre des entrées EDL à partir d'un enregistrement d'incident de sécurité pour Palo Alto Networks - Next-Generation Firewall

Les observables joints à un enregistrement d'incident de sécurité sont soumis pour approbation en tant qu'entrées de liste dynamique externe (EDL) aux EDL. Un processus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d’approbation des entrées EDL fait partie du workflow préconfiguré. Le pare-feu importe les entrées EDL (adresses IP, URL, domaines) qui sont incluses dans les listes EDL et applique la politique.

Avant de commencer

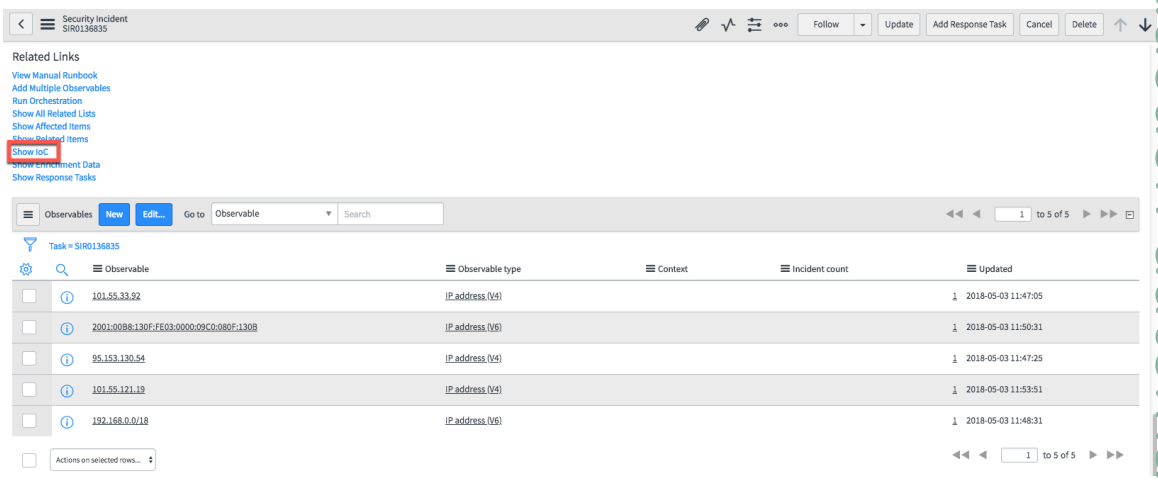
Rôle requis : sn_si.analyst pour soumettre des entrées EDL. Pour approuver des entrées EDL : l’approbation est affectée à sn_si.admin par défaut, mais cette autorisation peut être attribuée à la demande de votre organisation.

Pourquoi et quand exécuter cette tâche

Les utilisateurs disposant du rôle sn_si.analyst soumettent des entrées EDL en demandant un blocage sur les observables joints à un enregistrement d’incident de sécurité. Une fois soumise, une entrée EDL avec l’état En attente est générée et envoyée pour approbation. L’exemple suivant montre une demande de bloc pour un observable d’URL.

Procédure

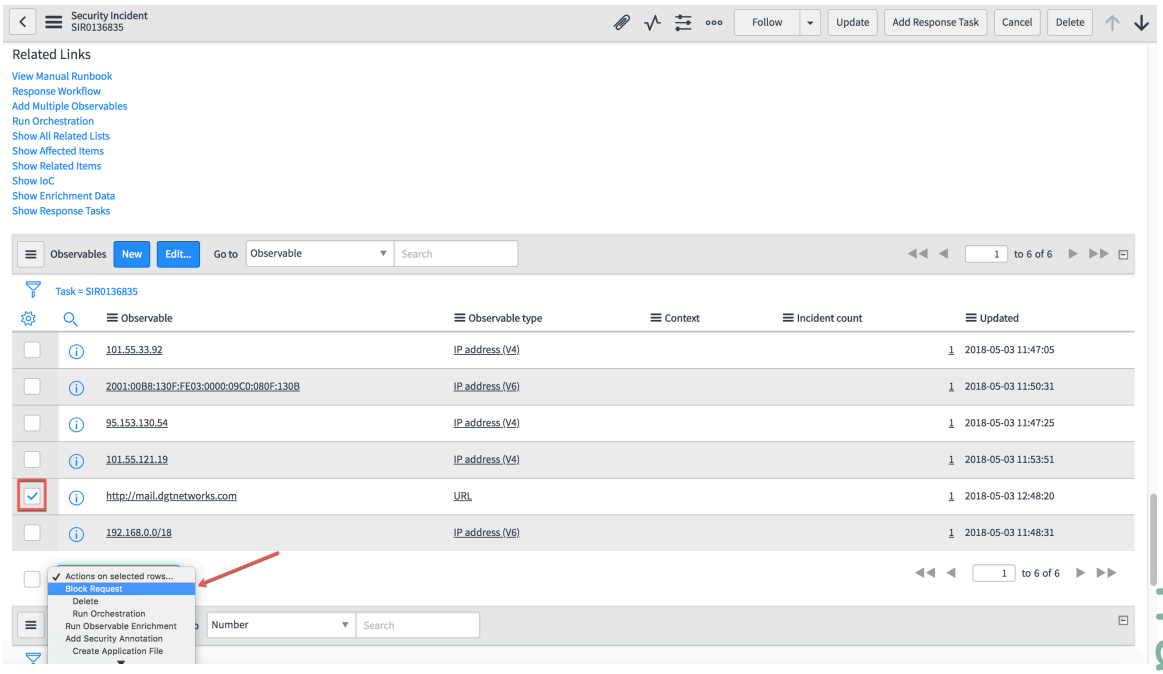
1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**et cliquez sur un enregistrement d’incident de sécurité pour l’ouvrir.
2. Cliquez sur le lien connexe **Afficher l’IoC** .



3. Dans la liste connexe Observables, sélectionnez les observables que vous voulez bloquer et, dans la liste **Actions sur les lignes sélectionnées** , sélectionnez **Demande de bloc**.

Traduction automatique

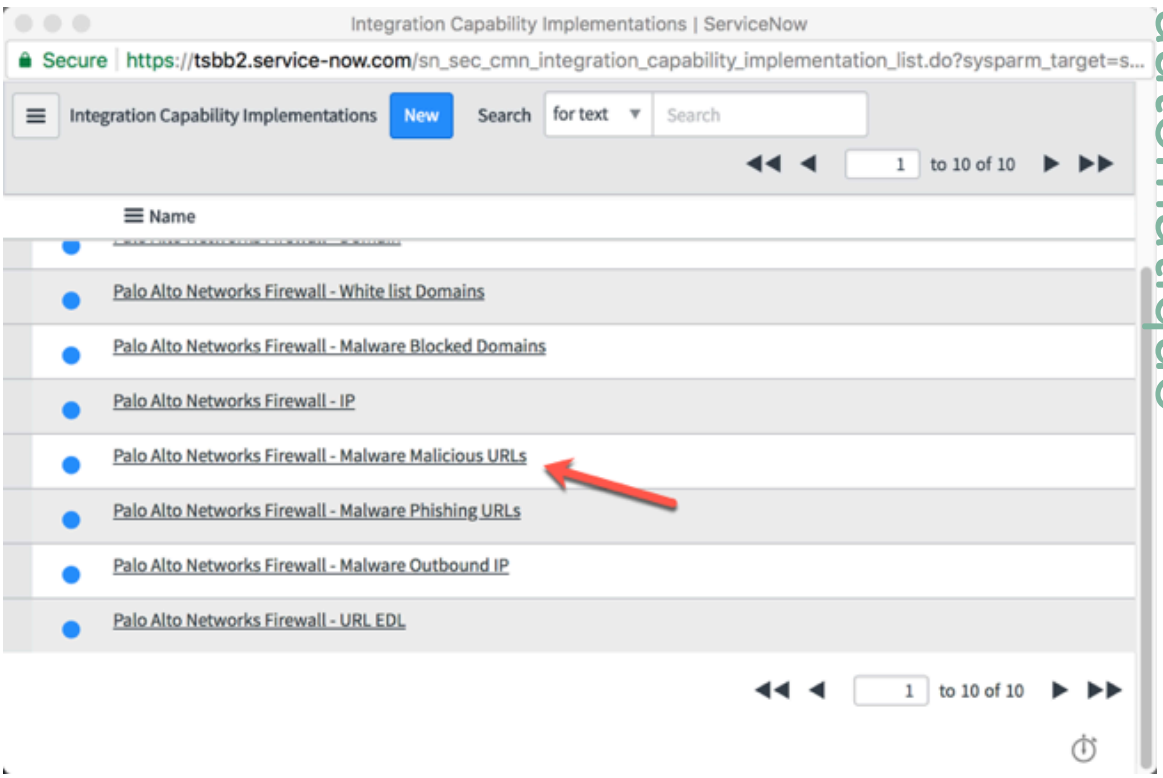
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans la boîte de dialogue qui s'affiche, cliquez sur l'icône de recherche ( ).

5. Dans la liste qui s'affiche, sélectionnez l'EDL à laquelle vous souhaitez joindre cette entrée.

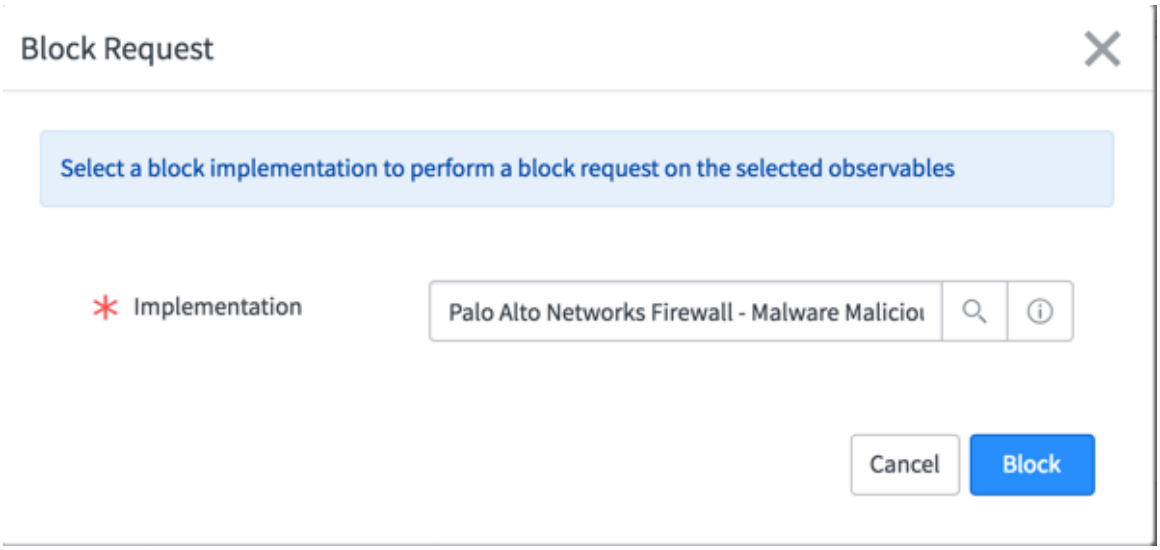
Remarque : Pour cet exemple, le type observable d'entrée (URL) doit correspondre au type observable EDL (URL).



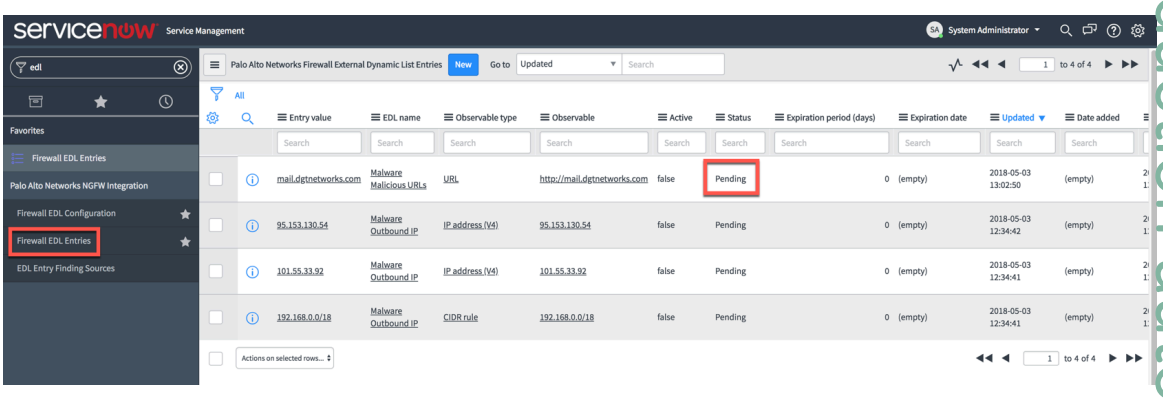
6. Dans la boîte de dialogue Demande de bloc avec le nom de l'EDL affiché dans le champ **Implémentation** , cliquez sur **Bloquer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

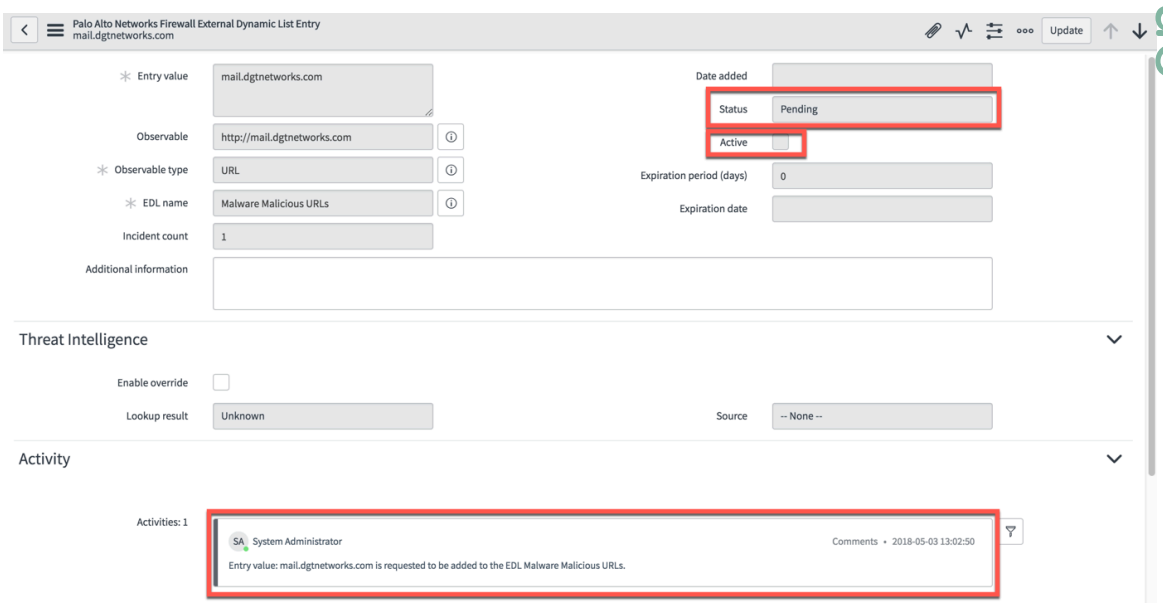


7. Accédez à la **Intégration de Palo Alto Networks NGFW** > **Entrées de l'EDL du pare-feu** et cliquez sur **Entrées EDL de pare-feu**.



8. Dans la liste Entrées de la liste dynamique externe du pare-feu Palo Alto Networks, cliquez sur votre observable dans la colonne **Valeur d'entrée** pour ouvrir l'enregistrement.

   Pour cet exemple, l'enregistrement de **mail.dgtnetworks.com s'affiche** .

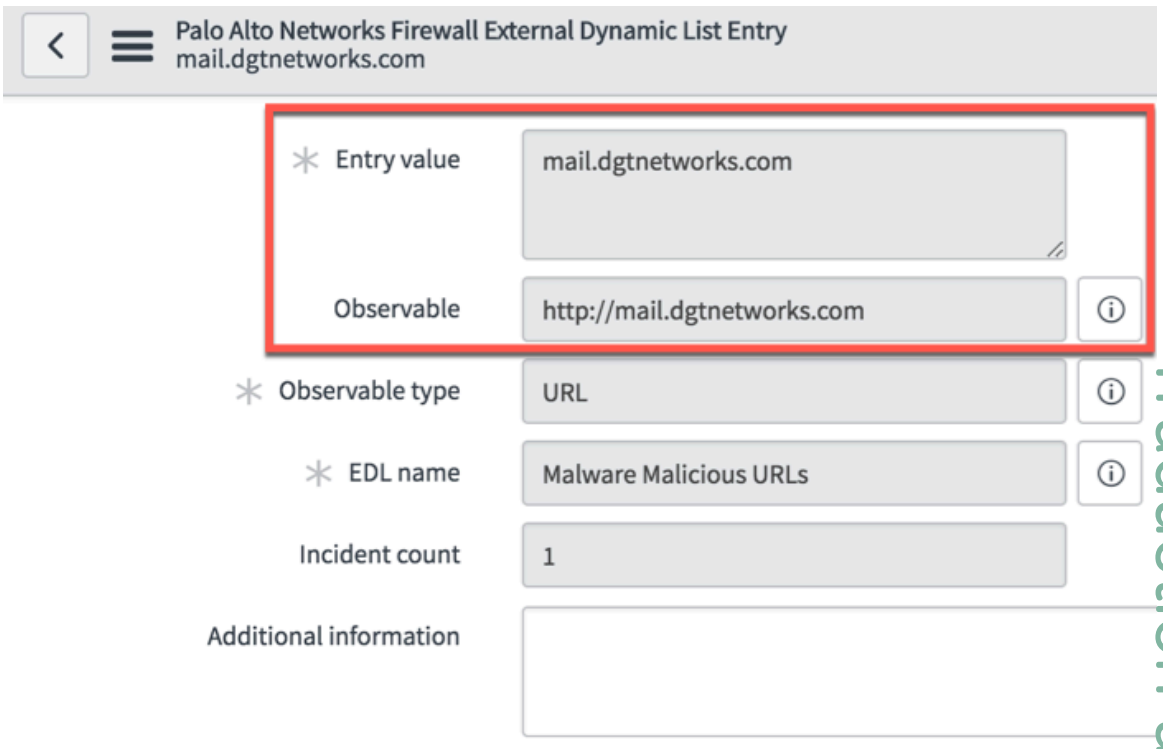


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'état est En attente, la case Actif est décochée et les notes de travail indiquent qu'il existe une demande d'ajout de l'observable. Cette demande d'entrée EDL est prête à être approuvée.

Les champs Valeur d'entrée et Observable présentent des formats différents pour l'observable d'URL.



L'icône en regard du champ Observable est un lien vers la ServiceNow AI Platform® table Observable.

La valeur du champ Observable (http://mail.dgtnetworks.com) est liée à la table Observable et correspond au format qui a été apporté à partir de l'événement déclenchant l'incident Réponse aux incidents de sécurité .

Le ServiceNow AI Platform® peut modifier automatiquement les entrées EDL afin qu'elles soient compatibles avec le format d'URL EDL Palo Alto Networks .

Dans cet exemple, l'observable a été créé avec le protocole http:// (http://mail.dgtnetworks.com), et ce format est affiché dans le champ Observable. Le protocole http:// est automatiquement supprimé de l'observable par le afin qu'il ServiceNow AI Platform® soit compatible avec Palo Alto Networks et puisse être récupéré. Par conséquent, mail.dgtnetworks.com s'affiche dans le champ Valeur d'entrée .

Que faire ensuite

Approuver les entrées EDL.

Information associée

Exceptions d'entrée EDL pour Palo Alto Networks - Next-Generation Firewall

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Soumettre des entrées EDL de la liste de blocage pour Palo Alto Networks - Next-Generation Firewall

Pour les observables déterminés comme malveillants et non associés à un incident de sécurité spécifique ServiceNow AI Platform , vous soumettez des entrées de liste dynamique externe (EDL) à partir de la liste de blocage.

Avant de commencer

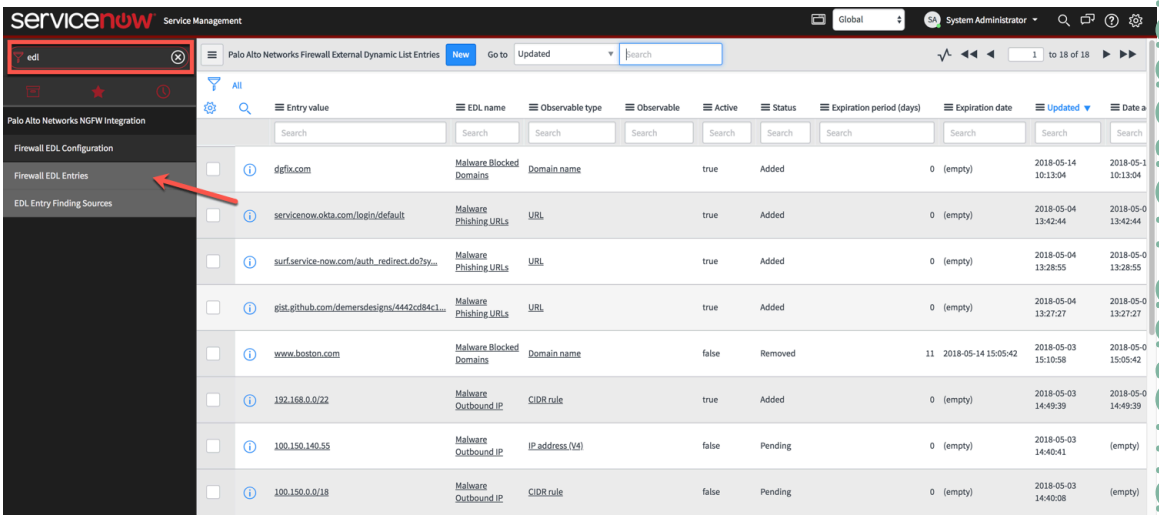
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Lorsque vous souhaitez bloquer un observable que vous avez déterminé comme malveillant, ou autoriser un observable que vous avez déterminé comme non malveillant et que l'observable n'est pas associé à un enregistrement d'incident de sécurité spécifique ServiceNow AI Platform , vous soumettez des entrées EDL directement à partir de la liste de blocage. Des exemples de ces types d'entrées EDL peuvent être des URL ou des domaines pour des sites spécifiques.

Procédure

1. Accédez à la **Tous** > **Intégration de Palo Alto Networks NGFW** > **Entrées de l'EDL du pare-feu**.



2. Cliquez sur le module **Entrées EDL du pare-feu** .
3. Dans la liste Entrées de la liste dynamique externe du pare-feu Palo Alto Networks, cliquez sur **Nouveau**.
4. Dans le nouvel enregistrement qui s'affiche, dans le champ **Valeur d'entrée** , saisissez une valeur pour votre observable.
   Les deux résultats possibles de cette entrée :

   Les autres champs du formulaire sont renseignés automatiquement.

   Un observable correspondant est trouvé et un message s'affiche indiquant qu'un observable correspondant existe. Sélectionnez l'EDL à laquelle vous souhaitez joindre cette entrée, puis cliquez sur **Soumettre**. Sélectionnez l'EDL à laquelle vous souhaitez attacher cette entrée avant de définir la période d'expiration.

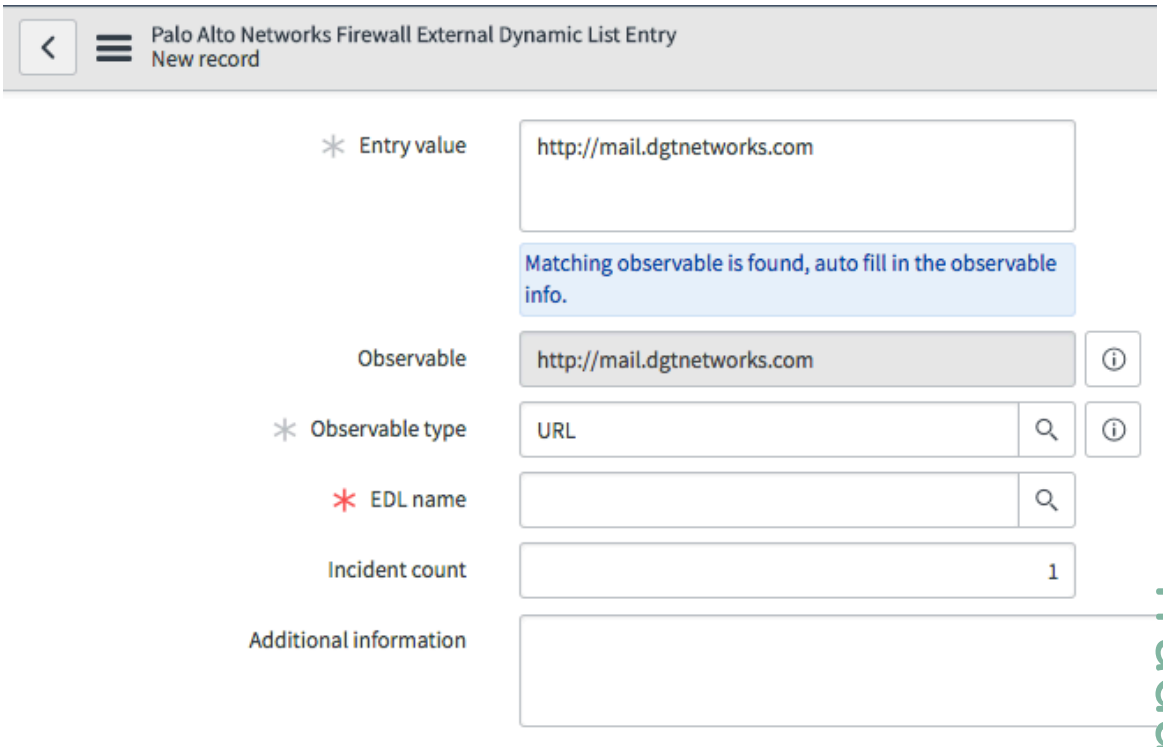
   Un message vous demandant de remplir le formulaire s'affiche.

   Aucun observable correspondant n'a été trouvé et vous devez remplir le formulaire. Une fois que vous l'avez terminée, sélectionnez l'EDL à laquelle vous souhaitez joindre l'observable, puis cliquez sur **Soumettre**. Un enregistrement d'observable est créé.

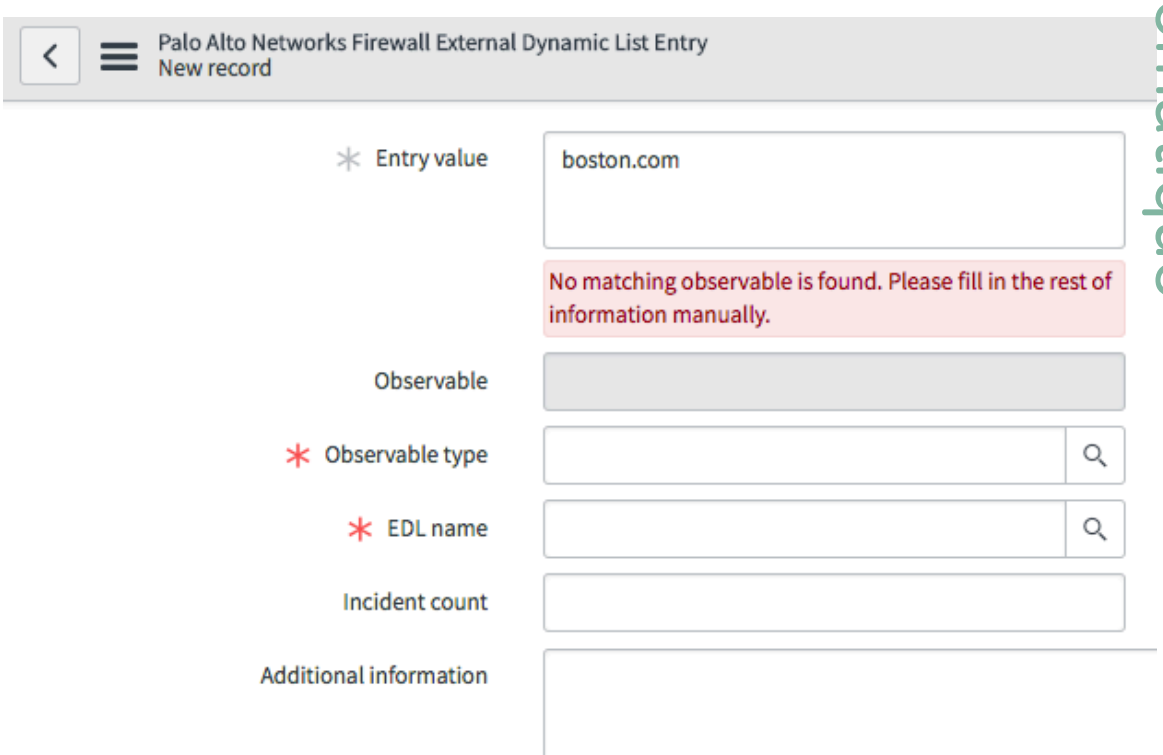
La figure suivante montre un exemple d'observable de domaine existant et comment les champs sont complétés automatiquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur l'icône de recherche pour sélectionner l'EDL à laquelle vous souhaitez joindre l'entrée.
6. Cliquez sur **Envoyer**.
   Si l'approbation par e-mail est configurée dans votre workflow, une demande d'approbation par e-mail est envoyée.
7. Si un message s'affiche vous demandant de renseigner manuellement le reste des informations, renseignez les champs.

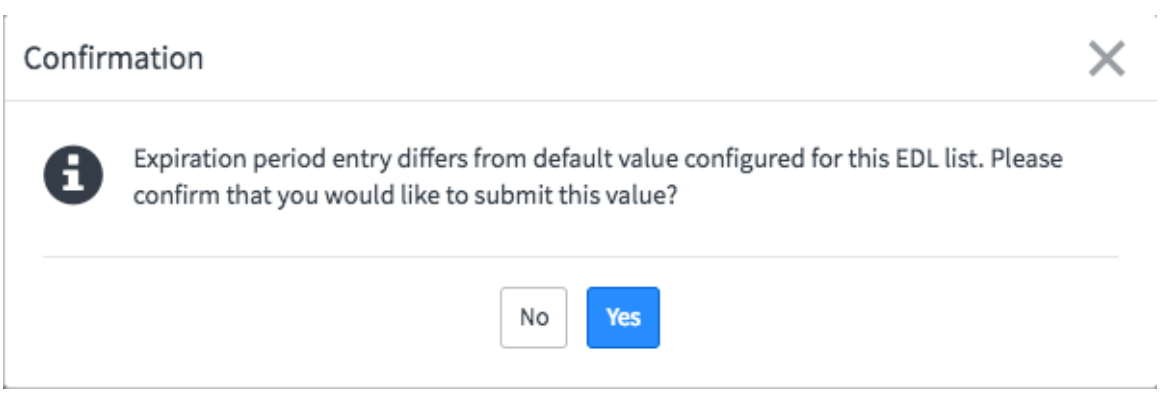


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type d'observable	Type d’observable pris en charge à partir de la boîte de dialogue.
Nom de l'EDL	EDL à laquelle vous souhaitez joindre l’entrée. **Remarque :** Sélectionnez l’EDL à laquelle vous souhaitez joindre l’entrée avant de définir la période d’expiration.
Activer le remplacement (sélectionné par défaut)	Rechercher le résultat ou la source. Une fois configurée, elle vous permet **d’entrer un résultat de recherche** et la source utilisée pour trouver les résultats. Ces champs sont généralement renseignés lors de la création d’un enregistrement d’incident de sécurité. Dans ce cas, il n’y a pas de résultat ou de source de recherche, et vous renseignez ces champs manuellement.
Rechercher un résultat	Sélectionnez **Inconnu** ou **Malicieux**.
Source	Source qui effectue une recherche de menace sur l’entrée EDL, par exemple, ThreatCrowd...
Période d’expiration	La période d’expiration héritée de l’EDL par défaut. Vous pouvez remplacer cette valeur, mais uniquement lors de la création de l’entrée. 0 indique que l’entrée EDL n’expire jamais. Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous saisissez. Vous pouvez entrer une valeur minimale de 1, mais il n’y a pas de valeur maximale. Par exemple, si vous saisissez 30 jours à 14h01 le 1er mai, l’entrée EDL expirera à 14h01 le 31 mai.

8. Cliquez sur **Envoyer**.
   Si vous avez modifié la période d’expiration par défaut de l’entrée EDL, une boîte de dialogue de confirmation d’avertissement s’affiche indiquant que la période diffère de l’EDL sélectionnée.



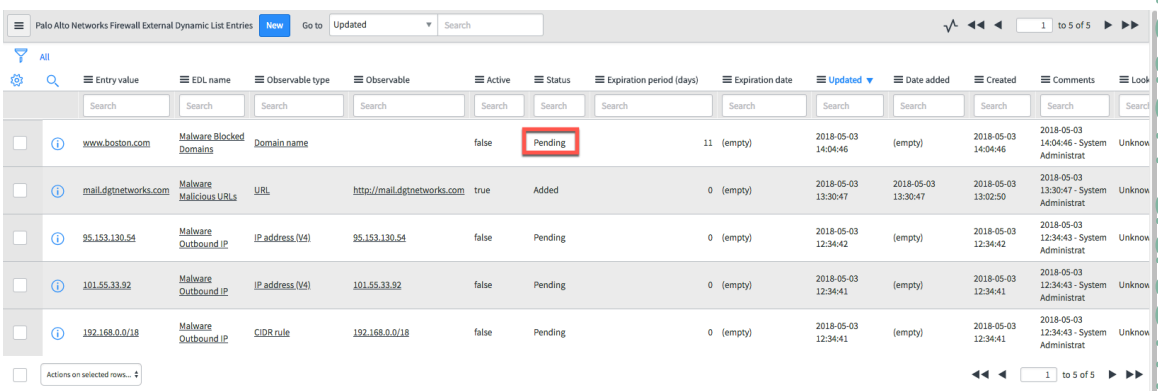
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Choisissez une option pour configurer la période d'expiration.

Option	Description
Oui	Confirme votre remplacement d'expiration, sauvegarde l'enregistrement et vous renvoie à la liste **Entrées de la liste dynamique externe du pare-feu Palo Alto Networks** . Si l'approbation par e-mail est configurée dans votre workflow, une demande d'approbation par e-mail est envoyée.
Non	Annule le remplacement. À ce stade, vous pouvez modifier la valeur de la **période d'expiration**. Après avoir modifié la valeur, cliquez sur **Soumettre** pour revenir à la liste **des entrées de la liste dynamique externe du pare-feu Palo Alto Networks** .

10. Si elle n'est pas affichée, accédez à la liste **des entrées de la liste dynamique externe du pare-feu Palo Alto Networks** et notez que l'état de l'entrée est En attente.



L'entrée est maintenant prête à être approuvée.

Que faire ensuite

Approuver les entrées EDL.

Information associée

Exceptions d'entrée EDL pour Palo Alto Networks - Next-Generation Firewall

Approuver les entrées EDL

Un processus d'approbation pour les entrées de liste dynamique externe (EDL) fait partie du workflow préconfiguré. Vous approuvez les entrées EDL avant qu'elles ne soient activées sur les EDL. Une fois que vous approuvez l'entrée EDL, le pare-feu récupère l'entrée et votre observable est bloqué à partir de ce moment-là.

Avant de commencer

Rôle requis : l'approbation des entrées EDL est affectée par défaut à sn_si.admin, mais cette autorisation peut être attribuée en fonction des besoins de votre organisation. Dans l'exemple suivant, l'administrateur dispose d'un ServiceNow AI Platform pouvoir d'approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

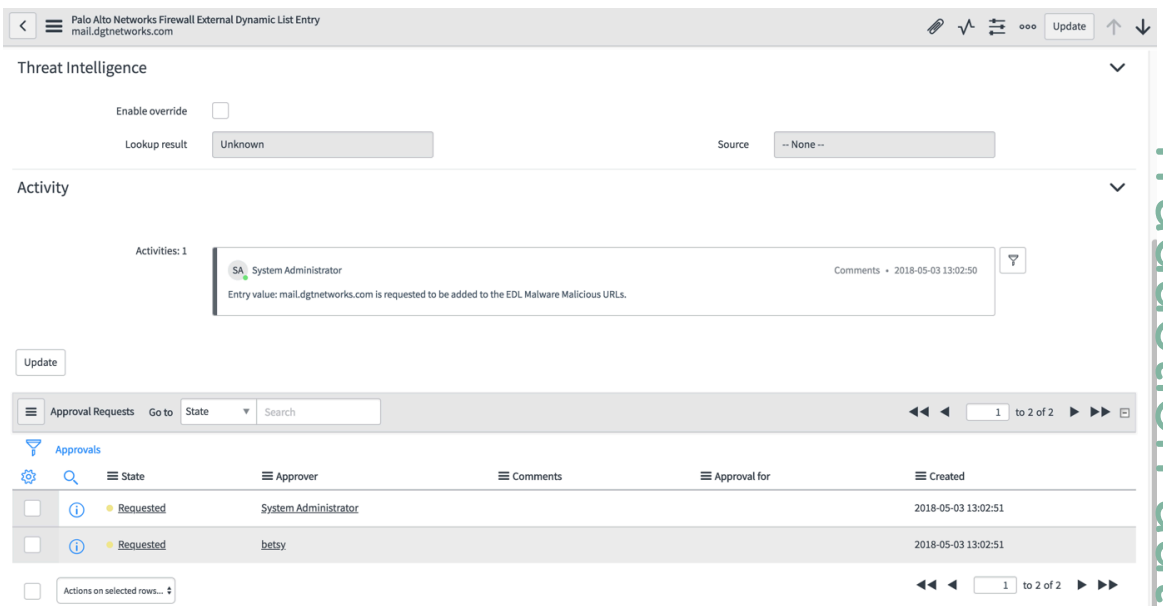
Pourquoi et quand exécuter cette tâche

Lorsque le processus d'approbation est activé, une entrée EDL n'est pas activée ou désactivée sur l'EDL tant qu'elle n'est pas approuvée.

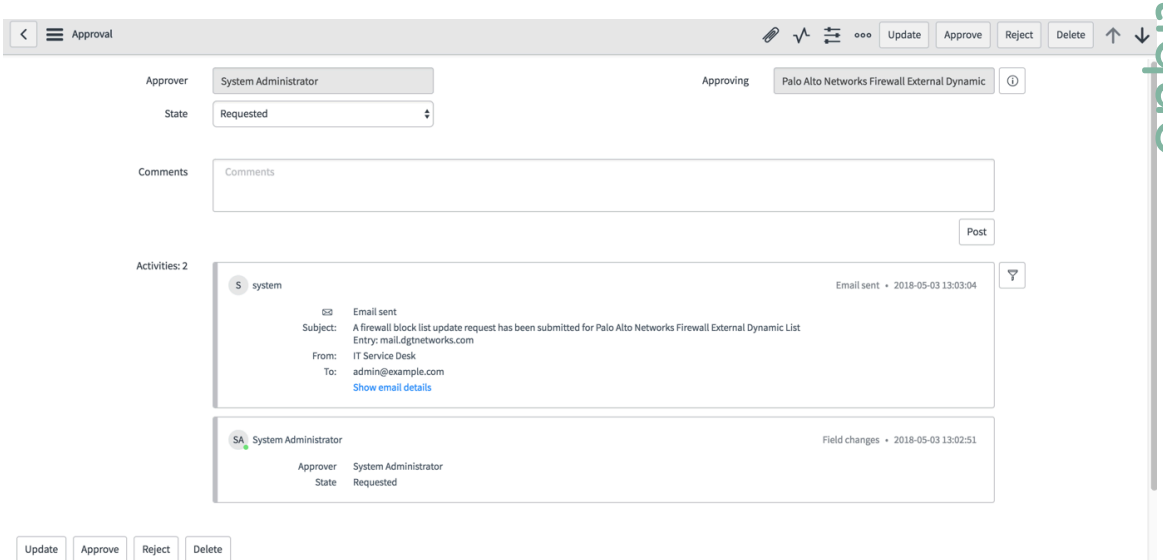
Procédure

1. Accédez à la **Tous** > **Intégration de Palo Alto Networks NGFW** > **Entrées de l'EDL du pare-feu** et ouvrez l'enregistrement EDL.
2. Sur l'enregistrement EDL, faites défiler jusqu'à la section Demandes d'approbation.

   Remarque : Si vous avez sélectionné des formulaires à onglets dans les paramètres système, la section apparaît sous forme d'onglet dans l'enregistrement.



3. Dans Demandes d'approbation, cliquez sur un élément dans la colonne **État** pour l'ouvrir. L'enregistrement de l'approbation s'affiche.



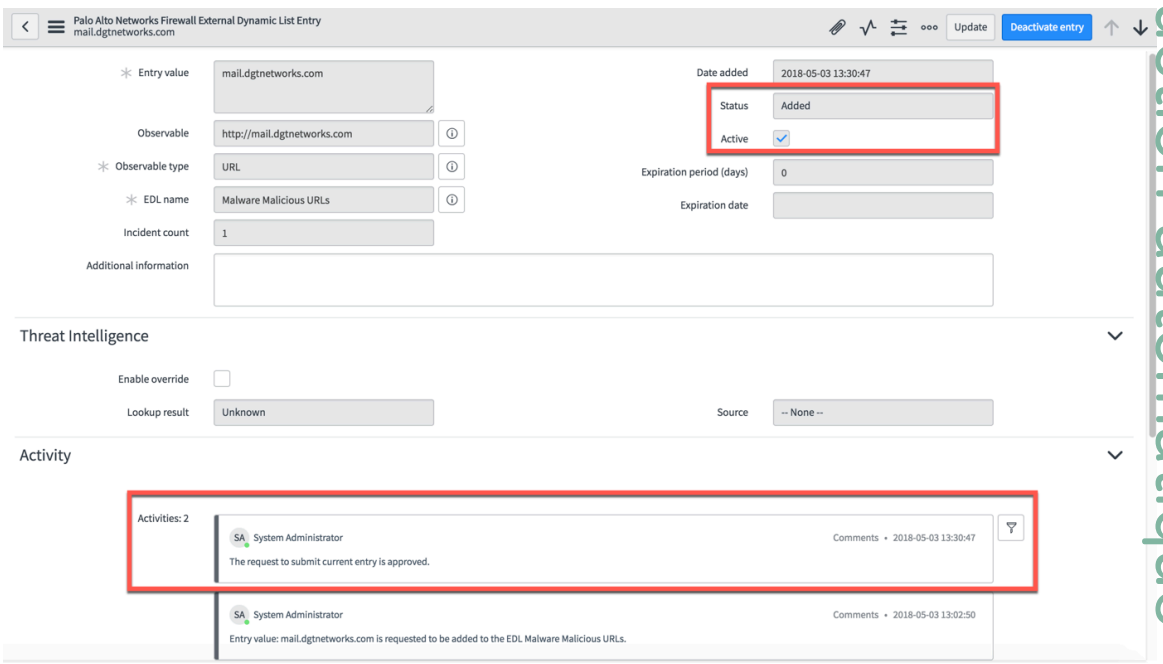
4. Choisissez une option pour approuver l'entrée EDL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Approuver	Sur l'enregistrement d'entrée, le champ **État**bascule sur Ajouté et la case **Actif** est cochée. Le bouton **Désactiver**est affiché et actif. Les notes de travail montrent que la de–mande d'entrée EDL a été approuvée.
Refuser	Sur l'enregistrement de l'entrée, le champ État bas-cule sur **Rejeté** et la case **Actif** est décochée, indi-quant que l'entrée n'est pas bloquée sur le pare-feu. Les notes de travail montrent que la de–mande d'entrée EDL a été rejetée.

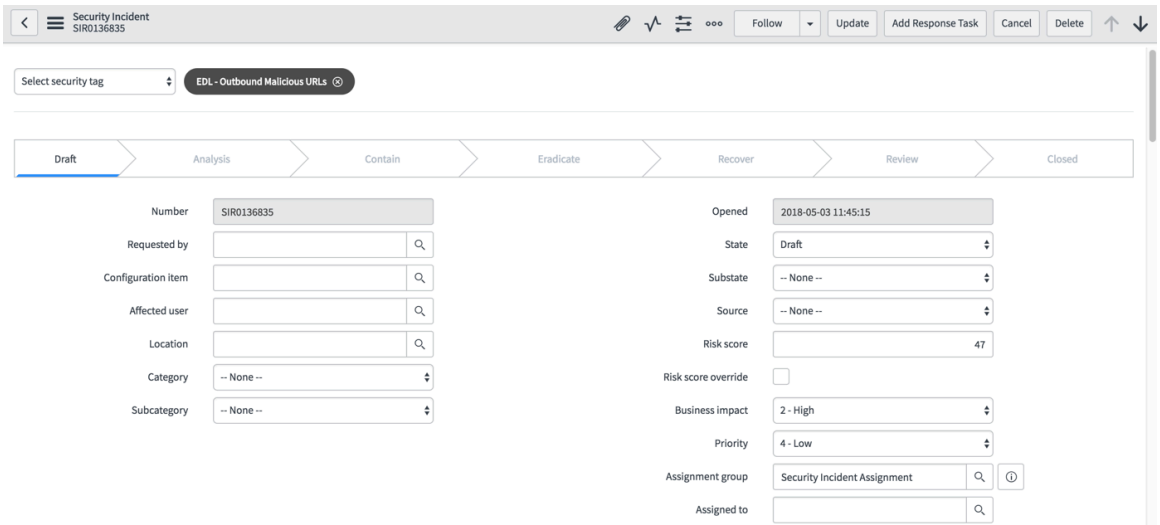
Une fois que vous avez approuvé l'entrée EDL et qu'elle est activée, l'EDL Palo Alto Networks - Next-Generation Firewall est récupérée après l'intervalle de récupération suivant. Une fois l'entrée récupérée, l'observable est bloqué à partir de ce moment-là. Dans la figure suivante, notez que la case Actif est cochée, que l'état est Ajouté et que les notes de travail indiquent que la demande a été approuvée.



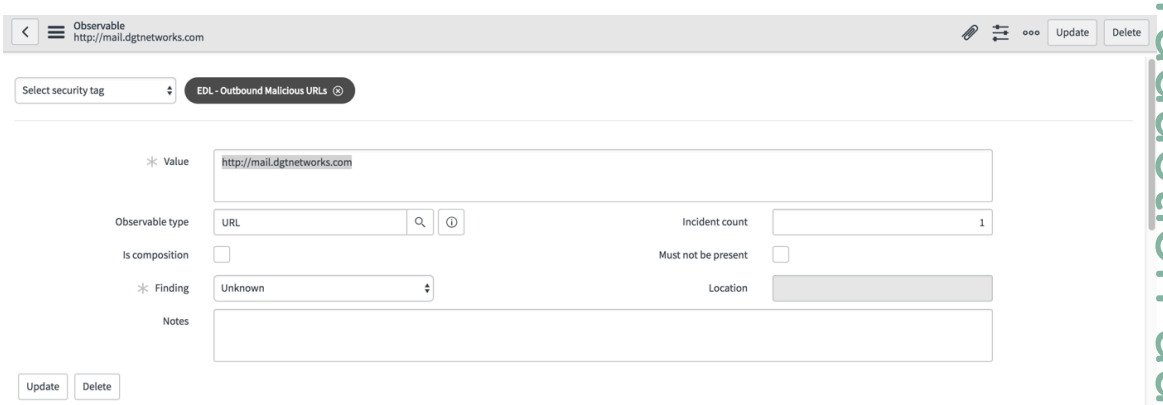
Une fois l'entrée EDL approuvée et activée, l'enregistrement de l'incident de sécurité est marqué d'une balise de sécurité. La balise s'affiche en haut de l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La balise de sécurité s'affiche également sur l'enregistrement de l'observable.



Exceptions d'entrée EDL pour Palo Alto Networks - Next-Generation Firewall

Il existe des restrictions pour l'ajout d'entrées de liste dynamique externe (EDL) aux EDL. En cas de doublon, de compatibilité ou de conflits CIDR (Classless Inter-Domain Routing) lorsque vous essayez d'ajouter des entrées EDL à des EDL, des messages d'erreur s'affichent pour vous aider à résoudre ces erreurs.

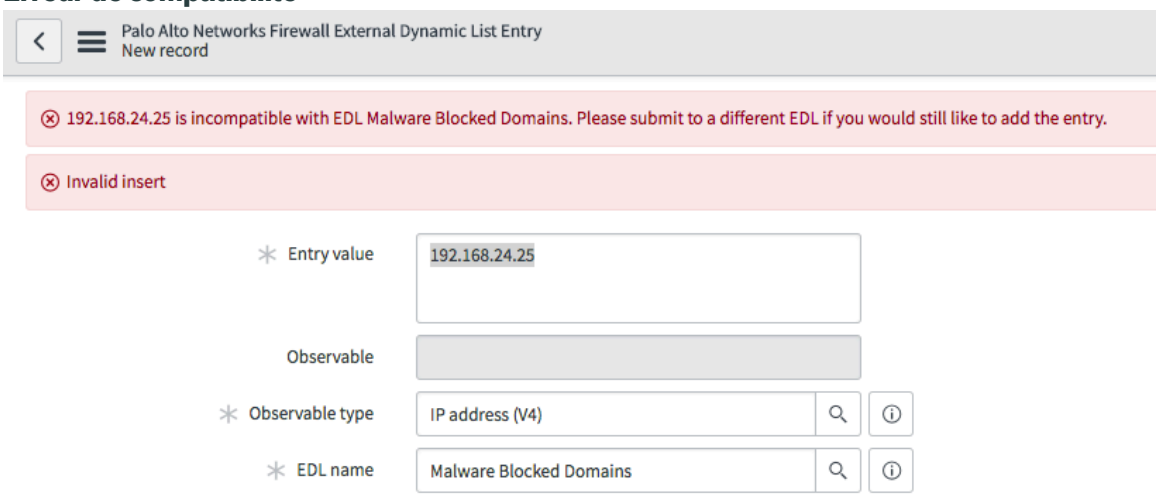
Exception de compatibilité

Chaque EDL n'accepte que les entrées compatibles avec son type d'observable. Si vous créez une EDL de domaine et que vous essayez d'y joindre une adresse IP observable, un message d'erreur incompatible s'affiche. Par exemple, une EDL de domaine ne peut accepter que des observables de domaine, comme illustré dans la figure suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

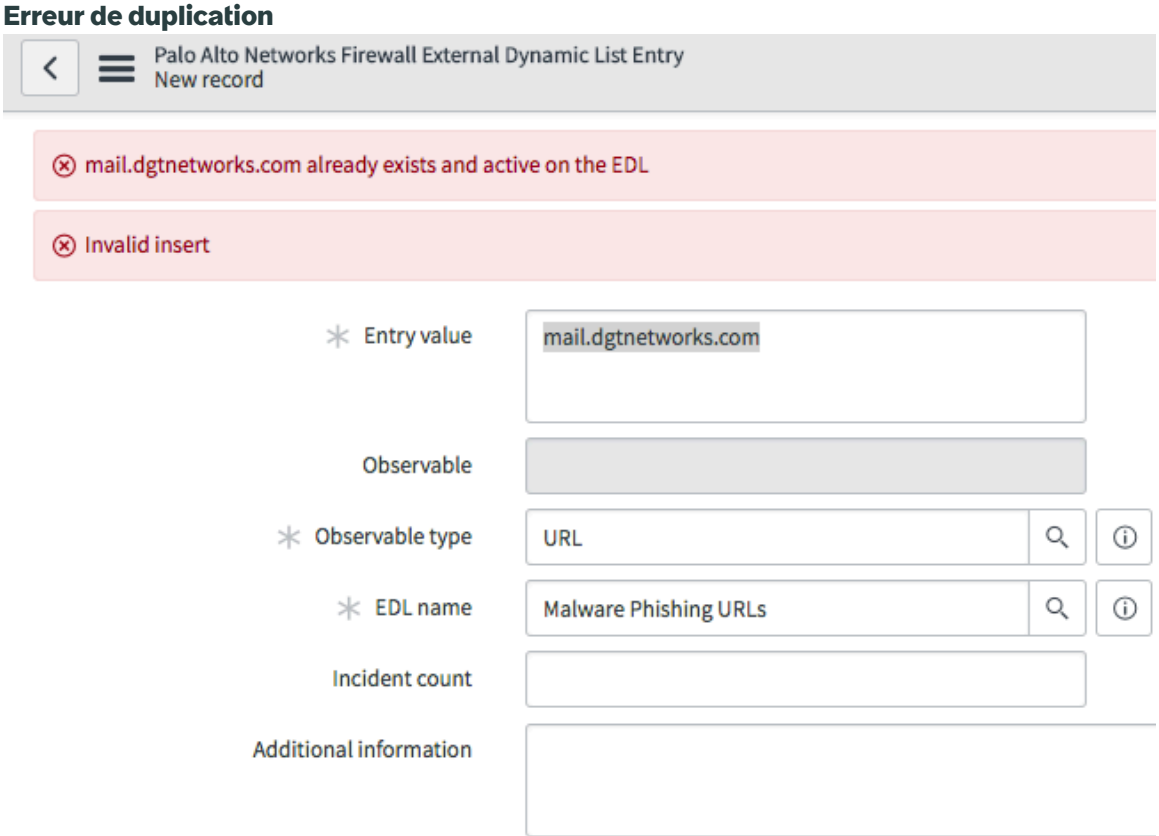
Erreur de compatibilité



Exception de duplication

Un observable ne peut pas être activé sur plusieurs EDL du même type d'observable. Si un observable d'URL est déjà activé sur une EDL d'URL et que vous essayez d'activer le même observable sur une EDL d'URL d'hameçonnage, un message d'erreur de duplication s'affiche.

Erreur de duplication



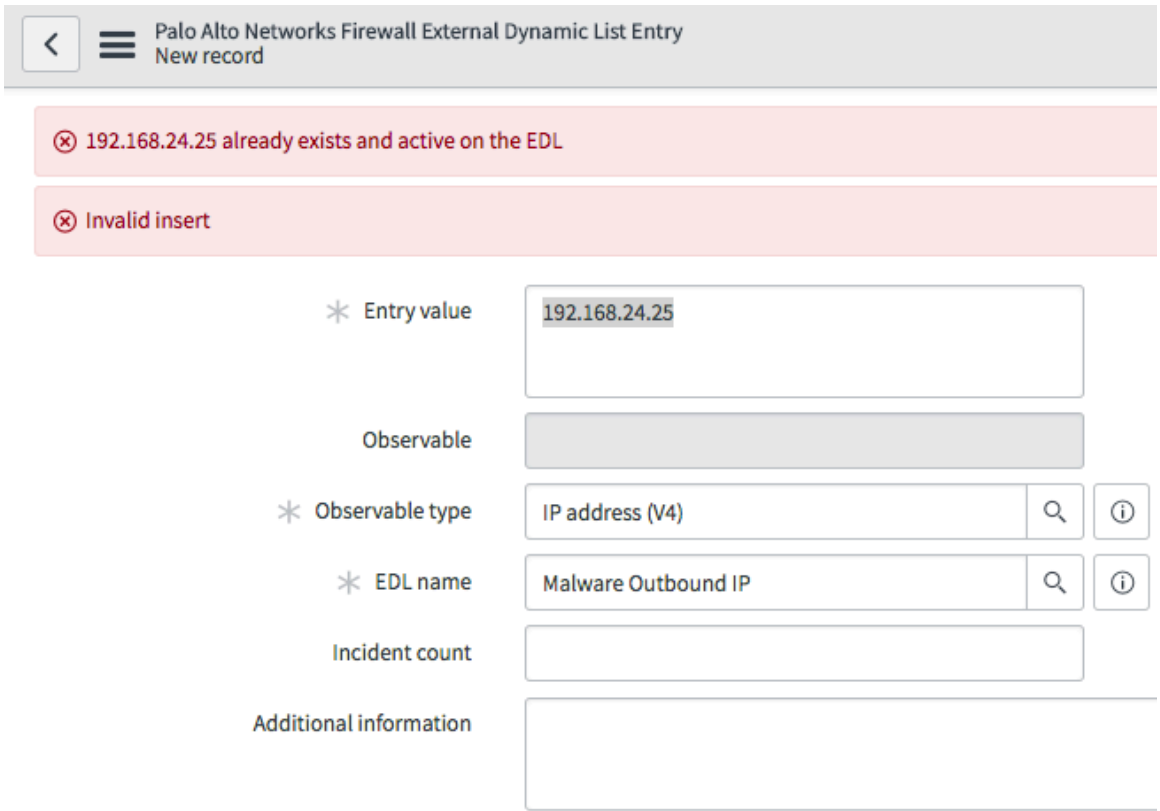
Exception CIDR (Classless Inter-Domain Routing)

Si vous tentez de joindre une seule adresse IP à une EDL et que cette adresse IP fait partie d'un observable CIDR déjà présent sur une EDL, une erreur de conflit CIDR s'affiche. Cette erreur indique que l'adresse IP unique est déjà incluse sur l'EDL dans le cadre de l'observable CIDR. Par exemple, 192.168.24.25 fait partie du bloc CIDR 192.168.0.0/22.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conflit CIDR



(Facultatif) Modifier le nom de la balise de sécurité pour Palo Alto Networks - Next-Generation Firewall

Si la case **Balise d'affichage** est cochée lorsque vous créez l'enregistrement Liste dynamique externe (EDL), vous pouvez modifier les noms et les couleurs des balises de sécurité. Les balises de sécurité vous aident à suivre les observables qui sont déjà bloqués.

Avant de commencer
Rôle requis : sn_si.admin

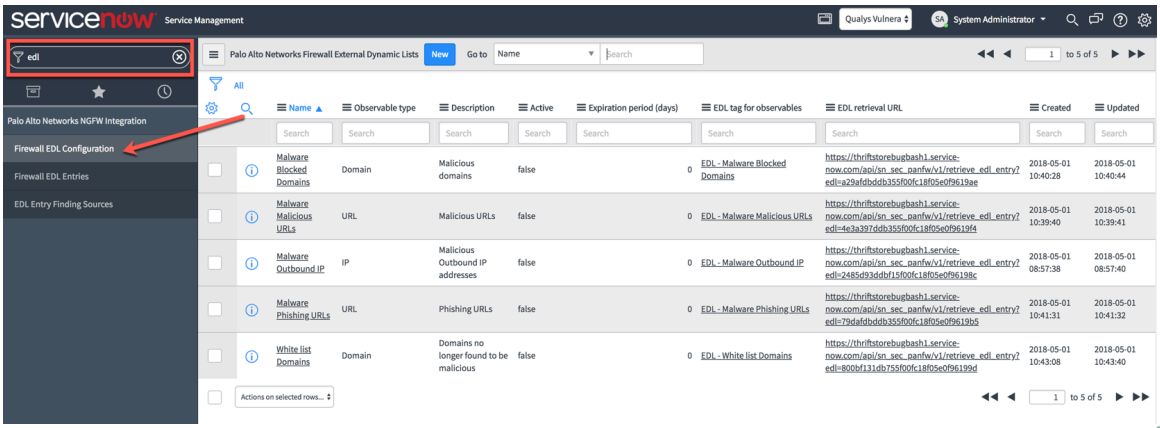
Pourquoi et quand exécuter cette tâche
Les balises de sécurité vous aident à identifier rapidement quels incidents de sécurité ont des observables sur une liste bloquée. Les balises vous aident également à déterminer si un observable est déjà bloqué ou s'il a été supprimé d'une EDL. Par défaut, la couleur de la balise de sécurité est le noir pour les entrées de la liste de blocs et le gris pour les entrées de la liste d'autorisation. Vous pouvez modifier les noms et les couleurs des balises pour vous aider à reconnaître plus facilement certaines balises.

Traduction automatique

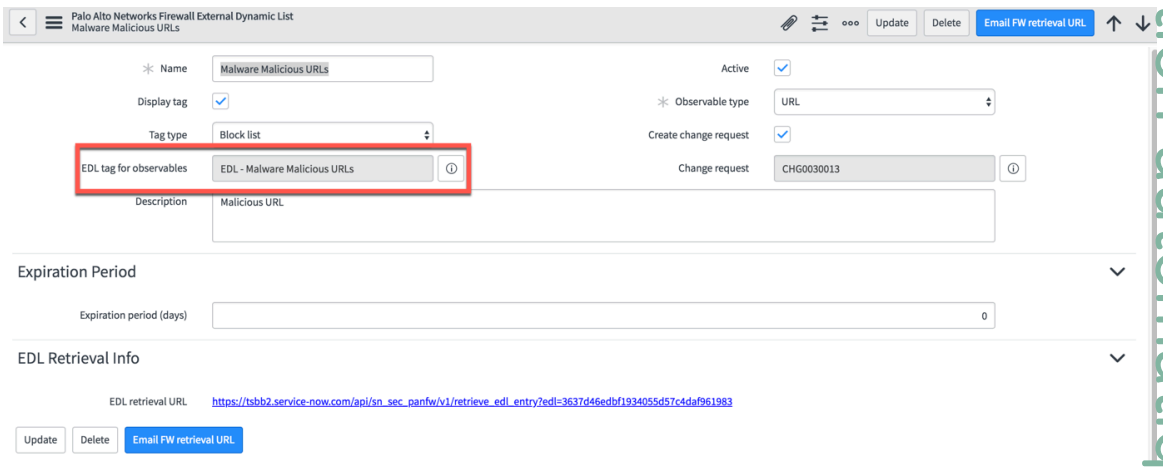
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

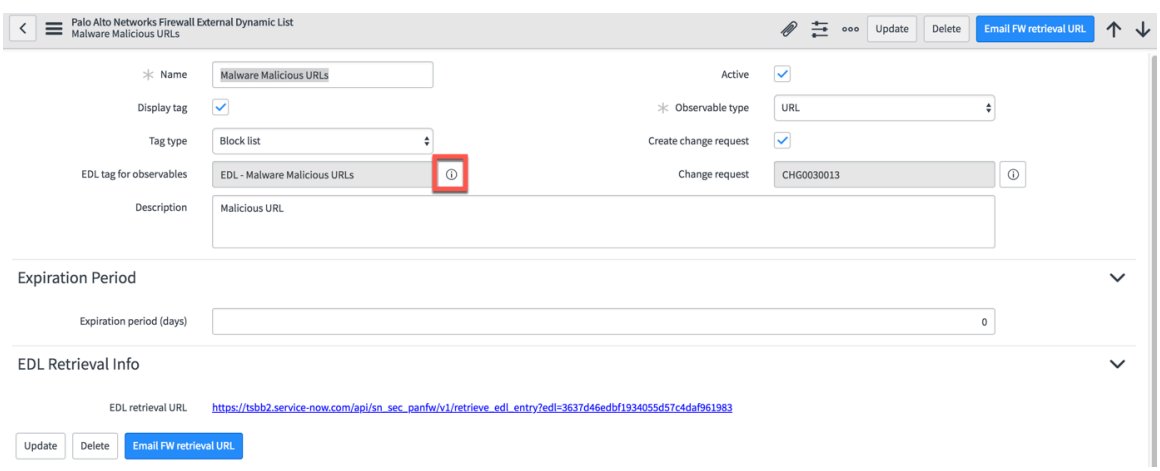
1. Accédez à la **Tous** > **Intégration de Palo Alto Networks NGFW** > **Configuration de l'EDL du pare-feu**.



2. Cliquez sur un élément dans la colonne **Nom** pour l'ouvrir
   L'enregistrement EDL s'affiche. Par défaut, le nom de la balise de sécurité est la même que celle que vous avez saisie dans le champ **Nom** de l'EDL lors de sa création. Par défaut, le nom comprend également un préfixe *EDL* , par exemple, EDL – Malware Malicious URLs.



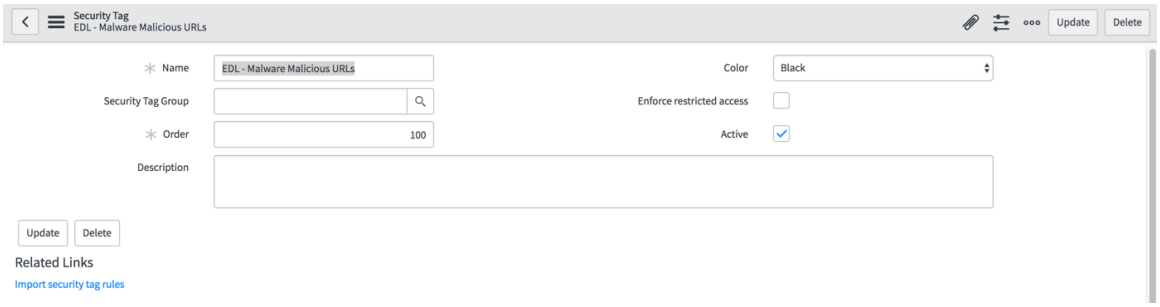
3. Cliquez sur l'icône d'informations (icône ⓘ) en regard de **la balise EDL pour les observables** , puis **sur Ouvrir l'enregistrement**.



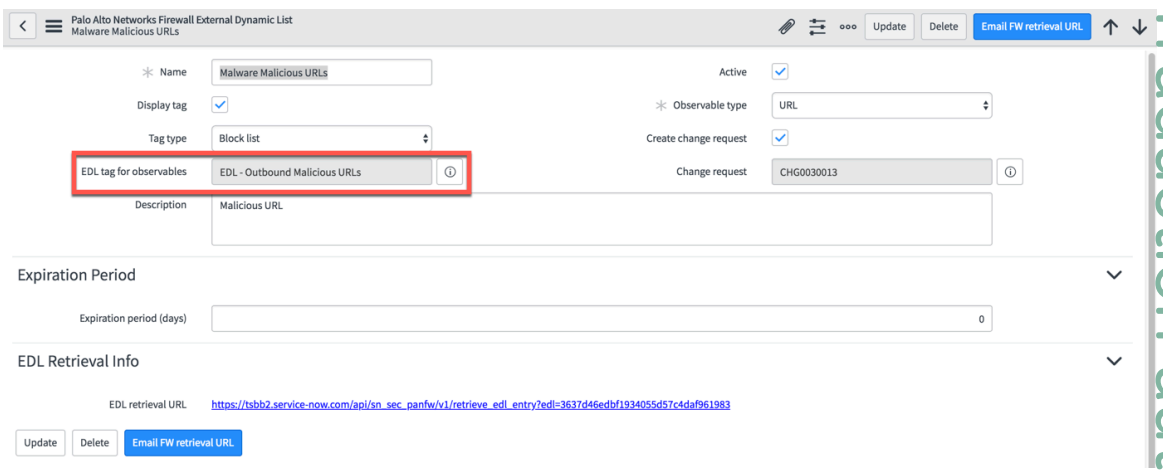
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

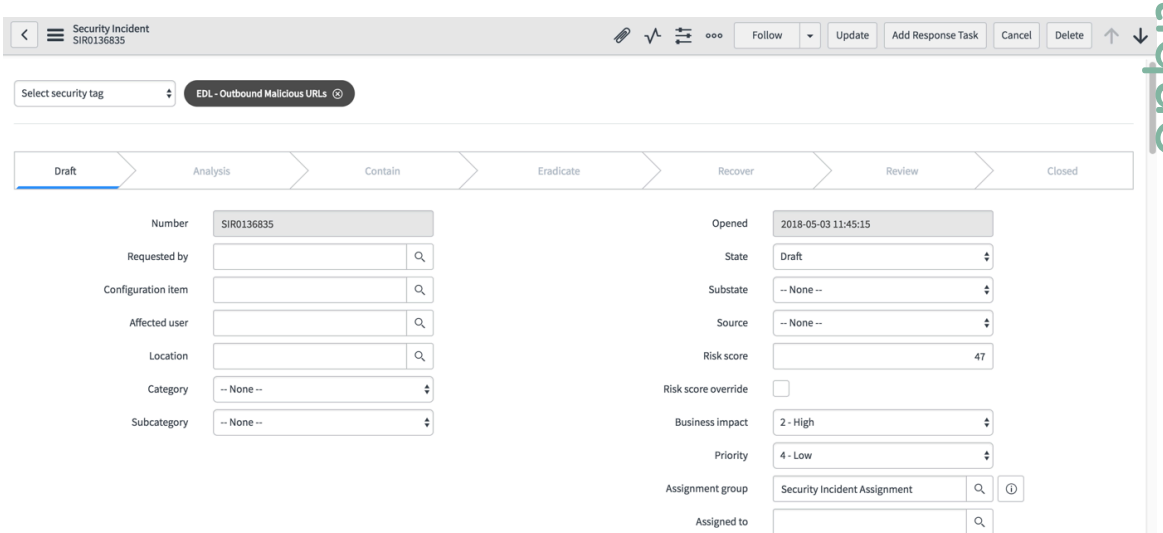
Le formulaire Balise de sécurité s'affiche.



4. Dans le champ **Nom** , modifiez le nom de la balise de sécurité et cliquez sur **Mettre à jour**.
   L'enregistrement EDL mis à jour s'affiche avec le nom de balise modifié. Dans l'exemple suivant, sortant a été ajouté au nom de la balise. Conservez le préfixe EDL dans votre nouveau nom de balise pour vous aider à identifier la balise associée à l'intégration Palo Alto Networks - Next-Generation Firewall .



Les balises de sécurité sont affichées pour chaque type d'observable (IP, URL, domaine) sur l'enregistrement d'incident de sécurité et l'enregistrement d'observable chaque fois que cet observable est ajouté à une EDL.



Si un observable a déjà été ajouté à une EDL et qu'une balise de sécurité est affichée sur un incident de sécurité pour cet observable, la balise de sécurité EDL s'affiche également automatiquement sur tous les enregistrements d'incident de sécurité ultérieurs qui sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

créés. Cette duplication vous indique que l'observable figure déjà sur une liste bloquée. Vous n'avez pas besoin d'ajouter cet observable et de le bloquer à nouveau.

Lorsqu'un observable n'est plus bloqué, aucune balise de sécurité ne s'affiche sur l'enregistrement d'incident de sécurité ou l'enregistrement d'observable. Dans ce cas, aucune balise de sécurité n'indique que la date d'expiration de l'observable peut être passée ou que l'observable a été désactivé d'une EDL.

Désinstaller

Si vous souhaitez désinstaller Palo Alto Networks - Next-Generation Firewall votre ServiceNow AI Platform instance et supprimer tous les restes de l'intégration, consultez le site de documentation pour obtenir des instructions sur la ServiceNow désinstallation des applications.

Avant de commencer

Rôle requis : Administrateur système (admin)

Voir Désinstaller les applications sur le site Web de la documentation produit ServiceNow .

Intégration PhishTank

PhishTank est un système communautaire de vérification de l'hameçonnage dans lequel les utilisateurs soumettent les menaces suspectées et les autres utilisateurs du système votent pour déterminer si les menaces d'hameçonnage sont légitimes. Lorsqu'ils sont intégrés au ServiceNow AI Platform Opérations de sécurité produit, les résultats des renseignements sur les menaces fournissent aux analystes des informations supplémentaires sur les incidents ou les enquêtes de sécurité liés au hameçonnage.

L'intégration PhishTank effectue des recherches sur les URL de sites d'hameçonnage potentiels.

Le workflow recherche les nouveaux observables à mesure qu'ils arrivent dans des incidents de sécurité. Si les observables sont d'un type reconnu par l'intégration de l'API, ils sont évalués. Les observables considérés comme malveillants sont balisés.

Installer et configurer PhishTank

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que l'application s'intègre PhishTank correctement à ServiceNow AI Platform Opérations de sécurité.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâches de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform à votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (administrateur) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	et vérifie les résultats attendus. Ce rôle a également accès au Opérations de sécurité module.
Procurez-vous une clé API.	Visitez le site web pour plus d'informations sur les PhishTank clés API et pour créer un compte : site web PhishTank .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Conditions requises pour la version Madrid et ultérieures Pour la version Madrid et les versions familiales ultérieures, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Orchestration du support de sécurité Pour en savoir plus sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Rôle requis : admin

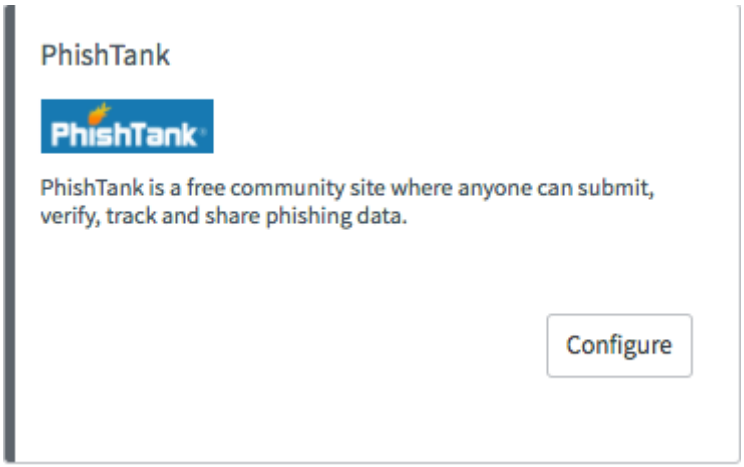
Procédure

1. Si vous n'avez pas installé l'application pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes d'installation.
2. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la PhishTank tuile.

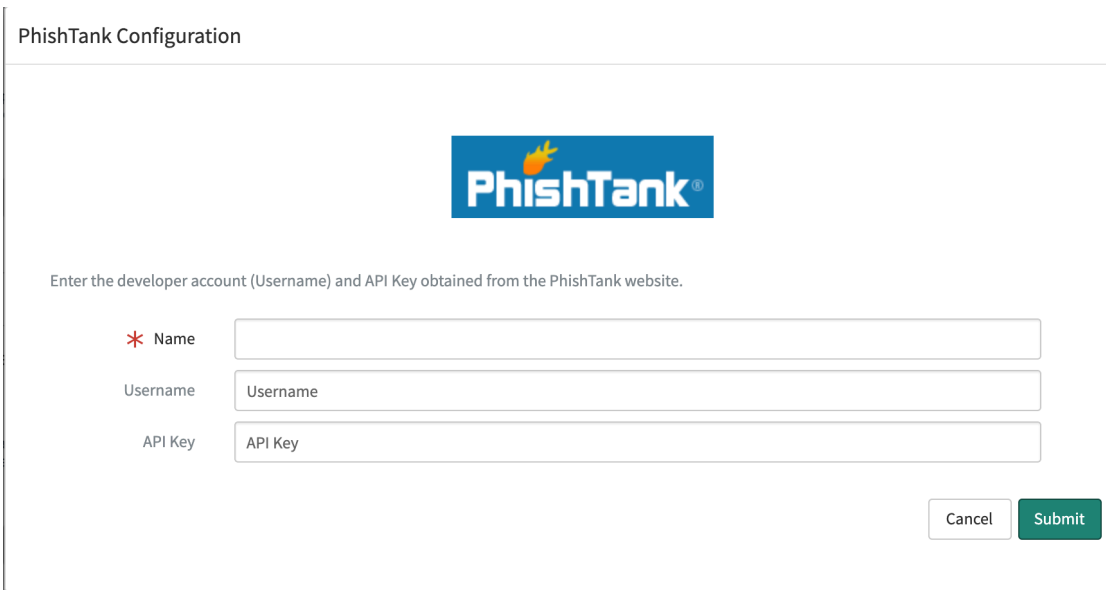
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Configurer**.



4. Dans la boîte de dialogue **Configuration de PhishTank** , saisissez le nom de la configuration, le nom d'utilisateur (compte de développeur créé dans PhishTank) et la clé API que vous avez obtenue sur le PhishTank site Web et cliquez sur **Soumettre**.



Traduction automatique

5. Vérifiez la réussite de la configuration.
La configuration est terminée avec succès à moins qu'un message d'erreur ne s'affiche.

Trouble?

Si un message d'erreur s'affiche pendant la configuration, la clé API PhishTank peut être non valide.

Vérifier les résultats attendus pour PhishTank

Les observables sont générés automatiquement par un incident de sécurité et analysés par l'application. Les résultats de la recherche sont affichés dans l'onglet Résultats de la recherche de menace au bas de l'enregistrement d'incident de sécurité.

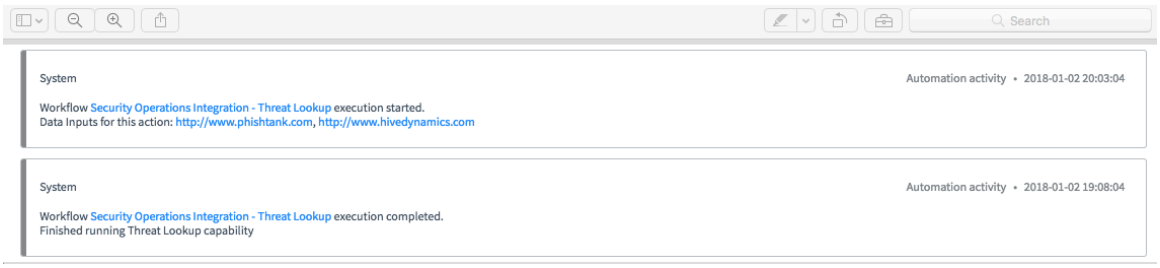
Avant de commencer

Rôle requis : sn_si.analyst

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez le formulaire d'incident de sécurité avec lequel vous travaillez et vérifiez que la recherche a été exécutée avec succès.

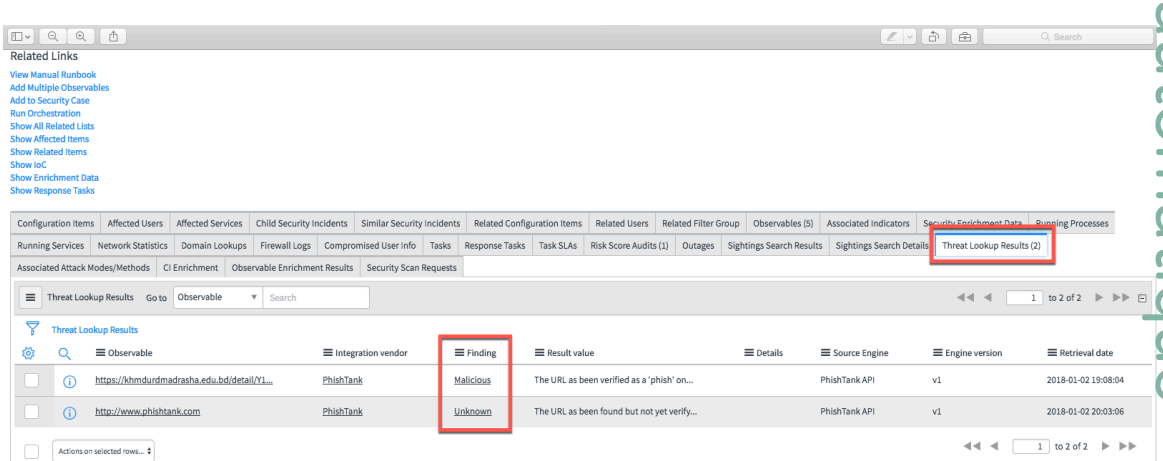


   Une fois l'application configurée, le flux se lance automatiquement lors de la création de l'incident. L'état d'exécution et d'achèvement de la recherche est ensuite affiché dans les notes de travail de l'enregistrement d'incident de sécurité.

2. Passez en revue les notes de travail pour plus d'informations et sur la procédure à suivre si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

3. Accédez au bas de l'incident de sécurité et cliquez sur le lien connexe **Afficher toutes les listes connexes** .

   Remarque : Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres système. Si les formulaires à onglets ne sont pas affichés, cliquez sur l'icône d'engrenage Paramètres dans le coin supérieur droit de la bannière. Dans la boîte de dialogue **Paramètres système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que **Formulaires à onglets** et **Avec le formulaire** sont sélectionnés.



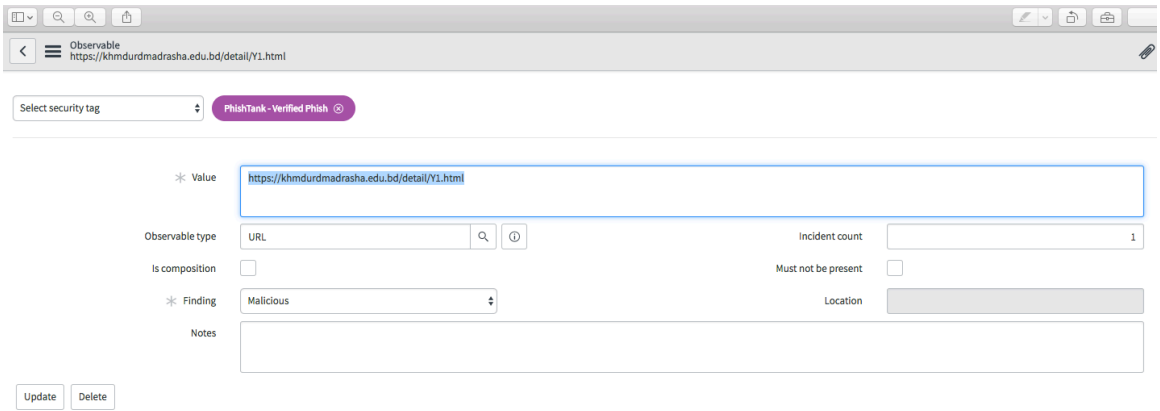
   L'onglet Résultats de la recherche de menace au bas de l'enregistrement d'incident de sécurité affiche les résultats de la recherche.

   La colonne **Résultat** affiche Inconnu pour les enregistrements qui ne sont pas déterminés comme malveillants. Pour les résultats correspondant à malveillant, Malveillant s'affiche dans la colonne **Résultat** .

4. Dans la colonne **Observable** , cliquez sur un observable pour ouvrir un enregistrement et afficher plus d'informations.

Traduction automatique

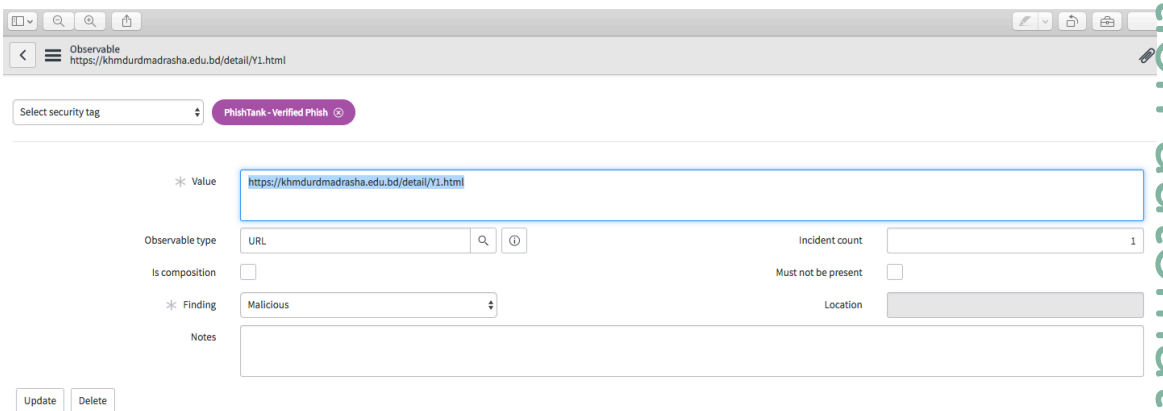
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Sur l'enregistrement de l'observable, pour les recherches correspondantes malveillantes, le champ **Recherche** est affiché. L'observable est étiqueté avec la Renseignements sur les menaces source qui l'a trouvé malveillant, dans ce cas, l'application PhishTank .

5. Pour afficher les données brutes, revenez à l'incident de sécurité et cliquez sur l'icône d'informations bleues en regard d'un observable.

6. Dans la fenêtre qui s'affiche, cliquez sur **Ouvrir l'enregistrement**.



Le lien créé par l'API et le champ **Recherche** affiché avec les résultats.

Traduction automatique

Trouble?

Si vous ne voyez pas de résultats sous **l'onglet Résultats de la recherche de menace** , vérifiez que l'observable est d'un type pris en charge pour la recherche par l'intégration.

(Facultatif) Joindre manuellement un observable pour PhishTank

Vous pouvez joindre manuellement des observables à un incident de sécurité. Vous attachez manuellement des observables lorsque vous souhaitez effectuer des recherches de menaces sur des observables qui ne sont pas joints à un incident de sécurité lors du déclenchement de l'événement initial. En outre, vous pouvez effectuer cette tâche lorsque vous souhaitez obtenir plus d'informations sur un observable connexe.

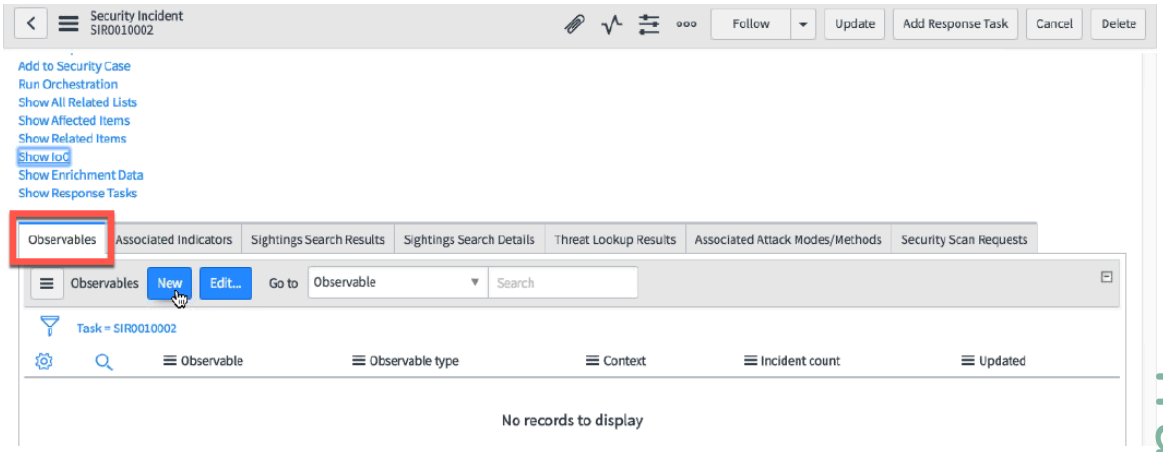
Avant de commencer

Rôle requis : sn_si.analyst

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

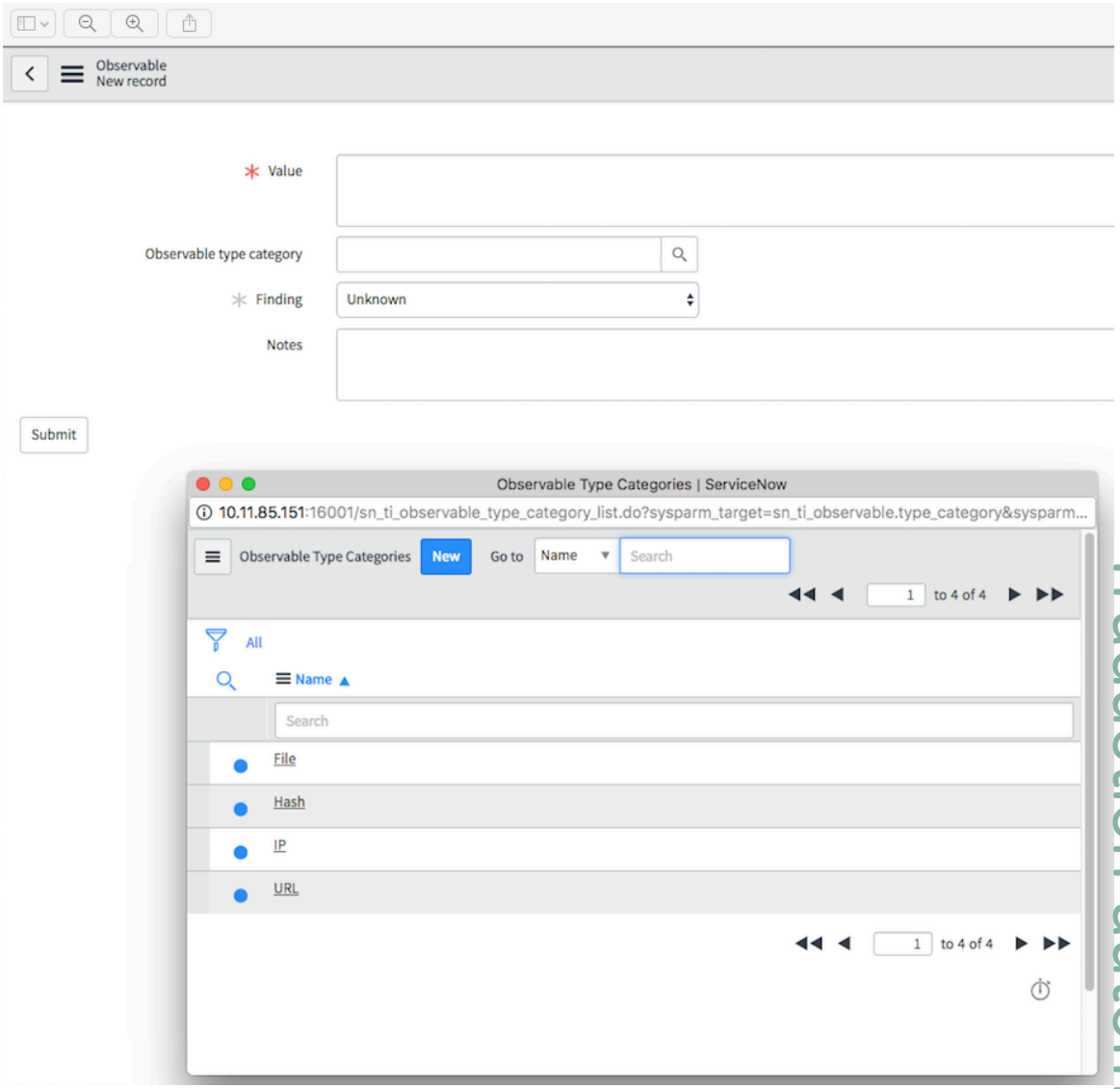
1. Accédez à votre incident de sécurité ouvert.
2. Dans l'enregistrement d'incident de sécurité ouvert, cliquez sur le lien **Afficher l'IoC**dans des **liens connexes** pour afficher l'onglet **Observables** .



3. Cliquez sur **Nouveau**.
   Le formulaire Observable s'affiche.
4. Dans le champ **Valeur** , entrez une URL.
5. Cliquez sur l'icône de recherche puis, dans la boîte de dialogue **Catégories de type d'observable** , cliquez sur **URL** dans la liste pour remplir le champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

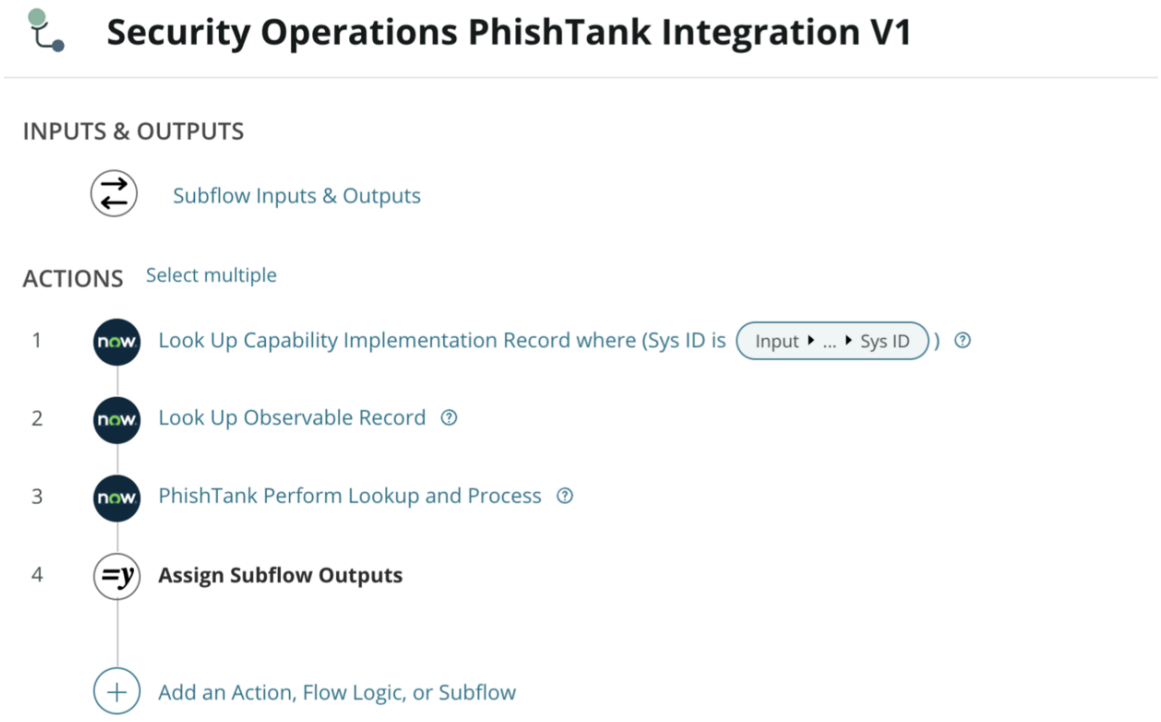


6. Cliquez sur **Envoyer**.

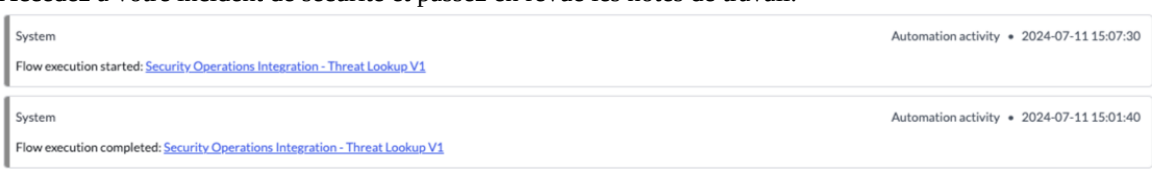
Le flux se lance et recherche le nouvel observable. L'état d'exécution et d'achèvement est affiché dans la section des notes de travail de l'enregistrement d'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

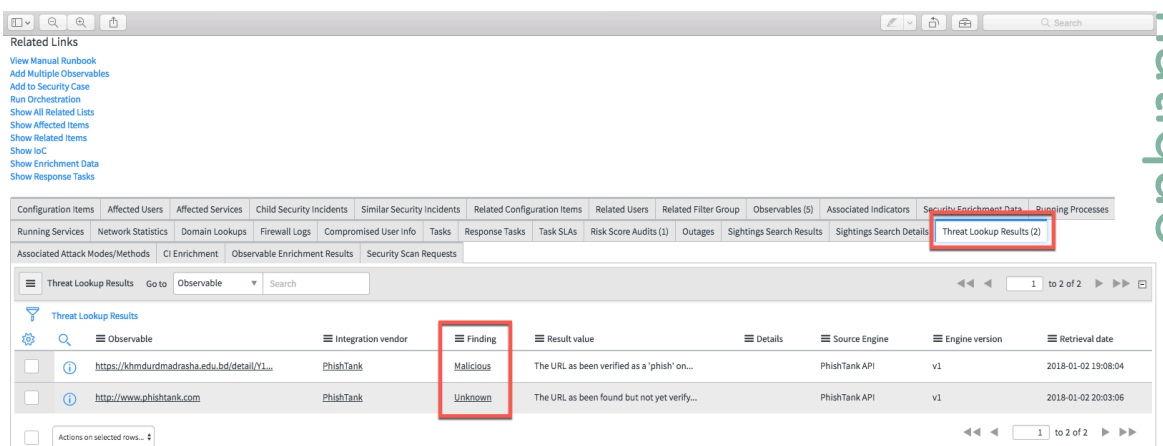


7. Accédez à votre incident de sécurité et passez en revue les notes de travail.



8. Cliquez sur le lien connexe **Afficher toutes les listes connexes** en bas de l'incident de sécurité.

9. Cliquez sur **l'onglet Résultats de la recherche de menace** pour afficher les résultats.



10. Dans la colonne **Observable** , cliquez sur l'icône d'information bleue en regard d'un observable donné pour obtenir plus d'informations et des données brutes.

11. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement**.

Traduction automatique

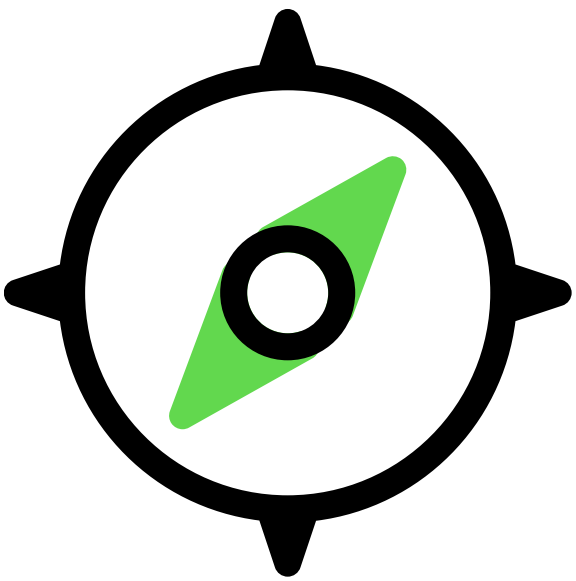
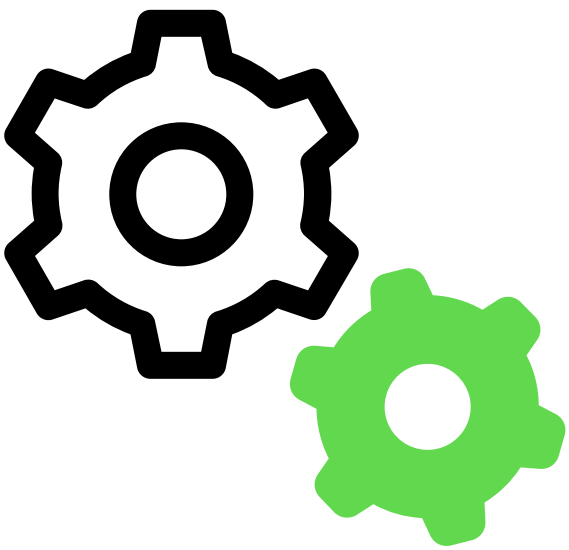
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Trouble?
Passez en revue les notes de travail pour plus d'informations et sur la procédure à suivre si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

Proofpoint Intégration pour Security Operations

L'intégration Proofpoint SIR prend en charge l'ingestion d'événements à partir de Proofpoint. SIR crée un incident pour chaque événement ingéré que les analystes peuvent examiner ou sur lequel ils peuvent travailler.

Premiers pas

Explorer	Configurer
	
En savoir plus sur l'intégration Proofpoint	Configurer pour l'espace Proofpoint de travail SIR

Traduction automatique

Découverte de Proofpoint l'intégration pour Security Operations

Vous pouvez configurer des profils d'événements dans SIR pour ingérer des événements à partir de Proofpoint. SIR crée un incident pour chaque événement ingéré que les analystes peuvent examiner ou sur lequel ils peuvent travailler.

Proofpoint Intégration pour les utilisateurs de Security Operations

Utilisateurs

Utilisateur	Description
Administrateur de sécurité	Créez des profils d'événement pour filtrer les événements ingérés. SIR crée des incidents pour ces événements ingérés.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Proofpoint Avantages de l’intégration pour Security Operations

Proofpoint Avantages de l’intégration pour Security Operations

Avantage	Fonctionnalité	Utilisateurs
Transférez les données d’événement dans votre instance et créez des incidents de sécurité. Examinez les incidents de sécurité à partir d’un emplacement unique pour détecter les événements jugés suspects ou malveillants.	Si les e-mails livrés et les clics autorisés sont ensuite jugés malveillants, il y a de fortes chances que ces messages aient été ouverts et utilisés par vos employés. Pour suivre ces messages à examiner, créez automatiquement des incidents de sécurité en fonction des profils d’événements que vous créez et configurez pour le trafic de messages pour l’intégration. En outre, vous pouvez également activer la création d’incidents de sécurité pour les messages et les clics bloqués à des fins d’audit.	Gestionnaires

Ce qu'il faut explorer ensuite

Pour en savoir plus sur la configuration et l'utilisation de Proofpoint, consultez :

- Configuration de Proofpoint l’intégration pour Security Operations
- Examiner les paramètres d’intégration de Proofpoint
- Afficher le tableau de bord d’analyse Proofpoint

Configuration de Proofpoint l’intégration pour Security Operations

Configurez votre implémentation de Proofpoint l’intégration pour Security Operations.

Vue d'ensemble de la configuration

1. Installer et configurer Proofpoint l’intégration.

   Téléchargez, installez et activez l’application d’intégration.

2. Créer un profil d’événement pour Proofpoint l’intégration pour Security Operations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créez un profil d'événement pour identifier les événements que vous souhaitez importer à partir du produit et les conditions que vous souhaitez utiliser pour créer des incidents de Proofpoint sécurité à partir des données importées.

3. Configuration de Proofpoint l'intégration pour Security Operations

   Passez en revue les paramètres d'intégration pour la création des profils d'événement.

Installer et configurer Proofpoint l'intégration

Installez et configurez l'application Proofpoint Integration for Security Operations à partir de ServiceNow® Store sur votre ServiceNow AI Platform instance.

Avant de commencer
Rôle requis : sn_si_admin

Procédure

1. Téléchargez l'intégration pour l'application Proofpoint à Opérations de sécurité partir de et ServiceNow® Store installez-la.
   Pour plus d'informations, voir Installer une application ServiceNow Store .
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Localisez l'intégration pour Opérations de sécurité la Proofpoint vignette et sélectionnez **Configurer**.
4. Remplissez les champs du formulaire.

Proofpoint Formulaire Configuration de l'intégration

Champ	Description
Nom	Nom de la configuration de l'intégration pour Opérations Proofpoint de sécurité.
Principal du service	Nom d'utilisateur du Proofpoint locataire.
Clé secrète	ID du Proofpoint locataire.

5. Sélectionnez **Soumettre**.

Résultats
Une fois que vous avez validé et soumis la configuration, l'intégration est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

Créer un profil d'événement pour Proofpoint l'intégration pour Security Operations

Créez un profil d'événement pour identifier les événements que vous souhaitez importer à partir du Proofpoint produit.

Pourquoi et quand exécuter cette tâche
Vous créez un profil d'événement en configurant les types d'événements, les mappages et les calendriers d'importation. Une barre de progression sur la page affiche toutes les étapes et est mise en surbrillance pour la configuration actuellement active.

Avant de commencer
Rôle requis : sn_si_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intégration SIR à Proofpoint** > **Profil des événements Proofpoint**.
2. Sur la page Profils d'événements, sélectionnez **Nouveau**.
3. Remplissez les champs du formulaire.

   La barre de progression s'affiche en commençant par Nom.

Formulaire de profil Proofpoint

Champ	Description
Nom	Nom du profil d'événement. Envisagez d'utiliser un nom qui inclut le type d'événement associé : ○ Clics bloqués ○ Clics autorisés ○ Messages bloqués ○ Messages remis
Source	La source configurée pour l'intégration sur la page Configurations d'intégration.
Ordre	Ordre dans lequel ce profil est exécuté. La valeur par défaut est 100.
Actif	Option permettant d'activer le profil.
Description	Description facultative pour ce profil d'événement.

4. Sélectionnez **Continuer**.
5. Choisissez un ou plusieurs types d'événements en les déplaçant de la colonne **Disponible** vers la colonne **Sélectionné** .
   Les types d'événements disponibles sont les suivants :
   - Clics bloqués
   - Clics autorisés
   - Messages bloqués
   - Messages remis
6. Sélectionnez **Continuer**.

   Les étapes de configuration liées au ou aux types d'événements sélectionnés s'affichent dans la barre de progression.

   Les valeurs des champs sources sont fournies à partir des données de protection contre les attaques ciblées (TAP) dans votre environnement à titre de référence.

   Le mappage par défaut des données des champs sources aux champs cibles s'affiche sur la page. Les données de base sont incluses à titre indicatif, mais vous pouvez modifier ce mappage.

7. **Facultatif :** Sélectionnez l'icône **f(x)** pour afficher les traductions par défaut incluses avec l'application.

   (Optional) Les valeurs multiples d'un champ sont séparées par des virgules.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Sélectionnez **Continuer**.
9. Dans la page Filtrage et agrégations, configurez les propriétés dans la table suivante.

Propriétés de filtrage et d'agrégation

Option	Description
Filtre basé sur les conditions pour les événements de messages	Option permettant d'activer le filtrage basé sur les événements du message.
Conditions de filtre d'événements du message	Conditions de filtre d'événement de message.
Filtre basé sur les conditions pour les événements de clics	Option permettant d'activer le filtrage basé sur les événements de clic.
Cliquer sur les conditions de filtre d'événements	Cliquez sur les conditions de filtre d'événement.
Conditions d'agrégation	Option permettant d'ajouter un incident entrant à un incident de sécurité ouvert au lieu d'en créer un nouveau.
Champs d'incident avec des valeurs correspondantes	Ajoutez les champs dont les Réponse aux incidents de sécurité valeurs doivent correspondre pour qu'un incident soit inclus dans une agrégation.
Enregistrer la note de travail pour le nouvel incident	Option permettant de consigner des notes de travail sur le parent Réponse aux incidents de sécurité.
Activer la relation ThreatID	Option permettant d'activer l'agrégation de tous les incidents dont les ThreatIDs correspondent.

10. Sélectionnez **Continuer**.
11. Sélectionnez l'un des types d'importation et la fréquence à laquelle vous souhaitez importer les données d'événement.

Option	Description
Ingestion des événements en cours	Option d'importation d'événements à intervalles réguliers définis avec une date de début, une date de fin et l'intervalle d'interrogation en minutes. ○ **Incrémentation de l'interrogation (minutes)** : intervalle en minutes entre les importations ○ **Définir le délai d'ingestion des événements initiaux** ○ **Délai d'ingestion initial de l'entrée**
Récupération ponctuelle	Option pour importer les événements une seule fois sur la base de la date configurée. Tous les événements de la date sélectionnée sont importés. Indiquez une date de début pour l'importation de l'événement (**Depuis la date**).

12. Sélectionnez **Finish** (Terminer).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Le profil d'événement nouvellement créé est inclus dans la liste des profils d'événement existants sur la page Profils d'événements.

Examiner les paramètres d'intégration de Proofpoint

Examinez les paramètres d'intégration de Proofpoint afin de pouvoir modifier les propriétés système de votre environnement.

Avant de commencer
Rôle requis : sn_si_admin

Procédure

1. Accédez à la **Tous** > **Intégration SIR à Proofpoint** > **Paramètres d'intégration de Proofpoint**.
2. Modifiez les paramètres suivants.

Paramètres d'intégration de Proofpoint

Nom de la propriété	Description
Délai d'expiration pour les appels restAPI. sn_sec_proofpoint.http_timeout	Délai (en secondes) pour l'extraction des données à partir des appels d'API. Type : entier Valeur par défaut : 3 000
Niveau de la connexion : débogage, informations, avertissement, erreur sn_sec_proofpoint.logging_verbosity	Niveau de verbosité du journal de l'application, c'est-à-dire le nom du type d'information. Vous pouvez mettre à jour la valeur en fonction des options suivantes : ○ erreur ○ avertir ○ infos ○ déboguer Valeur par défaut : info
Appliquer une limite au nombre d'événéments Proofpoint qui peuvent être regroupés en un seul incident. sn_sec_proofpoint.max_agrégations_per_si	Le nombre maximal d'événements Proofpoint qui peuvent être regroupés en un seul incident. Type : entier Valeur par défaut : 100
Appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés dans la période de 24 heures. sn_sec_proofpoint.max_si_per_day	Nombre maximal d'incidents pouvant être créés en 24 heures. Type : entier Valeur par défaut : 1 000
Nombre de jours que nous devons utiliser dans l'appel d'API pour les meilleurs cliqueurs, VAP. sn_sec_proofpoint.default_days	Nombre de jours de données à extraire pour les meilleurs cliqueurs et VAP. Vous pouvez également mettre à jour la valeur dans les options suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété	Description
	○ 14 ○ 30 ○ 90.0 Type : entier Valeur par défaut : 90
Marqueur booléen, s'il est activé, effectue un appel d'API et renseigne les détails Topclickers. sn_sec_proofpoint.call_topclickers_api	Activez l'option pour activer et extraire les données du clicker supérieur. Type : booléen Valeur par défaut : true
Ce marqueur booléen, s'il est activé, effectue un appel d'API et renseigne les détails VAP. sn_sec_proofpoint.call_vap_api	Activez l'option pour activer et extraire les données VAP. Type : booléen Valeur par défaut : faux
Il s'agit de restreindre le nombre maximum d'utilisateurs à afficher pour les topClickers, les utilisateurs VAP. sn_sec_proofpoint.maxresults	Nombre maximal d'utilisateurs à afficher pour les meilleurs cliqueurs et les utilisateurs VAP. Type : entier Valeur par défaut : 100
Active/Désactive l'utilisation de la période de chevauchement lors de l'interrogation planifiée des événements Proofpoint. sn_sec_proofpoint.allow_overlap	Activez ou désactivez la période de chevauchement lorsque l'interrogation planifiée est configurée. Type : booléen Valeur par défaut : faux
Temps de chevauchement, en minutes, à utiliser pendant l'interrogation programmée des événements Proofpoint lorsque le chevauchement est activé. sn_sec_proofpoint.overlap_time	Temps de chevauchement, en minutes, lorsque l'interrogation planifiée est configurée. Type : entier Valeur par défaut : 5

3. Sélectionnez **Enregistrer**.

Résultats
Configure les paramètres d'intégration avec de nouvelles valeurs.

Afficher le tableau de bord d'analyse Proofpoint

Le Proofpoint tableau de bord d'analyse fournit des détails sur les utilisateurs VAP et les meilleurs cliqueurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

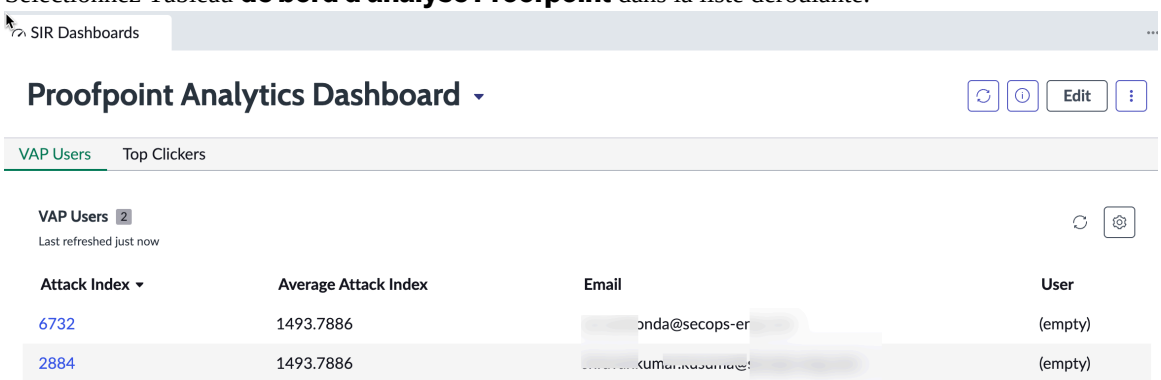
Les utilisateurs principalement ciblés par les attaques de sécurité sont considérés comme des utilisateurs VAP. Les employés qui cliquent fréquemment sur des liens suspects et de phishing sont considérés comme les meilleurs cliqueurs.

Avant de commencer

Rôle requis : sn_si_admin

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Espace de travail Réponse aux incidents de sécurité**.
2. **Sélectionnez Tableaux de bord SIR**.
3. Sélectionnez Tableau **de bord d'analyse Proofpoint** dans la liste déroulante.



4. Afficher des informations sur les utilisateurs VAP.
   a. Pour afficher la liste des utilisateurs VAP, sélectionnez l'onglet **Utilisateurs VAP** .
   b. Affichez les détails d'un utilisateur VAP en sélectionnant le nom d'utilisateur.
5. Afficher des informations sur les meilleurs cliqueurs.
   a. Affichez la liste des meilleurs cliqueurs en sélectionnant l'onglet **Top Clickers** .
   b. Affichez les détails d'un top clicker en sélectionnant le nom d'utilisateur.

Intégration Reverse Whois

Reverse Whois est un service qui effectue des recherches sur les noms de domaine enregistrés par des individus ou des organisations.

Effectuez des recherches de domaine à l'aide des termes de recherche dans les observables que vous attachez à un incident de sécurité. L'API Reverse Whois recherche les enregistrements de domaine en fonction des termes de recherche que vous entrez et renvoie tous les enregistrements qui correspondent à ces termes.

Les analystes utilisent parfois cette intégration avec l'intégration pour la Whois recherche sur les incidents de sécurité. L'intégration Whois fournit des informations d'enrichissement supplémentaires en fonction des recherches de domaine à partir de l'intégration Reverse Whois .

Installer et configurer Reverse Whois

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que l'application s'intègre Reverse Whois correctement au Opérations de sécurité produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow .	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (administrateur) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration. L'administrateur d'incident de sécurité attribue également le rôle d'analyste d'incident de sécurité (sn_si.analyste). • L'analyste des incidents de sécurité (sn_si.analyst) effectue des recherches de domaine auprès Reverse Whois des incidents de sécurité, les analyse et travaille avec eux.
Procurez-vous une clé API.	Visitez le site Web de l'API WhoisXML pour plus d'informations sur les clés API et pour créer un compte : Site Web de l'API WhoisXML . La configuration nécessite que vous saisissiez les clés API.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Conditions requises pour la version Madrid et ultérieures Pour la version Madrid et les versions familiales ultérieures, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Cadre de travail d'intégration de sécurité

Traduction automatique

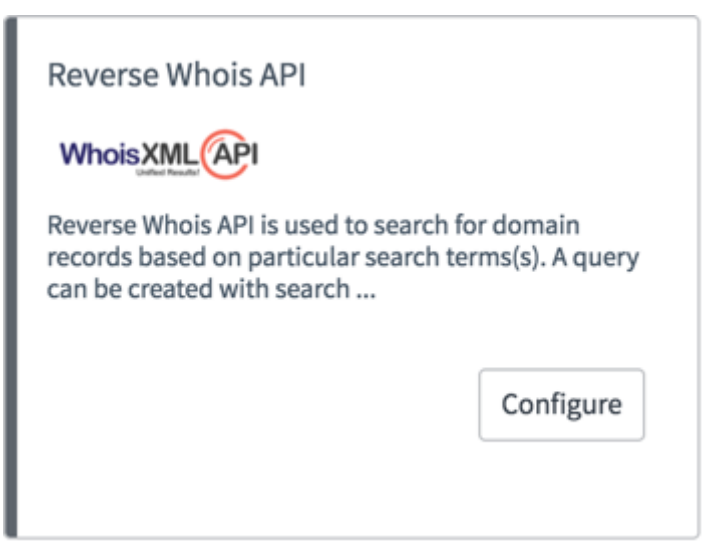
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	3. Security Support Common **4.** Orchestration du support de sécurité Pour en savoir plus sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Rôle requis : admin

Procédure

1. Si vous avez déjà installé et configuré l'application Reverse Whois , procédez comme suit :
   a. Supprimez la configuration existante.
   b. Installez et créez une configuration à l'aide de la clé API que vous avez obtenue.
2. Si vous n'avez pas installé l'application pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes d'installation.
3. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette API Reverse Whois .
4. Cliquez sur **Configurer**.



5. Dans la boîte de dialogue **Configuration de l'API Reverse Whois** , entrez la clé API que vous avez obtenue sur le site Web de l'API XML Whois .
6. Choisissez une option dans le tableau suivant pour filtrer les recherches de domaine en fonction de vos termes de recherche.

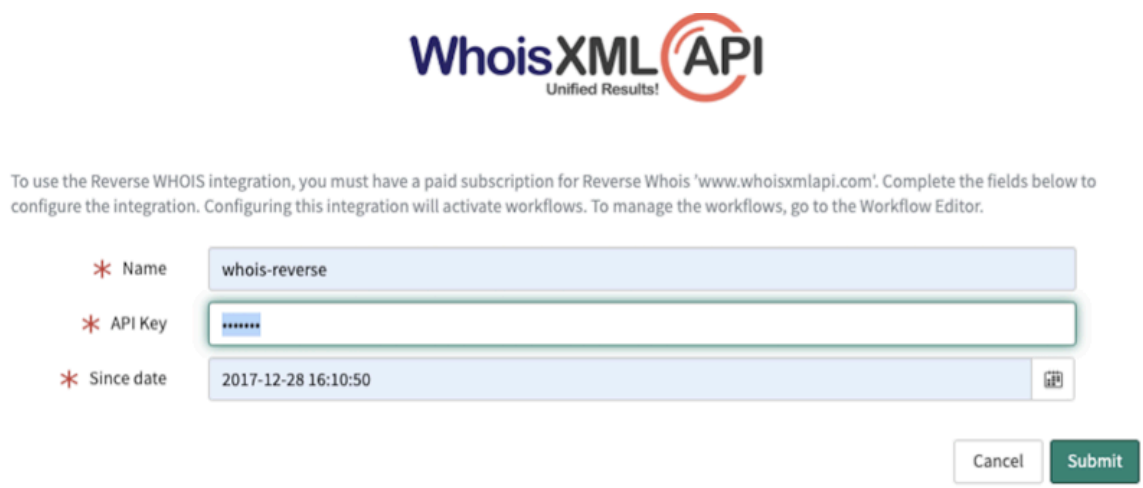
Description	Paramètre
Votre recherche inclut tous les domaines, actifs et expirés, qui ont été enregistrés après la date de	**Date de début** : date saisie au format aaaa-mm-jj. Par exemple, 1991-06-01 pour le 1er juin 1991.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Description	Paramètre
début pour les termes de recherche que vous saisissez. Il s'agit du paramètre recommandé.	
Votre recherche inclut tous les domaines actifs pour les termes de recherche que vous saisissez.	**Depuis la date** : Champ effacé.

Ces paramètres de configuration restent enregistrés jusqu'à ce que vous les modifiiez et s'appliquent à toutes les Reverse Whois recherches d'API.



7. Cliquez sur **Envoyer**.
   La configuration est terminée avec succès à moins qu'un message d'erreur ne s'affiche.

Trouble?
Si un message d'erreur s'affiche, la clé API peut être non valide.

Message d'erreur

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

(Facultatif) Installer et configurer Whois

Installez le module d'extension Whois pour fournir des informations d'enrichissement supplémentaires sur vos recherches de domaine à partir de l'API Reverse Whois . Cette recherche fournit des données d'enrichissement supplémentaires sur le domaine, telles que la date d'enregistrement, le nom du bureau d'enregistrement et le pays d'origine.

Avant de commencer

1. Si vous n'avez pas demandé d'autorisation pour l'application, consultez Obtenir une autorisation pour un produit ou une Opérations de sécurité application l'application à partir de ServiceNow Whois Store.
2. Obtenez les informations d'identification de la Whois clé API à partir du site Web du produit : site Web de l'API WHOIS .

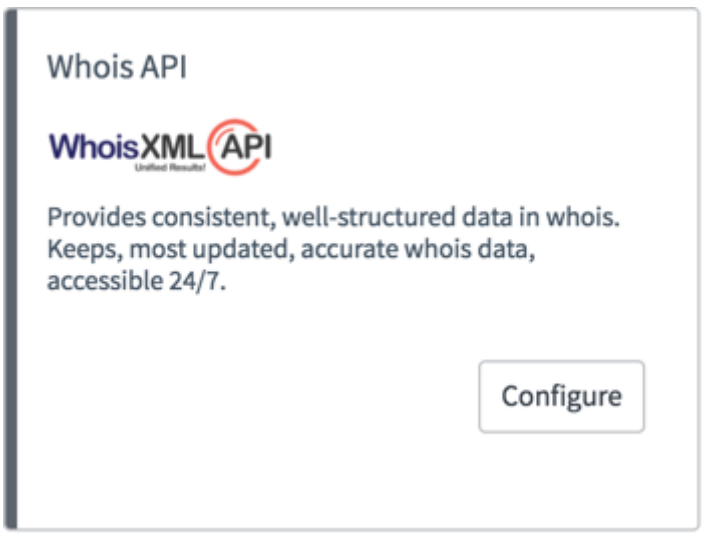
Rôle requis : admin

Traduction automatique

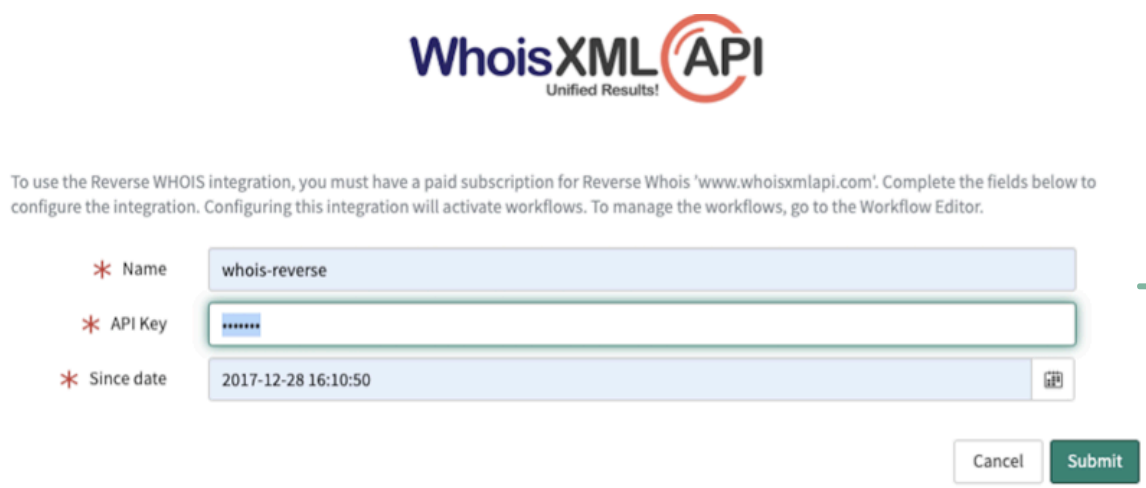
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si vous n'avez pas installé l'application, consultez Installer une Opérations de sécurité intégration et suivez les étapes pour l'installer.
2. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette API Whois .
3. Cliquez sur **Configurer**.



4. Dans la boîte de dialogue **Configuration de l'API Whois** , entrez la clé API que vous avez obtenue sur le site Web du produit.



5. Cliquez sur **Envoyer**.
   La configuration est terminée avec succès à moins qu'un message d'erreur ne s'affiche. Vous pouvez désormais exécuter des recherches d'enrichissement sur les domaines renvoyés par l'intégration Reverse Whois .

Trouble?

Si un message d'erreur s'affiche, la clé API peut être non valide.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Lancer une recherche pour Reverse Whois

Effectuez des recherches de domaine à l'aide des termes de recherche dans les observables que vous joignez manuellement à un enregistrement d'incident de sécurité.

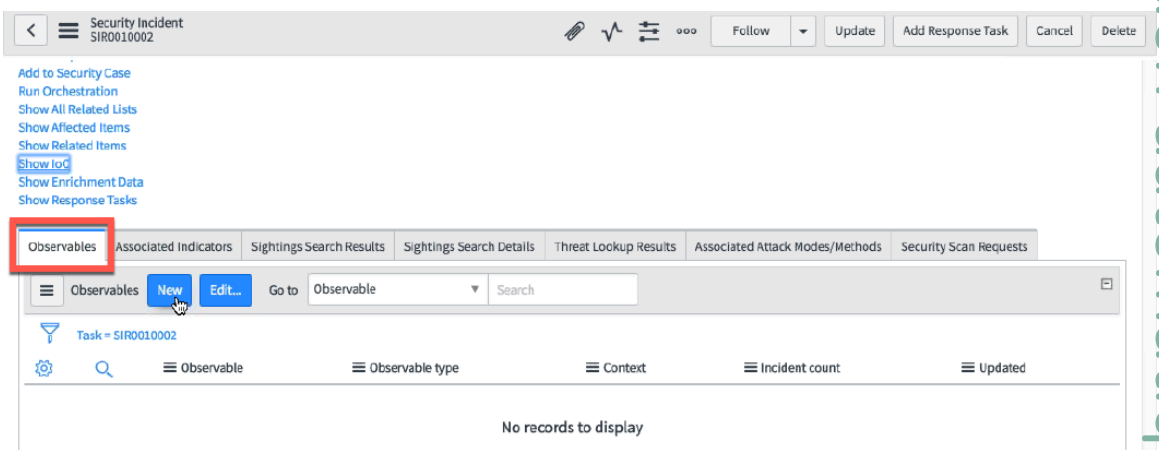
Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. S'il n'est pas ouvert, accédez à **Incident de sécurité** > **Incidents** > **Afficher les incidents** et ouvrez l'incident de sécurité avec lequel vous travaillez.
2. Au bas de l'enregistrement, cliquez sur le lien connexe **Afficher l'IoC** pour afficher l'onglet Observables.

> **Remarque :** Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres système. Si vous ne voyez pas d'onglets sur l'incident de sécurité, dans le coin supérieur droit de la bannière, cliquez sur l'icône d'engrenage **Paramètres** . Dans la boîte de dialogue **Paramètres système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que **Formulaires à onglets** et **Avec le formulaire** sont sélectionnés.



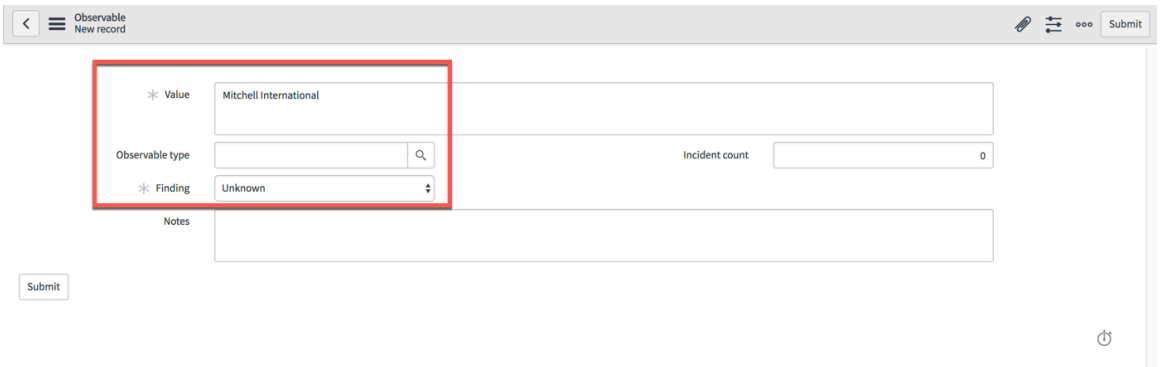
3. Dans l'onglet Observables, cliquez sur **Nouveau**.
4. Renseignez les champs.

Champs obligatoires du nouvel enregistrement

Champ	Description
Valeur	Terme de recherche unique pour un domaine.
Type d'observable	Ce champ est automatiquement effacé.
Résultat	Ce champ est automatiquement défini sur **Inconnu**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
   Vous revenez à l'enregistrement d'incident de sécurité et le flux lance la recherche.

Que faire ensuite

Vérifiez les résultats de la recherche sur l'incident de sécurité. Consultez Vérifier les résultats attendus pour Reverse Whois.

Vérifier les résultats attendus pour Reverse Whois

Les résultats de l'enrichissement sont affichés dans l'onglet **Domaines ReverseWhois** au bas de l'enregistrement d'incident de sécurité. Localisez les résultats de la recherche pour vérifier que celle-ci s'est exécutée correctement.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. S'il n'est pas déjà ouvert, accédez à **Incidents de sécurité** > **Incidents** > **Afficher les incidents** et localisez l'incident de sécurité avec lequel vous travaillez.



   Une fois que l'application est configurée et que vous avez joint un observable, le flux se lance automatiquement. Les notes de travail sur l'enregistrement d'incident de sécurité affichent l'état d'exécution et d'achèvement de la recherche.



2. Si vous ne pouvez pas vérifier que la recherche s'est exécutée avec succès, consultez les notes de travail pour plus d'informations sur la marche à suivre.

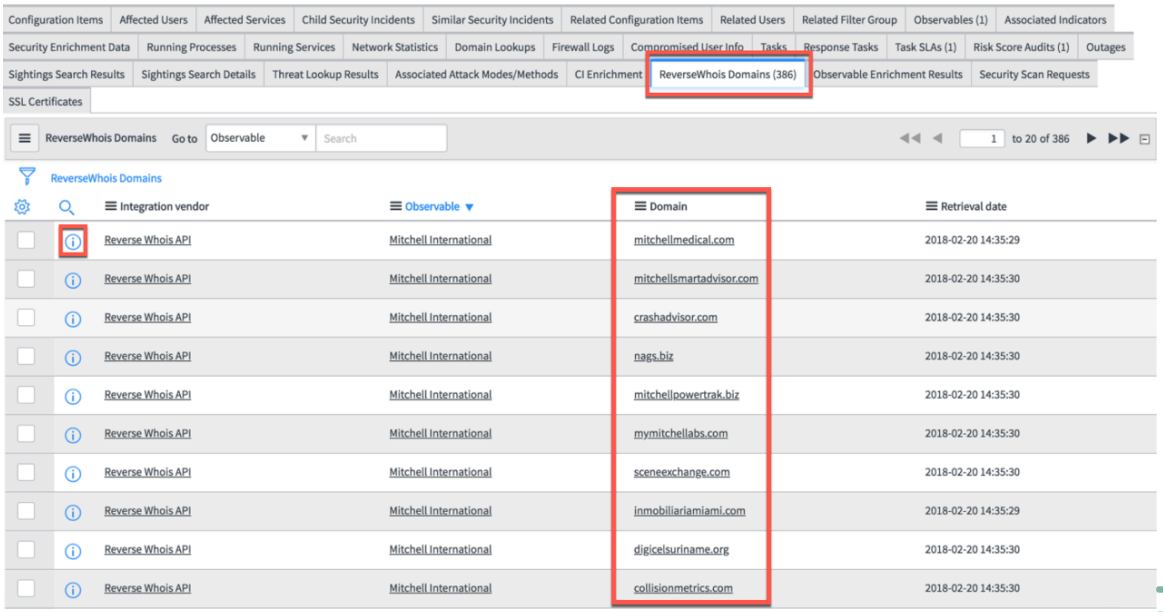


3. Accédez au bas de l'incident de sécurité et cliquez sur le lien connexe **Afficher toutes les listes connexes** .

> **Remarque :** Pour les résultats de recherche filtrés présentés dans la figure suivante, les paramètres de configuration de la vignette de configuration de l'API ont été enregistrés avec **1991-06-01**Reverse Whois saisi dans le champ **Depuis la date**.

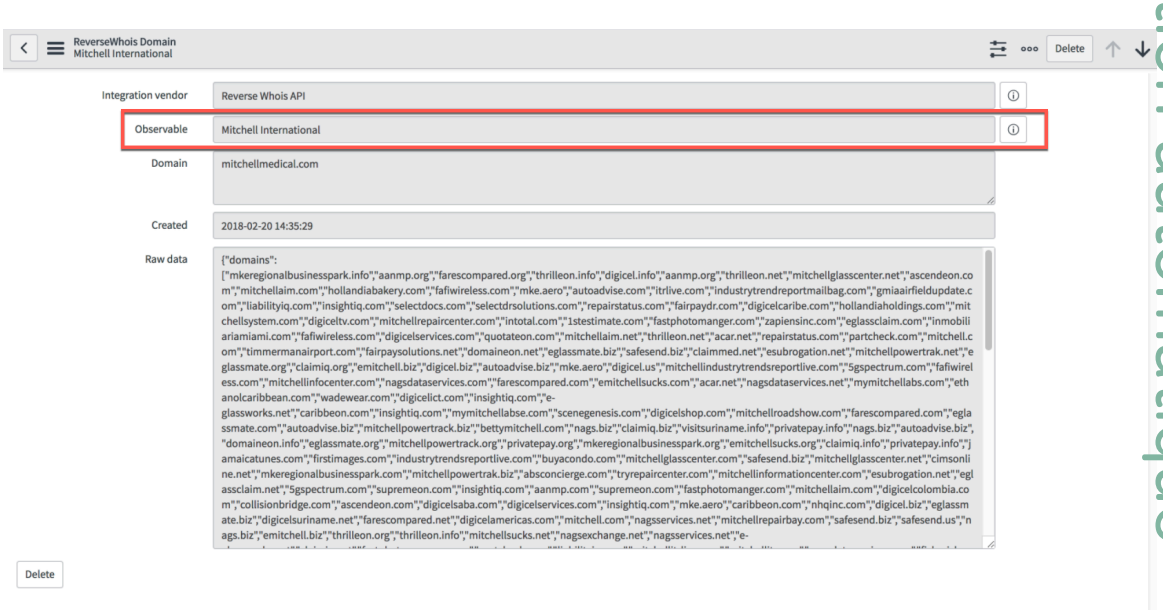
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les résultats de l'enrichissement sont affichés dans l'onglet **Domaines ReverseWhois** . Les domaines actifs de cet observable sont affichés dans la colonne **Domaine** .

4. Cliquez sur l'icône d'informations bleues en regard d'un élément, puis cliquez sur **Ouvrir l'enregistrement** dans la boîte de dialogue qui s'affiche.

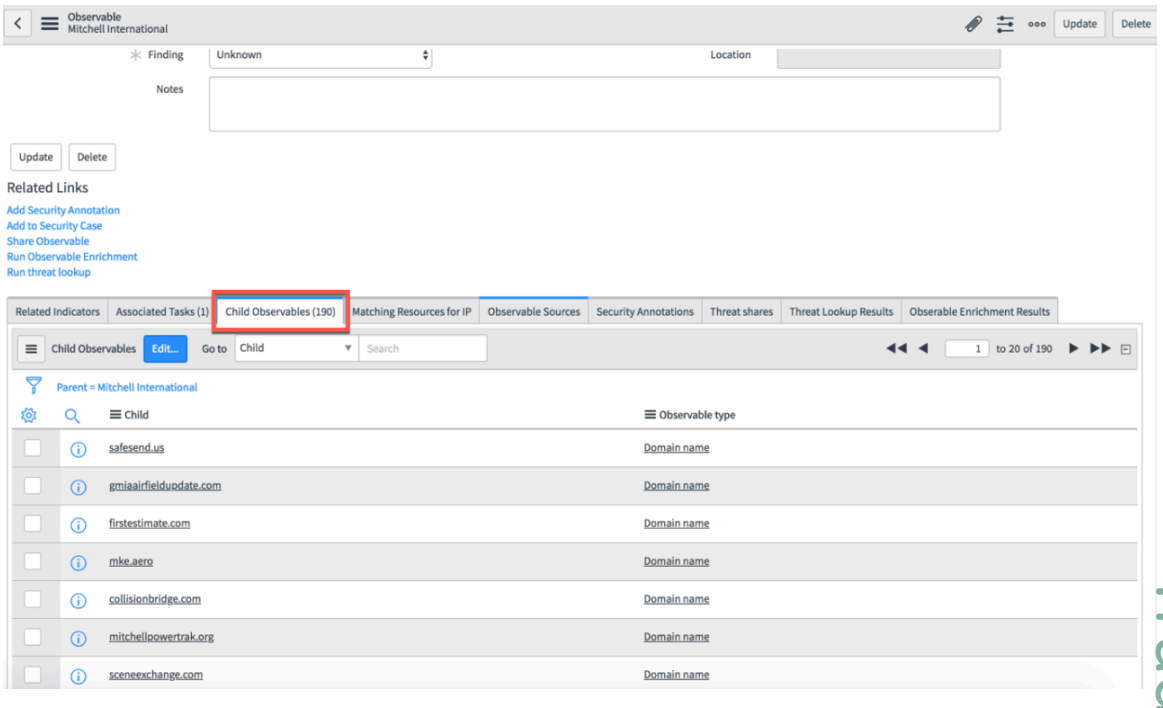


L'enregistrement s'affiche avec les détails de l'enrichissement, y compris les données brutes.

5. Revenez à l'incident de sécurité et, avec l'onglet **Domaines ReverseWhois** sélectionné, cliquez sur un observable dans la colonne **Observable** pour ouvrir un enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les observables enfants sont affichés dans l'onglet **Observables enfants** de l'enregistrement Observable. Les observables enfants ne sont générés que si l'application a renvoyé des Reverse Whois domaines.

Trouble?

Si la recherche échoue, vérifiez que les termes de recherche que vous avez entrés sont pris en charge par l'intégration. Consultez les notes de travail pour plus d'informations.

Que faire ensuite

Pour obtenir plus de données d'enrichissement sur les résultats de la recherche de domaine, vous pouvez exécuter l'intégration Whois pour effectuer des recherches d'enrichissement sur les observables enfants retournés par l'intégration Reverse Whois . Ces données d'enrichissement sur les observables enfants comprennent des informations sur la date d'enregistrement, le nom du bureau d'enregistrement et le pays d'origine.

(Facultatif) Exécuter la recherche d'enrichissement et vérifier les résultats attendus pour Whois

Exécutez l'intégration Whois pour effectuer des recherches d'enrichissement sur les domaines renvoyés par l'intégration Reverse Whois .

Avant de commencer

Vérifiez que vous avez installé et configuré les modules d'extension Reverse Whois et Whois . N'effectuez ces étapes qu'une fois que vous avez exécuté la recherche de domaine avec le module d'extension Reverse Whois .

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

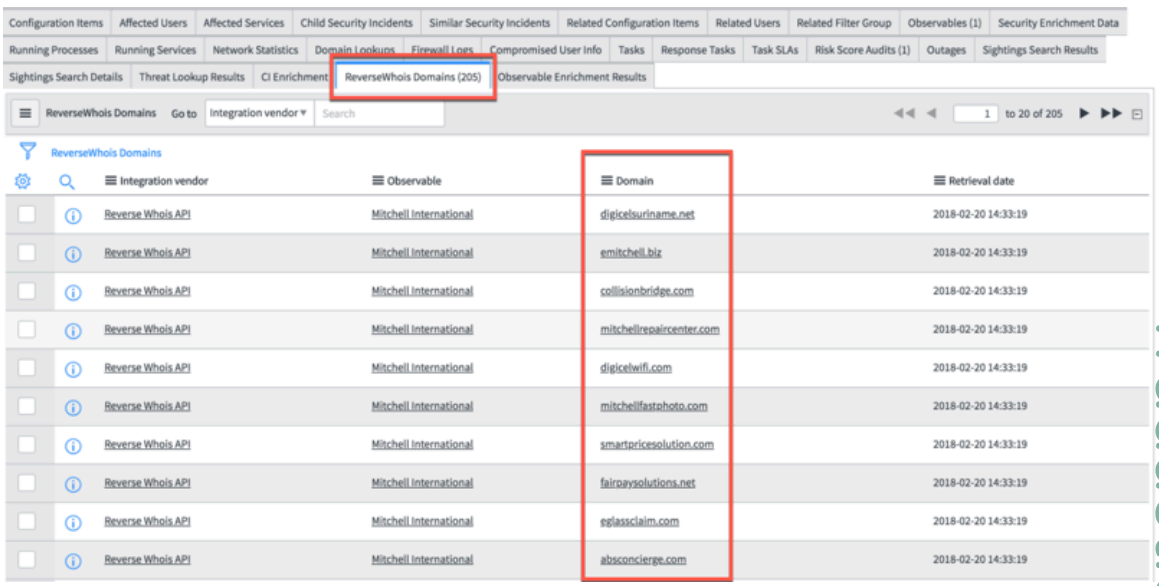
Les résultats sont affichés dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement observable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

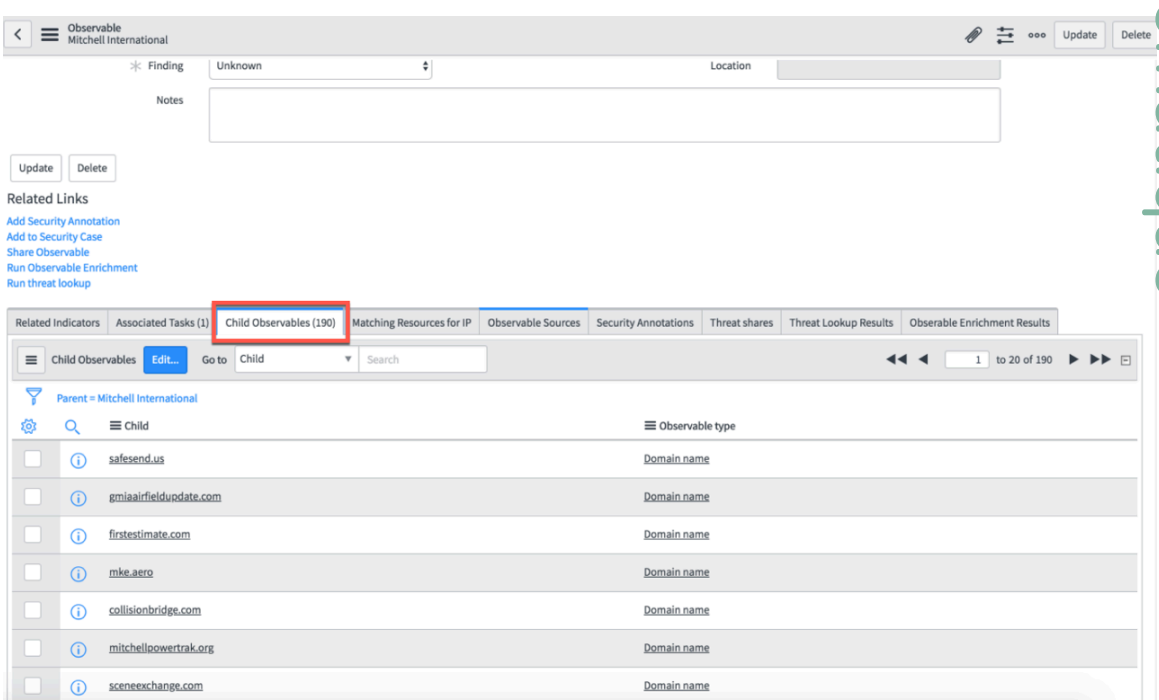
Procédure

1. Accédez à la **Tous** > **Incidents de sécurité** > **Incidents** > **Afficher les incidents** et localisez l'incident de sécurité avec lequel vous travaillez et qui a exécuté la recherche de domaine avec succès.
2. Ouvrez l'enregistrement et cliquez sur le lien connexe **Afficher toutes les listes connexes** .
3. Sélectionnez l'onglet **Inverser les domaines d'identification** en bas de l'enregistrement.



Dans la colonne **Domaines** , la liste des domaines renvoyés s'affiche.

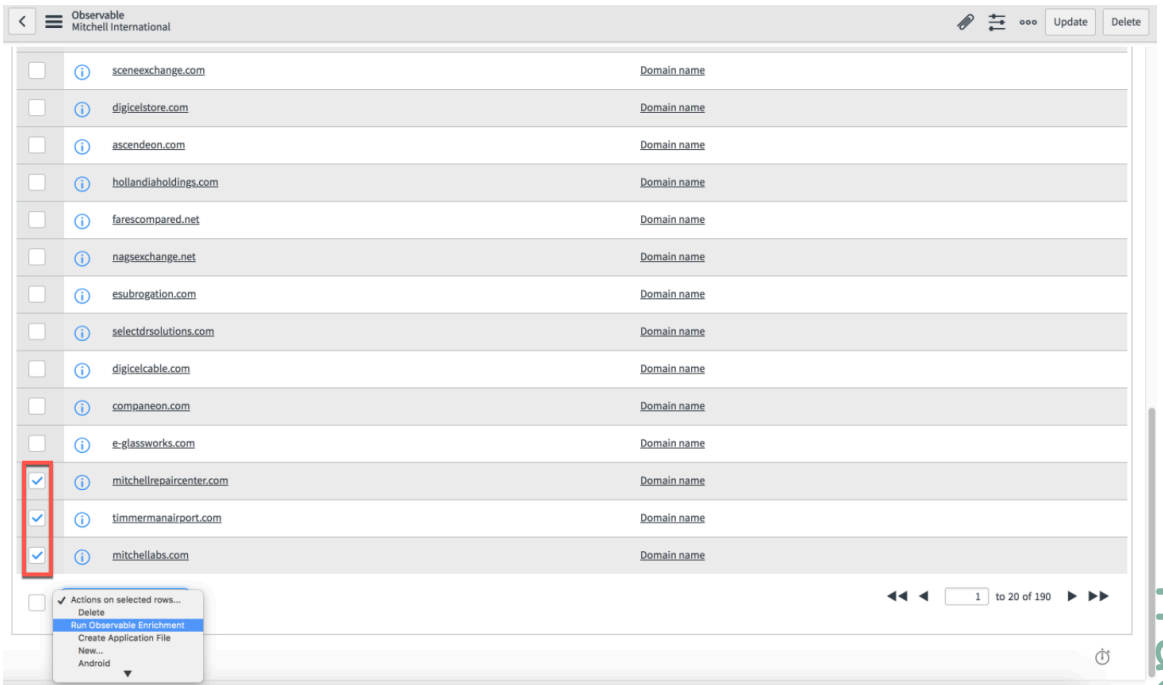
4. Dans la colonne **Observable** , cliquez sur un observable.
   Dans l'onglet **Observables enfants** , les observables enfants sont affichés. Les observables enfants ne sont générés que si l'analyse initiale de l'observable par l'application Reverse Whois a renvoyé des domaines.



5. Sélectionnez les observables enfants sur lesquels vous souhaitez exécuter l'enrichissement des observables puis, dans la liste de choix **Action sur les lignes sélectionnées** , sélectionnez **Exécuter l'enrichissement des observables**.

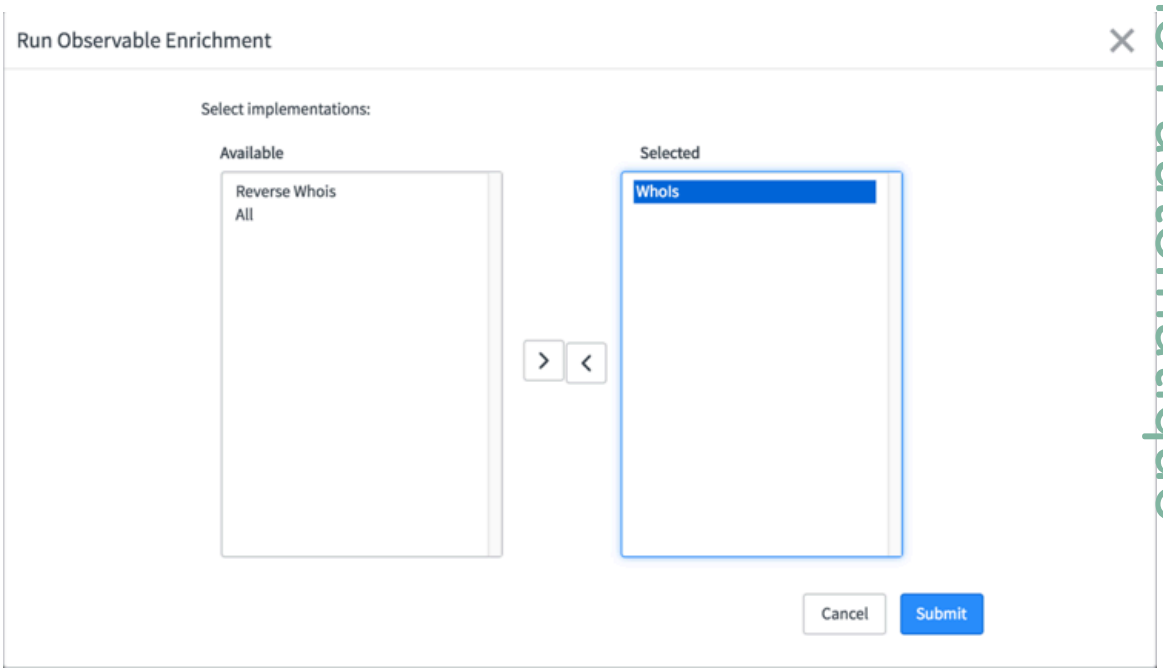
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La boîte **de dialogue Exécuter l'enrichissement de l'observable** s'affiche.

6. Déplacez l'intégration de **Disponible**Whois à **Sélectionné,** puis cliquez sur **Soumettre**.

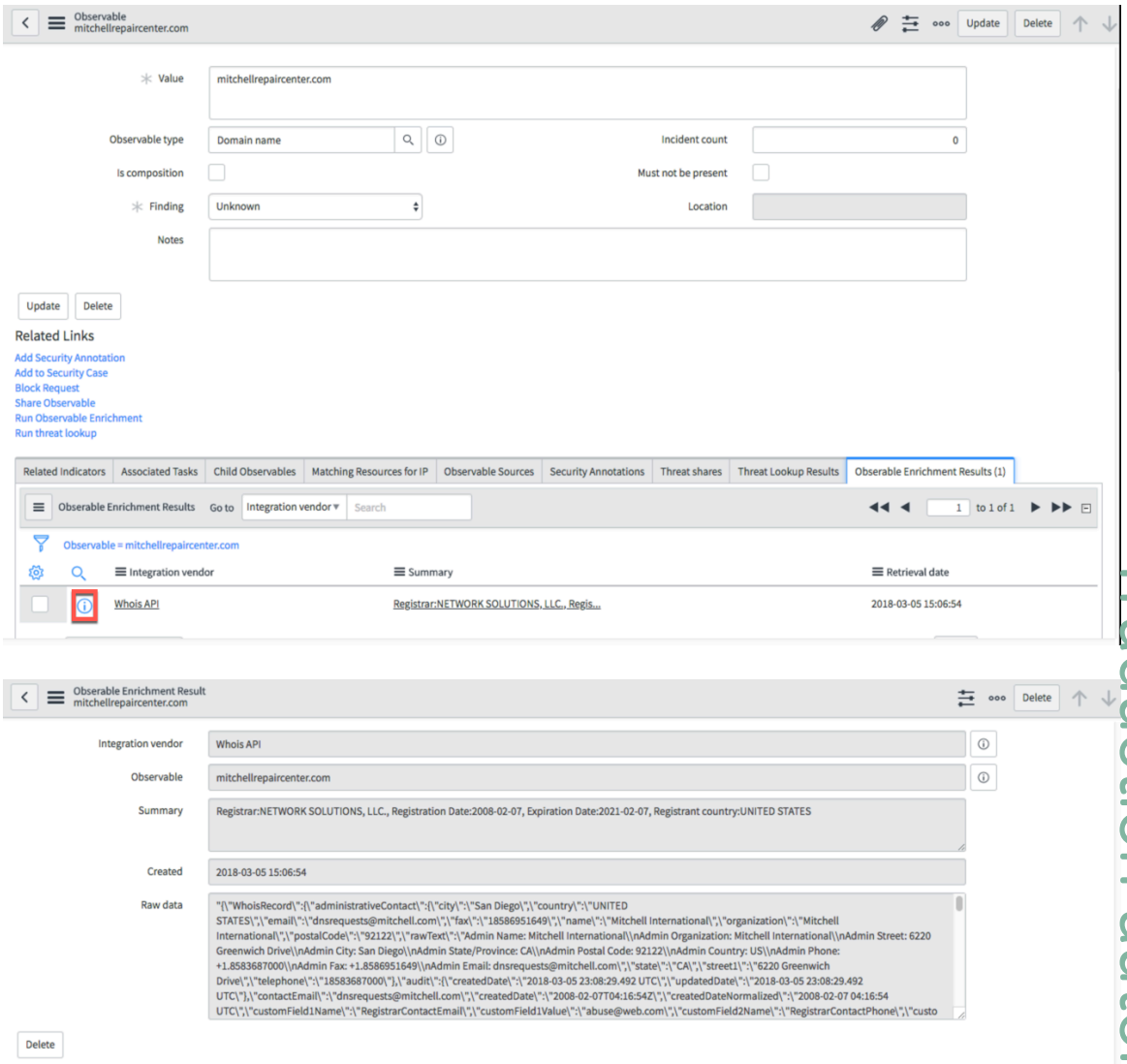


Les résultats sont affichés dans l'onglet **Résultats d'enrichissement des observables** de l'enregistrement d'observable.

7. Cliquez sur l'icône d'informations bleues, puis sur **Ouvrir l'enregistrement** dans la boîte de dialogue qui s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Davantage d'informations et de données brutes relatives à la recherche de domaine d'origine s'affichent, telles que la date d'enregistrement, le nom du bureau d'enregistrement et le pays d'origine.

Trouble?
Si vous ne parvenez pas à localiser les observables enfants ou les résultats de l'enrichissement, vérifiez que l'intégration s'est exécutée avec succès et que les Reverse Whois domaines ont été renvoyés. Veuillez également consulter les notes de travail versées au dossier pour obtenir de plus amples renseignements.

Information associée

Installer et configurer Reverse Whois

Vérifier les résultats attendus pour Reverse Whois

RISKIQ et WHOISIQ intégration

Grâce à l'intégration des RISKIQWHOISIQ API et au ServiceNow AI Platform® Opérations de sécurité produit, les analystes de sécurité disposent de données d'enrichissement supplémentaires et d'un aperçu de la validité des sites Web.

L'API RISKIQ Certificats SSL effectue des recherches sur les certificats SSL, qui incluent des détails sur l'autorité de certification émettrice, les organisations qui demandent des certificats, les certificats d'entité auxquels les certificats sont délivrés et le domaine. Les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

recherches de certificats SSL sont effectuées automatiquement lorsque des incidents de sécurité sont créés.

L'API RISKIQ WHOISIQ effectue des recherches sur d'autres types d'observables, tels que domaine, e-mail, serveur de noms, organisation, adresse et numéro de téléphone. Les observables d'URL et de domaine sont enrichis automatiquement lorsque des incidents de sécurité sont créés.

L'intégration nécessite le et Renseignements sur les menaces les Réponse aux incidents de sécurité produits.

Observables pris en charge pour RISKIQ et RISKIQ WHOISIQ

L'API RISKIQ prend en charge les recherches automatiques de certificats SSL sur l'adresse IP, le hachage de fichier, le numéro de série du certificat, le domaine et les observables d'URL. Les observables d'URL et de domaine sont enrichis automatiquement avec l'API WHOISIQ . Pour l'enrichissement des observables sur d'autres types d'observables avec l'API WHOISIQ , créez des observables et exécutez des recherches manuellement à partir de la table Observables.

Observables pris en charge

Le tableau suivant répertorie le type d'API utilisé dans cette intégration et les observables pris en charge par chaque API. La table indique également si une recherche se produit automatiquement lorsque des incidents de sécurité sont créés ou si la recherche est exécutée manuellement à partir de la table Observables.

Observables pris en charge et recherche

API	Observables pris en charge	Recherche (automatisée ou manuelle)
RISKIQ API de certificat SSL	• Adresse IP • Hachage de fichier (empreinte du certificat). Voir la figure suivante pour un exemple de hachage de fichier. • Numéro de série de certificat ou Numéro de série. Cette chaîne est un ID unique pour l'entité. Consultez la figure suivante pour obtenir un exemple de numéro de série de certificat. • Domaine (www.site.com ou site.com)	Recherche automatisée lors de la création d'incidents. Les résultats sont affichés dans l'onglet **Certificats SSL** de l'enregistrement d'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Observables pris en charge et recherche (suite)

API	Observables pris en charge	Recherche (automatisée ou manuelle)
	• URL **Remarque :** les analyses automatiques sont exécutées pour le format URL à l'aide du protocole `https://` , par exemple, `https://example.com/index.html`	
RISKIQ WHOISIQ API	• Domaine • URL	Recherche automatisée lors de la création d'incidents. Les résultats sont affichés dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement d'incident de sécurité.
RISKIQ WHOISIQ API	• Adresse e-mail • Nom de l'organisation • Numéro de téléphone • Adresse postale	La recherche manuelle est exécutée à partir de la table Observables. Les résultats sont affichés dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement observable.

Exemple de hachage de fichier et de numéro de série de certificat

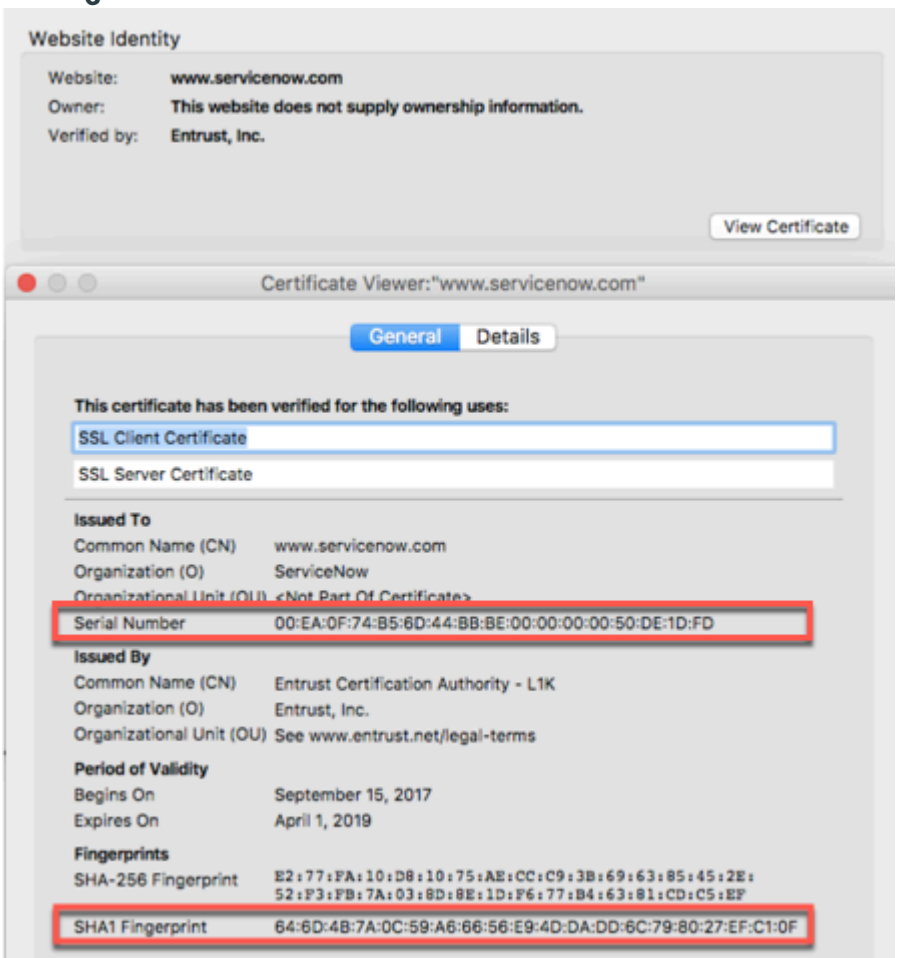
Cette figure est un exemple d'observables de hachage de fichier et de numéro de série de certificat utilisés pour les recherches de certificat SSL pour cette intégration. Le hachage de fichier fait référence à une empreinte digitale SHA-1. Cette valeur est affichée dans votre ServiceNow AI Platform instance sans les séparateurs deux-points. Par exemple, `646D4B7A0C59A66656E94DDADD6C798027EFC10F`.

L'observable de numéro de série de certificat fait référence à l'ID ou au numéro de série unique de l'entité. Cette valeur est également affichée sans les séparateurs deux-points. Par exemple, `00EA0F74B56D44BBBE00000000050DE1DFD`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Hachage de fichier et numéro de série du certificat



Installer et configurer RISKIQ et WHOISIQ

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que les applications et s'intègrent RISKIQ correctement à ServiceNow AI Platform Opérations de sécurité.WHOISIQ

Avant de commencer

Rôle requis : admin RISKIQ et WHOISIQ admin.

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (administrateur) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration et vérifie les résultats attendus. Ce rôle a également accès au Opérations de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

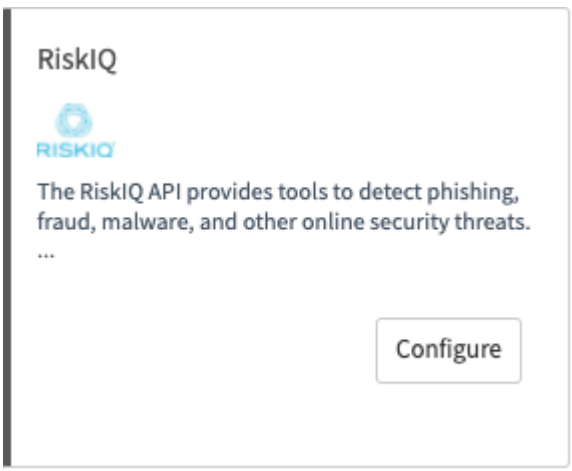
Tâche de configuration	Description
	module et affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). • L'analyste des incidents de sécurité (sn_si.analyst) travaille avec les enregistrements d'incidents de sécurité.
Obtenez un nom d'utilisateur et une clé API.	Visitez le site Web pour plus d'informations sur la clé API et comment créer un compte : site Web de RISKIQ . La configuration nécessite que vous entriez la clé API.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Conditions requises pour la version Madrid et ultérieures Pour la version Madrid et les versions familiales ultérieures, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Orchestration du support de sécurité Pour en savoir plus sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Traduction automatique

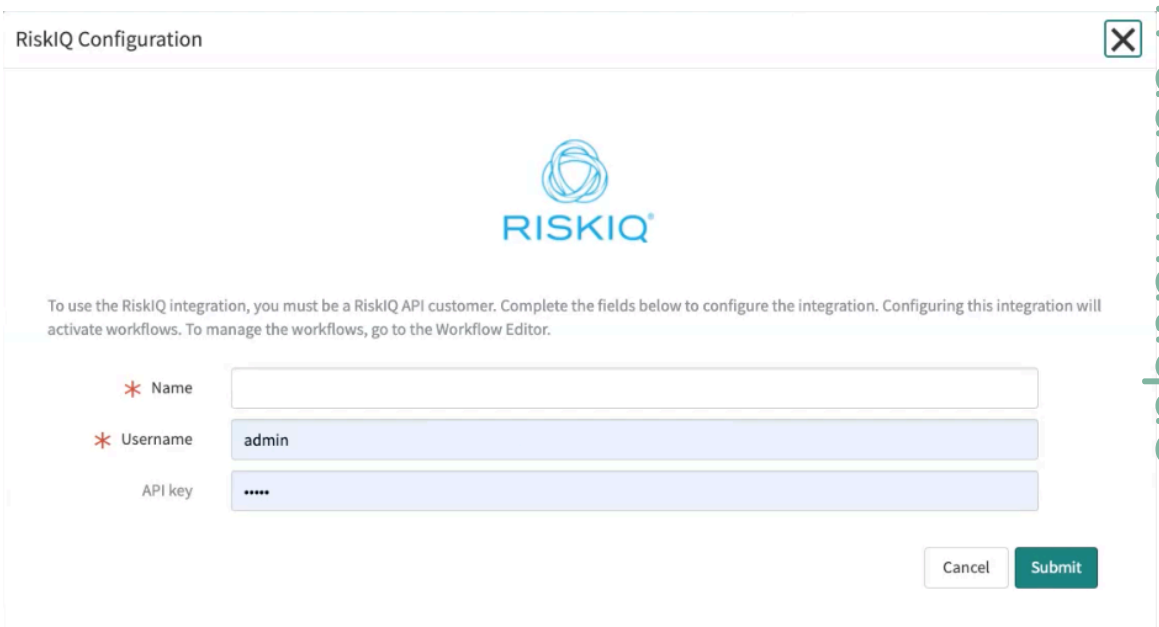
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si vous n'avez pas installé l'application pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes d'installation.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Intégrations** > **Configurations des intégrations** et localisez la vignette API.
3. Cliquez sur **Configurer**.



4. Dans la boîte de dialogue Configuration de RiskIQ qui s'affiche, entrez le **nom d'utilisateur** et la **clé API**.



5. Cliquez sur **Envoyer**.
6. Vérifiez la réussite de la configuration.
   Lorsque la configuration est terminée avec succès, la page Intégrations de sécurité avec les vignettes d'intégration s'affiche.

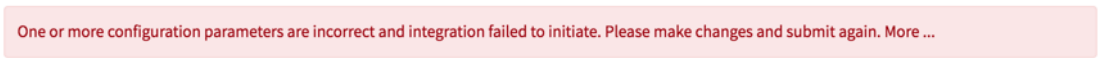
Trouble?

Si un message d'erreur s'affiche, le nom d'utilisateur ou la clé API n'est peut-être pas valide. Vérifiez que votre nom d'utilisateur et votre clé API sont corrects :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage



Vérifier les résultats attendus pour RISKIQ les recherches de certificat SSL

Lorsqu'un incident de sécurité génère des observables pour les URL, les domaines, les adresses IP, les hachages de fichiers de certificat (empreinte digitale SHA-1) et les numéros de série de certificat, les analystes d'incidents de sécurité utilisent les résultats de recherche de certificat SSL pour vérifier que les sites disposent de certificats émis par une autorité de certification publique (CA) approuvée.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Pour les observables pris en charge, les ServiceNow AI Platform analyses recherchent l'occurrence la plus récente d'URL, de domaines, d'adresses IP, de hachages de fichiers de certificat (empreinte digitale SHA-1) et de numéros de série de certificat. Voici les résultats possibles de l'analyse :

Une correspondance exacte est trouvée

Un émetteur valide d'un certificat SSL est répertorié dans l'enregistrement d'incident de sécurité.

Aucun résultat de certificat trouvé

Aucun résultat n'est répertorié sur l'enregistrement d'incident de sécurité.

Une correspondance exacte est trouvée pour un certificat auto-signé ou généré en interne

Les résultats d'un certificat SSL généré en interne sont affichés dans l'enregistrement d'incident de sécurité.

Aucune correspondance exacte n'est trouvée pour un certificat SSL primaire

Une valeur de recherche renvoie plusieurs entrées et un certificat primaire ne peut pas être identifié. Un message récapitulatif s'affiche sur l'enregistrement d'incident de sécurité.

Procédure

1. Pour afficher les observables et vérifier les résultats de la recherche, ouvrez l'enregistrement d'incident de sécurité avec lequel vous travaillez et localisez les notes de travail.

Example

Pour illustrer des exemples des résultats de recherche possibles pour cette intégration, supposons qu'un incident de sécurité a été généré avec les observables suivants :

- community.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- servicenow.com

Observables et emplacement des résultats de la recherche

Observable (exemple)	Résultats de l'analyse	Description et emplacement
community.servicenow.com	Certificat trouvé avec un hachage SHA1.	Une correspondance exacte est trouvée et un émetteur valide d'un certificat SSL est répertorié. Les résultats de la correspondance

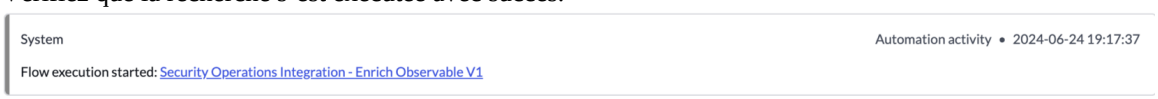
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Observable (exemple)	Résultats de l'analyse	Description et emplacement
		exacte sont affichés dans l'onglet **Certificats SSL** de l'enregistrement d'incident de sécurité.
invalidsubdomain.servicenow.com	Aucun certificat trouvé.	Un résumé indiquant qu'aucun résultat de certification n'a été trouvé est affiché dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement d'incident de sécurité.
mail.dgnetworks.com	Certificat trouvé avec hachage SHA1.	Une correspondance exacte est répertoriée pour un certificat auto-signé ou généré en interne. Les résultats sont affichés dans l'onglet **Certificats SSL** de l'enregistrement d'incident de sécurité.
servicenow.com	La recherche a renvoyé 138 certificats, et un seul certificat primaire n'a pas pu être identifié.	Aucune correspondance exacte n'est trouvée pour un certificat SSL principal, car une valeur de recherche renvoie plusieurs certificats. Un résumé indiquant qu'aucun certificat primaire n'a été trouvé est affiché dans l'onglet **Résultats de l'enrichissement des observables** de l'enregistrement d'incident de sécurité.

Une fois l'application configurée, le flux se lance automatiquement. L'état de la recherche et les observables sont affichés dans les notes de travail.

2. Vérifiez que la recherche s'est exécutée avec succès.





Trouble?
Si vous ne pouvez pas afficher les résultats attendus, vérifiez que l'observable est pris en charge par la recherche de certificat SSL pour l'intégration.

Information associée

Observables pris en charge pour RISKIQ et RISKIQ WHOISIQ

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

RISKIQ Recherches de certificat SSL qui renvoient une correspondance exacte

RISKIQ Les résultats de la recherche de certificats SSL pour une correspondance exacte sont affichés dans l'onglet **Certificats SSL** de l'enregistrement d'incident de sécurité. Une correspondance exacte fournit un nom d'autorité de certification valide, ce qui aide un analyste des incidents de sécurité à déterminer la validité d'un site Web.

Example: Correspondance exacte pour un certificat SSL valide

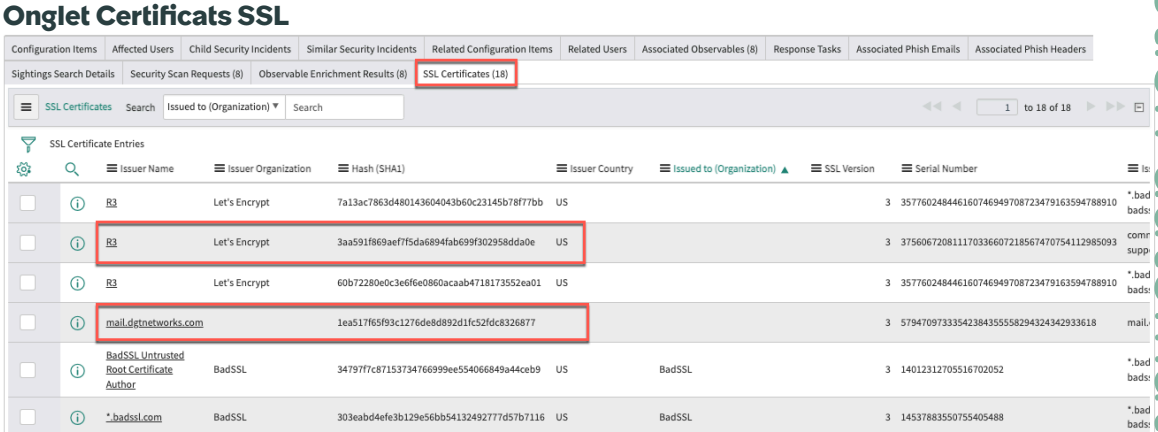
L'exemple suivant montre un émetteur valide d'un certificat SSL à partir d'une correspondance exacte dans les résultats de la recherche. Suivez les étapes pour afficher les résultats et les données brutes.

Remarque : Les figures des exemples suivants sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres système. Si votre écran ne correspond pas à la vue illustrée ci-dessous, suivez les étapes pour définir des formulaires à onglets.

1. Dans le coin supérieur droit de la bannière, cliquez sur l'icône Paramètres.
2. Dans la boîte de dialogue **Paramètres système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que **Formulaires à onglets** et **Avec le formulaire** sont sélectionnés.

1. Dans l'enregistrement de l'incident de sécurité, cliquez sur l'onglet **Certificats SSL** .

Onglet Certificats SSL



Des informations sur le nom de l'émetteur du certificat, l'organisation de l'émetteur et le destinataire de la délivrance du certificat (Organisation) sont affichées avec d'autres données.

18 éléments sont affichés dans la colonne **Nom de l'émetteur** . Le deuxième élément (R3) fournit un nom d'autorité de certification valide (Let's Encrypt) dans la colonne **Organisation de l'émetteur** .

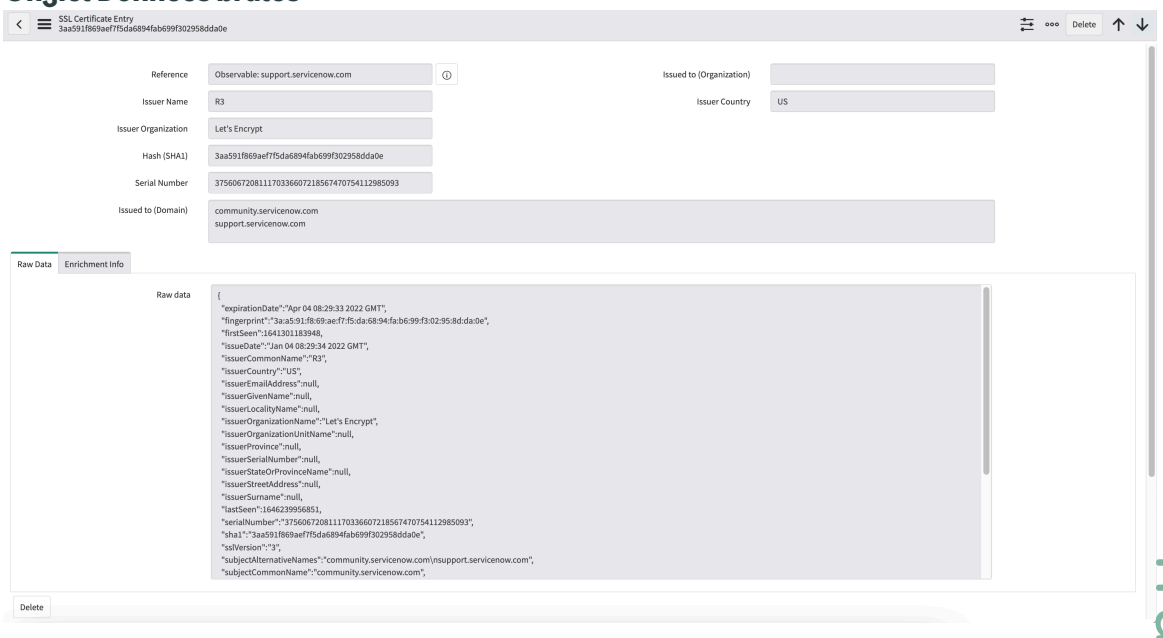
Aucune information dans les colonnes **Organisation de l'émetteur** et **Délivré à** ne s'affiche pour le deuxième élément (mail.dgtnetworks.com).

2. Cliquez sur le deuxième élément de la colonne **Nom de l'émetteur**, qui est (**R3**) pour ouvrir l'enregistrement d'entrée. Vous pouvez également cliquer sur l'icône d'informations en regard de l'élément, puis sur **Ouvrir l'enregistrement**.
3. Sélectionnez l'onglet **Données brutes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Données brutes



L'enregistrement d'entrée de certificat SSL inclut l'observable dans l'onglet **Données brutes** sous la colonne **Nom de l'entité** , ainsi que d'autres données.

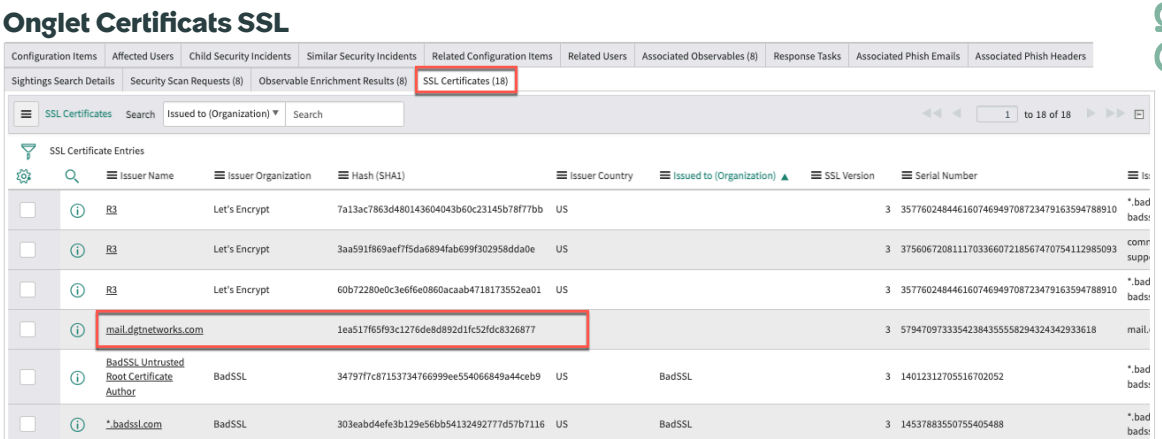
Notez que dans la colonne **Catégorie** , l'objet et l'émetteur correspondent à des entités reconnaissables dans la colonne Nom de **l'entité** . L'émetteur de ce certificat est très probablement valide et provient d'une autorité de certification publique de confiance. Notez également que l'objet et l'émetteur sont des entités différentes. Ces entités distinctes indiquent que le certificat n'est pas un certificat signé en interne par une autorité de certification inconnue.

Example: Correspondance exacte pour un certificat SSL autosigné

L'exemple suivant montre les résultats pour un certificat SSL auto-signé à partir de la recherche. Suivez les étapes pour afficher les résultats et les données brutes.

1. Revenez à l'enregistrement d'incident de sécurité. Dans la colonne **Nom de l'émetteur** , cliquez sur l'autre élément (**mail.dgtnetworks.com**).

Onglet Certificats SSL

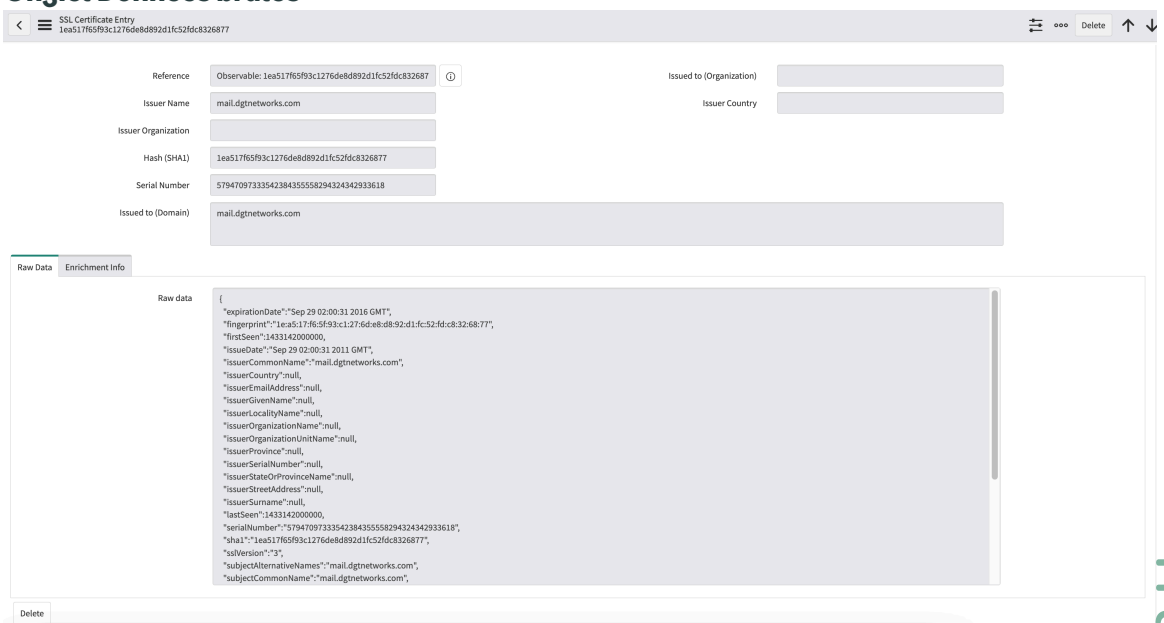


2. Dans l'enregistrement ouvert, sélectionnez l'onglet **Données brutes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Données brutes



La colonne **Catégorie** indique l'émetteur (mail.dgtnetworks.com et dgtsb. DGTNetworks.local) ne sont pas des autorités de certification publiques de confiance. Veuillez également noter que l'émetteur et le sujet sont la même entité (dgtsbs. DGTNetworks.local), et chacun contient le nom de l'observable (dgtsbs). Il s'agit peut-être d'un certificat auto-signé. Les certificats auto-signés peuvent justifier une enquête plus approfondie, car ces certificats ne sont pas émis par une autorité de certification connue.

RISKIQ Recherches de certificats SSL qui renvoient plusieurs certificats ou aucun certificat

Un analyste des incidents de sécurité peut utiliser plusieurs résultats de certificats SSL pour déterminer si un site fait partie d'une entité commune reconnaissable. Aucun résultat de certificat SSL peut indiquer que les sites avec des noms obscurs ou suspects n'ont pas de certificats de confiance. Les résultats de la recherche des observables qui ne renvoient pas de certificats SSL ou qui renvoient plusieurs certificats SSL sont affichés dans l'onglet Résultats de l'enrichissement des observables de l'enregistrement d'incident de sécurité.

Example: Aucun résultat de certificat SSL ou plusieurs résultats de certificat SSL

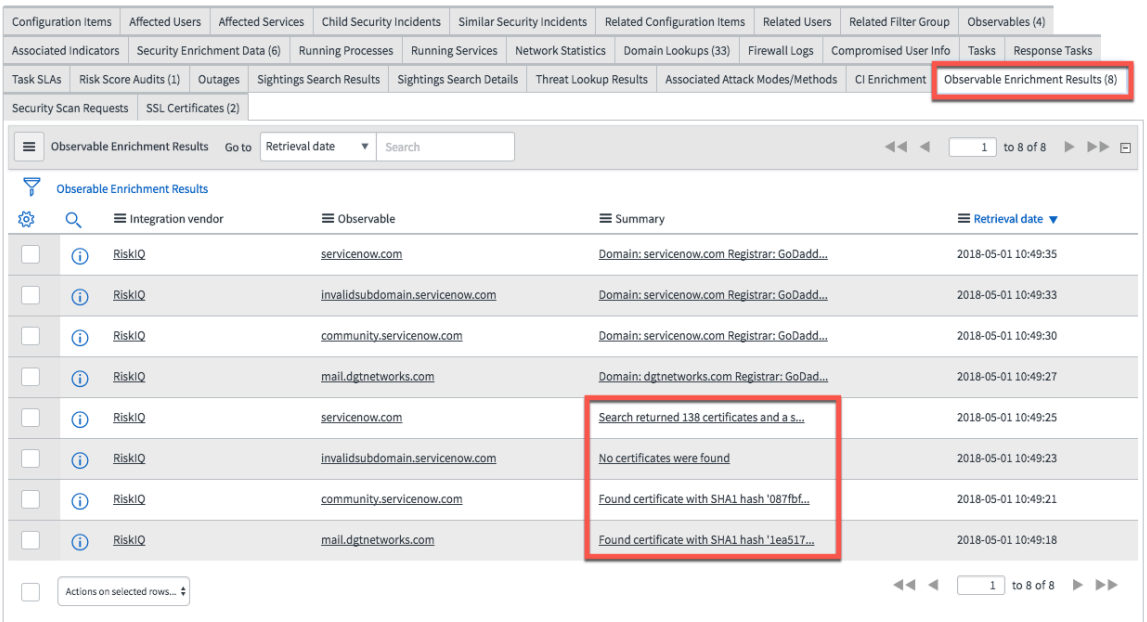
Suivez les étapes pour afficher les résultats pour les observables qui ne renvoient pas de certificats SSL ou qui renvoient plusieurs certificats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Dans l'enregistrement de l'incident de sécurité, cliquez sur l'onglet **Résultats de l'enrichissement des observables** .

Onglet Résultats de l'enrichissement de l'observable

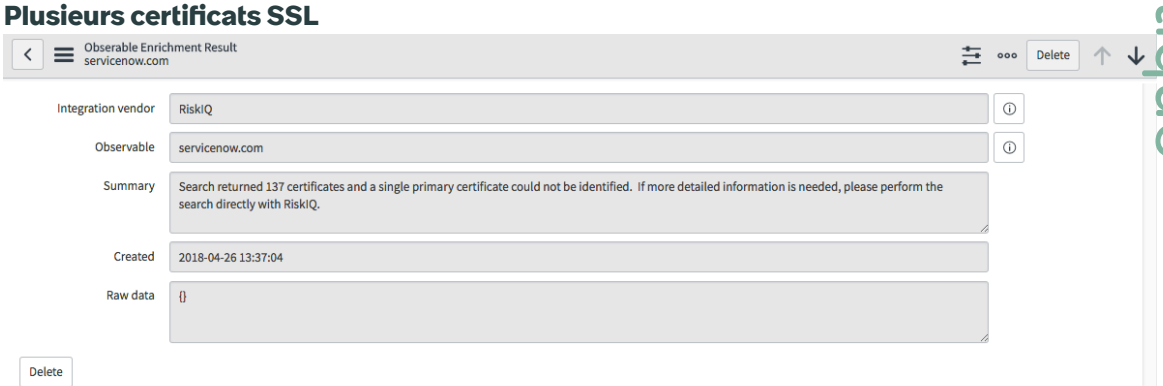


Les résultats d'enrichissement des observables pour la RISKIQ recherche et WHOISIQ s'affichent.

Dans la colonne **Observable** , servicenow.com correspond au message de recherche de 138 certificats retourné dans la colonne **Résumé** . De même, invalidsubdomain.servicenow.com correspond à Aucun certificat n'a été trouvé dans la colonne **Résumé**. Ces résumés indiquent que plusieurs certificats SSL ont été trouvés et qu'aucune correspondance exacte avec les certificats SSL n'a été trouvée, respectivement.

2. Dans la colonne **Observable** , cliquez sur **servicenow.com**.

Plusieurs certificats SSL



Le message récapitulatif qui s'affiche sur l'enregistrement indique que plusieurs résultats pour les certificats SSL ont été renvoyés pour servicenow.com et qu'un certificat SSL primaire n'a pas pu être associé. Ce message est souvent renvoyé lors de recherches qui incluent des noms de domaine courants, tels que servicenow.com.

Si vous avez besoin de plus d'informations sur un domaine commun, vous pouvez effectuer la recherche directement avec l'API RISKIQ .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Revenez à l'onglet **Résultats de l'enrichissement des observables** et, dans la colonne **Observable** , cliquez sur **invalidsubdomain.servicenow.com**.



Remarque :

- Si aucun certificat SSL n'est trouvé pour l'observable actuel, le champ Résumé affiche le message Aucun certificat n'a été trouvé.
- Si aucun certificat SSL actif n'est trouvé pour l'observable actuel, le champ Résumé affiche le message Aucun certificat actif n'a été trouvé.

Vérifier les résultats attendus pour WHOISIQ les recherches d'URL

Lorsqu'un incident de sécurité génère des observables pour des URL ou des domaines, l'API WHOISIQ procède automatiquement à l'enrichissement de l'observable lors de sa création. Les résultats de la recherche sont affichés dans les onglets **Résultats de l'enrichissement des observables** et **Certificats SSL** de l'enregistrement d'incident de sécurité.

Avant de commencer

Remarque : Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres système.

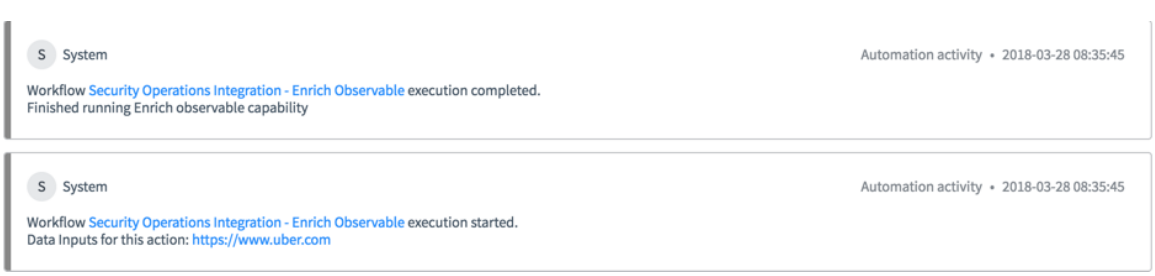
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Les résultats de l'enrichissement des observables sont affichés dans l'onglet **Résultats de l'enrichissement des observables** au bas de l'enregistrement d'incident de sécurité. Pour les observables pris en charge, une recherche de certificat SSL est également exécutée et les résultats sont affichés dans **l'onglet Certificats SSL**.

Procédure

1. Ouvrez l'enregistrement d'incident de sécurité avec lequel vous travaillez et vérifiez que la recherche a été effectuée avec succès dans les notes de travail.

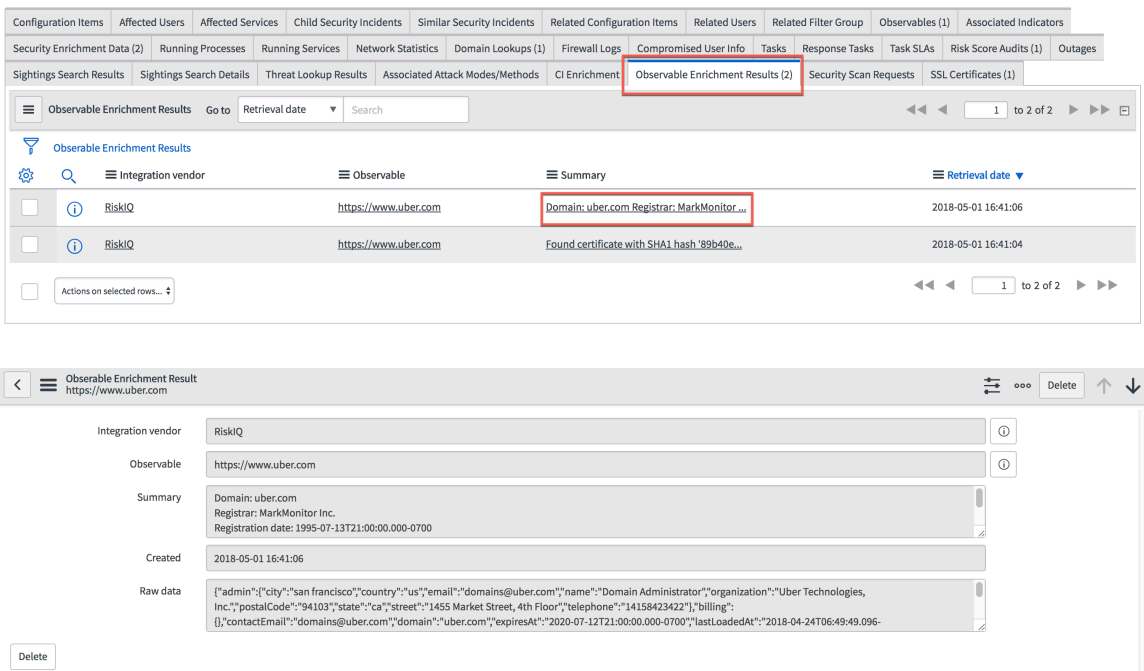


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois l’application configurée, le flux se lance automatiquement lors de la création de l’incident. L’état d’exécution et d’achèvement de la recherche est affiché dans les notes de travail de l’enregistrement d’incident de sécurité.

2. Si vous ne pouvez pas vérifier que la recherche s’est exécutée avec succès, consultez les notes de travail pour plus d’informations sur la marche à suivre.
3. Lorsque l’incident de sécurité est ouvert, cliquez sur le lien connexe **Afficher toutes les listes connexes** .
4. Cliquez sur l’onglet **Résultats de l’enrichissement de l’observable** pour le sélectionner.
5. Dans la colonne **Résumé**, cliquez sur le premier élément, **Domaine : Bureau d’enregistrement uber.com : Markmonitor...**



L’enregistrement qui s’affiche contient des informations sur le domaine.

6. Revenez à l’onglet **Résultats de l’enrichissement des observables** et, dans la colonne **Résumé**, cliquez sur le deuxième élément, **Certificat trouvé avec hachage SHA1...**

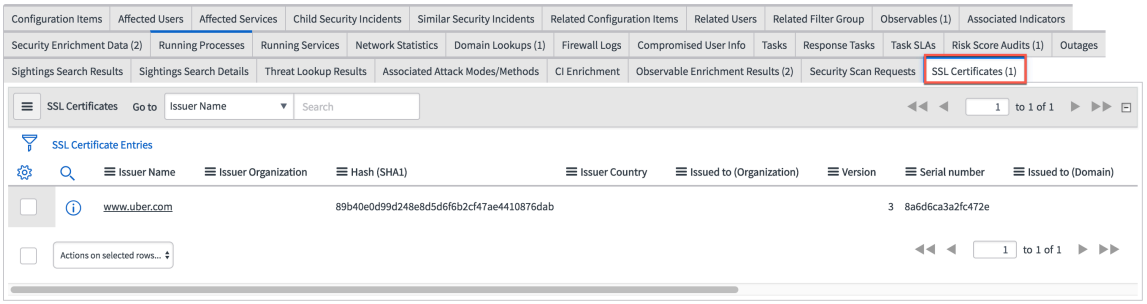


Cet enregistrement indique qu’un certificat SSL a été trouvé avec un hachage de fichier.

7. Revenez à l’enregistrement d’incident de sécurité et cliquez sur l’onglet **Certificats SSL** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les résultats du certificat SSL pour le hachage de fichier sont également affichés ici.

Trouble?

Si vous ne pouvez pas afficher les résultats attendus, examinez les notes de travail. Vérifiez également que l'observable est pris en charge pour la recherche par l'intégration.

Information associée

Observables pris en charge pour RISKIQ et RISKIQ WHOISIQ

Créer un observable pour les recherches manuelles WHOISIQ

Les analystes d'incidents de sécurité utilisent les informations issues de l'enrichissement des observables avec l'API WHOISIQ pour en savoir plus sur les adresses e-mail, les noms et les numéros de téléphone des organisations.

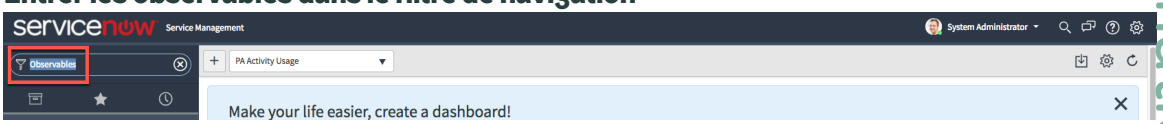
Avant de commencer

Rôle requis : sn_si.analyst

Procédure

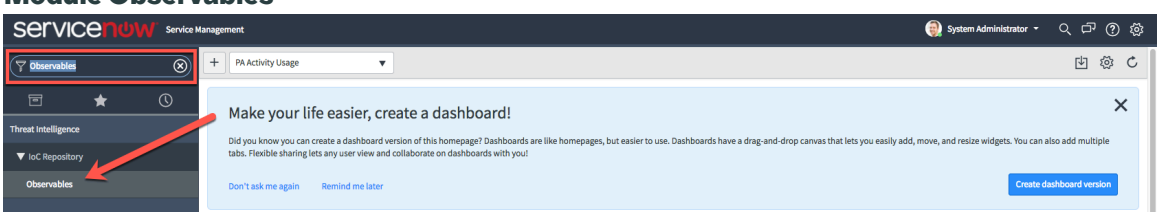
1. Accédez à la **Tous** > **Référentiel IoC** > **Observables**.

Entrer les observables dans le filtre de navigation



Le module Observables s'affiche sous le panneau de navigation.

Module Observables

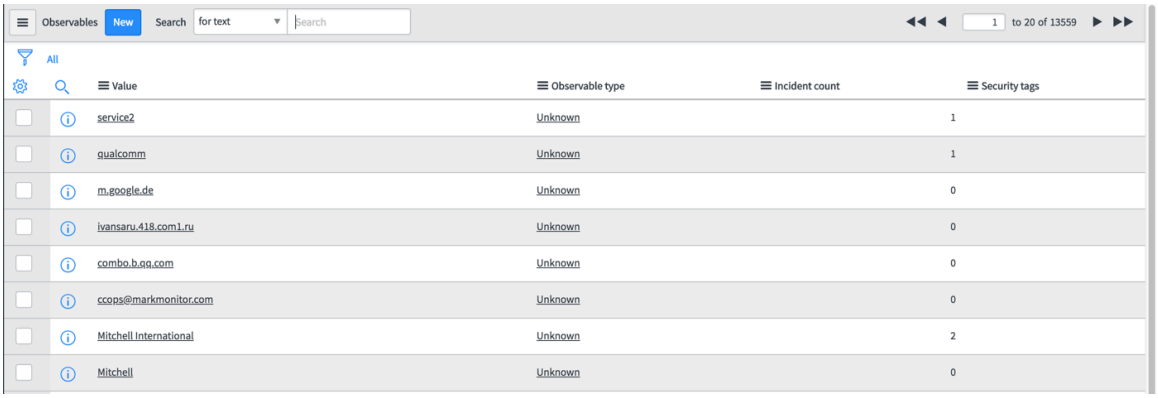


2. Cliquez sur le module **Observables** pour afficher la liste des observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

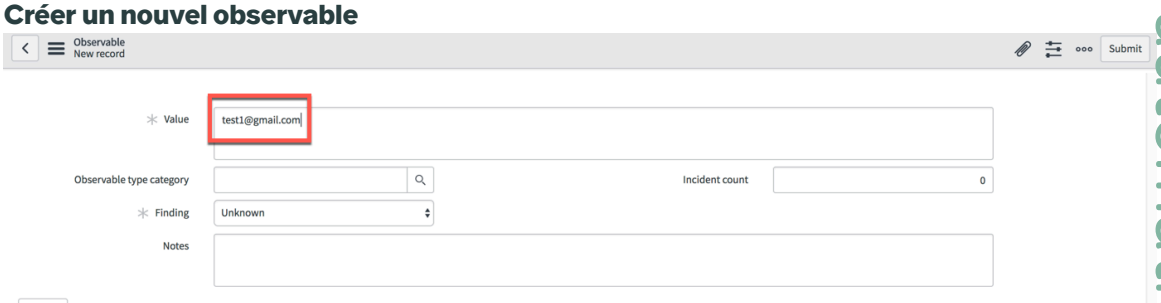
Liste des observables



3. Cliquez sur **Nouveau** pour créer un nouvel observable.
4. Dans le formulaire Observable, renseignez les champs.

Champ	Description
Valeur	Adresse e-mail, nom de l'organisation, numéro de téléphone ou adresse postale. Par exemple, `test1g–mail.com`
Type d'observable	Le champ est automatiquement effacé.
Résultat	Le champ est automatiquement défini sur **Inconnu**.

Créer un nouvel observable



5. Cliquez sur **Envoyer**.
   Vous êtes renvoyé à la liste Observables. Dans la colonne **Valeur** , votre nouvel observable s'affiche.

   Remarque : Si vous ne parvenez pas à localiser votre observable sur la partie de la liste qui s'affiche, utilisez la fonctionnalité de recherche pour le trouver.

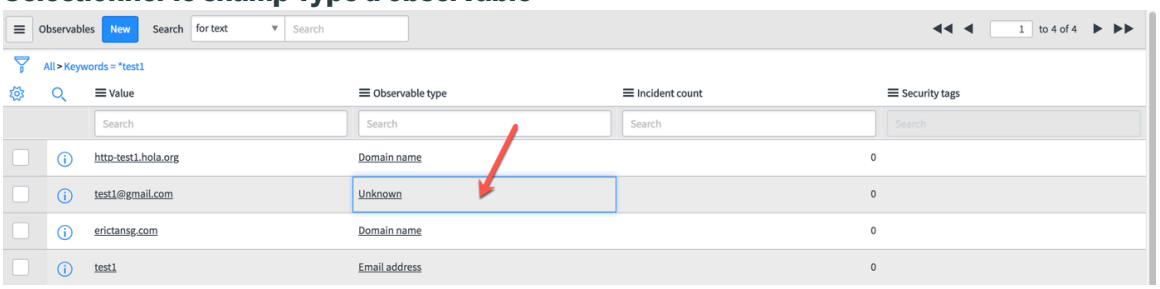
6. Modifiez le champ **Type d'observable** pour changer le type **d'Inconnu** en **Adresse e-mail** pour correspondre à votre observable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans la colonne **Type d'observable** , cliquez un seul fois à droite du texte **inconnu** pour le sélectionner.

Sélectionner le champ Type d'observable

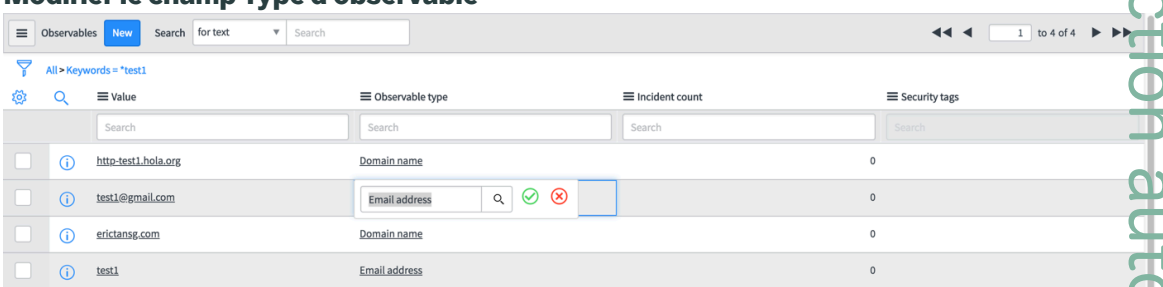


Le champ sélectionné est entouré en bleu.

b. Avec le champ délimité en bleu, double-cliquez n'importe où à l'intérieur du champ en surbrillance pour ouvrir l'éditeur.

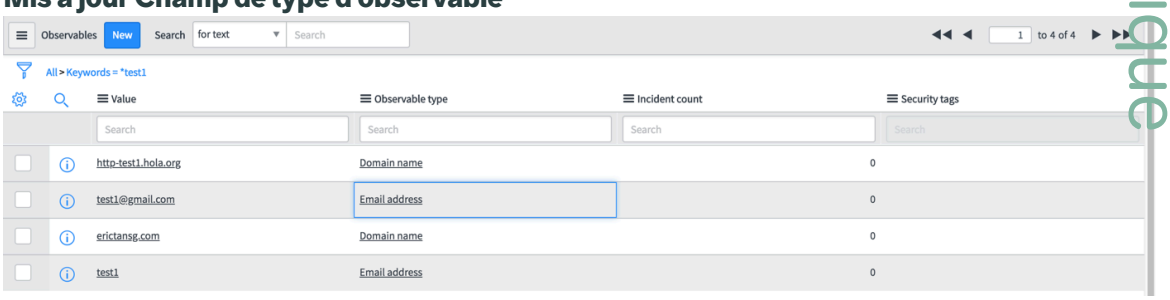
c. Dans le champ qui s'affiche, saisissez le type d'observable (`adresse e-mail`) et cliquez sur la coche verte pour enregistrer la valeur.

Modifier le champ Type d'observable



Dans la colonne **Type d'observable** de la liste, l'adresse e-mail s'affiche pour votre nouvel observable.

Mis à jour Champ de type d'observable



Que faire ensuite

Si vous avez créé et modifié un observable pour la recherche, exécutez la recherche d'enrichissement de l'observable à partir de l'enregistrement observable avec l'API WHOISIQ .

Vérifier les résultats attendus pour les recherches manuelles WHOISIQ

Exécuter une recherche manuelle sur un observable lorsque celui-ci ne génère pas automatiquement un incident de sécurité. Pour les recherches d'enrichissement d'observables à l'aide de l'API WHOISIQ pour les adresses e-mail, les noms d'organisations,

Traduction automatique

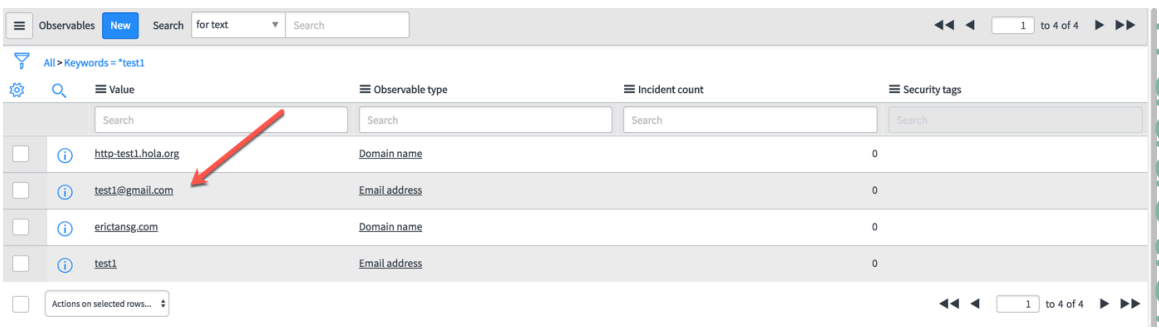
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les numéros de téléphone ou les adresses postales, lancez la recherche manuellement à partir de la table Observables.

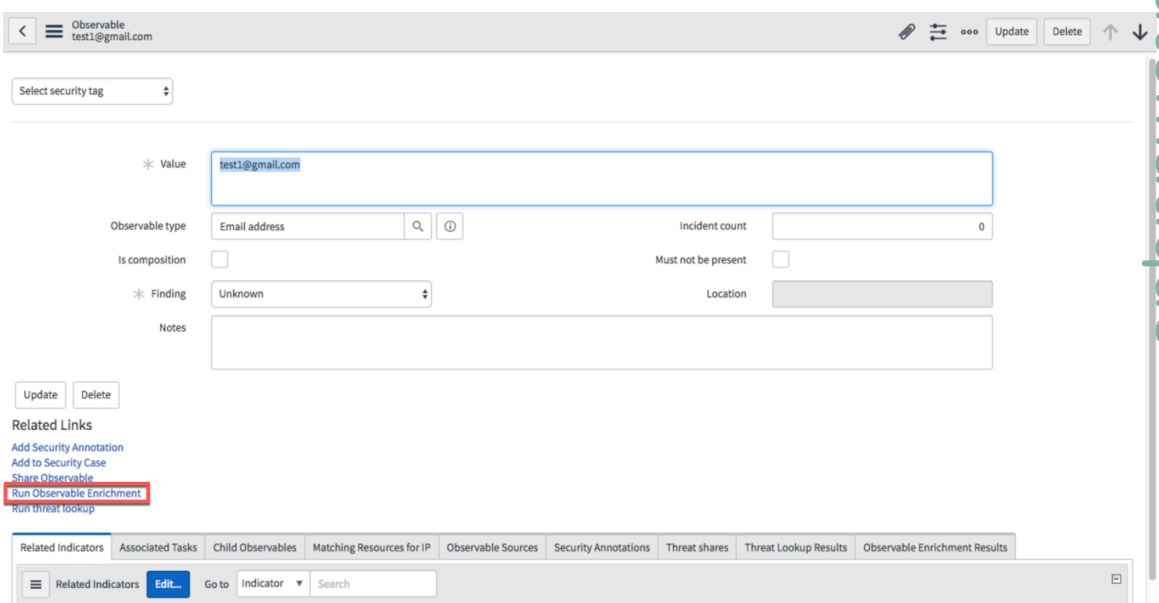
Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Créez un observable pour une recherche manuelle à l'aide de l'API WHOISIQ . Pour en savoir plus sur la création et la modification d'un observable, reportez-vous à la section Créer un observable pour les recherches manuelles WHOISIQ.

Procédure
1. Accédez à la **Tous** > **Référentiel IoC** > **Observables** et localisez l'observable dans la liste avec laquelle vous travaillez.
2. Cliquez sur votre observable dans la colonne **Valeur** pour ouvrir l'enregistrement.



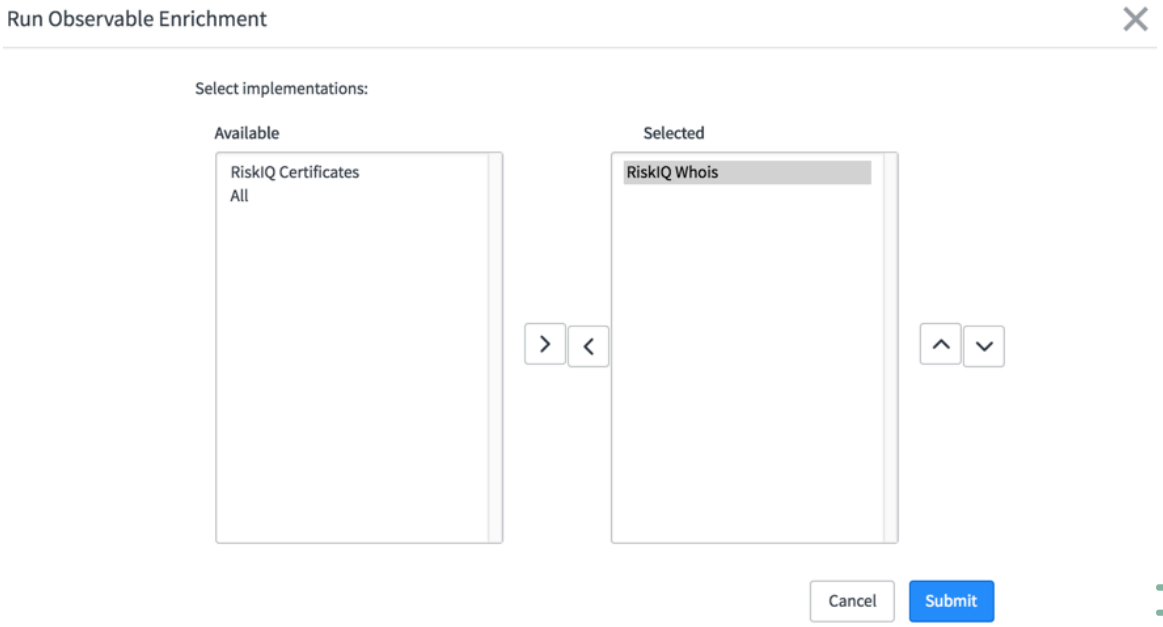
3. Cliquez sur le lien connexe **Exécuter l'enrichissement de l'observable** pour exécuter la recherche.



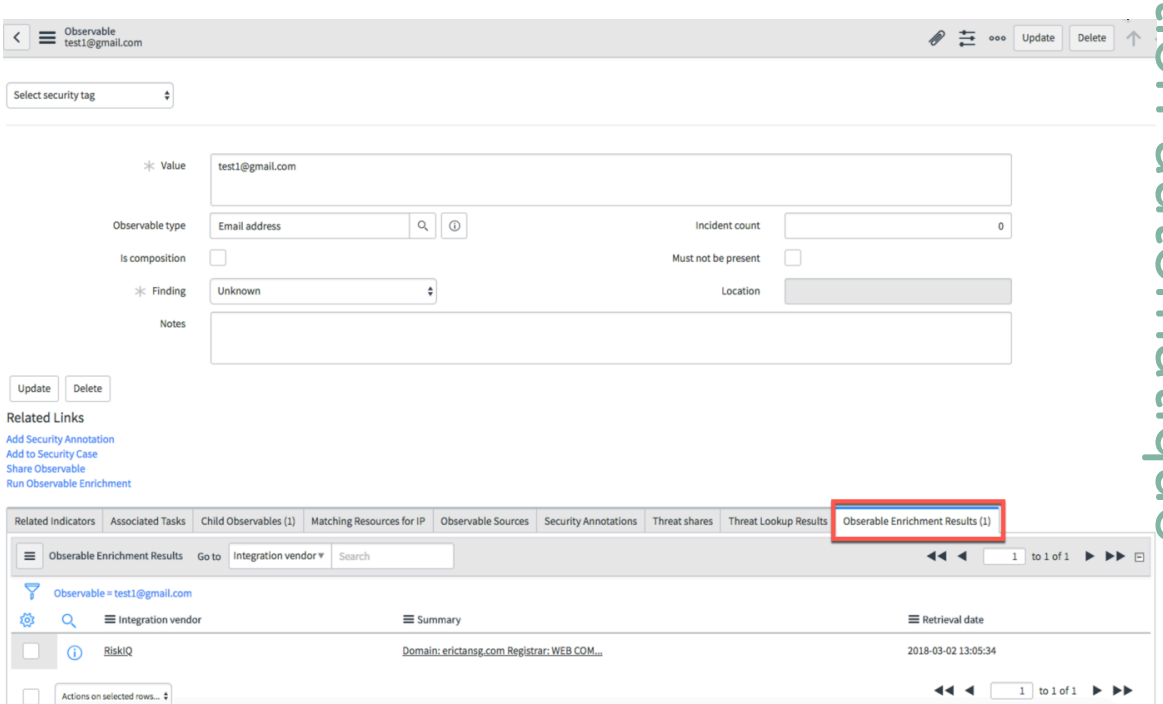
4. Dans la fenêtre **Exécuter l'enrichissement de l'observable** , déplacez **RiskIQ Whois** vers la liste sélectionnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
   Les résultats de la recherche sont affichés dans l'onglet **Résultats d'enrichissement des observables** de l'enregistrement observable.



Trouble?

Si aucun résultat n'est renvoyé pour l'observable, un message s'affiche dans la colonne **Résumé** . Si vous ne voyez pas de résultats, vérifiez que l'observable est pris en charge par l'API.

Information associée

Observables pris en charge pour RISKIQ et RISKIQ WHOISIQ

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration Shodan

Shodan est un moteur de recherche qui analyse les informations des bannières de service à partir d'appareils connectés dans le monde entier. Les bannières de service incluent des informations sur un système informatique, telles que le nom d'hôte, le type d'appareil, le système d'exploitation, l'emplacement géographique et le FAI connecté. Lorsqu'elles sont intégrées au produit, ces informations de bannière ServiceNow AI Platform Opérations de sécurité de service fournissent aux analystes des données d'enrichissement supplémentaires et des informations sur les incidents de sécurité ou les enquêtes.

L'intégration nécessite les modules d'extension Réponse aux incidents de sécurité et Renseignements sur les menaces .

L'intégration Shodan effectue un enrichissement sur les observables suivants :

- Adresses IP
- URL

L'application recherche de nouveaux observables toutes les cinq minutes. Si les observables sont d'un type reconnu par l'intégration Shodan , les observables sont enrichis.

Installer et configurer

Avant d'exécuter l'intégration sur votre instance, effectuez les étapes d'installation et de configuration afin que l'application s'intègre Shodan correctement à ServiceNow AI Platform Opérations de sécurité.

Avant de commencer

Effectuez la liste de vérification de configuration suivante avant l'installation. Ces tâches d'installation sont nécessaires pour une installation et une configuration fluides.

Tâches de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform à votre instance.	Les rôles suivants sont requis pour l'installation, la configuration et la vérification des résultats attendus : • L'administrateur système (administrateur) installe l'application et affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin). • L'administrateur d'incident de sécurité (sn_si.admin) supervise la configuration et vérifie les résultats attendus. Ce rôle a également accès au Opérations de sécurité module.
Procurez-vous la Shodan clé API.	Créez un compte et obtenez la clé API sur le Shodan site Web : Site Web de Shodan .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Pour la version Madrid et les versions familiales ultérieures, le module d'extension Réponse aux incidents de sécurité Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité

Traduction automatique

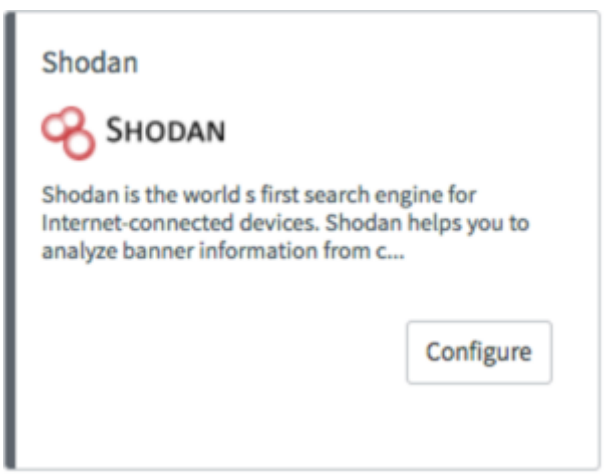
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de configuration	Description
	produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. **1.** Security Incident Response **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Orchestration du support de sécurité Pour en savoir plus sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Rôle requis : admin

Procédure

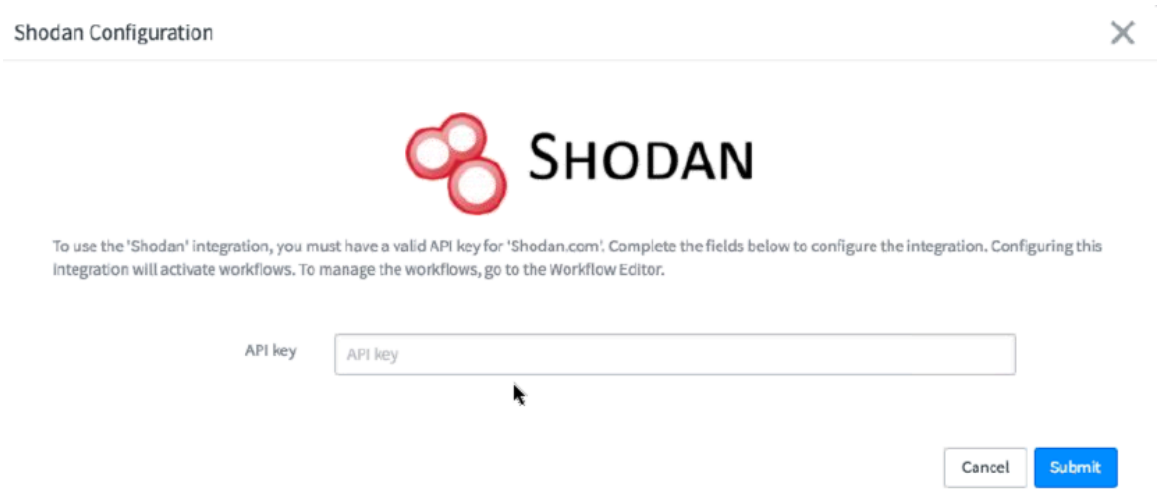
1. Si vous n'avez pas installé l'application pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes d'installation.
2. Une fois l'installation terminée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la Shodan tuile.



3. Cliquez sur **Configurer**.
4. Dans la boîte de dialogue **Configuration de Shodan** , entrez la clé API que vous avez obtenue sur le Shodan site Web et cliquez sur **Soumettre**.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique



5. Vérifiez la réussite de la configuration.
   La configuration est terminée avec succès à moins qu'un message d'erreur ne s'affiche.

   Trouble?

   Si un message d'erreur s'affiche pendant la configuration, la clé API Shodan peut être non valide.

Vérifier les résultats attendus

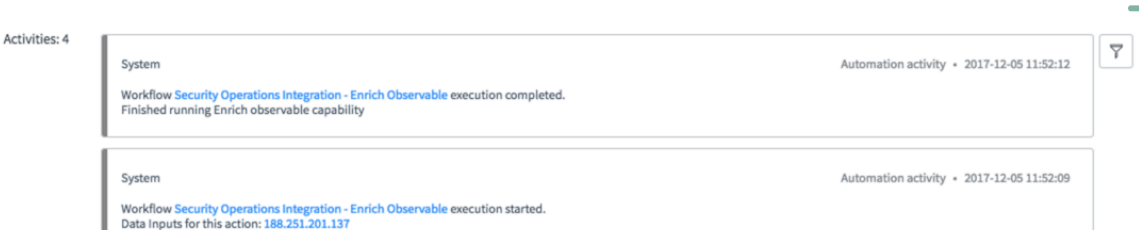
Les observables sont générés automatiquement par un incident de sécurité et analysés par l'application. Les résultats de l'enrichissement sont affichés dans les onglets **Résultats de l'enrichissement des observables** et **Bannières réseau** .

Avant de commencer

Rôle requis : sn_si.analyst.

Procédure

1. Ouvrez l'incident de sécurité avec lequel vous travaillez et vérifiez que la recherche a été exécutée avec succès.



   Une fois l'application configurée, le workflow se lance automatiquement lors de la création de l'incident. L'état d'exécution et d'achèvement de la recherche est affiché dans les notes de travail de l'incident de sécurité.

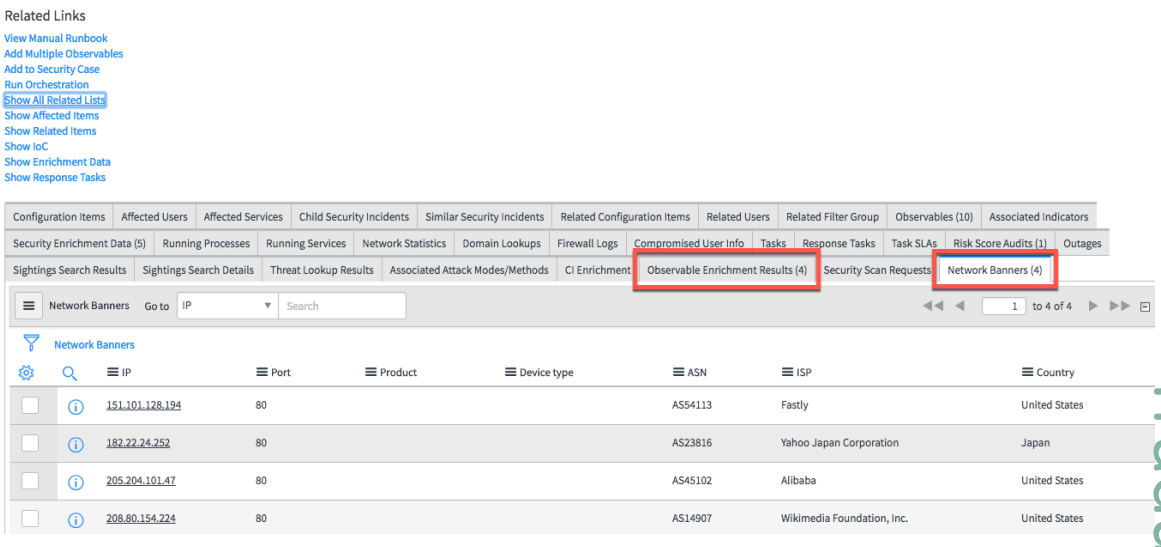
2. Passez en revue les notes de travail pour plus d'informations et sur la procédure à suivre si vous ne pouvez pas vérifier que la recherche s'est correctement exécutée.

3. Accédez au bas de l'incident de sécurité et cliquez sur le lien **Afficher toutes les listes connexes** dans **Liens connexes**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les figures des étapes suivantes sont affichées avec le paramètre **Formulaires à onglets** actif dans les paramètres système. Si les formulaires à onglets ne sont pas affichés, cliquez sur l'icône d'engrenage Paramètres dans le coin supérieur droit de la bannière. Dans la boîte de dialogue **Paramètres système** qui s'affiche, cliquez sur **Formulaires** et vérifiez que **Formulaires à onglets** et **Avec le formulaire** sont sélectionnés.



Les résultats sont affichés dans les onglets **Résultats de l'enrichissement des observables** et **Bannières réseau** au bas de l'incident de sécurité.

4. Une fois l'onglet **Bannières réseau** sélectionné, cliquez sur l'icône d'informations bleues en regard d'un observable.

5. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement** pour afficher les données brutes et plus de détails.

Trouble?

Si vous ne voyez pas les résultats sous les onglets **Résultats d'enrichissement de l'observable** et **Bannières réseau** , vérifiez que l'observable est d'un type pris en charge pour la recherche par l'intégration.

(Facultatif) Joindre manuellement un observable pour Shodan

Vous pouvez joindre manuellement des observables à un incident de sécurité. Vous attachez manuellement des observables lorsque vous souhaitez effectuer des recherches de menaces sur des observables qui ne sont pas joints à un incident de sécurité lors du déclenchement de l'événement initial. En outre, vous pouvez effectuer cette tâche lorsque vous souhaitez obtenir plus d'informations sur un observable connexe.

Avant de commencer

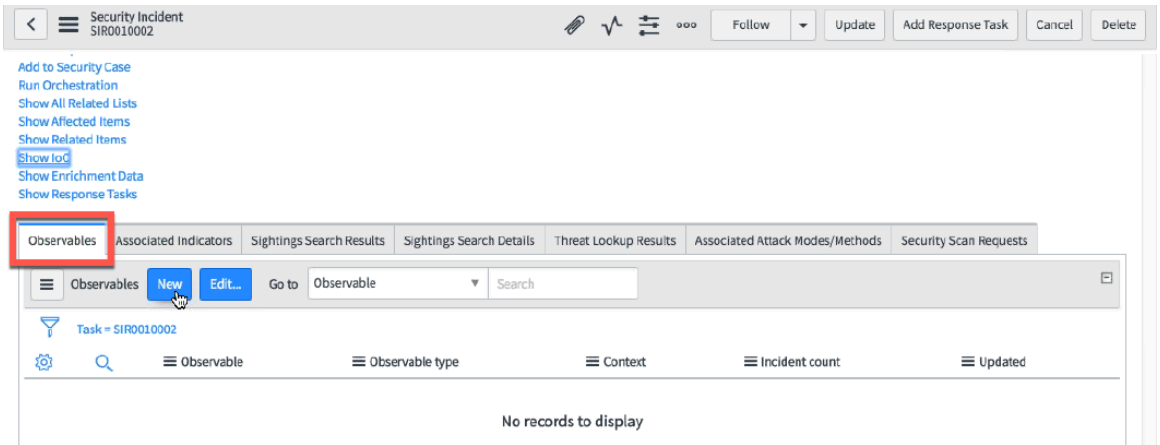
Rôle requis : sn_si.analyst

Procédure

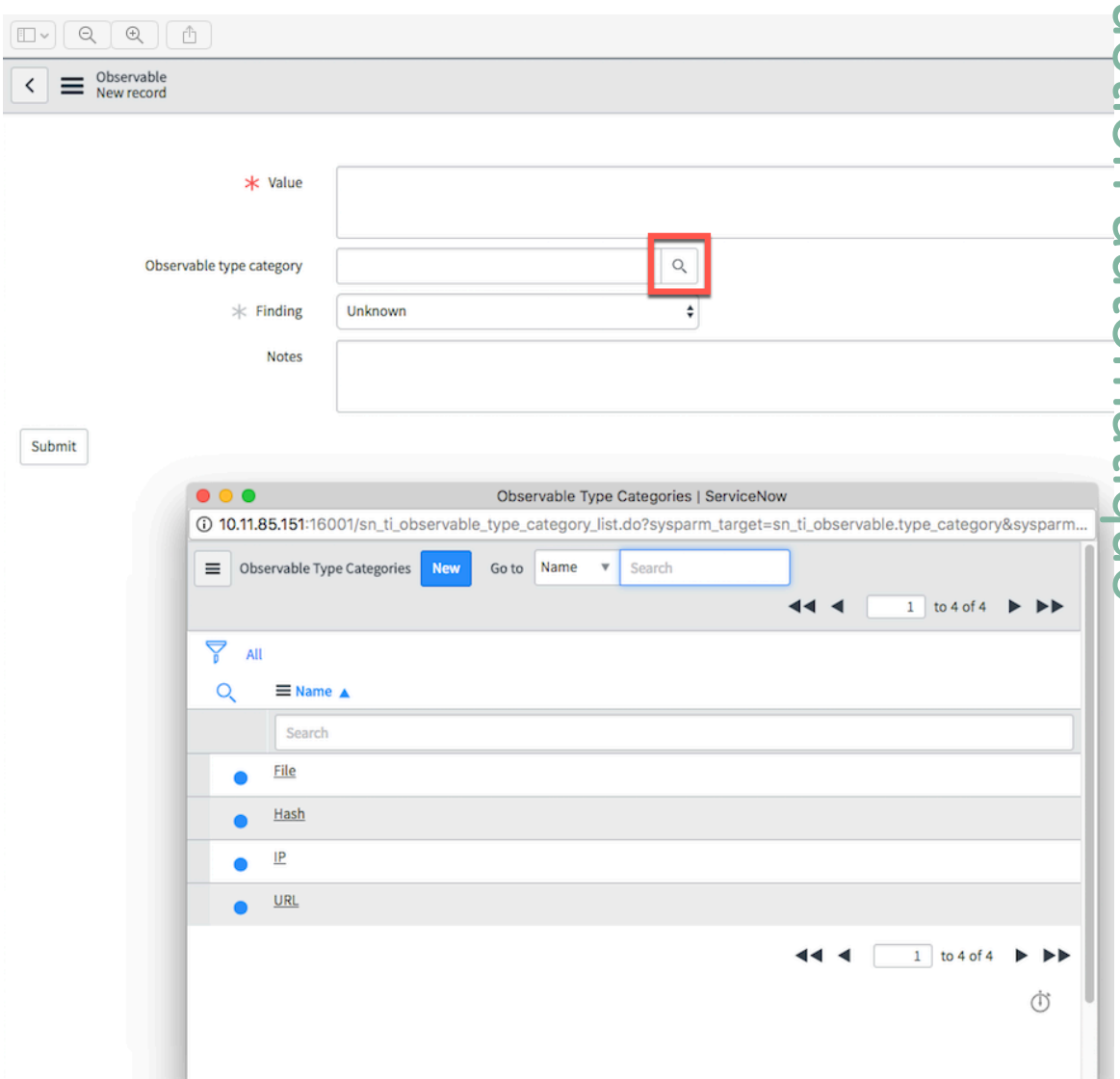
1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents** et ouvrez un incident de sécurité auquel vous souhaitez joindre l'observable.
2. Au bas de l'enregistrement, cliquez sur le lien **Afficher l'IoC**dans les **liens connexes**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans l'onglet **Observables** , cliquez sur **Nouveau**.
   Le formulaire Observable s'affiche.
4. Dans le champ **Valeur** , saisissez un observable (adresse IP ou URL).
5. Cliquez sur l'icône de recherche puis, dans la boîte de dialogue **Catégories de type d'observable** , cliquez sur le type d'observable souhaité dans la liste pour remplir le champ.



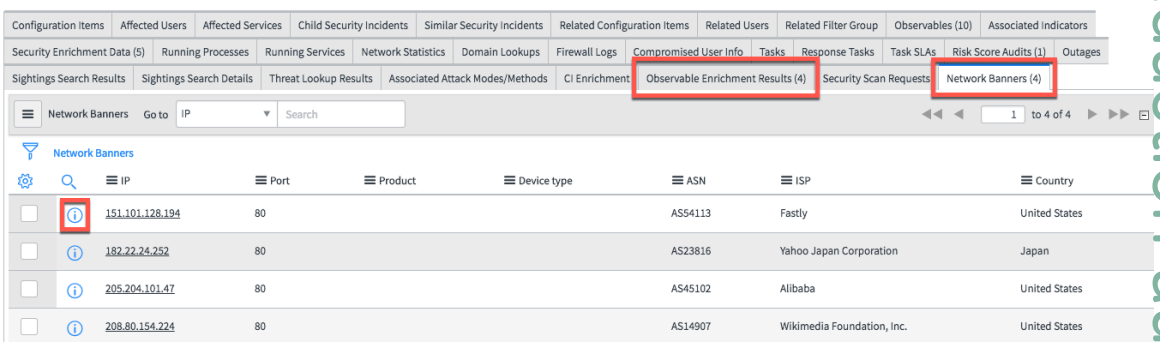
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Envoyer**.
   Le workflow lance et vérifie le nouvel observable. L'état d'exécution et d'achèvement est affiché dans la section des notes de travail de l'enregistrement d'incident de sécurité.
7. Accédez à votre incident de sécurité et passez en revue les notes de travail.



8. Au bas de l'enregistrement, cliquez sur le lien connexe **Afficher toutes les listes connexes** .
9. Cliquez sur les onglets **Résultats de l'enrichissement de l'observable** ou **Bannières réseau** pour les résultats, puis cliquez sur l'icône d'informations bleue en regard d'un observable pour obtenir plus d'informations sur un élément spécifique.



10. Dans la boîte de dialogue qui s'affiche, cliquez sur **Ouvrir l'enregistrement** pour afficher les données brutes et plus de détails.
11. **Facultatif :** Cliquez sur l'icône des paramètres bleus près de l'icône de recherche pour personnaliser la sortie et l'ordre des colonnes.
12. Dans les **colonnes Personnaliser la liste**, sélectionnez les paramètres disponibles, déplacez-les vers la colonne **Sélectionné** , puis cliquez sur **OK**.

Traduction automatique

Trouble?
Passez en revue les **notes de travail** pour plus d'informations et sur la procédure à suivre si vous ne pouvez pas vérifier que la recherche a été effectuée avec succès.

Secureworks CTP Intégration de l'ingestion de tickets

L'intégration Secureworks Counter Threat Platform d'ingestion de tickets vous permet d'extraire Secureworks CTP automatiquement des tickets, de les convertir en incidents de sécurité et d'effectuer des actions de réponse automatisées.

Les principales fonctionnalités de cette intégration sont les suivantes :

- Ingestion automatique des tickets sélectionnés (y compris les pièces jointes) en fonction d'un calendrier prédéfini.
- Mappage des champs de ticket et d'événement aux Réponse aux incidents de sécurité champs.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Aperçu des incidents de sécurité mappés aux champs de ticket.
- Filtrage et agrégation des tickets.
- Récupération sur demande des événements associés à un ticket.
- Suivi périodique des mises à jour clés des tickets.
- Automatisation des mises à jour et des fermetures de tickets en fonction de l'état de l'incident SIR
- Mise à jour du ticket principal.
- Synchronisation des journaux de travail SecureWorks avec Réponse aux incidents de sécurité les notes de travail.

Configurer votre ServiceNow AI Platform instance pour l'intégration de l'ingestion Secureworks CTP de tickets

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre ServiceNow AI Platform instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application afin de garantir une installation et une configuration fluides.

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles et requis ServiceNow AI PlatformRéponse aux incidents de sécurité .	Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre ServiceNow AI Platform instance. • Un utilisateur disposant du rôle d'administrateur ServiceNow AI Platform (admin) installe l'application à partir de et ServiceNow Store lui affecte le rôle d'administrateur SIR (sn_si.admin). • Un utilisateur disposant du rôle sn_si.admin supervise les tâches suivantes dans le ServiceNow AI Platform: ◦ Nomme, crée et modifie des profils. ◦ Sélectionne et mappe Secureworks CTP les champs de ticket aux champs d'incident de sécurité. ◦ Prévisualise les détails de l'incident de sécurité pour plus d'exactitude avant de finaliser la configuration. ◦ Planifie l'ingestion de tickets en cours. ◦ Active la mise à jour des tickets lorsqu'un incident SIR SIR est créé et fermé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	◦ Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst). ◦ Les utilisateurs disposant du sn_si.analyst travaillent sur des incidents de sécurité. Pour plus d'informations sur les rôles et l'attribution de rôles aux utilisateurs, voir Gestion des rôles
Vérifiez que vous utilisez les versions suivantes : • API de ticket SecureWorks 4.0 • API d'événements SecureWorks 1.0 • API d'enrichissement SecureWorks 1.0	Si vous avez accès au Secureworks CTP portail, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant d'installer l'application pour l'intégration.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. 1. Réponse aux incidents de sécurité 2. Ingestion d'événements et d'alertes pour Opérations de sécurité (obligatoire pour les intégrations SIEM) : Cette application nécessite : ◦ com.glide.hub.integration.runtime => Exécution du Centre d'intégration ServiceNow ◦ com.glide.hub.action_step.rest => Étape d'action du Centre d'intégration ServiceNow : REST **Remarque :** Les composants du concentrateur d'intégration sont installés avec le module d'extension d'ingestion d'événements et d'alertes. Si ceux-ci ne sont pas installés, contactez le support client pour obtenir de l'aide. Pour plus d'informations sur l'installation Opérations de sécurité des applications principales, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installez et configurez l'application pour l'intégration ServiceNow d'ingestion de tickets SecureWorks CTP

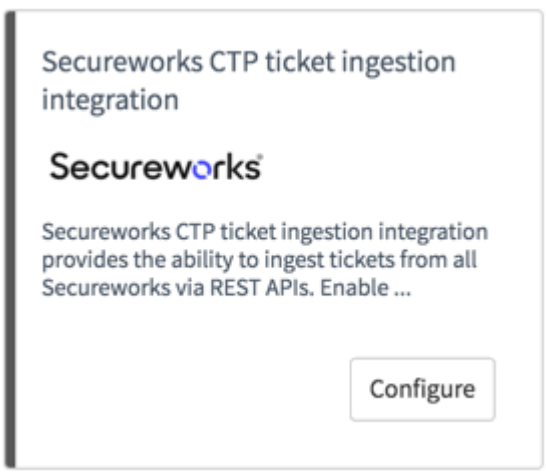
Avant d'exécuter l'intégration sur votre ServiceNow AI Platform instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre correctement aux Réponse aux incidents de sécurité produits sur Opérations de sécurité votre ServiceNow AI Platform instance.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si vous n'avez pas installé l'application Secureworks CTP de ticket à partir de ServiceNow Store pour l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette d'intégration de l'ingestion Secureworks CTP de tickets.



3. Pour configurer l'application, cliquez sur **Nouveau**.
4. Sinon, si un bouton **Configurer** est affiché sur une tuile, cliquez dessus pour modifier une configuration existante.
5. Dans la boîte de dialogue qui s'affiche, renseignez les champs.

Champ	Description
Nom	Nom de l'instance Secureworks CTP utilisée pour l'intégration. Vous ne pouvez saisir que des valeurs al–phanumériques et des traits d'union (-) dans ce champ.
Description	Entrez une description pour le compte d'utilisateur.
Nom d'utilisateur	Saisissez le nom d'utilisateur du compte d'API Se-cureworks CTP . Notez que le nom d'utilisateur est sensible à la casse. Pour trouver le nom d'utilisateur, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Connectez-vous au Secureworks CTP portail. ○ Accédez à la **Compte** > **Gestion des comptes** > **Informations d'identification API**. Le nom d'utilisateur s'affiche sur la page Informations d'identification de l'API.
Mot de passe de l'API	Saisissez le mot de passe de l'API Secureworks CTP . Pour trouver le mot de passe de l'API, procédez comme suit : ○ Connectez-vous au Secureworks CTP portail. ○ Accédez à la **Compte** > **Gestion des comptes** > **Informations d'identification API**. Le mot de passe de l'API s'affiche sur la page Informations d'identification de l'API. Pour plus d'informations sur la façon d'obtenir le nom d'utilisateur et le mot de passe de l'API, suivez les étapes de la section Génération d'une clé API persistante du Guide de l'API de billetterie Secure-Works.

6. Cliquez sur **Envoyer**.
   Une fois validée et soumise, chaque configuration est enregistrée sur la page Intégrations de sécurité sous forme de vignette.

Résultats

Si vos mosaïques de configuration enregistrées ne sont pas affichées sur la page Intégrations de sécurité. Dans le coin supérieur droit de la page, dans la liste de choix **Afficher les configurations** , cliquez sur **Oui**.

Créer un profil pour l'intégration de l'ingestion de tickets SecureWorks CTP

Créez un profil dans votre ServiceNow AI Platform instance et déterminez quels tickets doivent être ingérés et quels tickets seront utilisés pour créer des incidents de sécurité. Avant que des incidents de sécurité ne soient créés à partir de tickets ingérés, les valeurs de champ des tickets sont affichées sur une mise en page d'un ServiceNow AI Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera affiché.

L'intégration vous permet d'ingérer des tickets en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance. Tous les tickets sont initialement ingérés pour un type de ticket configuré dans un profil. Les tickets ingérés peuvent ensuite être filtrés davantage pour spécifier quels tickets créent des incidents de sécurité.

Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les tickets identifiés comme à haut risque. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir de tickets ingérés, les valeurs de champ individuelles des tickets sont mappées aux champs correspondants sur une mise en page d'incident de sécurité pour un aperçu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identifier la source du profil

Indiquez le nom et la source du profil.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Pour créer un profil pour un ticket dans votre ServiceNow AI Platform instance, accédez à **Intégration de l'ingestion de tickets SecureWorks** > **Profils Secureworks**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs.

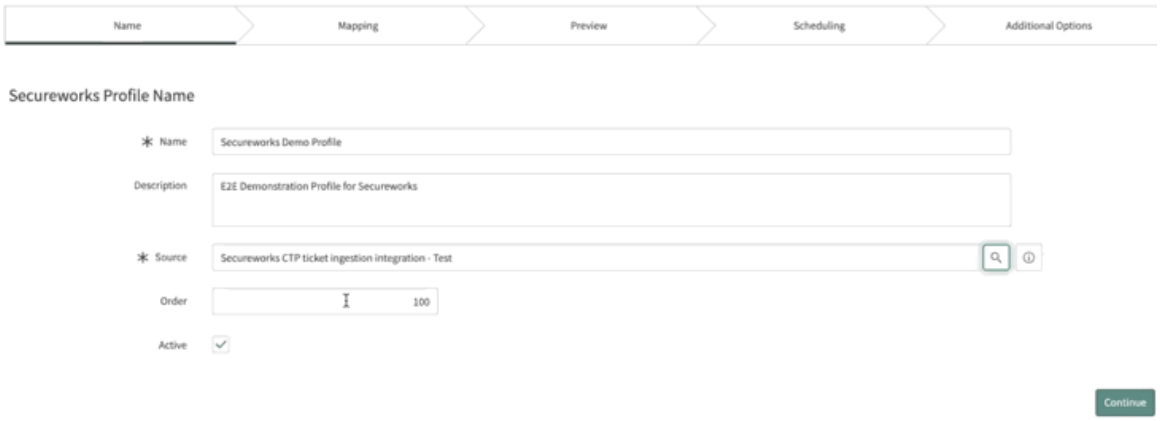
   Un exemple de formulaire rempli suit la table.

Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre ServiceNow AI Platform instance doivent être uniques.
Source	Sélectionnez la source à partir de laquelle vous souhaitez ingérer les données.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Plus la valeur de commande est faible, plus la priorité est élevée.
Actif	Cette option est désactivée par défaut. Si cette option est désactivée, le profil n'est pas actif. **Remarque :** Vous devez remplir toutes les sections du profil avant de l'activer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La figure suivante est un exemple de formulaire rempli.



Que faire ensuite

Mappez les champs de ticket.

Mappage des champs de ticket pour l'intégration SecureWorks CTP

Mappez les champs de ticket et d'événement aux champs du formulaire d'incident de sécurité.

Pour l'étape de mappage, vous devez d'abord ingérer des exemples de tickets, puis vous assurer que tous les champs de ticket pertinents sont mappés à l'endroit approprié sur le Réponse aux incidents de sécurité formulaire, puis visualiser l'incident de sécurité dans la section d'aperçu.

Le mappage des champs d'exemple de ticket implique les éléments suivants :

- Extraction et remplissage des exemples de données : Voir Ingestion de l'échantillon de tickets SecureWorks
- Mappage des champs de ticket à l'incident de sécurité : voir Mappage des champs de ticket SecureWorks aux champs Réponse aux incidents de sécurité

Ingestion de l'échantillon de tickets SecureWorks

Sélectionnez les exemples de tickets à ingérer.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Vous pouvez soit extraire les cinq échantillons de tickets les plus récents, soit fournir les ID de ticket uniques pour les tickets spécifiques que vous souhaitez utiliser pour votre expérience de mappage.
   Dans la liste de choix **Préférence d'ingestion** , sélectionnez l'une des options suivantes :
   - Récupérer les tickets les plus récents : les 5 tickets les plus récents sont récupérés.
   - Sélectionner les tickets en fonction de l'ID du ticket : spécifiez l'ID du ticket pour que le ticket soit récupéré. Vous pouvez spécifier un maximum de 5 ID de tickets séparés par des virgules.
3. Cliquez sur **Extraire les données d'échantillon** pour extraire les dernières données d'échantillon de ticket à partir du Secureworks CTP serveur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’extraction des billets d’échantillon peut prendre quelques instants. Un message indiquant que la transaction fonctionne s’affiche en haut de l’écran. Les tickets récupérés sont affichés sous forme d’onglets individuels. Cliquez sur un onglet pour afficher les données du ticket. Pour chaque ticket, vous pouvez voir les champs de ticket et leurs valeurs, ainsi que les détails de l’événement de contribution qui a déclenché le ticket.

Remarque : Vous verrez les détails des événements de contribution uniquement s’ils se sont produits au cours des 7 derniers jours. Les événements de plus de 7 jours ne sont pas affichés.

Que faire ensuite

Une fois que vous avez extrait les exemples de données, l’étape suivante consiste à mapper les champs de ticket à l’incident de sécurité.

Mappage des champs de ticket SecureWorks aux champs Réponse aux incidents de sécurité

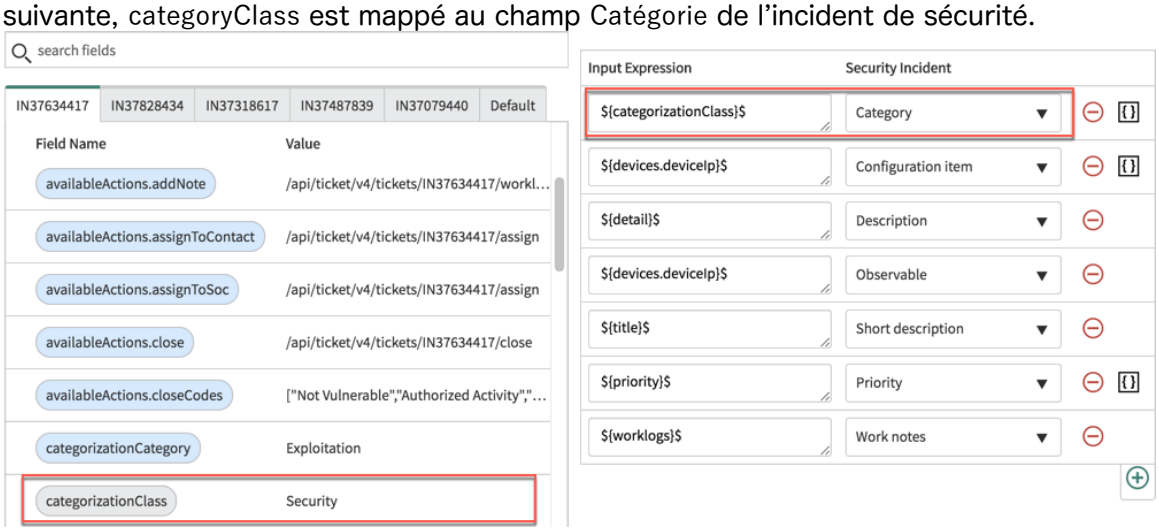
Mappez les champs de ticket ou d’événement individuels aux champs d’un ServiceNow AI Platform SIR incident de sécurité.

Mappage de champs de ticket

En tant qu’utilisateur disposant du rôle sn_si.admin, utilisez les champs de la section Exemples de tickets à gauche et mappez-les aux champs d’incident de sécurité de la colonne **Mappage de champ d’incident SIR** . Modifiez la configuration du mappage en faisant glisser les champs de ticket ou d’événement à gauche et en les déposant dans la section Mappage du champ d’incident SIR à droite. Le mappage sur la droite associe le champ de ticket entrant à un champ d’incident de sécurité sortant.

1. Pour faire correspondre une valeur de champ du côté gauche du formulaire à un champ de l’incident de sécurité sur le côté droit du formulaire, cliquez tout en maintenant enfoncé le nom d’un champ bleu sur le côté gauche du formulaire.
2. Vous pouvez saisir manuellement le nom du champ dans la colonne Expression d’entrée ou glisser-déplacer le nom du champ. Par exemple, la description, et déposez-la dans un champ de la colonne **Expression d’entrée** à côté d’un nom de champ dans la colonne **Incident de sécurité** .

   La valeur du champ est affichée dans la colonne Expression d’entrée. Dans l’image suivante, categoryClass est mappé au champ Catégorie de l’incident de sécurité.



Remarque : Si vous saisissez manuellement le nom du champ d’événement dans la section **Expression d’entrée** , vous devez ajouter un préfixe `${Event :eventfield}$` avant le nom du champ en cours de mappage.

Traduction automatique

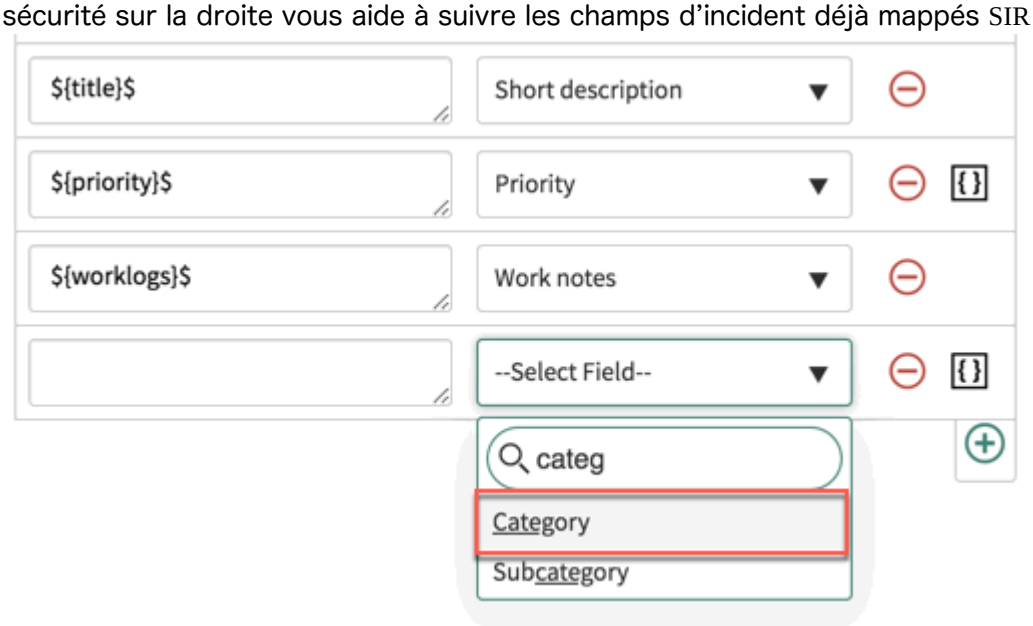
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour vous assurer qu'aucun champ de ticket ou d'événement n'est négligé ou dupliqué dans le processus de mappage, des champs sont codés par couleur. Le code couleur des champs de ticket vous aide à suivre les valeurs de ticket que vous avez déjà mappées, car elles deviennent grisées, tandis que tous les champs non mappés restants apparaissent en bleu. Cela vous aide à visualiser mieux quelles valeurs de champ ont été ajoutées à l'incident de sécurité et si des informations de ticket importantes restantes restent non mappées.

Les champs bleu clair sur la gauche indiquent qu'un champ de ticket n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un ticket entrant ou un champ d'événement à plusieurs champs d'un incident de sécurité. Un champ gris indique qu'un champ a été sélectionné et mappé à un champ de l'incident de sécurité. Ce code couleur vous aide à suivre le mappage.

3. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit :
   a. À droite du formulaire, dans la section Mappage du champ d'incident SIR , en bas de la grille, cliquez sur l'icône plus (+). Un nouveau champ s'affiche.
   b. Dans la colonne Incident de sécurité, développez la liste de choix qui s'affiche, puis sélectionnez un champ.

      Dans la liste de choix développée pour le nouveau champ, certains champs sont ombrés. Dans la figure suivante, la catégorie a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. Semblable au code couleur pour les champs de ticket sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident déjà mappés SIR .



Remarque : Comme plusieurs observables peuvent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs.
Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité possède une liste de choix dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste de choix, le champ n'est pas renseigné sur l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Vous pouvez également saisir une valeur dans le champ Rechercher de la nouvelle ligne.

d. À gauche du formulaire, sélectionnez le champ Ticket et faites-le glisser vers un champ d'incident de sécurité approprié à droite.

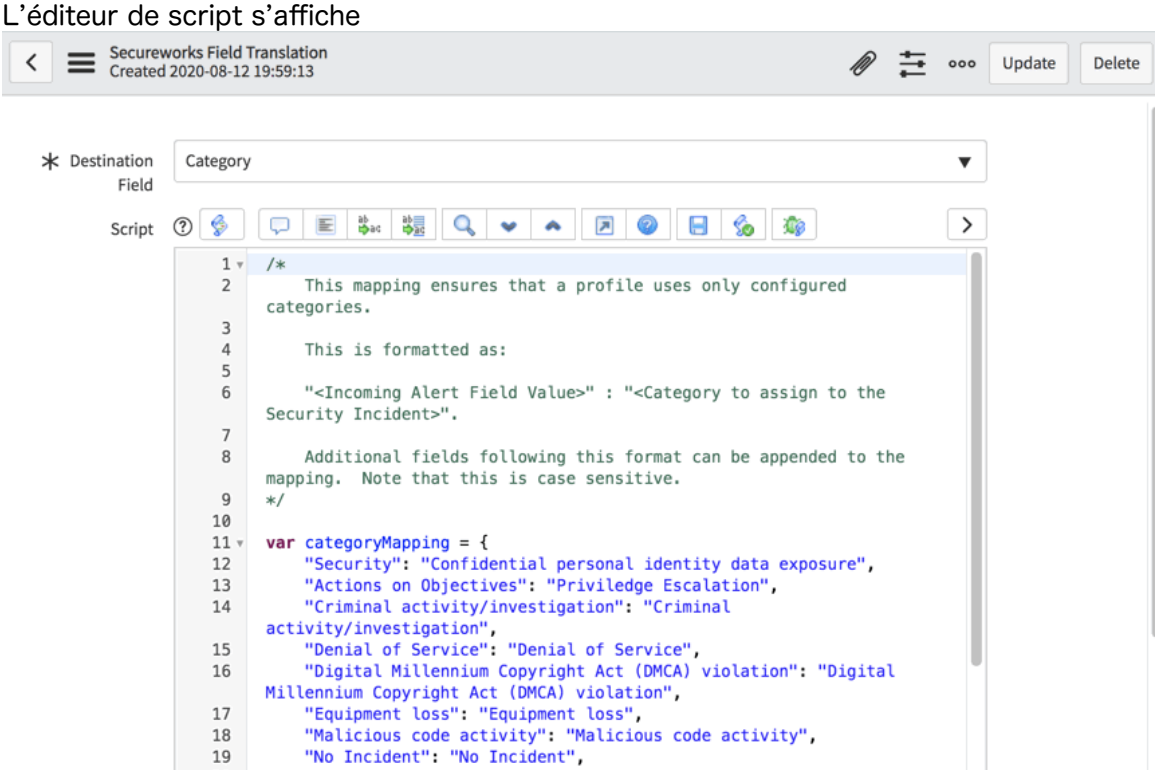
4. Supprimez les champs à l'aide de l'icône - en regard du nom du champ dans la section Mappage du champ d'incident SIR.

5. Poursuivez le mappage en ajoutant ou en supprimant des valeurs de champ au mappage.

Formater la traduction du champ

Dans certains cas, les champs de ticket peuvent ne pas se traduire directement dans les champs de l'incident SIR de sécurité. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident de sécurité à l'aide de la SIR fonctionnalité Formater la traduction du champ.

Pour utiliser l'éditeur de script, cliquez sur l'icône {} en regard du champ Catégorie. L'éditeur de script s'affiche



.

Entrez les modifications apportées au script, cliquez sur **Mettre à jour** pour enregistrer les modifications et revenir à la page Mappage.

Conditions de génération d'incidents

Une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de pouvoir spécifier quels tickets doivent créer des incidents de sécurité par rapport à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ceux qui doivent être filtrés (par exemple, les tickets de priorité faible). Vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incidents pour définir des critères supplémentaires qu'un ticket entrant doit satisfaire pour créer un incident de sécurité. Pour définir les conditions de génération d'incidents, procédez comme suit.

1. Faites défiler la page jusqu'à la section **Conditions de génération d'incidents** sur le formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

   Le générateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

   Les options des listes de choix pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section **Exemple d'ingestion de ticket** pour les tickets ingérés. Ces champs sont dynamiques et changent en fonction des tickets que vous ingérez. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux Secureworks CTP valeurs du ticket. Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférerez peut-être retourner à votre Secureworks CTP console et vérifier vos tickets pour les mots-clés.

   Remarque : Les *champs de ticket des journaux de travail*, *des appareils*, *des pièces jointes*, *des observateurs*, des *actions disponibles* et des *codes de fermeture* peuvent avoir plusieurs valeurs (car les valeurs sont stockées dans des tableaux). Comme la condition de filtre ne peut récupérer que des chaînes, vous devez utiliser la condition de filtre *contient* pour ces champs afin de vous assurer que les données sont filtrées correctement.

2. À l'aide des listes de choix et des champs du générateur de conditions, définissez des filtres pour la première ligne.
3. Pour ajouter plus de conditions, à droite des champs, cliquez sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. (Facultatif) Sur la deuxième ligne, définissez une deuxième condition de filtre.

   Ce type de filtrage des conditions de génération d'incidents vous aide à affiner les tickets et à limiter le nombre d'incidents de sécurité inutiles que vous créez sans modifier la règle ou les filtres sous-jacents. Si des critères de filtrage supplémentaires sont définis, seuls les tickets qui correspondent à tous les critères sont mappés aux incidents de sécurité.

Critères d'agrégation de tickets pour gérer des tickets similaires et éviter les incidents en double

Définissez des critères d'agrégation de tickets supplémentaires qui regroupent un ticket entrant à un incident de sécurité existant SIR au lieu de créer des incidents similaires potentiellement en double. En utilisant des critères de correspondance de champ pour chaque profil, cette option d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données de ticket connexes sur un seul incident de sécurité. Pour définir les critères, procédez comme suit ci-dessous :

1. Faites défiler jusqu'à la section **Critères d'agrégation de tickets** sur le formulaire et cochez la case Conditions **d'agrégation** pour activer cette option.

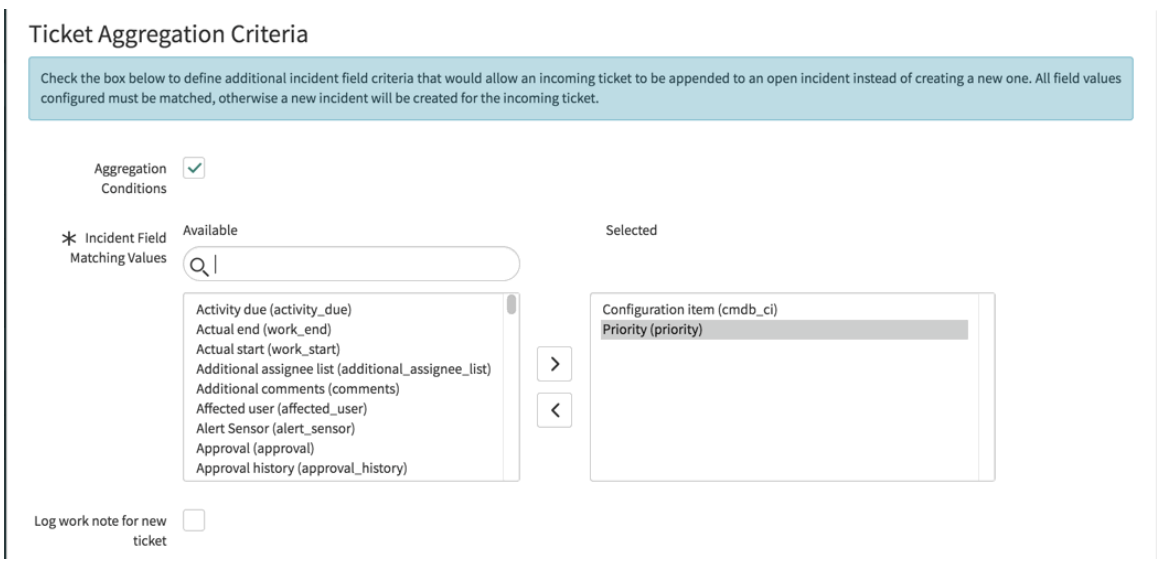
   Les colonnes Valeurs correspondantes au champ Incident s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés sur l'incident SIR de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans votre NOW Platform et déplacez-les vers la liste Sélectionné.

   Toutes les valeurs de champ que vous sélectionnez doivent correspondre pour ajouter ce ticket entrant à un incident de sécurité existant. Cela inclut les champs, tels que les observables et les éléments de configuration, auxquels plusieurs valeurs de champ de ticket peuvent être mappées. Toutes les valeurs doivent correspondre. Si seul un sous-ensemble des valeurs correspond, les conditions d'agrégation de tickets ne seront pas remplies et un nouvel incident de sécurité sera créé. Voir la capture d'écran ci-dessous pour le mappage de champs à valeurs multiples.



   Si un nouveau ticket correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation à l'étape de mappage, le nouveau ticket est automatiquement ajouté à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher tous les tickets agrégés ajoutés sur une liste connexe sur un incident de sécurité. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi ces tickets sont regroupés à des incidents de sécurité existants. Si cet onglet n'est pas affiché dans un incident de sécurité, faites défiler l'enregistrement vers la gauche sous **Liens connexes** et cliquez sur le lien **Afficher toutes les listes connexes** .

   Remarque : La liste connexe des tickets agrégés SecureWorks n'est pas disponible avec le système de base. Vous devez configurer la mise en page de la liste connexe et l'inclure explicitement avec les autres listes connexes.

3. (Facultatif) Pour enregistrer une note de travail pour un nouveau ticket récemment ajouté à l'incident de sécurité, cochez cette case pour activer cette option. La note de travail indique qu'un nouveau ticket a été ajouté, ainsi qu'un lien vers les détails du ticket et tout autre détail qui a pu être ajouté au champ Note de travail dans votre section de mappage.

   Vous avez correctement mappé les valeurs d'un Secureworks CTP ticket aux champs d'un incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage de génération d'incidents. Vous avez également ajouté des tickets aux incidents de sécurité existants

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

lorsque les valeurs des champs ticket correspondent aux critères d'agrégation configurés.

4. Cliquez sur **Continuer** pour poursuivre la configuration du profil. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité

Prévisualiser les valeurs mappées dans l'incident de sécurité

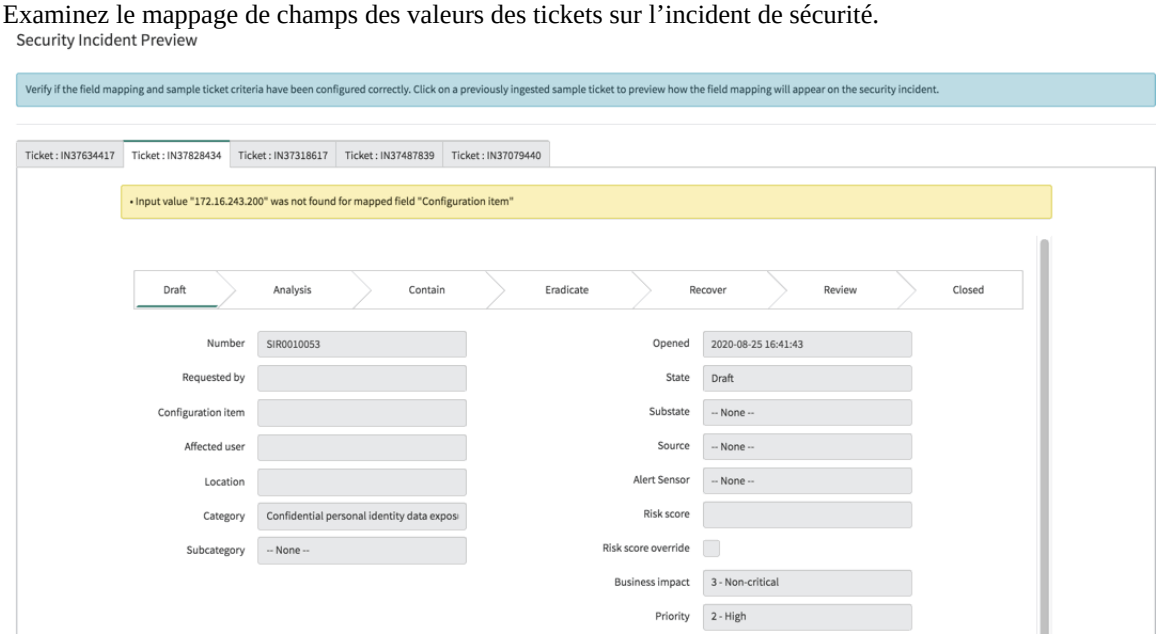
Une fois l'étape de mappage terminée, affichez un aperçu des valeurs que vous avez mappées dans un SIR incident de sécurité. Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs de ticket que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas effectué avec succès, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de sécurité ne sont pas enregistrés en tant qu'incidents SIR réels dans le produit Security Incident Response.

Procédure

1. Si l'aperçu de l'incident de sécurité ne s'affiche pas, cliquez sur **Aperçu** dans la barre de progression.
   Les tickets sont affichés sous forme d'onglets.
2. Cliquez sur un onglet pour prévisualiser l'incident de sécurité.
   Cette vue est en lecture seule et aucun enregistrement de cet incident de sécurité n'est enregistré.
3. Examinez le mappage de champs des valeurs des tickets sur l'incident de sécurité.



L'image précédente est un exemple d'aperçu avec une erreur de mappage des échantillons qui ont été ingérés.

4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage des champs sur l'incident de sécurité. Définissez le calendrier.

Définir un calendrier pour l'ingestion de tickets SecureWorks CTP

Vérifiez les paramètres par défaut pour la récupération de ticket ou modifiez la planification si nécessaire. Cette étape vous permet de filtrer votre récupération de ticket en fonction d'une plage de dates et d'un intervalle d'interrogation.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous choisissez également la fréquence à laquelle vous interrogerez les futurs tickets qui correspondent à la configuration du profil de ticket. Configurez ces intervalles d'interrogation par profil. Lors de la planification, vous préférez peut-être équilibrer la charge du système par rapport à l'urgence de l'incident. Une valeur par défaut d'une minute est définie pour n'importe quel profil, mais vous préférez peut-être modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

Procédure

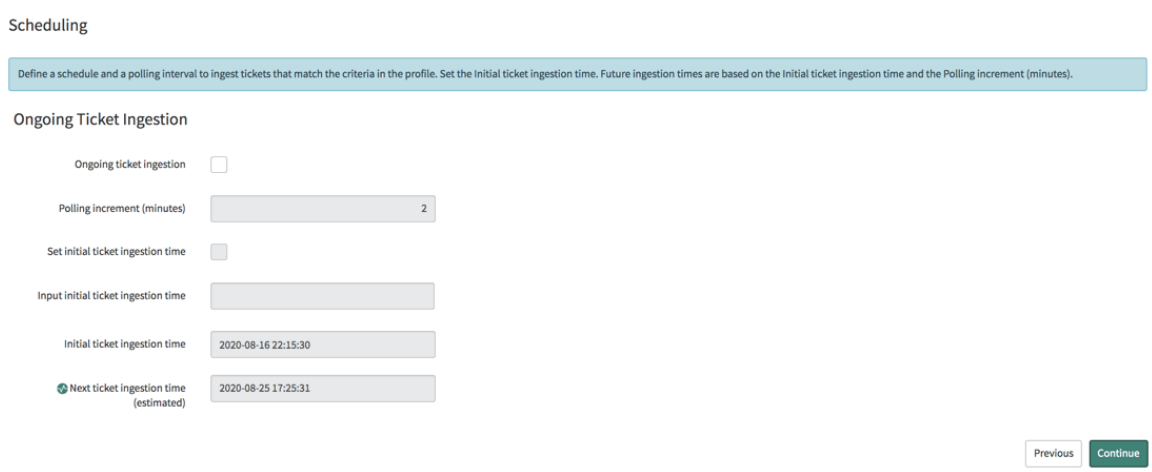
1. Si la page Planification de la barre de progression ne s'affiche pas, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les tickets sont extraits du Secureworks CTP portail.

Option	Description
Ingestion de ticket en cours sélectionnée	En fonction du paramètre par défaut, l'instance ServiceNow AI Platform extrait du Secureworks CTP portail de nouveaux tickets toutes les cinq minutes. Les incidents de sécurité sont créés si des tickets sont trouvés et que les critères de filtrage de génération d'incidents sont correspondants. Pour équilibrer l'ingestion de tickets par rapport à la charge du serveur, et pour extraire les données les plus récentes, vous préférez utiliser cinq minutes. Toutefois, cette valeur peut être modifiée si nécessaire.
○ Ingestion de ticket en cours sélectionnée ○ Définir le délai d'ingestion du ticket initial	Délai d'ingestion initial Si vous souhaitez planifier l'ingestion initiale à une heure précise, procédez comme suit : ○ Sélectionnez les champs Ingestion de ticket en cours et Définir le délai d'ingestion du ticket initial. ○ Spécifiez l'heure dans le champ Entrer le délai d'ingestion du ticket initial. L'ingestion initiale aura lieu à l'heure spécifiée ici. Les ingestions suivantes seront basées sur le calendrier défini dans le champ Incrémentation de l'interrogation (minutes). À titre d'exemple pour la planification, si vous avez une tâche de ticket quotidienne qui s'exécute une fois par jour à 4 heures, heure locale, vous pouvez configurer le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	profil de ticket correspondant dans votre ServiceNow AI Platform instance pour qu'il s'exécute à 4 h 05, heure locale, afin de capturer immédiatement le ticket et de créer un incident de sécurité. Saisissez 04 05 00 dans le champ Inges–tion de ticket initiale. Dans le champ In–crémentation du sondage (minutes), sai–sissez 1 440 (24 heures) pour planifier la prochaine ingestion de ticket pendant 24 heures à compter de l'ingestion de ticket initiale. Le délai d'ingestion du ticket initial et l'heure d'ingestion du ticket suivant sont affichés dans les champs. Pour configurer les paramètres de cet exemple, procédez comme suit : ○ Sélectionnez l'option **Ingestion de ticket en cours** . ○ Dans le champ Incrémentation de l'inter–rogation (minutes), saisissez 1440 (24 heures). ○ Sélectionnez l'option **Définir le délai d'in gestion du ticket initial** . ○ Dans le champ Entrer le délai d'inges–tion du ticket initial, saisissez 04 05 00. L'heure de la prochaine ingestion de ti–cket est affichée dans le champ Délai d'ingestion du ticket suivant (estimé).



3. Cliquez sur **Continuer** pour accéder à la page Options supplémentaires.

Automatiser les mises à jour et la fermeture des tickets en fonction de l'état de l'incident SIR

L'intégration Secureworks CTP d'ingestion de tickets dispose d'une interface bidirectionnelle qui permet aux tickets de créer des incidents de sécurité, ainsi qu'une possibilité de mettre à jour les tickets une fois l'incident de sécurité créé et/ou fermé avec les détails pertinents

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de l'incident tels que le numéro de l'incident de sécurité, le groupe d'affectation, l'URL de l'incident de sécurité, et ainsi de suite.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Si la page Options supplémentaires de la barre de progression ne s'affiche pas, sélectionnez **Options supplémentaires**.
2. Terminez la configuration de la mise à jour des tickets lors de la création de l'incident de sécurité.

Option ou champ	Description
Mettre à jour les notes de travail SIR avec les journaux de travail SecureWorks	Sélectionnez cette option pour activer la fonctionnalité de synchronisation des journaux de travail et SIR des notes de travail SecureWorks. Cela vous permet de suivre les mises à jour apportées au ticket Secureworks CTP après la création de l'incident de sécurité. **Remarque :** ○ Si le champ des journaux de travail SecureWorks a été mappé au champ des notes de travail SIR, les journaux de travail SecureWorks sont récupérés jusqu'à la création de l'incident de sécurité. ○ Si la fonctionnalité de synchronisation est activée, seuls les journaux de travail créés ou mis à jour après la création d'un incident de sécurité sont récupérés.
Mettre à jour les tickets SecureWorks lors de la création de l'incident SIR	Sélectionnez cette option pour mettre à jour le Secureworks CTP ticket et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir du ticket. Cela peut se produire à la fois pour les tickets déclencheurs initiaux qui créent l'incident de sécurité et pour les tickets agrégés.
Commentaires initiaux envoyés au ticket SecureWorks	Lorsqu'un incident de sécurité est créé, le ticket est automatiquement mis à jour Secureworks CTP avec des commentaires. Vous pouvez modifier le texte par défaut et utiliser le format ${nom de champ}$ pour ajouter ou modifier les champs disponibles dans le formulaire d'incident de sécurité.
Fermer les tickets SecureWorks lors de la fermeture de l'incident SIR	Sélectionnez cette option si vous souhaitez utiliser l'option de fermeture de ticket automatisée. Cela peut se produire à la fois pour les tickets déclencheurs initiaux qui créent l'incident de sécurité et pour les tickets agrégés. Lorsqu'un incident de sécurité est fermé, le ticket correspondant est automati-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	quement fermé Secureworks CTP avec le même code de fermeture que l'incident de sécurité et les commentaires de fermeture par défaut spécifiés dans le profil. **Remarque :** Vous ne pouvez pas utiliser cette option pour mettre à jour le statut du Master Ticket.
Commentaires de fermeture envoyés au ticket SecureWorks	Les commentaires de fermeture par défaut sont affichés ici. Vous pouvez modifier le texte par défaut et utiliser le format ${nom de champ}$ pour ajouter ou modifier tous les champs disponibles dans le formulaire d'incident de sécurité.

3. Cliquez sur **Terminer** pour terminer la configuration et faire passer le profil à l'état **En attente** .
   Une boîte de dialogue de confirmation s'affiche. Vous avez configuré le profil avec succès. Activez ce profil pour extraire des tickets du portail en fonction de Secureworks CTP votre planification.

Facultatif : copier un profil CTP SecureWorks

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils pour gagner du temps.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
En tant qu'utilisateur disposant du rôle sn_si.admin, si vous copiez un profil, le nom du profil est initialement modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) et n'est donc pas activé accidentellement avant de terminer la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

1. Accédez à la **Tous** > **Intégration de l'ingestion de tickets SecureWorks** > **Profil SecureWorks**.
2. Dans la liste Profils SecureWorks qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix **Actions sur les lignes sélectionnées** , cliquez sur **Copier**.
   Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient (copie). Bien que le profil d'origine soit activé (vrai), la copie est désactivée à ce stade (faux). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.

   Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil. Notez que l'état de la colonne **Actif** est défini sur faux, car le profil doit être activé.

Que faire ensuite
Vous êtes invité à activer le nouveau profil une fois que vous avez terminé les étapes de configuration.

Traduction automatique

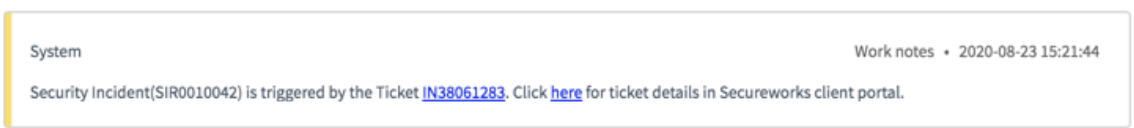
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Changements apportés au formulaire Réponse aux incidents de sécurité après l'ingestion du ticket

Une fois qu'un Secureworks CTP ticket a été ingéré, un incident de sécurité est créé et les mises à jour correspondantes sont apportées à l'enregistrement d'incident de sécurité.

Notes de travail

Une note de travail contenant les détails du ticket qui a déclenché l'incident de sécurité est publiée.



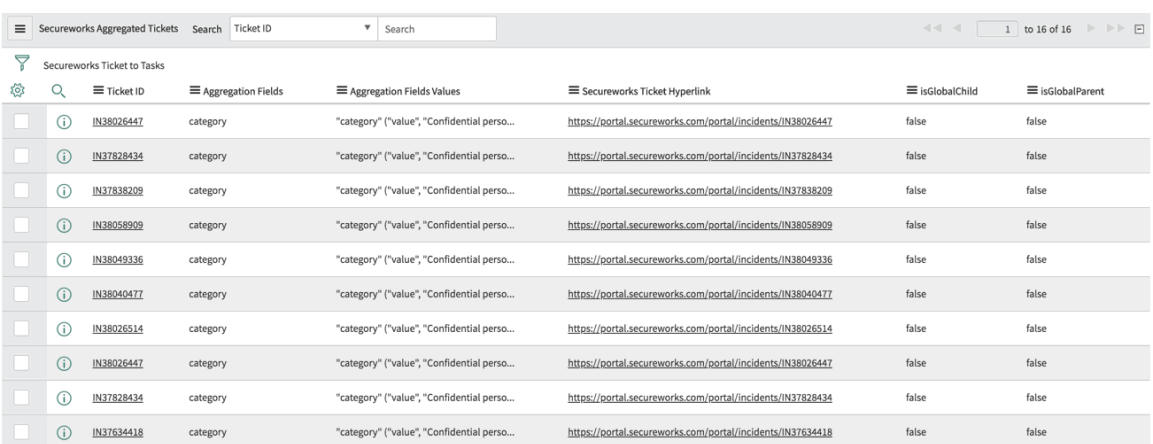
Cliquez sur le lien du ticket pour accéder à l'enregistrement interne du ticket de tâche SecureWorks. Le lien hypertexte **« Cliquer ici »** vous dirige vers le tableau de Secureworks CTP bord où vous pouvez afficher les détails du ticket.

Si vous aviez sélectionné l'option **Enregistrer la note de travail pour le nouveau ticket** dans les critères d'agrégation de tickets, comme décrit dans la page Créer un profil : mappage, une note de travail est publiée lorsque le ticket est agrégé.



Tickets agrégés

Cliquer sur **Listes connexes** > **Tickets agrégés SecureWorks** pour afficher le ticket agrégé à l'incident de sécurité. Cliquez sur le lien hypertexte du ticket pour afficher le ticket dans le tableau de Secureworks CTP bord.



Créer un incident de sécurité : sélectionnez un ticket dans la liste, cliquez sur le menu **Actions** , puis sur **Créer un incident de sécurité**. Cette option crée un nouvel incident de sécurité pour le ticket et ce ticket est désagrégé de l'incident de sécurité parent.

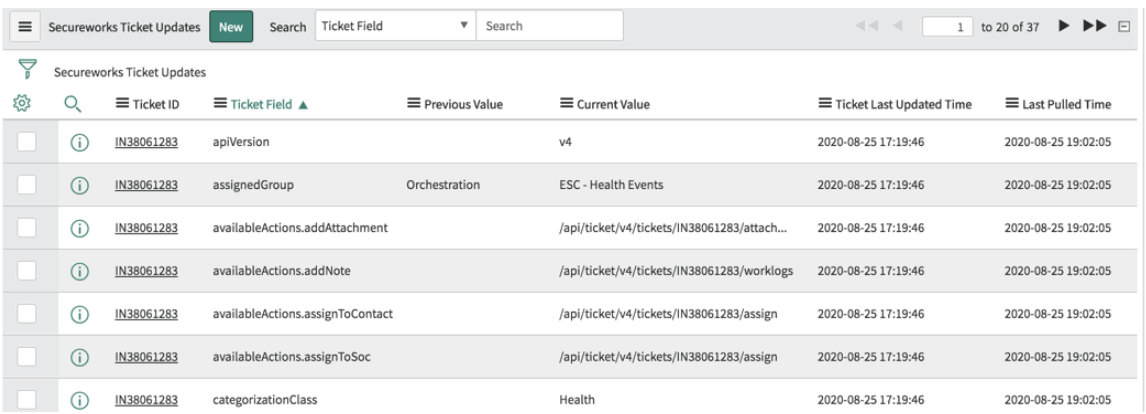
Supprimer l'enregistrement de ticket : sélectionnez un ticket dans la liste, cliquez sur le menu **Actions** , puis sur **Supprimer**. Cette option supprime l'enregistrement du ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

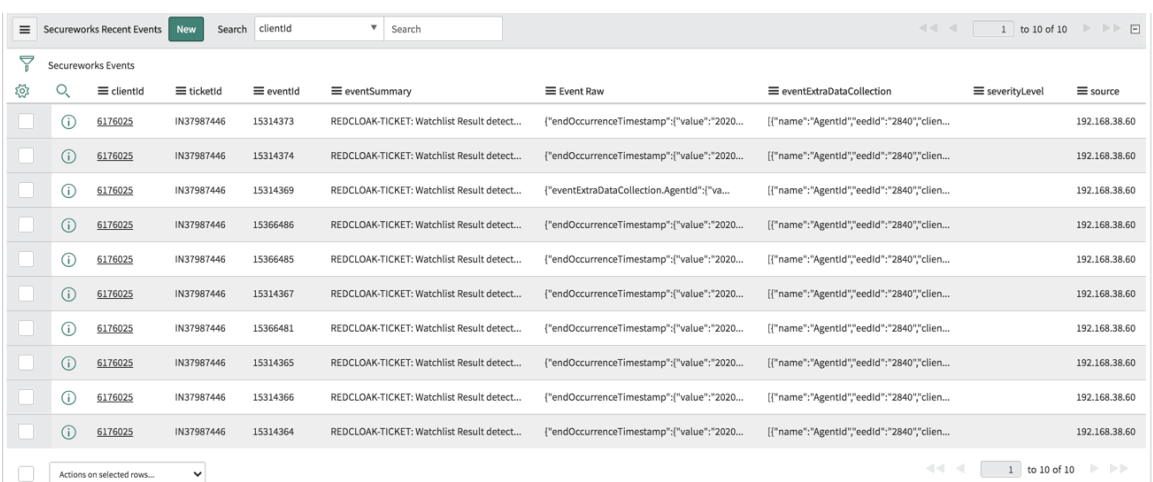
Mises à jour des tickets SecureWorks

Cela montre les champs de ticket standard et suit les changements apportés aux tickets à chaque intervalle d'interrogation. Ceci est utile car vous pouvez afficher directement toutes les mises à jour de tickets sans accéder au tableau de Secureworks CTP bord. Tout changement apporté aux valeurs est affiché dans les champs Valeur précédente et Valeur actuelle.



Événements récents SecureWorks

Cliquez sur l'option **Extraire les événements SecureWorks récents** sous les **liens connexes pour** afficher les événements SecureWorks les plus récents.



Par défaut, un nombre maximum de 50 événements sera affiché. Vous pouvez modifier ce paramètre par défaut dans les paramètres d'intégration SecureWorks.

Afficher les tickets SecureWorks et les incidents de sécurité correspondants

Les tickets importés Secureworks CTP sont initialement stockés dans la table d'importation de billets. Affichez tous les Secureworks CTP tickets qui ont été importés avant que toute condition de filtre ne soit appliquée.

Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intégration de l'ingestion de tickets SecureWorks** > **Importation sécurisée du ticket**.
2. Vous pouvez afficher tous les tickets qui ont été importés avant qu'ils Secureworks CTP ne soient regroupés ou que des conditions de filtre ne soient appliquées.
3. Cliquez sur un ID de ticket pour afficher les données brutes du ticket.
4. Accédez à la **Ingestion de tickets SecureWorks** > **Ticket SecureWorks pour la tâche**.
   Les Secureworks CTP tickets et leurs incidents de sécurité correspondants sont affichés.

Avis de fermeture de ticket principal SecureWorks CTP

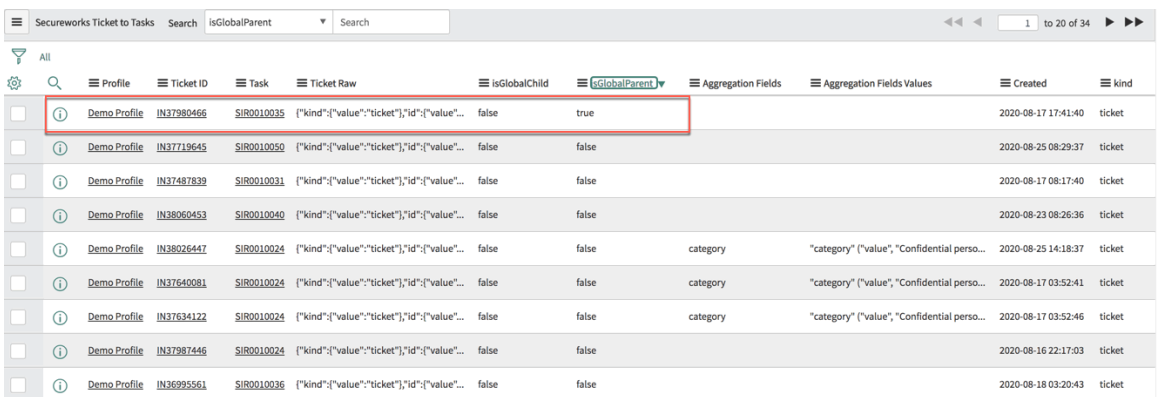
Avant de fermer un incident de sécurité créé par un Secureworks CTP ticket principal, vous devez vérifier que tous les tickets enfants associés au ticket principal sont fermés.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

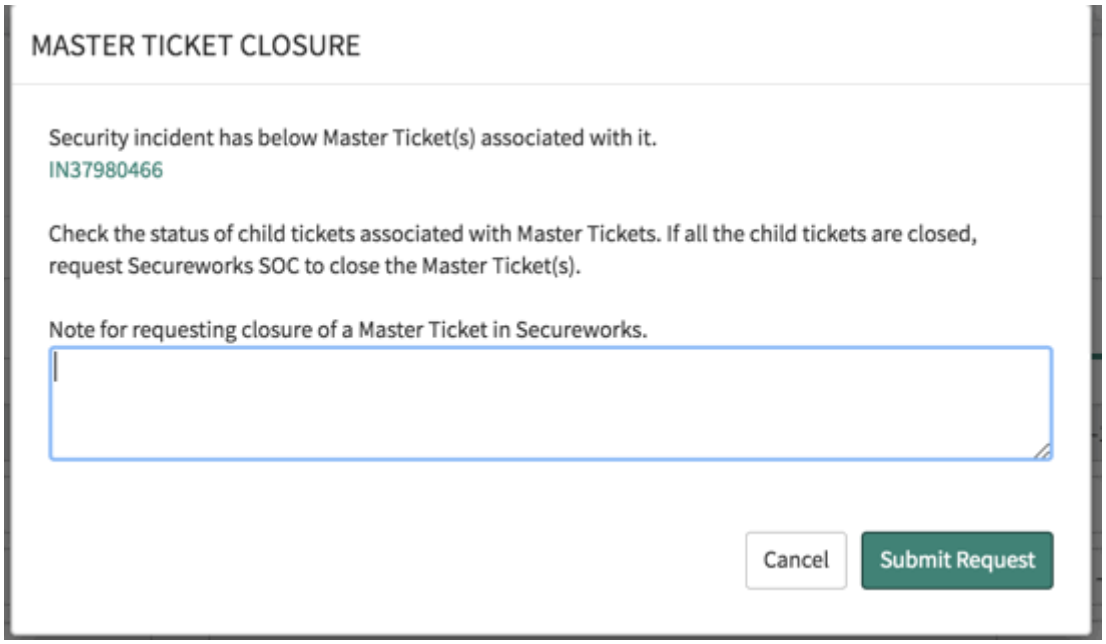
1. Accédez à la **Tous** > **Ingestion de tickets SecureWorks** > **Ticket SecureWorks pour la tâche**.
   Les Secureworks CTP tickets et leurs incidents de sécurité correspondants sont affichés.



2. Cliquez sur l'incident de sécurité avec le champ **isGlobalParent** défini sur **vrai.**
3. Modifiez l'état de l'incident de sécurité sur **Fermé**, spécifiez les codes de fermeture, puis cliquez sur **Enregistrer**.
   La boîte de dialogue suivante s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cet incident de sécurité est associé à un Master Ticket SecureWorks. Un Master Ticket peut être associé à un ou plusieurs tickets enfants. Pour que le ticket principal puisse être fermé, vous devez d'abord vérifier si tous les tickets enfants associés à ce ticket principal sont fermés.

4. Ajoutez une note demandant la fermeture du ticket principal dans Secureworks, puis cliquez sur **Soumettre la demande**.
   Le Master Ticket est désormais réaffecté à l'équipe SOC de SecureWorks.
5. Une fois la demande envoyée, vous pouvez fermer l'incident de sécurité.
6. Accédez à la **Application** > **Module**.

Paramètres de configuration

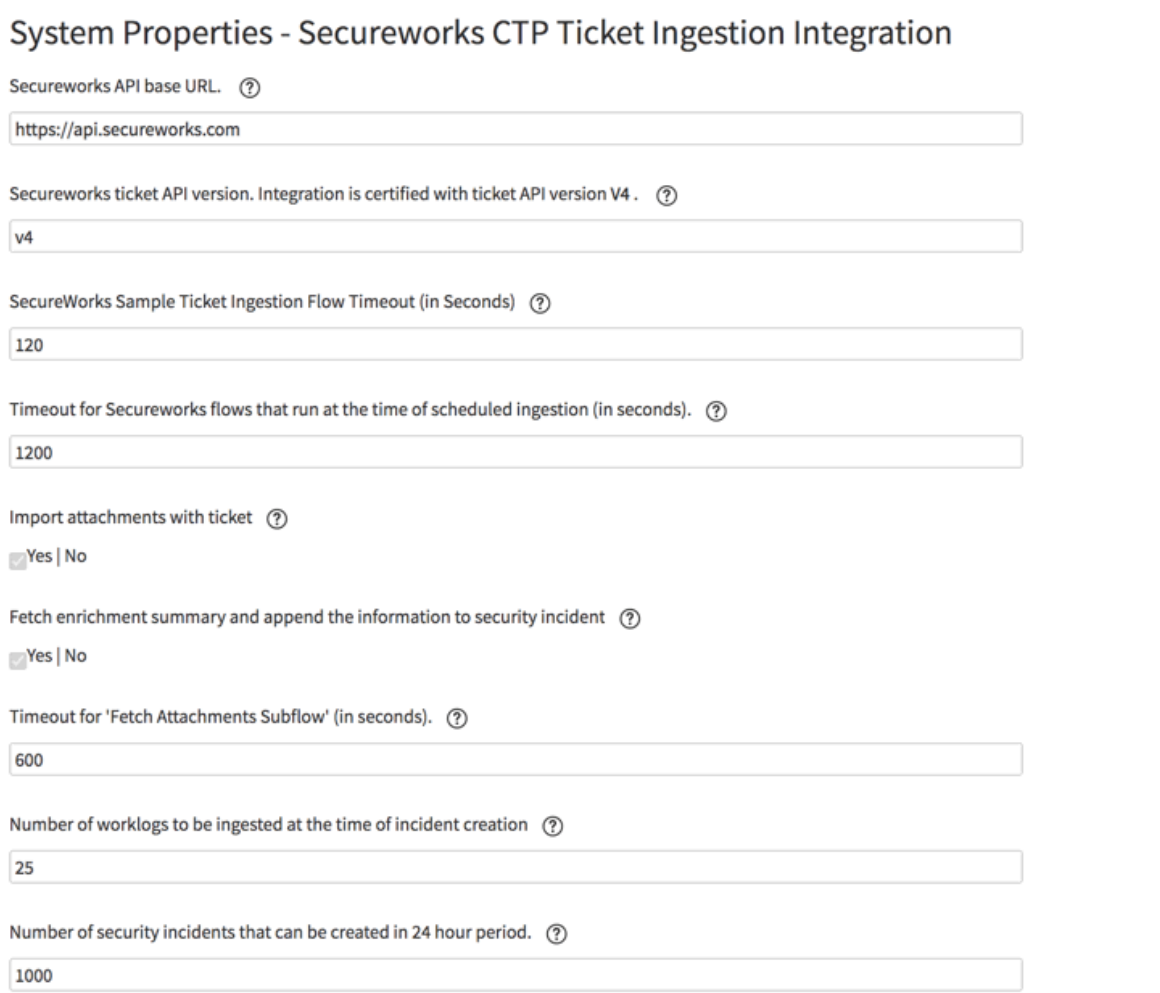
Utilisez cette option pour modifier les propriétés système par défaut de l'intégration d'ingestion Secureworks CTP de tickets.

Pour modifier les propriétés système, connectez-vous en tant qu'utilisateur disposant du rôle *sn_si.admin* et accédez à **Intégration de l'ingestion de tickets SecureWorks** > **Paramètres d'intégration SecureWorks**.

Les paramètres de configuration par défaut s'affichent. Vous pouvez modifier ces paramètres si nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Tous les paramètres d'intégration modifiés seront appliqués au cours de l'intervalle d'interrogation suivant, tel que défini dans le profil.

Intégration de Security Incident Response avec zScaler

Vous pouvez utiliser le produit pour connecter les Intégration de Security Incident Response avec zScaler journaux de votre Zscaler Internet Access serveur (ZIA) au ServiceNow AI Platform fichier . Cette intégration vous permet d'afficher des tableaux de bord, de créer des alertes personnalisées et d'enquêter sur les incidents de sécurité.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Vue d'ensemble

Le Zscaler produit Internet et passerelle Web est fourni à partir du cloud. Il vous fournit les points de données clés et des informations sur l'environnement de sécurité de votre entreprise. Intégration de Security Incident Response avec zScaler Connecte le Zscaler Internet Access produit à votre ServiceNow AI Platform instance. En utilisant le Zscaler produit sur le ServiceNow AI Platform, vous obtenez plus d'informations sur l'utilisation d'Internet par votre organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Principales fonctionnalités de l'intégration

Cette intégration comprend les fonctionnalités clés suivantes :

- Recherche de la réputation des observables par rapport à la bibliothèque de menaces globale conservée par le Zscaler produit.

> **Remarque :** La Zscaler bibliothèque mondiale des menaces répertorie les menaces par tendances, pays d'origine, destination cible, volume et diverses catégories de menaces. Cette bibliothèque de menaces globale vous permet d'examiner vos observables par rapport au paysage des menaces globales.

- Conservation des observables dans une liste bloquée ou une liste d'autorisation sur le Zscaler produit.
- Possibilité d'extraire et de passer en revue les Zscaler rapports de bac à sable du produit pour obtenir un hachage MD5. La fonctionnalité Cloud Sandbox du Zscaler produit exécute et analyse les fichiers dans un environnement virtuel pour détecter les comportements malveillants.
- Alertes de sécurité à partir des événements Patient 0 générés dans le Zscaler produit lorsqu'un utilisateur télécharge un fichier malveillant inconnu.
- Plusieurs listes de catégories d'URL qui agissent comme des listes bloquées ou des listes d'autorisation telles que définies dans le Zscaler produit.
- ServiceNow AI Platform incidents de sécurité qui peuvent être balisés pour identifier la catégorie d'URL à laquelle les observables sont ajoutés.
- Périodes d'expiration qui conservent la taille des entrées de liste de catégories d'URL en faisant automatiquement expirer ou en supprimant les entrées les plus anciennes.
- Workflow d'approbation pour l'ajout et la suppression d'observables des listes de catégories d'URL.
- Entrées de catégorie d'URL pouvant être liées aux enregistrements d'observables et aux incidents de sécurité comprenant des résultats de renseignements sur les menaces et des détails sur les raisons pour lesquelles une entrée est bloquée.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Zscaler Site web de la documentation produit	Site web de la documentation produit ZScaler
ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Premiers pas avec Intégration de Security Incident Response avec zScaler

Activez et configurez le produit pour qu'il s'interface Zscaler Internet Access avec votre instance et Réponse aux incidents de sécurité votre ServiceNow AI Platform produit.

Liste de vérification

Tâche de configuration	Description
Affectez et vérifiez les rôles et Réponse aux incidents de sécurité requisServiceNow AI Platform.	Ces rôles sont requis pour la configuration et la vérification des résultats attendus :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description

	• Le rôle administrateur installe l'intégration à partir de et ServiceNow Store attribue le rôle sn_si.admin.
	• Le rôle sn_si.admin effectue les tâches suivantes :
	  ○ Configure l'intégration.
	  ○ Crée, active et supprime les listes de catégories d'URL.
	  ○ Affecte le rôle sn_si.analyst.
	• Le rôle sn_si.analyst crée des entrées et travaille sur les incidents de sécurité.

Vérifiez que les ServiceNow applications principales sont installées et activées avant de configurer cette intégration.	Le ServiceNow Centre d'intégration module d'extension Enterprise Pack Installer [com.glide.hub.integrations.enterprise] est requis. Le Réponse aux incidents de sécurité module d'extension (com.snc.security_incident) est requis. Ce module d'extension installe automatiquement toutes les dépendances pour le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications pour l'intégration. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ces applications ne sont pas déjà installées, installez et activez chaque application une par une dans l'ordre suivant : **1.** Réponse aux incidents de sécurité Dépendance (com.snc.si_dep) **2.** Cadre de travail d'intégration de sécurité **3.** Security Support Common **4.** Orchestration du support de sécurité **5.** Renseignements sur les menaces Prise en charge commune **6.** Trusted Security Circles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	7. Opérations de sécurité Assistant de configuration 8. Réponse aux incidents de sécurité
Vérifiez les Zscaler versions.	• Cette intégration est prise en charge sur la Zscaler Internet Access version 1.0 ou ultérieure. • Cette intégration est testée avec les versions suivantes Zscaler : ○ Zscaler Client Connector pour Windows : 3.0 ○ Connecteur client Zscaler pour macOS : 3.0 ○ Zscaler Client Connector pour Linux : version bêta ○ Connecteur cloud Zscaler - 6.1
Vérifiez que vous disposez des autorisations requises Zscaler et que vous avez configuré l'accès au Zscaler Internet Access API.	• Vous devez disposer des informations d'identification administrateur pour Zscaler Internet Access. • Vous devez disposer d'un abonnement valide à l'API de service dans le cloud. Zscaler L'assistance doit fournir votre clé. • Vous devez avoir Zscaler Internet Access les informations d'identification d'administrateur (nom d'utilisateur et mot de passe). L'authentification API repose sur la combinaison de la clé API et Zscaler Internet Access des informations d'identification de l'administrateur. **Remarque :** Pour plus d'informations sur la Zscaler Internet Access gestion des clés API, consultez la documentation Zscaler .

Configurer l'accès aux Zscaler Internet Access API

Configurez l'accès Zscaler Internet Access au serveur pour authentifier la connexion sécurisée entre l'instance ServiceNow AI Platform et le Zscaler serveur.

Avant de commencer

Rôle requis : Zscaler Internet Access admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Une fois Zscaler activé votre abonnement API au service cloud de votre organisation, il est disponible sur la Zscaler Internet Access page Gestion des clés API avec l'URL de base. Votre organisation ne peut disposer que d'une seule clé API ou jeton. Supprimez la clé ou le jeton existant avant d'en ajouter un nouveau.

L'URL de base de l'API est `${Cloud_Name}/api/v1`. Vérifiez le nom du Zscaler cloud qui a été mis en service pour votre organisation et utilisez-le pour remplacer `{Cloud_Name}` dans l'URI de base. Voici quelques exemples d'URL de base :

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net
- example.zscaler.net
- example.zscloud.net

Remarque : Pour plus d'informations sur le portail d'administration Zscaler Internet Access , consultez la documentation de gestion des clés API Zscaler et la documentation du portail Zscaler .

Procédure

1. Connectez-vous en tant qu'administrateur au portail d'administration Zscaler Internet Access .
2. Accédez à la **Administration** > **Sécurité de l'API de service dans le cloud**.
3. Cliquez sur **Ajouter une clé API**.
   Si vous ne voyez pas l'option **Ajouter une clé API** , supprimez la clé existante.
   La nouvelle clé API est immédiatement valide et s'affiche dans l'onglet.

Résultats

Vous avez récupéré l'URL de base et la clé API pour configurer l'accès à partir de l'instance ZscalerServiceNow AI Platform .

Installer et configurer Intégration de Security Incident Response avec zScaler

Installez et configurez le produit d'accès Intégration de Security Incident Response avec zScaler Internet à partir de pour ServiceNow Store commencer à utiliser l'intégration sur votre ServiceNow AI Platform instance.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Téléchargez le Intégration de Security Incident Response avec zScaler produit à partir de et ServiceNow Store installez-le.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la Intégration de Security Incident Response avec zScaler tuile et cliquez sur **Configurer** > **Créer une configuration**.
4. Remplissez les champs du formulaire.

Traduction automatique

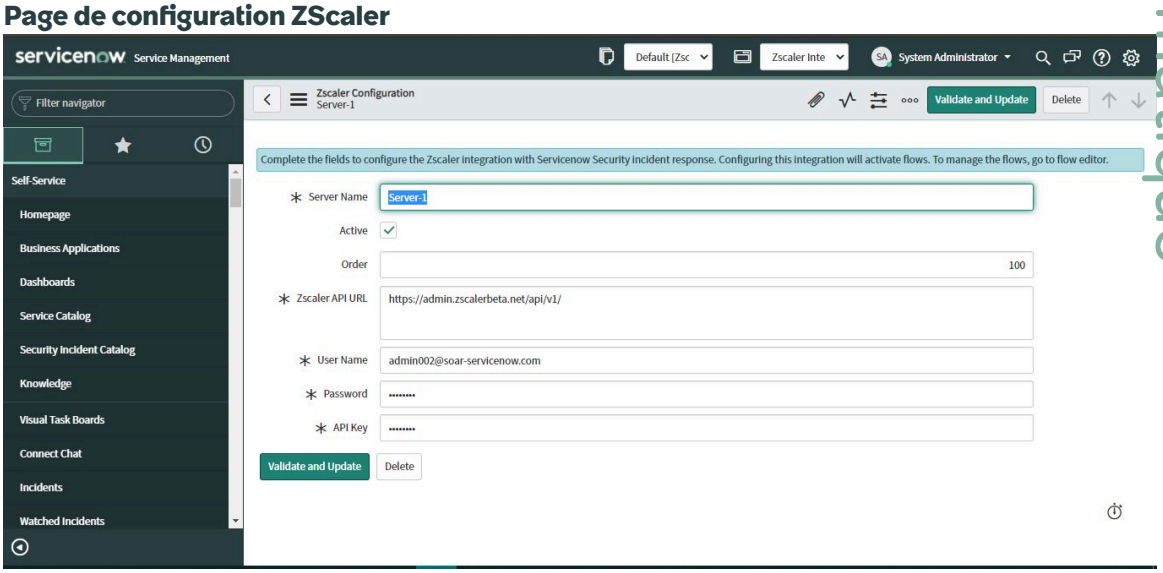
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Zscaler Formulaire de configuration

Champ	Description
Nom du serveur	Zscaler Nom du serveur. Par exemple, ZSserver.
Actif	Indique que le profil est actif.
Ordre	Priorité du flux. La valeur de ce champ indique l'ordre des workflows lorsque deux profils ou plus partagent des conditions de déclenchement. Le flux avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, 400. La valeur par défaut est 100.
Zscaler URL D'API	URL de base qui héberge l'API Zscaler . Par exemple https://example.zscalerbeta.net
Nom d'utilisateur	Nom d'utilisateur du Zscaler Internet Access compte administrateur.
Mot de passe	Mot de passe du Zscaler Internet Access compte administrateur.
Clé API	Clé API que vous avez obtenue à partir du portail d'administration Zscaler Internet Access .

L'exemple suivant montre la page de configuration de Zscaler.

Page de configuration ZScaler



5. Cliquez sur **Valider et mettre à jour**.

Résultats

Une fois que vous avez validé et enregistré cette configuration, revenez à la Zscaler page Configurations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter des Zscaler Internet Access listes de catégories d'URL

Ajoutez les catégories d'URL disponibles dans le Zscaler produit Internet Access à l'instance ServiceNow AI Platform afin de spécifier une action pour chaque URL afin d'y accéder facilement pour un filtrage granulaire et la création de politiques.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Le fournit Intégration de Security Incident Response avec zScaler une liste d'autorisation par défaut et des listes de catégories d'URL de refus pour aider à filtrer le contenu.

Les catégories d'URL que vous ajoutez à l'instance ServiceNow AI Platform doivent déjà se trouver dans votre Zscaler Internet Access environnement. Vous ne pouvez pas utiliser Intégration de Security Incident Response avec zScaler pour créer des catégories d'URL sur Zscaler.

Remarque : Pour plus d'informations sur les listes de catégories d'URL dans le Zscaler produit, consultez la documentation Zscaler sur les catégories d'URL .

Procédure

1. Accédez à la **Tous** > **Intégration ZScaler** > **URL ZScaler Listes de catégories**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Zscaler Formulaire Listes de catégories d'URL

Champ	Description
Source	Nom du serveur. Vous ne pouvez afficher que les serveurs précédemment configurés Zscaler Internet Access à partir de la liste des catégories d'URL.
Actif	Indicateur indiquant que la liste de catégories d'URL est active.
Catégorie d'URL	Champ activé une fois que vous avez sélectionné la source. Vous pouvez afficher la liste des catégories d'URL créées dans Zscaler.
Période d'expiration (jours)	Période d'expiration de la liste de catégories d'URL. 0 (par défaut) indique que l'entrée de liste de catégories d'URL n'expire jamais. En changeant cette valeur, tout observable qui a été ajouté à cette catégorie d'URL est actif pendant le nombre de jours que vous entrez. Vous pouvez saisir une valeur minimale de 1. Par exemple, si vous définissez la période d'expiration sur 30 jours, les entrées sont supprimées de la liste des catégories après 30 jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Balise d'affichage	Balise de sécurité qui apparaît sur l'incident SIR de sécurité. Lorsque vous activez l'option **Balise d'affichage** , le champ Balise pour les Zscaler observables est disponible sur le formulaire.
Créer une demande de changement	Demande de changement et tâches de changement dans votre ServiceNow AI Platform instance pour les enregistrements joints à la liste de catégories d'URL. Lorsque vous activez l'option **Créer une demande de changement** , le champ Demande de **changement** est disponible sur le formulaire.
Exiger l'approbation	Liste des groupes d'approbateurs. Après avoir soumis une demande, une approbation du groupe est requise pour terminer la demande. Lorsque vous activez l'option **Exiger l'approbation** , les champs **Approbateurs pour l'ajout d'observables** et **Approbateurs pour la suppression d'observables** sont disponibles sur le formulaire. ○ **Approbateurs pour l'ajout d'observables** : sélectionnez les approbateurs à l'aide de la fonction Rechercher pour ajouter les observables à partir de la page Liste de **catégories d'URL Zscaler** . Cette option vous permet d'ajouter le(s) groupe(s) d'utilisateurs pour les approbations. ○ **Approbateurs pour la suppression d'observables** : sélectionnez les approbateurs pour la suppression des observables à l'aide de la recherche à partir de la page Liste de **catégories d'URL de Zscaler** . Cette option vous permet de supprimer le(s) groupe(s) d'utilisateurs de la liste d'approbation.
Description	Description de la liste de catégories d'URL Zscaler . Utilisez ce champ pour ajouter plus de détails sur l'enregistrement de catégorie d'URL.

4. Cliquez sur **Envoyer**.
   Une soumission réussie déclenche une notification par e-mail au groupe d'approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Soumettre des observables à partir d'un enregistrement d'incident de sécurité à une liste de catégories d'URL

Soumettez les observables joints à un enregistrement d'incident de sécurité à une liste de catégories d'URL configurée à l'aide de la demande d'autorisation ou de blocage. L'ajout d'observables à la liste d'autorisation ou de blocage pour les analyses de sécurité permet aux utilisateurs d'examiner le contenu à partir de ces URL et d'accéder à du contenu fiable.

Avant de commencer

Rôle requis : sn_si.analyst

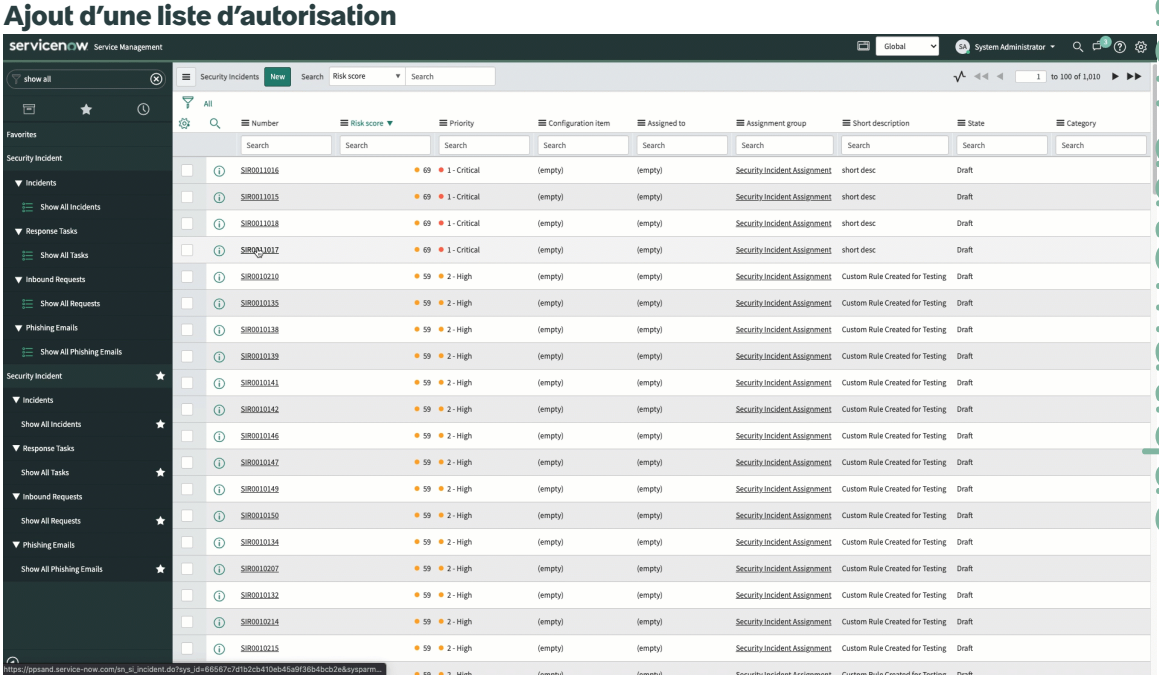
Pourquoi et quand exécuter cette tâche

Vous soumettez des entrées d'observables à l'aide de l'action Autoriser ou Bloquer la demande de la liste connexe Observables associés. Les observables sont des artefacts trouvés sur un réseau ou un système d'exploitation qui sont susceptibles d'indiquer une intrusion. Utilisez la liste des catégories d'URL configurées précédemment pour sélectionner l'observable que vous souhaitez soumettre. Une fois la demande envoyée, une demande d'approbation est envoyée à votre groupe d'approbation.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
   Dans cet exemple, vous voyez comment sélectionner un incident de sécurité et un observable, et comment ajouter une liste d'autorisation.

Ajout d'une liste d'autorisation



2. Sélectionnez l'incident de sécurité que vous souhaitez associer à la demande d'autorisation Zscaler ou de blocage.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
   Si vous ne trouvez aucun observable, cliquez sur **Nouveau**.
4. Sélectionnez un observable, puis dans le menu Actions, cliquez sur **Autoriser/Bloquer la demande**.
5. Dans la boîte de dialogue Demande d'autorisation/de blocage, indiquez si vous souhaitez effectuer la demande d'autorisation ou de blocage sur l'observable.
6. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Consultez les notes de travail pour connaître l'état de votre soumission et les balises de sécurité.
   Cliquez sur les liens dans les notes de travail pour plus d'informations sur l'état ou pour analyser les détails sur le Concepteur de flux. Les balises de sécurité sont des métadonnées sur l'enregistrement qui répond et définissent qui doit avoir accès à des types spécifiques de contenu de sécurité.
8. Pour afficher l'état de l'observable que vous avez sélectionné, accédez à **Intégration Zscaler** > **Entrées de la liste de catégories d'URL Zscaler**.
9. Sur la page Entrées de la liste des catégories d'URL Zscaler, cliquez sur l'observable pour afficher l'enregistrement.

Approuver les observables dans des listes de catégories d'URL

Approuvez les observables qui sont ajoutés à une liste de catégories d'URL afin que ces entrées figurent sur les listes d'autorisation ou de refus appropriées.

Avant de commencer
Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tous** > **Intégration Zscaler** > **Approbations Zscaler**.
2. Sélectionnez l'enregistrement à approuver.
3. Cliquez sur **Approuver**.
   Le groupe d'approbateurs reçoit une notification par e-mail pour la demande d'approbation. Une fois que les approbateurs ont cliqué sur le lien **Approuver/Rejeter** contenu dans l'e-mail, l'état devient Approuvé.

Soumettre l'incident de sécurité à la liste de catégories d'URL Zscaler

Soumettez des entrées directement pour les observables qui ne sont pas associés à un enregistrement d'incident de sécurité spécifique ServiceNow AI Platform afin que les entrées des observables figurent sur les listes d'autorisation ou de refus appropriées.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez également ajouter des observables à la liste des catégories d'URL directement à partir de l'enregistrement Observable.

Procédure

1. Accédez à la **Tous** > **Intégration Zscaler** > **Entrées de la liste de catégories d'URL Zscaler**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Zscaler Formulaire d'entrées de listes de catégories d'URL

Champ	Description
Valeur d'entrée	Nom de l'observable. Si un observable correspondant est trouvé, le reste du formulaire est automatiquement rempli.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si aucun observable correspondant n'est trouvé, vous devez renseigner le reste des informations manuellement.
Observable	Valeur (par exemple, adresse IP ou hachage) associée à l'observable.
Type d'observable	Classification des observables, telle qu'une adresse IP ou un hachage de fichier.
Liste de catégories d'URL	Catégorie d'URL. Par exemple, si une organisation utilise example.com pour les services Office 365, elle Zscaler example.com classe en services professionnels et Office 365.
Source	Nom du serveur. Vous ne pouvez afficher que les serveurs précédemment configurés Zscaler à partir de la liste des catégories d'URL.
Nombre d'incidents	Nombre d'incidents dans lesquels cet observable apparaît. Cette valeur est automatiquement mise à jour lorsque l'observable est ajouté à un autre incident manuellement ou via un workflow.
Actif	Indicateur indiquant que la liste de catégories d'URL est active.
Statut	État spécifie si l'observable est approuvé ou rejeté.
Période d'expiration (jours)	Période d'expiration de la liste de catégories d'URL. 0 (par défaut) indique que l'entrée de liste de catégories d'URL n'expire jamais. Si vous modifiez cette valeur, tous les observables que vous ajoutez à cette catégorie d'URL sont actifs pendant le nombre de jours que vous entrez. Vous pouvez saisir une valeur minimale de 1. Par exemple, si vous définissez la période d'expiration sur 30 jours, les entrées sont supprimées de la liste des catégories après 30 jours. **Remarque :** Si vous modifiez la période d'expiration par défaut de l'entrée de liste de catégories d'URL, un avertissement indiquant que la période diffère de la période configurée dans la liste de catégories d'URL sélectionnée, s'affiche.
Information supplémentaire	Champ dans lequel vous pouvez ajouter plus de détails sur l'observable.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exécuter une recherche de menaces à l'aide de la Zscaler bibliothèque de menaces globale

Exécutez une recherche de menaces sur un observable à l'aide de la bibliothèque de menaces globale du produit. Zscaler Prend en charge les Zscaler Internet Access recherches par rapport aux adresses IP, URL et domaines de type des observables.

Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez effectuer des recherches de renseignements sur les menaces sur un ou plusieurs observables pour déterminer s'ils sont associés à des menaces de sécurité connues. Lorsqu'un observable est associé à un incident de sécurité pour la première fois, toutes les implémentations de recherche de menaces actives effectuent ServiceNow AI Platform une recherche automatique de menaces. Vous pouvez afficher les résultats par rapport à la liste connexe Résultats de recherche de menace.

Par défaut, la configuration avec l'ordre le moins élevé est sélectionnée pour effectuer la recherche de menaces par rapport Zscaler Internet Access à la bibliothèque de menaces globale du produit. Vous pouvez également effectuer la recherche de menaces manuellement.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité sur lequel vous souhaitez exécuter la recherche de menace.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Sélectionnez l'observable, puis dans le menu Actions, cliquez sur **Exécuter une recherche de menace**.
   Dans cet exemple, vous verrez comment sélectionner un incident de sécurité et un observable, comment exécuter une recherche de menaces et comment afficher les résultats dans les notes de travail.



Résultats
Une fois que vous avez lancé la recherche de menace, vous pouvez consulter les notes de travail pour connaître l'état de votre soumission.

Soumettre à l'analyse Zscaler Sandbox

Utilisez le Zscaler Internet Access service sandbox des produits pour analyser les fichiers dans un environnement virtuel afin de détecter les comportements malveillants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

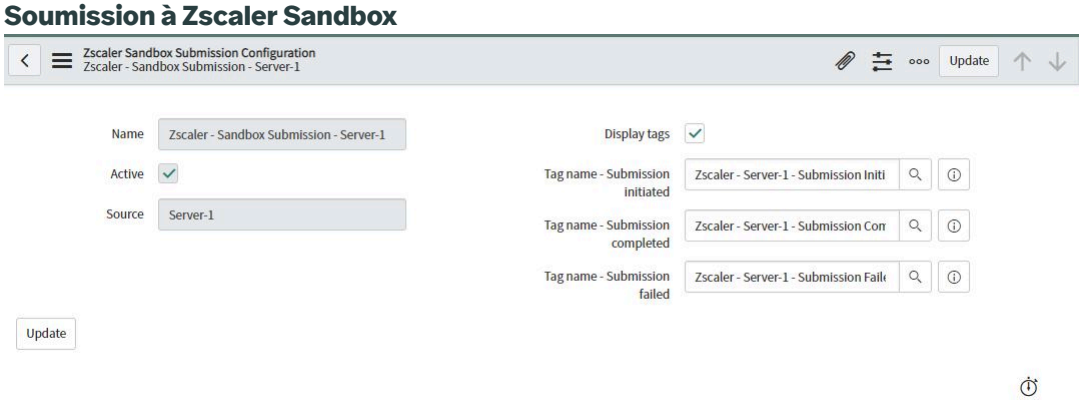
Avant de commencer
Rôle requis : sn_si.admin

Pourquoi et quand exécuter cette tâche
Lorsque vous créez une Zscaler configuration, une Zscaler soumission à Sandbox est créée par défaut dans le module Configuration Sandbox de Zscaler.

Les champs nom et source sont renseignés automatiquement et la configuration est activée par défaut. Vous ne pouvez modifier que la balise d'affichage et les options actives. Zscaler Internet Access Le produit vous permet d'extraire uniquement le rapport de bac à sable pour les observables de type hachage MD5.

L'analyse du fichier associé au hachage MD5 doit être terminée et le rapport correspondant doit être dans le bac à Zscaler sable. Si le hachage MD5 que vous envoyez n'a pas de rapport dans Zscaler, vous obtenez un message d'erreur.

Soumission à Zscaler Sandbox



Procédure
1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité sur lequel vous souhaitez exécuter l'analyse sandbox.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Sélectionnez un observable de type hachage MD5, puis dans le menu Actions, sélectionnez **Soumettre au bac à sable**.
   Créez un observable de type hachage MD5 si vous ne trouvez pas d'observable de type hachage MD5 existant.
5. Dans la boîte de dialogue Soumission de fichier, sélectionnez l'option **Zscaler - Soumission au bac à sable - Serveur** dans la configuration Soumission et cliquez sur **Soumettre au bac à sable**.
   Une fois que vous avez lancé la soumission du bac à sable, vous pouvez afficher les notes de travail pour voir l'état de votre soumission. Une balise est également ajoutée à l'incident de sécurité.
6. Dans les notes de travail, cliquez sur le lien dans la publication Résultats de soumission du bac à sable.

Résultats
Vous pouvez également afficher les résultats à partir de l'onglet Afficher toutes les listes connexes et Résultats de soumission du bac à sable.

Configurer des alertes par e-mail pour les événements Patient 0

Configurez Zscaler Internet Access le produit pour identifier et analyser les fichiers inconnus et potentiellement malveillants, tels que les événements Patient 0, afin de protéger votre réseau contre les fichiers malveillants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

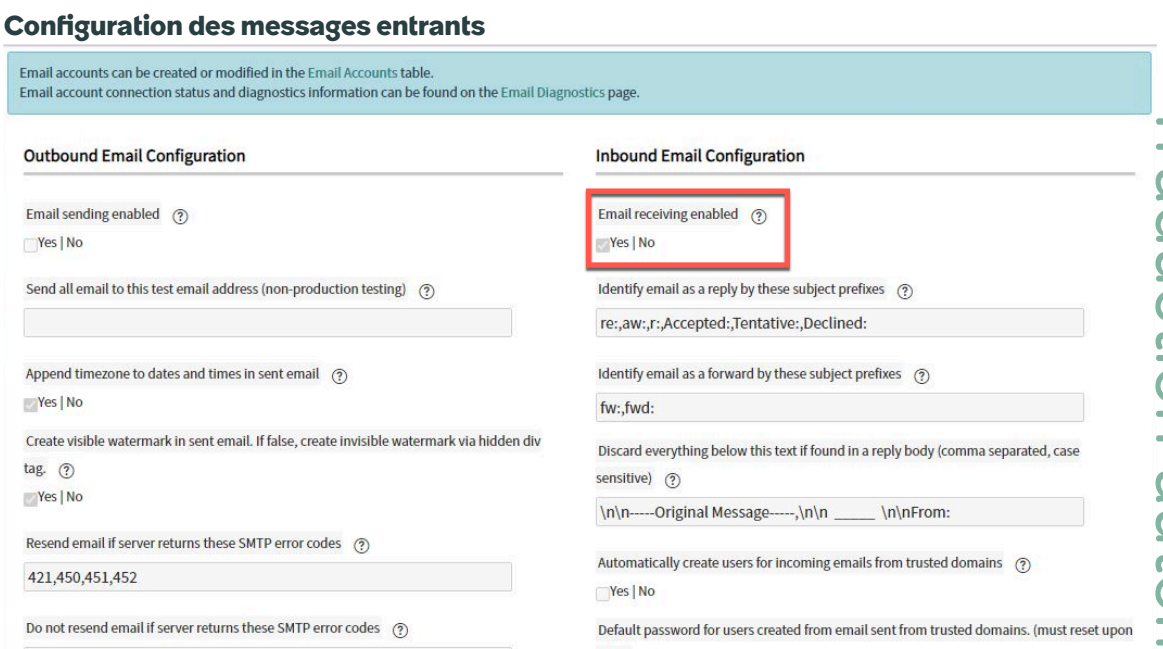
Rôle requis : sn_si.admin, Zscaler Internet Access admin

Pourquoi et quand exécuter cette tâche

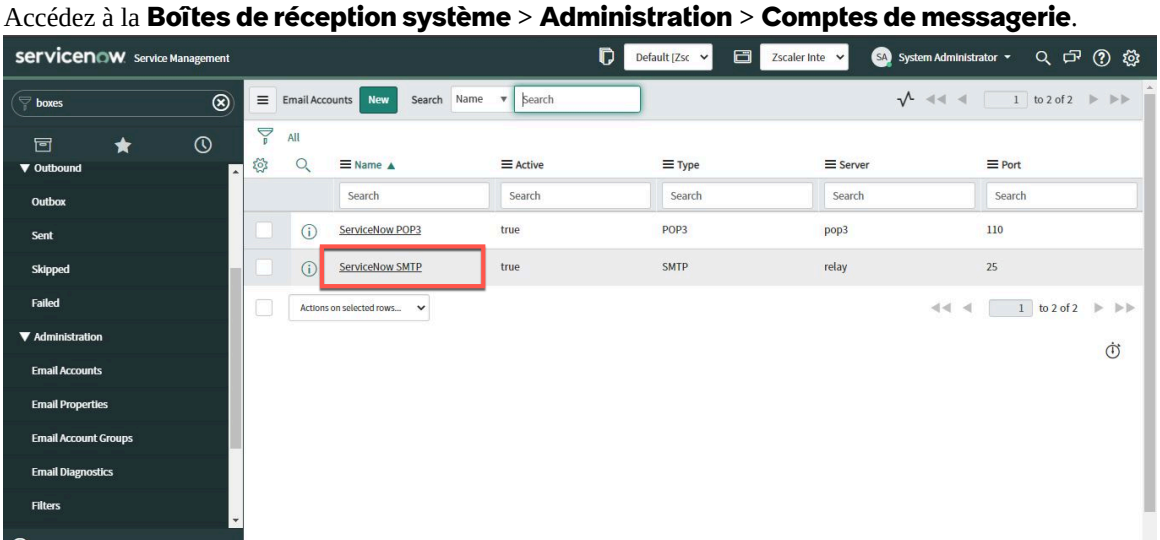
Le patient O est une classe d'alerte qui inclut un fichier inconnu qui a été autorisé à télécharger, mais qui s'avère malveillant. L'événement patient 0 est classé comme critique. Vous pouvez configurer l'pour ServiceNow AI Platform recevoir des alertes par e-mail à intervalles réguliers pour les événements Patient 0.

Procédure

1. Accédez à la **Tous** > **Boîtes de réception système** > **Administration** > **Propriétés d'e-mail**.
2. Dans la section Configuration des e-mails entrants, sélectionnez l'option **Réception d'e-mail activée** .



3. Cliquez sur **Enregistrer**.
4. Accédez à la **Boîtes de réception système** > **Administration** > **Comptes de messagerie**.



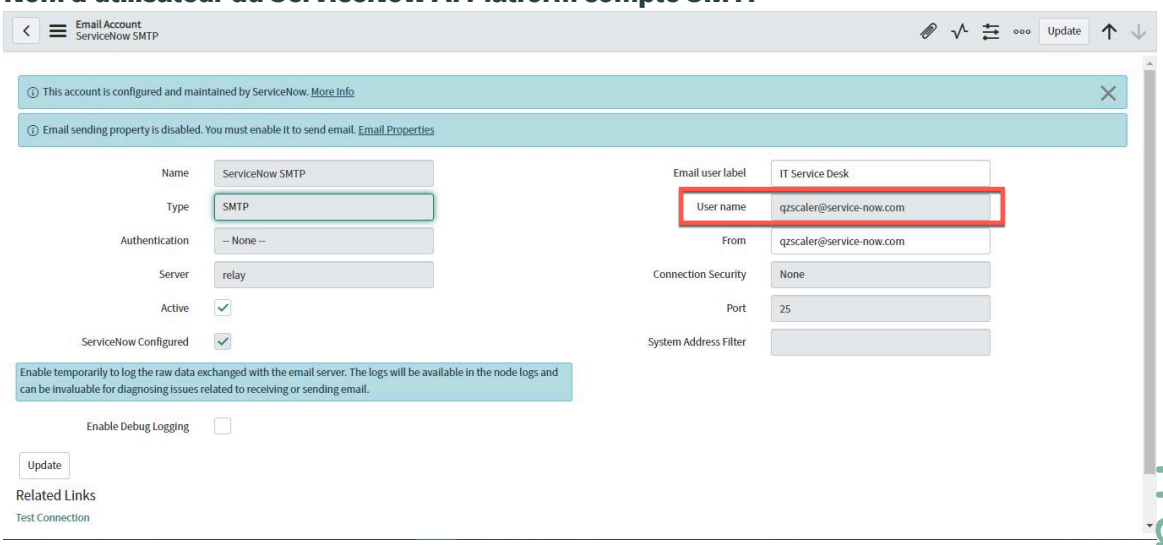
5. Sélectionnez le compte **de messagerie SMTP ServiceNow** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notez le nom d’utilisateur. Le nom d’utilisateur identifié ici est l’adresse e-mail que vous utilisez pour configurer Zscaler les ServiceNow AI Platform alertes Patient 0.

Nom d’utilisateur du ServiceNow AI Platform compte SMTP



6. Connectez-vous au portail d’administration Zscaler Internet Access .

> **Remarque :** Pour plus d’informations sur le portail d’administration Zscaler Internet Access , consultez la documentation Zscaler .

7. Accédez à la **Administration** > **Alertes** > **Publier des alertes**.
8. Cliquez sur **Ajouter un abonnement aux alertes**.
9. Remplissez les champs du formulaire.

Formulaire Ajouter un abonnement aux alertes

Champ	Description
E-mail	ServiceNow AI Platform Adresse e-mail du compte SMTP.
Description	Champ pour ajouter plus de détails sur les alertes Patient 0.

10. Cliquez sur **Enregistrer**.

ServiceNow Opérations de sécurité Module complémentaire pour Vue d’ensemble de Splunk

Le ServiceNow Opérations de sécurité module complémentaire permet Splunk à un administrateur de logiciel de collecter des données et de créer des Splunk incidents et des événements dans le ServiceNow AI Platform.

Le module complémentaire est installé à partir de Splunkbase.

> **Important :** Splunk est également pris en charge pour l’environnement de fournisseur de services gérés (MSP).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de l'intégration Splunk

Les procédures de configuration du ServiceNow Opérations de sécurité module complémentaire pour Splunk comprennent le téléchargement du fichier de module complémentaire dans Splunk, l'installation du module complémentaire et la configuration de l'instance où les ServiceNow incidents et événements de sécurité sont créés.

Rôle requis

Avant d'effectuer les procédures de configuration de l'intégration Splunk, assurez-vous de définir un utilisateur d'intégration avec les rôles sn_si.integration_user et sn_si.analyst sur votre instance ServiceNow. En outre, pour effectuer des importations, vous devez disposer du rôle import_transformer pour obtenir une autorisation de lecture et d'écriture sur les tables de sécurité. Le rôle sn_si.integration_user doit être défini avec la partie import_transformer du rôle.

Télécharger l'application Opérations de sécurité ServiceNow

La première étape de la configuration de l'intégration ServiceNow à Splunk consiste à télécharger l'application ServiceNow Opérations de sécurité à partir de Splunkbase.

Avant de commencer
Rôle requis : admin

Procédure

1. Ouvrez Splunkbase.
2. Recherchez ServiceNow Security Operations Integration .
3. Téléchargez l'application.

Installer le module complémentaire ServiceNow Security Operations pour Splunk

Installez le **module complémentaire Opérations de sécurité ServiceNow pour que Splunk** associe Splunk à ServiceNow.

Avant de commencer
Rôle requis : admin

Procédure

1. Ouvrez Splunk.
2. Cliquez sur l'icône **Engrenage des applications** ou sur l'élément de menu contextuel **Gérer les applications** .
3. Cliquez sur **Installer l'application à partir du fichier**.
4. Cliquez sur **Choisir un fichier**, sélectionnez sn_sec_ops.spl, puis cliquez sur **Charger**.
5. Si vous y êtes invité, redémarrez Splunk.
   Le ServiceNow Opérations de sécurité module complémentaire pour Splunk est installé et prêt à être configuré.

Configurer ou changer l'instance où les incidents ou les événements sont créés

Pour configurer ou modifier l'instance où les ServiceNow nouveaux incidents de sécurité et événements de sécurité sont créés, utilisez l'action Configurer dans la liste des applications.

Avant de commencer
Rôle requis : sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez **Splunk**.
2. Cliquez sur l'icône **Engrenage des applications** ou sur l'élément de menu contextuel **Gérer les applications** .
3. Dans la liste des applications, recherchez des applications **ServiceNow** à l'aide du filtre.
4. Recherchez **ServiceNow Security Operations Integration** et cliquez sur **l'action de configuration** correspondante.
5. Remplissez les champs du formulaire.

Champ	Description
Spécifier le serveur ServiceNow	
URL	URL de votre Splunk Enterprise Security console ou Splunk Cloud instance. L'URL doit inclure le port de l'API, par exemple : `https://mysplunkserver.com:8089`
Type d'authentification	Option permettant de sélectionner le type d'authentification. Vous pouvez sélectionner **Authentification de base** ou **Authentification OAuth 2.0**. ○ Si vous utilisez le nom d'utilisateur du compte API et le mot de passe de l'API pour la configuration, cochez la case **Authentification de base**. Désactivé par défaut. ○ Si vous utilisez l'authentification OAuth 2.0 pour la configuration, cochez la case **Authentification OAuth 2.0** . Désactivé par défaut.
Authentification de base	
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise Security console.
Mot de passe	Mot de passe que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise Security console.
Confirmer le mot de passe	Entrez le mot de passe pour le confirmer.
Authentification OAuth 2.0	
ID client	ID client de l'application créée sur le serveur ServiceNow.
Secret client	Secret client de l'application créée sur le serveur ServiceNow.

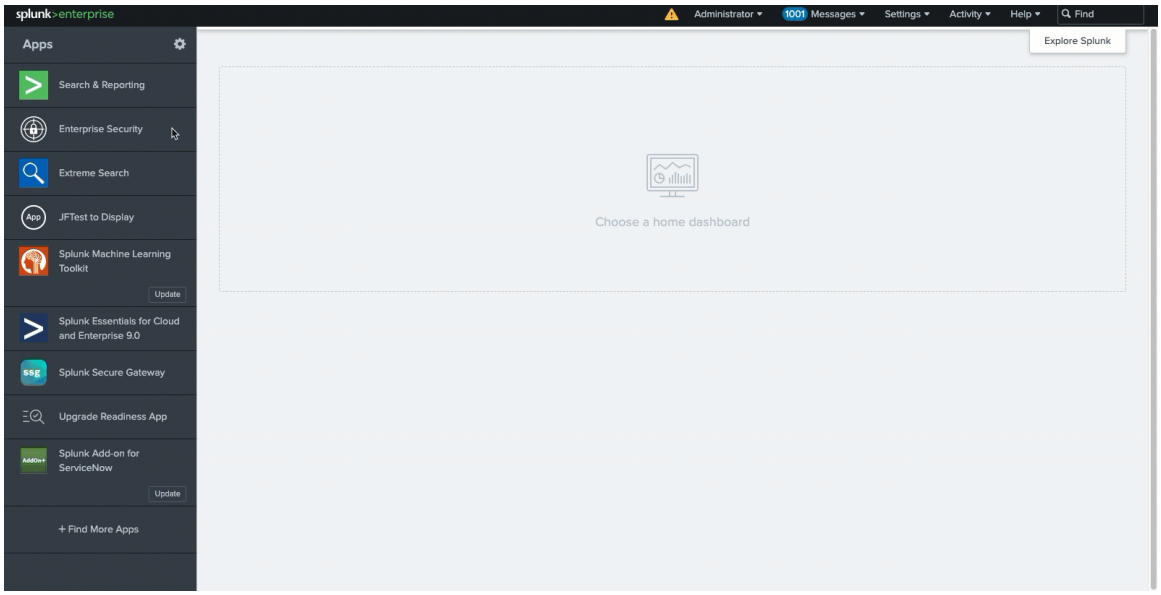
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
URL de redirection	L’URL vers laquelle vous serez redirigé. Vous pouvez copier et coller cette URL dans l’URL de redirection de votre registre ServiceNow.
Proxy facultatif	
Proxy URL	URL proxy de votre Splunk Enterprise Security console ou Splunk Cloud instance.
Port	Adresse du port.
Nom d'utilisateur	Nom d’utilisateur que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console.
Mot de passe	Mot de passe que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console.
Confirmer le mot de passe	Entrez le mot de passe pour le confirmer.
Configuration du niveau de connexion	
Niveau de connexion	Niveau des journaux de génération de rapports générés par l’intégration, c’est-à-dire le nom du type d’information. Vous pouvez également mettre à jour la valeur dans les options suivantes : ○ **info** ○ **erreur** ○ **avertir** ○ **debug** Par défaut, la valeur est **info**.
Sélection d’API	
Sélection d’API	Sélectionnez l’une des API suivantes : ○ API de table ○ API de jeu d'importation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Enregistrer**.
7. Vous pouvez également rechercher **l'intégration d'ingestion d'événements ServiceNow** et cliquer sur **l'action de configuration** correspondante.

   L'intégration d'ingestion d'événements ServiceNow est configurée en trois onglets différents.

   - **Splunk primaire** : configuration Splunk par défaut ou principale.
   - **Splunk secondaire** : (facultatif) la sauvegarde ou la deuxième configuration Splunk.
   - **Niveau de connexion** : niveau des journaux de génération de rapports générés par l'intégration, c'est-à-dire le nom du type d'information.
8. Sélectionnez l'onglet **primaire de Splunk** .
9. Remplissez les champs du formulaire.

Champ	Description
Étiquette de l'action du workflow	Nom de la Splunk Enterprise Security console principale ou de l'instance Splunk Cloud principale utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge. Par exemple, entrez SplunkES2.
URL	URL de votre Splunk Enterprise Security console principale ou de l'instance Splunk Cloud principale. L'URL doit inclure le port de l'API, par exemple : https://mysplunkserver.com:8089
Point de terminaison	Point de terminaison de votre Splunk Enterprise Security console principale ou de l'instance Splunk Cloud principale.

Traduction automatique

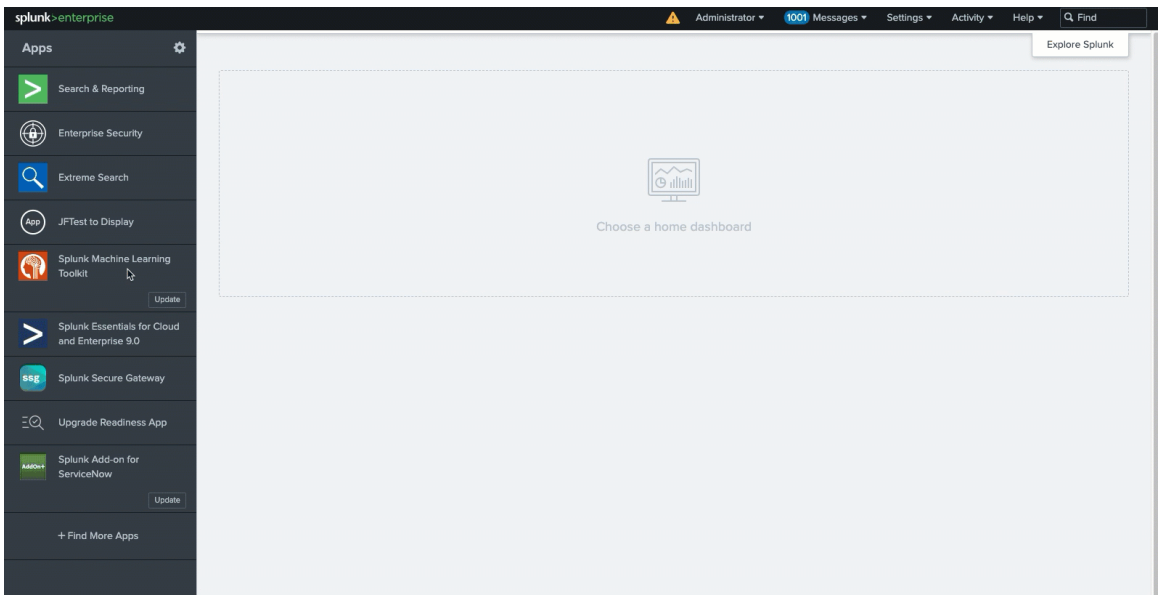
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type d'authentification	Option permettant de sélectionner le type d'authentification. Vous pouvez sélectionner **Authentification de base** ou **Authentification OAuth 2.0**. ○ Si vous utilisez le nom d'utilisateur du compte API et le mot de passe de l'API pour la configuration, cochez la case **Authentification de base**. Désactivé par défaut. ○ Si vous utilisez l'authentification OAuth 2.0 pour la configuration, cochez la case **Authentification OAuth 2.0** . Désactivé par défaut.
Authentification de base	
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise Security console.
Mot de passe	Mot de passe que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise Security console.
Confirmer le mot de passe	Entrez le mot de passe pour le confirmer.
Authentification OAuth 2.0	
ID client	ID client de l'application créée sur le serveur ServiceNow. Pour en savoir plus sur l'obtention de l'ID client, consultez Configurer le registre d'application sur l'instance ServiceNow
Secret client	Secret client de l'application créée sur le serveur. Pour plus d'informations sur l'obtention du secret client, voir Configurer le registre d'application sur l'instance ServiceNow
URL de redirection	L'URL vers laquelle vous serez redirigé. Vous pouvez copier et coller cette URL dans l'URL de redirection de votre registre ServiceNow. Pour plus d'informations, voir Configurer le registre d'application sur l'instance ServiceNow
Configuration de proxy facultative	
Proxy URL	URL proxy de votre Splunk Enterprise Security console secondaire ou Splunk Cloud instance secondaire.
Port	Adresse du port.
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console secondaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mot de passe	Mot de passe que vous avez créé pour le compte Proxy sur la Splunk Enterprise Security console secondaire.
Confirmer le mot de passe	Entrez le mot de passe pour le confirmer.



10. **Facultatif :** Sélectionnez l’onglet **secondaire Splunk** .
11. **Facultatif :** Remplissez les champs du formulaire.

Champ	Description
Étiquette de l’action du workflow	(Optional) Nom de la console secondaire ou de l’instance Splunk Enterprise SecuritySplunk Cloud secondaire utilisée pour l’intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge. Par exemple, entrez `SplunkES2`.
URL	URL de votre Splunk Enterprise Security console secondaire ou de l’instance Splunk Cloud secondaire. L’URL doit inclure le port de l’API, par exemple : `https://mysplunkserver.com:8089`
Point de terminaison	Point de terminaison de votre Splunk Enterprise Security console secondaire ou de l’instance Splunk Cloud secondaire.
Type d'authentification	Option permettant de sélectionner le type d’authentification. Vous pouvez sélectionner **Authentification de base** ou **Authentification OAuth 2.0**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Si vous utilisez le nom d'utilisateur du compte API et le mot de passe de l'API pour la configuration, cochez la case **Authentification de base**. Désactivé par défaut. ○ Si vous utilisez l'authentification OAuth 2.0 pour la configuration, cochez la case **Authentification OAuth 2.0** . Désactivé par défaut.
Authentification de base	
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise Security console.
Mot de passe	Mot de passe que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise Security console.
Confirmer le mot de passe	Entrez le mot de passe pour le confirmer.
Authentification OAuth 2.0	
ID client	ID client de l'application créée sur le serveur ServiceNow.
Secret client	Secret client de l'application créée sur le serveur ServiceNow.
URL de redirection	L'URL vers laquelle vous serez redirigé. Vous pouvez copier et coller cette URL dans l'URL de redirection de votre registre ServiceNow.
Configuration de proxy facultative	
Proxy URL	URL proxy de votre Splunk Enterprise Security console secondaire ou Splunk Cloud instance secondaire.
Port	Adresse du port.
Nom d'utilisateur	Nom d'utilisateur que vous avez créé pour le compte proxy sur la Splunk Enterprise Security console secondaire.
Mot de passe	Mot de passe que vous avez créé pour le compte Proxy sur la Splunk Enterprise Security console secondaire.
Confirmer le mot de passe	Entrez le mot de passe pour le confirmer.

Traduction automatique

12. Sélectionnez l'onglet **Niveau de connexion** .
13. Remplissez les champs du formulaire.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Niveau de journal	Niveau des journaux de génération de rapports générés par l'intégration, c'est-à-dire le nom du type d'information. Vous pouvez également mettre à jour la valeur dans les options suivantes : ○ **info** ○ **erreur** ○ **avertir** ○ **debug** Par défaut, la valeur est **info**.

14. Cliquez sur **Enregistrer**.
    Une fois la validation terminée, la page Intégrations de sécurité s'affiche avec chacune de vos configurations. Sur chaque vignette de configuration valide, les boutons **Mettre à jour** et Supprimer s'affichent, comme illustré dans la figure suivante.

    Remarque : Vous devez utiliser uniquement l'authentification de base ou l'authentification OAuth 2.0. Activez l'une des authentifications et saisissez les détails de l'authentification correspondants. L'activation des deux affichera une erreur.

    Une fois validée et soumise, chaque configuration de serveur d'ingestions d'événements est enregistrée sur la page Intégrations Splunk de sécurité sous forme de tuile. Si vos vignettes de configuration enregistrées ne sont pas affichées sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste Afficher les configurations, cliquez sur **Oui**.

Configurer le registre d'application sur l'instance ServiceNow

Enregistrez l'application auprès de l'instance pour utiliser l'autorisation OAuth.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **OAuth système** > **Registre d'application**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Créer un point de terminaison d'API OAuth pour les clients externes**.
4. Remplissez les champs du formulaire.

Champ	Description
Nom	Nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès OAuth.
ID client	(Lecture seule) ID unique de l'application généré automatiquement. L'instance utilise l'ID client lors de la demande d'un jeton d'accès.
Secret client	Chaîne secrète partagée que l'instance et l'application cliente ou le site Web utilisent pour autoriser les communications entre eux. L'instance utilise le

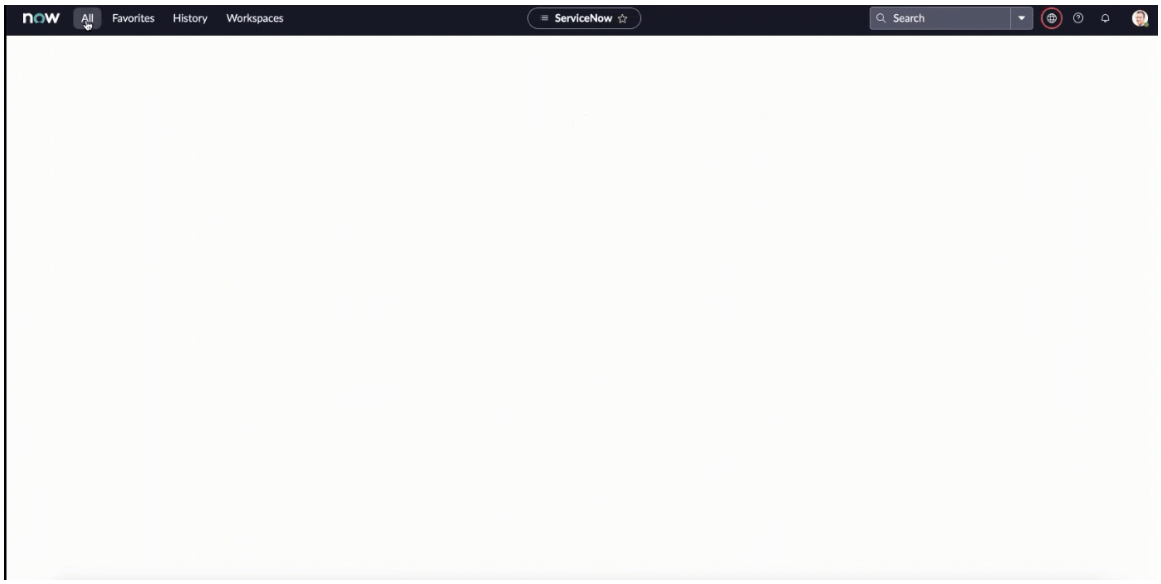
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	secret client lorsqu'elle demande un jeton d'accès. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets client existants, cliquez sur l'icône de verrouillage.
URL de redirection	URL de rappel vers laquelle le serveur d'autorisation redirige. Saisissez autant d'URL que nécessaire pour tous les consommateurs de jetons possibles. L'instance associe l'URL de la demande entrante à l'une des URL de redirection. Si aucune correspondance n'est établie, l'instance utilise la première URL de redirection.
URL du logo	URL contenant une image à utiliser comme logo de l'application. Le logo apparaît sur la page d'approbation lorsque l'utilisateur reçoit une demande d'accès à une application cliente à une ressource restreinte sur l'instance.
Application	Le nom de l'application.
Accessible depuis	Définissez le périmètre de l'application. Sélectionnez l'une des options suivantes : ○ **Tous les champs d'application de l'application** ○ **Ce périmètre de l'application uniquement**
Actif	Cochez cette case pour activer le registre d'application.
Durée de vie du jeton d'actualisation	Nombre de secondes de validité d'un jeton d'actualisation. L'instance utilise la valeur Durée de vie lors de la demande d'un jeton d'actualisation. Par défaut, les jetons d'actualisation expirent dans 100 jours (8640 000 secondes).
Durée de vie du jeton d'accès	Nombre de secondes pendant lesquelles un jeton d'accès est valide. L'instance utilise la valeur Durée de vie lors de la demande d'un jeton d'accès. Par défaut, les jetons d'accès expirent au bout de 30 minutes (1 800 secondes).
Commentaires	Informations supplémentaires à associer à l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
6. Cliquez sur **Envoyer**.

Commandes de recherche manuelle

Les commandes de recherche manuelle sont saisies à partir de n'importe quelle fenêtre de recherche. Vous pouvez créer un incident ou un événement de sécurité. Après la commande, des paires de noms de champs et de valeurs sont utilisées pour créer l'enregistrement souhaité.

Événement de sécurité

La commande d'événement de sécurité, **snsecevent**, crée un événement avec ServiceNow la classification de sécurité.

Ces événements peuvent être examinés seuls, ou des règles d'alerte internes ServiceNow , ou des actions manuelles peuvent transformer un événement ou une collection d'événements en incident de sécurité.

Si l'événement devient un incident de sécurité et que chaque paramètre est envoyé dans l'événement, ces données sont utilisées pour renseigner l'incident de sécurité comme suit :

Événement de sécurité

Nom de paramètre	Obligatoire	Utiliser	Utiliser dans un incident de sécurité
nœud	Oui	Le nœud représente le serveur ou l'élément de configuration de l'événement. Idéalement, ce nœud est mappé à un CI existant dans ServiceNow.	Utiliser dans un incident de sécurité
type	Oui	La catégorie de l'événement.	Description brève
ressource	Oui	Élément de configuration.	Description brève

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Événement de sécurité (suite)

Nom de paramètre	Obligatoire	Utiliser	Utiliser dans un incident de sécurité
source	Non	L'origine de ces données. Par défaut, le serveur Splunk génère les données.	Journal d'activité
external_url	Non	URL d'exploration vers le bas à utiliser ServiceNow pour revenir aux données Splunk concernant cet événement. Par défaut, cette URL contient le lien de résultat d'une alerte ou un lien vers la page de recherche Splunk par défaut.	URL externe accessible via le bouton **Explorer vers le bas** sur le formulaire d'incident de sécurité
time_of_event	Non	Heure à laquelle l'événement a été connecté dans Splunk.	N/A
Toutes les autres valeurs (catégorie, sous-catégorie dans l'exemple)	Non	Tout champ qui ne fait pas partie du champ d'information de l'événement. Si un incident de sécurité est créé, il est utilisé.	Si le champ existe et n'est pas renseigné, l'incident de sécurité utilise cette valeur. Par exemple, la catégorie transmise par l'événement devient la catégorie du nouvel incident de sécurité. Si aucun champ portant ce nom n'existe, la valeur est placée dans le journal d'activité.

Incident de sécurité

La commande d'incident de sécurité, **snsecincident**, crée un incident de sécurité dans votre ServiceNow instance.

Incident de sécurité

Paramètre	Obligatoire	Utiliser
short_description	Oui	Description courte de l'incident sur une ligne.
catégorie	Non	Catégorie de l'incident de sécurité. Si cette catégorie n'existe pas, elle est créée.
sous-catégorie	Non	Sous-catégorie. Si cette sous-catégorie n'existe pas, elle est créée.
cmdb_ci	Non	Élément de configuration de l'incident de sécurité. Idéalement,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incident de sécurité (suite)

Paramètre	Obligatoire	Utiliser
		cet élément est mappé à un CI existant dans ServiceNow.
description	Non	La description plus longue et détaillée de l'incident.

Il existe de nombreuses colonnes utiles possibles : tout ce qui se trouve dans la carte de transformation des incidents de sécurité peut être utilisé. Si de nouvelles colonnes sont ajoutées à l'incident de sécurité, elles sont également utilisées, tant qu'elles figurent dans la carte de transformation. Quelques colonnes utiles : emplacement, priorité, assignment_group, assigned_to, affected_user, attack_vector et watch_list.

Actions d'événement Splunk

Lors de l'examen des journaux Splunk, vous pouvez créer rapidement des événements de sécurité et des incidents de sécurité à partir de n'importe quel élément du journal à l'aide des actions d'événement.

Cliquez sur l'une de ces actions pour créer une commande de recherche manuelle renseignée avec les données de l'entrée de journal et exécutez-la pour générer le nouvel enregistrement.

Ces actions sont facilement configurées pour ajouter des champs à vos données normalisées. Dans Splunk, à l'aide de **Paramètres** > **Champs** > **Actions du workflow**, vous pouvez sélectionner et modifier l'une ou l'autre de ces actions à l'aide des champs de recherche manuelle.

Vous pouvez choisir où l'action est affichée, pour quels champs et modifier la chaîne de recherche qui contient une commande de recherche pour créer votre enregistrement.

Alertes Splunk à enregistrement unique

Dans n'importe quelle alerte, vous pouvez spécifier des événements de sécurité ou des incidents de sécurité à créer lorsque l'alerte est déclenchée.

Ouvrez ou créez votre alerte, et lorsque vous modifiez des actions, sélectionnez le type d'enregistrement souhaité et remplissez la boîte de dialogue d'alerte.

Champs personnalisés à enregistrements multiples Alertes Splunk

Les alertes multi-enregistrements (définies à l'aide des actions de déclenchement **Créer plusieurs incidents de sécurité ServiceNow** et **Créer plusieurs événements de sécurité ServiceNow**) peuvent créer automatiquement des enregistrements avec n'importe quel ensemble de champs pris en charge.

Celles-ci agissent différemment des autres actions d'alerte en ce sens que des valeurs par défaut sont fournies. Toutefois, la plupart des données proviennent des résultats de recherche pour cette alerte.

Remarque : Dans les versions précédentes du module complémentaire et de cette documentation, les alertes scriptées étaient prises en charge. Cette fonctionnalité a été déconseillée et remplacée par ces instructions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un champ personnalisé à plusieurs enregistrements Alerte Splunk

Pour créer une alerte Splunk à enregistrements multiples avec des champs personnalisés, vous devez créer une recherche conçue pour correspondre aux colonnes ServiceNow que vous souhaitez renseigner.

Avant de commencer
Rôle requis : sn_si.admin

Procédure

1. Accédez à **Rechercher**.
2. Dans la zone **de recherche** , créez une recherche qui génère les données de votre enregistrement. Consultez les exemples de critères de recherche recommandés .
3. Cliquez sur **Enregistrer sous** , puis sélectionnez **Alerte**.
4. Définissez le nom, les autorisations et le calendrier selon vos besoins.
5. Cliquez sur **Ajouter des actions**.
6. Effectuez l'une des sélections suivantes.
   - Pour créer un événement par résultat de votre recherche, sélectionnez **Créer plusieurs événements de sécurité ServiceNow**.
   - Pour créer un incident par résultat de votre recherche, sélectionnez **Créer plusieurs incidents de sécurité ServiceNow**.
7. Définissez les valeurs par défaut selon vos besoins.
   Si le champ des résultats de recherche est vide ou absent, les valeurs par défaut sont utilisées. S'il y a une valeur dans le résultat, les valeurs par défaut sont remplacées.

Champs personnalisés et multi-enregistrements Exemples d'alertes Splunk

Lorsque vous créez plusieurs alertes Splunk d'enregistrement avec des champs personnalisés, vous devez définir des critères de recherche pour générer des données d'alerte. Des exemples de critères de recherche pour les incidents et les événements de sécurité sont présentés.

Recherche d'incidents de sécurité

Pour un incident de sécurité, ce critère génère une recherche pour remplir les colonnes de la table d'incident de sécurité.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Recherche d'événements de sécurité

Pour un événement de sécurité, il s'agit de la même recherche, mais elle remplit les champs Événement à la place. Si cet événement est transformé en incident de sécurité et que tous les champs qui n'existent pas dans l'événement sont renseignés, ils sont transférés à l'incident de sécurité. Sinon, ils restent dans le champ d'informations supplémentaires de l'événement et de l'alerte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Remarque : Les critères de recherche que vous utilisez ajouteront autant d'enregistrements que vous en trouverez dans la recherche. Il peut ajouter 5 ou 10 000 000 000 d'enregistrements. Ce n'est donc PAS une méthode recommandée pour le transfert en masse de données. L'objectif de cette méthode est d'ajouter un enregistrement par appel REST dans l'instance ServiceNow.

Génération de rapports d'erreurs Splunk

Chaque fois qu'un problème de connectivité se produit avec votre instance ServiceNow, une erreur est consignée dans Splunk avec les informations décrivant le problème.

Les messages d'erreur sont stockés dans un nouvel index nommé **servicenow** avec le type **de source servicenow**.

Pour rechercher des journaux d'erreurs, assurez-vous de spécifier l'index **ServiceNow** dans votre recherche. Vous pouvez également consulter la documentation Splunk actuelle sur la façon d'ajouter le nouvel index **ServiceNow** aux index de recherche par défaut.

Splunk Enterprise Event Ingestion Intégration pour Opérations de sécurité par ServiceNow

L'intégration Splunk Enterprise des données d'événements et d'alertes avec le produit (SIR) permet aux analystes d'incidents de sécurité de collecter et de traiter les journaux de sécurité et les données d'événements Réponse aux incidents de sécurité connexes.

Vue d'ensemble

Les données sont collectées en temps réel et sont utilisées par les analystes pour identifier et signaler les cybermenaces potentielles. Les événements de sécurité collectés peuvent être transformés en alertes déclenchées qui sont ingérées automatiquement avec cette intégration. En outre, des événements de sécurité individuels peuvent être transférés manuellement à la demande de l'interface Splunk Enterprise de recherche et de reporting vers le Réponse aux incidents de sécurité produit de la ServiceNow AI Platform pour créer des incidents de sécurité. Vous pouvez récupérer des événements notables à partir de Splunk Enterprise la recherche avec la configuration de grappe de tête de recherche. Pour ce faire, vous pouvez utiliser l'URL et le port d'API de n'importe quelle tête de recherche faisant partie de la grappe.

Cette intégration fournit à un analyste du centre des opérations de sécurité (SOC) une visibilité sur les événements et les données d'alerte connexes. Ces données peuvent être intégrées dans ServiceNow AI Platform Réponse aux incidents de sécuritéSIR des incidents de sécurité pour une enquête plus approfondie et une correction. Les profils des Splunk alertes ingérées en cours et des événements transférés sont créés dans votre ServiceNow AI Platform instance. Ces profils personnalisent la façon dont les différents Splunk champs d'alerte et d'événement sont affichés sur SIR les incidents de sécurité. Un mappage par défaut des champs d'alerte est fourni ; il peut être modifié et augmenté pour répondre aux besoins spécifiques du client.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Créez plusieurs profils d'ingestion d'alertes pour créer des incidents de sécurité SIR pour des types de menaces spécifiques tels que l'hameçonnage et les programmes malveillants.
- Créez plusieurs profils d'événements pour le transfert d'événements sur demande à partir de votre Splunk console afin de créer des incidents de sécurité SIR.
- Glisser-déposer le mappage des valeurs de champs d'alerte et d'événement Splunk vers les champs d'incident de sécurité SIR associés.
- Aperçu de la mise en page de l'incident de sécurité en fonction d'échantillons d'alertes ou d'événements pour valider la SIR configuration du profil.
- Ingérer des alertes historiques, ainsi que des alertes futures en cours à intervalles configurables.
- Regroupez les événements ou les alertes aux incidents de sécurité existants en fonction des valeurs de champ correspondantes SIR pour éviter les incidents de sécurité en double.

Versions prises en charge ServiceNow AI Platform

Le module d'extension com.snc.si_dep est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications.

Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour assurer une installation fluide :

1. Cadre de travail d'intégration de sécurité
2. Security Support Common
3. Orchestration du support de sécurité
4. Security Incident Response

Pour plus d'informations sur l'installation Opérations de sécurité des applications principales, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

ServiceNow Compléments

Le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise n'est requis que si vous préférez transférer manuellement les événements de votre Splunk Enterprise console vers votre ServiceNow AI Platform instance. Cet ServiceNow addon est disponible dans splunkbase .

Ce ServiceNow module complémentaire d'ingestion d'événements Security Operations pour Splunk Enterprise l'application dans splunkbase n'est pas requis pour l'ingestion d'alerte automatisée prise en charge par l'intégration.

Versions prises en charge par Splunk

Cette intégration prend en charge la version 6.0 ou ultérieure de Splunk Enterprise. L'intégration prend également en charge le Splunk service Enterprise Cloud.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Serveur MID

Cette intégration nécessite qu'un Serveur MID soit installé et configuré dans votre ServiceNow AI Platform® instance pour vous connecter au service si le serveur est déployé au sein de Splunk votre réseau d'entrepriseSplunk. Si vous utilisez le service, un serveur MID n'est Splunk Cloud pas nécessaire. Pour plus d'informations sur les serveurs MID, voir Serveur MID .

Architecture d'intégration et connexion des systèmes

Pour en savoir plus sur l'architecture de l'intégration, y compris les termes clés et les détails de connexion aux systèmes externes, reportez-vous à la section Architecture d'intégration et connexion de systèmes externes pour l'intégration Splunk Enterprise Event Ingestion.

Liste de vérification

Pour obtenir une liste de contrôle imprimable de ces rubriques, reportez-vous à la section Liste de vérification pour Splunk Enterprise Security l'intégration de l'ingestion d'événements notables. Vous pouvez utiliser cette liste pour suivre votre progression au fur et à mesure que vous exécutez les tâches de l'intégration.

Les images utilisées dans les rubriques suivantes ont été générées pour la version Kingston du ServiceNow AI Platform fichier . Pour plus d'informations sur l'interface utilisateur San Diego, consultez Gérer les menaces de sécurité à l'aide de l'Espace de travail de l'analyste de sécurité.

Les rubriques suivantes sont numérotées. Suivez les rubriques énumérées ci-dessous dans l'ordre dans lequel elles sont présentées pour une installation et une configuration fluides de l'application.

Configurer votre ServiceNow AI Platform® instance pour l'intégration Splunk Enterprise Event Ingestion

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre ServiceNow AI Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application afin de garantir une installation et une configuration fluides.

Procédure

1. Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform® et Réponse aux incidents de sécurité (SIR).

   Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre ServiceNow AI Platform® instance.

   - Un utilisateur disposant du rôle d'administrateur ServiceNow AI Platform® (admin) installe l'application à partir de et ServiceNow Store lui affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin).
   - Si vous souhaitez transférer des événements manuellement pour Splunk Enterprise cette intégration, un utilisateur disposant du ServiceNow AI Platform® rôle administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

affecte un utilisateur ayant le rôle (sn_sec_splunk_v2.api_account_access) dans le ServiceNow AI Platform®. Ce rôle permet à un utilisateur ayant le rôle d'administrateur Splunk Enterprise d'accéder à l'API dans le qui est requise pour le transfert manuel d'événements ServiceNow AI Platform® pour cette intégration.

Le rôle (sn_sec_splunk_v2.api_account_access) n'est pas requis pour l'intégration si vous ingérez automatiquement des alertes depuis Splunk Enterprise votre ServiceNow AI Platform® instance.

- Un utilisateur disposant du rôle **sn_si.ingestion_profile_admin** supervise les tâches suivantes dans le ServiceNow AI Platform®:
  - Nomme, crée et modifie les profils d'alerte et d'événement.
  - Sélectionne et mappe les valeurs des alertes et des événements aux ServiceNow AI Platform® incidents de sécurité.
  - Prévisualise les détails de l'incident de sécurité pour plus d'exactitude avant de finaliser la configuration.
  - Planifie l'ingestion d'alerte en cours.
  - Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst).
  - Les utilisateurs disposant du sn_si.analyst travaillent sur des incidents de sécurité.

Pour plus d'informations sur les rôles et l'affectation de rôles aux utilisateurs, reportez-vous à la section Gestion des rôles .

2. Vérifiez que vous utilisez la version 6.0 ou ultérieure de l'API Splunk .

   Si vous avez accès à la Splunk Enterprise console, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.

3. Vérifiez que vous avez installé et configuré un Serveur MID.

   Un Serveur MID dans votre ServiceNow AI Platform® instance est requis pour se connecter au Splunk service si le serveur est déployé au sein de Splunk votre réseau d'entreprise. Pour plus d'informations sur les serveurs MID, voir Serveur MID

   Si vous utilisez le service, un serveur MID n'est Splunk Cloud pas nécessaire.

4. Vérifiez que les ServiceNow applications principales nécessaires à la prise en charge de l'intégration sont installées et activées.

   Le Réponse aux incidents de sécurité module d'extension Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration.

   Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide.

   a. Security Incident Response

   b. Cadre de travail d'intégration de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Security Support Common

d. Orchestration du support de sécurité

Pour plus d'informations sur l'installation Opérations de sécurité des applications principales, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Que faire ensuite

Vous avez correctement configuré votre ServiceNow AI Platform® instance pour l'intégration. L'étape suivante consiste à installer l'application Splunk Enterprise Event Ingestion à partir de ServiceNow Store pour l'intégration. Pour plus d'informations, consultez Installez et configurez l'application ServiceNow pour l'intégration Splunk Enterprise Event Ingestion.

Si vous n'avez pas enregistré les recherches dans votre Splunk Enterprise console pour l'ingestion, ou si vous effectuez simultanément la configuration initiale de cette intégration dans votre Splunk Enterprise console et le produit de votre ServiceNow AI Platform® instance, consultez la Opérations de sécurité rubrique Enregistrer les recherches pour l'intégration dans votre Splunk EnterpriseSplunk Enterprise Event Ingestion console pour plus d'informations.

Si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise console pour l'intégration, consultez Configurer votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise pour plus d'informations.

Installez et configurez l'application ServiceNow pour l'intégration Splunk Enterprise Event Ingestion

Avant d'exécuter l'intégration sur votre ServiceNow AI Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre correctement aux Réponse aux incidents de sécurité produits sur Opérations de sécurité votre ServiceNow AI Platform® instance.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

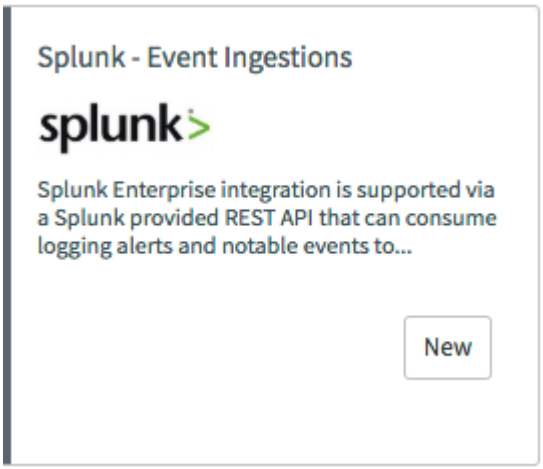
Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Si vous n'avez pas installé l'application Splunk Enterprise Event Ingestion à partir de pour ServiceNow Store l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette Ingestions d'événements Splunk .
3. Pour configurer l'application, cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sinon, si un bouton **Configurer** est affiché sur une tuile, cliquez dessus pour modifier une configuration existante.
5. Dans la boîte de dialogue Configuration des ingestions d'événements qui s'affiche, renseignez les champs.

Champ	Description
Nom	Nom de la console ou Splunk Cloud de l'instance Splunk Enterprise utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge. Par exemple, entrez HQ-USA, ou HQ USA.
URL de Base de l'API Splunk	URL de votre Splunk Enterprise console ou Splunk Cloud instance.
Authentification de base	Désactivé par défaut. Si vous utilisez le nom d'utilisateur du compte API et le mot de passe de l'API pour la configuration, cochez la case.
Nom d'utilisateur du compte API	Nom d'utilisateur que vous avez créé pour votre compte utilisateur individuel sur la Splunk Enterprise console.
Mot de passe de l'API	Mot de passe que vous avez créé pour votre compte utilisateur individuel sur la Splunk Enterprise console.
Basé sur un jeton (disponible à partir de la version 12.0.0)	Authentification basée sur les jetons que vous avez créée pour votre compte d'utilisateur d'API sur la Splunk Enterprise console.
Jeton	Jeton que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise console.
Serveur MID	Serveur MID spécifique configuré dans votre environnement. Seuls les serveurs MID actifs et validés sont disponibles dans cette liste de choix.

Traduction automatique

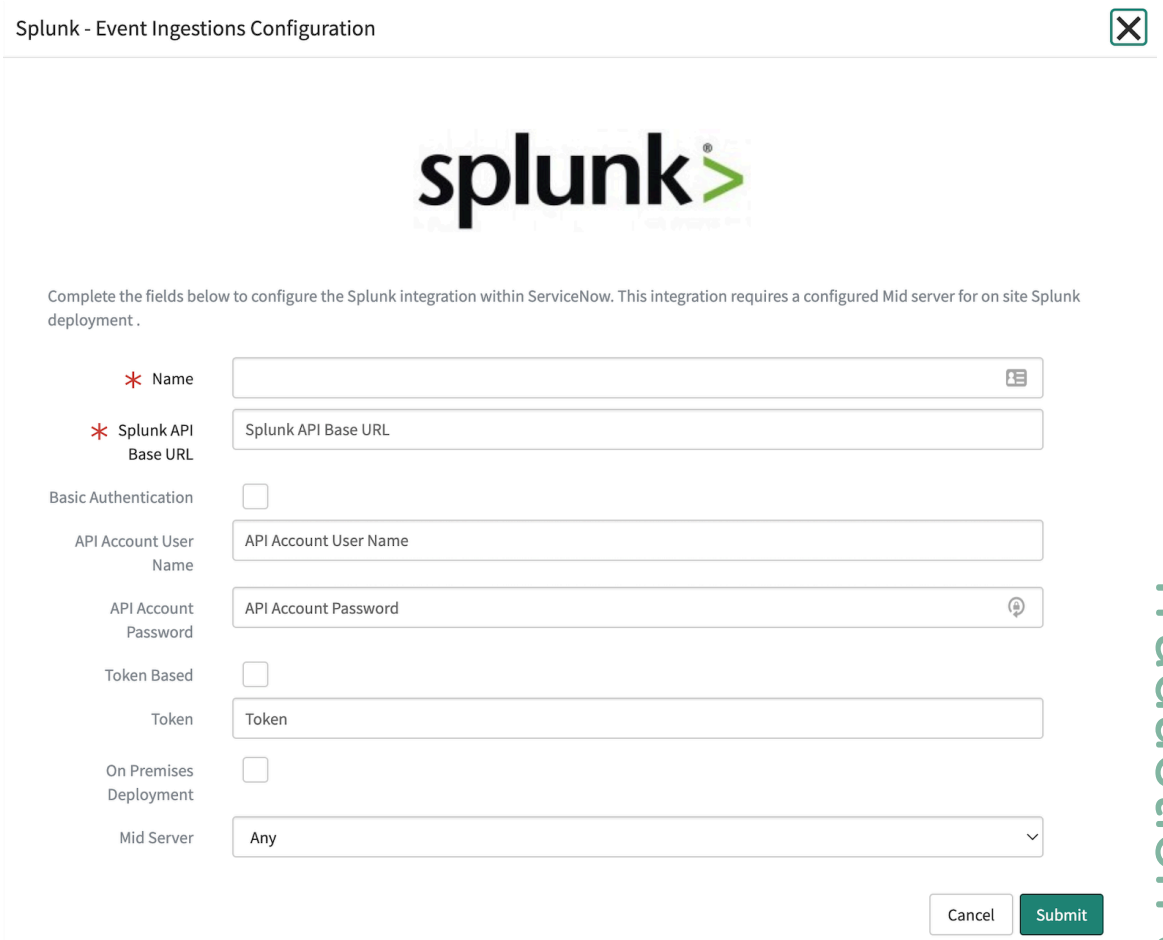
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Déploiement sur site	Désactivé par défaut. Si vous utilisez la version cloud de Splunk Enterprise, vérifiez que la case est décochée. Si cette option est activée, la liste de choix Serveur MID s'affiche. Si vous utilisez une version locale de Splunk Enterprise, procédez comme suit pour sélectionner un Serveur MID. **a.** Cochez la case. Une liste de choix s'affiche. La valeur par défaut est **N'importe lequel**. **b. Sélectionnez N'importe lequel** uniquement si ce Serveur MID est configuré pour l'intégrationSplunk Enterprise Event Ingestion. **c.** Dans la liste de choix, sélectionnez le ServiceNow AI Platform® serveur MID que vous avez configuré dans votre instance pour cette intégration spécifique.

La figure suivante est un exemple de formulaire rempli pour la configuration d'une version locale d'avec Splunk Enterprise un serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Chaque Splunk Enterprise alerte que vous ingérez à partir de votre Splunk Enterprise console nécessite un profil d'événement unique dans votre ServiceNow AI Platform® instance. Toutefois, la source que vous configurez dans le formulaire Configuration des ingestions d'événements peut être réutilisée pour plusieurs ServiceNow AI Platform® profils tant que chaque profil ingère des alertes déclenchées uniques Splunk .

6. Cliquez sur **Envoyer**.
   Une fois la validation terminée, la page Intégrations de sécurité s'affiche avec chacune de vos configurations. Sur chaque vignette de configuration valide, les boutons **Configurer** et **Supprimer** s'affichent comme illustré dans la figure suivante.

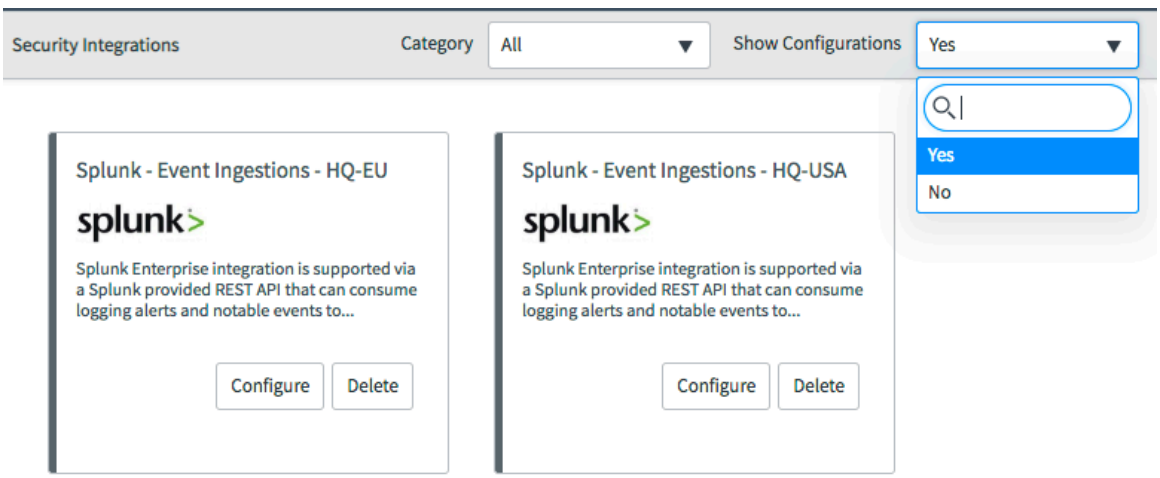
   Remarque : Vous devez utiliser uniquement l'authentification de base ou l'authentification basée sur les jetons. Activez l'une des authentifications et saisissez les détails de l'authentification correspondants. L'activation des deux affichera une erreur.

   Une fois validée et soumise, chaque configuration de serveur d'ingestions d'événements est enregistrée sur la page Intégrations Splunk de sécurité sous forme de tuile. Si les tuiles de configuration que vous avez enregistrées ne s'affichent pas sur la page Intégrations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de sécurité, dans le coin supérieur droit de la page, dans la liste de choix Afficher les configurations, cliquez sur **Oui**.



Trouble?

Si un message d'erreur s'affiche après avoir cliqué sur **Soumettre**, saisissez à nouveau vos informations et cliquez sur **Soumettre**.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer un profil d'événement.

Configurer les paramètres d'ingestion d'événements d'entreprise Splunk

Utilisez les paramètres d'ingestion d'événements d'entreprise Splunk pour modifier les configurations prédéfinies et leurs valeurs en fonction de vos besoins.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Accédez à la **Tous** > **Intégration Splunk** > **Paramètres de Splunk Integration**.
2. Renseignez les champs du formulaire.

Paramètres de Splunk Integration

Champ	Description
Nombre maximal d'alertes à afficher dans la création de profil. sn_sec_splunk_v2.max_alertes_à_affichage	Option permettant de définir le nombre maximal d'alertes que vous souhaitez afficher lors de la création d'un profil d'événement. Par défaut, la valeur est définie sur 500.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nombre maximal d'incidents de sécurité à créer en une journée. sn_sec_splunk_v2.max_si_per_day	Option permettant de définir le nombre maximal d'incidents de sécurité qui peuvent être créés en une journée. Par défaut, la valeur est définie sur 1 000.
Nombre maximal d'événements à extraire de Splunk par appel. sn_sec_splunk_v2.max_événements_par_appel	Option permettant de définir le nombre maximal d'événements à récupérer à partir de Splunk pour chaque appel. Par défaut, la valeur est 100.
Nombre de jours pendant lesquels un élément reste dans la table des files d'attente après s'être terminé ou avoir généré des erreurs à des fins d'information ou de débogage. sn_sec_splunk_v2.queue_item_expire	Option permettant de définir le nombre de jours pendant lesquels un élément doit rester dans la table des files d'attente après l'achèvement ou une erreur survenue en raison de l'information ou du débogage. Par défaut, la valeur est définie sur 14.
Nombre de jours de conservation des données d'importation d'événement, d'événement à tâche et d'alertes déclenchées. sn_sec_splunk_v2.retention_period	Option permettant de déterminer le nombre de jours pendant lesquels vous souhaitez conserver les données d'importation d'événement, d'événement à tâche et d'alertes déclenchées. Par défaut, la valeur est définie sur 30.
Activez ce paramètre pour mettre à jour les configurations de source Splunk existantes pour la prise en charge de l'authentification basée sur les jetons. Vous devrez mettre à jour la configuration d'intégration avec les détails du jeton une fois ce paramètre activé. sn_sec_splunk_v2.upgrade_existing_tile	Option permettant de mettre à jour la configuration source Splunk existante sur la prise en charge de l'authentification basée sur les jetons à partir d'une version existante. **Remarque :** Après la mise à niveau vers la nouvelle version, le champ de jeton devient indisponible. Vous devez activer ce paramètre pour obtenir l'authentification basée sur le jeton, après quoi vous devez mettre à jour la configuration d'intégration avec les détails du jeton. Par défaut, la valeur est définie sur Non.
Niveau de journalisation : débogage, informations, avertissement, erreur. sn_sec_splunk_v2.logging.verbosité	
Durée de vie de recherche Splunk en secondes. sn_sec_splunk_v2.sid_ttl	Par défaut, la valeur est définie sur 14.
Nombre de minutes de chevauchement à ajouter lors de l'extraction des événements à partir de Splunk (pour surmonter le délai d'indexation de Splunk). sn_sec_splunk_v2.overlap_time	Par défaut, la valeur est définie sur 0.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Taille du lot de la règle d'alerte à utiliser pour déclencher des requêtes de recherche Splunk pendant l'ingestion. sn_sec_splunk_v2.rules_batch_size	Par défaut, la valeur est définie sur 50.
Limite d'événements par alerte déclenchée pour gérer le pic. sn_sec_splunk_v2.spike_events_limit	Par défaut, la valeur est définie sur 1 000.
Le caractère du délimiteur pour diviser les valeurs dans les mappages de champs. sn_sec_splunk_v2.délimiteur	

3. Sélectionnez **Enregistrer**.

Créer et nommer un profil d'événement

Créez un profil d'événement dans votre ServiceNow AI Platform instance et déterminez quelles alertes créent des Splunk incidents de sécurité.

Avant de commencer
Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche
Avant ServiceNow AI Platform Réponse aux incidents de sécurité que les incidents de sécurité (SIR) ne soient créés à partir d'alertes ingérées, les valeurs de champ des alertes sont affichées sur une mise en page d'un ServiceNow AI Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera affiché.

Du point de vue de l'intégration, à l'aide des API disponibles, Splunk les événements sont transmis individuellement et manuellement en tant qu'événements discrets, ou ils sont combinés en alertes déclenchées qui sont automatiquement ingérées dans l'environnement Opérations de sécurité de votre ServiceNow AI Platform instance. Les workflows d'intégration ingèrent différents types d'alertes, telles que les tentatives d'accès non autorisé et les programmes malveillants, par exemple.

Ces alertes sont ingérées en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance. Toutes les alertes sont initialement ingérées pour un type d'alerte configuré dans un profil. Les alertes ingérées peuvent ensuite être filtrées davantage pour spécifier quelles alertes créent des incidents de sécurité. Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les alertes identifiées comme à haut risque. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir des alertes ingérées, les valeurs de champ individuelles des alertes filtrées sont mappées aux champs correspondants sur une mise en page d'incident de sécurité pour un aperçu.

Les noms d'alerte des profils d'événements dans votre ServiceNow AI Platform instance doivent être uniques et ne peuvent être mappés qu'à un seul profil d'événement actif à la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

fois. Il s'agit des noms d'alertes déclenchées que vous avez configurés dans votre Splunk service dans le cadre de la configuration de l'intégration. Pour plus d'informations sur la configuration des alertes dans votre Splunk Enterprise environnement, voir Enregistrer les recherches pour l'intégration dans votre Splunk EnterpriseSplunk Enterprise Event Ingestion console.

L'application ServiceNow AI Platform ingère des alertes spécifiques à l'aide des workflows de l'intégration. Toutes les alertes qui répondent aux critères de sélection dans votre Splunk console d'entreprise sont initialement ingérées dans votre ServiceNow AI Platform instance.

Un profil dans votre ServiceNow AI Platform est une encapsulation d'une Splunk alerte dans votre Splunk console d'entreprise. Il existe une relation un-à-un entre les alertes ingérées avec un profil et les connexions à votre Splunk console d'entreprise : une alerte pour une connexion. Il existe une seule connexion https à une tête de recherche dans votre Splunk Enterprise console. Plusieurs alertes peuvent provenir d'une seule tête de recherche. Si vous vous connectez à plusieurs têtes de recherche dans votre Splunk Enterprise console, vous devez créer plusieurs profils dans votre ServiceNow AI Platform instance pour ingérer ces alertes.

Étapes pour créer des profils pour l'ingestion d'alerte planifiée

Procédure

1. Pour créer un profil d'événement pour une alerte, dans votre ServiceNow AI Platform instance, accédez à **Intégration Splunk ES** > **Profils d'événements Splunk ES**.
2. Si le formulaire de profil d'événement n'est Splunk pas affiché, cliquez sur **Nom** dans la barre de progression.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs.

   Un exemple de formulaire rempli suit la table.

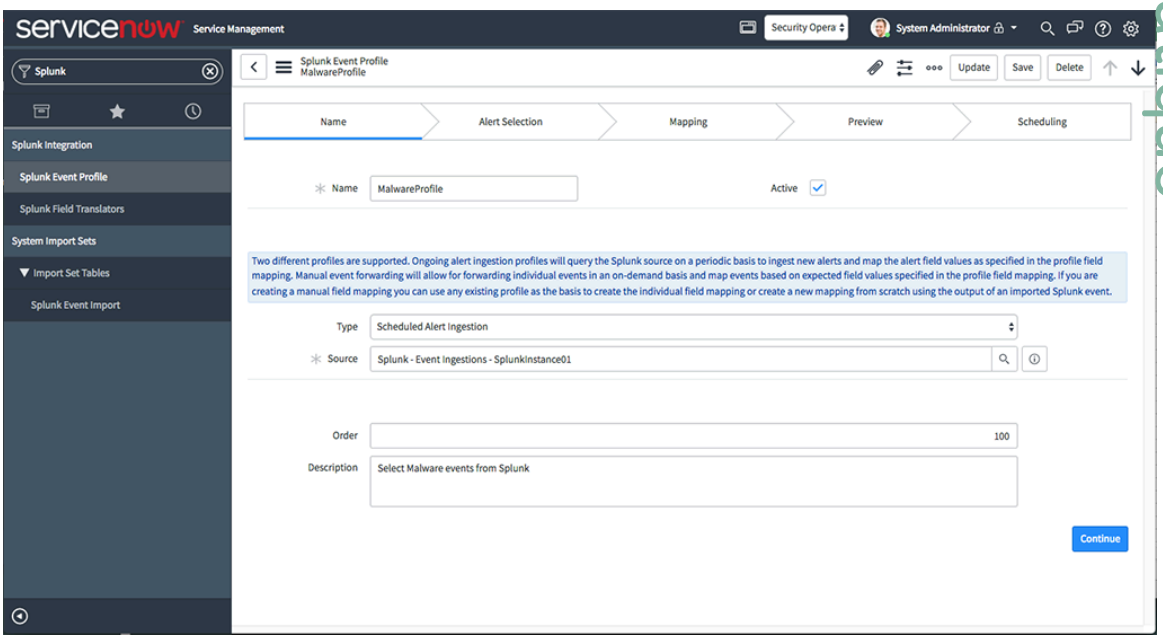
Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre ServiceNow AI Platform instance doivent être uniques.
Actif	La case à cocher est désactivée par défaut. L'option Actif est désactivée et n'est pas disponible à la sélection tant que vous n'avez pas terminé toutes les étapes de configuration du profil et cliqué sur **Terminer**.
Type	Sélectionnez le type de profil dans la liste de choix. ○ Ingestion d'alerte planifiée : ce type de profil prend en charge les alertes déclenchées qui sont ingérées selon un calendrier que vous configurez. Renseignez les champs et cliquez sur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Continuer pour passer à l'étape de sélection des alertes du profil. ○ Transfert manuel d'événements : ce type de profil prend en charge des événements individuels qui sont transférés manuellement à partir de votre Splunk Enterprise console sur demande. Consultez les étapes suivantes pour remplir le formulaire pour ces types de profils.
Type de source	Splunk Serveur ou extrémité de recherche que vous avez configuré pour ingérer des alertes. Si vous avez configuré plusieurs Splunk serveurs, sélectionnez le serveur approprié pour les types d'alertes que vous prévoyez d'ingérer pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Laissez ce paramètre par défaut. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Le workflow dans le profil avec le numéro le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli pour une alerte planifiée.



5. Pour un profil avec une alerte planifiée, choisissez une option pour poursuivre la configuration du profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Continuer	Enregistrez le profil et la progression de l'étape de sélection d'alerte.
Mettre à jour	Enregistrez les mises à jour de ce profil et revenez à la liste des profils d'événements Splunk .
Enregistrer	Enregistrez ce profil et restez sur la page.
Supprimer	Supprimez cet enregistrement de profil et revenez à la liste des profils d'événements Splunk .

Étapes pour créer des profils pour le transfert manuel d'événements

6. Pour créer un profil qui prend en charge le transfert manuel d'événements, procédez comme suit.

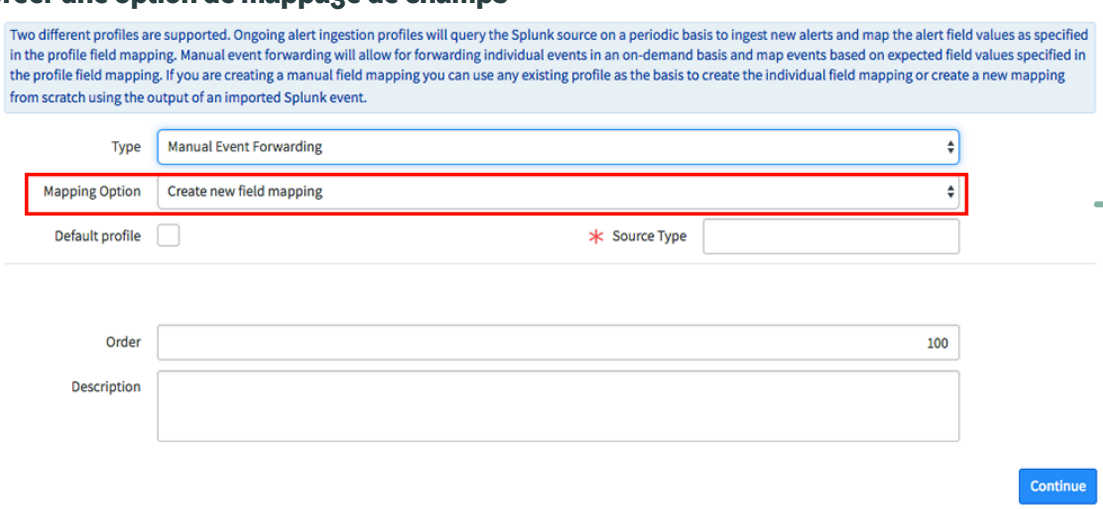
   Pour les événements que vous transférez sur demande à partir de votre Splunk console d'entreprise, vous pouvez baser le mappage de champs individuel sur n'importe quel profil existant. Vous pouvez également créer une grille de mappage pour les données de pièce jointe exportées. Les événements que vous transférez manuellement ne sont pas planifiés dans le profil d'événement.

   a. Si ce n'est pas déjà fait, dans la liste de choix du champ Type, sélectionnez **Transfert d'événements manuel.**

   b. Dans le champ Option de mappage qui s'affiche, dans la liste de choix, choisissez une option de mappage pour continuer.

      Reportez-vous aux figures et tableaux suivants pour plus d'informations sur les options de mappage disponibles dans la liste de choix Options de mappage.

Créer une option de mappage de champs



Créer une nouvelle option de mappage de champs

Option ou champ	Description
Créer une option de mappage de champs	Nouveau mappage de champs pour votre événement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
	Si vous n'avez pas de mappage de champs similaire au profil que vous créez, sélectionnez cette option pour créer une nouvelle carte.
Profil par défaut	Profil de transfert d'événements par défaut pour tous les Splunk événements. La valeur par défaut est effacée (désactivée). Lorsque cette option est activée, ce profil devient le profil par défaut pour le transfert manuel d'événements. Ce profil est le seul qui est actif et utilisé pour chaque Splunk mappage de champs d'événement à un SIR incident de sécurité. Un profil s'adapte à tous les événements transférés. Le champ Source n'est pas disponible si l'option de profil par défaut est activée.
Type de source	Splunk serveur. Ce champ n'est pas disponible si l'option de profil par défaut est activée. Si disponible, l'option Type de source permet un mappage de champs d'événements unique aux champs d'incident de sécurité en fonction du Splunk type de source. Si vous souhaitez gérer les événements de journalisation de pare-feu différemment des événements de détection de point de terminaison et qu'ils ont différents Splunk types de sources, vous pouvez créer différents profils d'événements en fonction des types de sources pour répondre à cette exigence.
Ordre	La valeur par défaut est 100. Laissez ce paramètre par défaut. Si vous avez créé un grand nombre de profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow dans le profil avec le numéro le plus bas a la priorité la plus élevée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

Pour un profil avec un nouveau mappage de champs, vérifiez que vous avez saisi une valeur dans le champ Type de source et cliquez sur **Continuer** pour passer à l'étape de mappage de la configuration.

Pour un profil avec un mappage de champs existant, reportez-vous à la figure et au tableau suivants pour plus d'informations.

Sélectionner un profil existant pour l'option de mappage de champ



Sélectionner un profil existant pour l'option de mappage de champ

Option ou champ	Description
Sélectionner un profil existant pour le mappage de champs	Un mappage de champs existant pour votre événement. Le champ Copier à partir du profil s'affiche. Suivez ces étapes pour copier un mappage de champs existant pour ce profil. **i.** À gauche du champ Copier à partir du profil qui s'affiche, cliquez sur l'icône de recherche. **ii.** Dans la liste Profils d'événements qui s'affiche Splunk , cliquez sur le nom du profil qui contient la carte que vous souhaitez copier. Le nom du profil s'affiche dans le champ Copier à partir du profil.
Profil par défaut	Profil de transfert d'événements par défaut pour tous les Splunk événements. La valeur par défaut est effacée (désactivée). Lorsque cette option est activée, ce profil devient le profil par défaut pour le transfert manuel d'événements. Ce profil est le seul profil actif. Il est utilisé pour le mappage de champs Splunk d'événements à un SIR incident de sécurité. Un profil s'adapte à tous les événements transférés. Le champ Source n'est pas disponible si l'option de profil par défaut est activée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
Type de source	Splunk serveur. Ce champ n'est pas disponible si l'option de profil par défaut est sélectionnée. Si disponible, l'option Type de source permet un mappage de champs d'événements unique aux champs d'incident de sécurité en fonction du Splunk type de source. Si vous souhaitez gérer les événements de journalisation de pare-feu différemment des événements de détection de point de terminaison et qu'ils ont différents Splunk types de sources, vous pouvez créer différents profils d'événements en fonction des types de sources pour répondre à cette exigence.
Ordre	La valeur par défaut est 100. Laissez ce paramètre par défaut. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow dans le profil avec le numéro le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

Au bas du formulaire de sélection d'un mappage existant pour votre profil, cliquez sur **Terminer** pour terminer la configuration du profil.

Que faire ensuite

Vous avez terminé avec succès les étapes de création de profils pour les alertes planifiées et le transfert manuel d'événements. Pour les profils destinés au transfert manuel d'événements, vous avez terminé la configuration du profil. L'étape suivante consiste à charger les données de la pièce jointe à l'étape de mappage.
Pour les profils des alertes planifiées, l'étape suivante consiste à sélectionner les alertes en vue de leur ingestion automatique.

Sélectionner les alertes planifiées pour l'intégration Splunk Enterprise Event Ingestion

Une fois que vous avez créé un profil pour une alerte planifiée, sélectionnez une Splunk alerte pour ce profil que vous souhaitez mapper à un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Affichez les alertes disponibles dans votre ServiceNow AI Platform instance afin de savoir quelles valeurs de champ sont disponibles pour le mappage. Sélectionnez une alerte pour vérifier que vous recevez les résultats attendus sur la mise en page de formulaire de base avant de mapper les valeurs aux champs sur SIR les incidents de sécurité. Vous ne pouvez sélectionner qu'une seule alerte dans la liste de ce formulaire.

Procédure

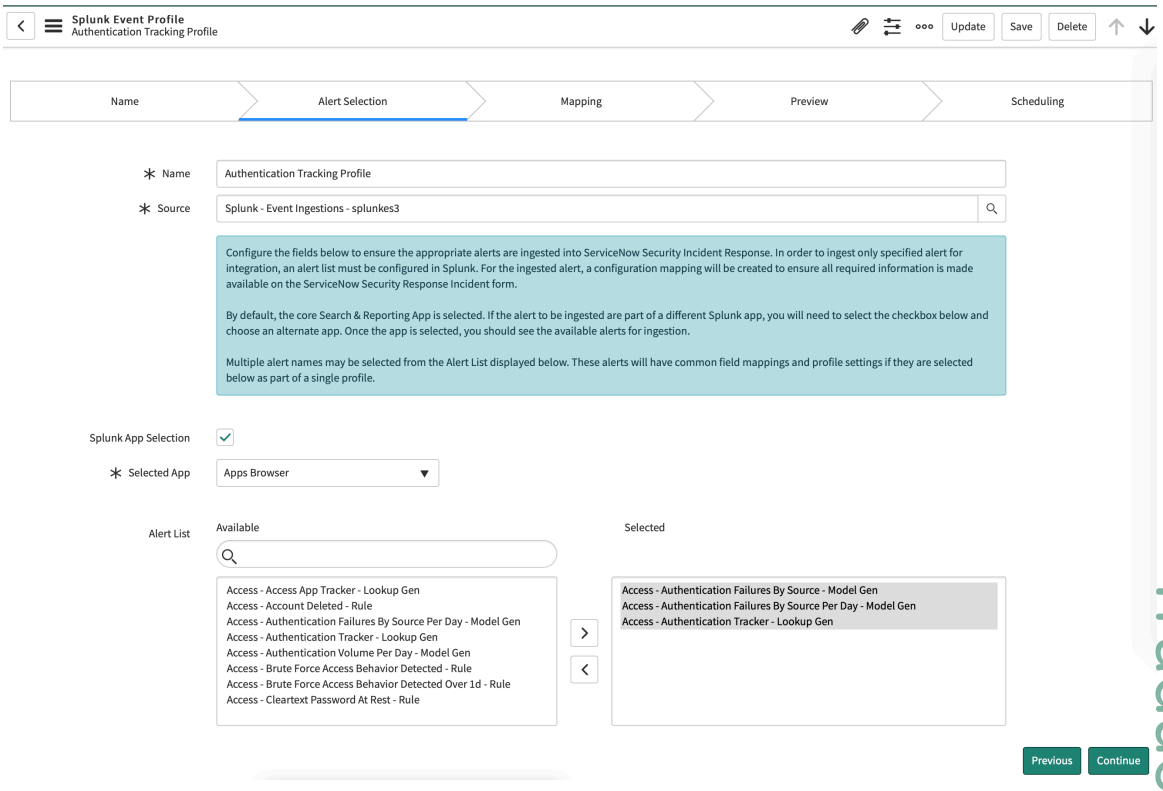
1. Si la page de sélection d'alerte n'est pas affichée, sélectionnez-la dans la barre de progression pour l'afficher. Par défaut, l'application de recherche et de reporting principale est sélectionnée.
2. Si l'alerte à ingérer fait partie d'une autre Splunk application, sélectionnez **Sélection d'application Splunk** et choisissez votre Splunk application dans la liste **des applications sélectionnées** .
3. Dans la **liste des alertes**, choisissez une alerte et déplacez-la de la colonne **Disponible** vers la colonne **Sélectionné** .
   Vous pouvez également choisir plusieurs alertes. Si les alertes sont sélectionnées dans le cadre d'un profil unique, les alertes auront des mappages de champs et des paramètres de profil communs.

   La liste des alertes de ce formulaire correspond à la liste des alertes de votre Splunk console. Jusqu'à 500 alertes sont affichées sur ce formulaire. Si plus de 500 alertes sont répertoriées dans votre console Splunk sur la page Alertes, seules les 500 premières alertes sont affichées sur ce formulaire dans votre ServiceNow AI Platform instance.

Option	Description
Dans le champ de recherche Liste d'alertes, saisissez du texte.	La colonne située sous le champ de recherche est filtrée avec les options disponibles en fonction du texte que vous entrez. Sélectionnez une alerte et, à l'aide des touches fléchées, déplacez l'alarme sélectionnée de **Disponible** à **Sélectionné**.
Dans la liste des alertes, double-cliquez sur une alerte.	La colonne **Sélectionné** est renseignée avec votre sélection.
Dans la liste d'alertes, cliquez sur une règle d'alarme.	L'alarme est sélectionnée. À l'aide des touches fléchées, déplacez l'alerte sélectionnée de **Disponible** à **Sélectionné**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Choisissez une option pour continuer.

Option	Description
Poursuivez ou cliquez sur Mappage dans la barre de progression	Le formulaire Mappage s'affiche. **Le mappage** est sélectionné dans la barre de progression. L'étape suivante consiste à mapper les champs d'alerte à un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements Splunk s'affiche.
Précédent	L'étape **Nom** s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements Splunk s'affiche.

Que faire ensuite

Vous avez sélectionné avec succès une alerte pour un profil d'alerte planifiée. L'étape suivante consiste à mapper les valeurs d'alerte aux champs d'un incident de sécurité.

Mappage des alertes et des événements pour l'intégration Splunk Enterprise Event Ingestion

Après avoir identifié les sources de l'ingestion d'alerte planifiée ou du transfert manuel d'événements, l'étape suivante consiste à mapper les champs d'événements individuels aux champs d'un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

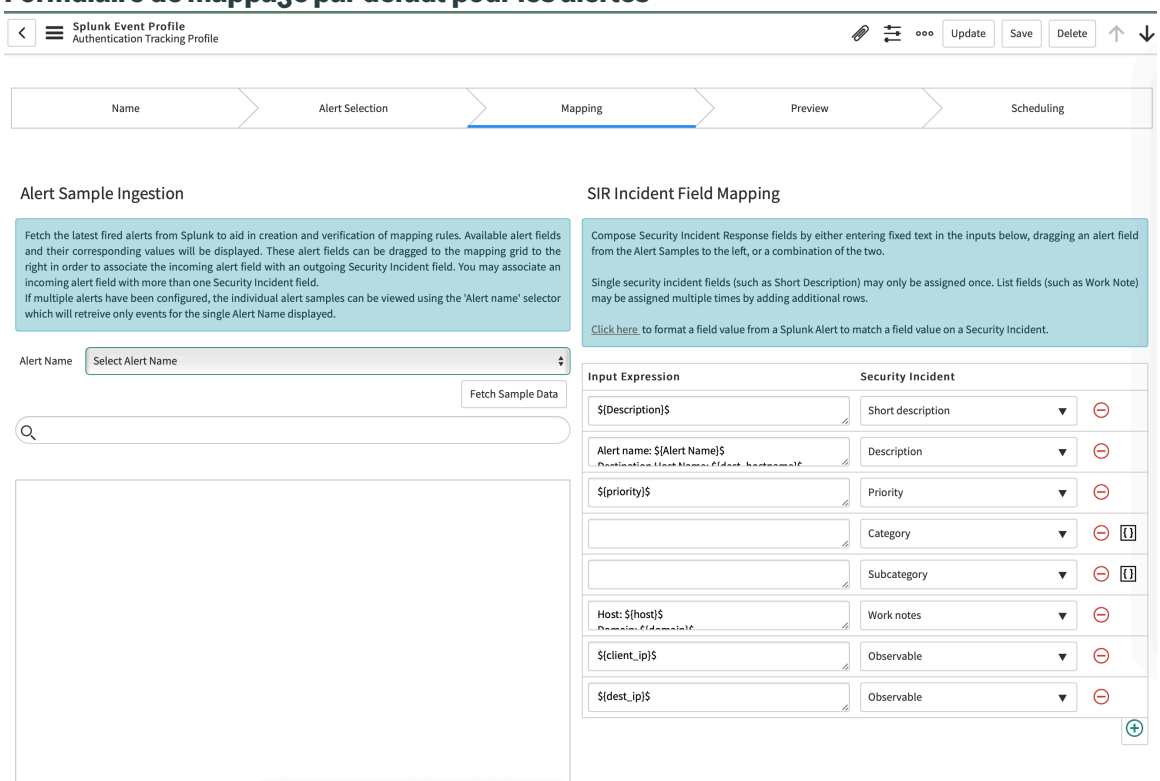
Vue d'ensemble du mappage des alertes et des événements

Pour l'étape de mappage, en tant qu'utilisateur disposant du rôle **sn_si.ingestion_profile_admin** , vous pouvez ingérer des échantillons d'alertes à partir de votre Splunk Enterprise console ou exporter des données d'événement pour un Splunk Enterprise événement.

Les figures suivantes illustrent les grilles de mappage par défaut fournies pour chaque type de profil d'événement. Ce mappage par défaut peut être modifié. Cette modification vous permet de personnaliser les champs qui renseignent l'incident de sécurité. Avec l'étape de mappage, vous pouvez visualiser l'impact de l'ajout ou de la suppression de champs d'événements sur les valeurs des champs d'incident de SIR sécurité.

Sélectionnez le **nom de l'alerte**, puis une fois que vous avez cliqué pour **extraire un exemple de données**, les valeurs des champs d'alerte Splunk sont renseignées sur le côté gauche du formulaire lorsque des échantillons d'alertes sont ingérés par le profil. Il s'agit des champs d'alerte Splunk que vous mappez aux champs d'incident SIR de sécurité.

Formulaire de mappage par défaut pour les alertes

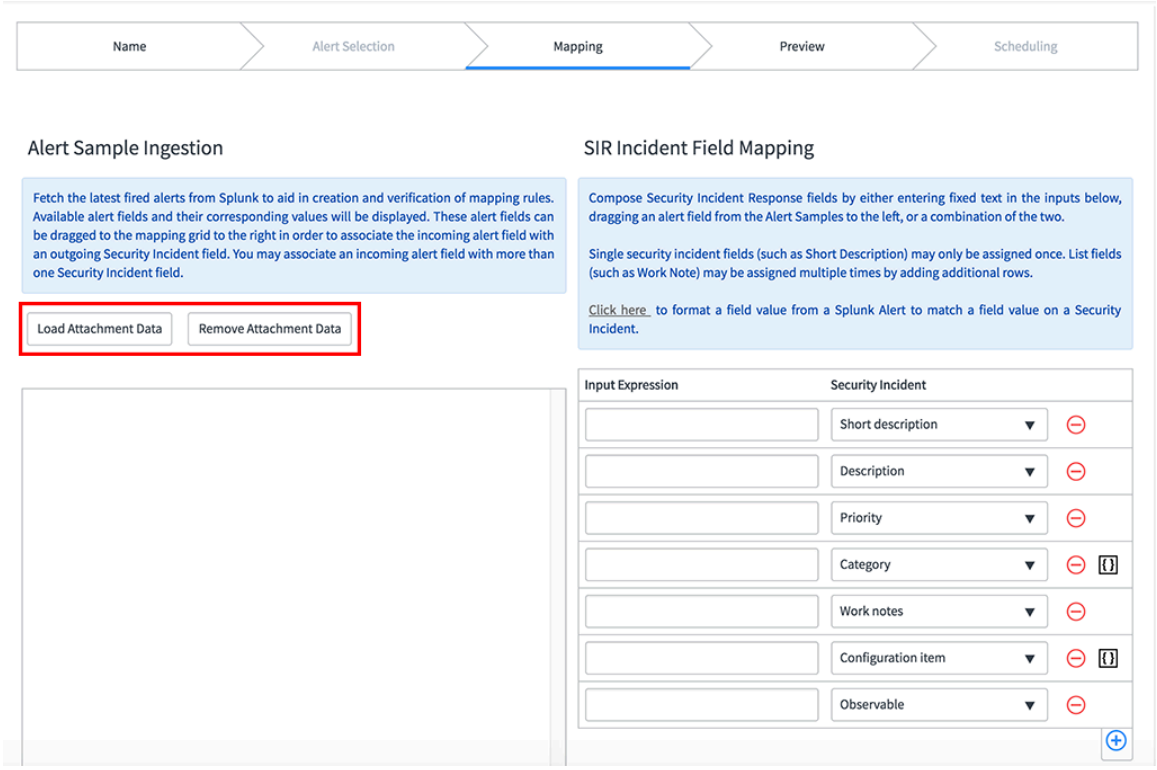


Une fois que vous avez cliqué pour charger les données de pièce jointe pour les événements transférés, les champs d'événement Splunk sont renseignés sur le côté gauche du formulaire. Il s'agit des Splunk champs de données mappés aux champs d'incident SIR de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de mappage par défaut pour les événements transférés



Vous préférez peut-être examiner quelques échantillons d'alertes sur votre Splunk console à ingérer pour l'étape de configuration du mappage de champ. Cette étape est étiquetée **Mappage** sur la barre de progression. Si cette page n'est pas affichée, cliquez sur **Mappage** dans la barre de progression.

Le mappage des alertes et l'exportation d'événements sur demande à partir de votre Splunk console d'entreprise incluent les concepts et les tâches suivants :

- Extraire des exemples de données pour les profils d'alerte ingérés automatiquement. Une fois les données extraites d'une alerte déclenchée sur la console, les Splunk Enterprise champs d'alerte disponibles et leurs valeurs correspondantes sont affichés dans une mise en page de mappage par défaut sur le côté gauche du formulaire de mappage. Des onglets s'affichent pour vous permettre d'afficher les valeurs d'un ID d'alerte que vous avez extrait. Vérifiez que tous les champs critiques de la section Ingestion d'échantillons d'alerte à gauche du formulaire sont mappés à la grille à droite du formulaire.
- Si nécessaire, chargez les données d'échantillon d'événement pour tous les profils d'événement transférés manuellement. Les exemples de données relatifs à ces événements sont exportés dans un fichier .xml à partir de la Splunk Enterprise console et chargés dans votre ServiceNow AI Platform® instance. Les données importées sont affichées dans la section Ingestion d'échantillons d'alerte à gauche du formulaire.
- Modifiez la configuration de mappage en faisant glisser les alertes du côté gauche et en les déposant sur la grille de mappage de droite. La grille de mappage sur la droite associe le champ d'alerte entrante à un champ d'incident de sécurité sortant.
- Personnalisez la grille de mappage en ajoutant ou en supprimant des champs. Suivez les champs négligés ou dupliqués à l'aide du code couleur fourni.
- Définissez des conditions de filtre afin de pouvoir spécifier quelles alertes sont ingérées dans l'application SIR et quelles alertes sont filtrées.
- Définissez des critères de champ d'incident supplémentaires qui regroupent une alerte entrante à un incident de sécurité existant SIR afin d'éviter les incidents en double.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

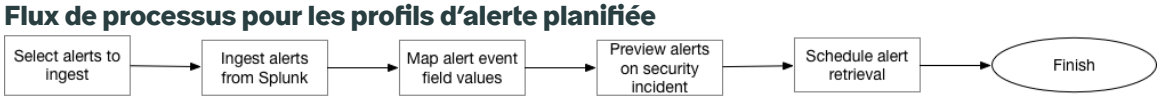
Ce filtrage supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'événement de sécurité connexes sur un seul incident de sécurité.

- Dans certains cas, les valeurs des champs d'événements dans la Splunk console Enterprise peuvent ne pas être traduites directement dans les champs de l'incident SIR de sécurité. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, les valeurs des champs Alerte de programme malveillant et Infection virale de la Splunk console se traduisent toutes deux par Activité de code malveillant dans le champ Catégorie de l'incident SIR de sécurité.

Profils d'alertes planifiées

Après la création d'un profil d'alerte planifiée, le flux de processus pour la configuration est illustré dans la figure suivante.

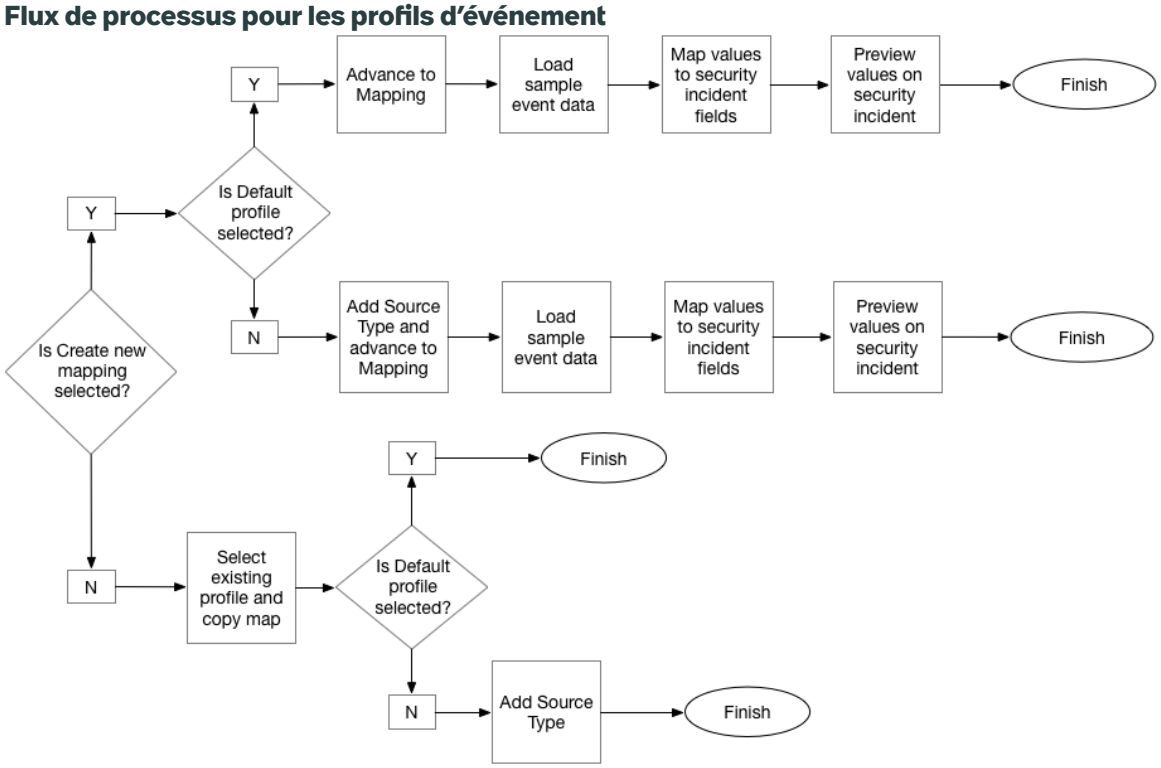
Flux de processus pour les profils d'alerte planifiée



Profils de transfert d'événements manuels

Après la création d'un profil pour un événement, le flux de processus pour la configuration est illustré dans la figure suivante.

Flux de processus pour les profils d'événement



L'étape suivante consiste à ingérer les alertes déclenchées ou à exporter des données et à mapper les valeurs aux champs d'incident SIR de sécurité.

Mapper les alertes pour l'intégration Splunk Enterprise Event Ingestion

Au cours de l'étape de mappage de champs d'événements, vous mappez les champs d'événements individuels des alertes déclenchées ou des données d'événements importées

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

aux champs d'un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

La grille de mappage préconfigurée des champs d'incident de sécurité par défaut peut être modifiée. Le code couleur des champs d'événements vous aide à surveiller les valeurs de champ que vous avez déjà mappées. Cette étape vous permet de visualiser l'impact de vos modifications sur les champs de l'incident de sécurité.

Mappez jusqu'à cinq alertes de la colonne Ingestion d'échantillons d'alerte à gauche du formulaire aux champs d'incident de sécurité dans la colonne Mappage du champ d'incident SIR à droite.

Créez des cartes personnalisées en ajoutant ou en supprimant des champs sur la grille de mappage située à droite du formulaire. La personnalisation des champs vous permet de mapper Splunk les champs qui ne sont pas affichés sur la grille de mappage par défaut de l'incident SIR de sécurité.

Procédure

1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Pour un profil avec une alerte planifiée, sous Ingestion d'échantillon d'alarme, sélectionnez l'alerte dans le **nom de l'alerte** et cliquez sur **Extraire les données d'échantillon** pour extraire la dernière instance d'une alerte déclenchée à partir de la Splunk Enterprise console.

   Les alertes s'affichent sous forme d'onglets. Vous pouvez ingérer jusqu'à cinq des alertes les plus récentes.

   L'extraction des exemples d'événements peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran.

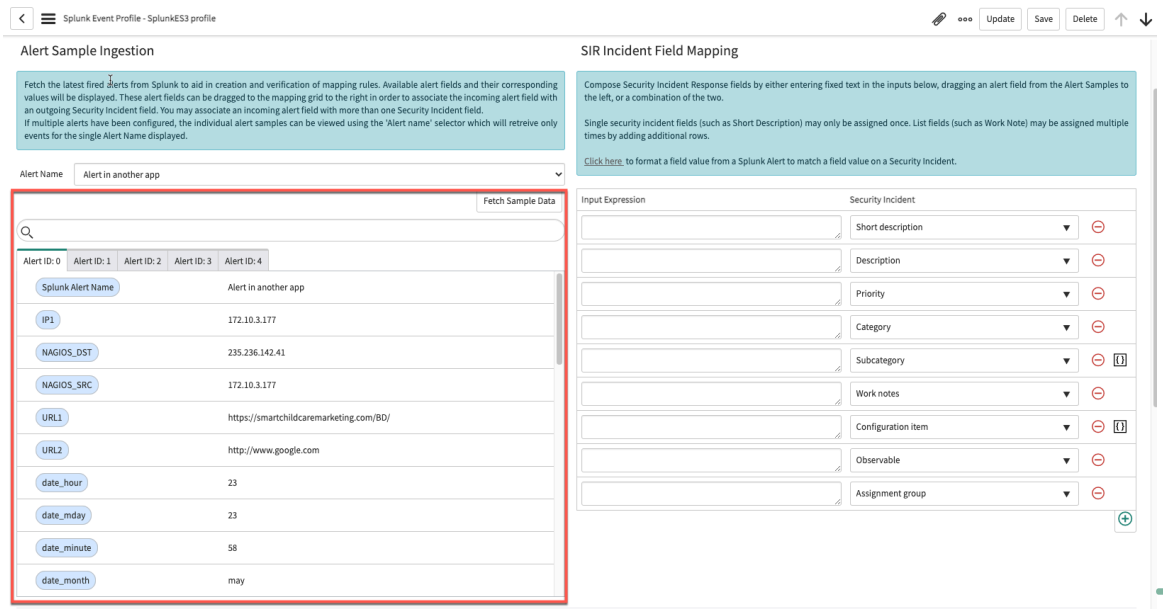
   Remarque : Un champ de mappage supplémentaire, **Nom d'alerte Splunk**, est ajouté par l'intégration pour permettre de retracer un événement jusqu'à la règle d'alerte source dans Splunk. Cela peut être utile dans les scénarios où plusieurs Splunk alertes sont combinées dans un seul profil.

   Lorsqu'un seul champ contient plusieurs valeurs, celles-ci sont analysées et mappées aux entrées de champ individuelles de la section de mappage de champ d'incident SIR. Par exemple, les adresses IP, les noms de ressources ou les URL sources peuvent avoir plusieurs entrées de champ observables ou plusieurs CI, ceux-ci sont analysés et mappés à des entrées de champ individuelles dans la section de mappage de champ d'incident SIR.

   Dans la figure suivante, les paires nom de champ de l'alerte ingérée, ou de l'exemple d'événement importé, s'affichent sur le côté gauche de ce formulaire une fois l'extraction terminée. Il s'agit des valeurs que vous mappez aux champs d'incident de sécurité du côté Mappage du champ d'incident SIR du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour les profils d'alerte planifiée, passez à l'étape cinq pour mapper les valeurs.
4. Pour le profil d'un type d'événement que vous souhaitez exporter à partir de votre Splunk Enterprise console, procédez comme suit pour charger les données de la pièce jointe dans votre ServiceNow AI Platform® instance.
   a. Si vous n'êtes pas déjà connecté, connectez-vous à votre Splunk Enterprise console.
   b. Accédez à l'onglet Rechercher et entrez un nom pour une recherche qui contient les données d'événement que vous souhaitez exporter.

      Par exemple, programme malveillant est un terme de recherche utilisé pour tous les événements de programme malveillant que vous pouvez transférer avec le workflow de cette intégration.

   c. Développez l'événement et, dans la colonne Champ, sélectionnez les champs que vous souhaitez importer.

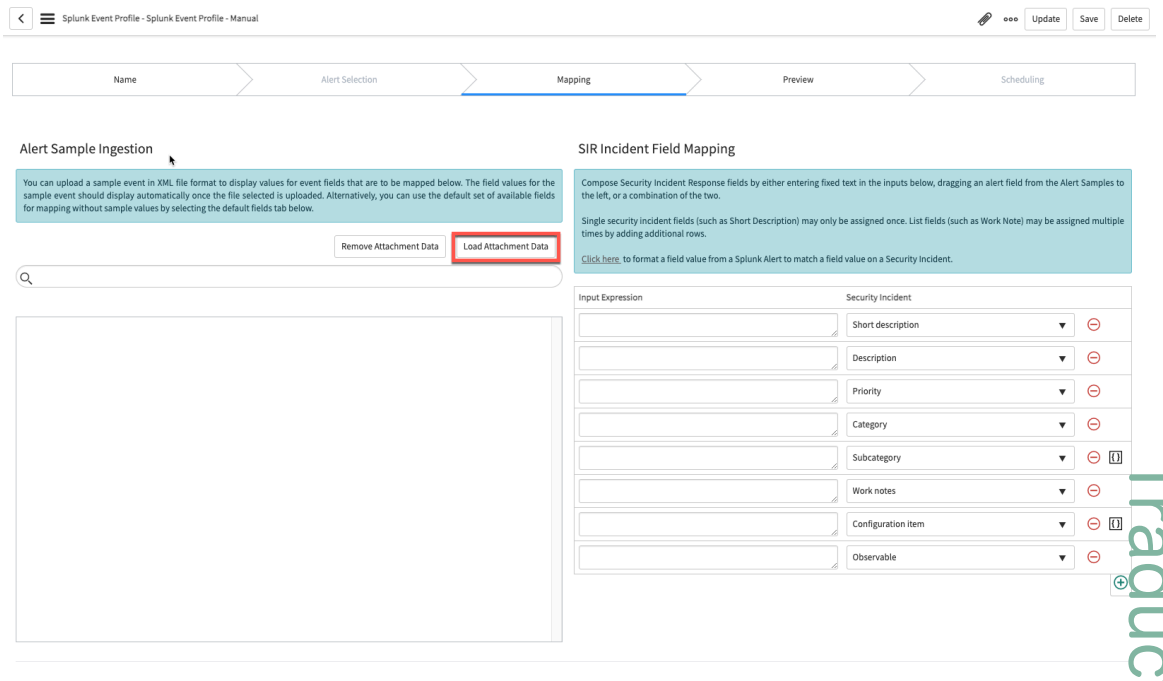
      Ces champs correspondent aux paires champ-valeur qui sont exportées et affichées sur la page de mappage de votre ServiceNow AI Platform® instance.

   d. Dans votre Splunk Enterprise console, en haut à droite de la page de recherche, cliquez sur l'icône **Exporter** .
   e. Dans la liste du champ Format de la boîte de dialogue qui s'affiche, cliquez sur **Format XML**.
   f. **Facultatif :** Entrez un nouveau nom de fichier.
   g. Cliquez sur **Exporter**.
      Le fichier est téléchargé sur votre ServiceNow AI Platform® instance.
   h. Si la page Mappage n'est pas déjà affichée dans votre ServiceNow AI Platform® instance, cliquez sur **Mappage** dans la barre de progression.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Dans la colonne Ingestion d'échantillons d'alerte, cliquez sur **Charger les données de la pièce jointe**.



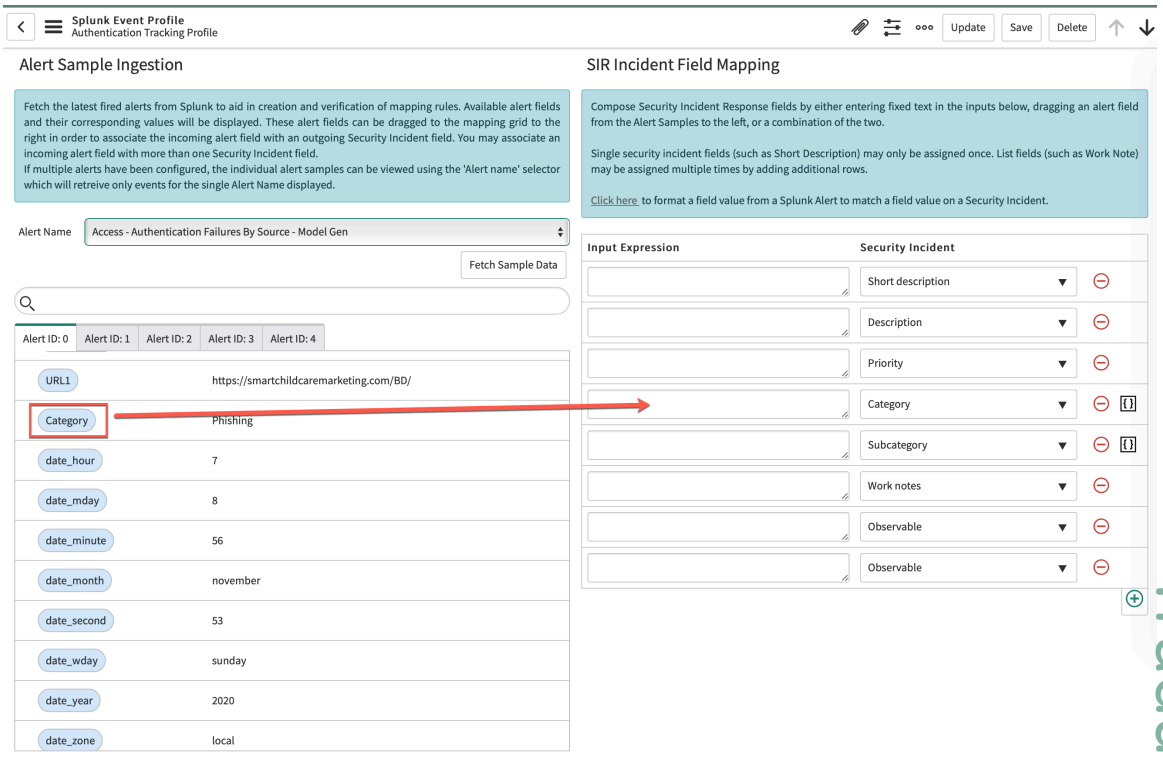
j. Dans la boîte de dialogue qui s'affiche, cliquez sur **Choisir des fichiers** et accédez au fichier .xml que vous avez exporté, puis cliquez sur **Ouvrir**.
Les paires de valeurs des champs que vous avez exportés pour l'événement s'affichent sur le côté gauche du formulaire de mappage.

Dans la figure suivante, les paires de données d'une alerte planifiée ingérée s'affichent sur le côté gauche de ce formulaire. Les paires de valeurs des événements importés sont également affichées de ce côté du formulaire. Il s'agit des valeurs de champ que vous mappez aux champs d'incident de sécurité du côté Mappage du champ d'incident Sir du formulaire.

5. Pour faire correspondre une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez tout en maintenant enfoncé le nom d'un champ bleu sur le côté gauche du formulaire.
6. Faites glisser le nom du champ, par exemple la catégorie, et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

Traduction automatique

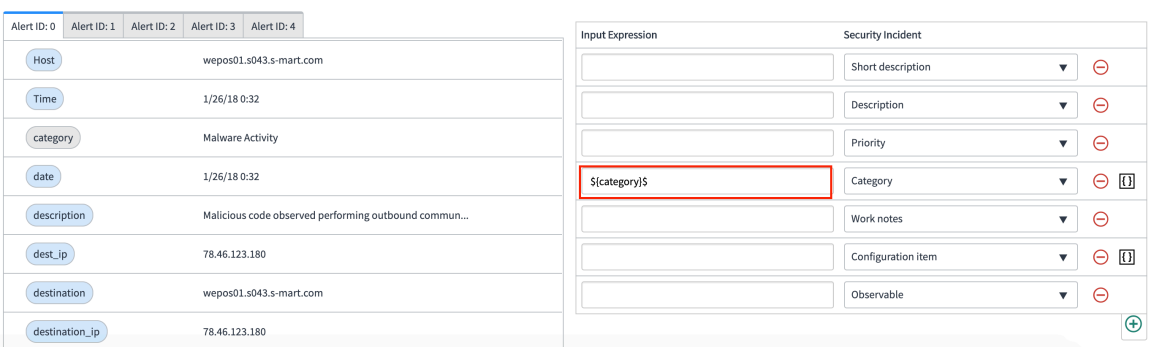
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, la catégorie est mappée au champ de catégorie de l'incident de sécurité. Toutefois, vous pouvez faire correspondre n'importe quelle valeur du côté gauche à un champ sur la droite. Vérifiez que la valeur est correctement mappée sur l'incident de sécurité pendant l'étape d'aperçu.

Pour vous assurer qu'aucun événement n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par des couleurs. Les champs bleu clair sur la gauche indiquent qu'aucun champ n'est encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ d'alerte entrante à plusieurs champs sur un incident de sécurité.

Un champ gris indique qu'un champ a été sélectionné et mappé à un champ de l'incident de sécurité. Ce code couleur vous aide à suivre le mappage, car dans certains cas, les champs d'événement d'alerte peuvent n'être affectés qu'une seule fois. Par exemple, vous ne pouvez affecter des valeurs à des champs tels qu'une seule fois à une description brève. Toutefois, vous pouvez affecter plusieurs fois des champs de liste tels que Note de travail en ajoutant des lignes supplémentaires à la grille de mappage.

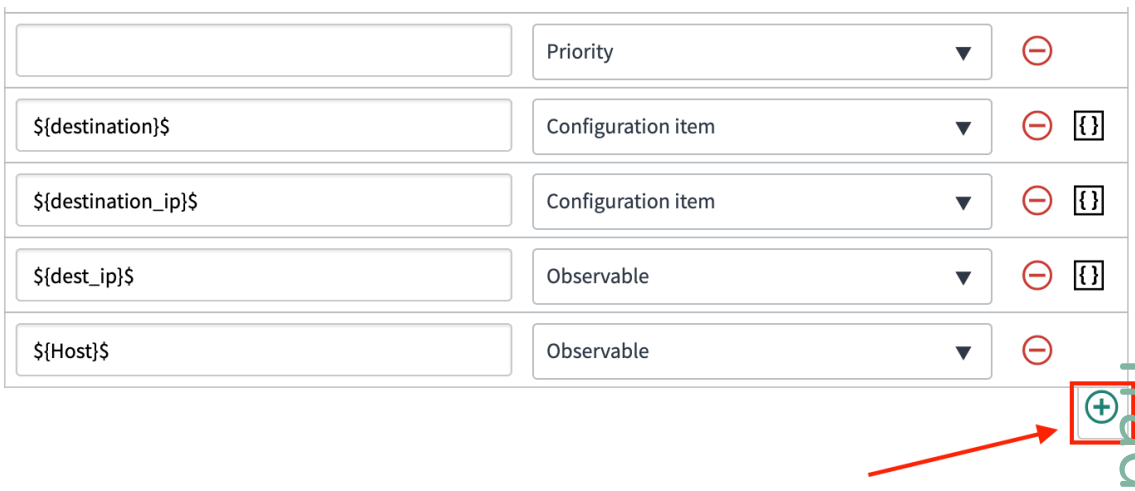


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Pour ajouter des champs au mappage par défaut de l'incident de sécurité sur le côté droit du formulaire, procédez comme suit.

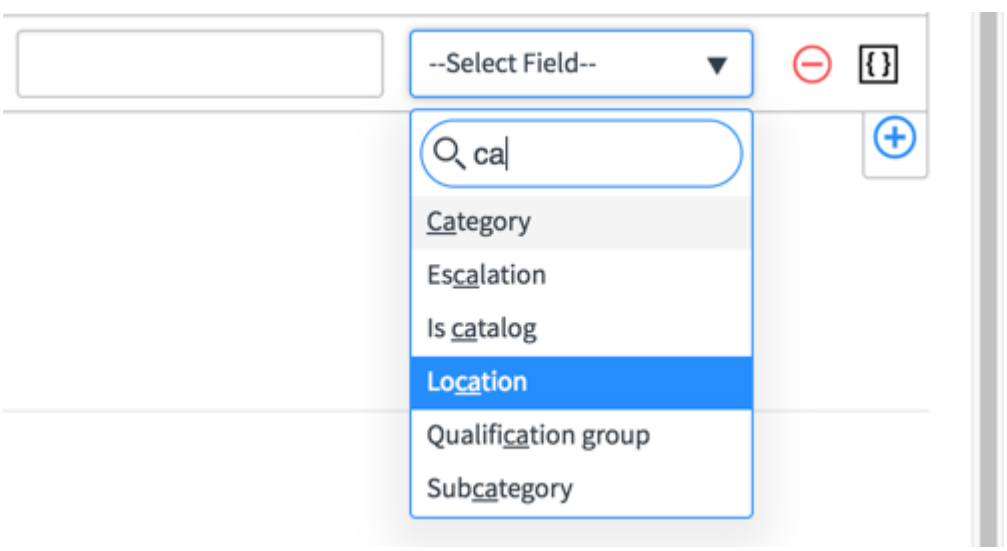
   a. À droite du formulaire, dans la section Mappage du champ d'incidents SIR, au bas de la grille, cliquez sur l'icône plus.



   Un nouveau champ s'affiche.

   b. Dans la colonne Incident de sécurité, développez la liste qui s'affiche, puis sélectionnez un champ.

   Dans la liste développée du nouveau champ, certains champs sont ombrés. Dans la figure suivante, la catégorie a un arrière-plan gris, car elle a été mappée dans l'incident de sécurité. Semblable au code couleur pour les champs d'alerte sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre le mappage.



Traduction automatique

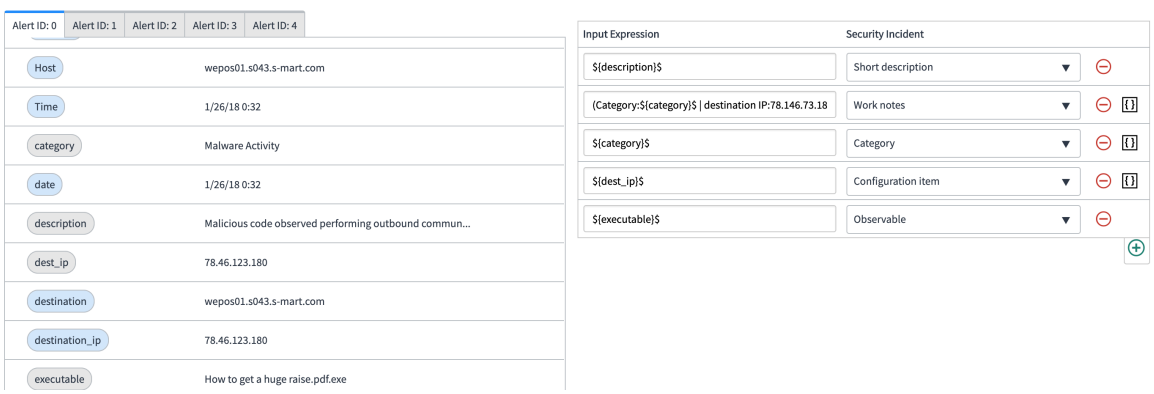
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Afin que plusieurs observables puissent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs.
Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité comporte une liste dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste, le champ n'est pas renseigné sur l'incident de sécurité.

c. Vous pouvez également saisir une valeur dans le champ Rechercher de la nouvelle ligne.

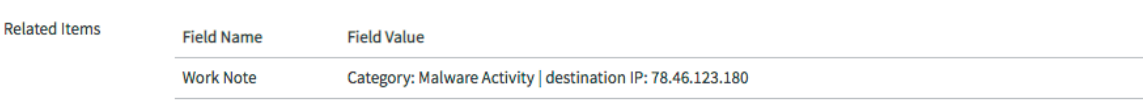
d. Sur le côté gauche du formulaire, cliquez avec le bouton gauche pour sélectionner **l'ID d'alerte** souhaité dans le champ expression d'entrée.
Avec la fonction de glissement, mappez-le à côté de votre nouveau champ.

8. Poursuivez le mappage en ajoutant ou en supprimant des champs et en ajoutant des valeurs à la carte.
La figure suivante est un exemple de grille de mappage modifiée. Dans le champ inférieur à droite, le champ Notes de travail est ajouté et comporte plusieurs valeurs. Les valeurs sont séparées par des espaces et des signes de ponctuation (Category :${category} | destination IP :78.146.73.180).



Dans l'aperçu, ces valeurs sont affichées dans les notes de travail sur l'incident de sécurité. Étant donné que la valeur se rapporte à un champ que vous avez ajouté à la grille et que plusieurs valeurs sont mappées au champ Notes de travail, les valeurs s'affichent telles qu'elles sont saisies. Dans cet exemple, les espaces et les signes de ponctuation que vous avez entrés dans le champ s'affichent dans la section Éléments connexes sous forme de note de travail sur l'aperçu de l'incident de sécurité.

L'image suivante est un exemple de la façon dont les valeurs de l'image précédente sont affichées sur l'incident de sécurité.



Conditions de filtrage de génération d'incidents

9. Facultatif : Une fois que vous avez terminé les étapes de mappage au niveau du champ précédentes, vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de filtre pour définir des critères supplémentaires qu'une alerte entrante doit satisfaire pour créer un incident de SIR sécurité.
Pour définir des conditions de filtrage, procédez comme suit.

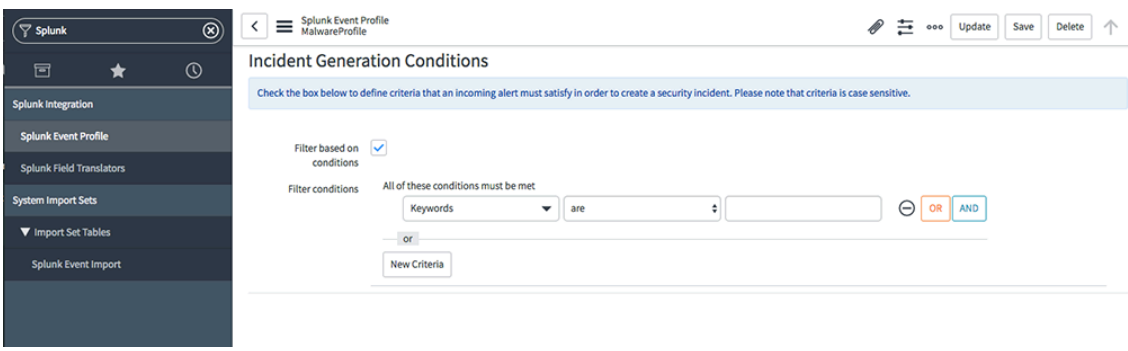
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Faites défiler la page jusqu'à la section Conditions de génération d'incidents sur le formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

(Optional) Le générateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

Les options des listes pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'alerte pour l'alerte que vous avez ingérée. Ces champs sont dynamiques et changent en fonction de l'alerte Splunk que vous ingérez ou de l'événement que vous transférez manuellement. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'alerte ou de l'événement Splunk Enterprise . Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférerez peut-être revenir à votre Splunk Enterprise console et passer en revue vos alertes et événements concernant les mots clés.

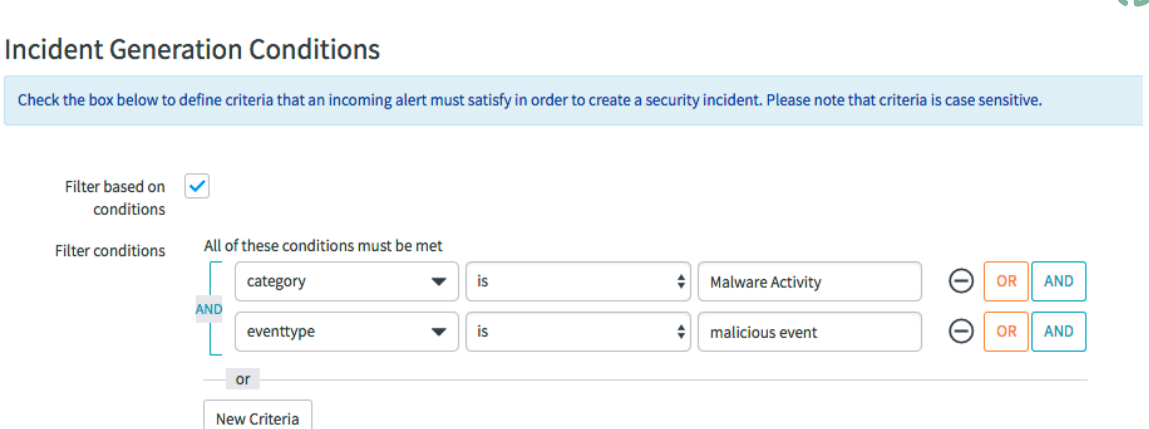


b. À l'aide des listes et des champs du générateur de conditions, définissez des filtres pour la première ligne.

c. Pour ajouter plus de conditions, à droite des champs, cliquez sur **ET** ou **OU**.
Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

d. **Facultatif :** Sur la deuxième ligne, définissez une deuxième condition de filtre.

(Optional) L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création d'incidents de sécurité.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(Optional) Vous avez défini les conditions de déclenchement afin que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

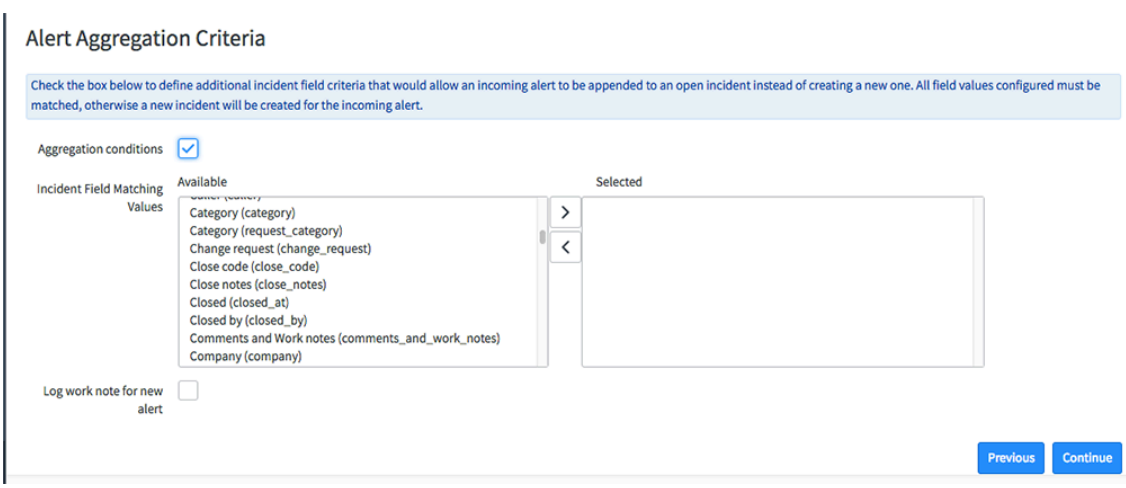
Ce type de filtrage vous aide à isoler les événements de sécurité et limite le nombre d'incidents de sécurité que vous créez. Si des critères de filtrage supplémentaires sont définis, seules les alertes requises sont ingérées sans qu'il soit nécessaire de modifier la requête ou la Splunk configuration des alertes déclenchées.

Agrégation d'alertes pour éviter les incidents en double

10. **Facultatif :** Pour éviter de créer des incidents de sécurité en double, définissez des critères de champ d'incident supplémentaires afin que les alertes entrantes soient regroupées en un incident de sécurité ouvert. Pour définir ces critères, procédez comme suit.

    a. Faites défiler jusqu'à la section Critères d'agrégation d'alertes sur le formulaire et cochez la case Conditions d'agrégat pour activer cette option.

    (Optional) Les colonnes Valeurs correspondantes au champ Incident s'affichent. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés sur l'incident SIR de sécurité.



    b. Dans la liste Disponible, sélectionnez les valeurs de champ que vous souhaitez faire correspondre aux incidents de sécurité existants dans ServiceNow AI Platform votre et déplacez-les vers la liste Sélectionné.

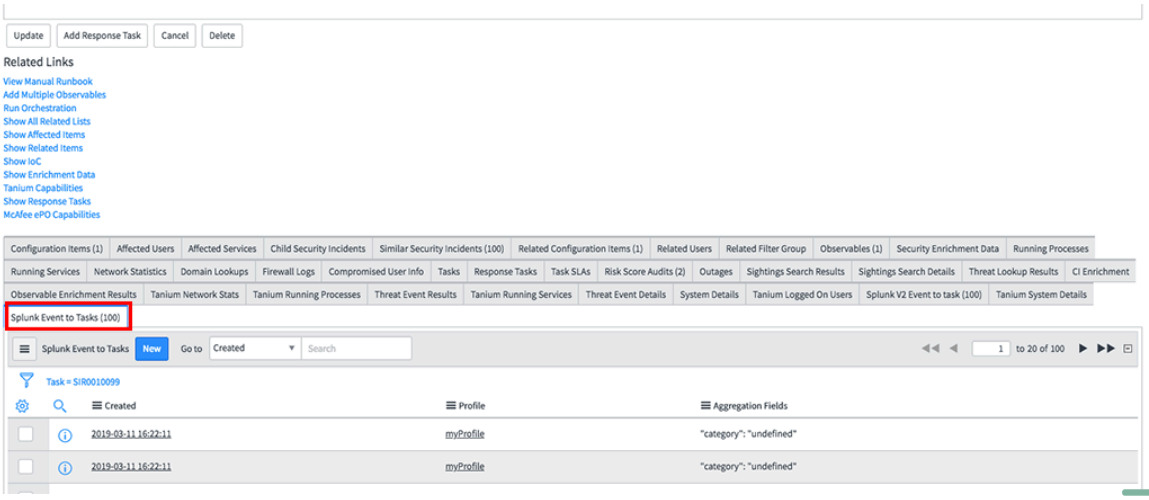
    (Optional) Toutes les valeurs de champ que vous sélectionnez doivent être mises en correspondance pour ajouter cette alerte entrante à un incident de sécurité existant. Si vous préférez examiner les valeurs de champ sur les incidents de sécurité à utiliser pour ce critère, accédez à **Incidents** > **Afficher tous les incidents**.

    Si une nouvelle alerte correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation à l'étape de mappage, l'alerte est automatiquement ajoutée à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur disposant du rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher toutes les alertes agrégées ajoutées sur une liste connexe sur un incident de sécurité. Toutes les alertes agrégées sur un incident de sécurité sont affichées dans la Splunk liste connexe Événement à Tâches. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi des alertes sont ajoutées aux incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'enregistrement sous Liens connexes et cliquez sur le lien **Afficher toutes les listes connexes** .



c. Facultatif : Pour enregistrer une note de travail pour une nouvelle alerte récemment ajoutée à l'incident de sécurité, cochez la case pour activer cette option.
La note de travail indique qu'une nouvelle alerte a été ajoutée, ainsi qu'un lien vers les détails de l'alerte.

Vous avez mappé avec succès les valeurs d'une alerte ou d'un Splunk événement aux champs d'un SIR incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage. Vous avez également ajouté des alertes ou des événements aux incidents de sécurité existants SIR .

11. Facultatif : Ouvrez l'éditeur de script et poursuivez la modification.

(Optional) Pour plus d'informations sur l'éditeur de script, reportez-vous à la section Utiliser l'éditeur de script pour formater les valeurs d'alerte pour l'intégration Splunk Enterprise Event Ingestion.

12. Choisissez-en un pour poursuivre la configuration du profil.

Option	Description
Continuer	Le formulaire Mappage s'affiche. **L'aperçu** est sélectionné dans la barre de progression. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements s'affiche Splunk .
Précédent	Le formulaire Alert Selection (Sélection d'alerte) s'affiche.
Supprimer	Supprimez ce profil d'événement pour afficher la liste des profils d'événement Splunk .

Que faire ensuite

L'étape suivante consiste à prévisualiser les valeurs que vous avez mappées sur l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prévisualiser l'incident de sécurité pour l'intégration Splunk Enterprise Event Ingestion

Une fois l'étape de mappage terminée, affichez un aperçu des valeurs que vous avez mappées dans un ServiceNow AI Platform® Réponse aux incidents de sécurité incident de sécurité (SIR). Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs d'alerte que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

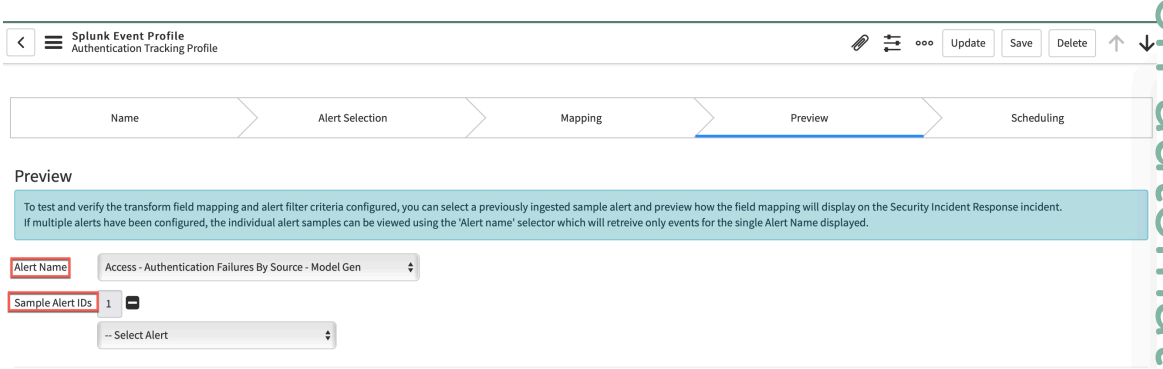
Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas effectué avec succès, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le SIR produit.

Procédure

1. Si l'aperçu de l'incident de sécurité ne s'affiche pas, cliquez sur **Aperçu** dans la barre de progression.
2. Sélectionnez le **nom de l'alerte** , puis sélectionnez un élément dans la liste **Exemples d'ID d'alerte** .

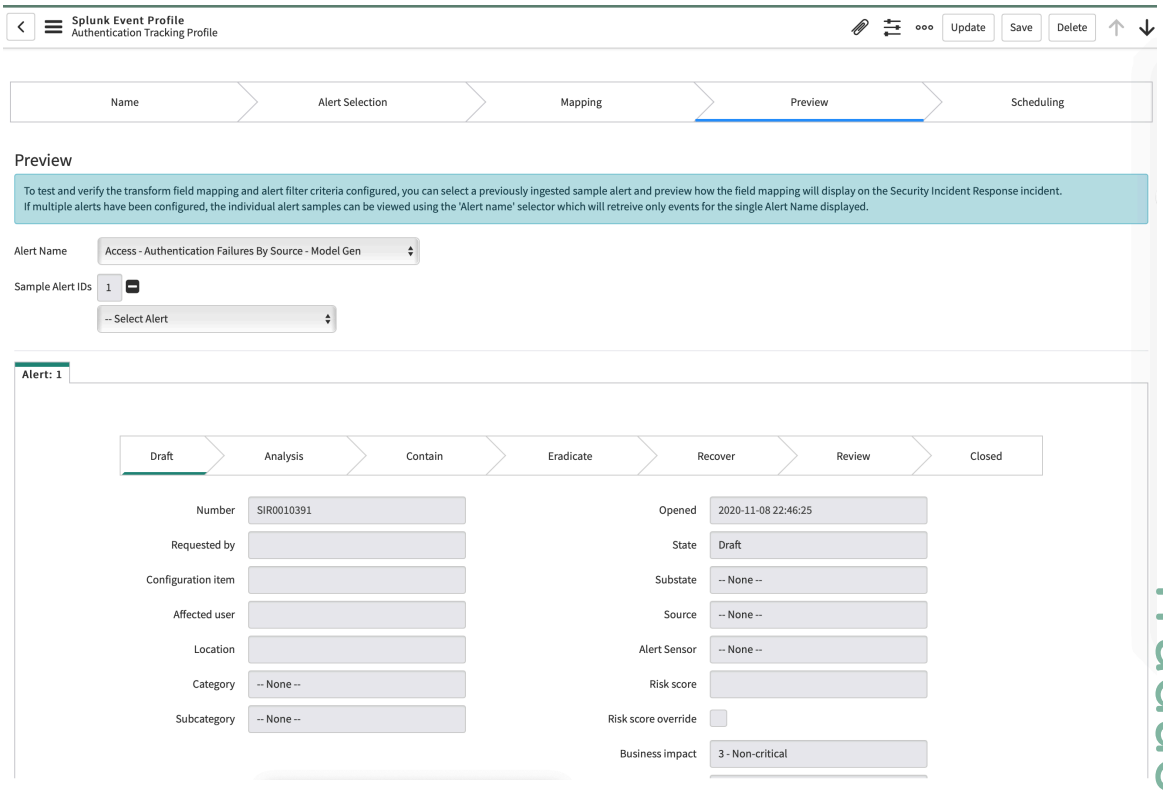


L'incident de sécurité s'affiche. Ne modifiez aucune information dans les champs. Cette vue est en lecture seule et aucun enregistrement de cet incident de sécurité n'est enregistré.

3. Examinez le mappage de champs des valeurs d'alerte sur l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



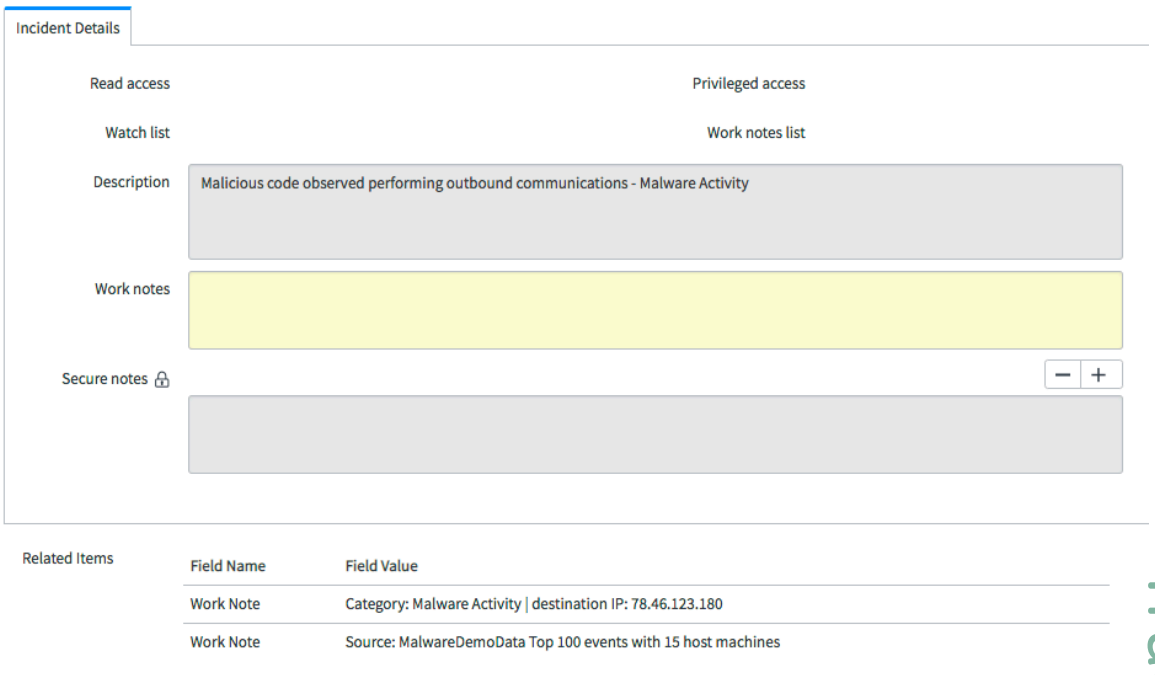
L'image précédente est un exemple d'aperçu avec une erreur de mappage. Dans cet exemple, un champ sur l'incident de sécurité n'existe pas pour une valeur, ou le champ ne prend pas en charge la valeur que vous avez mappée. Un message d'erreur s'affiche indiquant qu'aucune valeur d'entrée n'a été trouvée pour le champ Élément de configuration .

4. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
5. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
6. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

La figure suivante est un exemple d'onglet Détails de l'incident dans la moitié inférieure d'un SIR incident de sécurité une fois que tous les messages d'erreur ont été résolus. Pour cet exemple, les champs Description et Notes de travail ont été mappés, et ces champs sont renseignés avec les valeurs des paires de valeurs extraites de la Splunk Enterprise console. Le premier champ Notes de travail n'a pas de valeur. Ce champ a été laissé vide sur la grille de mappage pendant l'étape de mappage. Les champs Note de travail supplémentaires qui ont des valeurs ont été ajoutés à la grille de mappage au cours de l'étape de mappage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Une fois que vous avez corrigé les erreurs et vérifié que les champs sont comme vous le souhaitez, choisissez une option pour continuer.

Option	Description
Continuer	Le formulaire de planification s'affiche pour les profils avec des alertes planifiées. **La planification** est sélectionnée dans la barre de progression.
Terminer	Pour les profils configurés pour le transfert manuel d'événements, cliquez sur **Terminer**. Il n'existe aucune étape de planification pour les profils avec des données d'événement qui sont exportés sur demande directement depuis la Splunk Enterprise console.
Mettre à jour	Vos données sont enregistrées et vous revenez à la liste des profils d'événement Splunk .
Précédent	L'étape Mappage s'affiche dans la barre de progression.
Supprimer	Supprimez ce profil d'événement pour afficher la liste des profils d'événement Splunk .

Que faire ensuite

Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à Planifier et récupérer les alertes pour l'intégration Splunk Enterprise Event Ingestion.

Planifier et récupérer les alertes pour l'intégration Splunk Enterprise Event Ingestion

Pour les profils d'ingestion automatisée d'alertes, cette étape est la dernière étape de la configuration du profil d'événement. Au cours de cette étape, vous pouvez vérifier les paramètres par défaut pour la récupération des alertes ou modifier la planification si

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

nécessaire. Cette étape vous permet de filtrer la récupération de vos alertes en fonction d'une plage de dates.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Une fois que vous avez terminé toutes les étapes de la barre de progression de la configuration du profil, comme illustré dans la figure suivante, vous avez terminé la configuration des profils pour le transfert manuel d'événements. Aucune planification n'est disponible pour les événements transférés manuellement à partir de votre Splunk Enterprise console. Pour les profils d'ingestion automatisée d'alertes, vous choisissez si vous souhaitez ingérer des alertes historiques pendant l'étape de planification. Vous pouvez également choisir la fréquence à laquelle vous interrogerez les alertes futures qui correspondent à la configuration du profil d'alerte.

Barre de progression



Pour les profils d'ingestion d'alerte automatisée, avant que le profil ne soit activé, vous vérifiez et modifiez la planification et la récupération des alertes. Cette étape est la dernière étape du processus de configuration du profil d'événement pour les profils d'alerte planifiée.

Configurez ces intervalles d'interrogation par profil. Les performances de l'intégration de l'ingestion Splunk d'événements sont impactées par les différents intervalles d'interrogation. Lors de la planification, vous préférez peut-être équilibrer la charge du système par rapport à l'urgence de l'incident. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférez peut-être modifier ce paramètre en fonction de l'urgence de l'incident et de la charge prévue sur votre système.

Dans la Splunk Enterprise console, vous définissez une alerte à déclencher basée sur des incréments ou sur une heure spécifique. Utilisez ce paramètre pour vous aider à configurer la planification dans votre ServiceNow AI Platform instance afin que les incréments de temps de votre Splunk Enterprise console se synchronisent avec la planification que vous avez configurée dans votre ServiceNow AI Platform instance.

Procédure

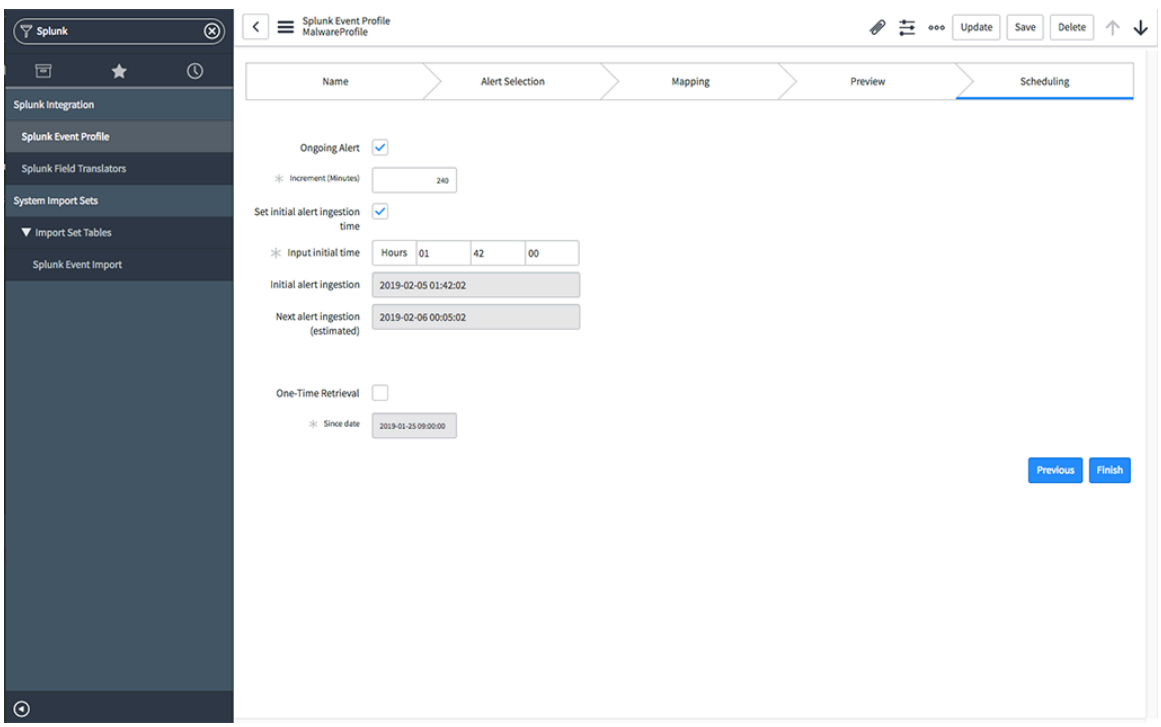
1. Si la page Planification de la barre de progression ne s'affiche pas, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les alertes sont extraites de la Splunk Enterprise console.

Option	Description
◦ Champ Alerte en cours sélectionné ◦ Champ Récupération ponctuelle effacé	Alerte en cours En fonction du paramètre par défaut, l'instance ServiceNow AI Platform extrait du Splunk Enterprise serveur de nouvelles alertes toutes les cinq minutes. Les incidents de sécurité sont créés si des alertes déclen–

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	chées sont trouvées et que les critères de filtrage sont vérifiés. Pour équilibrer l'ingestion d'alertes par rapport à la charge du serveur et pour extraire les données les plus récentes, vous préférez utiliser cinq minutes. Toutefois, cette valeur peut être modifiée si nécessaire.
◦ Champ Alerte en cours effacé ◦ Champ de récupération ponctuelle sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez une extraction ponctuelle pour ingérer des alertes basées sur des événements historiques. Lorsqu'il est configuré, un profil est utilisé une seule fois pour récupérer les alertes déclenchées, y compris les alertes des événements historiques basés sur une plage de dates. À droite du champ **Depuis la date** , cliquez sur l'icône Calendrier. Dans le calendrier qui s'affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire des alertes. À partir de la valeur **Depuis la date** , les alertes déclenchées sont récupérées jusqu'à la date actuelle. Une fois les alertes extraites, ce paramètre ne récupère pas les alertes déclenchées pour ce profil à partir de la date actuelle. Ce paramètre renseigne l'incident de sécurité avec toutes les alertes trouvées pour la plage que vous saisissez.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, si vous avez une alerte quotidienne Splunk qui s'exécute une fois par jour à 4 h (heure locale), vous pouvez configurer le profil d'alerte correspondant dans votre ServiceNow AI Platform instance pour qu'il s'exécute à 4 h 05, heure locale, afin de capturer immédiatement l'alerte et de créer un incident de sécurité. Saisissez `04 05 00` dans le champ **Ingestion d'alerte initiale** . Dans le champ **Incrémentation (minutes),** saisissez `1 440` (24 heures) pour planifier la prochaine ingestion d'alerte pendant 24 heures à compter de l'ingestion d'alerte initiale. Le délai d'ingestion de l'alerte initiale et l'heure d'ingestion de l'alerte suivante sont affichés dans les champs.

3. Pour configurer les paramètres de cet exemple, procédez comme suit.

   a. Une fois la page Planification affichée, cochez la case **Alerte en cours** pour activer cette option.

   b. Dans le champ **Incrémentation (minutes),** saisissez `1 440` (24 heures).

   c. Cochez la case **Sélectionner l'ingestion d'alerte initiale** pour activer la modification des champs Ingestion d'alerte initiale et Ingestion d'alerte suivante.

   d. Dans le champ Ingestion d'alerte initiale, saisissez `04 05 00`.
   Dans le champ **Prochaine ingestion d'alerte (estimée),** l'heure de la prochaine ingestion d'alerte s'affiche.

4. Cliquez sur **Terminer** pour terminer la configuration.
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Ce profil est activé et extrait les alertes de la Splunk Enterprise console en fonction de votre planification. Il existe une limite de 1 000 incidents de sécurité pouvant être créés dans une période de 24 heures. Jusqu'à 100 événements par alerte déclenchée. Les événements suivants sont ignorés une fois les limites atteintes.

Architecture d'intégration et connexion de systèmes externes pour l'intégration Splunk Enterprise Event Ingestion

La rubrique suivante décrit l'architecture d'intégration développée pour prendre en charge l'ingestion des alertes déclenchées à partir de la Splunk Enterprise console. Ces informations clarifient, à un niveau élevé, le fonctionnement conceptuel de l'intégration. Cela explique également pourquoi des étapes de configuration sont nécessaires avant d'installer l'application à partir du ServiceNow Store.

Termes clés utilisés pour cette intégration

Les termes clés suivants sont utilisés lors de l'installation et de la configuration. Pour plus d'informations sur ces termes, consultez le site Web de la documentation produit ServiceNow et le site Web et les ressources de Splunk sur la page Ressources Splunk .

ServiceNow AI Platform

Un produit d'entreprise ServiceNow . Il ServiceNow AI Platform s'agit de la base sur laquelle reposent les composants individuels tels que Réponse aux incidents de sécurité (SIR), IT Service Management (ITSM) et d'autres produits.

ServiceNow Module complémentaire Splunkbase

Une ServiceNow application installée sur votre Splunk Enterprise console qui prend en charge l'option de transfert manuel d'événements de l'intégration. Le transfert manuel d'événements est une fonctionnalité facultative de l'intégration. Ce ServiceNow module complémentaire Splunkbase n'est pas requis pour l'ingestion d'alerte automatisée fournie par l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Réponse aux incidents de sécurité (SIR)

Une ServiceNow AI Platform application qui suit la progression des incidents de sécurité depuis la découverte et l'analyse initiale, en passant par le confinement, l'éradication et la récupération, jusqu'à la revue et la fermeture finales post-incident.

Splunk Enterprise

Produit SIEM (Gestion automatisée des événements d'incident de sécurité) ou service dans le cloud qui collecte les données utilisées pour l'analyse et la gestion des incidents. Ce service est sur un hôte qui est parfois également appelé Splunk console dans ce guide.

alerte Splunk

Une recherche que vous configurez et enregistrez pour Splunk rechercher des données spécifiques en fonction des paramètres que vous avez configurés dans le Splunk Enterprise service. Lorsque vous extrayez des alertes de Splunk, vous extrayez également tous les événements associés à cette alerte.

Splunk Alerte déclenchée

Recherche configurée dans la Splunk Enterprise console qui renvoie des résultats et les marque comme alertes déclenchées. Les alertes déclenchées sont ingérées depuis la Splunk console dans votre ServiceNow AI Platform instance pour cette intégration. Les alertes déclenchées ont un ou Splunk plusieurs événements.

Splunk événement

Un ou plusieurs éléments de données qui entraînent le déclenchement des alertes du Splunk service. Dans votre ServiceNow AI Platform instance, vous pouvez rechercher quels Splunk événements ont déclenché ServiceNow AI Platform des incidents de sécurité.

Serveur MID

Cette application facilite la communication et le mouvement de données entre les applications, les sources de données et les ServiceNow AI Platform services externes. Cette application est généralement requise pour l'intégration avec les technologies sur site. Pour cette Splunk Enterprise Event Ingestion intégration, le Serveur MID facilite la communication entre l'instance ServiceNow AI Platform et l'instance sur site de Splunk Enterprise. Un serveur MID n'est pas nécessaire si vous intégrez votre ServiceNow AI Platform instance à une Splunk Cloud instance.

Administrateur d'incidents de sécurité (sn_si.admin)

L'utilisateur disposant de ce rôle supervise la configuration de l'intégration avec le SIR produit dans votre ServiceNow AI Platform instance.

Analyste des incidents de sécurité (sn_si.analyst)

L'utilisateur disposant de ce rôle interagit avec les incidents de sécurité du ServiceNow Réponse aux incidents de sécurité produit et les analyse.

Administrateur de profil d'incident de sécurité (sn_si.ingestion_profile_admin)

L'utilisateur disposant de ce rôle configure le module d'extension, crée, modifie, supprime et gère les profils d'ingestion pour Azure Sentinel, Splunk et Splunk ES Integration pour le SIR produit dans votre ServiceNow AI Platform instance.

Connexion aux systèmes externes

Un profil d'événement est un conteneur que vous créez, nommez et configurez pour Splunk une connexion et un appel uniques au service afin d'extraire les alertes déclenchées les plus récentes qui correspondent à des critères spécifiques. Une fois que les alertes déclenchées correspondant à votre profil ont été extraites de , vous sélectionnez celle que vous souhaitez afficher en tant ServiceNow AI Platform Réponse aux incidents de sécurité SIR qu'incident de Splunk sécurité. Une vue par défaut des champs d'alerte Splunk Enterprise est disponible, et vous pouvez modifier ce mappage des champs d'alerte sur les champs d'un SIR incident de sécurité pour répondre à vos besoins. Vous prévisualisez votre mappage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pour vérifier que toutes les valeurs de champ d'alerte requises sont renseignées sur l'incident SIR de sécurité. Pour terminer la configuration du profil d'alerte, vous planifiez la récupération des alertes, puis activez le profil. Après avoir activé le profil dans le ServiceNow AI Platform, vous êtes prêt à ingérer automatiquement les alertes historiques et en cours Splunk .

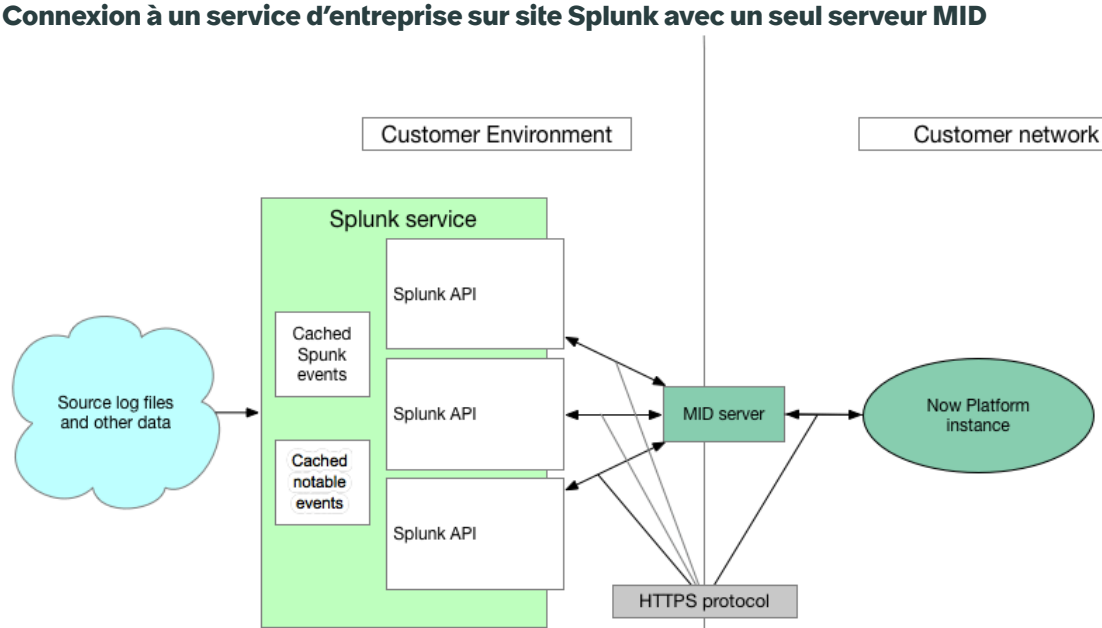
En tant qu'utilisateur disposant du rôle sn_si.admin, si vous déterminez qu'une nouvelle alerte déclenchée est similaire aux alertes précédemment ingérées, vous pouvez regrouper les nouvelles alertes déclenchées aux incidents de sécurité existants SIR . Vous définissez des critères pour spécifier les valeurs de champ cible correspondantes dans le profil d'alerte Splunk Enterprise qui définissent quand un incident de sécurité existant est mis à jour et quand un nouvel incident de sécurité est créé. Si la fonctionnalité d'agrégation est activée dans votre profil d'événement, lorsque le jeu d'importation est transformé, votre ServiceNow AI Platform instance recherche un enregistrement existant dans la table cible ayant la même valeur dans les champs cible et source. Si un enregistrement existant avec une valeur correspondante dans la table cible est trouvé, cet enregistrement est mis à jour. Si aucun enregistrement correspondant n'est trouvé, un nouvel enregistrement est créé dans la table cible. Si elle est activée, l'option d'agrégation met à jour les incidents de sécurité existants avec de nouvelles alertes déclenchées, et vous évitez de créer plusieurs incidents de sécurité. Pour plus d'informations sur la mise à jour des enregistrements à l'aide des options d'agrégation, voir Mise à jour des enregistrements à l'aide de la coalescence .

Cette application utilise le service d'API Splunk pour récupérer des informations à partir du Splunk service. Une connexion HTTPS sortante du serveur MID vers cet environnement est nécessaire pour que l'intégration fonctionne correctement.

Une fois connectée au Splunk service, l'intégration prend en charge l'extraction et l'ingestion d'alertes et d'événements déclenchés qui déclenchent des incidents de sécurité.

Le flux de données de base est illustré dans les figures suivantes. Dans chaque figure, votre ServiceNow AI Platform extrait (ingère) des données. Splunk n'envoie pas de données pour les alertes planifiées.

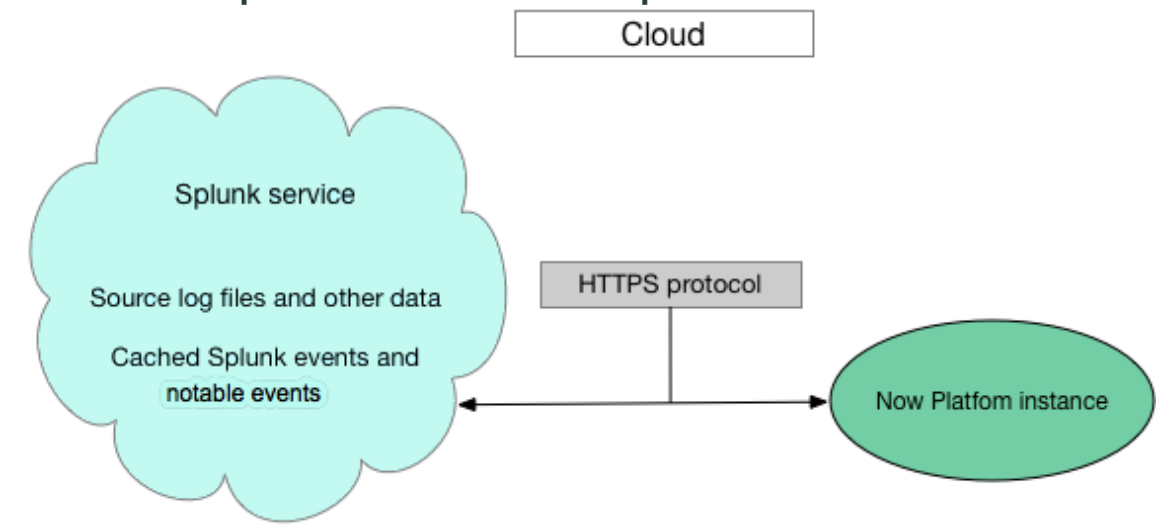
Connexion à un service d'entreprise sur site Splunk avec un seul serveur MID



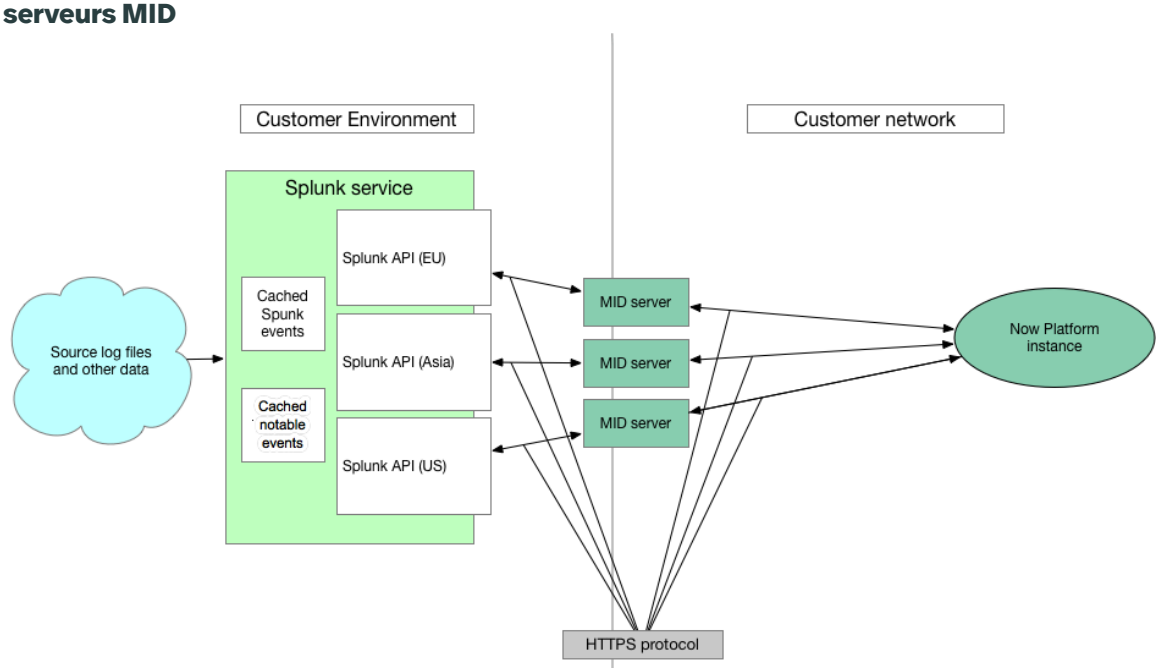
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connexion à une Splunk instance de cloud d'entreprise



Plusieurs connexions au Splunk service d'entreprise à l'aide de plusieurs serveurs MID



Traduction automatique

Copier Splunk Enterprise Event Ingestion des profils d'une instance à une autre à l'aide de la fonction d'exportation/importation

Vous pouvez exporter et importer Splunk Enterprise Event Ingestion des paramètres de profil d'une ServiceNow AI Platform instance à une autre ServiceNow AI Platform .

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Cette fonctionnalité permet à l'administrateur de sécurité de copier des profils qui ont été testés et vérifiés sur une ServiceNow AI Platform instance, par exemple en non-production, vers une autre ServiceNow AI Platform instance, par exemple en production, sans avoir besoin

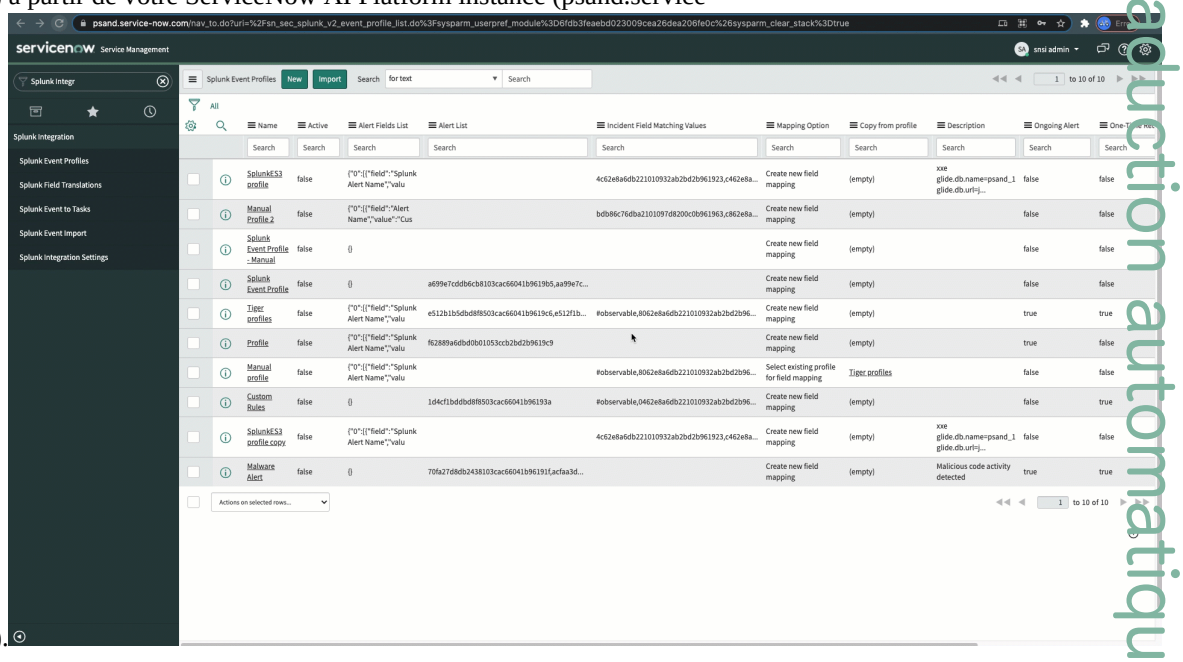
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de refaire tous les paramètres de configuration. Les paramètres exportés et importés incluent le nom de profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les exemples de données extraites, la planification et les informations sur la source des vignettes de configuration.

Remarque : Lorsque vous exportez un type de profil de transfert d'événements manuel, les données de pièce jointe utilisées pour le mappage des champs d'exemple sont copiées, mais le fichier de pièce jointe lui-même n'est pas exporté.

Procédure

1. Accédez à la **Tous** > **Intégration Splunk** > **Profils d'événement Splunk**.
2. Sélectionnez un profil que vous souhaitez exporter vers une autre ServiceNow AI Platform instance. Vous pouvez sélectionner plusieurs profils pour l'exportation.
3. Dans le menu Actions, cliquez sur **Exporter**.
4. Une fois que le message d'exportation terminée s'affiche, cliquez sur **Télécharger**. L'illustration suivante montre l'exportation d'un Splunk profil (profil manuel 2) à partir de votre ServiceNow AI Platform instance (psand.service-now.com).



Le fichier payload.xml exporté est téléchargé sur votre ordinateur. Le fichier contient le nom du profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les exemples de données extraits, la planification et les informations sur la source des vignettes de configuration. Lorsque vous sélectionnez et téléchargez plusieurs profils, ils apparaissent dans le même fichier payload.xml.

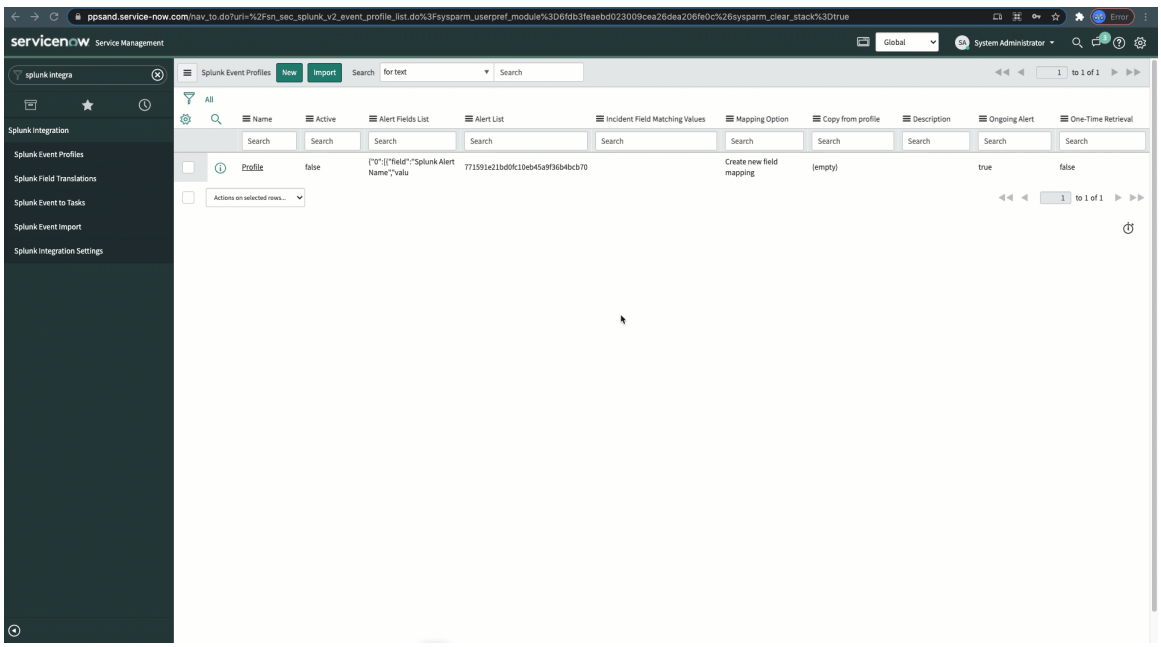
Vous pouvez maintenant procéder à l'importation du profil dans une autre ServiceNow AI Platform instance.

5. Accédez à la **Intégration Splunk** > **Profils d'événement Splunk**.
6. Cliquez sur **Importer**.
7. Cliquez sur **Choisir un fichier** et sélectionnez le fichier XML sur votre ordinateur.
8. Cliquez sur **Charger**.
9. Cliquez sur **Fermer et recharger les profils**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’illustration suivante montre l’importation d’un Splunk profil (profil manuel 2) de l’instance ServiceNow AI Platform (psand.service-now.com) vers une autre ServiceNow AI Platform instance (ppsand.service-now.com).



Vous avez importé le profil avec succès à partir d’une autre ServiceNow AI Platform instance.

Vérifiez que les paramètres de configuration de la source exportée (Splunk compte API et Splunk URL du serveur) et du serveur MID sont valides et disponibles dans l’instance importée ServiceNow AI Platform . Mettez à jour votre Splunk Enterprise Event Ingestion configuration si nécessaire.

10. **Facultatif :** Vérifiez les paramètres du serveur MID après l’importation d’un profil.
11. **Facultatif :** Accédez à la **Security Operations** > **Configurations d'intégration**.
12. **Facultatif :** Sélectionnez la vignette de Splunk Enterprise Event Ingestion configuration, puis cliquez sur **Mettre à jour**.
13. **Facultatif :** Examinez et mettez à jour les détails de la source et du serveur MID selon vos besoins.

Copier un profil d’événement pour l’intégration Splunk Enterprise Event Ingestion

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d’un profil existant, vous préférerez peut-être copier les profils d’alarme pour gagner du temps.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

La copie d’un profil existant et de ses paramètres associés est facultative.

Si vous copiez un profil, le nom du profil est initialement modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) et n’est donc pas activé

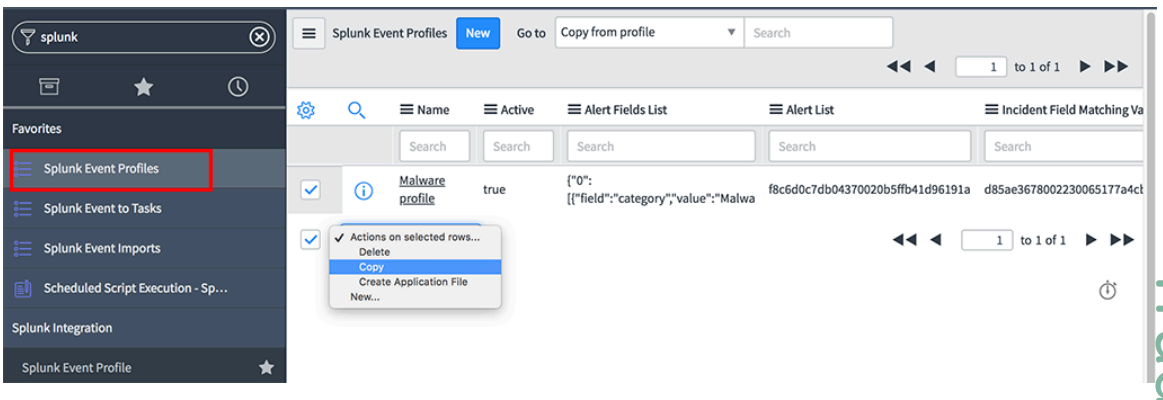
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

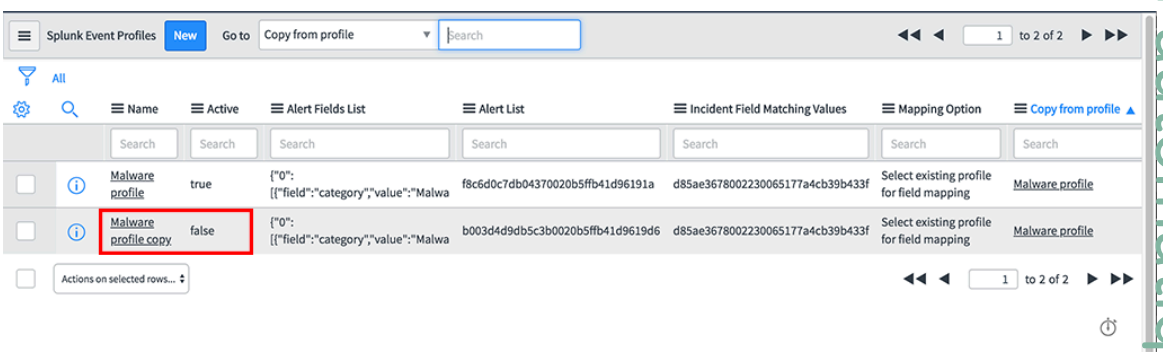
accidentellement avant de terminer la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

1. Accédez à la **Tous** > **Intégration Splunk** > **Profil d'événement Splunk**.
2. Dans la liste Profils d'événements Splunk qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.



Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (vrai), la copie est désactivée à ce stade (faux). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil.

Que faire ensuite

Vous êtes invité à activer le nouveau profil une fois que vous avez terminé les étapes de configuration.

Configurer votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise

Si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise console pour cette intégration, installez et configurez le module complémentaire Security Operations Event Ingestion pour l'application ServiceNow dans Splunk Enterprise votre console d'entreprise ou votre Splunk instance Splunk Cloud.

Avant de commencer

Vérifiez que vous avez installé l'application pour cette intégration avant ServiceNow Store d'installer le module d'extension du module d'extension à partir de splunkbase requis pour l'ingestion manuelle d'événements. Si vous n'avez pas installé l'application pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'intégration à partir de , ServiceNow Store consultez Installez et configurez l'application ServiceNow pour l'intégration Splunk Enterprise Event Ingestion et suivez les instructions pour l'installer.

Rôle requis : ServiceNow AI Platform administrateur (admin)

Pourquoi et quand exécuter cette tâche

L'installation et la configuration du ServiceNow module complémentaire d'ingestion d'événements Security Operations sont facultatives.

Si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise console pour l'intégration, téléchargez, installez et configurez le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise from splunkbase dans votre Splunk Enterprise console.

Ce ServiceNow module complémentaire d'extension est nécessaire pour que des incidents de sécurité puissent être créés à partir d'événements exportés manuellement dans votre ServiceNow AI Platform instance. Ce ServiceNow module complémentaire d'ingestion d'événements Security Operations pour Splunk Enterprise l'application est disponible sur splunkbase .

Pour le transfert manuel d'événements, vous pouvez identifier jusqu'à deux points de terminaison différents ServiceNow AI Platform (instances) dans votre Splunk Enterprise console. Vous transférez manuellement les événements au ou aux points de terminaison pour créer des incidents de sécurité. Par exemple, vous pouvez spécifier à la fois une instance intermédiaire (développement) et une instance de production. En spécifiant des instances distinctes et en nommant les workflows primaire et secondaire pour chaque instance, vous pouvez choisir où vous souhaitez transférer différents événements.

Procédure

1. Si vous n'avez pas encore installé le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise, procédez comme suit pour l'installer et le configurer.

   a. Accédez à splunkbase .

   b. Recherchez le module complémentaire d'ingestion d'événements ServiceNow Opérations de sécurité Security Operations pour Splunk Enterprise.

   > **Remarque :** Vérifiez que vous avez sélectionné ServiceNow Opérations de sécurité le module complémentaire d'ingestion d'événements pour Splunk Enterprise. D'autres ServiceNow modules complémentaires sont affichés dans cette liste. Ces modules complémentaires sont destinés à différentes ServiceNow Splunk intégrations et ne sont pas nécessaires pour cette intégration.

   c. Téléchargez l'application.

   d. Ouvrez votre Splunk Enterprise compte.

   e. Sur la page Applications, cliquez sur l'icône en forme d'engrenage ou sur le raccourci **Gérer les applications** dans la liste déroulante du menu.

   f. En haut à gauche de la page Applications qui s'affiche, cliquez sur **Installer l'application à partir d'un fichier**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

g. Cliquez sur **Choisir un fichier**, sélectionnez ServiceNow le module complémentaire Security Operations Event Ingestion pour Splunk Enterprise, puis cliquez sur **Charger**.

h. Si vous y êtes invité, redémarrez Splunk Enterprise.
Le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise est installé dans votre Splunk Enterprise console d'entreprise. L'étape suivante pour configurer l'addon.

2. Pour configurer l'additif, procédez comme suit.

a. Dans Splunk Enterprise, cliquez **sur l'icône** en forme d'engrenage Applications ou **sur Gérer les applications** dans la liste déroulante du menu.

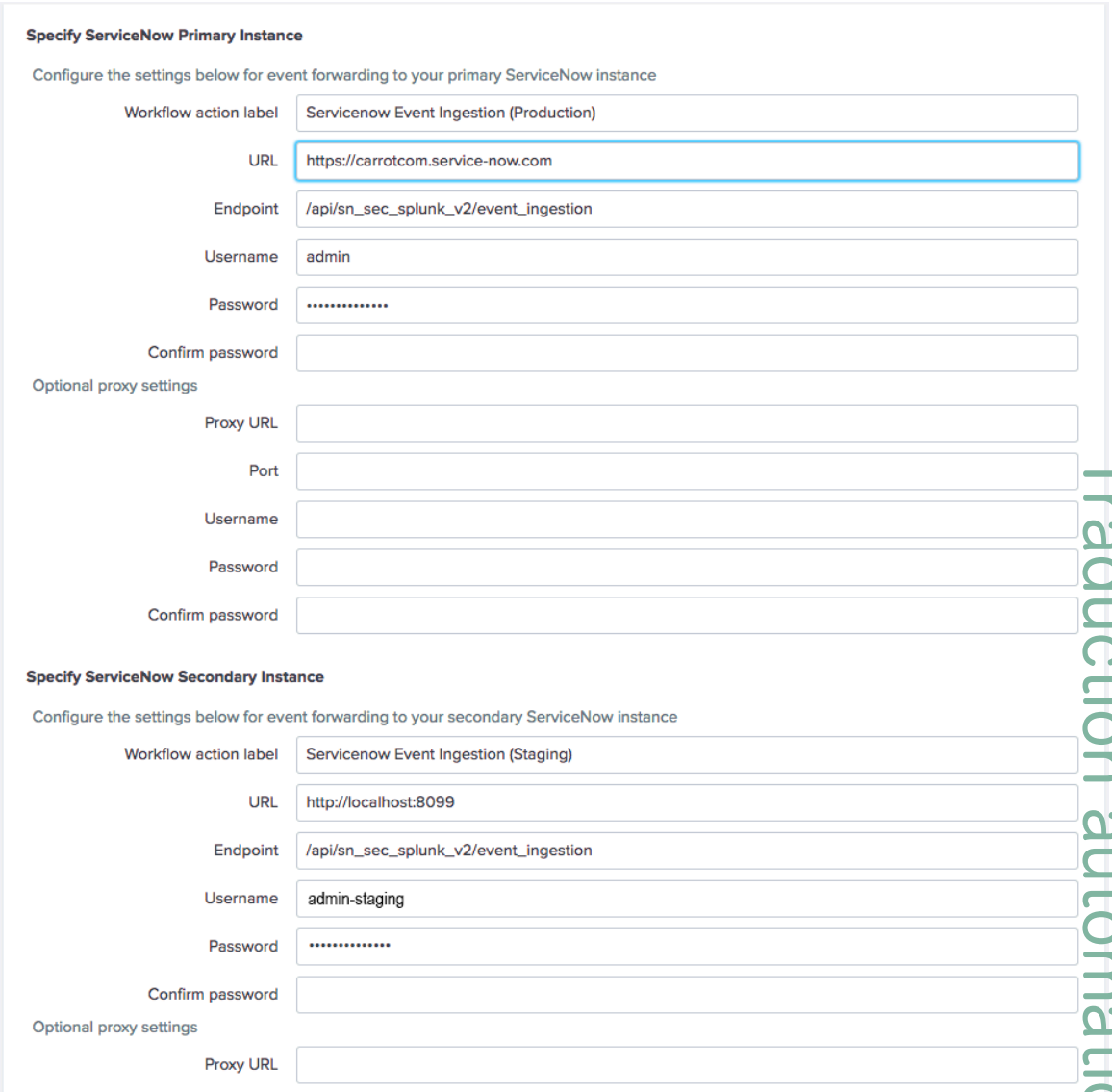
b. Dans la liste des applications qui s'affiche, dans la colonne **Actions** , cliquez sur **Configurer le module complémentaire d'ingestion d'événements**ServiceNow Opérations de sécurité pour Splunk Enterprise.

c. Remplissez le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La figure suivante est un exemple de formulaire rempli dans votre Splunk Enterprise console.



Champ de la section Spécifier l'instance primaire ServiceNow	Description
Étiquette de l'action du workflow	Nom du workflow de ServiceNow AI Platform votre instance de production (principale). Ce nom est le nom d'une ServiceNow AI Platform instance que les utilisateurs qui surveillent Splunk les événements identifient comme instance primaire, par exemple, ServiceNow Ingestion d'événements (Production). La valeur par défaut pour ce champ est In–gestion d'événements ServiceNow (pro–duction). Dans votre Splunk Enterprise console, ce nom de workflow s'affiche pour l'instance de production (primaire) dans la liste dérou–lante Actions d'événement développée d'une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ de la section Spécifier l'instance primaire ServiceNow	Description
	recherche. Ce nom est le nom de votre instance de production. Vous pouvez modifier le nom.
URL	URL de l'instance ServiceNow AI Platform que vous avez saisie dans le champ d'étiquette Action du workflow précédent. Copiez l'URL dans votre navigateur et collez-la dans ce champ du formulaire.
Point de terminaison	Chemin de l'API de base. Pour plus d'informations, reportez-vous à la figure qui suit le tableau. Si vous n'avez pas de valeur pour le point de terminaison de votre ServiceNow AI Platform instance de production, procédez comme suit. **a.** Connectez-vous à votre ServiceNow AI Platform instance de production en tant qu'utilisateur avec le rôle d'administrateur système (admin). **b.** Entrez les API REST basées sur un script dans le panneau de navigation. **c.** Une fois le panneau de navigation actualisé, sélectionnez le module **API REST scriptées** qui s'affiche. **d.** Si l'ingestion d'événements n'est pas répertoriée dans la colonne Nom de la liste des API REST scriptées qui s'affiche, saisissez Ingestion d'événements dans le champ de recherche en haut. **e.** Dans la colonne Chemin de l'API de base de la page actualisée, copiez cette valeur et collez-la dans le champ Point de terminaison du formulaire. Un exemple de chemin d'accès de l'API de base est /api/sn_sec_splunk_v2/event_ingestion.
Nom d'utilisateur	Nom d'utilisateur de votre ServiceNow AI Platform instance. Ce nom est le nom d'utilisateur de l'instance ServiceNow AI Platform dans laquelle vous avez affecté un utilisateur avec le rôle (sn_sec_splunk_v2.api_account_access) pour le transfert manuel d'événements. Pour plus d'informations sur l'affectation de ce rôle, reportez-vous à la section Configurer votre ServiceNow AI Platform instance pour l'intégration Splunk Enterprise Event Ingestion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

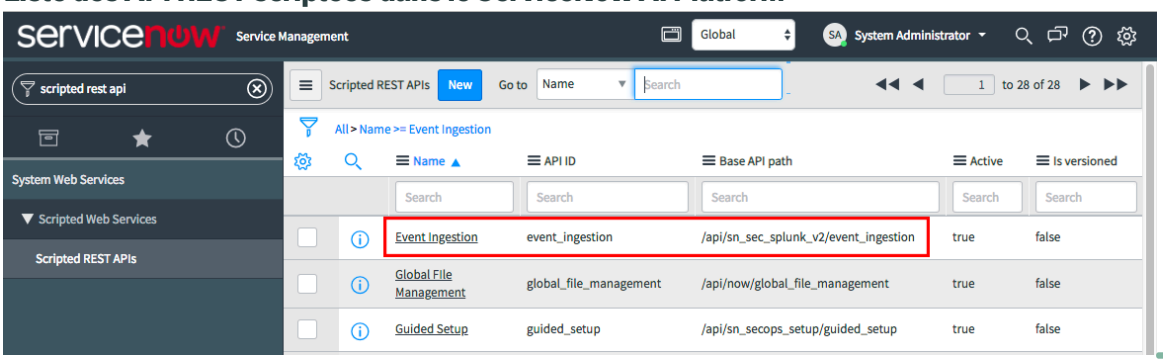
Champ de la section Spécifier l'instance primaire ServiceNow	Description
Mot de passe	Mot de passe de votre ServiceNow AI Platform instance. Ce mot de passe est le mot de passe de l'instance ServiceNow AI Platform dans laquelle vous avez affecté à un utilisateur le rôle (sn_sec_splunk_v2.api_account_access) pour le transfert manuel d'événements.
(Facultatif) Champs de la section Spécifier l'instance secondaire ServiceNow	Description Ces champs sont facultatifs. Vous n'êtes pas obligé de spécifier une instance secondaire.
Étiquette de l'action du workflow	Nom du workflow de ServiceNow AI Platform votre instance secondaire (intermédiaire). Ce nom est le nom d'une ServiceNow AI Platform instance que vos utilisateurs qui surveillent Splunk les événements identifient comme une instance secondaire, par exemple, ServiceNow Ingestion d'événements (Intermédiaire). Dans votre Splunk Enterprise console, ce nom de workflow est affiché pour l'instance intermédiaire (secondaire) dans la liste déroulante Actions d'événement développée d'une recherche. Cette ServiceNow AI Platform instance est votre instance intermédiaire. Vous pouvez modifier le nom.
URL	URL de l'instance ServiceNow AI Platform que vous avez saisie dans le champ Étiquette Action du workflow précédent pour l'instance secondaire ServiceNow AI Platform . Copiez l'URL dans votre navigateur et collez-la dans ce champ du formulaire.
Point de terminaison	Chemin de l'API de base. Cette valeur du chemin de l'API de base de votre instance secondaire est la même que celle du chemin de l'API de base de votre instance principale. Voir la figure précédente du formulaire pour plus d'informations.
Nom d'utilisateur	Nom d'utilisateur de votre ServiceNow AI Platform instance intermédiaire. L'utilisateur doit avoir le rôle (sn_sec_splunk_v2.api_account_access).
Mot de passe	Mot de passe de votre ServiceNow AI Platform instance intermédiaire. L'utilisateur doit avoir le rôle (sn_sec_splunk_v2.api_account_access).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La figure suivante est un exemple de la liste API REST scriptées dans votre ServiceNow AI Platform. La liste affiche l'emplacement de la valeur de point de terminaison d'une ServiceNow AI Platform instance que vous saisissez dans le formulaire dans le cadre de la configuration ServiceNow du module complémentaire Security Operations Event Ingestion for extension dans Splunk Enterprise votre Splunk Enterprise console.

Liste des API REST scriptées dans le ServiceNow AI Platform



3. Dans le formulaire de configuration de votre Splunk Enterprise console, cliquez sur **Enregistrer** pour enregistrer vos modifications.

   Après quelques instants, en haut à gauche du formulaire de votre Splunk Enterprise console, un message s'affiche indiquant que l'enregistrement a été mis à jour avec succès.

   Une fois le formulaire enregistré, les noms (étiquettes d'action de workflow) de vos ServiceNow AI Platform instances que vous avez créées dans le formulaire sont disponibles dans la liste de choix Actions d'événement sur un événement sélectionné d'une recherche dans votre Splunk Enterprise console.

Que faire ensuite

Si vous n'avez pas encore enregistré les recherches dans votre Splunk Enterprise console, l'étape suivante consiste à enregistrer les recherches sous forme d'alertes dans votre Splunk Enterprise console.

Enregistrer les recherches pour l'intégration dans votre Splunk EnterpriseSplunk Enterprise Event Ingestion console

Les étapes suivantes pour enregistrer les recherches dans votre Splunk Enterprise console sont fournies à un utilisateur disposant du Splunk Enterprise rôle administrateur.

Avant de commencer

Si vous avez déjà des recherches enregistrées et des alertes déclenchées dans votre Splunk Enterprise console, vous n'êtes pas obligé de modifier ces recherches pour cette intégration.

L'intégration du produit au Splunk service de notification d'événement extrait les informations sur les ServiceNow AI Platform® Opérations de sécurité événements et les alertes à partir de Splunk.

Avant d'ingérer des alertes dans votre Opérations de sécurité environnement, configurez les recherches dans votre Splunk Enterprise console afin d'extraire automatiquement les événements de sécurité pertinents que Splunk Enterprise vous souhaitez enregistrer en tant qu'alertes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous n’avez pas établi de recherches enregistrées et d’alertes déclenchées pour notification lorsque des événements de sécurité importants se produisent dans votre Splunk Enterprise console, procédez comme suit pour enregistrer les recherches.

Rôle requis : Splunk Enterprise administrateur

Procédure

1. Connectez-vous à votre compte Splunk Enterprise.
2. Cliquez sur l’onglet **Rechercher** .
3. Dans le champ Nouvelle recherche qui s’affiche, saisissez une valeur pour l’alerte, par exemple Programme malveillant.
4. Pour afficher les événements associés à votre recherche, cliquez sur l’icône de recherche ou appuyez sur Entrée à droite du champ Nouvelle recherche.
   Les résultats de la recherche avec les événements s’affichent.
5. Pour enregistrer la recherche sous forme d’alerte, dans le coin supérieur droit de la page, développez la liste de choix Enregistrer sous, puis sélectionnez **Alerte**.
6. Renseignez les champs du formulaire qui s’affiche.

Champ	Description
Titre	Nom descriptif de l’alerte, par exemple Événements de programme malveillant. Une fois cette recherche enregistrée en tant qu’alerte, les événements d’une alerte déclenchée dans le Splunk service sont automatiquement traités en alertes déclenchées à l’aide de ces données de recherche. Le titre de l’alerte déclenchée est utilisé dans le profil d’événement que vous créez dans votre ServiceNow AI Platform instance afin d’identifier les événements qui sont ingérés dans votre instance pour ServiceNow AI Platform® Réponse aux incidents de sécurité SIR la création d’un incident de sécurité.
(Facultatif) Description	Texte pour vous aider à distinguer cette alerte des autres alertes.
Type d'alerte	Dans les champs qui s’affichent, sélectionnez **Planifié** pour rechercher cette alerte selon une planification ou **En temps réel** pour rechercher cette alerte en continu.
Résultats du déclencheur	Vous préférez peut-être définir l’une des conditions de filtre suivantes : ○ Le nombre de résultats est supérieur ou inférieur à ○ Unique (une fois) pour chaque résultat
Actions de déclencheurs	Ajoutez des actions pour déclencher cette alerte. Développez la liste de choix Ajouter et cliquez sur **Ajouter aux alertes déclenchées** afin qu’il s’affiche sur le formulaire. Vous préférerez peut-être ce paramètre pour les alertes que vous ingérez dans votre ServiceNow AI Platform instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Enregistrer**.
   Votre alerte est enregistrée et s'affiche sous l'onglet Alertes de la page de recherche.
   Le Splunk service extrait les événements en faisant correspondre les critères que vous avez configurés dans l'alerte. Il met en cache les événements, et vous les demandez ensuite à partir de vos profils que vous configurez dans votre ServiceNow AI Platform instance. Étant donné que l'extraction d'ingestion des événements se produit à partir d'un cache dans le service, cette ingestion à partir de Ur ServiceNow AI Platform n'a pas d'impact sur les Splunk performances de votre Splunk plateforme.

Que faire ensuite

Vous avez terminé avec succès la configuration requise pour l'intégration dans votre Splunk Enterprise console. Si vous n'avez pas encore installé l'application pour l'intégration à partir de , ServiceNow Store l'étape suivante consiste à installer l'application pour l'intégration et à la configurer.

Utiliser l'éditeur de script pour formater les valeurs d'alerte pour l'intégration Splunk Enterprise Event Ingestion

Utilisez l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage.

Avant de commencer

Outre les champs directement mappés à partir des valeurs d'alerte extraites et les valeurs d'alerte que vous saisissez manuellement, vous pouvez éventuellement utiliser l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. L'éditeur de script modifie les valeurs d'une Splunk alerte afin que les valeurs prises en charge par l'incident ServiceNow AI Platform® Réponse aux incidents de sécurité de sécurité soient mappées aux champs Catégorie, Élément de configuration (CI) et Observable.

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

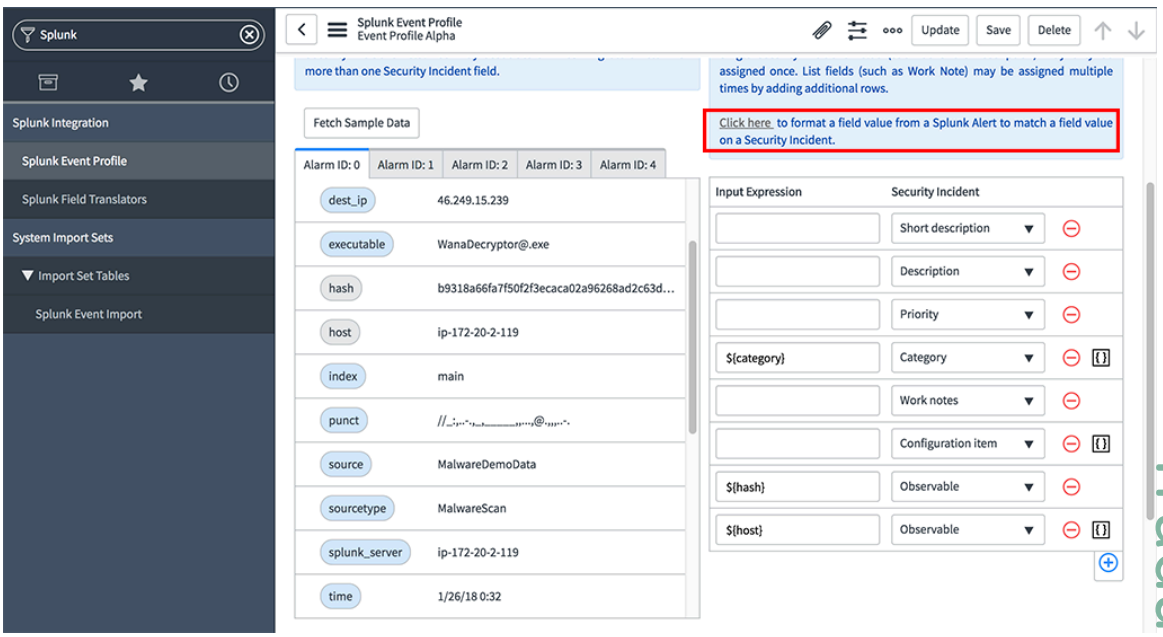
Dans certains cas, Splunk Enterprise les valeurs d'alerte sont mappées aux champs Catégorie, Élément de configuration (CI) et Observable de l'incident SIR et ne sont pas prises en charge. Vous préférez peut-être modifier les valeurs mappées. Si vous souhaitez convertir la valeur d'une Splunk Enterprise alerte en une valeur prise en charge par ces champs sur l'incident SIR de sécurité, utilisez l'éditeur de script.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Une fois le formulaire de mappage affiché, cliquez sur le lien pour ouvrir l'éditeur de script.

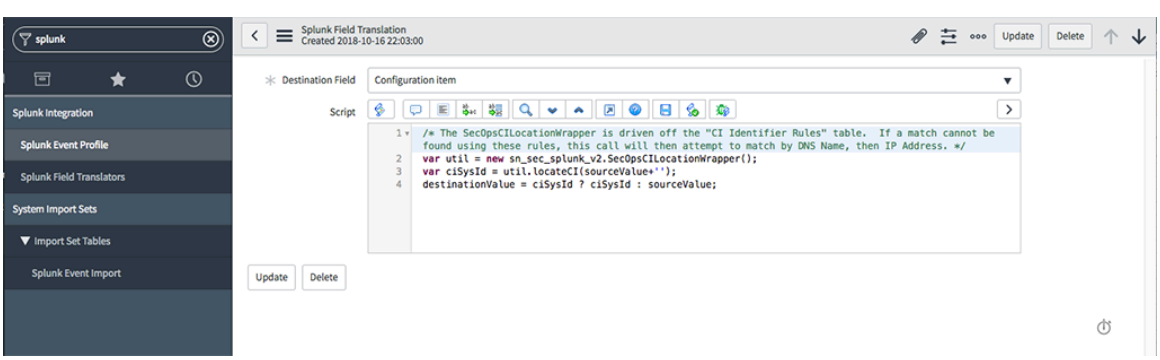


2. Dans la liste de choix, sélectionnez un champ de destination pour la valeur que vous souhaitez modifier.
3. Sinon, dans la section Mappage du champ d'incidents SIR, cliquez sur l'icône de crochet [{}] en regard d'un champ pour ouvrir l'éditeur de script pour ce champ.

   Dans certains cas, un include de script peut être approprié pour le champ Élément de configuration. Pour une alerte, par exemple, une valeur de l'élément de configuration peut ne pas être mise en correspondance.

   Comme le montre la figure suivante, si une correspondance pour un nom d'hôte est introuvable dans le ServiceNow AI Platform® CMBD pour le champ Élément de configuration, vous pouvez modifier la règle de sorte que si une adresse IP est trouvée, elle remplit le champ Élément de configuration. Si aucune valeur n'est spécifiée pour l'alarme, le champ de l'incident de sécurité est défini sur Null.

   L'éditeur s'ouvre avec le champ affiché dans Champ de destination. L'image suivante montre l'éditeur avec le champ Élément de configuration comme champ de destination.



4. Entrez les modifications apportées au script et cliquez sur **Mettre à jour** pour enregistrer vos modifications. La Splunk table Traductions de champ s'affiche.
5. Fermez la table pour revenir au formulaire de mappage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification pour l'intégration Splunk Enterprise Event Ingestion

Utilisez cette liste de vérification pour vous guider à travers toutes les tâches de l'intégration. La liste de vérification suivante comprend des tâches de configuration et d'installation ainsi que des exemples de cas d'utilisation qui incluent les résultats attendus pour l'intégration.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Suivez votre progression avec l'installation, l'installation et la configuration de l'intégration avec la table suivante. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante. Chaque ligne de la table répertorie les tâches et identifie les rôles requis pour effectuer les tâches. Les rubriques numérotées du guide d'installation et de configuration sont également référencées.

Rôles requis : les rôles sont répertoriés pour chaque étape ci-dessous.

Procédure

1. En tant qu'utilisateur disposant du rôle d'administrateur ServiceNow AI Platform , configurez votre ServiceNow AI Platform instance.
   - Affectez aux utilisateurs les rôles **sn_si.ingestion_profile_admin** (ou sn_si.admin) et sn_si.analyst selon les besoins.
   - Installez et configurez un serveur MID si le Splunk serveur est déployé dans votre réseau d'entreprise.
   - Vérifiez que les modules d'extension ServiceNow Réponse aux incidents de sécurité sont activés pour votre version du ServiceNow AI Platform.
   - Si vous souhaitez transférer manuellement des événements de votre Splunk Enterprise console vers votre ServiceNow AI Platform instance, vérifiez que vous avez affecté le rôle (sn_sec_splunk_v2.api_account_access) à un utilisateur disposant de l'autorisation d'administrateur Splunk Enterprise d'entreprise.

   Pour plus d'informations, consultez Configurer votre ServiceNow AI Platform instance pour l'intégration Splunk Enterprise Event Ingestion.

   Vous avez terminé avec succès les étapes de configuration et vérifié les résultats attendus pour l'intégration.
2. En tant qu'utilisateur disposant du ServiceNow AI Platform rôle administrateur, installez et configurez l'application Splunk Enterprise Event Ingestion à partir du ServiceNow Store.
   a. Téléchargez et installez l'application sur votre ServiceNow AI Platform instance.
   b. Configurez l'application et connectez-vous à votre Splunk Enterprise console.

   Pour plus d'informations, consultez Installez et configurez l'application ServiceNow pour l'intégration Splunk Enterprise Event Ingestion.
3. **Facultatif :** Si vous avez l'intention d'exporter des événements manuellement de votre Splunk Enterprise console vers votre ServiceNow AI Platform instance, effectuez les tâches suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. En tant qu'administrateur Splunk Enterprise , installez, configurez et activez le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise à partir de splunkbase dans votre Splunk Enterprise console.

b. En tant qu'administrateur Splunk Enterprise , si ce n'est pas déjà fait, enregistrez les recherches en tant qu'alertes dans votre Splunk Enterprise console.

(Optional) Pour plus d'informations, consultez Configurer votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise et Enregistrer les recherches pour l'intégration dans votre Splunk EnterpriseSplunk Enterprise Event Ingestion console.

4. En tant qu'utilisateur disposant du rôle ServiceNow AI Platform **sn_si.ingestion_profile_admin** , créez et nommez un profil d'événement.

Sélectionnez le type de profil dans la liste de choix. Les options sont un profil d'alerte planifiée que vous utilisez pour ingérer des exemples de données ou un profil d'événement que vous utilisez pour exporter manuellement des données de pièce jointe à partir de votre Splunk Enterprise console.

- Pour une alerte planifiée, sélectionnez une alerte disponible.
- Pour le profil des données exportées manuellement, créez une nouvelle carte ou copiez une carte existante.

Pour plus d'informations, consultez Créer et nommer un profil d'événement.

5. En tant qu'utilisateur disposant du rôle ServiceNow AI Platform **sn_si.ingestion_profile_admin**, mappez les valeurs ingérées ou les données de pièce jointe exportées depuis vers ServiceNow AI Platform les incidents de Splunk Enterprise sécurité.

a. Extrayez un exemple de données pour une alerte planifiée.

b. Exporter les données de la pièce jointe manuellement à partir d'un Splunk Enterprise événement.

c. Modifiez la configuration de mappage par défaut.

d. Vous pouvez éventuellement ajouter des critères de filtrage, ajouter une alerte à un incident de sécurité existant et utiliser l'éditeur de script.

Pour plus d'informations, consultez Mappage des alertes et des événements pour l'intégration Splunk Enterprise Event Ingestion et Mapper les alertes pour l'intégration Splunk Enterprise Event Ingestion.

6. En tant qu'utilisateur disposant du rôle ServiceNow AI Platform **sn_si.ingestion_profile_admin** , prévisualisez les données Splunk Enterprise affichées sur un ServiceNow AI Platform incident de sécurité.

Corrigez les erreurs ou ajoutez les données manquantes afin qu'aucun message d'erreur ne s'affiche.

Pour plus d'informations, consultez Prévisualiser l'incident de sécurité pour l'intégration Splunk Enterprise Event Ingestion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. En tant qu'utilisateur disposant du rôle ServiceNow AI Platform **sn_si.ingestion_profile_admin** , planifiez la récupération d'alerte pour un profil avec une alerte planifiée.

   Pour plus d'informations, consultez Planifier et récupérer les alertes pour l'intégration Splunk Enterprise Event Ingestion.

Splunk Enterprise Security Intégration de l'ingestion d'événements

L'intégration Splunk Enterprise Security de l'ingestion Réponse aux incidents de sécurité d'événements notables au produit (SIR) permet aux analystes d'incidents de sécurité de collecter et de traiter les données d'événements notables (appelés notables).

Vue d'ensemble de l'intégration de l'ingestion d'événements Splunk Enterprise Security

Les données sont ingérées en permanence en fonction d'un calendrier d'interrogation configuré et sont utilisées par les analystes pour identifier les cybermenaces potentielles et y répondre. Les événements de sécurité collectés peuvent être corrélés en événements Splunk Enterprise Security notables, puis ingérés automatiquement avec cette intégration. En outre, des événements notables individuels peuvent être transférés manuellement à la demande depuis la console Incident Review et l'interface Splunk Enterprise Security de génération de rapports vers le Réponse aux incidents de sécurité produit pour créer des incidents de ServiceNow AI Platform sécurité.

Cette intégration fournit à un analyste du centre des opérations de sécurité (SOC) une visibilité sur les événements notables et les données d'événement de contribution connexes. Ces données peuvent être intégrées dans ServiceNow AI Platform Réponse aux incidents de sécuritéSIR des incidents de sécurité pour une enquête plus approfondie et une correction. Des profils sont créés dans votre ServiceNow AI Platform instance pour gérer différents types d'événements notables créés via des recherches de corrélation dans Splunk Enterprise Security. Ces profils personnalisent la façon dont les différents Splunk champs d'événement sont affichés sur SIR les incidents de sécurité.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

- Créez plusieurs profils d'ingestion d'événements notables pour créer des incidents de sécurité SIR pour des types spécifiques de menaces tels que le hameçonnage, les programmes malveillants et les tentatives d'accès non autorisé.
- Créez plusieurs profils d'événements pour le transfert d'événements sur demande à partir de votre Splunk ES console d'examen d'incident afin de créer des incidents de sécurité SIR.
- Glisser-déposer le mappage des valeurs de champs d'événements Splunk notables vers les champs d'incident de sécurité SIR associés.
- Aperçu de la mise en page de l'incident de sécurité basé sur un SIR échantillon d'événements notables pour valider les détails du mappage d'événements.
- Ingérez les événements notables historiques, ainsi que les événements notables en cours, nouveaux et mis à jour à intervalles configurables.
- Filtrez les événements notables qui ne répondent pas aux critères de génération d'incidents SIR, par exemple, les événements de priorité faible, les événements qui n'ont pas encore atteint un état spécifique, et ainsi de suite.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Regroupez les événements ou les alertes aux incidents de sécurité existants en fonction des valeurs de champ correspondantes SIR pour éviter les incidents de sécurité en double.
- Mettez à jour les événements notables en fonction des conditions de création et/ou de fermeture d'incidents SIR via une interface bidirectionnelle pour que les mises à jour des événements notables soient Splunk ES synchronisées avec le statut de l'incident ServiceNow SIR.

Versions prises en charge ServiceNow AI Platform

Le module d'extension com.snc.si_dep est requis pour cette intégration. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications.

Les applications suivantes Opérations de sécurité doivent être installées et activées à partir du ServiceNow Store. Installez, puis activez une application à la fois dans l'ordre indiqué ci-dessous pour assurer une installation fluide :

1. Cadre de travail d'intégration de sécurité
2. Security Support Common
3. Security Incident Response

Pour plus d'informations sur l'installation Opérations de sécurité des applications principales, reportez-vous aux sections Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

ServiceNow Compléments

Le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk ES n'est requis que si vous préférez transférer les événements manuellement de votre Splunk Enterprise Security console Incident Review vers votre ServiceNow AI Platform instance. Cet ServiceNow addon est disponible dans splunkbase .

Ce ServiceNow module complémentaire d'ingestion d'événements Security Operations pour Splunk Enterprise l'application dans splunkbase n'est pas requis pour l'ingestion d'alerte automatisée prise en charge par l'intégration.

Versions prises en charge par Splunk

Cette intégration a été testée avec Splunk Enterprise la version 8.0.1 et avec Splunk Enterprise Security la version 6.2.1 de l'application.

Serveur MID

Cette intégration nécessite l'installation et la configuration d'un Splunk serveur MID dans votre ServiceNow AI Platform® instance pour se connecter au service lorsque le Splunk serveur est déployé au sein de votre réseau d'entreprise. Si vous utilisez le service, un serveur MID n'est Splunk Cloud pas nécessaire. Voir Serveur MID pour plus d'informations sur les serveurs MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Références

Référence	Identificateur de document	Titre de document
1	Splunk Site Web du produit	Site web du produit Splunk Enterprise Security .

Liste de vérification

Pour obtenir une liste de contrôle imprimable de ces rubriques, reportez-vous à la section Liste de vérification pour Splunk Enterprise Security l'intégration de l'ingestion d'événements notables. Vous pouvez utiliser cette liste pour suivre votre progression au fur et à mesure que vous exécutez les tâches de l'intégration.

Termes clés utilisés dans cette intégration

Cette section décrit certains des termes clés utilisés dans cette intégration.

Les termes clés suivants sont utilisés lors de l'installation et de la configuration. Pour plus d'informations sur ces termes, consultez le site Web de la documentation produit ServiceNow et le site Web et les ressources de Splunk sur la page Ressources Splunk .

ServiceNow AI Platform

Un produit d'entreprise ServiceNow . Il ServiceNow AI Platform s'agit de la base sur laquelle reposent les composants individuels tels que Réponse aux incidents de sécurité (SIR), IT Service Management (ITSM) et d'autres produits.

ServiceNow Module complémentaire Splunkbase

Une ServiceNow application installée sur votre Splunk Enterprise Security console qui prend en charge l'option de transfert manuel d'événements de l'intégration. Le transfert manuel d'événements est une fonctionnalité facultative de l'intégration. Ce ServiceNow module complémentaire Splunkbase n'est pas requis pour l'ingestion d'événements notables automatisée fournie par l'intégration qui extrait les événements de .Splunk

Réponse aux incidents de sécurité (SIR)

Une ServiceNow AI Platform application qui suit la progression des incidents de sécurité depuis la découverte et l'analyse initiale, en passant par le confinement, l'éradication et la récupération, jusqu'à la revue et la fermeture finales post-incident.

Splunk Enterprise Security

Splunk Enterprise Security aide les équipes à bénéficier d'une visibilité et d'informations de sécurité à l'échelle de l'organisation pour une surveillance continue, la réponse aux incidents, les opérations SOC et fournir aux dirigeants une fenêtre sur les risques métier. Splunk Enterprise Security est une solution de sécurité premium nécessitant une licence payante. Ce service se trouve sur un hôte ou une offre cloud Splunk appelée Splunk console dans ce guide.

Splunk Enterprise Security Événement notable

Lorsqu'une recherche de corrélation identifie un événement ou un modèle d'événements, elle crée un événement notable. Les recherches de corrélation filtrent les données de sécurité et mettent en corrélation les événements pour identifier un type particulier d'incident (ou modèle d'événements), puis créer des événements notables.

Splunk événement

Un ou plusieurs éléments de données qui entraînent les événements notables du Splunk service. Dans votre ServiceNow AI Platform instance, vous pouvez rechercher quels Splunk événements ont déclenché ServiceNow AI Platform des incidents de sécurité.

Serveur MID

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette application facilite la communication et le mouvement de données entre les applications, les sources de données et les ServiceNow AI Platform services externes. Cette application est généralement requise pour l'intégration avec les technologies sur site. Pour cette Splunk Enterprise Security intégration d'ingestion d'événements, le Serveur MID facilite la communication entre l'instance ServiceNow AI Platform et l'instance sur site de Splunk Enterprise Security. Un serveur MID n'est pas nécessaire si vous intégrez votre ServiceNow AI Platform instance à une Splunk Cloud instance.

Administrateur d'incidents de sécurité (sn_si.admin)

L'utilisateur disposant de ce rôle supervise la configuration de l'intégration avec le SIR produit dans votre ServiceNow AI Platform instance.

Analyste des incidents de sécurité (sn_si.analyst)

L'utilisateur disposant de ce rôle interagit avec les incidents de sécurité du ServiceNow Réponse aux incidents de sécurité produit et les analyse.

Configurer votre ServiceNow AI Platform® instance pour l'intégration Splunk Enterprise Security

La section suivante répertorie les tâches de configuration que vous devez effectuer dans votre ServiceNow AI Platform® instance avant d'installer l'application à partir du ServiceNow Store.

Rôle requis : sn_si.ingestion_profile_admin.

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Reportez-vous au tableau suivant et vérifiez que vous avez effectué toutes les tâches répertoriées avant de télécharger et d'installer l'application afin de garantir une installation et une configuration fluides.

1. Vérifiez que vous avez affecté les rôles et (SIR) requis.ServiceNow AI Platform®Réponse aux incidents de sécurité

   Les rôles suivants sont requis pour l'installation, la configuration et l'utilisation de l'intégration dans votre ServiceNow AI Platform® instance.

   - Un utilisateur disposant du rôle d'administrateur ServiceNow AI Platform® (admin) installe l'application à partir de et ServiceNow Store lui affecte le rôle d'administrateur d'incident de sécurité (sn_si.admin).
   - Si vous souhaitez transférer manuellement Splunk Enterprise Security des événements notables pour cette intégration, un utilisateur disposant du ServiceNow AI Platform® rôle administrateur affecte un utilisateur ayant le rôle (sn_sec_splunkes.api_account_access) dans le ServiceNow AI Platform®. Ce rôle permet à un utilisateur ayant le rôle d'administrateur Splunk Enterprise Security d'accéder à l'API dans le qui est requise pour le transfert manuel d'événements ServiceNow AI Platform® pour cette intégration.

     Le rôle (sn_sec_splunkes.api_account_access) n'est pas requis pour l'intégration si vous ingérez automatiquement des Splunk Enterprise Security événements notables depuis votre ServiceNow AI Platform® instance.

   - Un utilisateur disposant du rôle **sn_si.ingestion_profile_admin** supervise les tâches suivantes dans le ServiceNow AI Platform®:

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Nomme, crée et modifie les profils d'événements.
- Sélectionne et mappe les valeurs depuis les ServiceNow AI Platform® incidents de Splunk Enterprise Security sécurité.
- Prévisualise les détails de l'incident de sécurité pour plus d'exactitude avant de finaliser la configuration.
- Planifie l'ingestion d'événements notables en cours.
- Active les mises à jour d'événements notables lorsqu'un incident SIR est créé et fermé.
- Affecte le rôle d'analyste des incidents de sécurité (sn_si.analyst).
- Les utilisateurs disposant du sn_si.analyst travaillent sur des incidents de sécurité.

Pour en savoir plus, reportez-vous à Gestion des rôles .

2. Affectez le rôle d'utilisateur Splunk .

   Affecter un rôle d'utilisateur Analyste de la sécurité (ess_analyst) dans Splunk ES pour effectuer toutes les activités liées à l'intégration sur le Splunk serveur.

3. Vérifiez que vous utilisez la version 7.2.6 ou ultérieure de l'API Splunk . Les versions antérieures ne sont pas prises en charge.

   Si vous avez accès à la Splunk Enterprise Security console, vous avez accès à l'API requise pour cette intégration. Aucune autre configuration spéciale n'est requise pour l'API.

4. Vérifiez que vous avez installé et configuré un Serveur MID.

   A Serveur MID dans votre ServiceNow AI Platform® instance est nécessaire pour se connecter au service si le serveur est déployé au sein de SplunkSplunk votre réseau d'entreprise. (pour en savoir plus, consultez Serveur MID).

   Si vous utilisez le service dans le cloud, un n'est Splunk Enterprise SecurityServeur MID pas obligatoire.

5. Vérifiez que les ServiceNow applications principales nécessaires à la prise en charge de l'intégration sont installées et activées.

   Le Réponse aux incidents de sécurité module d'extension Dependency (com.snc.si_dep) est requis. Ce module d'extension installe automatiquement toutes les dépendances requises pour prendre en charge le Réponse aux incidents de sécurité produit. Installez et activez ce module d'extension avant d'installer et d'activer les autres Opérations de sécurité applications requises par l'intégration.

   Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Security Incident Response

b. Cadre de travail d'intégration de sécurité

c. Structure de support de la sécurité commun

Pour plus d'informations sur l'installation des Opérations de sécurité applications principales, consultez Obtenir une autorisation pour un produit ou une Opérations de sécurité application et Activer une ServiceNow Store application.

Vous avez correctement configuré votre ServiceNow AI Platform® instance pour l'intégration. L'étape suivante consiste à installer l'application d'ingestion d'événements Splunk Enterprise Security notables à partir de pour ServiceNow Store l'intégration. Pour plus d'informations, consultez Installer et configurer Splunk Enterprise Security l'intégration de l'ingestion d'événements notables .

Si vous souhaitez exporter des événements notables manuellement et à la demande à partir de votre Splunk Enterprise Security console pour l'intégration, consultez Configurer votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables pour plus d'informations.

Installer et configurer Splunk Enterprise Security l'intégration de l'ingestion d'événements notables

Avant d'exécuter l'intégration sur votre ServiceNow AI Platform® instance, effectuez ces étapes d'installation et de configuration afin que l'application s'intègre correctement aux Réponse aux incidents de sécurité produits sur Opérations de sécurité votre ServiceNow AI Platform® instance.

Avant de commencer

Rôle requis : ess_analyst

Affectez un rôle d'utilisateur Analyste de la sécurité (ess_analyst) dans Splunk ES pour effectuer toutes les activités liées à l'intégration sur le serveur Splunk.

Procédure

1. Si vous n'avez pas installé l'application d'ingestion d'événements Splunk Enterprise Security à partir de pour ServiceNow Store l'intégration, consultez Installer une Opérations de sécurité intégration et suivez les étapes pour l'installer.
2. Une fois l'application installée, accédez à **Intégrations** > **Configurations des intégrations** et localisez la vignette Ingestions d'événements Splunk .
3. Pour configurer l'application, cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sinon, si un bouton **Configurer** est affiché sur une tuile, cliquez dessus pour modifier une configuration existante.
5. Dans la boîte de dialogue Configuration des ingestions d'événements qui s'affiche, renseignez les champs.

Champ	Description
Nom	Nom de la console ou Splunk Cloud de l'instance Splunk Enterprise Security utilisée pour l'intégration. Les espaces sont pris en charge pour les noms, mais les parenthèses ne sont pas prises en charge. Par exemple, entrez SplunkES2.
URL de Base de l'API Splunk	URL de votre Splunk Enterprise Security console ou Splunk Cloud instance. L'URL doit inclure le port de l'API, par exemple : https://mysplunkserver.com:8089
Authentification de base	Désactivé par défaut. Si vous utilisez le nom d'utilisateur du compte API et le mot de passe de l'API pour la configuration, cochez la case.
Nom d'utilisateur du compte API	Nom d'utilisateur que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise Security console.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mot de passe de l'API	Mot de passe que vous avez créé pour votre compte d'utilisateur d'API sur la Splunk Enterprise Security console.
Basé sur un jeton (disponible à partir de la version 12.0.0)	Jeton que vous avez créé pour votre compte d'utilisateur d'API sur la console Splunk Enterprise Security.
Jeton	Jeton que vous avez créé pour votre compte d'utilisateur d'API sur la console de sécurité d'entreprise Splunk .
Déploiement sur site	Désactivé par défaut. Si vous utilisez une version sur site de Splunk Enterprise Security, vérifiez que cette case est cochée.
Serveur MID	Option permettant de choisir un Serveur MID particulier à configurer dans votre environnement, qui sera utilisé par cette intégration pour extraire des événements notables dans ServiceNow. Vous pouvez sélectionner un serveur MID spécifique dans la liste ou sélectionner **N'importe lequel** pour permettre la sélection automatique d'un serveur MID valide dans la liste pour cette intégration. **Remarque :** ◦ Le serveur MID sélectionné pendant ce temps de configuration s'applique tout au long de cette intégration. ◦ Seuls les serveurs MID actifs et validés sont affichés dans cette liste. Par défaut, la valeur est définie sur **Quelconque**. Par exemple, il existe trois serveurs MID A, B et C. Si vous sélectionnez **N'importe lequel**, l'un de ces MID Servers est sélectionné automatiquement et s'applique à l'ensemble de cette intégration. Si vous sélectionnez un serveur MID spécifique, par exemple C, le serveur MID C sélectionné s'applique tout au long de cette intégration. Si vous souhaitez modifier le Serveur MID, vous devez le reconfigurer à partir de la vignette Configuration de l'application.

La figure suivante est un exemple de formulaire rempli pour la configuration d'une version locale d'avec Splunk Enterprise Security un serveur MID.

Traduction automatique

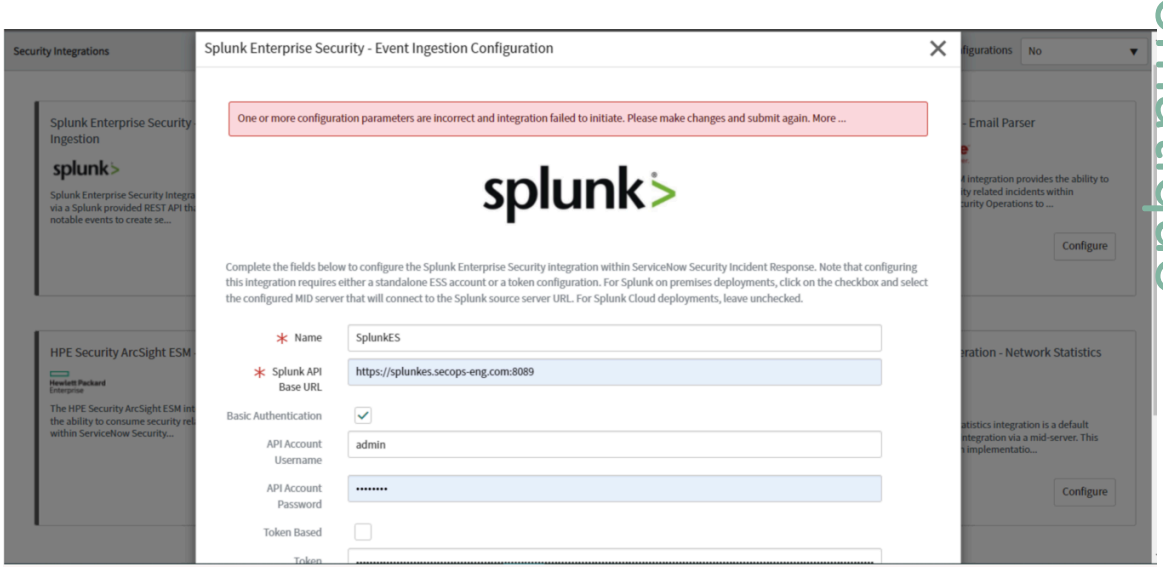
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Chaque Splunk Enterprise Security type d'événement notable que vous ingérez à partir de votre Splunk Enterprise Security console d'examen des incidents nécessite un profil d'événement unique dans votre ServiceNow AI Platform® instance. Toutefois, la source que vous configurez dans le formulaire Configuration des ingestions d'événements peut être réutilisée pour plusieurs ServiceNow AI Platform® profils tant que chaque profil ingère des types d'événements notables uniques.

6. Cliquez sur **Envoyer**.
   Une fois la validation terminée, la page Intégrations de sécurité s'affiche avec chacune de vos configurations. Sur chaque vignette de configuration valide, les boutons **Mettre à jour** et Supprimer s'affichent, comme illustré dans la figure suivante.

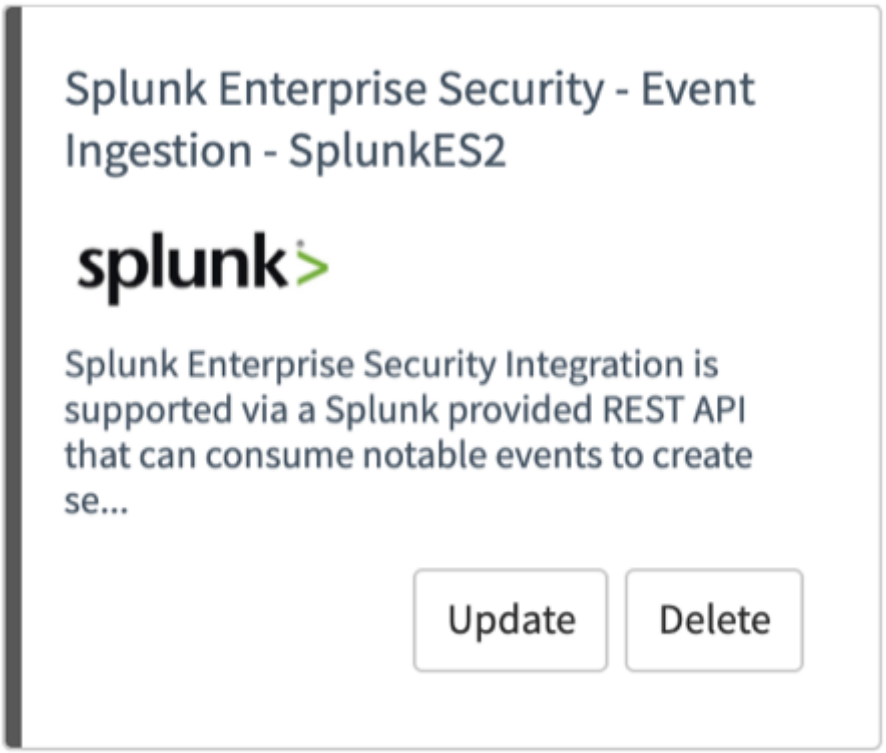
Remarque : Les utilisateurs doivent utiliser soit l'authentification de base, soit l'authentification basée sur les jetons. L'activation des deux générera l'erreur suivante.



Remarque : Si les utilisateurs préfèrent mettre à jour les tuiles de configuration existantes en fonction des jetons, ils doivent activer Activez ce paramètre pour mettre à jour les configurations sources existantes Splunk pour le paramètre de prise en charge de l'authentification basée sur les jetons dans Splunk le module Paramètres d'entreprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois validée et soumise, chaque configuration de serveur d'ingestions d'événements est enregistrée sur la page Intégrations Splunk de sécurité sous forme de tuile. Si vos tuiles de configuration enregistrées ne s'affichent pas sur la page Intégrations de sécurité, dans le coin supérieur droit de la page, dans la liste Afficher les configurations, sélectionnez **Oui**.

Que faire ensuite

Vous avez correctement installé et configuré l'application. L'étape suivante consiste à créer un profil d'événement.

Configurer les Splunk paramètres de sécurité d'entreprise

Utilisez les paramètres de sécurité d'entreprise Splunk (ES) pour modifier les configurations prédéfinies et leurs valeurs selon vos besoins.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Accédez à la **Tous** > **Intégration Splunk ES** > **Paramètres Splunk ES**.
2. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres Splunk ES

Champ	Description
Appliquez une limite au nombre d'événements notables qui peuvent être regroupés en un seul incident.	Option permettant d'appliquer une limite au nombre d'événements notables que vous souhaitez regrouper en un seul incident. Par défaut, la valeur est 100.
Appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés dans une période de 24 heures.	Option permettant d'appliquer une limite au nombre d'incidents de sécurité qui peuvent être créés sur une période de 24 heures. Par défaut, la valeur est définie sur 1 000.
Appliquer une limite au nombre de valeurs à analyser dans chaque champ reçu de Splunk.	Option permettant d'appliquer une limite au nombre de valeurs que vous souhaitez analyser pour chaque champ reçu de Splunk. Par défaut, la valeur est définie sur 1 000.
Nombre de règles de corrélation à extraire Splunk.	Option permettant de définir le nombre de règles de corrélation à récupérer Splunk. Par défaut, la valeur est définie sur 500.
Le paramètre Durée de vie pour Splunk la tâche de recherche en secondes.	Option permettant de définir le paramètre de durée de vie pour la Splunk recherche sous forme de secondes. Par défaut, la valeur est définie sur 600.
Nombre de types notables à regrouper dans une seule recherche.	Option permettant de définir le nombre total de types notables que vous souhaitez regrouper en une seule recherche. Par défaut, cette valeur est définie sur 20.
Nombre de jours de conservation des métadonnées de la Splunk tâche de recherche dans ServiceNow	Option permettant de définir le nombre de jours pendant lesquels vous souhaitez conserver les métadonnées de la tâche de recherche Splunk dans ServiceNow. Par défaut, la valeur est définie sur 30.
Le caractère du délimiteur pour diviser les valeurs dans les mappages de champs.	Option permettant de définir le caractère de délimiteur pour diviser les valeurs en mappages de champs. Par défaut, la valeur est définie comme suit : (,).
Nombre de minutes de chevauchement à ajouter lors de l'extraction des événements (Splunk pour surmonter le délai d'indexation de Splunk)	Option permettant de définir le nombre de minutes de chevauchement à ajouter lors de la récupération des événements à partir de Splunk pour surmonter le délai d'indexation à partir de Splunk.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par défaut, la valeur est définie sur 30.
Extraire les événements notables mis à jour	Option permettant de récupérer les événements notables mis à jour. Par défaut, la valeur est définie sur Non.
Activez ce paramètre pour mettre à jour les configurations sources existantes Splunk pour la prise en charge de l'authentification basée sur les jetons. Vous devez mettre à jour la configuration d'intégration avec les détails du jeton une fois ce paramètre activé.	Option permettant de mettre à jour la configuration source existante Splunk sur la prise en charge de l'authentification basée sur les jetons à partir d'une version existante. **Remarque :** Après la mise à niveau vers la nouvelle version, le champ de jeton devient indisponible. Vous devez activer ce paramètre pour obtenir l'authentification basée sur les jetons, après quoi vous devez mettre à jour la configuration d'intégration avec les détails du jeton. Par défaut, la valeur est définie sur Non.
Cochez la case pour extraire les notables fermés pendant l'ingestion.	Option permettant d'extraire les événements fermés dans l'instance ServiceNow Splunk ES. Si cette option n'est pas cochée, seuls les événements actifs sont transférés vers l'instance. Par défaut, la valeur est définie sur Non.

3. Cliquez sur **Enregistrer**.

Erreurs d'authentification

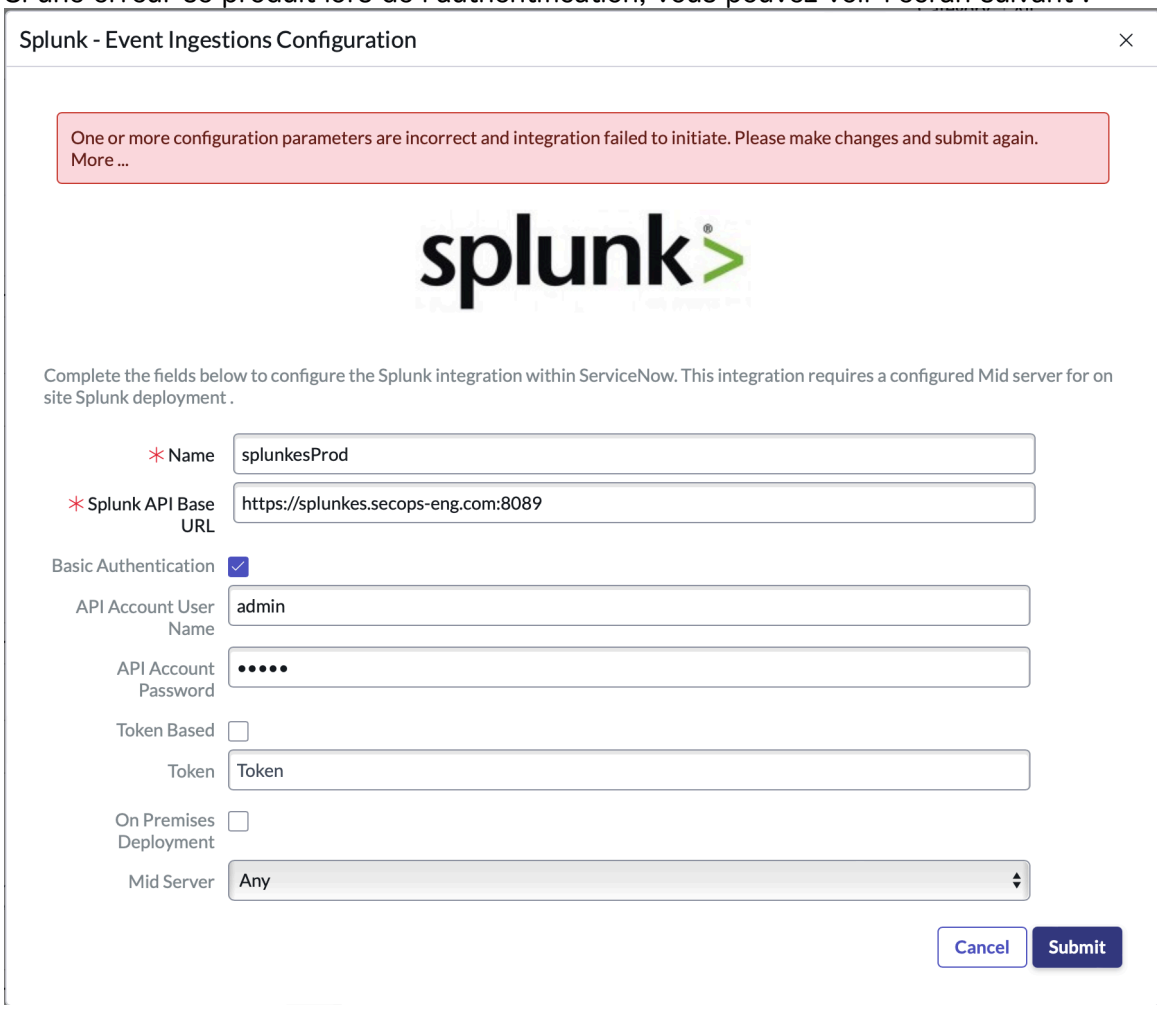
Cette section décrit certaines erreurs d'authentification courantes et la façon dont elles peuvent être résolues.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Problème de validation de certificat

Si une erreur se produit lors de l'authentification, vous pouvez voir l'écran suivant :



Si vous avez vérifié que les informations d'identification de votre compte API et les informations de l'URL de base Splunk sont correctes, cette erreur peut être due à un problème avec le certificat Splunk pour la communication du port 8089. ServiceNow® L'instance nécessite un certificat valide avec un nom commun qui correspond au nom d'hôte du serveur pour établir des connexions sécurisées. Pour plus d'informations, voir Certificats . Si cette erreur s'affiche, vous pouvez vérifier que le problème est dû à un problème de certificat en consultant les journaux système.

Une condition d'erreur similaire à la suivante apparaîtra probablement :



Pour procéder à l'authentification, vous devez remplacer le certificat Splunk par défaut fourni pour l'accès à l'API sur le port 8089. Pour obtenir des instructions détaillées sur le remplacement du certificat SSL, consultez KB0778285 .

Créer et nommer un profil d'événement pour l'intégration d'ingestion d'événements Splunk Enterprise Security

Vous créez un profil d'événement dans votre ServiceNow AI Platform instance et déterminez quels Splunk événements notables créent des incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Avant ServiceNow AI Platform Réponse aux incidents de sécurité que les incidents de sécurité (SIR) ne soient créés à partir d'événements notables ingérés, les valeurs de champ des alertes sont affichées sur une mise en page d'un ServiceNow AI Platform incident de sécurité afin que vous puissiez prévisualiser la façon dont l'incident de sécurité réel sera créé.

Du point de vue de l'intégration, à l'aide des API disponibles, Splunk ES les événements notables sont transmis individuellement et manuellement en tant qu'événements notables discrets, ou ils sont automatiquement ingérés dans l'environnement Opérations de sécurité de votre ServiceNow AI Platform instance en fonction du type de profil défini.

Les workflows d'intégration ingèrent différents types d'événements notables, tels que les tentatives d'accès non autorisé et les programmes malveillants, par exemple. Ces événements notables sont ingérés en fonction des profils que vous configurez dans l'environnement Opérations de sécurité de votre instance.

Tous les notables sont initialement ingérés pour un type de recherche de corrélation configuré dans un profil. Les notables ingérés peuvent ensuite être filtrés davantage pour spécifier quels notables créent des incidents de sécurité. Par exemple, vous pouvez préférer les filtres qui créent des incidents de sécurité uniquement pour les événements notables identifiés comme à haut risque. Avant qu'un profil ne soit activé et qu'il crée des incidents de sécurité à partir d'événements notables ingérés, les valeurs de champ individuelles des événements notables sont mappées aux champs correspondants sur une mise en page de l'incident de sécurité pour un aperçu.

Procédure

1. Les noms des profils d'événements dans votre ServiceNow AI Platform instance doivent être uniques et ne peuvent être mappés qu'à un seul profil d'événement actif à la fois.
2. L'application ServiceNow AI Platform ingère des notables spécifiques à l'aide des workflows de l'intégration.
   Tous les événements notables qui répondent aux critères de sélection dans votre Splunk ES console sont initialement ingérés dans votre ServiceNow AI Platform instance.
3. Un profil dans votre ServiceNow AI Platform est une encapsulation d'un événement notable dans votre Splunk ES console.
   Il existe une relation un-à-un entre les événements notables qui sont ingérés avec un profil et les connexions à votre Splunk ES console : un type d'événement notable pour une connexion.
4. Pour créer des profils pour les événements notables planifiés, reportez-vous à la section Configurer un profil pour l'ingestion d'événements notables planifiés.
5. Pour créer des profils pour le transfert manuel d'événements, reportez-vous à la section Configurer un profil pour le transfert manuel d'événements.

Configurer un profil pour l'ingestion d'événements notables planifiés

Selon le profil défini, Splunk ES les événements notables sont automatiquement ingérés dans l'environnement Opérations de sécurité de votre ServiceNow AI Platform instance.

La table suivante répertorie les tâches que vous devez suivre pour configurer un profil pour l'ingestion planifiée d'événements notables :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étapes pour configurer un profil pour l'ingestion d'événements notables planifiés

Tâche	Section
Créer un profil d'événement	Reportez-vous à la rubrique Créer des profils pour l'ingestion d'événements notables planifiés.
Sélectionner les événements notables en fonction du nom de recherche de corrélation	Reportez-vous à la rubrique Sélectionner les événements notables en fonction du nom de la règle de corrélation pour le profil pour Splunk ES l'intégration de l'ingestion d'événements.
Mapper les champs d'événements notables	Reportez-vous à la rubrique Mappage des champs d'événement notable pour l'intégration Splunk Enterprise Security.
Créer des mappages personnalisés	Reportez-vous à la rubrique Créer des mappages pour Splunk ES l'examen des incidents d'événements notables et les détails de l'événement de contribution (ingestion planifiée).
Prévisualiser l'incident de sécurité	Reportez-vous à la rubrique Prévisualiser l'incident de sécurité pour l'intégration d'ingestion d'événements Splunk Enterprise Security.
Planifier et récupérer les événements notables nouveaux et mis à jour	Reportez-vous à la rubrique Planifier et récupérer les événements notables nouveaux et mis à jour pour l'intégration d'ingestion d'événements Splunk Enterprise Security.
Automatiser les mises à jour et les clôtures d'événements notables en fonction de l'état de l'incident SIR	Reportez-vous à la rubrique Automatiser les mises à jour et les clôtures d'événements notables en fonction de l'état de l'incident SIR.

Créer des profils pour l'ingestion d'événements notables planifiés

Vous pouvez configurer un profil pour que les événements notables soient automatiquement ingérés.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Pour créer un profil d'événement pour un événement notable ou un type de règle de corrélation dans votre ServiceNow AI Platform instance, accédez à **Intégration Splunk** > **Profil d'événement Splunk**.
2. Si le formulaire de profil d'événement n'est Splunk pas affiché, cliquez sur **Nom** dans la barre de progression.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs.

   Un exemple de formulaire rempli suit la table.

Traduction automatique

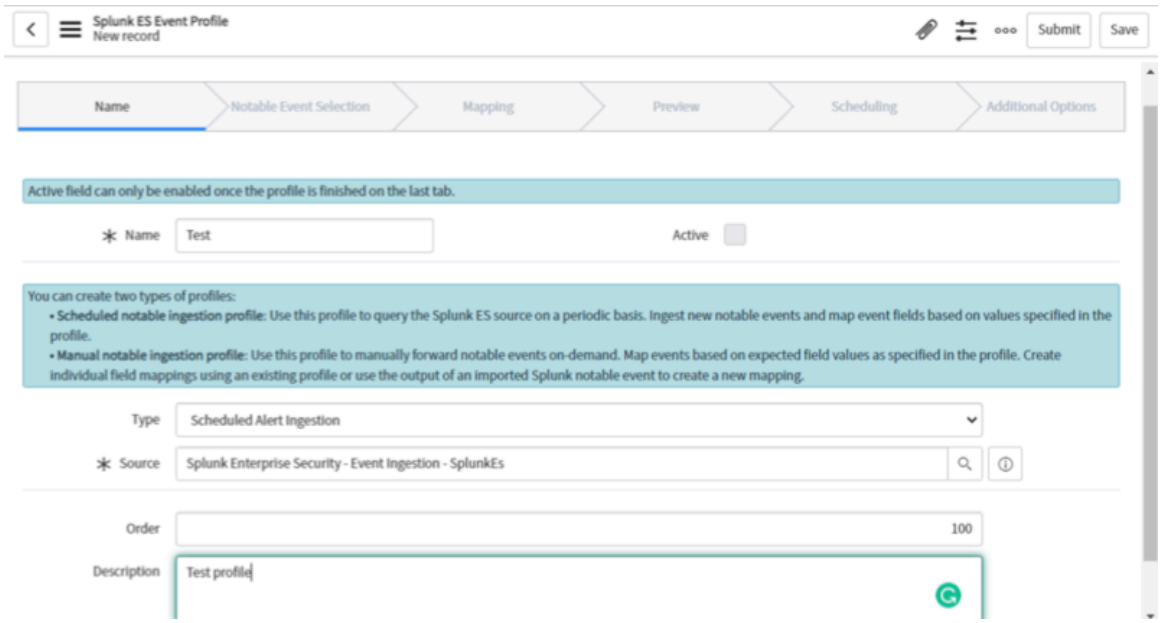
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom unique pour le profil. Si les noms ne sont pas uniques, une erreur s'affiche et les noms de profil en double ne sont pas enregistrés. Les noms de profil dans votre ServiceNow AI Platform instance doivent être uniques.
Actif	La case à cocher est désactivée par défaut. Vous devez remplir toutes les sections du profil avant de l'activer.
Type	Sélectionnez le type de profil dans la liste de choix. ○ Ingestion d'événements planifiés : ce type de profil prend en charge les événements notables qui sont ingérés sur un calendrier configuré. Renseignez les champs. ○ Transfert manuel d'événements : ce type de profil prend en charge les événements notables qui sont transmis manuellement à partir de votre Splunk Enterprise Security console Incident Review sur demande. Consultez les étapes suivantes pour remplir le formulaire pour ces types de profils.
Source	Splunk Serveur ou extrémité de recherche que vous avez configuré pour ingérer des événements notables. Si plusieurs Splunk serveurs sont configurés, sélectionnez le serveur approprié pour les types d'événements notables qui seront ingérés pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent les mêmes conditions de déclenchement. Le workflow dans le profil avec le numéro le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte supplémentaire pour vous aider à distinguer ce profil des autres profils.

La figure suivante est un exemple de formulaire rempli pour un type d'événement notable planifié.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Pour un profil avec un événement notable planifié, choisissez une option pour poursuivre la configuration du profil.

Option	Description
Continuer	Enregistrez le profil et progressez jusqu'à l'étape de sélection d'événement.
Mettre à jour	Enregistrez les mises à jour de ce profil et revenez à la liste des profils d'événements Splunk .
Enregistrer	Enregistrez ce profil et restez sur la page.
Supprimer	Supprimez cet enregistrement de profil et revenez à la liste des profils d'événements Splunk .

Que faire ensuite

L'étape suivante consiste à sélectionner des événements notables pour une ingestion automatique.

Sélectionner les événements notables en fonction du nom de la règle de corrélation pour le profil pour Splunk ES l'intégration de l'ingestion d'événements

Une fois que vous avez créé un profil pour une ingestion de type d'événement notable planifiée, sélectionnez un nom de Splunk Enterprise Security règle de corrélation pour ce profil pour lequel vous souhaitez mapper les événements notables correspondants à un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Affichez les règles de corrélation disponibles dans votre ServiceNow AI Platform instance afin de connaître les types d'événements notables pour lesquels vous souhaitez ingérer et créer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

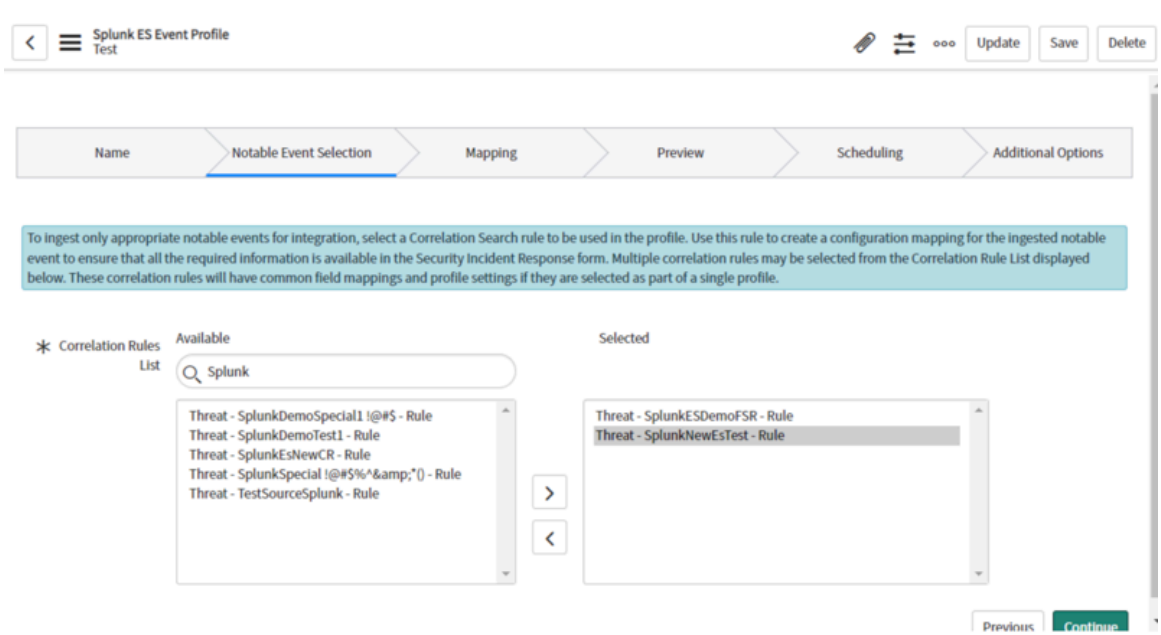
des incidents de sécurité. Sélectionnez une règle de corrélation. Vous pouvez sélectionner un ou plusieurs événements notables dans la liste de ce formulaire.

Procédure

1. Si la page Sélection d'événement notable n'est pas affichée, sélectionnez-la dans la barre de progression pour l'afficher.
2. Dans la liste Règle de corrélation, choisissez l'une des options suivantes pour sélectionner une ou plusieurs règles de corrélation et les déplacer et les déplacer de la colonne Disponible vers la colonne Sélectionné.

   La liste des règles de corrélation figurant sur ce formulaire correspond à la liste des règles de corrélation dans votre Splunk ES console Revue des incidents. Jusqu'à 500 règles de corrélation sont affichées sur ce formulaire. Si plus de 500 règles de corrélation sont répertoriées dans votre Splunk ES, seuls les 500 premiers événements notables sont affichés sur ce formulaire dans votre ServiceNow AI Platform instance.

Option	Description
Dans le champ de recherche Liste de règles de corrélation, saisissez du texte.	La colonne située sous le champ de recherche est filtrée avec les options disponibles en fonction du texte que vous entrez. Sélectionnez une règle de corrélation et, à l'aide des touches fléchées, déplacez l'alarme sélectionnée de **Disponible** à **Sélectionné**.
Dans la liste Règle de corrélation, double-cliquez sur une règle de corrélation.	La colonne **Sélectionné** est renseignée avec votre sélection.
Dans la liste Règle de corrélation, cliquez sur une règle de corrélation.	La règle de corrélation est sélectionnée. À l'aide des flèches, déplacez la règle de corrélation sélectionnée de **Disponible** à **Sélectionné**.



3. Choisissez une option pour continuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Poursuivez ou cliquez sur Mappage dans la barre de progression	Le formulaire Mappage s'affiche. **Le mappage** est sélectionné dans la barre de progression. L'étape suivante consiste à mapper les champs d'événements notables à un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements notables Splunk s'affiche.
Précédent	L'étape **Nom** s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements notables Splunk s'affiche.

Que faire ensuite

Vous avez sélectionné avec succès une règle de corrélation pour un profil planifié Splunk Enterprise Security . L'étape suivante consiste à mapper les valeurs d'événements notables aux champs d'un incident de sécurité.

Mappage des champs d'événement notable pour l'intégration Splunk Enterprise Security

Une fois que vous avez identifié la règle de corrélation spécifique et le type d'événement notable pour le profil, l'étape suivante consiste à mapper les champs d'événement notable individuels aux champs d'un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Vue d'ensemble du mappage

Pour l'étape de mappage, vous pouvez ingérer des exemples d'événements notables pour la règle de corrélation sélectionnée ou exporter des données d'événements notables pour les événements notables transférés manuellement. Le processus de mappage d'événements est identique, quel que soit le type de profil que vous créez.

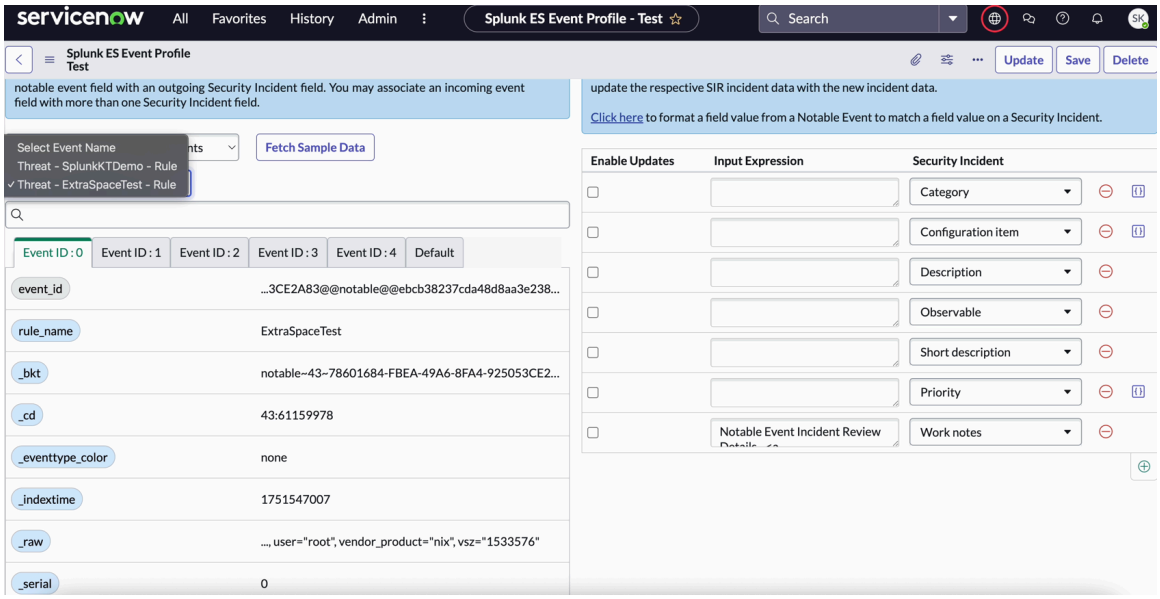
Les figures suivantes sont des exemples des configurations de mappage par défaut fournies pour chaque type de profil d'événement. Vous pouvez personnaliser les champs qui renseignent l'incident de sécurité. Au cours de cette phase de mappage, vous pouvez vous assurer que toutes les données de champ d'événement notables pertinentes sont mappées à l'endroit approprié sur le formulaire d'incident SIR, puis visualiser l'incident SIR dans la section d'aperçu.

Si plusieurs corrélations sont utilisées, les événements notables peuvent être récupérés en sélectionnant l'événement requis. Utilisez **le nom de l'alerte** pour choisir votre alerte si vous avez configuré plusieurs alertes pour l'ingestion.

Une fois que vous avez cliqué pour extraire les données, les noms de champs d'événements notables et les Splunk valeurs correspondantes sont renseignés sur le côté gauche du formulaire. Il s'agit des champs d'événements Splunk notables qui peuvent être mappés aux champs d'incident SIR de sécurité. Certains champs peuvent être mappés plusieurs fois aux champs d'incident de sécurité SIR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous préférez peut-être examiner quelques exemples d'événements notables sur votre Splunk console à ingérer pour l'étape de configuration du mappage de champ. Cette étape est étiquetée Mappage dans la barre de progression. Si cette page n'est pas affichée, cliquez sur **Mappage** dans la barre de progression. Vous pouvez ingérer jusqu'à cinq échantillons d'événements notables pour faciliter le processus de mappage des champs d'événements Splunk Enterprise Security notables. Il existe des options permettant d'ingérer les cinq événements notables les plus récents pour la règle de corrélation sélectionnée ou d'ingérer jusqu'à cinq événements notables spécifiques en fonction des ID d'événements notables.

Vous trouverez ci-dessous un résumé des étapes requises pour cartographier les événements notables :

- Ingestion d'exemples d'événements notables planifiés : pour les exemples de données utilisés pour les profils d'événements notables ingérés automatiquement, les champs d'événements notables disponibles et leurs valeurs correspondantes sont affichés dans une mise en page de mappage par défaut sur le côté gauche du formulaire de mappage une fois les données d'exemple récupérées. Des onglets s'affichent pour vous permettre d'afficher les valeurs d'un ID d'événement notable spécifique que vous avez extrait. Vérifiez que tous les champs critiques de la section d'ingestion d'échantillons d'événements notables à gauche du formulaire sont mappés aux ServiceNow champs d'incident de sécurité à droite du formulaire.
- Mappage de champs : modifiez la configuration du mappage en faisant glisser les champs d'événements notables du côté gauche et en les déposant dans la section de mappage des ServiceNow incidents SIR à droite. Le mappage sur la droite associe le champ d'événement notable entrant à un champ d'incident de sécurité sortant.
- Expérience de mappage : personnalisez la grille de mappage en ajoutant ou en supprimant des champs à l'aide de l'icône + située en bas de la section de mappage des champs d'incidents SIR. Suivez les champs négligés ou dupliqués avec le code couleur fourni (les champs mappés sont grisés, les champs bleus ne sont pas mappés).
- Conditions de génération d'incidents : une fois la section de mappage terminée, vous pouvez définir des conditions de filtre afin de spécifier quels événements notables doivent créer des incidents de sécurité par rapport à quels événements notables doivent être filtrés, par exemple, les événements notables de faible priorité. Cette opération est effectuée dans la section Conditions de génération d'incident située sous la section Mappage d'événements notables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Critères d'agrégation d'événements : définissez des critères d'agrégation d'événements supplémentaires qui regroupent un événement notable entrant à un incident de sécurité existant SIR au lieu de créer des incidents similaires, potentiellement en double. En utilisant des critères de correspondance de valeur de champ pour chaque profil, cette option d'agrégation supplémentaire peut réduire le nombre d'incidents de sécurité actifs qui se chevauchent en plaçant toutes les données d'événement notables de sécurité connexes sur un seul incident de sécurité.
- Formater la traduction du champ : dans certains cas, les valeurs des champs Événement dans les événements notables Enterprise Splunk peuvent ne pas se traduire directement dans les champs de l'incident SIR de sécurité. Pour ces valeurs, vous pouvez utiliser un éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage. Utilisez l'éditeur de script si vous souhaitez formater des valeurs similaires, mais pas identiques. Par exemple, avec l'éditeur de script, une valeur de catégorie Alerte de programme malveillant et Infection par un virus peut avoir des valeurs de champ différentes pour la catégorie source, mais les deux valeurs peuvent être traduites en une activité de code malveillant commune dans le champ Catégorie de l'incident de sécurité à l'aide de la SIR fonctionnalité Formater la traduction du champ.

L'étape suivante consiste à ingérer des événements notables et à mapper les valeurs aux champs d'incident SIR de sécurité.

Créer des mappages pour Splunk ES l'examen des incidents d'événements notables et les détails de l'événement de contribution (ingestion planifiée)

Au cours de l'étape de mappage de champs d'événements notables, vous mappez les champs d'événements individuels des événements notables aux champs d'un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

La grille de mappage peut être personnalisée en fonction du type d'événement notable sélectionné dans la sélection de règle de corrélation. Le code couleur des champs d'événements vous aide à suivre les valeurs d'événements que vous avez déjà mappées à mesure qu'elles deviennent grisées, tandis que tous les champs non mappés restants apparaissent en bleu. Cela vous aide à mieux visualiser les valeurs de champ qui ont été ajoutées à l'incident de sécurité et si des informations d'événement importantes restantes ne sont pas mappées.

Mappez jusqu'à cinq événements notables de la colonne Ingestion d'échantillons d'événements notables à gauche du formulaire aux champs d'incident de sécurité de la colonne Mappage de champ d'incidents SIR à droite.

Créez des mappages personnalisés en ajoutant ou en supprimant des champs sur la grille de mappage sur le côté droit du formulaire. Les champs par défaut qui sont généralement des champs importants à renseigner sur le formulaire de réponse aux incidents de sécurité s'affichent. Toutefois, ces champs peuvent être supprimés et tous les champs supplémentaires peuvent être affichés à l'aide des boutons + et -. Créez des cartes personnalisées en ajoutant ou en supprimant des champs sur la grille de mappage située à droite du formulaire. La personnalisation des champs vous permet de mapper Splunk les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

champs qui ne sont pas affichés sur la grille de mappage par défaut de l'incident SIR de sécurité.

Procédure

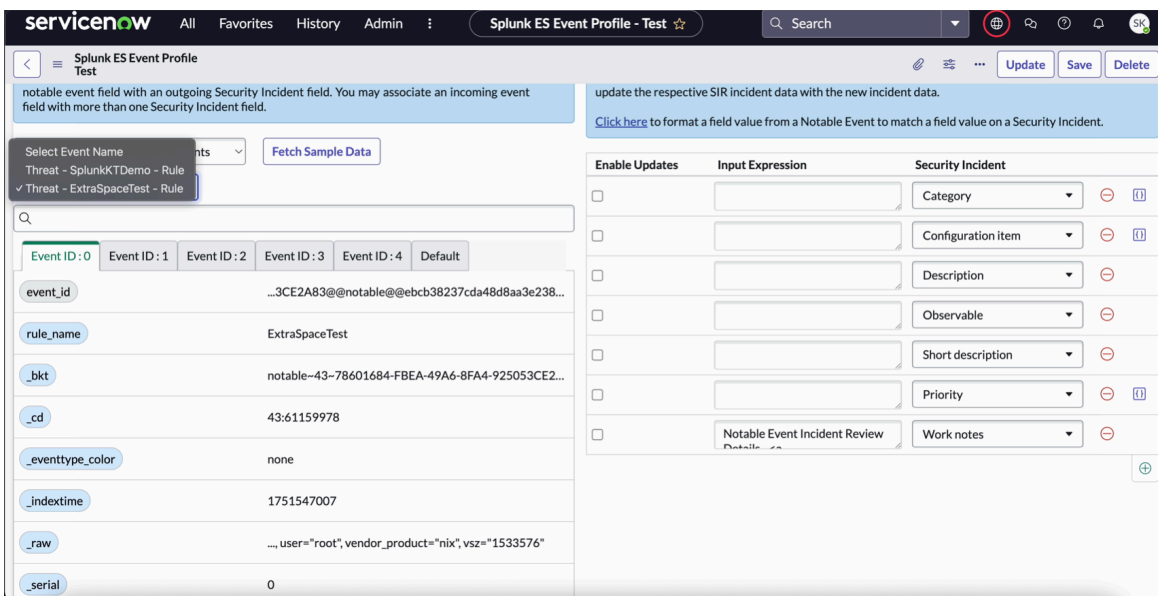
1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Pour un profil avec une ingestion planifiée, sous Ingestion d'échantillons d'événements notables, cliquez sur **Extraire les données d'échantillon** pour extraire les derniers exemples d'événements notables de la Splunk Enterprise console pour la règle de corrélation sélectionnée.

   Remarque : Vous pouvez soit extraire les échantillons d'événements notables les plus récents, soit fournir les ID d'événements notables uniques pour les événements notables spécifiques que vous souhaitez utiliser pour votre expérience de mappage d'événements notables.

   Les résultats des champs et des valeurs d'événements notables sont affichés sous forme d'onglets individuels. Vous pouvez ingérer jusqu'à cinq événements notables.

   L'extraction d'exemples d'événements notables peut prendre quelques instants. Un message indiquant que la transaction fonctionne s'affiche en haut de l'écran.

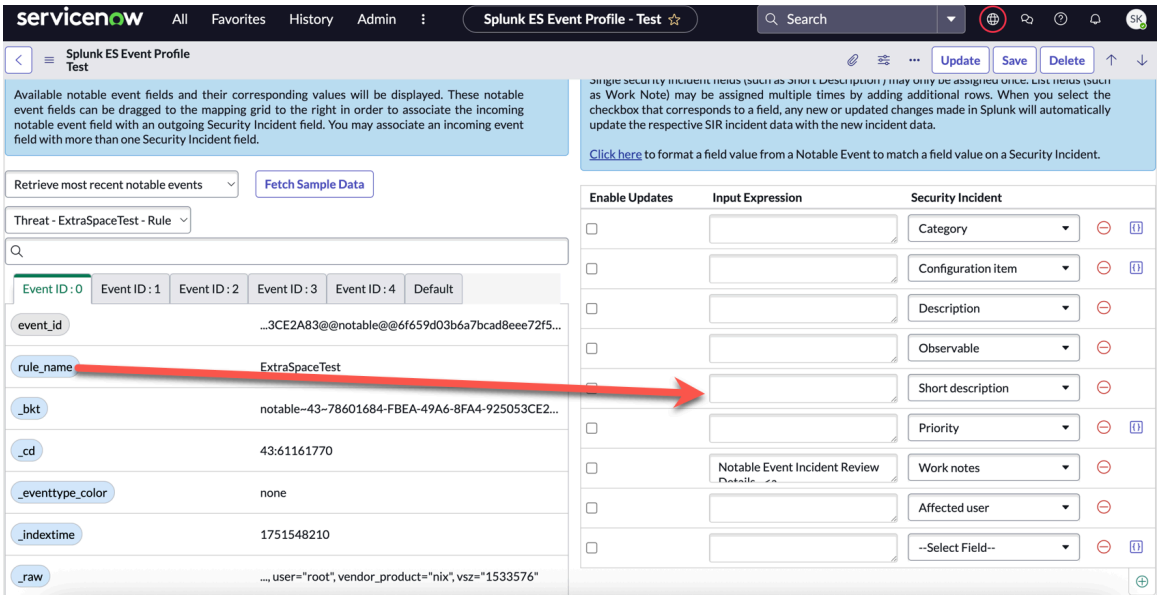
   Dans la figure suivante, les paires de valeur de nom de champ pour l'événement notable ingéré, ou les exemples d'événements importés, sont affichées sur le côté gauche de ce formulaire une fois l'extraction d'ingestion terminée. Il s'agit des valeurs que vous mappez aux champs d'incident de sécurité du côté Mappage du champ d'incident SIR du formulaire.



3. Pour faire correspondre une valeur de champ du côté gauche du formulaire à un champ de l'incident de sécurité sur le côté droit du formulaire, cliquez tout en maintenant enfoncé le nom d'un champ bleu sur le côté gauche du formulaire.
4. Faites glisser le nom du champ, par exemple rule_name, et déposez-le sur un champ de la colonne Expression d'entrée en regard d'un nom de champ dans la colonne Incident de sécurité.

Traduction automatique

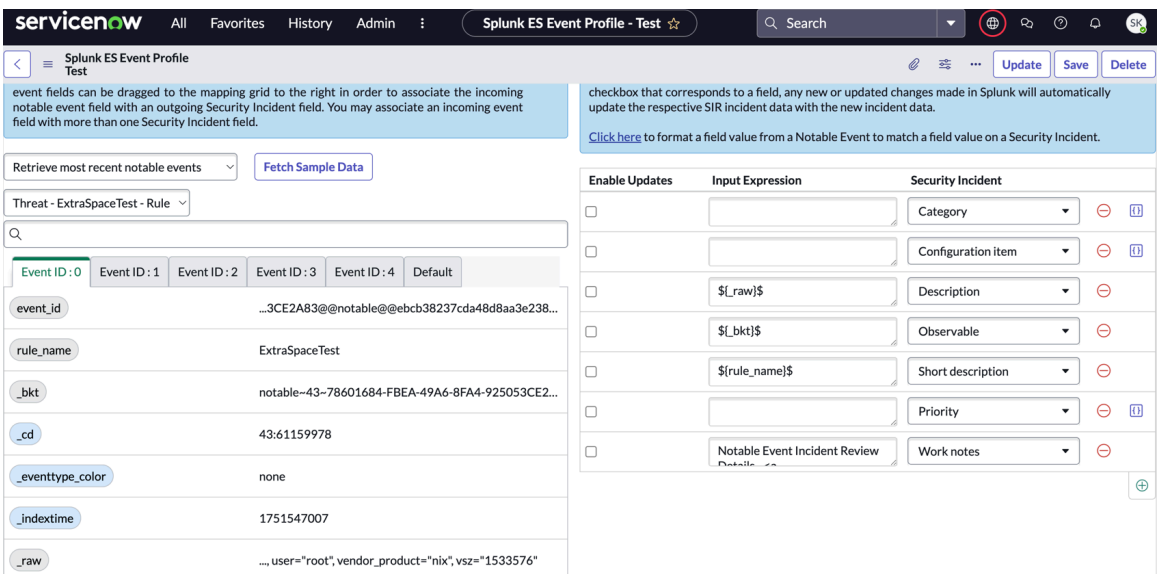
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La valeur du champ est affichée dans la colonne Expression d'entrée. Dans l'image suivante, rule_name est mappé au champ Brève description de l'incident de sécurité. Toutefois, vous pouvez faire correspondre n'importe quelle valeur du côté gauche à un champ sur la droite. Vérifiez que la valeur est correctement mappée sur l'incident de sécurité pendant l'étape d'aperçu.

Pour vous assurer qu'aucun champ d'événement n'est négligé ou dupliqué dans le processus de mappage, les champs sont codés par couleur. Les champs bleu clair sur la gauche indiquent qu'un champ d'événement notable n'est pas encore sélectionné et mappé sur l'incident de sécurité. Vous préférez peut-être associer un champ notable entrant à plusieurs champs d'un incident de sécurité.

Un champ gris indique qu'un champ a été sélectionné et mappé à un champ de l'incident de sécurité. Ce code couleur vous aide à suivre le mappage.



5. Pour ajouter des champs aux champs par défaut affichés sur l'incident de sécurité sur le côté droit du formulaire, procédez comme suit.

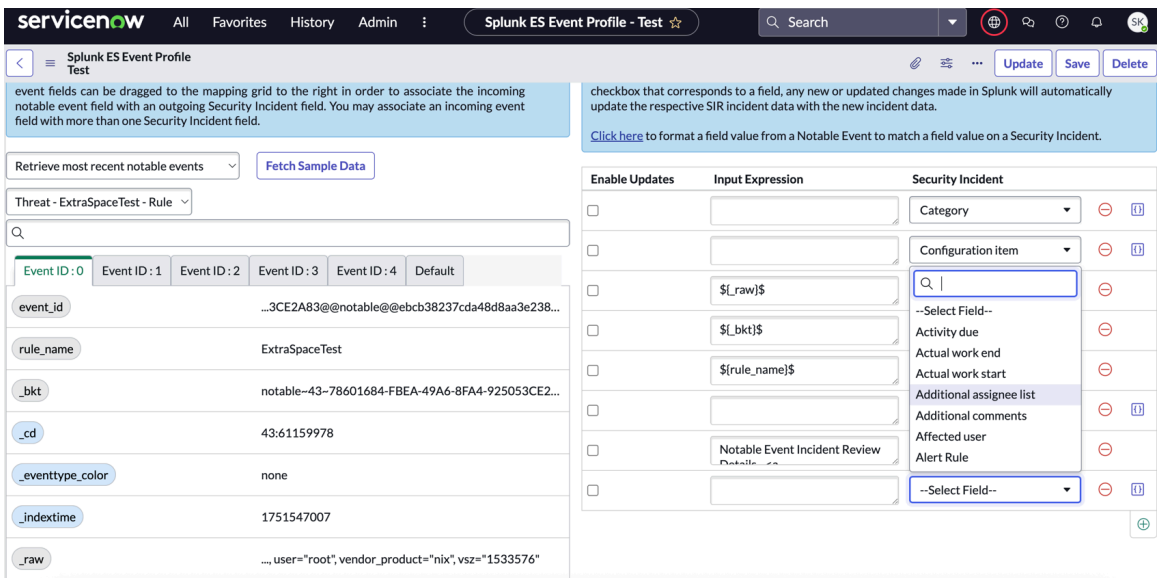
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. À droite du formulaire, dans la section Mappage du champ d'incidents SIR, au bas de la grille, cliquez sur l'icône plus.
Un nouveau champ s'affiche.

b. Dans la colonne Incident de sécurité, développez la liste qui s'affiche, puis sélectionnez un champ.

Dans la liste développée du nouveau champ, certains champs sont ombrés. Dans la figure suivante, rule_name a un arrière-plan gris, car il a été mappé dans l'incident de sécurité. Semblable au code couleur pour les champs d'événements notables sur le côté gauche du formulaire, ce code couleur pour les champs d'incident de sécurité sur la droite vous aide à suivre les champs d'incident SIR déjà mappés.



Remarque : Afin que plusieurs observables puissent être affichés sur le même incident de sécurité, le champ Observable peut être mappé plusieurs fois avec des valeurs différentes. De même, les champs Élément de configuration et Notes de travail prennent en charge plusieurs valeurs.
Si vous essayez de mapper deux valeurs à un champ qui ne peut pas prendre en charge plusieurs valeurs, lorsque vous prévisualisez l'incident, un message d'erreur s'affiche indiquant qu'il n'y a aucune valeur pour le champ. De même, si un champ d'un incident de sécurité comporte une liste dans laquelle vous pouvez choisir plusieurs options, et que vous essayez de mapper une option à ce champ qui n'est pas affichée dans la liste, le champ n'est pas renseigné sur l'incident de sécurité.

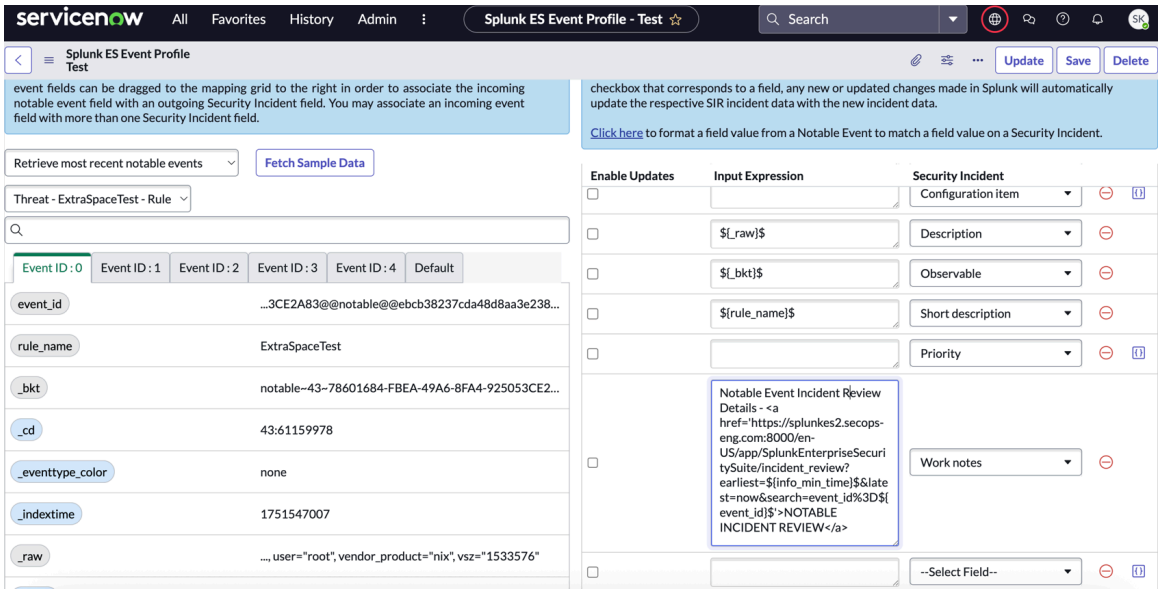
c. Vous pouvez également saisir une valeur dans le champ Rechercher de la nouvelle ligne.

d. Sur le côté gauche du formulaire, cliquez avec le bouton gauche pour sélectionner **l'ID d'événement** souhaité dans le champ expression d'entrée.

6. Poursuivez le mappage en ajoutant ou en supprimant des valeurs de champ au mappage.
La figure suivante est un exemple de mappage modifié. Dans le champ inférieur à droite, le champ Notes de travail est ajouté et comporte plusieurs valeurs. Notez que pour le champ de chaîne de texte long, vous pouvez développer le champ de mappage pour voir la chaîne complète et redimensionner selon vos besoins en tirant le coin inférieur droit du champ comme indiqué dans la capture d'écran ci-dessous avec le champ Notes de travail ajouté :

Traduction automatique

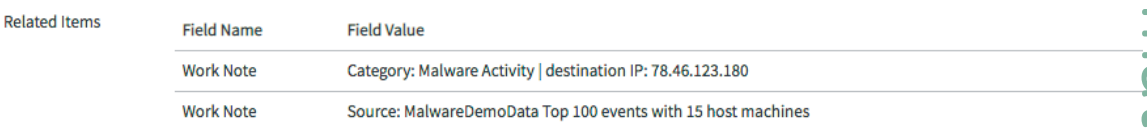
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



⚠ Avertissement : Veuillez noter que dans la section **Mappage du champ d'incident SIR** , l'URL et le numéro de port mentionnés dans le champ **expression d'entrée** ne sont qu'un exemple et non l'URL ou le numéro de port fourni prêt à l'emploi.

Dans l'aperçu, ces valeurs sont affichées dans les notes de travail sur l'incident de sécurité. Étant donné que la valeur concerne un champ que vous avez ajouté à la section de mappage et que plusieurs valeurs sont mappées au champ Notes de travail, les valeurs s'affichent telles que saisies. Dans cet exemple, les espaces et les signes de ponctuation que vous avez entrés dans le champ s'affichent dans la section Éléments connexes sous forme de note de travail sur l'aperçu de l'incident de sécurité.

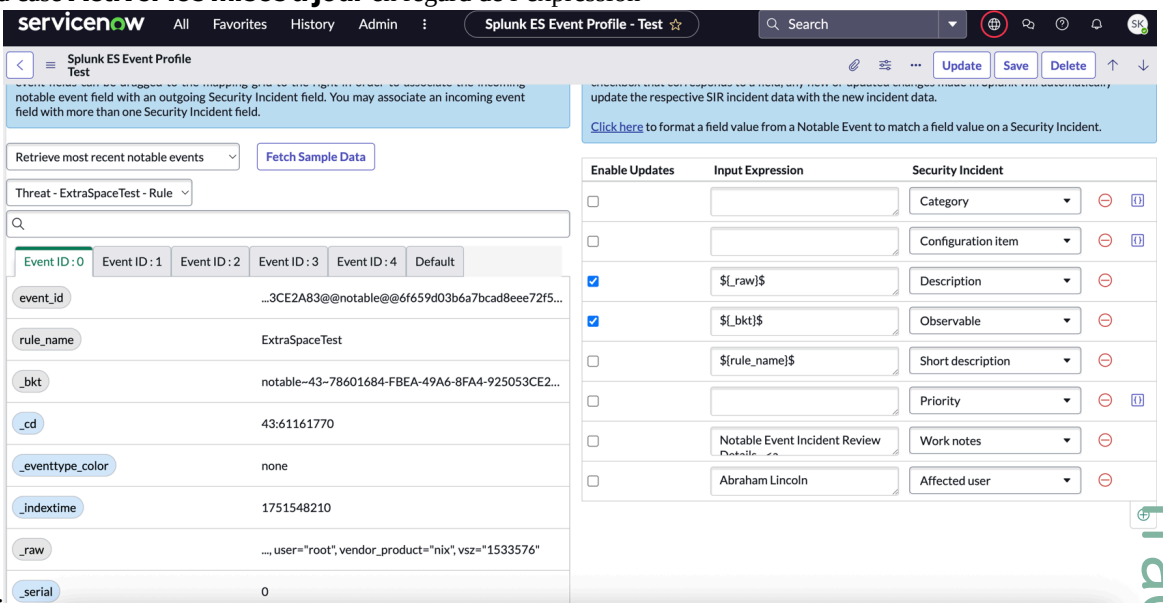
L'image suivante est un exemple de la façon dont les valeurs de l'image précédente sont affichées sur l'incident de sécurité.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Pour recevoir des mises à jour pour les champs mappés dans SIR, cochez la case **Activer les mises à jour** en regard de l'expression d'entrée.

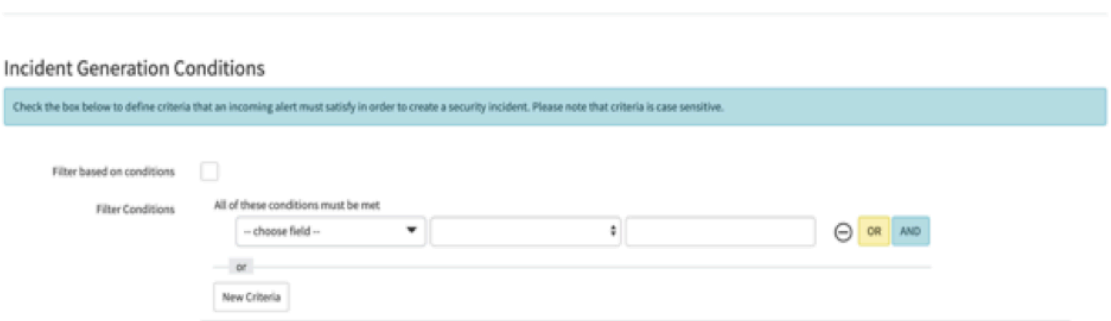


8. **Facultatif :** Une fois que vous avez terminé les étapes de mappage de champ précédentes, vous pouvez utiliser les mêmes valeurs de champ dans le générateur de conditions de génération d'incident pour définir des critères supplémentaires qu'un événement notable entrant doit satisfaire pour créer un incident de SIR sécurité.
Pour définir les conditions de génération d'incidents, procédez comme suit.

   a. Faites défiler la page jusqu'à la section Conditions de génération d'incidents sur le formulaire et cochez la case **Filtre basé sur les conditions** pour activer l'option.

   (Optional) Le générateur de conditions de filtre s'affiche. Utilisez ces filtres pour créer des incidents de sécurité qui correspondent aux conditions spécifiques décrites dans les champs.

   Les options des listes pour le premier champ du générateur de conditions de filtre correspondent aux champs affichés dans la section Ingestion d'échantillons d'événements notables pour les événements que vous avez ingérés. Ces champs sont dynamiques et changent en fonction des Splunk événements notables que vous ingérez ou de l'événement que vous sélectionnez pour les échantillons d'événements notables transférés manuellement. Les critères que vous saisissez sont sensibles à la casse et doivent correspondre exactement aux valeurs de l'événement Splunk Enterprise Security notable. Si vous n'êtes pas sûr des valeurs à saisir dans les champs de filtre, vous préférerez peut-être revenir à votre Splunk Enterprise Security console et passer en revue vos événements notables pour les mots clés.



Traduction automatique

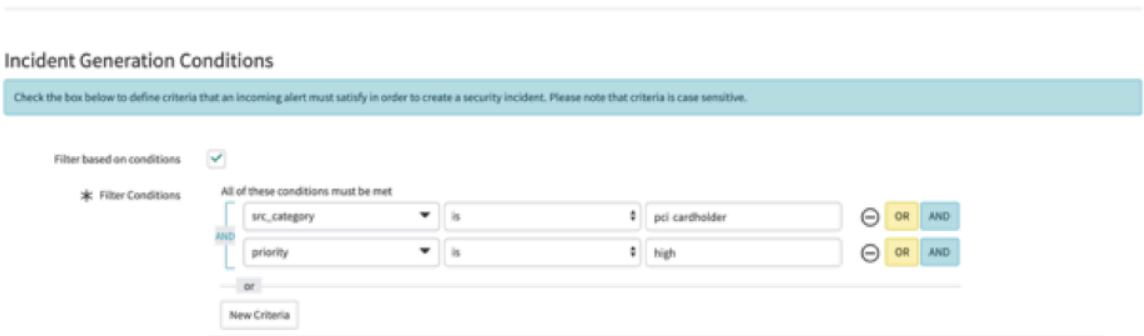
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

b. À l'aide des listes et des champs du générateur de conditions, définissez des filtres pour la première ligne.

c. Pour ajouter plus de conditions, à droite des champs, cliquez sur **ET** ou **OU**.
Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

d. Facultatif : Sur la deuxième ligne, définissez une deuxième condition de filtre.

(Optional) L'image suivante est un exemple avec deux conditions qui doivent être mises en correspondance avant la création d'incidents de sécurité.



(Optional) Vous avez défini les conditions de génération d'incidents afin que les incidents de sécurité ne soient créés que lorsque les deux conditions de filtrage que vous avez saisies correspondent.

Ce type de filtrage des conditions de génération d'incidents vous aide à affiner les événements de sécurité et à limiter le nombre d'incidents de sécurité inutiles que vous créez sans modifier la recherche de corrélation sous-jacente ou les filtres dans Splunk. Si des critères de filtrage supplémentaires sont définis, seuls les événements notables qui correspondent à tous les critères sont mappés aux incidents.

Remarque : Si l'un des noms de champs d'événements contient des caractères spéciaux tels que des guillemets ("), des traits d'union ('), des traits de soulignement (-), at (@) ou des esperluettes (&), ces caractères peuvent devoir être remplacés à des fins de mappage de traduction et éventuellement créer un nom d'événement en double. Le mappage peut être effectué de manière appropriée, mais un suffixe numérique est ajouté pour différencier les champs avec des noms d'événements en double. Par exemple, si le premier champ d'événement est alerts.alert et que le second champ d'événement est alerts@alerts, ces champs ne peuvent pas être identifiés de façon unique, car les caractères de texte standard restants sont identiques. Dans ce cas, un suffixe est ajouté au deuxième champ d'événement et le champ est renommé en alerts@alert(1).

(Optional) Critères d'agrégation d'événements pour gérer les notables similaires et empêcher les incidents en double

9. Facultatif : Pour éviter de créer des incidents de sécurité en double, définissez des critères d'agrégation d'événements supplémentaires afin que les événements notables entrants soient regroupés en un incident de sécurité ouvert.
Pour définir les critères, suivez les étapes ci-dessous.

Traduction automatique

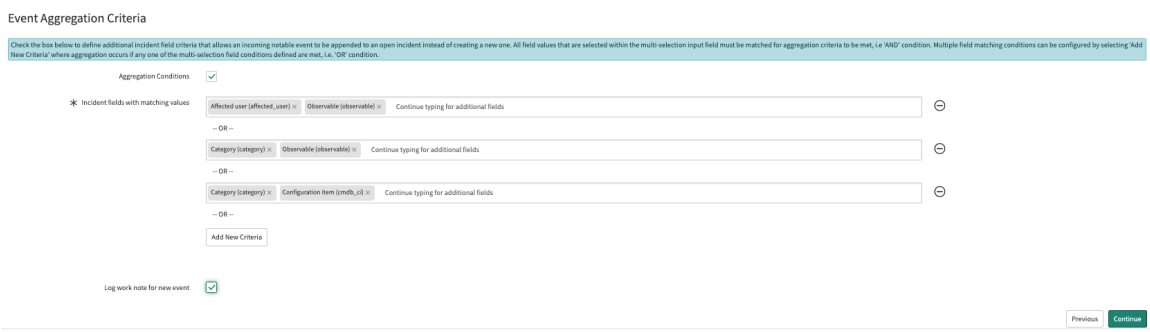
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Faites défiler la page jusqu'à la section Critères d'agrégation d'événements sur le formulaire et cochez la case Conditions **d'agrégat** pour activer cette option.

(Optional) Les champs Incident avec les valeurs correspondantes sont affichés. Ces noms de champs sont les champs de l'incident de sécurité qui incluent tous les champs personnalisés configurés sur l'incident SIR de sécurité.

b. Dans le champ d'entrée à sélection multiple, sélectionnez les valeurs de champ que vous souhaitez faire correspondre sur les incidents de sécurité existants dans votre ServiceNow AI Platform.

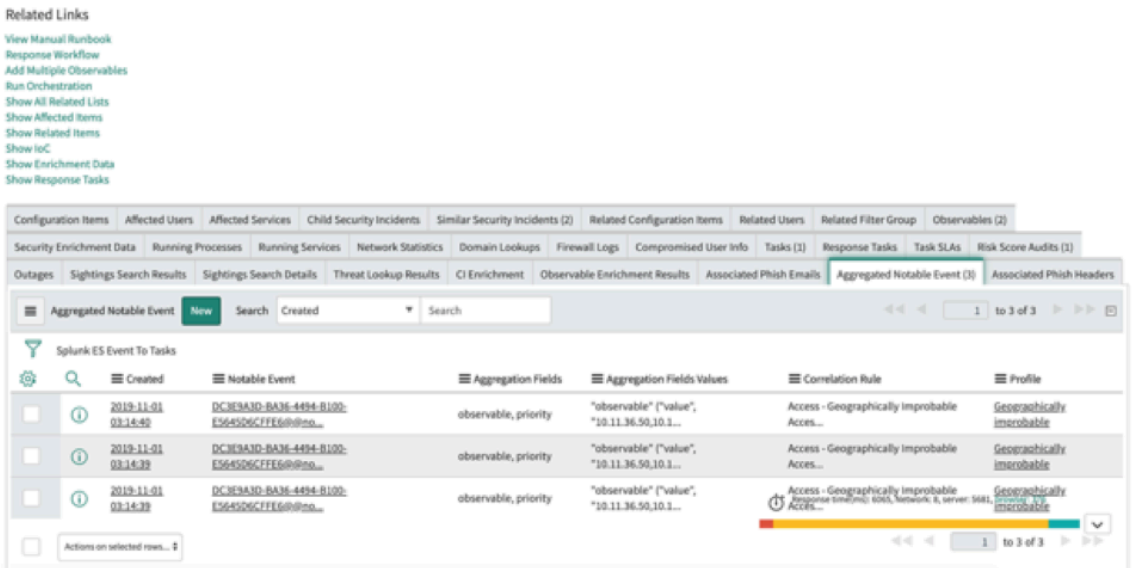
c. Utilisez Ajouter de **nouveaux critères** pour sélectionner plusieurs conditions de correspondance de champ.
Toutes les valeurs de champ que vous sélectionnez dans le champ d'entrée de sélection multiple sont mises en correspondance pour les critères d'agrégation à l'aide de la condition ET. Cliquez sur **Ajouter un nouveau critère** pour sélectionner plusieurs conditions de correspondance de champ où l'agrégation se produit si l'une des conditions de champ multi-sélectionnées qui sont définies est remplie à l'aide de la condition OU.



Si un nouvel événement notable correspond à toutes les valeurs sélectionnées dans les conditions de champ d'agrégation à l'étape de mappage, le nouvel événement notable est automatiquement ajouté à l'incident de sécurité le plus récemment ouvert avec les mêmes valeurs de champ. En tant qu'utilisateur ayant le rôle sn_si.analyst travaillant sur des incidents de sécurité, vous pouvez afficher tous les événements notables regroupés ajoutés sur une liste connexe sur un incident de sécurité. Tous les événements notables regroupés d'un incident de sécurité sont affichés dans la Splunk liste connexe Événement à Tâches. Cette liste détaille les horodatages associés et les valeurs de champ agrégées. Ces informations vous aident à comprendre pourquoi ces événements notables sont regroupés à des incidents de sécurité existants. Si cet onglet n'est pas affiché, faites défiler vers la gauche de l'enregistrement sous Liens connexes et cliquez sur le lien **Afficher toutes les listes connexes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Facultatif : Pour consigner une note de travail pour un nouvel événement notable récemment ajouté à l'incident de sécurité, cochez la case pour activer cette option.
La note de travail indique qu'un nouveau notable a été ajouté, ainsi qu'un lien vers les détails de l'alerte et tout autre détail qui a pu être ajouté au champ Note de travail dans votre section de mappage.

Vous avez mappé avec succès les valeurs d'un Splunk événement notable aux champs d'un SIR incident de sécurité. En outre, vous avez configuré des conditions supplémentaires pour limiter la création d'incidents de sécurité avec des critères de filtrage de génération d'incidents. Vous avez également ajouté des événements notables aux incidents de sécurité existants SIR lorsque les valeurs de champ d'événement correspondent aux critères d'agrégation configurés.

10. Choisissez-en un pour poursuivre la configuration du profil.

Option	Description
Continuer	Le formulaire Mappage s'affiche. **L'aperçu** est sélectionné dans la barre de progression. L'étape suivante consiste à prévisualiser les champs que vous avez mappés sur un SIR incident de sécurité.
Mettre à jour	Vos données sont enregistrées et la liste des profils d'événements Splunk s'affiche.
Précédent	Le formulaire de sélection des événements notables s'affiche.
Supprimer	Supprimez ce profil d'événement et la liste des profils d'événements Splunk s'affiche.

Que faire ensuite

L'étape suivante consiste à prévisualiser les valeurs que vous avez mappées sur l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prévisualiser l'incident de sécurité pour l'intégration d'ingestion d'événements Splunk Enterprise Security

Une fois l'étape de mappage terminée, affichez un aperçu des valeurs que vous avez mappées dans un ServiceNow AI Platform® Réponse aux incidents de sécurité incident de sécurité (SIR). Cette étape d'aperçu vous permet de vérifier que vous avez mappé tous les champs notables que vous souhaitez afficher sur l'incident de sécurité.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

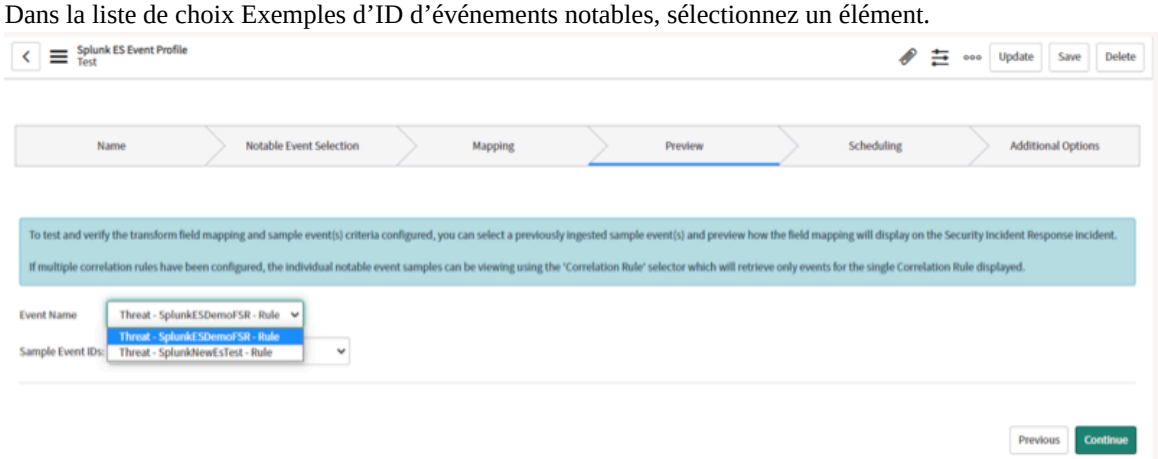
Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Prévisualisez un incident de sécurité et modifiez à nouveau le mappage si nécessaire pour corriger les champs contenant des erreurs ou pour renseigner les données manquantes. Si l'aperçu n'est pas effectué avec succès, vous ne pouvez pas passer à l'étape de planification. Les aperçus des incidents de SIR sécurité ne sont pas enregistrés en tant qu'incidents réels dans le SIR produit.

Procédure

1. Si l'aperçu de l'incident de sécurité ne s'affiche pas, cliquez sur **Aperçu** dans la barre de progression.
2. Dans la liste de choix Nom d'événement, sélectionnez un élément si plusieurs événements ont été utilisés.
3. Sélectionnez les ID d'événements dans la liste de choix Exemples d'ID d'événements notables.
4. Dans la liste de choix Exemples d'ID d'événements notables, sélectionnez un élément.

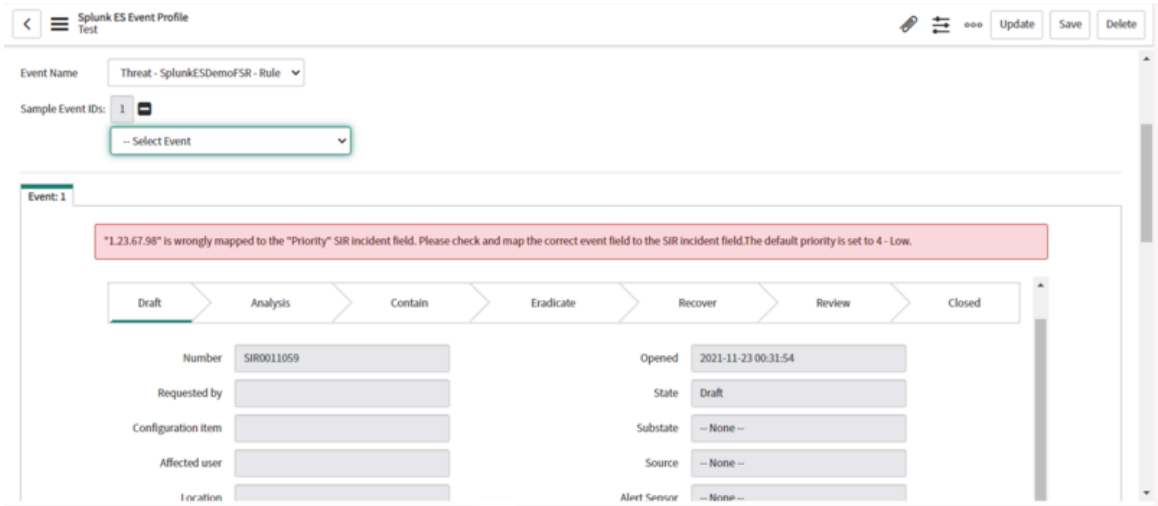


   L'incident de sécurité s'affiche. Ne modifiez aucune information dans les champs. Cette vue est en lecture seule et aucun enregistrement de cet incident de sécurité n'est enregistré.

5. Examinez le mappage de champs des valeurs d'événements notables de l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



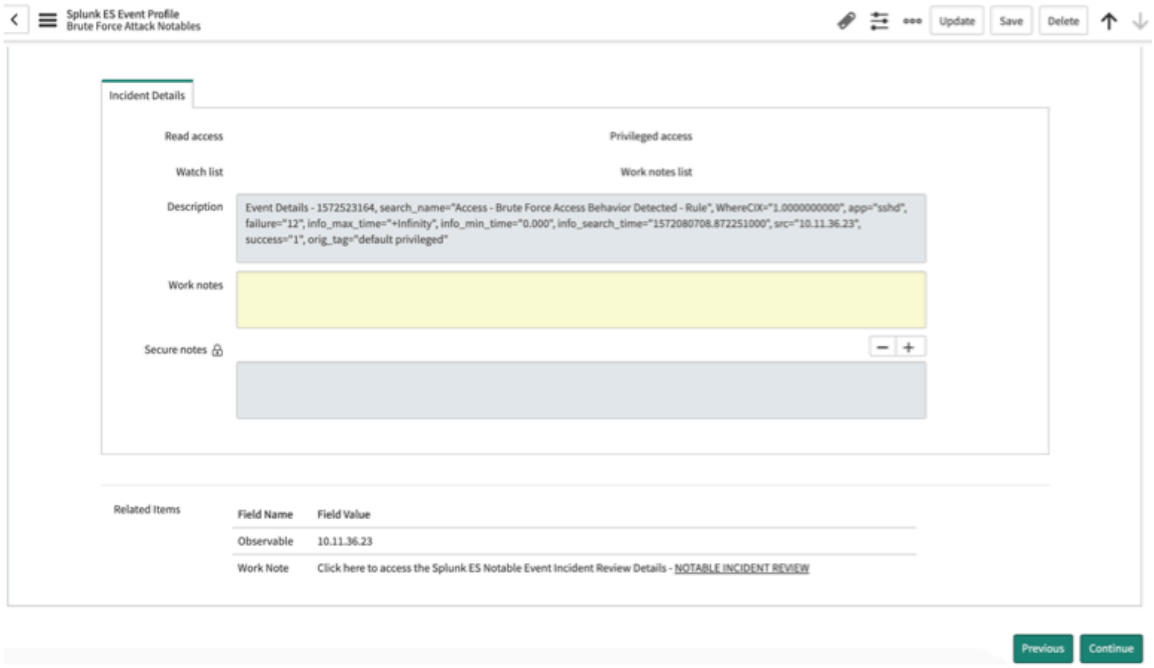
L'image précédente est un exemple d'aperçu avec une erreur de mappage. Dans cet exemple, une valeur de champ de l'événement notable n'a pas de valeur acceptable pour le champ de référence sur le formulaire d'incident SIR. Un message d'erreur s'affiche indiquant qu'une valeur d'entrée n'a pas été trouvée pour le champ Élément de configuration dans la base de ServiceNow® données de gestion des clients (CMDB). Par conséquent, la valeur de ce champ mappé n'apparaîtra pas sur le formulaire d'incident de sécurité SIR sans autre modification.

6. Pour résoudre cette erreur, cliquez sur **Mappage** dans la barre de progression.
7. Modifiez le mappage pour corriger les valeurs incorrectes ou renseigner les données manquantes.
8. Prévisualisez à nouveau le mappage et continuez à corriger les erreurs décrites dans les messages d'erreur.

La figure suivante est un exemple d'onglet Détails de l'incident dans la moitié inférieure d'un SIR incident de sécurité une fois que tous les messages d'erreur ont été résolus. Pour cet exemple, les champs Description et Notes de travail ont été mappés, et ces champs sont renseignés avec les valeurs des paires de valeurs extraites des échantillons d'événements Splunk Enterprise Security notables. Le premier champ Notes de travail n'a pas de valeur. Ce champ a été laissé vide sur la grille de mappage lors de l'étape de mappage. Les champs Note de travail supplémentaires qui ont des valeurs ont été ajoutés à la section de mappage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Une fois que vous avez corrigé les erreurs et vérifié que les champs sont comme vous le souhaitez, choisissez une option pour continuer.

Option	Description
Continuer	Le formulaire de planification s'affiche pour les profils avec des événements notables planifiés. **La planification** est sélectionnée dans la barre de progression.
Terminer	Pour les profils configurés pour le transfert manuel d'événements, cliquez sur **Terminer**. Il n'existe aucune étape de planification pour les profils avec des données d'événement qui sont exportés sur demande directement depuis la Splunk Enterprise Security console.
Mettre à jour	Vos données sont enregistrées et vous revenez à la liste des profils d'événement Splunk .
Précédent	L'étape Mappage s'affiche dans la barre de progression.
Supprimer	Supprimez ce profil d'événement pour afficher la liste des profils d'événement Splunk .

Que faire ensuite

Si aucun message d'erreur n'est affiché et que vous êtes satisfait du mappage de champs sur l'incident de sécurité, l'étape suivante consiste à Planifier et récupérer les alertes pour l'intégration Splunk Enterprise Event Ingestion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Planifier et récupérer les événements notables nouveaux et mis à jour pour l'intégration d'ingestion d'événements Splunk Enterprise Security

Pour les profils d'ingestion d'événements notables automatisés, cette étape est requise dans la configuration du profil d'événement. Au cours de cette étape, vous pouvez vérifier les paramètres par défaut pour la récupération des événements notables ou modifier la planification si nécessaire. Cette étape vous permet également de récupérer les événements historiques notables à l'aide d'une plage de dates.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Pour les profils d'ingestion automatisée d'événements notables, vous choisissez si vous souhaitez ingérer tous les événements notables historiques pendant l'étape de planification. Vous choisissez également la fréquence à laquelle vous interrogerez les événements notables futurs nouveaux et les événements notables mis à jour qui correspondent à la configuration du profil d'alerte.

Pour les profils d'ingestion automatisée d'événements notables, avant que le profil ne soit activé, vous vérifiez et modifiez la planification et la récupération des alertes. Il s'agit d'une étape nécessaire pour tout le processus de configuration de profil d'événement pour les profils d'alerte planifiée.

Vous configurez ces intervalles d'interrogation par profil. Les différents intervalles d'interrogation peuvent affecter les performances de l'intégration Splunk de l'ingestion d'événements. Lors de la planification, vous préférerez peut-être trouver un équilibre entre la réduction de la surcharge d'interrogation sur le serveur et le Splunk Enterprise Security désir d'être averti dès que possible lorsqu'un événement notable est créé ou mis à jour. Une valeur par défaut de cinq minutes est définie pour n'importe quel profil, mais vous préférez peut-être modifier ce paramètre à une minute si nécessaire.

Extraction d'événements notables nouveaux et mis à jour

Lorsque la planification d'interrogation est définie, la tâche planifiée extrait les événements notables nouveaux et mis à jour qui ont été extraits précédemment, mais qui ne répondent pas aux critères de filtrage des incidents. Cela vous donne la possibilité de créer des incidents basés sur des critères qui peuvent ne pas être présents lors de la création d'un événement notable pour la première fois, mais qui deviennent disponibles après une mise à jour (par exemple, pendant la phase d'enquête). Une fois qu'un incident a été créé pour un événement notable spécifique, ses mises à jour ultérieures sont ignorées, car il est prévu que l'incident notable soit maintenant traité comme un incident de sécurité actif ServiceNow® . Toutefois, tous les autres notables qui ont été précédemment ingérés mais qui n'ont pas réussi à répondre aux critères de génération d'incidents continueront d'être extraits et vérifiés par rapport aux critères de génération d'incidents jusqu'à ce qu'ils fassent partie d'un incident actif.

Procédure

1. Si la page Planification de la barre de progression ne s'affiche pas, sélectionnez **Planification**.
2. Choisissez-en un pour planifier comment et quand les événements notables sont extraits de la Splunk Enterprise Security console.

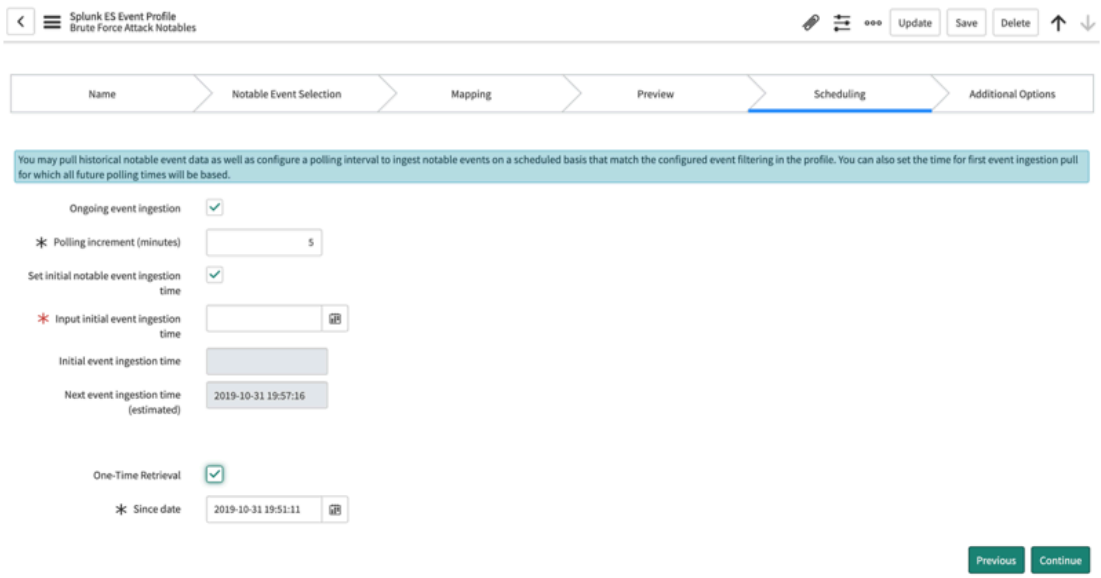
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
◦ Champ d’ingestion d’événements en cours sélectionné ◦ Champ Récupération ponctuelle effacé	Événement en cours En fonction du paramètre par défaut, l’instance ServiceNow AI Platform extrait du Splunk Enterprise Security serveur les événements notables nouveaux et mis à jour toutes les cinq minutes. Les incidents de sécurité sont créés si des événements notables sont détectés et que les critères de filtrage de génération d’incidents sont mis en correspondance. Pour équilibrer le désir d’obtenir les données les plus récentes, le paramètre par défaut est de cinq minutes. Toutefois, cette valeur peut être réduite à une minute si nécessaire.
◦ Champ Événement notable en cours effacé ◦ Champ de récupération ponctuelle sélectionné	Récupération ponctuelle Utilisez cette configuration si vous souhaitez une extraction ponctuelle pour ingérer des événements historiques notables. Lorsque ce paramètre est configuré, un profil est utilisé une fois pour récupérer des événements notables à partir d’événements historiques basés sur une plage de dates. À droite du champ Depuis la date, cliquez sur l’icône Calendrier. Dans le calendrier qui s’affiche, sélectionnez la date à laquelle vous souhaitez commencer à extraire des alertes. À partir de la valeur Depuis la date, les événements notables sont récupérés jusqu’à la date actuelle. Notez que vous pouvez revenir jusqu’à sept jours en arrière à partir de la date actuelle. Cette fonctionnalité n’est pas destinée à récupérer des quantités importantes d’événements Splunk Enterprise Security historiques pour des raisons d’archivage, mais plutôt un nombre minimal d’événements en cours qui sont activement traités au moment de l’activation du profil. Une fois les événements notables extraits, ce paramètre ne récupère pas d’autres événements notables pour ce profil à partir de la date actuelle. Ce paramètre renseigne l’incident de sécurité avec tous les événements notables trouvés pour la plage que vous saisissez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Par exemple, pour planifier une heure d'ingestion d'événement notable initial, si vous avez un contrôle de sécurité quotidien Splunk qui s'exécute une fois par jour à 4 heures du matin, heure locale, vous pouvez configurer le profil d'événement notable correspondant dans votre ServiceNow AI Platform instance pour qu'il s'exécute à 4 h 05, heure locale, pour capturer immédiatement l'événement de défaillance de sécurité et créer un incident de sécurité. Saisissez `04 05 00` dans le champ Ingestion de l'événement initial. Dans le champ Incrémentation (minutes), saisissez `1 440` (24 heures) pour planifier la prochaine ingestion d'événement pendant 24 heures à compter de l'ingestion d'événement initiale. Le délai d'ingestion de l'événement initial et l'heure d'ingestion de l'événement suivant sont affichés dans les champs.

3. Pour configurer les paramètres de cet exemple, procédez comme suit.

   a. Une fois la page Planification affichée, cochez la case **Ingestion d'événements en cours** pour activer cette option.

   b. Dans le champ Incrémentation (minutes), saisissez `1 440` (24 heures).

   c. Cochez la case **Sélectionner l'ingestion d'événement initial** pour activer la modification des champs Ingestion d'événement initial et Ingestion d'événement suivant.

   d. Dans le champ Ingestion de l'événement initial, saisissez `04 05 00`.
   Dans le champ Ingestion d'événement suivante (estimée), l'heure de l'ingestion d'événement suivante s'affiche.

4. Cliquez sur l'un des éléments suivants pour poursuivre la configuration du profil.

Option	Description
Continuer	Le formulaire Options supplémentaires s'affiche. **Options supplémentaires** est sélectionnée dans la barre de progression. L'étape suivante consiste à mettre à jour les événements notables lorsque l'incident SIR est créé et/ou fermé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Mettre à jour	Vos données sont enregistrées et la liste des profils de sécurité d'événement s'affiche Splunk .
Précédent	Le formulaire de planification s'affiche.
Supprimer	Supprimez ce profil d'événement pour afficher la liste des profils d'événement Splunk Enterprise Security .

Automatiser les mises à jour et les clôtures d'événements notables en fonction de l'état de l'incident SIR

Les incidents de sécurité peuvent être créés et mis à jour après leur création grâce à une interface bidirectionnelle avec l'intégration Splunk Enterprise Security .

Avant de commencer

L'intégration Splunk Enterprise Security dispose d'une interface bidirectionnelle qui permet aux événements notables de créer des incidents de sécurité et de mettre à jour les événements notables après la création et/ou la clôture de l'incident de sécurité.

Les détails pertinents de l'incident comprennent le SIR numéro d'incident, le groupe d'affectation et l'URL SIR de l'incident. Cette section constitue la dernière partie de la configuration du profil qui fournit des options facultatives pour mettre à jour les Splunk Enterprise Security événements notables.

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

1. Si la page Options supplémentaires de la barre de progression ne s'affiche pas, sélectionnez **Options supplémentaires**.
2. Suivez les instructions ci-dessous pour terminer la configuration de la mise à jour des événements notables en fonction des mises à jour des incidents de sécurité.

Option ou champ	Description
Mise à jour des événements notables lors de la création d'un incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour l'état de l'événement notable et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'événement notable. Cela peut se produire à la fois pour les événements notables déclencheurs initiaux qui créent l'incident de sécurité, ainsi que pour les événements agrégés.
Mise à jour de statut de l'événement notable initial	Vous devez sélectionner dans le menu une option d'état qui affiche toutes les valeurs d'état disponibles récupérées à partir du Splunk Enterprise Security serveur. Cela peut inclure un état créé personnalisé, tel que ServiceNow - Affecté, comme illustré dans la capture d'écran ci-dessous. Sélectionnez la valeur d'état à définir pour tous les événements notables lorsqu'un incident de sécurité est créé pour un évé-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

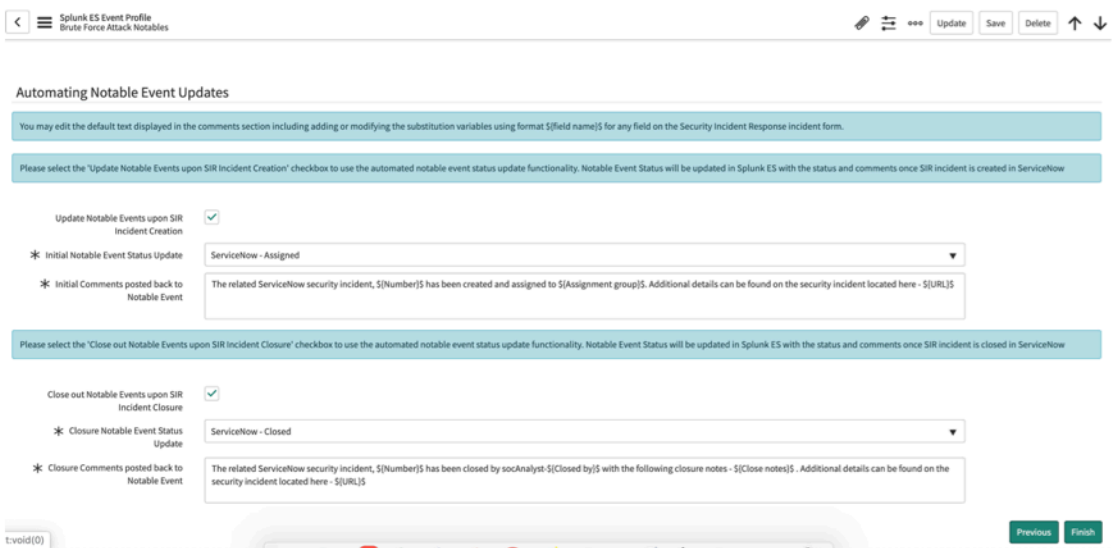
Option ou champ	Description
	nement notable ingéré. Cela inclut les notables qui créent de nouveaux incidents et les notables qui sont ingérés et agrégés à un incident ouvert existant.
Commentaires initiaux renvoyés à l'événement notable	Outre la mise à jour de la valeur d'état notable, vous pouvez également publier des commentaires sur l'historique d'examen des incidents d'événements notables. Comme indiqué dans les instructions, vous pouvez modifier le texte par défaut affiché dans la section des commentaires, y compris ajouter ou modifier les variables de substitution en utilisant le format ${nom du champ}$ pour n'importe quel champ du formulaire d'incident Réponse aux incidents de sécurité .
Fermer les événements notables lors de la fermeture d'un incident SIR	Sélectionnez cette option si vous souhaitez mettre à jour l'état de l'événement notable et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est fermé à partir de l'événement notable. Cela se produit à la fois pour les événements notables déclencheurs initiaux qui créent l'incident de sécurité et pour les événements agrégés.
Mise à jour de statut de l'événement notable de la fermeture	Vous devez sélectionner une option d'état dans le menu Liste qui affiche toutes les valeurs d'état disponibles récupérées à partir du Splunk Enterprise Security serveur. Cela peut inclure un état créé personnalisé, tel que ServiceNow - Affecté, comme illustré dans la capture d'écran ci-dessous. Sélectionnez la valeur d'état à définir pour tous les événements notables lorsqu'un incident de sécurité est créé pour un événement notable ingéré. Cela inclut les notables qui créent de nouveaux incidents ainsi que les notables qui sont ingérés et agrégés à un incident ouvert existant.
Commentaires de fermeture publiés dans Événement notable	Outre la mise à jour de la valeur d'état notable, vous pouvez également publier des commentaires de fermeture dans l'historique d'examen des incidents d'événements notables. Comme indiqué dans les instructions, vous pouvez modifier le texte par défaut affiché dans la section des commentaires, y compris ajouter ou modifier les variables de substitution en utilisant le format ${nom du champ}$ pour n'importe quel champ du formulaire d'incident Réponse aux incidents de sécurité .
Mettre à jour l'activité d'automatisation SIR avec commentaires événement Splunk	Option permettant de mettre à jour vos commentaires d'événement Splunk dans l'activité d'automatisation SIR . Le commentaire dans l'activité d'automatisation SIR apparaît avec le préfixe `Commentaire de Splunk`.
Mettre à jour les commentaires Splunk avec les notes de travail SIR	Option permettant de mettre à jour vos SIR notes de travail dans les commentaires d'événement Splunk. Le commentaire dans l'événement Splunk apparaît avec le préfixe `Commentaire de ServiceNow`.

Traduction automatique

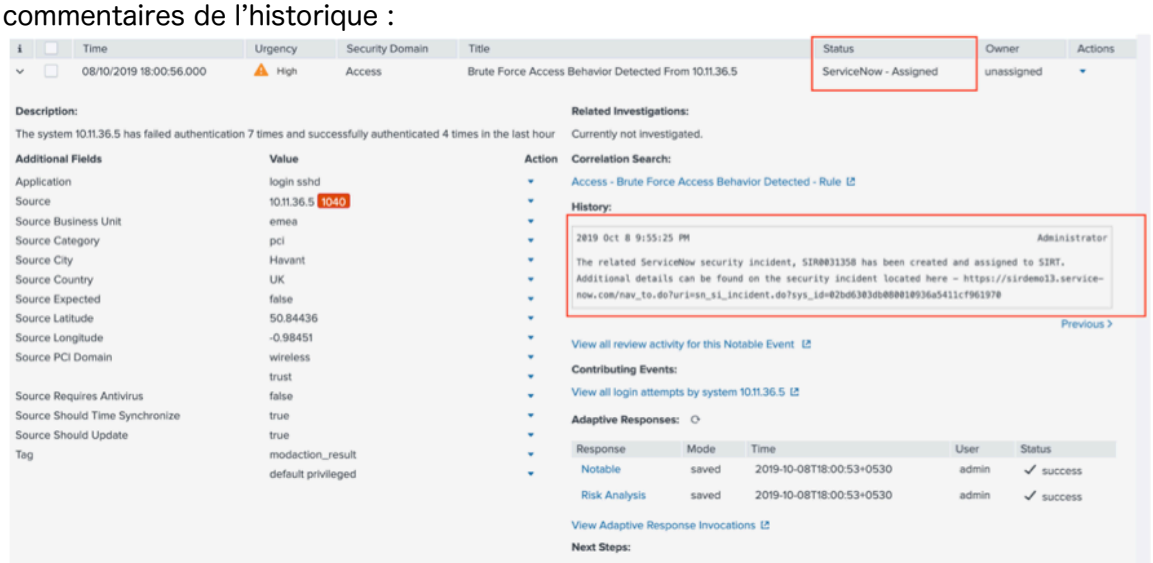
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Terminer** pour terminer la configuration.
   Une boîte de dialogue de confirmation s'affiche. Vous avez terminé avec succès l'installation et la configuration de l'intégration. Activez ce profil pour extraire des événements notables de la Splunk Enterprise Security console en fonction de votre planification. Il existe une limite de 1 000 incidents de sécurité pouvant être créés dans une période de 24 heures. Jusqu'à 100 événements notables sont par alerte déclenchée. Les événements notables suivants sont ignorés une fois les limites atteintes.

   L'image suivante montre l'onglet Options supplémentaires avec les valeurs par défaut renseignées :



   Lorsque la configuration des options supplémentaires est activée, l'examen de l'incident d'événement notable affiche le changement de statut et une mise à jour des commentaires de l'historique :



Configurer un profil pour le transfert manuel d'événements

Selon le profil défini, Splunk ES les événements notables sont transmis manuellement sous forme d'événements notables discrets dans l'environnement Opérations de sécurité de votre ServiceNow AI Platform instance.

Pour configurer un profil pour le transfert manuel d'événements notables :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Section
Créer un profil d'événement	Reportez-vous à la rubrique Créer des profils pour les événements transférés manuellement.
Mapper les champs d'événements notables	Reportez-vous à la rubrique Mappage des champs d'événement notable pour l'intégration Splunk Enterprise Security.
Créer des mappages personnalisés	Reportez-vous à la rubrique Créer des mappages pour Splunk ES l'examen des incidents d'événements notables et les détails de l'événement de contribution (transfert manuel).
Prévisualiser l'incident de sécurité	Reportez-vous à la rubrique Prévisualiser l'incident de sécurité pour l'intégration d'ingestion d'événements Splunk Enterprise Security.
Configurer votre environnement pour l'ingestion Splunk manuelle	Reportez-vous à la rubrique Configurer votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables.
Automatiser les mises à jour et les clôtures d'événements notables en fonction de l'état de l'incident SIR	Reportez-vous à la rubrique Automatiser les mises à jour et les clôtures d'événements notables en fonction de l'état de l'incident SIR.

Créer des profils pour les événements transférés manuellement

Vous pouvez configurer un profil pour les événements transférés manuellement.

Avant de commencer
Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Procédure

Pour créer un profil qui prend en charge le transfert manuel d'événements, procédez comme suit.

Pour les événements que vous transférez à la demande à partir de votre Splunk Enterprise Security console, vous pouvez baser le mappage de champs individuel sur n'importe quel profil existant. Vous pouvez également créer une grille de mappage pour les données de pièce jointe exportées. Les événements que vous transférez manuellement ne sont pas planifiés dans le profil d'événement.

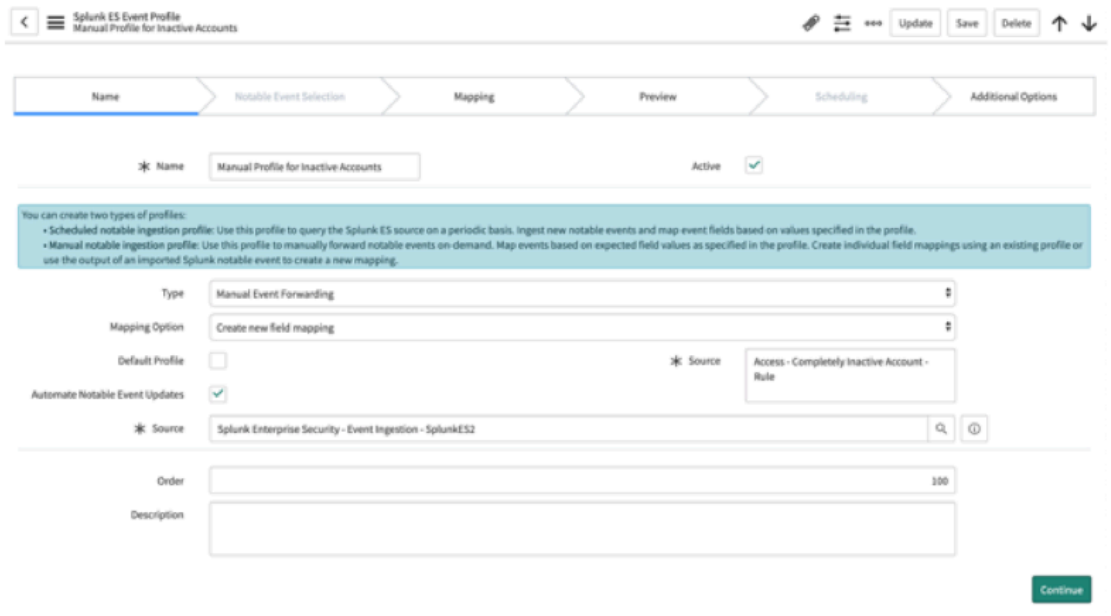
a. Si ce n'est pas déjà fait, dans la liste de choix du champ Type, sélectionnez **Transfert d'événements manuel.**

b. Dans le champ Option de mappage qui s'affiche, dans la liste de choix, choisissez une option de mappage pour continuer.

Reportez-vous aux figures et tableaux suivants pour plus d'informations sur les options de mappage disponibles dans la liste de choix Options de mappage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Créer une nouvelle option de mappage de champs

Option ou champ	Description
Créer une option de mappage de champs	Nouveau mappage de champs pour votre événement. Si vous n'avez pas de mappage de champs similaire au profil que vous créez, sélectionnez cette option pour créer une nouvelle carte.
Profil par défaut	Profil de transfert d'événements par défaut pour tous les Splunk événements. La valeur par défaut est effacée (désactivée). Lorsque cette option est activée, ce profil devient le profil par défaut pour le transfert manuel d'événements. Ce profil est utilisé lorsqu'il n'y a aucune correspondance sur la source de l'événement transféré manuellement. Il devient le profil par défaut pour tous les événements de sources inconnues. Le champ Source n'est pas disponible si l'option de profil par défaut est activée.
Source (champ Événement notable)	Il s'agit d'un champ qui définit généralement la règle de corrélation qui a déclenché le notable, par exemple, les attaques par force brute. Ce champ n'est pas disponible si l'option de profil par défaut est activée. S'il est disponible, ce champ permet un mappage de champs d'événements uniques sur les champs d'incident de sécurité en

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

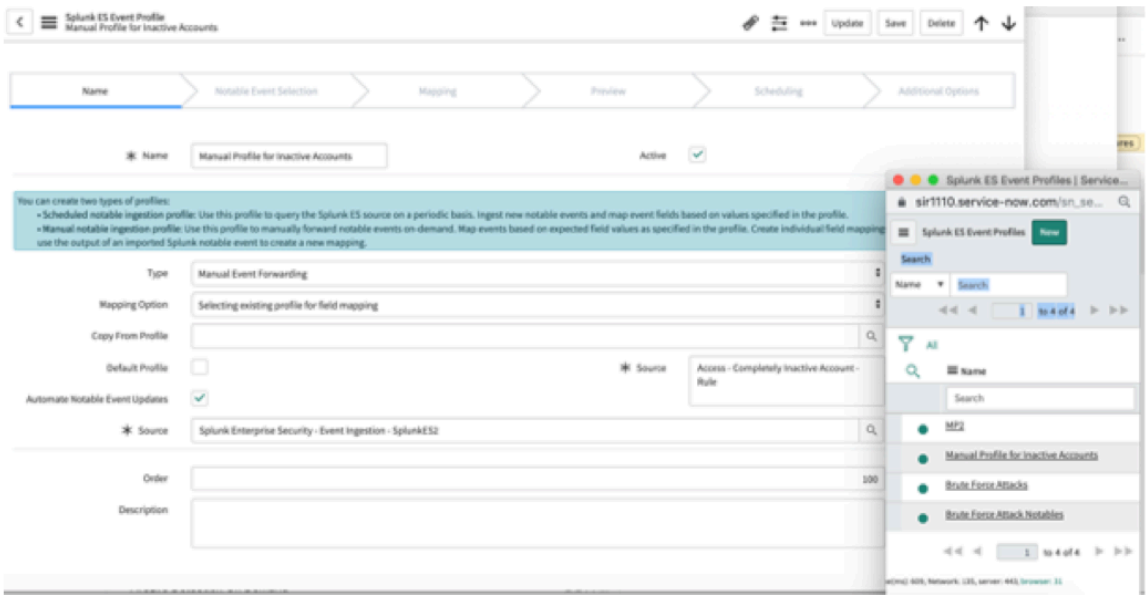
Option ou champ	Description
	fonction de la règle de corrélation Splunk qui est généralement différente pour différents types d'événements. Si vous souhaitez gérer différentes règles de corrélation séparément, vous pouvez créer différents profils d'événement de profil en fonction de la règle de corrélation pour satisfaire à cette exigence.
Automatiser les mises à jour des événements notables	Cochez cette case si vous souhaitez mettre à jour l'état de l'événement notable et ajouter des commentaires supplémentaires lorsqu'un incident SIR est créé à partir de l'événement notable et/ou lorsque l'incident SIR est fermé. Cela se produit à la fois pour les événements notables déclencheurs initiaux qui créent l'incident SIR, ainsi que pour les événements agrégés.
Source (Splunk serveur)	Serveur Splunk que vous avez configuré comme source des événements notables. Si plusieurs serveurs sont Splunk configurés, sélectionnez le serveur approprié pour les types d'événements notables qui seront mis à jour pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Laissez ce paramètre par défaut. Si vous avez créé un grand nombre de profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow dans le profil avec le numéro le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

Pour un profil avec un nouveau mappage de champs, vérifiez que vous avez saisi une valeur dans le champ Type de source et cliquez sur **Continuer** pour passer à l'étape de mappage de la configuration.

Pour un profil avec un mappage de champs existant, reportez-vous à la figure et au tableau suivants pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Sélectionner un profil existant pour l'option de mappage de champ

Option ou champ	Description
Sélectionner un profil existant pour le mappage de champs	Réutilisez un mappage de champ existant pour votre nouveau profil d'événement notable. Le champ Copier à partir du profil s'affiche. Suivez ces étapes pour copier un mappage de champs existant pour ce profil. **i.** À gauche du champ Copier à partir du profil qui s'affiche, cliquez sur l'icône de recherche. **ii.** Dans la liste Profils d'événements ES qui s'affiche Splunk , cliquez sur le nom du profil qui contient la carte que vous souhaitez copier. Le nom du profil s'affiche dans le champ Copier à partir du profil.
Profil par défaut	Profil de transfert d'événements par défaut pour tous les événements notables avec une Splunk source sans correspondance. La valeur par défaut est effacée (désactivée). Lorsque cette option est activée, ce profil devient le profil par défaut pour le transfert manuel d'événements. Le champ Source n'est pas disponible si l'option de profil par défaut est activée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option ou champ	Description
Source (champ Événement notable)	Il s'agit d'un champ qui définit généralement la règle de corrélation qui a déclenché le notable, par exemple, les attaques par force brute. Ce champ n'est pas disponible si l'option de profil par défaut est activée. S'il est disponible, ce champ permet un mappage de champs d'événements uniques sur les champs d'incident de sécurité en fonction de la règle de corrélation Splunk qui est généralement différente pour différents types d'événements. Si vous souhaitez gérer différentes règles de corrélation séparément, vous pouvez créer différents profils d'événement de profil en fonction de la règle de corrélation pour satisfaire à cette exigence.
Automatiser les événements notables	Cochez cette case si vous souhaitez mettre à jour l'état de l'événement notable et ajouter des commentaires supplémentaires lorsqu'un incident de sécurité est créé à partir de l'événement notable ou lorsque l'incident de sécurité est fermé. Cela se produit à la fois pour les événements notables déclencheurs initiaux qui créent l'incident de sécurité et pour les événements agrégés.
Source (Splunk serveur)	Splunk Serveur ou extrémité de recherche que vous avez configuré comme source des événements notables. Si plusieurs serveurs sont Splunk configurés, sélectionnez le serveur approprié pour les types d'événements notables qui seront mis à jour pour le profil. Vous devez saisir une valeur.
Ordre	La valeur par défaut est 100. Laissez ce paramètre par défaut. Si vous avez créé plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le workflow dans le profil avec le numéro le plus bas a la priorité la plus élevée.
(Facultatif) Description	Texte pour vous aider à distinguer ce profil des autres profils.

Au bas du formulaire de sélection d'un mappage existant pour votre profil, cliquez sur **Terminer** pour terminer la configuration du profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer des mappages pour Splunk ES l'examen des incidents d'événements notables et les détails de l'événement de contribution (transfert manuel)

Au cours de l'étape de mappage de champs d'événements notables, vous mappez les champs d'événements individuels des événements notables aux champs d'un ServiceNow AI Platform Réponse aux incidents de sécurité incident de sécurité (SIR).

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Mappez jusqu'à cinq événements notables de la colonne Ingestion d'échantillons d'événements notables à gauche du formulaire aux champs d'incident de sécurité de la colonne Mappage de champ d'incidents SIR à droite.

Créez des mappages personnalisés en ajoutant ou en supprimant des champs sur la grille de mappage sur le côté droit du formulaire. Les champs par défaut, qui sont généralement des champs importants à renseigner sur le formulaire d'incident SIR, s'affichent. Toutefois, ces champs peuvent être supprimés et tous les champs supplémentaires peuvent être affichés à l'aide des boutons + et -. Créez des cartes personnalisées en ajoutant ou en supprimant des champs sur la grille de mappage située à droite du formulaire. La personnalisation des champs vous permet de mapper Splunk les champs qui ne sont pas affichés sur la grille de mappage par défaut de l'incident SIR de sécurité.

Procédure

1. Si le formulaire de mappage n'est pas affiché, cliquez sur **Mappage** dans la barre de progression.
2. Suivez ces étapes pour charger les données de la pièce jointe dans votre ServiceNow AI Platform® instance.

   a. Si vous n'êtes pas déjà connecté, connectez-vous à votre Splunk Enterprise console.

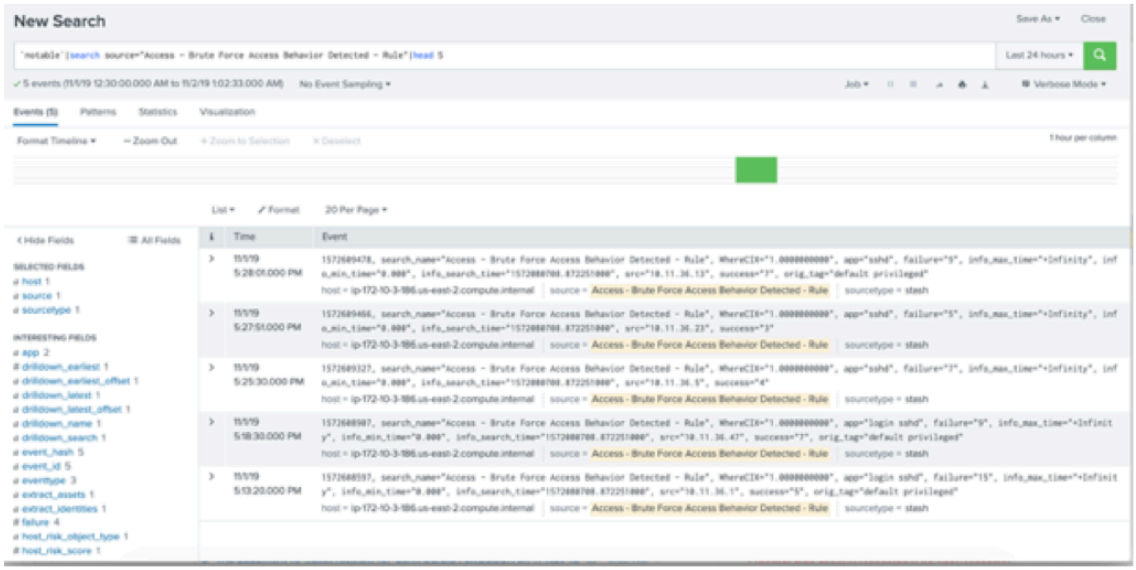
   b. Accédez à l'onglet Rechercher et entrez un nom pour une recherche qui contient les données d'événements notables que vous souhaitez exporter.
   Un exemple de format de recherche pour récupérer des événements notables pour la règle de corrélation du comportement d'accès en force brute serait le suivant : 'notable'|search source="Access - Comportement d'accès en force brute détecté - Règle ».

   c. Développez l'événement notable et, dans la colonne Champ, sélectionnez les champs que vous souhaitez importer.

   Ces champs correspondent aux paires champ-valeur qui sont exportées et affichées sur la page de mappage de votre ServiceNow AI Platform® instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

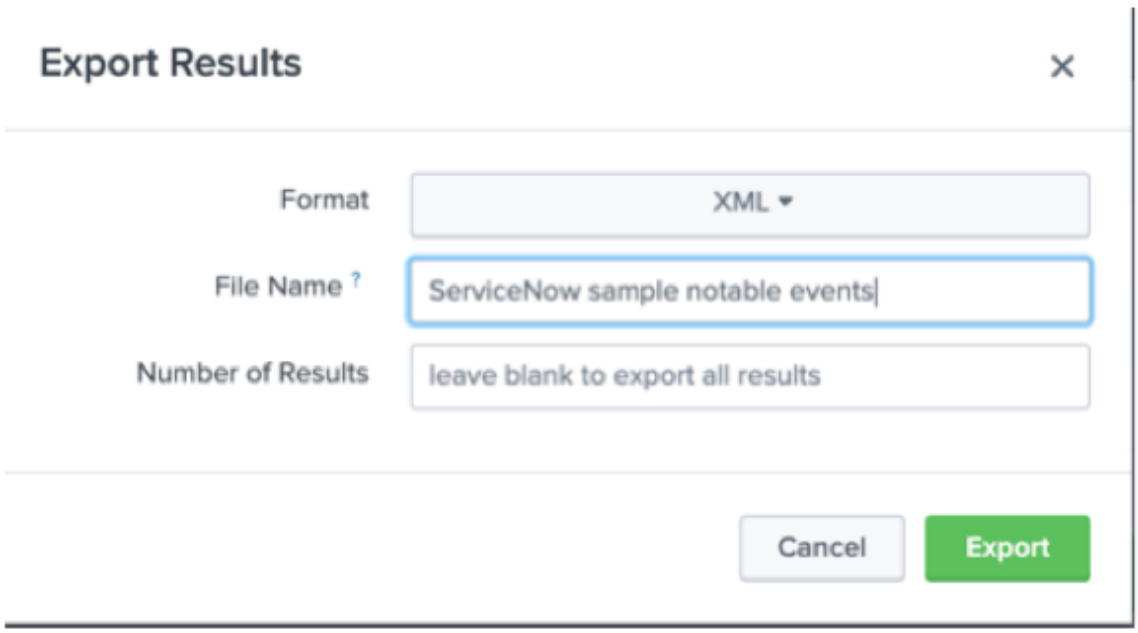


d. Dans votre Splunk Enterprise console, en haut à droite de la page de recherche, cliquez sur l'icône **Exporter** .

e. Dans la liste de choix du champ Format de la boîte de dialogue qui s'affiche, cliquez sur **Format XML**.

f. Facultatif : Entrez un nouveau nom de fichier.

g. Cliquez sur **Exporter**.



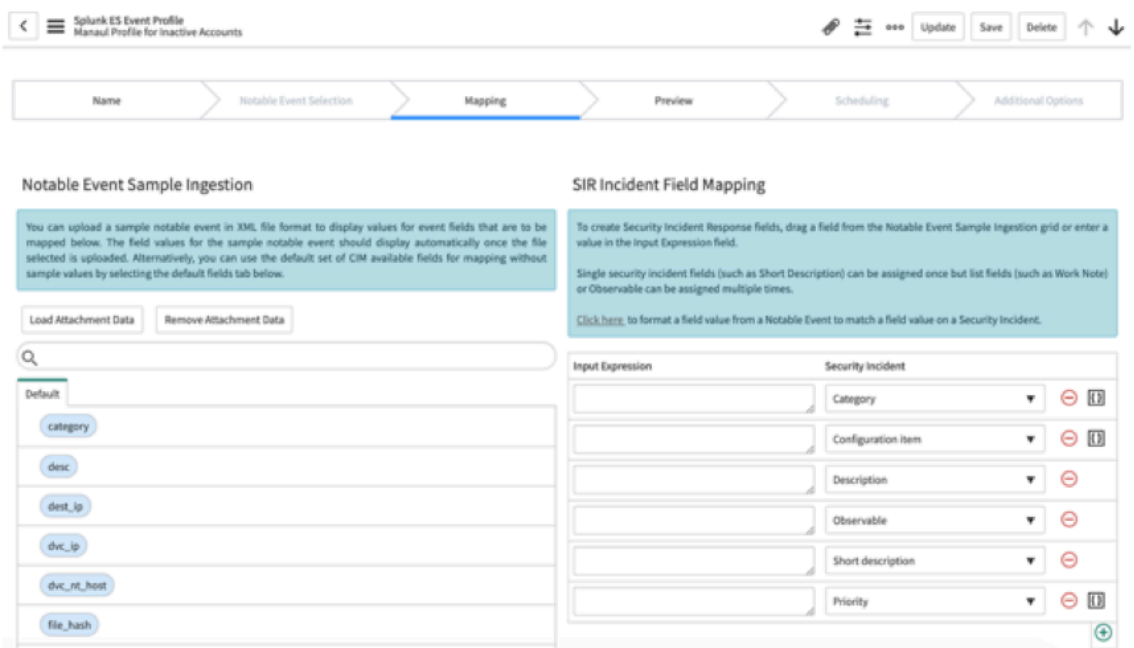
Le fichier XML de l'événement notable exporté Splunk doit maintenant être téléchargé sur votre ServiceNow AI Platform® instance.

h. Si la page Mappage n'est pas déjà affichée dans votre ServiceNow AI Platform® instance, cliquez sur **Mappage** dans la barre de progression.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Dans la colonne Ingestion d'échantillons d'événements notables, cliquez sur **Charger les données de la pièce jointe**.



j. Dans la boîte de dialogue qui s'affiche, cliquez sur **Choisir des fichiers** et accédez au fichier .xml que vous avez exporté, puis cliquez sur **Ouvrir**.
Une fois que vous avez cliqué pour charger les données de pièce jointe pour les événements transférés manuellement, les champs d'événements Splunk ES notables sont renseignés sur le côté gauche du formulaire. Il s'agit des valeurs de champ que vous mappez aux champs d'incident de sécurité du côté Mappage du champ d'incident Sir du formulaire.
Les paires de valeurs des champs que vous avez exportés pour l'événement s'affichent sur le côté gauche du formulaire de mappage.

3. Suivez les étapes 5 à 10 de la Créer des mappages pour Splunk ES l'examen des incidents d'événements notables et les détails de l'événement de contribution (ingestion planifiée) section.

Configurer votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables

Installez et configurez le ServiceNow module complémentaire Security Operations Event Ingestion for application dans Splunk Enterprise Security votre console d'entreprise ou votre Splunk instance Splunk Cloud si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise Security console pour cette intégration.

Avant de commencer

L'installation et la configuration du module complémentaire d'ingestion d'événements Security Operations pour l'application ServiceNow dans Splunk Enterprise Security votre console d'entreprise ou votre Splunk instance Splunk Cloud sont facultatives.

Vérifiez que vous avez installé l'application pour cette intégration avant ServiceNow Store d'installer le module d'extension du module d'extension à partir de splunkbase requis pour l'ingestion manuelle d'événements. Si vous n'avez pas installé l'application pour l'intégration à partir de , ServiceNow Store consultez Installer et configurer Splunk Enterprise Security l'intégration de l'ingestion d'événements notables et suivez les instructions pour l'installer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : Splunk Enterprise Security administrateur

Pourquoi et quand exécuter cette tâche

Si vous souhaitez exporter des événements manuellement et à la demande à partir de votre Splunk Enterprise console pour l'intégration, téléchargez, installez et configurez le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise Security from splunkbase dans votre Splunk Enterprise Security console. Ce ServiceNow module complémentaire d'extension est nécessaire pour que des incidents de sécurité puissent être créés à partir d'événements exportés manuellement dans votre ServiceNow AI Platform instance. Ce ServiceNow module complémentaire d'ingestion d'événements Security Operations pour Splunk Enterprise Security l'application est disponible sur splunkbase .

Pour le transfert manuel d'événements, vous pouvez identifier jusqu'à deux points de terminaison différents ServiceNow AI Platform (instances) dans votre Splunk Enterprise Security console. Vous transférez manuellement les événements au ou aux points de terminaison pour créer des incidents de sécurité. Par exemple, vous pouvez spécifier à la fois une instance intermédiaire (développement) et une instance de production. En spécifiant des instances distinctes et en nommant les workflows primaire et secondaire pour chaque instance, vous pouvez choisir où vous souhaitez transférer différents événements.

Procédure

1. Si vous n'avez pas encore installé le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise Security, procédez comme suit pour l'installer et le configurer.

   a. Accédez à splunkbase .

   b. Recherchez le module complémentaire d'ingestion d'événements ServiceNow Opérations de sécurité Security Operations pour Splunk Enterprise Security.

   > **Remarque :** Vérifiez que vous avez sélectionné ServiceNow Opérations de sécurité le module complémentaire d'ingestion d'événements pour Splunk Enterprise Security. D'autres ServiceNow modules complémentaires sont affichés dans cette liste. Ces modules complémentaires sont destinés à différentes ServiceNow Splunk intégrations et ne sont pas nécessaires pour cette intégration.

   c. Téléchargez l'application.

   d. Ouvrez votre Splunk Enterprise Security compte.

   e. Sur la page Applications, cliquez sur l'icône en forme d'engrenage ou sur le raccourci **Gérer les applications** dans la liste déroulante du menu.

   f. En haut à gauche de la page Applications qui s'affiche, cliquez sur **Installer l'application à partir d'un fichier**.

   g. Cliquez sur **Choisir un fichier**, sélectionnez ServiceNow le module complémentaire Security Operations Event Ingestion pour Splunk Enterprise Security, puis cliquez sur **Charger**.

   h. Si vous y êtes invité, redémarrez Splunk Enterprise.
   Le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise Security est installé dans votre Splunk Enterprise Security console. L'étape suivante pour configurer l'addon.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Pour configurer l’additif, procédez comme suit.

a. Dans Splunk Enterprise Security, cliquez **sur l’icône** en forme d’engrenage Applications ou **sur Gérer les applications** dans la liste déroulante du menu.

b. Dans la liste des applications qui s’affiche, dans la colonne **Actions** , cliquez sur **Configurer le module complémentaire d’ingestion d’événements**ServiceNow Opérations de sécurité pour Splunk Enterprise Security.

c. Remplissez le formulaire.

La figure suivante est un exemple de formulaire rempli dans votre Splunk Enterprise Security console.



Champ de la section Spécifier l’instance primaire ServiceNow	Description
Étiquette de l’action du workflow	Nom du workflow de ServiceNow AI Platform votre instance de production (principale). Ce nom est le nom d’une ServiceNow AI Platform instance que les utilisateurs qui surveillent Splunk les événements identifient comme instance primaire, par exemple, ServiceNow Ingestion d’événements (Production).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ de la section Spécifier l'instance primaire ServiceNow	Description
	La valeur par défaut pour ce champ est In–gestion d'événements ServiceNow (pro–duction). Dans votre Splunk Enterprise Security console, ce nom de workflow s'affiche pour l'ins–tance de production (primaire) dans la liste déroulante Actions d'événement dévelop–pée d'une recherche. Ce nom est le nom de votre instance de production. Vous pouvez modifier le nom.
URL	URL de l'instance ServiceNow AI Platform que vous avez saisie dans le champ d'étiquette Action du workflow précédent. Copiez l'URL dans votre navigateur et col–lez-la dans ce champ du formulaire.
Point de terminaison	Chemin de l'API de base. Pour plus d'informations, reportez-vous à la figure qui suit le tableau. Si vous n'avez pas de valeur pour le point de terminaison de votre ServiceNow AI Plat-form instance de production, procédez comme suit. **a.** Connectez-vous à votre ServiceNow AI Platform instance de production en tant qu'utilisateur avec le rôle d'administra–teur système (admin). **b.** Entrez les API REST basées sur un script dans le panneau de navigation. **c.** Une fois le panneau de navigation ac–tualisé, sélectionnez le module **API REST scriptées** qui s'affiche. **d.** Si l'ingestion d'événements n'est pas ré–pertoriée dans la colonne Nom de la liste des API REST scriptées qui s'affiche, sai–sissez Ingestion d'événements dans le champ de recherche en haut. **e.** Dans la colonne Chemin de l'API de base de la page actualisée, copiez cette valeur et collez-la dans le champ Point de ter–minaison du formulaire. Un exemple de chemin d'accès de l'API de base est /api/sn_sec_splunk_v2/event_ingestion.
Nom d'utilisateur	Nom d'utilisateur de votre ServiceNow AI Platform instance. Ce nom est le nom d'utilisateur de l'ins-tance ServiceNow AI Platform dans laquelle vous avez affecté un utilisateur avec le rôle (sn_sec_s-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

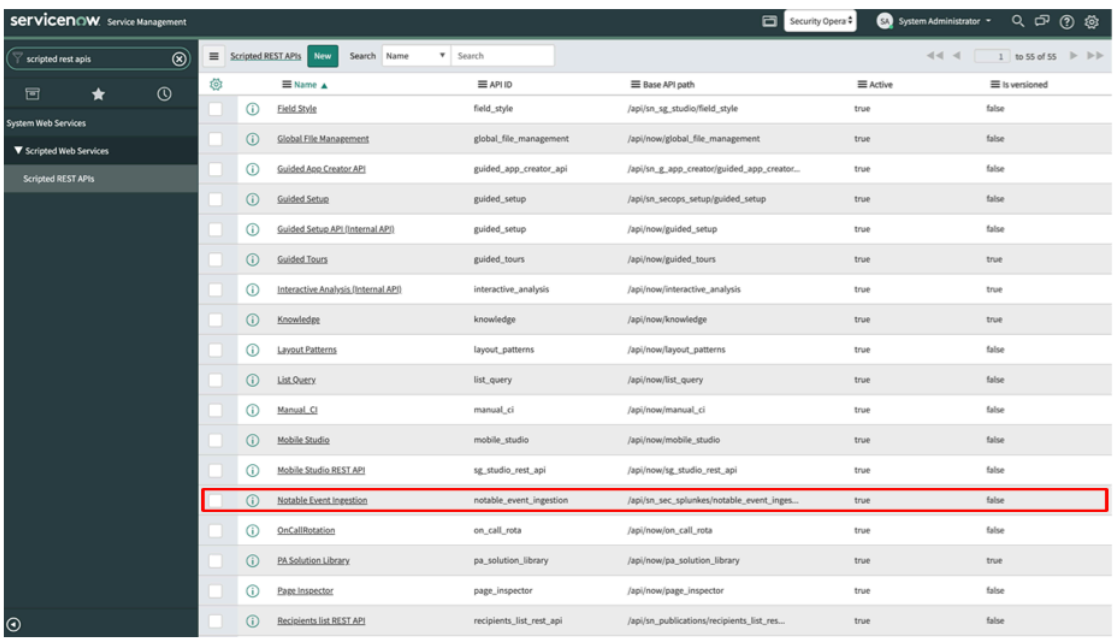
Champ de la section Spécifier l'instance primaire ServiceNow	Description
	plunk_v2.api_account_access) pour le transfert manuel d'événements. Pour plus d'informations sur l'affectation de ce rôle, reportez-vous à la section Configurer votre ServiceNow AI Platform instance pour l'intégration Splunk Enterprise Event Ingestion.
Mot de passe	Mot de passe de votre ServiceNow AI Platform instance. Ce mot de passe est le mot de passe de l'instance ServiceNow AI Platform dans laquelle vous avez affecté à un utilisateur le rôle (sn_sec_splunk_v2.api_account_access) pour le transfert manuel d'événements.
(Facultatif) Champs de la section Spécifier l'instance secondaire ServiceNow	Description Ces champs sont facultatifs. Vous n'êtes pas obligé de spécifier une instance secondaire.
Étiquette de l'action du workflow	Nom du workflow de ServiceNow AI Platform votre instance secondaire (intermédiaire). Ce nom est le nom d'une ServiceNow AI Platform instance que vos utilisateurs qui surveillent Splunk les événements identifient comme une instance secondaire, par exemple, ServiceNow Ingestion d'événements (Intermédiaire). Dans votre Splunk Enterprise Security console, ce nom de workflow est affiché pour l'instance intermédiaire (secondaire) dans la liste déroulante Actions d'événement développée d'une recherche. Cette ServiceNow AI Platform instance est votre instance intermédiaire. Vous pouvez modifier le nom.
URL	URL de l'instance ServiceNow AI Platform que vous avez saisie dans le champ Étiquette Action du workflow précédent pour l'instance secondaire ServiceNow AI Platform . Copiez l'URL dans votre navigateur et collez-la dans ce champ du formulaire.
Point de terminaison	Chemin de l'API de base. Cette valeur du chemin de l'API de base de votre instance secondaire est la même que celle du chemin de l'API de base de votre instance principale. Voir la figure précédente du formulaire pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ de la section Spécifier l'instance primaire ServiceNow	Description
Nom d'utilisateur	Nom d'utilisateur de votre ServiceNow AI Platform instance intermédiaire. L'utilisateur doit avoir le rôle (sn_sec_splunk_v2.api_account_access).
Mot de passe	Mot de passe de votre ServiceNow AI Platform instance intermédiaire. L'utilisateur doit disposer du rôle (sn_sec_splunkes.api_account_access).

La figure suivante est un exemple de la liste API REST scriptées dans votre ServiceNow AI Platform. La liste affiche l'emplacement de la valeur de point de terminaison d'une ServiceNow AI Platform instance que vous saisissez dans le formulaire dans le cadre de la configuration ServiceNow du module complémentaire Security Operations Event Ingestion for extension dans Splunk Enterprise Security votre Splunk Enterprise Security console.



3. Dans le formulaire de configuration de votre Splunk Enterprise Security console, cliquez sur **Enregistrer** pour enregistrer vos modifications.

   Après quelques instants, en haut à gauche du formulaire de votre Splunk Enterprise Security console, un message s'affiche indiquant que l'enregistrement a été mis à jour avec succès.

   Une fois le formulaire enregistré, les noms (étiquettes d'action de workflow) de vos ServiceNow AI Platform instances que vous avez créées dans le formulaire sont disponibles dans la liste de choix Actions d'événement sur un événement sélectionné d'une recherche dans votre Splunk Enterprise Security console.

Que faire ensuite

Si vous n'avez pas encore enregistré les recherches dans votre Splunk Enterprise Security console, l'étape suivante consiste à enregistrer les recherches sous forme d'alertes dans votre Splunk Enterprise Security console.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Copier un profil d'événement pour l'intégration d'ingestion d'événements Splunk Enterprise Security

Copiez un profil existant et ses paramètres associés au lieu de créer de nouveaux profils. Si vous créez plusieurs profils et que vous souhaitez réutiliser les paramètres d'un profil existant, vous préférerez peut-être copier les profils d'alarme pour gagner du temps.

Avant de commencer

Rôle requis : sn_si.ingestion_profile_admin

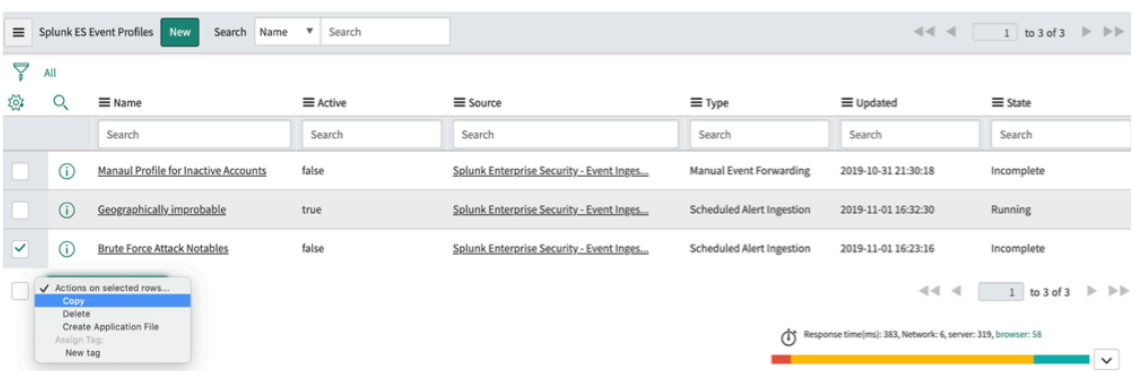
Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

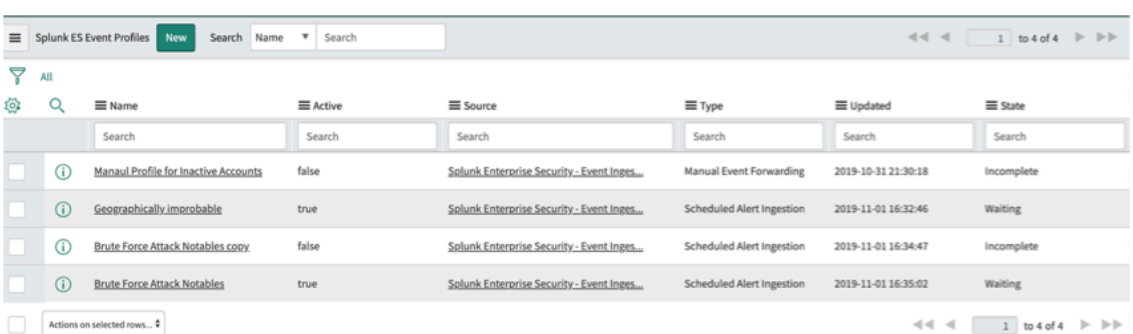
Si vous copiez un profil, le nom du profil est initialement modifié pour éviter les profils en double. En outre, le profil copié est désactivé (faux) afin qu'il ne soit pas activé accidentellement avant de terminer la configuration. Copiez les profils et utilisez les cartes existantes pour les incidents de sécurité que vous avez déjà prévisualisés et vérifiés.

Procédure

1. Accédez à la **Tous** > **Intégration Splunk** > **Profil d'événement Splunk**.
2. Dans la liste Profils d'événements Splunk qui s'affiche, sélectionnez un profil que vous souhaitez copier et, dans la liste de choix Actions sur les lignes sélectionnées, cliquez sur **Copier**.



Le profil est copié et affiché dans la liste. La copie contient tous les paramètres du profil d'origine, y compris la configuration du mappage et de la planification. Le nom du profil contient une copie. Bien que le profil d'origine soit activé (vrai), la copie est désactivée à ce stade (faux). Vous préférez peut-être modifier les valeurs du profil copié et le renommer afin que les paramètres de configuration s'appliquent au nouveau profil selon les besoins.



Vous avez copié avec succès les paramètres d'un profil existant vers un nouveau profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Vous êtes invité à activer le nouveau profil une fois l'étape de configuration terminée.

Utiliser l'éditeur de script pour formater les valeurs d'alerte pour l'intégration d'ingestion d'événements Splunk Enterprise Security

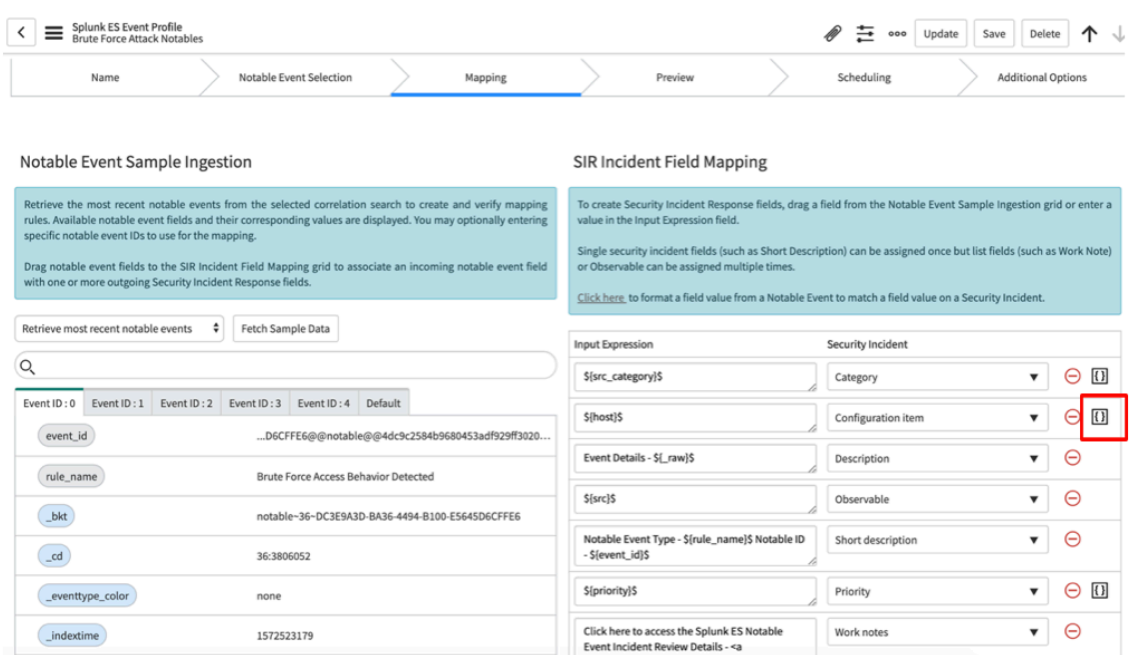
Outre les champs directement mappés à partir des valeurs d'événements notables ingérées et des valeurs que vous saisissez manuellement, utilisez l'éditeur de script pour formater les valeurs de champ sur l'incident de sécurité pendant l'étape de mappage.

Avant de commencer
Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche
Dans certains cas, Splunk Enterprise Security les valeurs d'événements notables sont mappées aux champs Catégorie, Élément de configuration (CI) et Observable de l'incident SIR ne sont pas pris en charge. Vous préférez peut-être modifier les valeurs mappées. Si vous souhaitez convertir la valeur d'un Splunk Enterprise Security événement notable en une valeur prise en charge par ces champs sur l'incident SIR de sécurité, utilisez l'éditeur de script.

Procédure
1. Une fois le formulaire de mappage affiché, cliquez sur le lien pour ouvrir l'éditeur de script.



2. Dans la liste de choix, sélectionnez un champ de destination pour la valeur que vous souhaitez modifier.

3. Sinon, dans la section Mappage du champ d'incidents SIR, cliquez sur l'icône de crochet [{}] en regard d'un champ pour ouvrir l'éditeur de script pour ce champ.

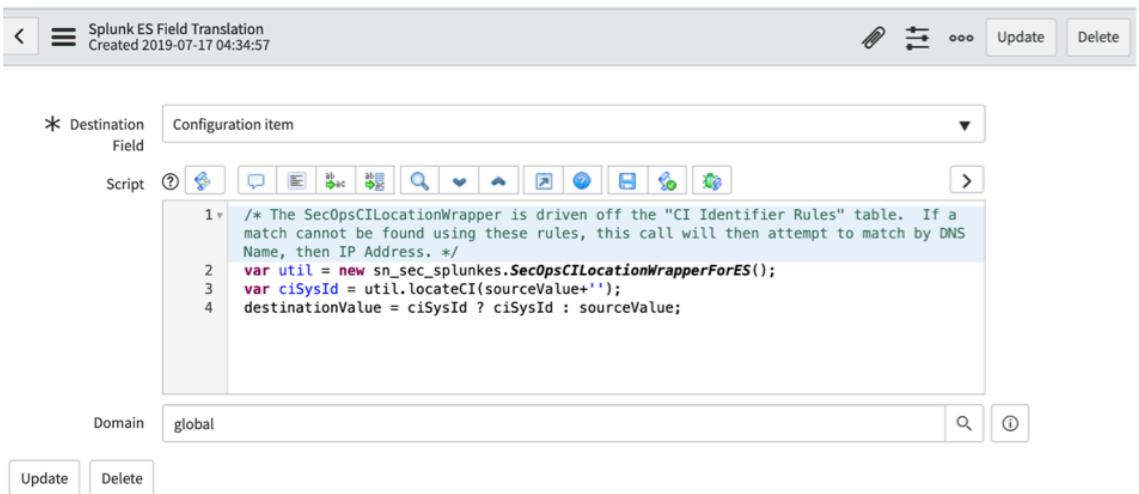
Dans certains cas, un include de script peut être approprié pour le champ Élément de configuration. Pour un événement notable, par exemple, une valeur de l'élément de configuration peut ne pas être mise en correspondance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comme le montre la figure suivante, si une correspondance pour un nom d'hôte est introuvable dans la ServiceNow AI Platform® CMDB pour le champ Élément de configuration, vous pouvez modifier la règle de sorte que si une adresse IP est trouvée, elle remplit le champ Élément de configuration. Si aucune valeur n'est spécifiée pour l'alarme, le champ de l'incident de sécurité est défini sur Null.

L'éditeur s'ouvre avec le champ affiché dans Champ de destination. L'image suivante montre l'éditeur avec le champ Élément de configuration comme champ de destination.



4. Entrez les modifications apportées au script et cliquez sur **Mettre à jour** pour enregistrer vos modifications. La Splunk table Traductions de champ s'affiche.
5. Fermez la table pour revenir au formulaire de mappage.

Copier Splunk Enterprise Security des profils d'une instance à une autre à l'aide de la fonction d'exportation/importation

Vous pouvez exporter et importer Splunk Enterprise Security des paramètres de profil d'une ServiceNow AI Platform instance à une autre ServiceNow AI Platform .

Avant de commencer

Les paramètres que vous pouvez exporter et importer incluent le nom du profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les exemples de données extraits, la planification et les informations sur la source des vignettes de configuration.

Rôle requis : sn_si.ingestion_profile_admin

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Cette fonctionnalité permet à l'administrateur de sécurité de copier des profils qui ont été testés et vérifiés sur une ServiceNow AI Platform instance, par exemple en non-production, vers une autre ServiceNow AI Platform instance, par exemple en production, sans avoir besoin de refaire tous les paramètres de configuration. Les paramètres exportés et importés incluent le nom de profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les exemples de données extraites, la planification et les informations sur la source des vignettes de configuration.

Traduction automatique

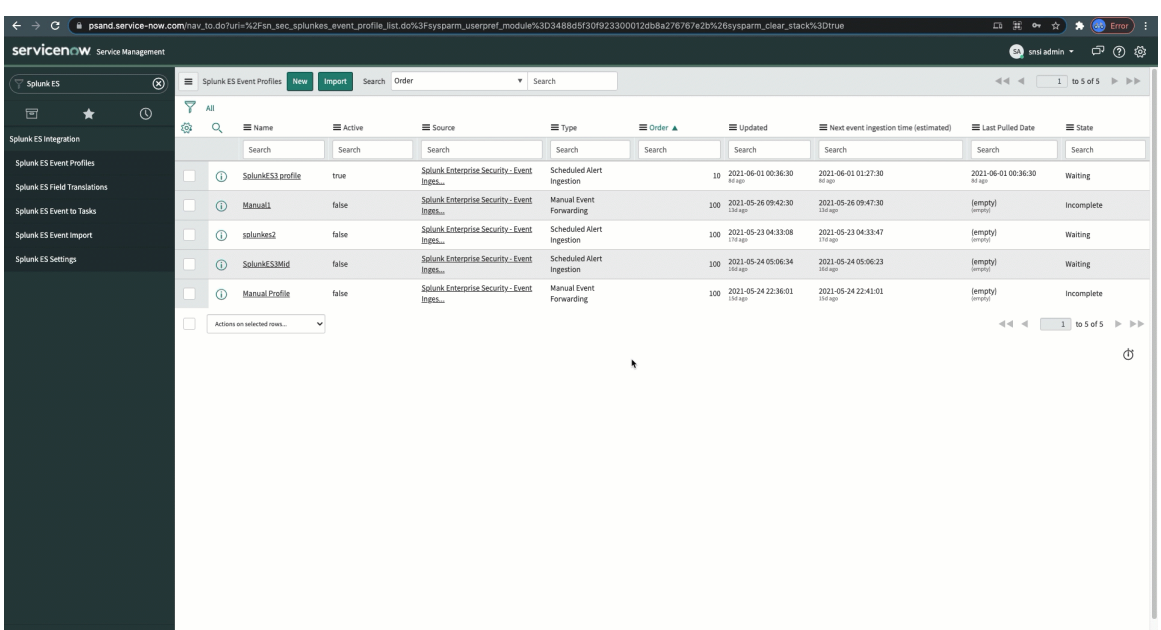
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque vous exportez un type de profil de transfert d'événements manuel, les données de pièce jointe utilisées pour le mappage des champs d'exemple sont copiées, mais le fichier de pièce jointe lui-même n'est pas exporté.

Procédure

1. Accédez à la **Tous** > **Intégration Splunk ES** > **Profils d'événements Splunk ES**.
2. Sélectionnez un profil que vous souhaitez exporter vers une autre ServiceNow AI Platform instance. Vous pouvez sélectionner plusieurs profils pour l'exportation.
3. Dans le menu Actions, cliquez sur **Exporter**.
4. Une fois que le message d'exportation terminée s'affiche, cliquez sur **Télécharger**.

   L'illustration suivante montre l'exportation d'un profil (SplunkES3profile) à partir de l'instance ServiceNow AI Platform (psand.service-now.com).



   Le fichier payload.xml exporté est téléchargé sur votre ordinateur. Le fichier contient le nom du profil, les règles de corrélation, les mappages, les filtres, les critères d'agrégation, les traductions de champs, les exemples de données extraits, la planification et les informations sur la source des vignettes de configuration. Lorsque vous sélectionnez et téléchargez plusieurs profils, ils apparaissent dans le même fichier payload.xml.

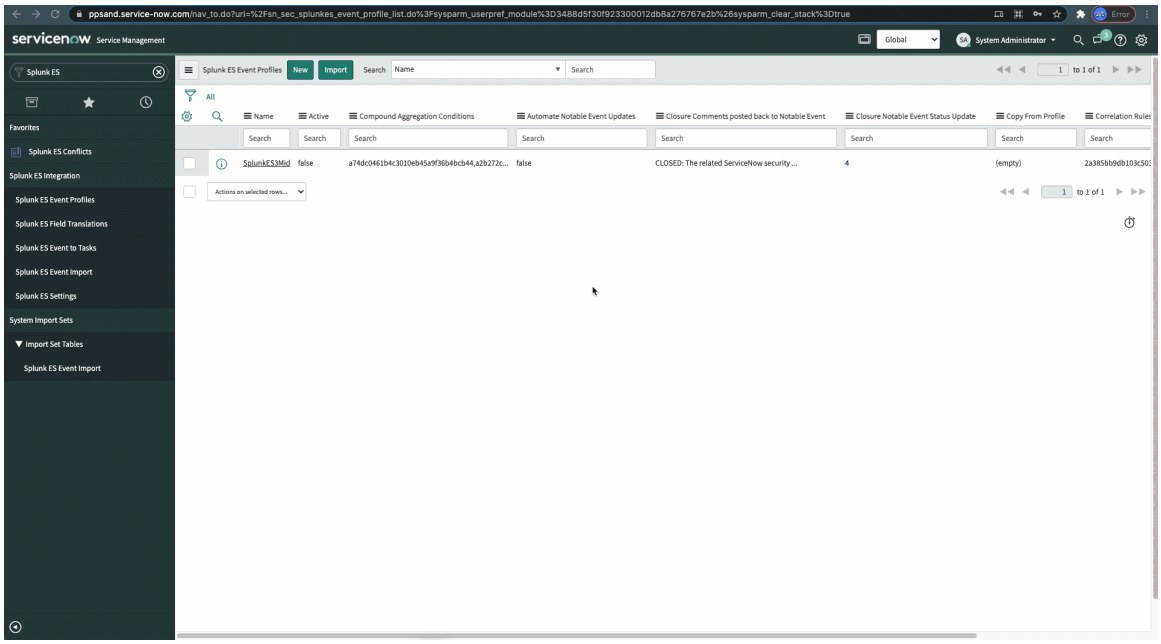
   Vous pouvez maintenant procéder à l'importation du profil dans une autre ServiceNow AI Platform instance.

5. Accédez à la **Intégration Splunk ES** > **Profils d'événements Splunk ES**.
6. Cliquez sur **Importer**.
7. Cliquez sur **Choisir un fichier** et sélectionnez le fichier XML sur votre ordinateur.
8. Cliquez sur **Charger**.
9. Cliquez sur **Fermer et recharger les profils**.

   L'illustration suivante montre l'importation d'un profil (SplunkES3profile) de l'instance ServiceNow AI Platform (psand.service-now.com) vers l'instance ServiceNow AI Platform (ppsand.service-now.com).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous avez importé le profil avec succès à partir d'une autre ServiceNow AI Platform instance.

Vérifiez que les paramètres de configuration de la source exportée (Splunk compte API et Splunk URL du serveur) et du serveur MID sont valides et disponibles dans l'instance importée ServiceNow AI Platform . Mettez à jour votre Splunk Enterprise Security configuration si nécessaire.

10. **Facultatif :** Vérifiez les paramètres du serveur MID après l'importation d'un profil.
11. **Facultatif :** Accédez à la **Security Operations** > **Configurations d'intégration**.
12. **Facultatif :** Sélectionnez la vignette de Splunk Enterprise Security configuration, puis cliquez sur **Mettre à jour**.
13. **Facultatif :** Examinez et mettez à jour les détails de la source et du serveur MID selon vos besoins.

Liste de vérification pour Splunk Enterprise Security l'intégration de l'ingestion d'événements notables

Utilisez cette liste de vérification pour vous guider à travers toutes les tâches de l'intégration. La liste de vérification suivante comprend des tâches de configuration et d'installation ainsi que des exemples de cas d'utilisation qui incluent les résultats attendus pour l'intégration.

Avant de commencer

Rôles requis : sn_si.ingestion_profile_admin, admin, sn_si.admin, sn_si.analyst, Splunk Enterprise Security administrateur

Remarque : Les utilisateurs disposant du rôle sn_si.admin peuvent effectuer toutes les opérations disponibles pour un administrateur de profil, car le rôle sn_si.admin hérite des autorisations requises par défaut.

Pourquoi et quand exécuter cette tâche

Suivez votre progression avec l'installation, l'installation et la configuration de l'intégration avec la table suivante. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante. Chaque ligne de la table répertorie les tâches et identifie les rôles requis pour effectuer les tâches. Les rubriques numérotées du guide d'installation et de configuration sont également référencées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les rôles requis pour chaque tâche sont répertoriés pour chaque étape dans le tableau suivant.

Procédure

1. Suivez votre progression avec l'installation, la configuration et la configuration de l'intégration. Terminez toutes les tâches d'une étape avant de passer à l'étape suivante.
2. Suivez les étapes du tableau dans l'ordre dans lequel elles se présentent.

Liste de vérification

☐	En tant qu'utilisateur disposant du rôle d'administrateur ServiceNow AI Platform , configurez votre ServiceNow AI Platform instance. ○ Affectez aux utilisateurs les rôles **sn_si.ingestion_profile_admin** (ou sn_si.admin) et sn_si.analyst selon les besoins. ○ Installez et configurez un serveur MID si le Splunk serveur est déployé dans votre réseau d'entreprise. ○ Vérifiez que les modules d'extension ServiceNow Réponse aux incidents de sécurité sont activés pour votre version du ServiceNow AI Platform. ○ (Facultatif) Si vous souhaitez transférer manuellement des événements de votre Splunk Enterprise Security console vers votre ServiceNow AI Platform instance, vérifiez que vous avez affecté le rôle (sn_sec_splunkes.api_account_access) à un utilisateur disposant de l'autorisation Splunk Enterprise Security administrateur. Pour plus d'informations, consultez Configurer votre ServiceNow AI Platform instance pour l'intégration Splunk Enterprise Security.
☐	En tant qu'utilisateur disposant du ServiceNow AI Platform rôle administrateur, installez et configurez l'application Splunk Enterprise Security à partir du ServiceNow Store. **a.** Téléchargez et installez l'application sur votre ServiceNow AI Platform instance. **b.** Configurez l'application et connectez-vous à votre Splunk Enterprise Security console. Pour plus d'informations, consultez Installer et configurer Splunk Enterprise Security l'intégration de l'ingestion d'événements notables.
☐	(Facultatif) Si vous avez l'intention d'exporter des événements manuellement de votre Splunk Enterprise Security console vers votre ServiceNow AI Platform instance, effectuez les tâches suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	○ En tant qu'administrateur Splunk Enterprise Security , installez, configurez et activez le ServiceNow module complémentaire Security Operations Event Ingestion for Splunk Enterprise Security à partir de splunkbase dans votre Splunk Enterprise Security console. ○ En tant qu'administrateur Splunk Enterprise Security , si ce n'est pas déjà fait, enregistrez les recherches en tant qu'événements notables dans votre Splunk Enterprise Security console. Pour plus d'informations, consultez Configurer votre Splunk environnement pour l'ingestion manuelle d'événements pour l'intégration de l'ingestion d'événements Splunk Enterprise Security notables.
☐	En tant qu'utilisateur disposant du rôle ServiceNow AI Platform **sn_si.ingestion_profile_admin** , créez et nommez un profil d'événement. Sélectionnez le type de profil dans la liste de choix. Les options sont un profil d'alerte planifiée que vous utilisez pour ingérer des exemples de données ou un profil d'événement que vous utilisez pour exporter manuellement des données de pièce jointe à partir de votre Splunk Enterprise Security console. ○ Pour une alerte planifiée, sélectionnez une alerte disponible. ○ Pour le profil des données exportées manuellement, créez une nouvelle carte ou copiez une carte existante. Pour plus d'informations, consultez Créer et nommer un profil d'événement pour l'intégration d'ingestion d'événements Splunk Enterprise Security.
☐	En tant qu'utilisateur disposant du rôle ServiceNow AI Platform **sn_si.ingestion_profile_admin**, mappez les valeurs ingérées ou les données de pièce jointe exportées depuis vers ServiceNow AI Platform les incidents de Splunk Enterprise Security sécurité. **a.** Extrayez un exemple de données pour une alerte planifiée. **b.** (Facultatif) Exporter les données de la pièce jointe manuellement à partir d'un Splunk Enterprise Security événement. **c.** Modifiez la configuration de mappage par défaut. **d.** Vous pouvez éventuellement ajouter des critères de filtrage, ajouter une alerte à un incident de sécurité existant et utiliser l'éditeur de script. Pour plus d'informations, consultez Mappage des champs d'événement notable pour l'intégration Splunk Enterprise Security et Créer des mappages pour Splunk ES l'examen des incidents d'événements notables et les détails de l'événement de contribution (ingestion planifiée).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

☐	○ En tant qu'utilisateur disposant du rôle ServiceNow AI Platform **sn_si.ingestion_profile_admin** , prévisualisez les données Splunk Enterprise affichées sur un ServiceNow AI Platform incident de sécurité. ○ Corrigez les erreurs ou ajoutez les données manquantes afin qu'aucun message d'erreur ne s'affiche. Pour plus d'informations, consultez Prévisualiser l'incident de sécurité pour l'intégration d'ingestion d'événements Splunk Enterprise Security.
☐	En tant qu'utilisateur disposant du rôle ServiceNow AI Platform **sn_si.ingestion_profile_admin** , planifiez la récupération d'alerte pour un profil avec une alerte planifiée. Pour plus d'informations, consultez Planifier et récupérer les événements notables nouveaux et mis à jour pour l'intégration d'ingestion d'événements Splunk Enterprise Security.

Vous avez terminé avec succès les étapes de configuration et vérifié les résultats attendus pour l'intégration.

Splunk - Intégration de l'enrichissement pour les incidents

L'intégration Splunk - Enrichissement des incidents recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.

Explorer	Configuration
Intégrations de Réponse aux incidents de sécurité	Introduction à l'intégration de la Splunk recherche pour Opérations de sécurité
Utiliser	**Développer**
• Exécuter une recherche de perceptions • Security Operations Integration - Flux de recherche de perceptions • Security Operations Integration - Flux de recherche d'observations Splunk • Afficher les détails de la recherche de perceptions • Afficher les résultats de recherche de perceptions	• ServiceNow Opérations de sécurité Directives pour le développement des intégrations • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et informations supplémentaires	
• Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté Security Operations	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Introduction à l'intégration de la Splunk recherche pour Opérations de sécurité

Splunk Le logiciel recherche, surveille et analyse les données volumineuses générées par les machines et s'intègre facilement à Opérations de sécurité. Avant de pouvoir utiliser l'intégration d'enrichissement Splunk des incidents, vous devez la télécharger à partir de et ServiceNow Store ajouter l'URL de base de l'API et les informations d'identification de connexion appropriées.

Avant de commencer

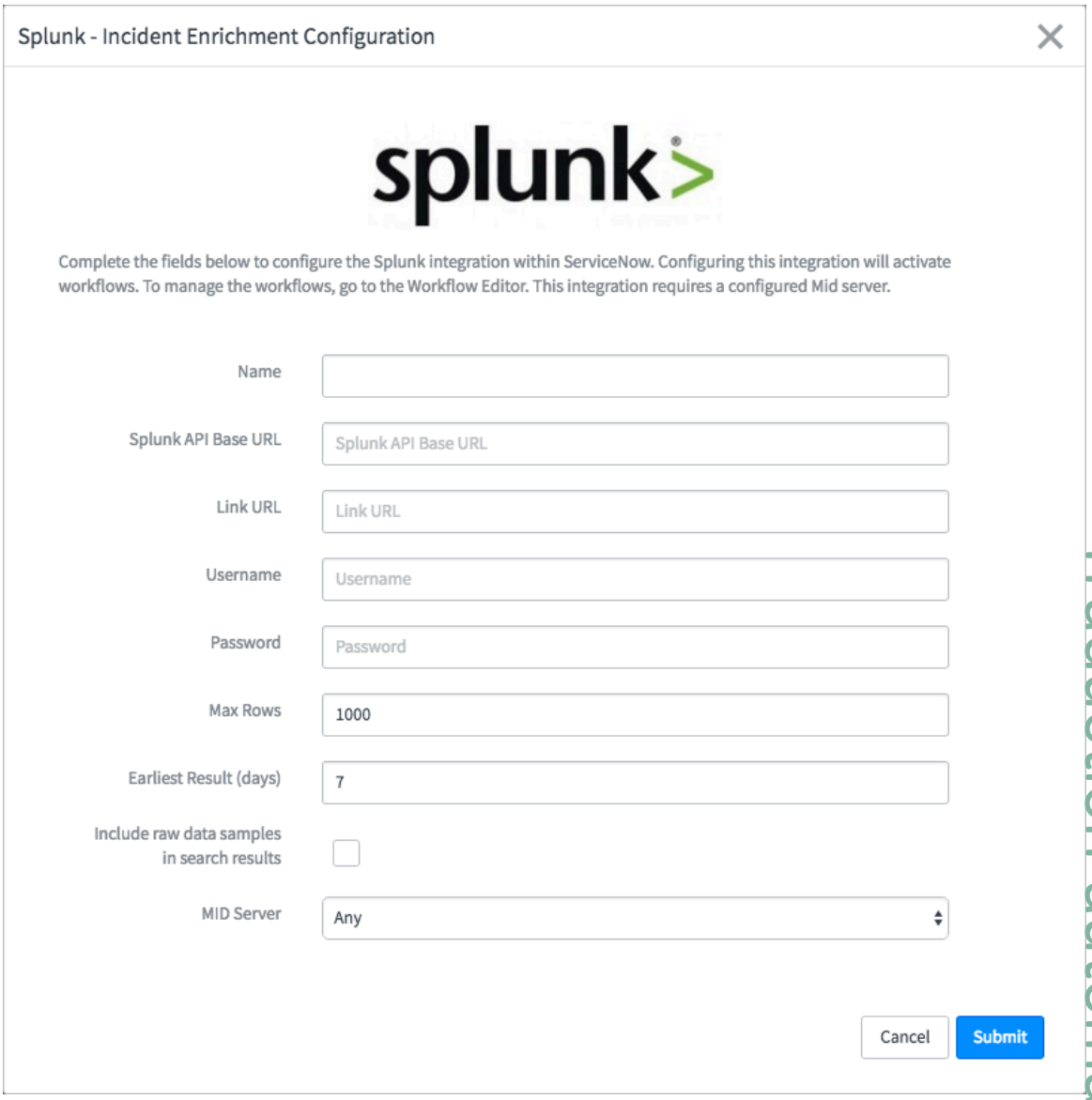
Rôle requis : sn_si.admin

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à Splunk la clé API et à l'ID API et procurez-les sous votre profil.
3. Dans votre instance, accédez à **Security Operations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte Splunk - Incident Enrichment, cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Renseignez les champs nécessaires.

Champ	Description
Nom	Nom de cette configuration.
URL de Base de l'API Splunk	URL de base que vous avez acquise sur le Splunk site.
URL de lien	[Facultatif] L'URL de lien qui renvoie à l'interface Web, lorsqu'elle Splunk est disponible.
Nom d'utilisateur	Votre nom d'utilisateur Splunk.
Mot de passe	Votre mot de passe Splunk.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend de votre paramètre dans la propriété **nombre de lignes de données brutes** dans les propriétés de Réponse aux incidents de sécurité.
Serveur MID	**Sélectionnez N'importe lequel** pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à **l'éditeur de workflow**.

6. Cliquez sur **Envoyer**.
   La carte de configuration d'intégration s'affiche.
7. Lors de l'affichage de la nouvelle carte de configuration, vous pouvez cliquer sur **Configurer** ou **Supprimer** pour modifier ou supprimer la configuration, respectivement.
8. Pour revenir à la liste d'origine des cartes de configuration d'intégration, sélectionnez **Non** dans la liste déroulante **Afficher les configurations** .

Expérience mobile pour Réponse aux incidents de sécurité

Utilisez votre équipement mobile Android ou iOS pour gérer vos tâches du centre des opérations de sécurité (SOC).

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Réponse aux incidents de sécurité

Si vous n'êtes pas familier avec les concepts de base du produit (SIR) sur votre ServiceNow AI Platform® instance, consultez Tableau de bord de vue d'ensemble Réponse aux incidents de sécurité pour plus d'informations sur Threat Réponse aux incidents de sécurité Intelligence et comment ce produit peut vous aider à hiérarchiser et à résoudre les cybermenaces qui pèsent sur votre organisation.

Vue d'ensemble

En tant que responsable du centre des opérations de sécurité (SOC) ou utilisateur disposant du rôle d'analyste de ServiceNow AI Platform sécurité (sn_si.analyst), vous pouvez vous connecter à une ServiceNow AI Platform instance directement à partir de votre équipement mobile. Avec le Application Security Incident Response Mobile, vous pouvez afficher, modifier et affecter vos incidents de sécurité et tâches de réponse les plus récents et les plus critiques SIR . Les notifications vous informent de l'arrivée des incidents de sécurité critiques qui vous sont affectés.

Avec le Application Security Incident Response Mobile, vous pouvez effectuer les tâches suivantes SIR à partir de votre équipement mobile :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Consultez la liste des incidents de sécurité critiques et des tâches de réponse.
- Recevez des notifications détaillées pour les incidents et les tâches de sécurité qui répondent aux critères de notification prédéfinis.
- Affichez des regroupements d'incidents ou de tâches de sécurité basés sur un ensemble prédéfini de requêtes ou de filtres.
- Consultez les notes de travail et les listes connexes des incidents de sécurité.
- Mettre à jour les incidents de sécurité et ajouter des notes de travail ou des pièces jointes.
- Modifiez les champs relatifs aux incidents de sécurité.
- Affectez des incidents de sécurité à vous-même ou à d'autres membres de votre équipe de sécurité.

Lorsqu'elles sont renseignées, vous pouvez afficher les listes connexes suivantes sur SIR les incidents de sécurité avec :Application Security Incident Response Mobile

- Élément de configuration
- Utilisateur affecté
- Services affectés
- Incidents de sécurité enfants
- Incidents de sécurité similaires (non pris en charge par ServiceNow AI Platform)
- Observables
- Tâches de réponse
- Tâches
- SLA de tâche
- Pièces jointes (non prises en charge par ServiceNow AI Platform)

La figure suivante illustre la façon dont vous vous connectez à votre ServiceNow AI Platform instance à partir de votre appareil mobile et la structure de l'écran d'accueil Application Security Incident Response Mobile qui est lu après la connexion.

Pour obtenir des instructions détaillées sur la configuration de votre ServiceNow AI Platform instance et l'installation de , reportez-vous à la Application Security Incident Response Mobile section Configurer une liste de vérification pour le Application Security Incident Response Mobile. Pour obtenir des instructions sur la façon de se connecter, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application Security Incident Response Mobile



Traduction automatique

Applications

Les applications correspondent aux ServiceNow® composants logiciels tels que Réponse aux incidents de sécurité (SIR), Réponse aux vulnérabilités (VR), Gouvernance, risque et conformité (GRC) qui fournissent des fonctions et des fonctionnalités spécifiques au sein de votre ServiceNow AI Platform instance. Après avoir installé l'application Réponse aux incidents de sécurité principale et votre Application Security Incident Response MobileServiceNow AI Platform instance, l'icône de l'application principale s'affiche au bas de votre iOSAndroid appareil mobile une fois connecté.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application Security Incident Response Mobile Icône (Incidents de sécurité)

Dossiers

Chaque ServiceNow® Mobile application contient des dossiers qui séparent les applets par catégorie. Dans l'image précédente de la page de destination, les **incidents de sécurité** et les **tâches de réponse aux incidents** sont des dossiers.

Applets

Les applets sont les différentes options au sein de l'application. Les icônes situées sous les sections **Incidents de sécurité** et **Tâches de réponse aux incidents** sont les applets disponibles du Application Security Incident Response Mobile.

Configurer une liste de vérification pour le Application Security Incident Response Mobile

La liste de vérification suivante comprend les tâches de configuration que vous devez accomplir dans votre ServiceNow AI Platform® instance et sur votre équipement mobile avant d'utiliser le Application Security Incident Response Mobile.

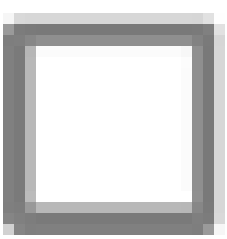
Avant de commencer

En option, imprimez cette liste de vérification et utilisez-la pour vous guider dans les tâches de configuration requises pour le Application Security Incident Response Mobile. Vérifiez que chaque élément de la liste est terminé afin de pouvoir afficher et modifier SIR les incidents de sécurité sur votre équipement mobile.

Les éléments de la liste de vérification sont affichés en surbrillance. Plus d'informations suivent chaque élément dans la colonne de droite. Temps estimé pour accomplir cette tâche : 15 à 20 minutes.

Rôles requis : admin, sn_si.analyst

Liste de vérification mobile

Élément	Description
	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que l'application Réponse aux incidents de sécurité principale est installée sur une ServiceNow AI Platform instance. Il s'agit de l'instance ServiceNow AI Platform que vous affichez sur votre appareil mobile. **Remarque :** L'application Réponse aux incidents de sécurité principale et l'instance ServiceNow AI Platform doivent provenir de la même version familiale. 1. Pour vérifier que l'application principale est installée sur votre instance, naviguez vers **Modules d'extension** et recherchez Réponse aux incidents de sécurité. 2. Si l'application principale n'est Réponse aux incidents de sécurité pas déjà installée, cliquez sur **Installer** pour l'installer. Pour plus d'informations sur l'installation de l'application Réponse aux incidents de sécurité principale, reportez-vous à la section Installer et configurer Réponse aux incidents de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification mobile (suite)

Élément	Description
	Si l'application principale n'est pas visible dans les modules d'extension, pour plus d'informations sur l'installation Réponse aux incidents de sécurité des applications principales et les droits sur les applications, reportez-vous à la section Opérations de sécurité et le ServiceNow Store.
☐	En tant qu'utilisateur disposant du rôle administrateur, vérifiez que le dispositif Application Security Incident Response Mobile est installé sur l'instance ServiceNow AI Platform que vous souhaitez afficher sur votre appareil mobile. **Remarque :** et Application Security Incident Response Mobile l'instance ServiceNow AI Platform doivent appartenir à la même version de famille. Téléchargez et installez le à partir de Application Security Incident Response Mobile sur ServiceNow Store votre ServiceNow AI Platform instance. Lorsque vous installez le Application Security Incident Response Mobile, ses dépendances, com.glide.sg et com.glide.sg.agent_native_client, sont également installées. Pour vérifier que ces dépendances sont installées : **1.** Accédez aux **modules d'extension.** **2.** Recherchez les ID de module d'extension (com.glide.sg et com.glide.sg.agent_native_client). **3.** S'ils ne sont pas activés, activez ces modules d'extension. Ces modules d'extension sont requis pour le .Application Security Incident Response Mobile Pour plus d'informations sur l'installation des applications et les autorisations associées aux applications, reportez-vous à la section Opérations de sécurité et le ServiceNow Store.
☐	En tant qu'utilisateur disposant du ServiceNow AI Platform rôle administrateur, vérifiez que vous avez affecté les utilisateurs mobiles disposant des rôles requis dans votre ServiceNow AI Platform instance. **1.** Pour afficher les rôles affectés à un utilisateur, accédez à **Utilisateurs et groupes** > **Utilisateurs**. **2.** Sélectionnez le nom d'utilisateur suivi de la liste connexe Rôles. Tous les rôles affectés à cet utilisateur s'affichent. **3.** Vérifiez qu'un utilisateur est affecté ou affectez-lui un rôle itil (IT Infrastructure Library Library). Les utilisateurs disposant du rôle ITIL peuvent créer, ouvrir, mettre à jour et fermer des incidents de sécurité. Seuls les utilisateurs ayant le rôle itil peuvent se voir affecter des tâches. **4.** Vérifiez qu'un utilisateur est affecté ou affectez-lui le rôle d'analyste de sécurité (sn_si.analyst). Les utilisateurs disposant du rôle sn_si.analyst peuvent lire et modifier les enregistrements d'incidents

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification mobile (suite)

Élément	Description
	de sécurité. Ce rôle est automatiquement ajouté lorsque vous affectez le rôle itil. **5.** Vérifiez que vous avez créé tous les groupes d'affectation requis et affecté des utilisateurs mobiles à ces groupes. **Remarque :** Si vous avez un grand nombre d'utilisateurs pour l'application mobile, vous pouvez également affecter le rôle sn_si.analyst à un groupe. Chaque utilisateur que vous ajoutez au groupe hérite de ce rôle. Pour plus d'informations sur les analystes de sécurité, reportez-vous à la section Affectation d'analystes de la sécurité. Pour plus d'informations sur les utilisateurs et l'affectation de rôles aux utilisateurs et aux groupes, voir Administration utilisateurs .
☐	En tant qu'utilisateur disposant du rôle sn_si.analyst, téléchargez l'application Agent la plus récente ServiceNow® sur votre équipement mobile. La version la plus récente de l'application Agent est disponible sur l'App Store d'Apple iOS et le Google Play Store.
☐	En tant qu'utilisateur disposant du rôle sn_si.analyst, vérifiez que les notifications sont activées sur votre équipement mobile et dans votre ServiceNow AI Platform instance. Les notifications vous informent lorsque des incidents de sécurité critiques vous sont affectés ou sont affectés à votre groupe d'affectation. Pour vous aider à corriger les notifications en temps opportun, après avoir activé les notifications, cliquez sur une notification dans le Application Security Incident Response Mobile pour accéder directement à l'incident de sécurité. Pour activer les notifications dans votre ServiceNow AI Platform instance afin qu'elles s'affichent sur votre appareil mobile, procédez comme suit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification mobile (suite)

Élément	Description
	1. Vérifiez que vous avez téléchargé et installé sur Application Security Incident Response Mobile votre ServiceNow AI Platform instance. 2. Dans Paramètres système de votre ServiceNow AI Platform instance, sous Notifications, vérifiez que vous avez activé **l'application mobile ServiceNow**. Pour plus d'informations sur la définition des notifications, consultez Définition des préférences de notification de l'utilisateur dans l'interface utilisateur principale . ServiceNow AI Platform Les notifications sont également affichées sur l'écran Messages de votre appareil mobile. Vérifiez que les notifications sont également activées dans les paramètres de votre appareil mobile.

Vous avez correctement configuré votre appareil mobile et le ServiceNow AI Platform pour le Application Security Incident Response Mobile. L'étape suivante consiste à vous connecter à votre ServiceNow AI Platform instance avec votre appareil mobile.

Connectez-vous au Application Security Incident Response Mobile

Ouvrez l'application mobile Réponse aux incidents de sécurité et ajoutez une ServiceNow AI Platform® instance avec Réponse aux incidents de sécurité sur votre équipement mobile.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

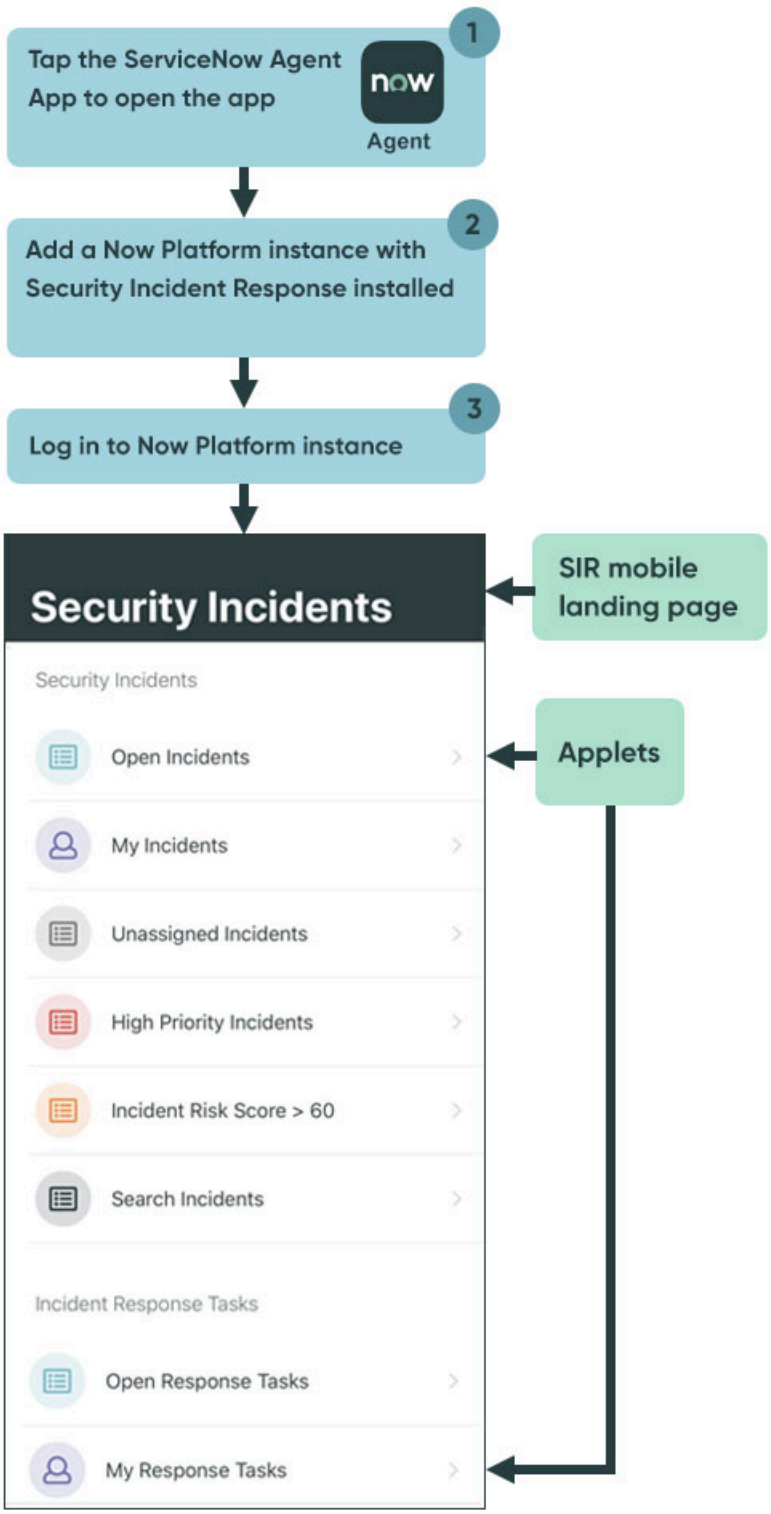
Temps pour terminer cette tâche : 5 à 10 minutes.

Vérifiez que vous avez effectué les étapes de configuration décrites à la section Configurer une liste de vérification pour le Application Security Incident Response Mobile.

Traduction automatique

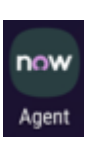
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application Security Incident Response Mobile



Procédure

1. Sur votre équipement mobile, appuyez sur l'application **ServiceNow Agent** pour l'ouvrir.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous n’êtes pas déjà connecté à une ServiceNow AI Platform instance, l’écran Instances s’affiche.

2. Si l’instance ServiceNow AI Platform avec l’application Réponse aux incidents de sécurité principale n’est pas déjà ajoutée à votre appareil mobile, procédez comme suit pour l’ajouter.

   a. Sur l’écran Instances qui s’affiche, appuyez sur  .
   Un écran s’affiche et vous invite à saisir et à enregistrer l’adresse d’une ServiceNow AI Platform instance.

   b. Renseignez les champs.

Champ	Description
Entrez l'adresse de l'instance ou scannez un code QR.	Choisissez-en un pour continuer : ▪ Avant le .service-now.com, entrez le nom de votre ServiceNow AI Platform instance, par exemple, sirmobileny. ▪ Saisissez une adresse. Cette adresse correspond à l’URL de votre ServiceNow AI Platform instance que vous souhaitez afficher sur votre appareil mobile, par exemple https://sirmobileny.service-now.com. ▪ Scannez un code QR.
(Facultatif) Saisir le pseudonyme	entrez un surnom pour cette instance. Si plusieurs instances ont été ajoutées à l’appareil, des surnoms peuvent vous aider à localiser rapidement une ServiceNow AI Platform instance.

   c. Appuyez sur **Enregistrer et se connecter**.

3. Sur l’écran de connexion qui s’affiche ServiceNow , saisissez le nom d’utilisateur et le mot de passe de l’instance ServiceNow AI Platform que vous souhaitez ajouter, puis appuyez sur **Connexion**.
   L’écran d’accueil Incidents de sécurité s’affiche. Vous vous êtes connecté avec succès au Application Security Incident Response Mobile.

4. Une fois connecté, vérifiez que les notifications sont activées dans le Application Security Incident Response Mobile.

   a. Sur l’écran d’accueil en bas, appuyez sur **Notification**.

   b. Sur l’écran Notifications, appuyez sur **Activer les notifications** si elles ne sont pas activées.
   Les notifications de sont ServiceNow AI Platform affichées sur l’écran Notifications dans le Application Security Incident Response Mobile.

5. Une fois que vous vous êtes connecté à une instance sur votre équipement mobile, il s’agit de l’instance par défaut ServiceNow AI Platform sur l’appareil.
   Si vous souhaitez en afficher une autre ServiceNow AI Platform sur l’appareil, vous devez vous déconnecter de l’instance par défaut. Pour vous déconnecter :

   a. Appuyez sur l’icône des paramètres.

   b. Appuyez sur **Déconnexion**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’écran Instances s’affiche avec toutes les ServiceNow AI Platform instances que vous avez ajoutées à l’appareil mobile.

c. **Facultatif :** Appuyez sur une autre instance pour vous y connecter ou suivez les étapes précédentes pour ajouter une autre instance.

Si l’écran des instances ne s’affiche Application Security Incident Response Mobile pas après que vous avez appuyé sur l’application **ServiceNow Agent** sur votre appareil, vérifiez que **ServiceNow Agent** est autorisé en tant qu’application de confiance sur votre appareil. Pour autoriser l’accès en tant qu’application de confiance, accédez aux paramètres et à la gestion générale des appareils sur votre appareil et appuyez sur l’option (Faire confiance à l’application, etc.) pour autoriser l’accès.

Si un message d’erreur s’affiche après que vous avez saisi vos informations d’identification sur l’écran de connexion, vérifiez que votre nom d’utilisateur et votre mot de passe pour l’instance ServiceNow AI Platform sont corrects.

Si vous rencontrez des problèmes d’affichage sur l’écran d’accueil, vérifiez votre connexion réseau.

Si vous ne pouvez pas afficher l’écran Instances après avoir appuyé sur l’application **ServiceNow Agent** , essayez de la désinstaller de votre appareil. Vérifiez que vous disposez de la version la plus récente de l’application sur l’App Store d’Apple iOS ou le Google Play Store et essayez de la réinstaller.

Afficher, modifier et affecter des incidents de sécurité ouverts avec Application Security Incident Response Mobile

En tant qu’analyste des incidents de sécurité, affichez, modifiez et affectez des incidents de sécurité ouverts Réponse aux incidents de sécurité (SIR) à partir de votre équipement mobile. Consultez les listes connexes et la piste d’audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Dans la liste des enregistrements, affectez-vous un incident de sécurité ouvert ou réaffectez-le. Vous pouvez également afficher les détails et les listes connexes de l’enregistrement ou ajouter une note de travail avant l’affectation. Temps pour terminer cette tâche : 5 à 10 minutes.

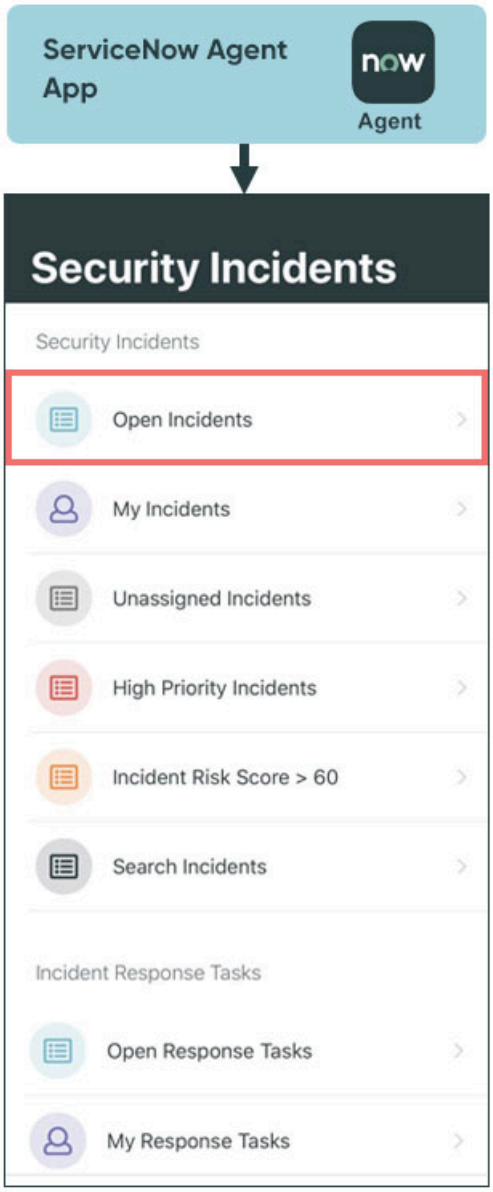
Procédure

1. Si vous n’êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.
2. Une fois la page de destination Incidents de sécurité affichée, appuyez sur **Incidents ouverts**.

Si vous quittez le Application Security Incident Response Mobile après vous être connecté, appuyez à tout moment sur l’application Now Agent pour revenir au dernier écran que vous aviez affiché.

Traduction automatique

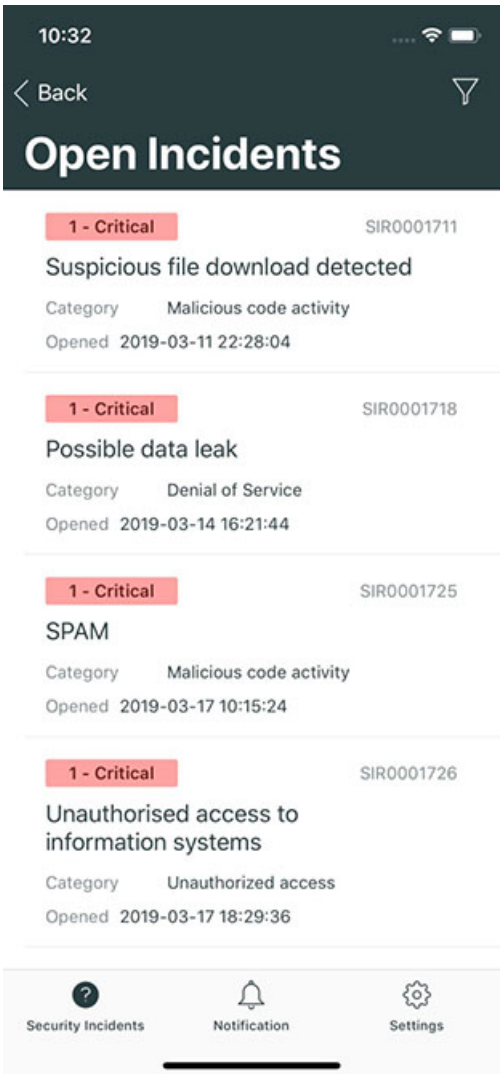
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L’écran Incidents ouverts s’affiche avec une liste des enregistrements d’incidents de sécurité ouverts.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. **Facultatif :** Reportez-vous à Rechercher des incidents de sécurité avec le Application Security Incident Response Mobile la section pour rechercher les incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre (icône affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.

4. Pour vous affecter un incident ou le réaffecter directement à partir de la liste des incidents de sécurité ouverts, balayez un enregistrement vers la gauche pour ouvrir le menu.

5. Choisissez-en un dans le menu qui s'affiche pour continuer.

Option	Description
Mes affectations	Affectez-vous l'incident de sécurité. Si l'incident de sécurité vous est déjà affecté, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation :

Traduction automatique

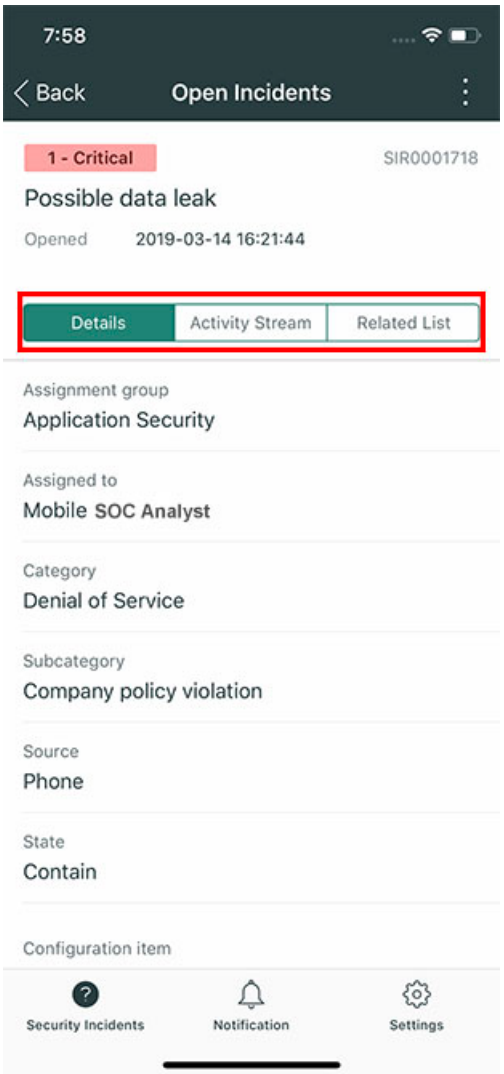
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation : **a.** Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône Envoyer (icône  ou sur **Soumettre** pour enregistrer et soumettre vos modifications.

6. Alternativement, pour afficher les détails d'un enregistrement d'incident de sécurité ouvert et pour afficher davantage d'enregistrements associés et de listes connexes, avec l'écran Incidents ouverts affiché, appuyez sur un enregistrement de la liste.
7. Sur l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Appuyez sur l'icône de menu (icône ⋮ en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez parmi les options suivantes. ○ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et entrer du texte. ○ Pour réaffecter l'incident, appuyez sur **Réaffecter** ou **Affecter à moi**. Suivez les instructions décrites dans le tableau précédent. Une fois que vous avez terminé vos modifications, appuyez sur l'icône Envoyer (icône ➤ ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône Plus (icône) pour ajouter une note de travail ou joindre un fichier.
Onglet Liste connexe	Une fois l'onglet Liste connexe sélectionné, affichez les éléments de toutes les listes connexes de l'incident de sécurité qui sont renseignées. Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Icônes d'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ○ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ○ Si affiché, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ○ Appuyez sur **Notification** pour afficher les notifications de et ServiceNow AI Platform de .Application Security Incident Response Mobile ○ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance ServiceNow AI Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle ServiceNow AI Platform .

Afficher, modifier et réaffecter les incidents de sécurité qui vous sont affectés avec le Application Security Incident Response Mobile

En tant qu'analyste des incidents de sécurité, affichez, modifiez et réaffectez Réponse aux incidents de sécurité (SIR) les incidents qui vous sont affectés. Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

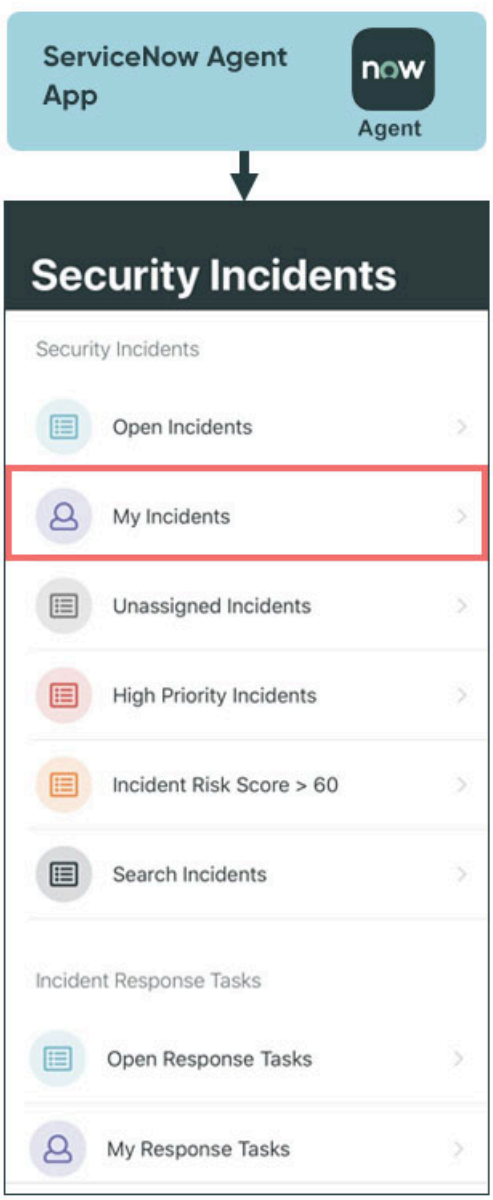
Pourquoi et quand exécuter cette tâche

Réaffectez un incident de sécurité ouvert à un autre analyste de votre groupe à partir de la liste des enregistrements. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps pour terminer cette tâche : 5 à 10 minutes.

Procédure

1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.
2. Avec l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Mes incidents**.

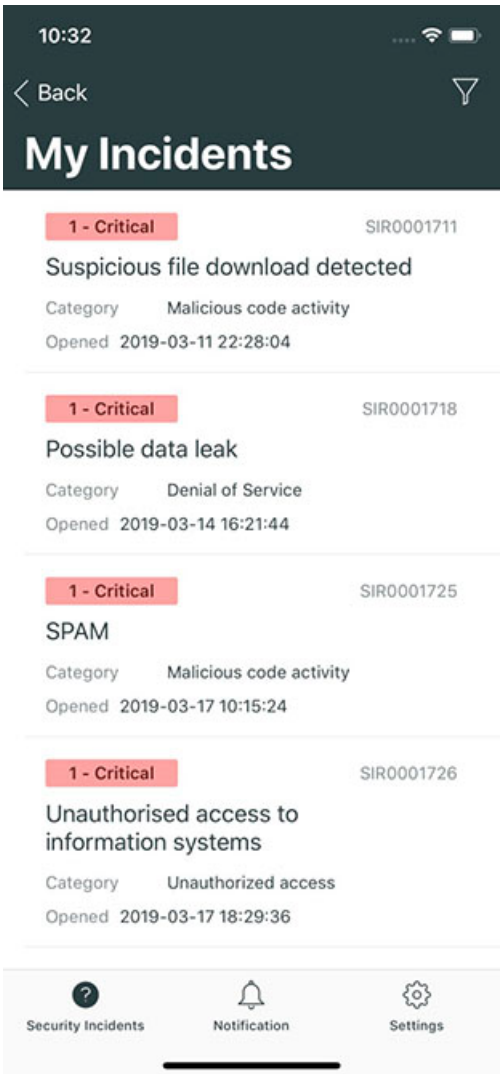
Si vous quittez le Application Security Incident Response Mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous aviez affiché.



L'écran Mes incidents s'affiche avec une liste des enregistrements d'incidents de sécurité ouverts qui vous sont affectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



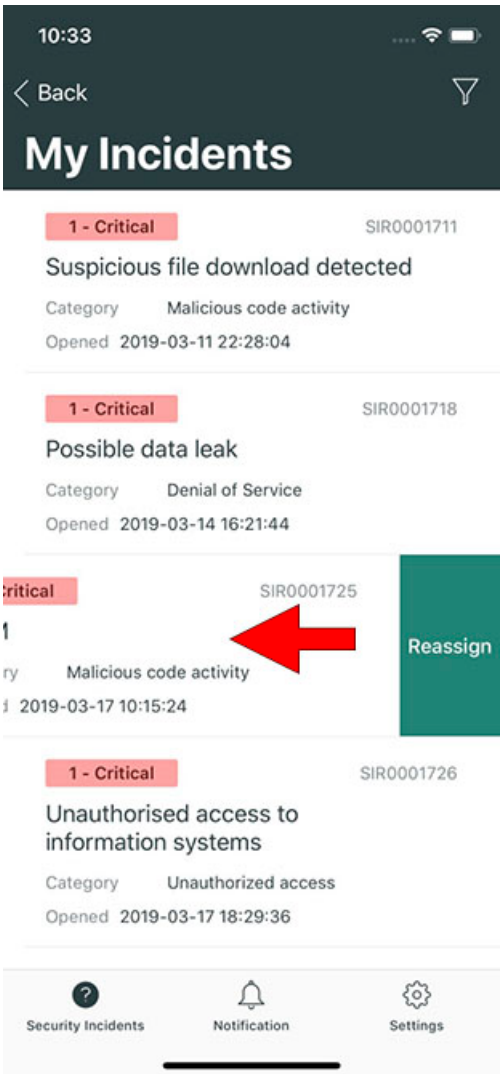
3. **Facultatif :** Reportez-vous à Rechercher des incidents de sécurité avec le Application Security Incident Response Mobile la section pour rechercher les incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.

4. Pour réaffecter un incident directement à partir de la liste, avec la liste des enregistrements d'incidents de sécurité ouverts affichée, faites glisser vers la gauche sur un enregistrement pour ouvrir le menu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

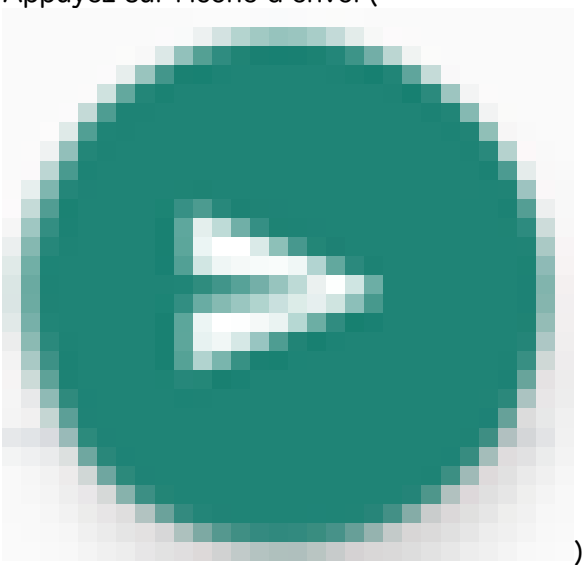


5. Modifiez les champs Groupe d’affectation ou Affecté à à partir du menu qui s’affiche.

Option	Description
Réaffecter	Pour réaffecter le groupe d’affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste qui s’affiche ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d’affectation lié à la sécurité. Pour affecter ou réaffecter l’incident de sécurité à un membre du groupe d’affecta–tion : **a.** Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s’affiche ou saisissez du texte dans le champ de recherche.

Traduction automatique

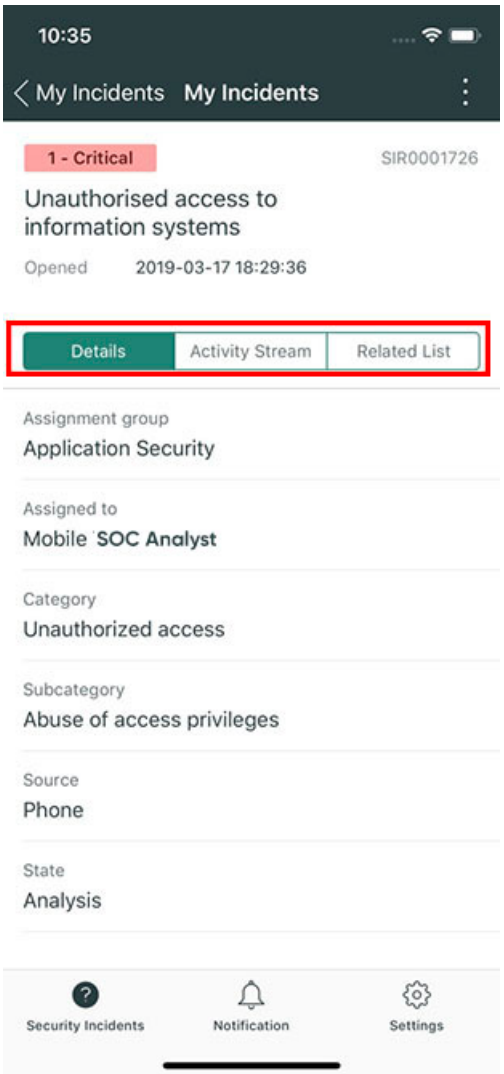
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Appuyez sur l’icône d’envoi () ou sur **Soumettre** pour enregistrer et soumettre vos modifications.

6. Alternativement, pour afficher les détails de l’enregistrement d’incident de sécurité ouvert, avec l’écran Mes incidents affiché, appuyez sur un enregistrement de la liste.
7. Sur l’enregistrement ouvert qui s’affiche, choisissez une option dans la table suivante pour continuer.

Traduction automatique

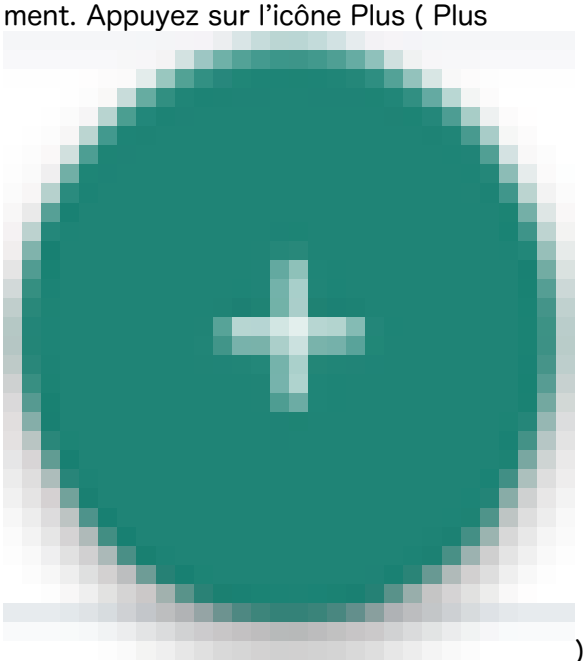
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Appuyez sur l'icône de menu ( ) en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez parmi les options suivantes. ○ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et entrer du texte. ○ Pour réaffecter l'incident, appuyez sur **Réaffecter**. Suivez les instructions décrites dans le tableau précédent. Une fois vos modifications terminées, appuyez sur l'icône Envoyer (

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	) ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône Plus (Plus ) pour ajouter une note de travail ou joindre un fichier.
Onglet Liste connexe	Une fois l'onglet Liste connexe sélectionné, affichez les éléments de toutes les listes connexes renseignées sur l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Icônes d'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ○ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ○ Si affiché, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ○ Appuyez sur **Notification** pour afficher les notifications de et ServiceNow AI Platform de .Application Security Incident Response Mobile ○ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance ServiceNow AI Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle ServiceNow AI Platform .

Affichez, modifiez et affectez des incidents de sécurité non affectés avec Application Security Incident Response Mobile

À partir de votre équipement mobile, affichez, modifiez et affectez des incidents non affectés Réponse aux incidents de sécurité (SIR). Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Dans la liste des enregistrements, affectez un incident de sécurité ouvert et non affecté à vous-même ou à un autre analyste de votre groupe. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps pour terminer cette tâche : 5 à 10 minutes.

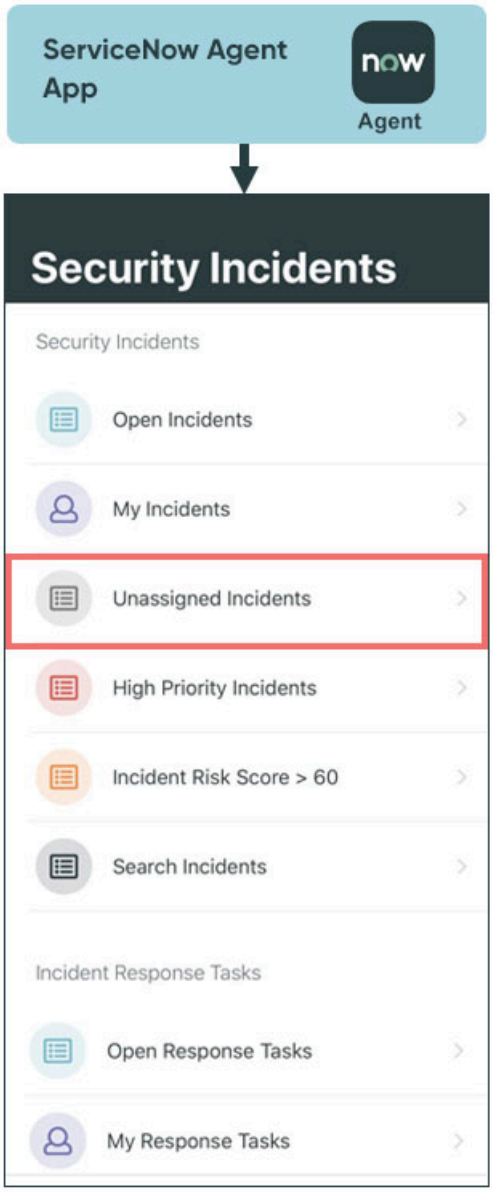
Procédure

1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.
2. Lorsque l'écran d'accueil Incidents de sécurité s'affiche, appuyez sur **Incidents non affectés**.

   Si vous quittez le Application Security Incident Response Mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous aviez affiché.

Traduction automatique

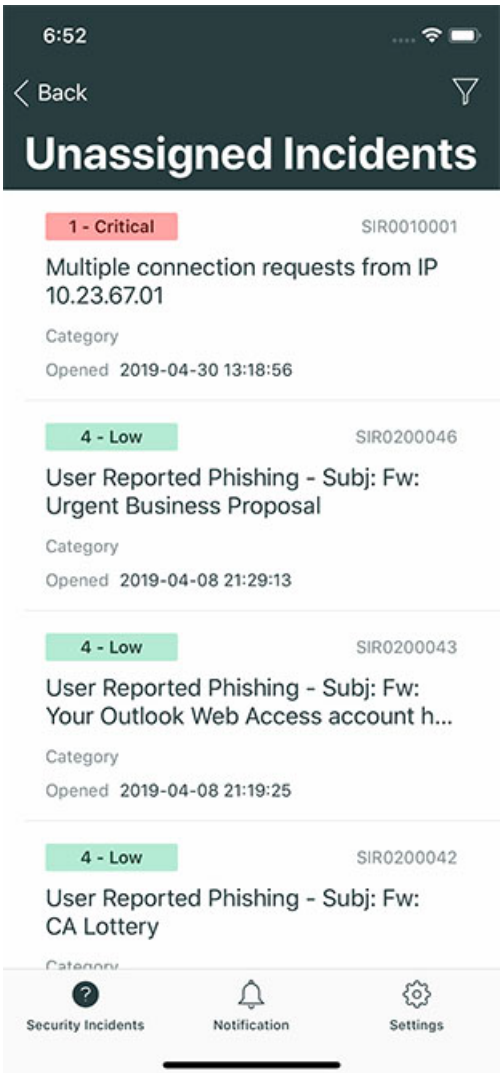
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L’écran Incidents non affectés s’affiche avec une liste des enregistrements d’incidents de sécurité non affectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



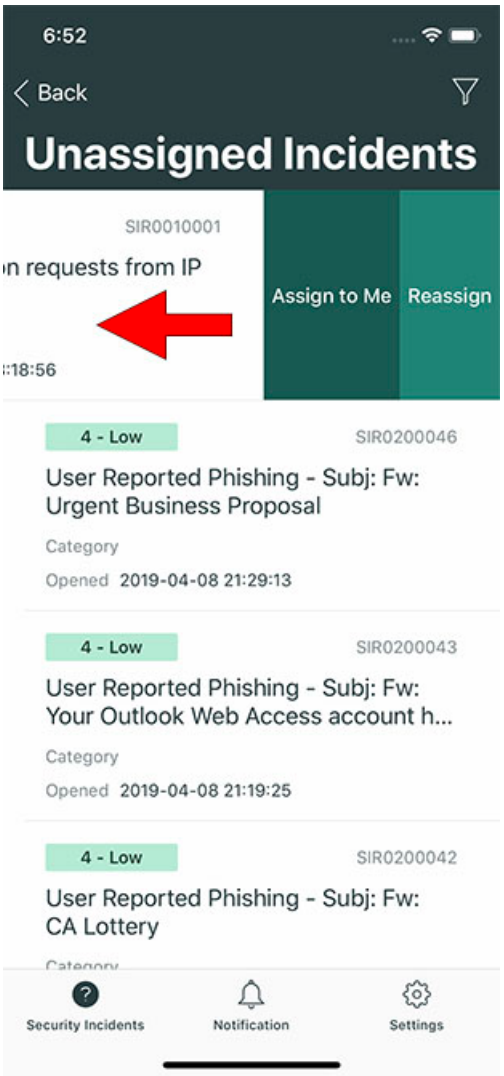
3. **Facultatif :** Reportez-vous à Rechercher des incidents de sécurité avec le Application Security Incident Response Mobile la section pour rechercher les incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre (icône affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.

4. Pour affecter ou réaffecter un enregistrement d'incident de sécurité ouvert directement à partir de la liste, avec la liste des enregistrements d'incidents de sécurité non affectés ouverts affichés, faites glisser vers la gauche sur un enregistrement pour ouvrir le menu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Choisissez-en un dans le menu pour continuer.

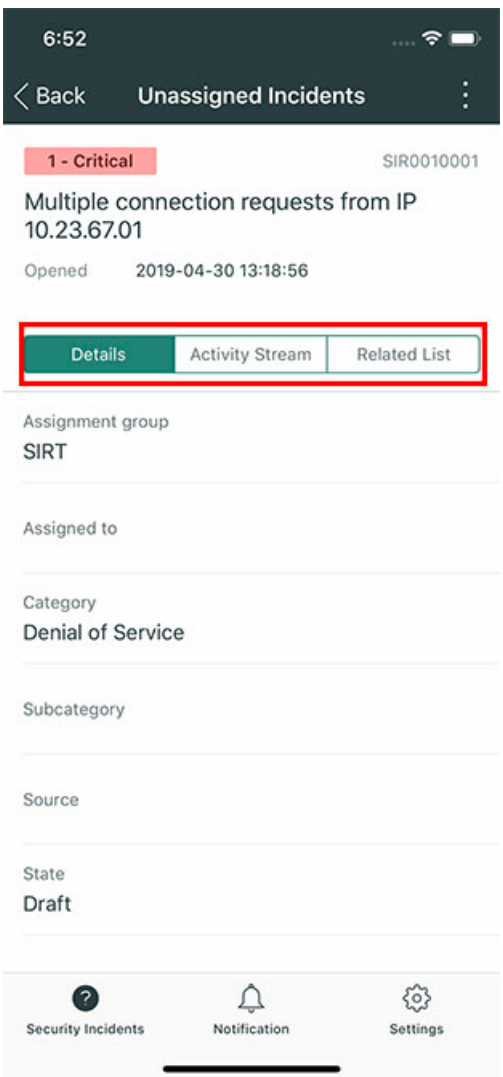
Option	Description
Mes affectations	Affectez-vous l'incident de sécurité. Si l'incident de sécurité vous est déjà affecté, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône Envoyer (icône ou sur **Soumettre** pour enregistrer et soumettre vos modifications.

6. Sinon, avec l'écran Incidents non affectés affiché, appuyez sur un enregistrement de la liste.
7. Sur l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.



Option	Description
Appuyez sur l'icône de menu (icône en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez parmi les options suivantes. ○ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et entrer du texte. ○ Pour affecter ou réaffecter l'incident, appuyez sur **Réaffecter** ou **Affecter à moi.** Suivez les instructions décrites dans le tableau précédent. Une fois que vous avez terminé vos modifications, appuyez sur l'icône Envoyer (icône  ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône Plus (icône ) pour ajouter une note de travail ou joindre un fichier.
Onglet Liste connexe	Une fois l'onglet Liste connexe sélectionné, affichez les éléments de l'une des listes connexes renseignées sur l'incident de sécurité. Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Icônes d'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ○ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ○ Si affiché, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ○ Appuyez sur **Notification** pour afficher les notifications de et ServiceNow AI Platform de .Application Security Incident Response Mobile ○ Appuyez sur **Paramètres** et choisissez-en un pour continuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	▪ Affichez des informations sur l'instance ServiceNow AI Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle ServiceNow AI Platform .

Affichez, modifiez et affectez des incidents de priorité élevée avec Application Security Incident Response Mobile

À partir de votre équipement mobile, affichez, modifiez et affectez des incidents de priorité Réponse aux incidents de sécurité élevée (SIR). Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Dans la liste des enregistrements, affectez un incident de sécurité critique ouvert à vous-même ou à un autre analyste de votre groupe. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps pour terminer cette tâche : 5 à 10 minutes.

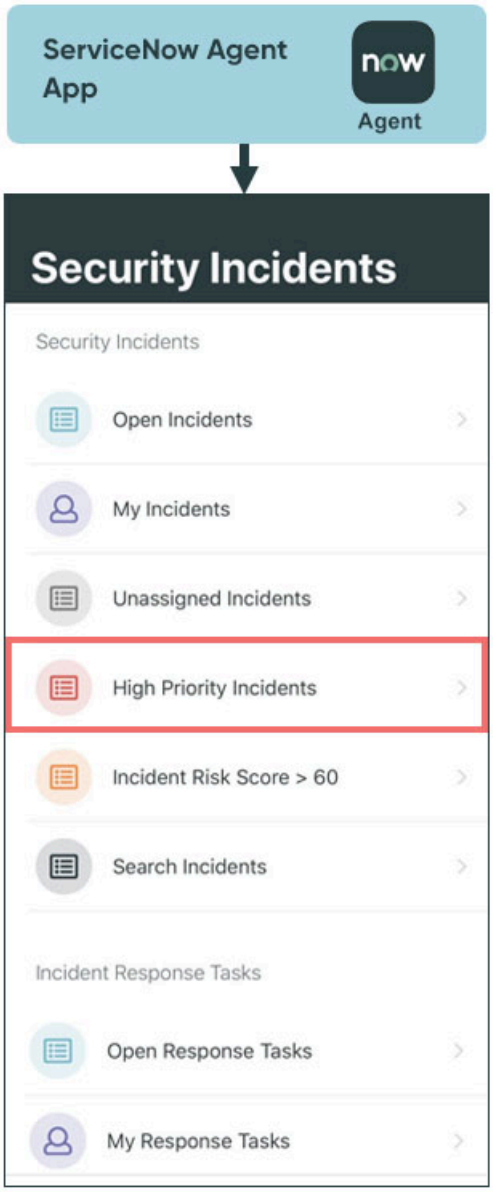
Procédure

1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.
2. Avec l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Incidents de priorité élevée**.

   Si vous quittez le Application Security Incident Response Mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous aviez affiché.

Traduction automatique

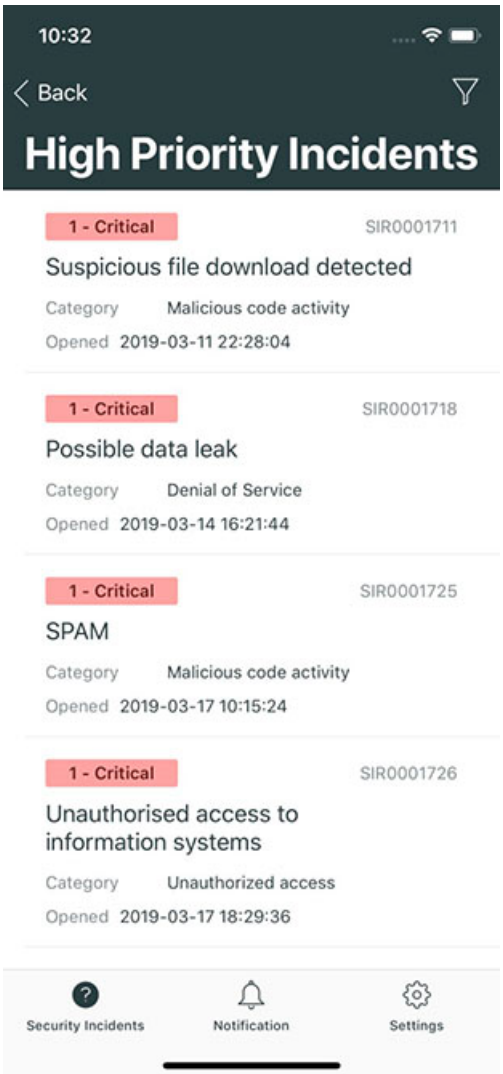
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L’écran Incidents de priorité élevée s’affiche avec une liste d’incidents de sécurité critiques (haute priorité).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



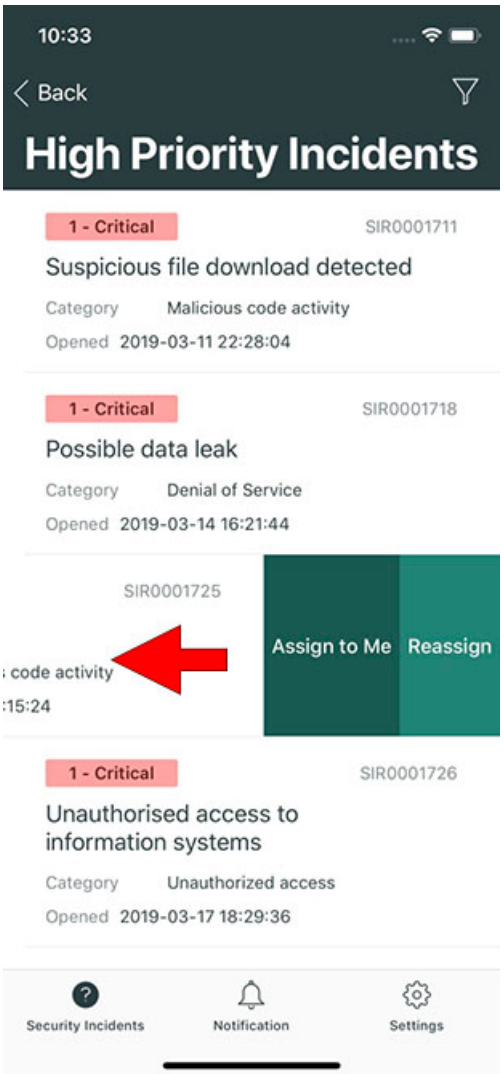
3. **Facultatif :** Reportez-vous à Rechercher des incidents de sécurité avec le Application Security Incident Response Mobile la section pour rechercher les incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre () affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.

4. Une fois la liste des enregistrements d'incidents de sécurité de priorité élevée ouverts affichée, faites glisser un enregistrement vers la gauche pour ouvrir le menu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

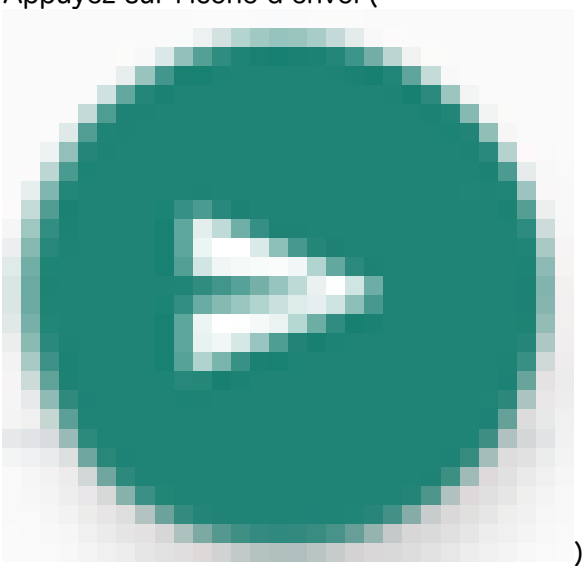


5. Choisissez-en un pour continuer.

Option	Description
Mes affectations	Affectez-vous l'incident de sécurité. Si l'incident de sécurité vous est déjà affecté, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation : **a. Appuyer sur Groupe d'affectation** **b.** Appuyez sur un groupe dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation :

Traduction automatique

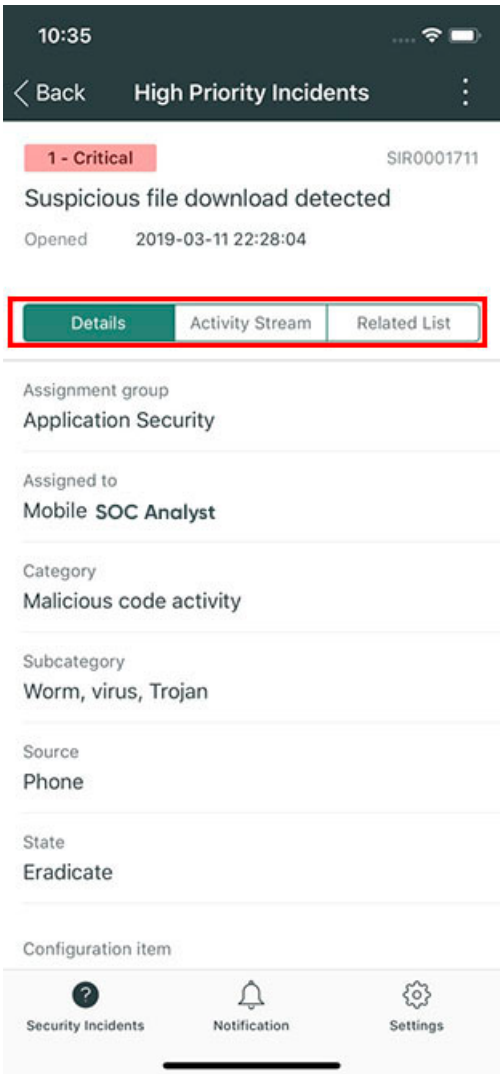
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Affecté à**. **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône d'envoi () ou sur **Soumettre** pour enregistrer et soumettre vos modifications.

6. Pour afficher les détails d'un enregistrement d'incident de sécurité ouvert et afficher davantage d'enregistrements associés et de listes connexes, avec l'écran Incidents de priorité élevée affiché, appuyez sur un enregistrement de la liste.
7. Sur l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.

Traduction automatique

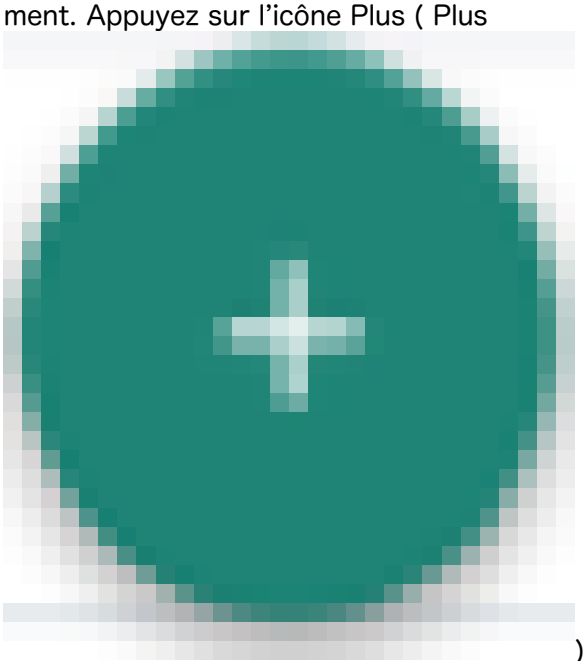
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Appuyez sur l'icône de menu ( ) en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez parmi les options suivantes. ○ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et entrer du texte. ○ Pour réaffecter l'incident, appuyez sur **Réaffecter** ou **Affecter à moi**. Suivez les instructions décrites dans le tableau précédent. Une fois vos modifications terminées, appuyez sur l'icône Envoyer (

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	) ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Une fois l'onglet Activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône Plus (Plus ) pour ajouter une note de travail ou joindre un fichier.
Onglet Liste connexe	Une fois l'onglet Liste connexe sélectionné, affichez les éléments de l'une des listes connexes renseignées sur l'incident de sécurité. Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Appuyez sur une icône d'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ○ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ○ Si affiché, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ○ Appuyez sur **Notification** pour afficher les notifications de et ServiceNow AI Platform de .Application Security Incident Response Mobile ○ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez des informations sur l'instance ServiceNow AI Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle ServiceNow AI Platform .

Affichez, modifiez et affectez des incidents de sécurité avec un score de risque supérieur à 60 avec le Application Security Incident Response Mobile

À partir de votre équipement mobile, affichez et modifiez Réponse aux incidents de sécurité (SIR) les incidents dont la valeur dans le champ de score de risque est supérieure à 60. Consultez les listes connexes et la piste d'audit des notes de travail pour plus de détails sur les incidents.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Dans la liste des enregistrements, affectez un incident de sécurité ouvert dont le score de risque est supérieur à 60 à vous-même ou à un autre analyste de votre groupe. Vous pouvez également afficher les détails et les listes connexes de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps pour terminer cette tâche : 5 à 10 minutes.

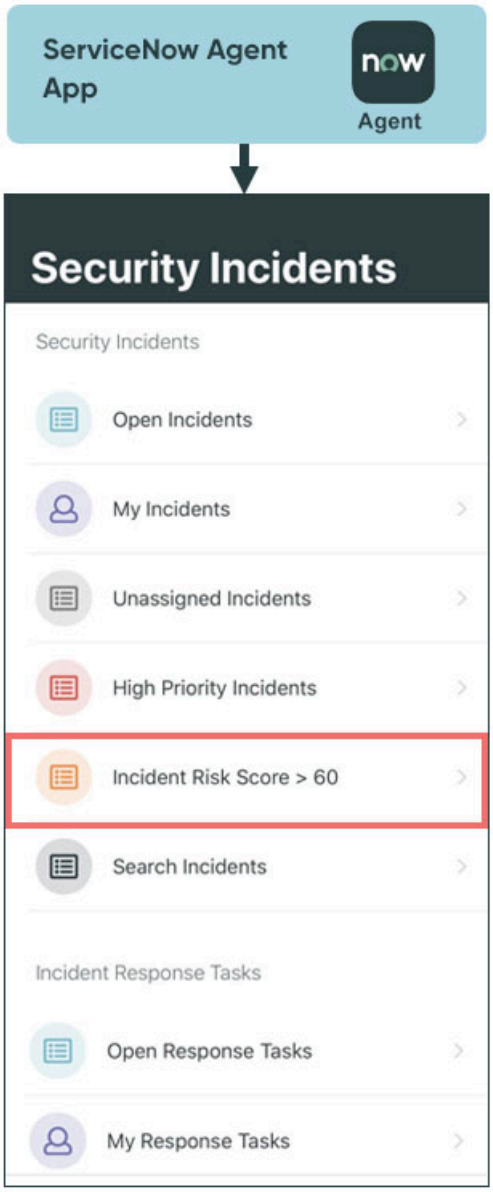
Procédure

1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.
2. Une fois l'écran d'accueil des incidents de sécurité affiché, appuyez sur **Score de risque > 60**.

Si vous quittez le Application Security Incident Response Mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous aviez affiché.

Traduction automatique

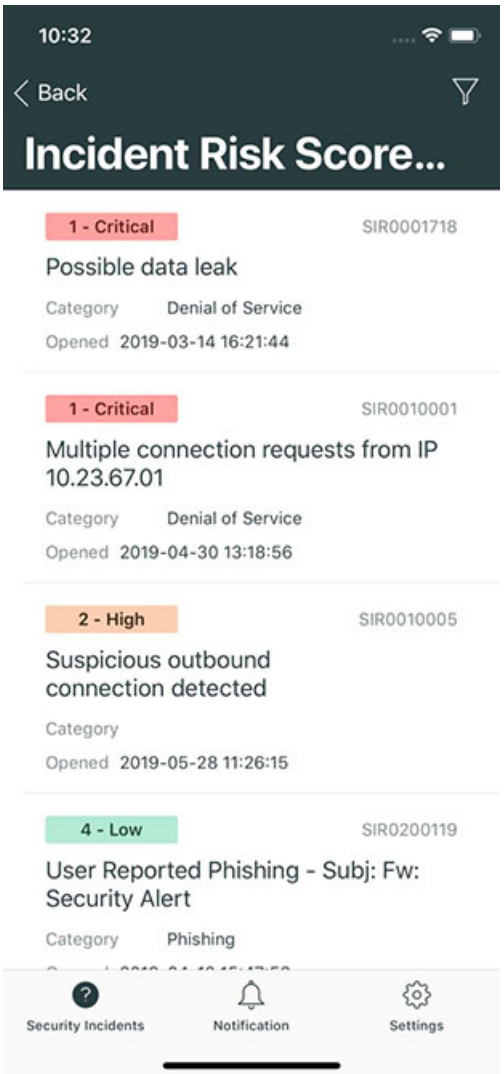
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L’écran Score de risque d’incident s’affiche avec une liste d’incidents de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



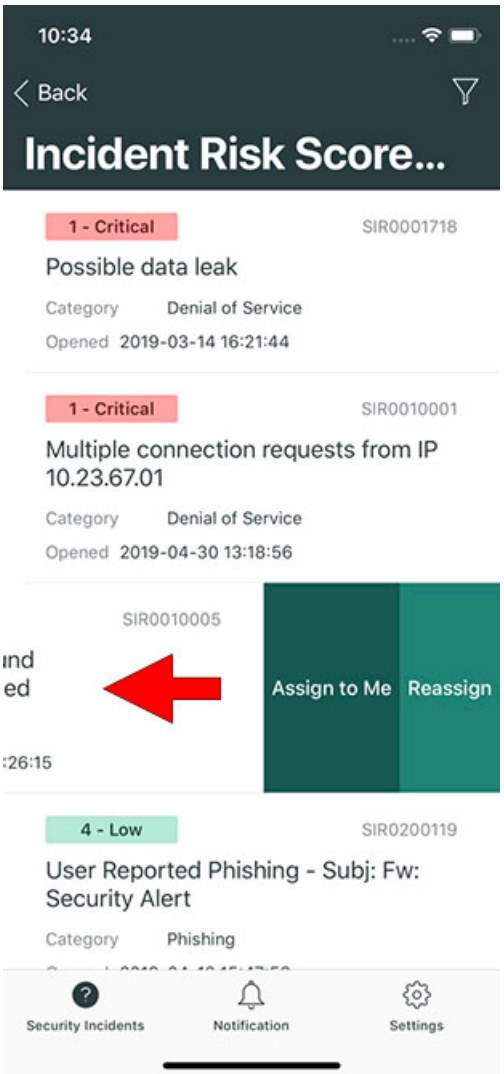
3. **Facultatif :** Reportez-vous à Rechercher des incidents de sécurité avec le Application Security Incident Response Mobile la section pour rechercher les incidents de sécurité qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre (icône affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.

4. Pour vous affecter un incident de sécurité ou le réaffecter directement à partir de la liste des enregistrements d'incidents de sécurité ouverts affichés, faites glisser un enregistrement vers la gauche pour ouvrir le menu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Choisissez-en un pour continuer.

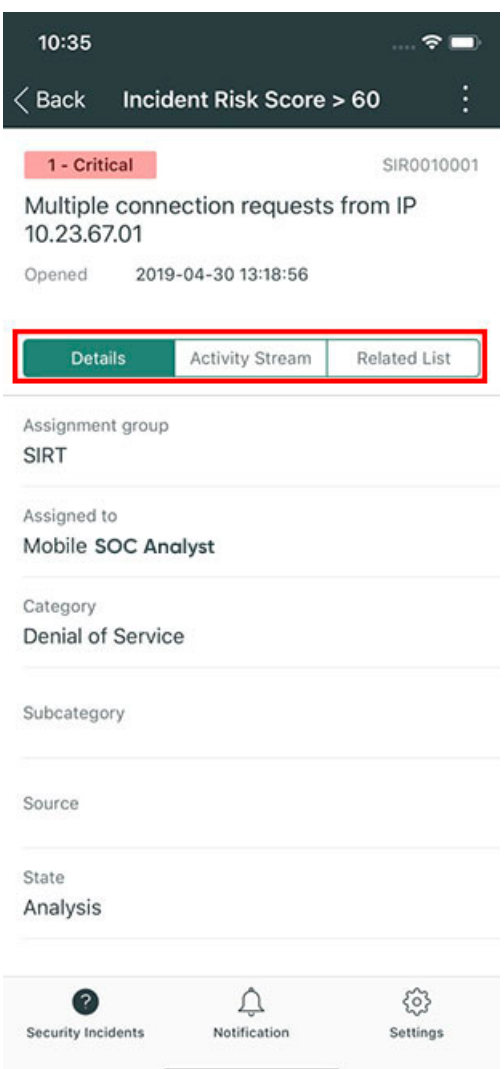
Option	Description
Mes affectations	Affectez-vous l'incident de sécurité. Si l'incident de sécurité vous est déjà affecté, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation : **a.** Appuyez sur **Groupe d'affectation**. **b.** Appuyez sur un groupe dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité. Pour affecter ou réaffecter l'incident de sécurité à un membre du groupe d'affectation :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	a. Appuyez sur **Affecté à** et **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Appuyez sur l'icône Envoyer (icône ou sur **Soumettre** pour enregistrer et soumettre vos modifications.

6. Alternativement, pour afficher les détails d'un enregistrement d'incident de sécurité ouvert et pour afficher davantage d'enregistrements associés et de listes connexes, avec l'écran Score de risque d'incident affiché, appuyez sur un enregistrement de la liste.
7. Sur l'enregistrement ouvert qui s'affiche, choisissez une option dans la table suivante pour continuer.



Option	Description
Appuyez sur l'icône de menu en haut à droite de l'écran.	Dans le menu qui s'affiche, choisissez parmi les options suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	○ Appuyez sur **Modifier**. Avec l'écran Modifier l'incident de sécurité affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et entrer du texte. ○ Pour réaffecter l'incident, appuyez sur **Réaffecter** ou **Affecter à moi**. Suivez les instructions décrites dans le tableau précédent. Une fois que vous avez terminé vos modifications, appuyez sur l'icône Envoyer (icône  ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour l'incident de sécurité.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, examinez la piste d'audit des notes de travail, des activités et des commentaires supplémentaires de l'enregistrement. Appuyez sur l'icône Plus (icône ) pour ajouter une note de travail ou joindre un fichier.
Onglet Liste connexe	Une fois l'onglet Liste connexe sélectionné, affichez les éléments de l'une des listes connexes renseignées sur l'incident de sécurité. Appuyez sur un élément de la liste qui s'affiche pour afficher les détails d'une liste connexe. Dans les listes d'éléments affichées, appuyez sur un élément pour continuer à afficher les flux d'activité et les listes connexes associés à l'incident de sécurité parent.
Icônes d'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ○ Appuyez sur l'icône Incidents de sécurité pour revenir à l'écran d'accueil. ○ Si affiché, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ○ Appuyez sur **Notification** pour afficher les notifications de et ServiceNow AI Platform de .Application Security Incident Response Mobile ○ Appuyez sur **Paramètres** et choisissez-en un pour continuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	▪ Affichez des informations sur l'instance ServiceNow AI Platform sur votre appareil. ▪ Déconnectez-vous de l'instance actuelle ServiceNow AI Platform .

Rechercher des incidents de sécurité avec le Application Security Incident Response Mobile

Rechercher Réponse aux incidents de sécurité des incidents de sécurité (SIR) sur une ServiceNow AI Platform® instance. Seuls les incidents qui correspondent aux critères de recherche spécifiques que vous saisissez sont affichés.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Temps pour terminer cette tâche : 5 à 10 minutes.

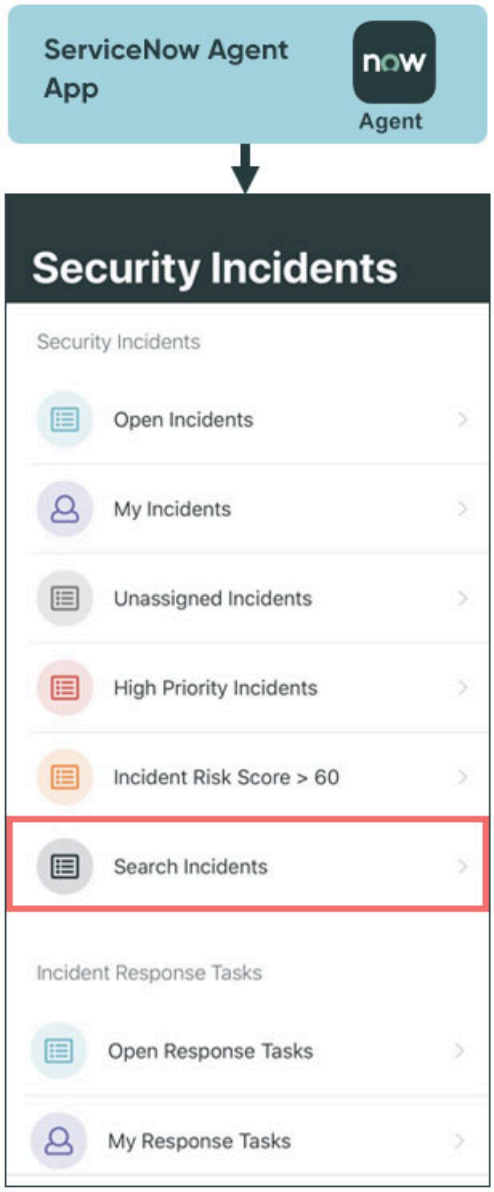
Procédure

1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.
2. Une fois l'écran d'accueil Incidents de sécurité affiché, appuyez sur **Rechercher des incidents**.

   Si vous quittez le Application Security Incident Response Mobile après vous être connecté, appuyez sur Now Agent à tout moment pour revenir au dernier écran que vous aviez affiché.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour limiter le nombre de résultats de recherche renvoyés, vous préférez peut-être remplir autant de champs que possible sur le formulaire.
Pour ajouter des critères de recherche, consultez le tableau suivant. Suivez les instructions après la table pour modifier les critères de recherche existants, effacer des critères de recherche ou soumettre une recherche.

Appuyer sur ce champ	Pour ajouter une entrée sur Android les appareils	Pour ajouter une entrée sur iOS les appareils
Numéro	Saisissez une valeur alphanumérique pour un incident de sécurité, par exemple, SIR0010004. Ce numéro est affiché dans le coin supérieur droit de l'incident de sécurité. La fonction recherche sur les chaînes numériques et les chaînes numériques	Saisissez une valeur alphanumérique pour un incident de sécurité, par exemple, SIR0010004. Ce numéro est affiché dans le coin supérieur droit de l'incident de sécurité. La fonction recherche sur les chaînes numériques et les chaînes numériques

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appuyer sur ce champ	Pour ajouter une entrée sur Android les appareils	Pour ajouter une entrée sur iOS les appareils
	partielles. Pour des recherches plus précises, saisissez plus de chiffres. Les laissez-passer (*) ne sont pas acceptés. Appuyez sur un nouveau champ pour entrer plus de critères ou sur pour soumettre une recherche.	partielles. Pour des recherches plus précises, saisissez plus de chiffres. Les laissez-passer (*) ne sont pas acceptés. Appuyez sur un nouveau champ pour entrer plus de critères ou sur **Rechercher** pour soumettre une recherche.
Description brève	Saisissez du texte dans le champ, par exemple, programme malveillant. La fonctionnalité recherche les chaînes de texte et les chaînes de texte partiel à partir du champ Brève description. Pour des recherches plus précises, saisissez plus de texte. Les laissez-passer (*) ne sont pas acceptés. Appuyez sur un nouveau champ pour entrer plus de critères ou sur pour soumettre une recherche.	Saisissez du texte dans le champ, par exemple, programme malveillant. La fonctionnalité recherche les chaînes de texte et les chaînes de texte partiel à partir du champ Brève description. Pour des recherches plus précises, saisissez plus de texte. Les laissez-passer (*) ne sont pas acceptés. Appuyez sur un nouveau champ pour entrer plus de critères ou sur **Rechercher** pour soumettre une recherche.
Priorité	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur l'icône de coche pour revenir à l'écran Rechercher des incidents.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des incidents.
Catégorie	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur l'icône de coche pour revenir à l'écran Rechercher des incidents.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des incidents.
État	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur l'icône de coche pour revenir à l'écran Rechercher des incidents.	Pour ajouter une entrée, appuyez sur un ou plusieurs éléments ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Appuyez sur **Terminé** pour revenir à l'écran Rechercher des incidents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appuyer sur ce champ	Pour ajouter une entrée sur Android les appareils	Pour ajouter une entrée sur iOS les appareils
Affecté à	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**.	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**.
Groupe d'affectation	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**.	Sélectionnez-en un dans la liste ou appuyez sur l'icône de recherche et tapez une entrée dans le champ de recherche. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**.

Pour Android les appareils, avec l'écran Rechercher des incidents affiché et tous vos critères saisis, choisissez-en un pour continuer.

Option	Description
Effacer ou modifier les critères de recherche avant d'exécuter une recherche	Pour effacer tous les critères saisis, avec l'écran Rechercher des incidents affiché, appuyez sur la flèche arrière pour effacer tous les champs et revenir à l'écran d'accueil Incidents de sécurité. La recherche n'est pas soumise et les critères de recherche sont effacés. Vous pouvez également modifier un champ : ○ Une fois l'écran Rechercher des incidents affiché, appuyez sur un champ contenant des critères de recherche pour le développer. ○ Appuyez sur un élément pour le désélectionner. Appuyez sur **Tout** pour sélectionner tous les éléments. Appuyez à nouveau sur **Tout** pour effacer tous les éléments. Pour effacer une valeur pour le groupe d'affectation et les champs Affecté à, pour aucune entrée, sélectionnez **Aucun**. ○ Appuyez sur l'icône de coche pour enregistrer les changements et revenir à l'écran Rechercher des incidents.
Soumettre une recherche	Une fois l'écran Rechercher des incidents affiché avec vos critères de recherche saisis, appuyez sur l'icône Envoyer (icône).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Les incidents de sécurité qui corres–pondent à vos critères de recherche s'af–fichent. Une fois la recherche terminée, les critères de recherche ne sont pas enregis–trés.

4. Pour iOS les appareils, avec l'écran Rechercher des incidents affiché, choisissez-en un pour continuer.

Option	Description
Effacer ou modifier les critères de recherche avant d'exécuter une recherche	Pour effacer tous les critères et revenir à l'écran d'accueil, appuyez sur l'icône de fermeture (X). Les critères de recherche saisis ne sont pas enregistrés. Vous pouvez également modifier un champ : ○ Une fois l'écran Rechercher des incidents affiché, appuyez sur un champ contenant des critères de recherche pour le déve–lopper. ○ Appuyez sur un élément de la liste pour le désélectionner ou appuyez sur **Tout effacer**. Pour effacer une valeur pour le groupe d'affectation et les champs Af–fecté à, pour aucune entrée, sélectionnez **Aucun**. ○ Appuyez sur **Terminé** pour enregistrer les changements et revenir à l'écran Re–chercher des incidents.
Soumettre une recherche	Avec l'écran Rechercher des incidents affiché avec vos critères de recherche saisis, appuyez sur **Recher cher**. Les incidents de sécurité qui corres–pondent à vos critères de recherche s'af–fichent. Une fois la recherche terminée, les critères de recherche ne sont pas enregis–trés.

5. **Facultatif :** Si votre recherche renvoie plusieurs enregistrements, vous pouvez Filtrer les enregistrements avec le Application Security Incident Response Mobile affiner les résultats de la recherche.

Affichez, modifiez et affectez des tâches de réponse ouvertes avec le Application Security Incident Response Mobile

Affichez, modifiez et affectez des tâches de réponse ouvertes. Vos modifications sont enregistrées dans la tâche Réponse aux incidents de sécurité de l'incident de sécurité parent.

Avant de commencer

Rôle requis : sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

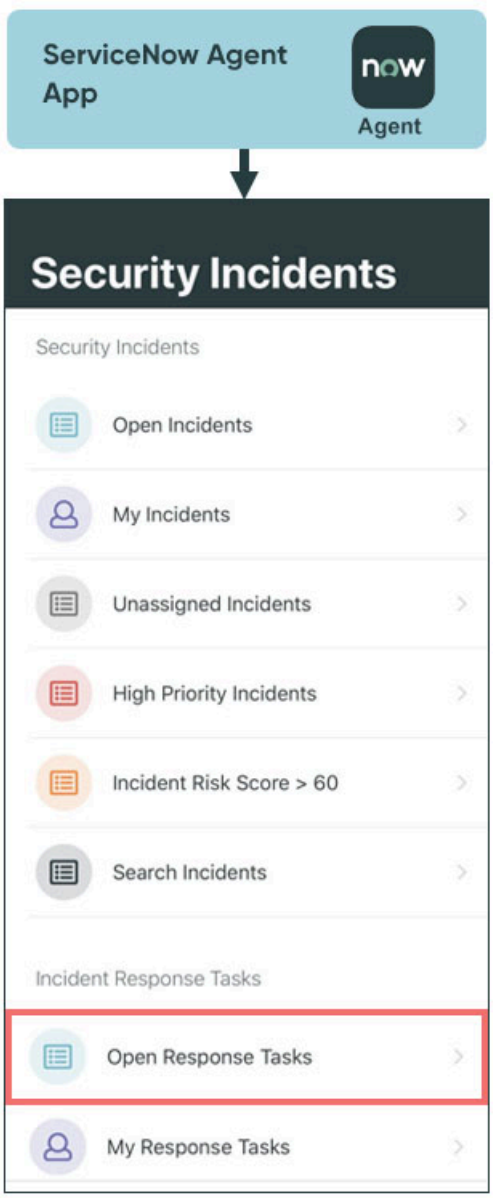
Pourquoi et quand exécuter cette tâche

Dans la liste des enregistrements, affectez une tâche de réponse ouverte et non affectée à vous-même ou à un autre analyste de votre groupe. Vous pouvez également afficher les détails de l'enregistrement ou ajouter une note de travail avant l'affectation. Temps pour terminer cette tâche : 5 à 10 minutes.

Procédure

1. Si vous n'êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.
2. Lorsque l'écran d'accueil Incidents de sécurité s'affiche, appuyez sur **Tâches de réponse ouvertes**.

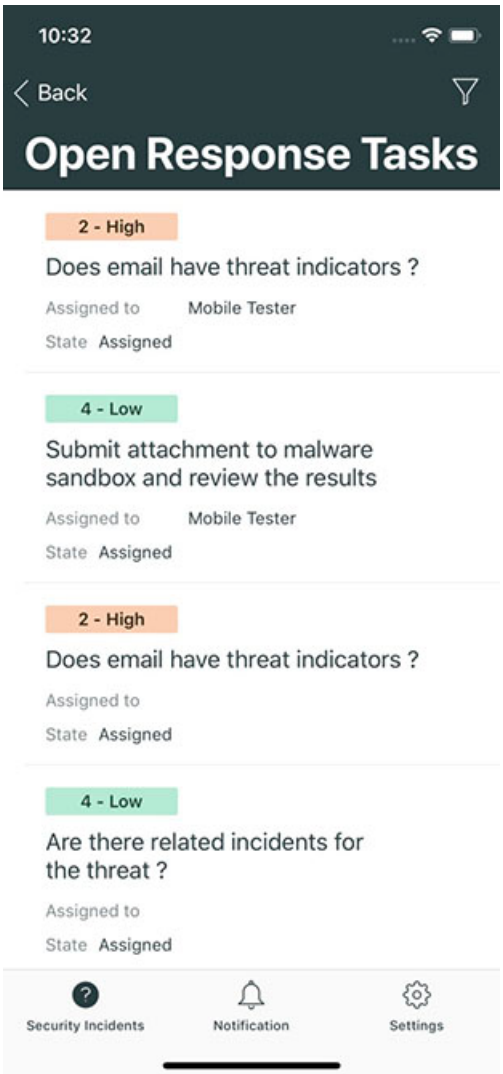
   Si vous quittez le Application Security Incident Response Mobile après vous être connecté, appuyez à tout moment sur l'application Now Agent pour revenir au dernier écran que vous aviez affiché.



L'écran Tâches de réponse ouvertes s'affiche avec une liste de tâches ouvertes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. **Facultatif :** Reportez-vous à Rechercher des incidents de sécurité avec le Application Security Incident Response Mobile la recherche de tâches qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre (icône affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.

4. Une fois la liste des tâches de réponse ouvertes affichée, pour affecter ou réaffecter directement à partir de la liste, faites glisser un enregistrement vers la gauche pour ouvrir le menu.

5. Choisissez-en un pour continuer.

Option	Description
Mes affectations	Vous affecter la tâche de réponse. Si la tâche vous est déjà affectée, cette option ne s'affiche pas.
Réaffecter	Pour affecter ou réaffecter le groupe d'affectation : **a. Appuyer sur Groupe d'affectation** **b.** Appuyez sur un groupe dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Le groupe doit être un groupe d'affectation lié à la sécurité.

Traduction automatique

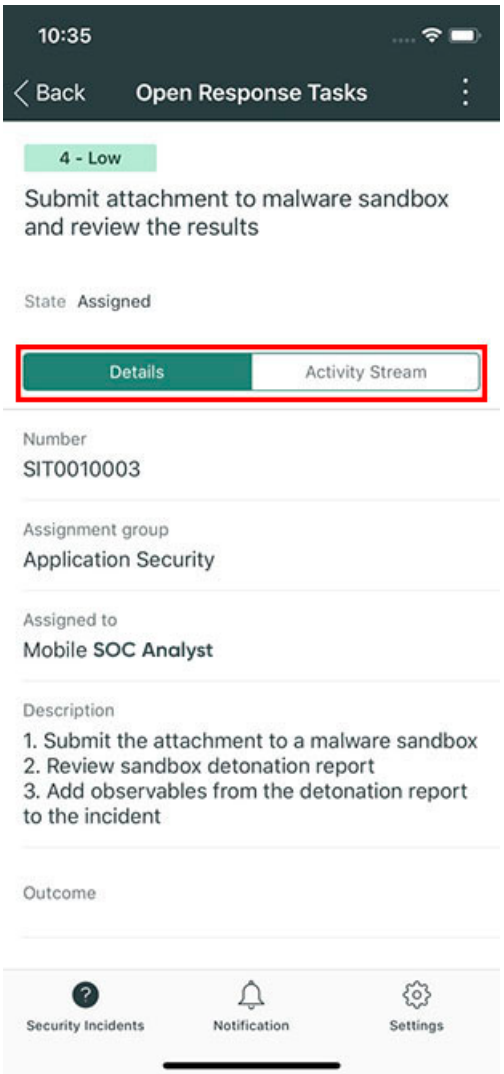
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Pour affecter ou réaffecter la tâche à un membre du groupe d'affectation : **a.** Appuyez sur **Affecté à** et **b.** Appuyez sur un nom dans la liste qui s'affiche ou saisissez du texte dans le champ de recherche. Un message s'affiche pour confirmer la mise à jour de l'enregistrement. La tâche sur l'incident de sécurité parent est affectée à un nouvel utilisateur et mise à jour dans votre ServiceNow AI Platform instance. Appuyez sur l'icône Envoyer (icône  ou sur **Soumettre** pour enregistrer et soumettre vos modifications.

6. Alternativement, pour afficher les détails d'un enregistrement de tâche de réponse ouvert, avec l'écran Tâches de réponse ouvertes affiché, appuyez sur un enregistrement de la liste.
7. Une fois les onglets de l'enregistrement de tâche de réponse affichés, choisissez-en un dans la table suivante pour continuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Onglet Détails	Une fois l'onglet Détails sélectionné, examinez les champs de la tâche de réponse. Pour modifier des champs ou affecter la tâche, appuyez sur l'icône de menu (icône Dans le menu qui s'affiche, choisissez parmi les options suivantes. ○ Appuyez sur **Modifier**. Avec l'écran Modifier la tâche de réponse affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options qui s'affichent. Vous pouvez également appuyer sur l'icône de recherche et entrer du texte. ○ Pour réaffecter la tâche, appuyez sur **Réaffecter** ou **Affecter à moi**. Une fois vos modifications terminées, appuyez sur l'icône Envoyer (icône ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour l'enregistrement. La

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	tâche Réponse aux incidents de sécurité sur l'incident de sécurité parent dans votre ServiceNow AI Platform instance est mise à jour.
Onglet Flux d'activité	Une fois l'onglet Flux d'activité sélectionné, choisissez-en un pour continuer. ○ Affichez la piste d'audit créée par les notes de travail dans l'enregistrement. Pour ajouter une note de travail ou joindre un fichier, appuyez sur l'icône Plus (icône). ○ Appuyez sur l'icône de menu (icône pour modifier ou réaffecter la tâche.
Icônes d'écran en bas de l'écran.	En bas de l'écran, choisissez-en un pour continuer. ○ Si affiché, appuyez sur une icône pour ouvrir une autre ServiceNow® application mobile. ○ Appuyez sur **Notification** pour afficher les notifications relatives aux incidents de sécurité critiques qui vous sont affectés ou à votre groupe d'affectation. ○ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez les informations relatives à l'instance ServiceNow AI Platform . ▪ Déconnectez-vous de l'instance ac–tuelle. Pour vous déconnecter d'une ServiceNow AI Platform instance sur votre appareil, avec la page de détails **affi chée**, appuyez sur Déconnexion.

Traduction automatique

Affichez, modifiez et réaffectez vos tâches de réponse avec le Application Security Incident Response Mobile

Affichez, modifiez et réaffectez les tâches de réponse qui vous sont affectées. Vos modifications sont enregistrées dans la tâche Réponse aux incidents de sécurité de l'incident de sécurité parent.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

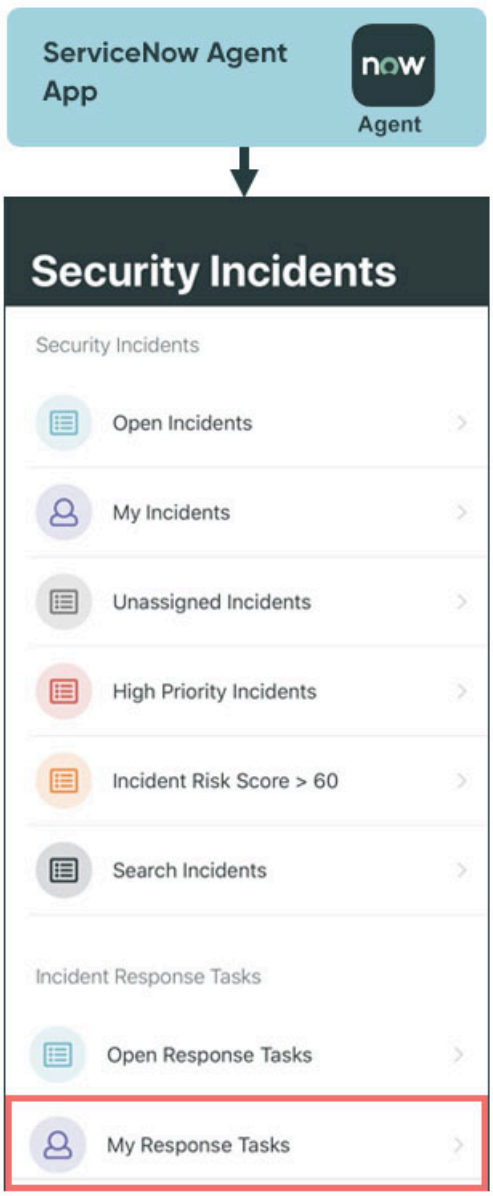
Dans la liste des enregistrements, réaffectez une tâche de réponse ouverte qui vous est affectée à un autre analyste de votre groupe. Vous pouvez également afficher les détails de l'enregistrement ou ajouter une note de travail avant la réaffectation. Temps pour terminer cette tâche : 5 à 10 minutes.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Si vous n’êtes pas connecté à votre ServiceNow AI Platform instance sur votre équipement mobile, reportez-vous à la section Connectez-vous au Application Security Incident Response Mobile.
2. Lorsque l’écran d’accueil Incidents de sécurité s’affiche, appuyez sur **Mes tâches de réponse**.

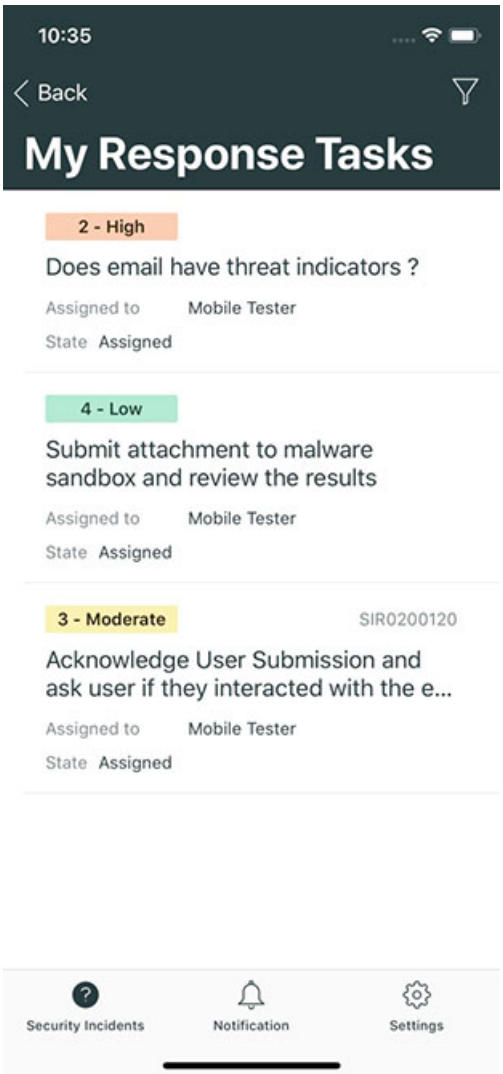
   Si vous sortez de après Application Security Incident Response Mobile vous être connecté, appuyez à tout moment sur l’application Now Agent (prestataire) pour revenir au dernier écran que vous aviez affiché.



L’écran Mes tâches de réponse s’affiche avec une liste des tâches de réponse qui vous sont affectées.

Traduction automatique

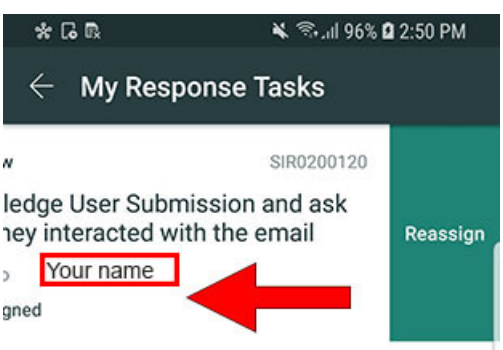
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. **Facultatif :** Reportez-vous à Rechercher des incidents de sécurité avec le Application Security Incident Response Mobile la recherche de tâches qui correspondent à des critères spécifiques.

   Alternativement, avec l'icône de filtre ( ) affichée, définissez des filtres pour limiter le nombre d'enregistrements dans la liste. Le filtrage des enregistrements sur les écrans de l'application mobile fonctionne comme avec un créateur de conditions sur le ServiceNow AI Platform.

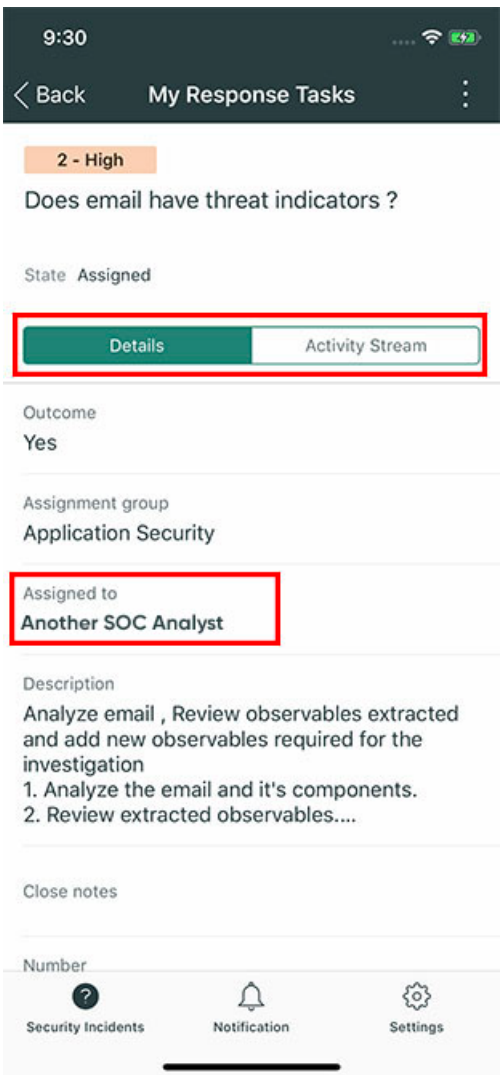
4. Pour réaffecter une tâche directement à partir de la liste des enregistrements de tâches qui vous sont affectés, faites glisser un enregistrement vers la gauche pour ouvrir le menu.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

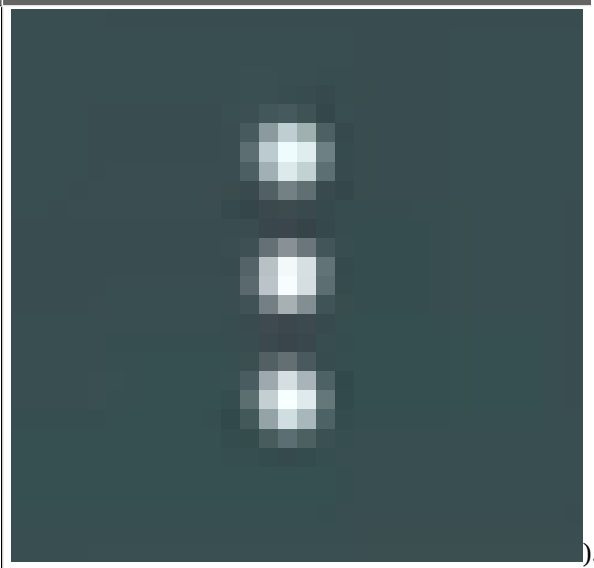
5. Appuyez sur **Réaffecter**.
6. Sur l'écran Affecter une tâche de réponse à un autre qui s'affiche, appuyez sur un champ pour le développer et sélectionnez un autre groupe ou utilisateur pour la tâche.
7. Appuyez sur l'icône d'envoi ( ) ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour la tâche de réponse.
   Un message s'affiche pour confirmer la mise à jour de l'enregistrement. La tâche est affectée à un nouvel utilisateur sur l'incident de sécurité parent et votre ServiceNow AI Platform instance est mise à jour.
8. Pour afficher les détails d'une tâche de réponse ouverte et les notes de travail, avec l'écran Mes tâches de réponse affiché, appuyez sur un enregistrement de la liste.
9. Une fois les champs de la tâche de réponse affichés, choisissez-en un dans la table suivante pour continuer.



Option	Description
Onglet Détails	Une fois l'onglet Détails sélectionné, examinez les champs de la tâche de réponse. Pour modifier des champs ou réaffecter la tâche, appuyez sur l'icône de menu (

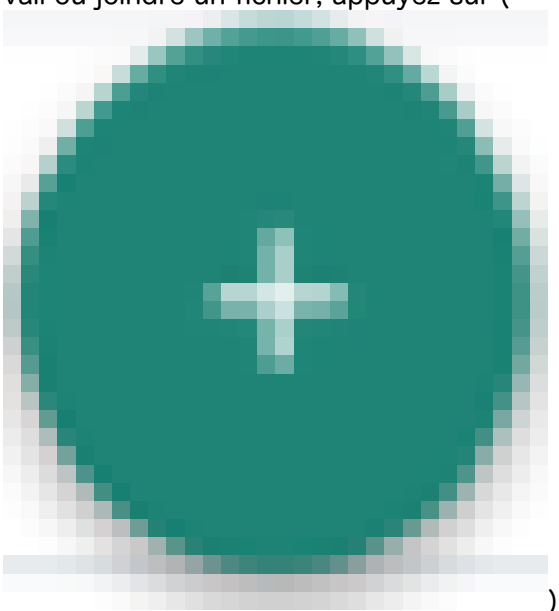
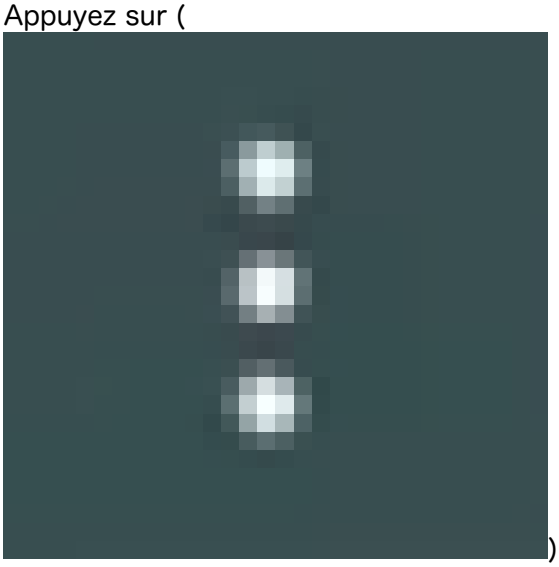
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	). Dans le menu qui s’affiche, choisissez parmi les options suivantes. ○ Appuyez sur **Modifier**. Avec l’écran Modifier la tâche de réponse affiché, appuyez sur un champ pour le développer et choisissez une ou plusieurs des options affichées. Vous pouvez également appuyer sur l’icône de recherche et entrer du texte. ○ Pour réattribuer la tâche, appuyez sur **Affecter à un autre**. Une fois vos modifications terminées, appuyez sur l’icône d’envoi () ou sur **Soumettre** pour enregistrer vos modifications et mettre à jour l’enregistrement. La tâche Réponse aux incidents de sécurité sur l’incident de sécurité parent dans votre ServiceNow AI Platform instance est mise à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Onglet Flux d’activité	Une fois l’onglet Flux d’activité sélectionné, choisissez-en un pour continuer. ○ Affichez la piste d’audit créée par les notes de travail sur l’enregistrement de tâche. Pour ajouter une note de tra–vail ou joindre un fichier, appuyez sur (). ○ Appuyez sur () pour modifier ou réaffecter la tâche.
Appuyez sur une icône d’écran en bas de l’écran.	En bas de l’écran, choisissez-en un pour continuer. ○ Si elle s’affiche, appuyez sur une autre icône pour ouvrir une autre ServiceNow® application principale et l’ouvrir. ○ Appuyez sur **Notification** pour afficher les notifications relatives aux incidents de sécurité critiques qui vous sont affectés ou à votre groupe d’affectation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	○ Appuyez sur **Paramètres** et choisissez-en un pour continuer. ▪ Affichez les informations relatives à l'instance ServiceNow AI Platform . ▪ Déconnectez-vous de l'instance ac–tuelle. Pour vous déconnecter d'une ServiceNow AI Platform instance sur votre appareil, avec la page de détails **affi chée**, appuyez sur Déconnexion.

Filtrer les enregistrements avec le Application Security Incident Response Mobile

Définissez des filtres supplémentaires pour limiter le nombre d'enregistrements qui s'affichent sur un écran. Le filtrage des enregistrements au sein de l'application mobile fonctionne comme avec un créateur de conditions sur ServiceNow AI Platform.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Temps nécessaire pour accomplir cette tâche : 5 minutes.

Procédure

1. Pour affiner les résultats de votre recherche ou pour entrer des critères de filtrage supplémentaires sur toute liste d'enregistrements affichée, appuyez sur l'icône de filtre (icône 
2. Une fois l'écran Filtres affiché, appuyez sur un champ pour le développer.
3. Parmi les options affichées, cochez la case ou appuyez sur un élément de votre filtre.
   Pour de nombreux filtres, vous pouvez sélectionner plus d'une option.
4. Appuyez sur la flèche arrière (icône  ou sur **TERMINÉ** pour enregistrer vos modifications dans un champ.
   Les critères que vous avez choisis s'affichent sur l'écran Filtres. Le nombre d'enregistrements qui correspondent à vos critères est également affiché en haut de l'écran. Appuyez sur **RÉINITIALISER** pour supprimer tous les filtres et restaurer le paramètre par défaut.
5. **Facultatif :** Répétez les étapes 1 à 4 avec l'écran Filtres affiché pour continuer à définir vos critères de filtrage.
6. Appuyez sur l'icône d'intersection  pour créer des conditions ET.
   Vous pouvez également appuyer sur l'icône d'intersection afin de créer des conditions OU.
7. Une fois que vous avez ajouté tous les critères souhaités, avec l'écran Filtres affiché, appuyez sur **TERMINÉ.**
   À l'écran, seuls les enregistrements qui correspondent à vos critères de filtre sont affichés.

Orchestration de la réponse aux incidents de sécurité

Orchestration de la réponse aux incidents de sécurité Les activités permettent aux utilisateurs d'interagir avec des systèmes et environnements Windows ou UNIX et de les récupérer à l'aide de l'orchestration de workflow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer

Avant d'utiliser Orchestration de la réponse aux incidents de sécurité, effectuez les étapes de configuration de diverses parties du système, notamment le remplissage de la CMDB, la configuration du serveur MID et la configuration des informations d'identification.

Avant de commencer

Rôle requis : admin

Pour utiliser Réponse aux incidents de sécurité, vous avez besoin d'une CMDB complète avec des noms de domaines. Pour plus d'informations, consultez Découverte .

Pourquoi et quand exécuter cette tâche

Procédure

1. Activez le Réponse aux incidents de sécurité module d'extension.
2. Configuration des serveurs MID .
3. Configurez les informations d'identification du service Windows MID Server .

Comprendre les workflows et les modèles de workflow d'Orchestration de Réponse aux incidents de sécurité

Le Réponse aux incidents de sécurité système de base comprend une série de workflows et de modèles de workflow conçus pour fonctionner avec les enregistrements d'incidents de sécurité.

Avant de commencer

Rôle requis : sn_si.basic

Pourquoi et quand exécuter cette tâche

Vous pouvez adapter tous les workflows et modèles de workflow pour mieux répondre à vos besoins, en supposant que vous disposez du rôle approprié : sn_sec_cmn.admin. Les workflows sont utilisés dans l'ensemble du système Security Operations pour effectuer diverses tâches.

Les modèles de workflow, cependant, sont déclenchés en sélectionnant une valeur dans le champ **Catégorie** d'un incident de sécurité. Lorsque cela se produit, le modèle de workflow associé à la sélection déclenche un modèle de workflow qui indique aux analystes de sécurité comment gérer un type spécifique de menace.

Par exemple, si vous sélectionnez **Déni de service** dans le champ **Catégorie** d'un incident de sécurité, le **modèle Incident de sécurité - Déni de service - est** exécuté et l'analyste est chargé de déterminer si la cible du DOS est critique pour l'entreprise. Si tel est le cas, la tâche suivante fait en sorte que la priorité de l'incident de sécurité est définie sur **1 - Critique**, puis exécute la tâche suivante. Et ainsi de suite.

Ainsi Réponse aux incidents de sécurité , les workflows et les modèles de workflow sont essentiellement les mêmes, sauf que les modèles sont utilisés pour un ensemble spécifique de fonctions au sein d'un incident de sécurité.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Workflows** > **Voir les workflows de sécurité**.
2. La liste des workflows et des modèles de workflow expédiés dans le système de base s'affiche.
   Tous les nouveaux workflows que vous avez créés dans la suite d'applications Opérations de sécurité sont également inclus dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur le nom du workflow ou du modèle de workflow que vous souhaitez afficher.

> **Remarque :** Les workflows peuvent être déclenchés de plusieurs façons différentes. Sachez que l'association d'un workflow à un déclencheur de workflow ne signifie pas nécessairement que le workflow est actif.

Orchestration de la réponse aux incidents de sécurité Workflows et activités

Plusieurs workflows et activités sont inclus dans Orchestration de la réponse aux incidents de sécurité.

Seuls les utilisateurs disposant du rôle sn_sec_cmn.admin peuvent le faire Éditeur de workflow .

Créer une demande de recherche de workflow de changements IoC

Le flux **Security Incident Response - Créer une demande de recherche de changements d'IoC** est déclenché par une règle métier pour s'exécuter automatiquement lorsqu'un IoC est ajouté ou modifié. Les analyses anti-programmes malveillants ne sont déclenchées que lorsque de nouvelles données sont saisies et que seules les nouvelles données sont analysées.

Avant de commencer
Rôle requis : sn_si.basic

Pourquoi et quand exécuter cette tâche
Si l'IoC est vide, le workflow ne s'exécute pas. Les analyses historiques sont conservées et consultables dans l'onglet **Demandes d'analyses de sécurité** et dans les notes de travail de l'incident de sécurité. Les incidents de sécurité existants sont automatiquement mis à jour.

> **Important :**
>
> Le workflow **Réponse aux incidents de sécurité : créer une demande de recherche de changements IoC** est migré vers Concepteur de flux. Le flux n'est déclenché que lorsque l'sn_ti_scanner a au moins un enregistrement.

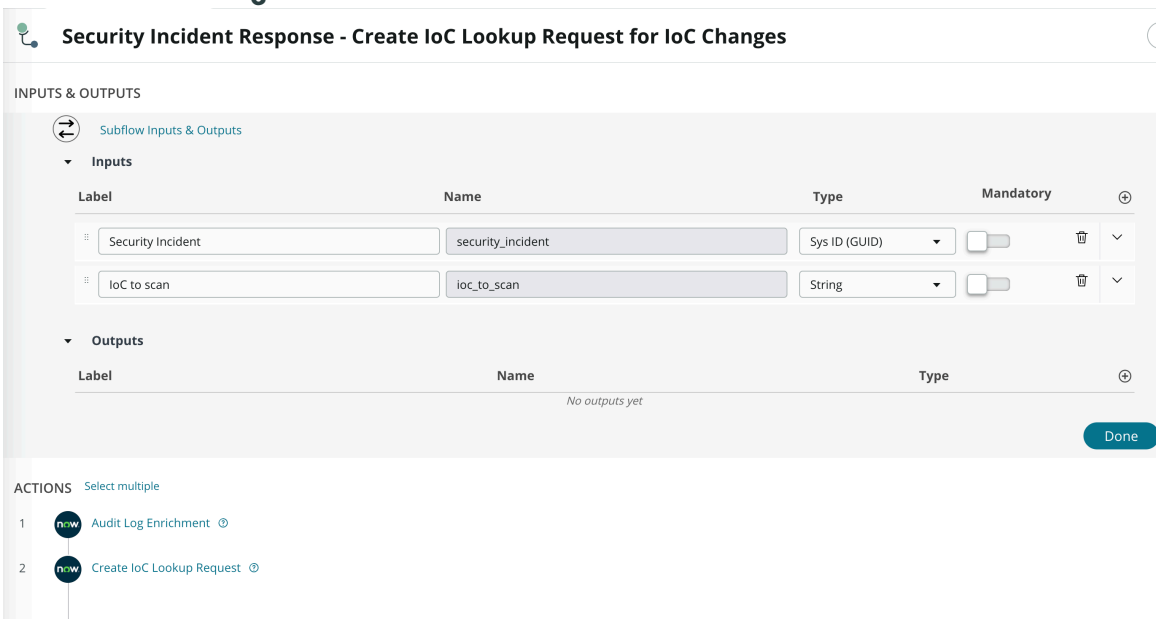
Les actions de Flow Designer incluent :

- Enrichissement du journal d'audit
- Créer une activité de demande de recherche d'IoC

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow des changements IoC



Créer une activité de demande de recherche d'IoC

L'activité Créer une demande de recherche d'IoC peut être utilisée avec n'importe quel workflow pour créer une demande de recherche de programme malveillant pour les champs d'IoC ajoutés ou modifiés.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Demande de recherche créée.
Échec	Demande de recherche non créée.

Variables d'entrée

Variable	Description
iocChaîne	Informations IoC au format JSON. IP, hachage, url.
siId	Identificateur système de l'incident de sécurité

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
ID scnReqID	Identificateur de demande de recherche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Incident Response - Obtenir le flux de statistiques réseau

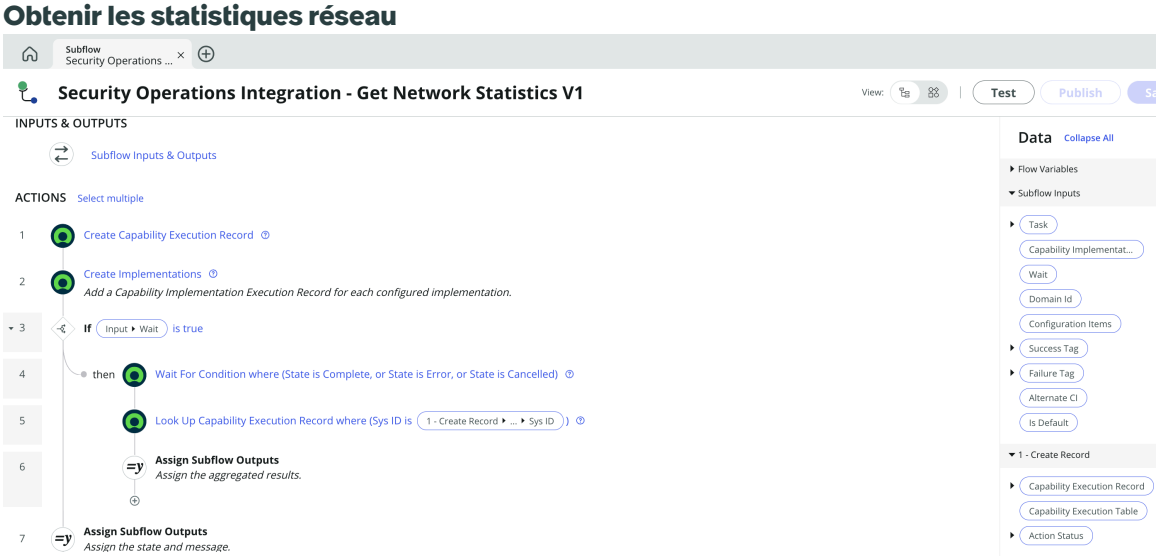
Le champ **Security Incident Response** > **Obtenir les statistiques réseau** le flux récupère les statistiques réseau d'une ressource Windows affectée lorsqu'elle est ajoutée à un incident de sécurité à l'état **Analyse** .

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Pour les nouveaux incidents de sécurité qui contiennent des éléments de configuration, le flux s'exécute automatiquement lorsque l'état passe à **Analyse**

Les incidents de sécurité existants sont automatiquement mis à jour lorsque vous êtes dans l'état **Analyse** et que vous ajoutez un nouvel élément de configuration.

Obtenir les statistiques réseau



Les actions de processus de flux comprennent :

- Obtenir le FQDN de l'élément de configuration Action de flux
- Déterminer le script Shell par système d'exploitation
- Si l'instruction est exécutée par Powershell
- Suivi de l'exécution : commencer l'action de flux
- Obtenir les statistiques réseau via netstat Action de flux
- Suivi de l'exécution de l'aptitude : action de flux d'échec
- Créer des enregistrements de données d'enrichissement Action de flux
- Suivi de l'exécution de l'aptitude : action de flux d'échec - Renvoie l'ID d'enrichissement.
- Suivi de l'exécution de l'aptitude : terminer l'action de flux

Procédure

1. Ouvrez un incident de sécurité.
2. Mettez à jour **l'état** sur **Analyse**, si nécessaire.
3. Ajoutez un élément de configuration (ordinateur, serveur ou similaire).
4. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Orchestration de la réponse aux incidents de sécurité fournit des informations statistiques sur le réseau dans le **Liens connexes** > **Enrichissements des incidents de sécurité** onglet. Pour plus d'informations, reportez-vous à la section Opérations de sécurité Mappage des données d'enrichissement.

Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Workflow Security Incident Response - Get Running Services

Le **workflow Réponse aux incidents de sécurité - Obtenir des services d'exécution** récupère une liste des services en cours d'exécution à partir des éléments de configuration (CI) basés sur Windows. ServiceNow Ce workflow est utilisé pour l'enrichissement des incidents au cours des enquêtes.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Le **workflow Réponse aux incidents de sécurité - Obtenir des services d'exécution** s'exécute automatiquement lorsque vous ajoutez un nouvel élément de configuration à un incident de sécurité Windows après que l'état a changé en **Analyse**. Les informations obtenues par ce workflow apparaissent dans les onglets **Afficher les données d'enrichissement** pour l'incident de sécurité.

Remarque : Si l'incident de sécurité reste à l'état **Brouillon** , le workflow **Réponse aux incidents de sécurité - Obtenir des services d'exécution** ne s'exécute pas.

Les activités du workflow comprennent :

Activité de script d'enrichissement du journal d'audit

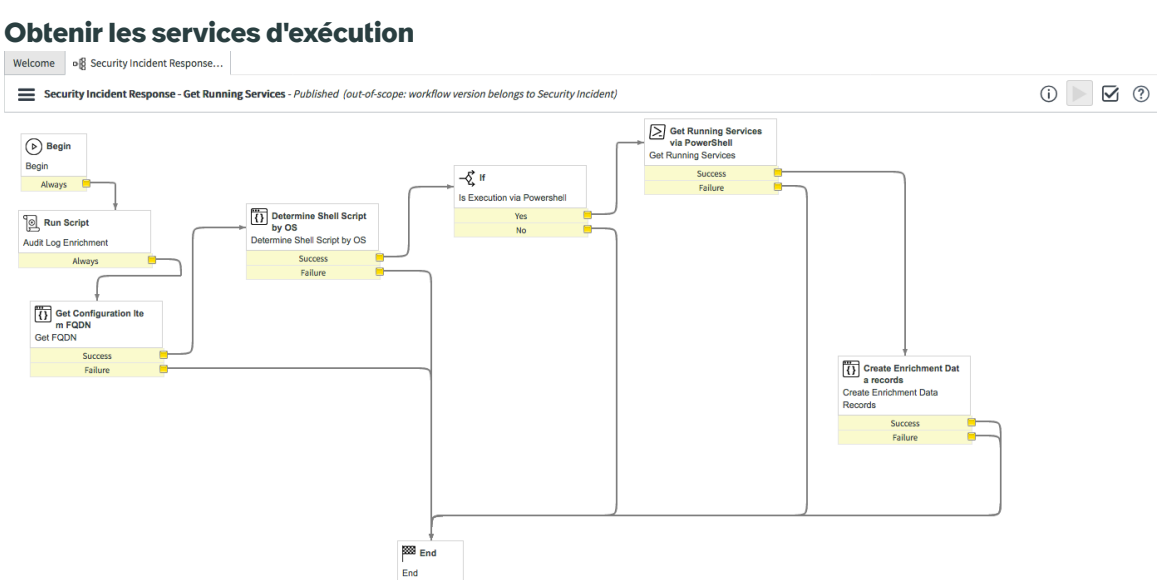
Obtenir le FQDN de l'élément de configuration Action de flux

Déterminer le script Shell par activité du système d'exploitation

Est une activité de l'exécution via PowerShell

Obtenir les services d'exécution : activité d'enrichissement WMI

Créer des enregistrements de données d'enrichissement Action de flux



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez un incident de sécurité.
2. Mettez à jour **l'état** sur **Analyse**, si nécessaire.
3. Ajoutez un élément de configuration Windows (serveur, ordinateur portable ou similaire).
4. Cliquez sur **Mettre à jour**.
   Réponse aux incidents de sécurité Fournit des informations sur les services d'exécution dans le **Liens connexes** > **Enrichissements des incidents de sécurité**onglet. Pour plus d'informations, consultez Opérations de sécurité Mappage des données d'enrichissement.

Déterminer le script Shell par activité du système d'exploitation

L'activité de workflow Déterminer le script Shell par système d'exploitation détermine le système d'exploitation à utiliser dans le workflow

L'activité Déterminer le script Shell par système d'exploitation peut être utilisée avec n'importe quel workflow pour déterminer quel script shell exécuter en fonction du système d'exploitation exécuté sur le système contenant l'élément de configuration.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Système d'exploitation trouvé.
Échec	Aucun système d'exploitation trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
ciSysId	Identificateur système de l'élément de configuration.
processType	Identificateur interne qui définit le script à extraire de la table.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
processScript	Agent ECC qui rassemble le processus d'exécution.
modèle d'exécution	Détermine si le script est exécuté via une sonde ou à l'aide de PowerShell.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
enrichmentMappingId	Identificateur système du mappage d'enrichissement utilisé pour transformer les données de réponse.

Obtenir les services d'exécution : enrichissement WMI

Le workflow **Réponse aux incidents de sécurité - Get Running Services** rassemble les services en cours d'exécution sur un élément de configuration ajouté à un incident de sécurité.

L'activité Obtenir les services d'exécution - Enrichissement WMI est lancée automatiquement pour récupérer les informations des services en cours d'exécution pour un hôte Windows.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
Cible [chaîne]	Nom de domaine complet (FQDN) du système cible.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Réponse [chaîne]	Chaîne JSON représentant les services en cours d'exécution sur le système cible. Les données JSON comprennent : **nom** Le nom du service **pid** Identificateur de processus du service d'exécution **service_type** (Facultatif) Type de service d'exécution. **start_name** Nom du système pour le service **chemin d'accès** Chemin d'accès au fichier de l'exécutable du service en cours d'exécution **start_mode** Mode de démarrage du service en cours d'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
	display_name Nom du service d'exécution tel qu'il apparaît à l'utilisateur

Restrictions

Le Serveur MID doit prendre en charge **PowerShell**.

Le hachage SHA-256 nécessite PowerShell V4.

Exécuter le flux de procdump

Le flux **Exécuter le procdump** exécute un vidage de processus sur un processus spécifié et l'enregistre dans un fichier qui peut être ciblé par les analystes de sécurité.

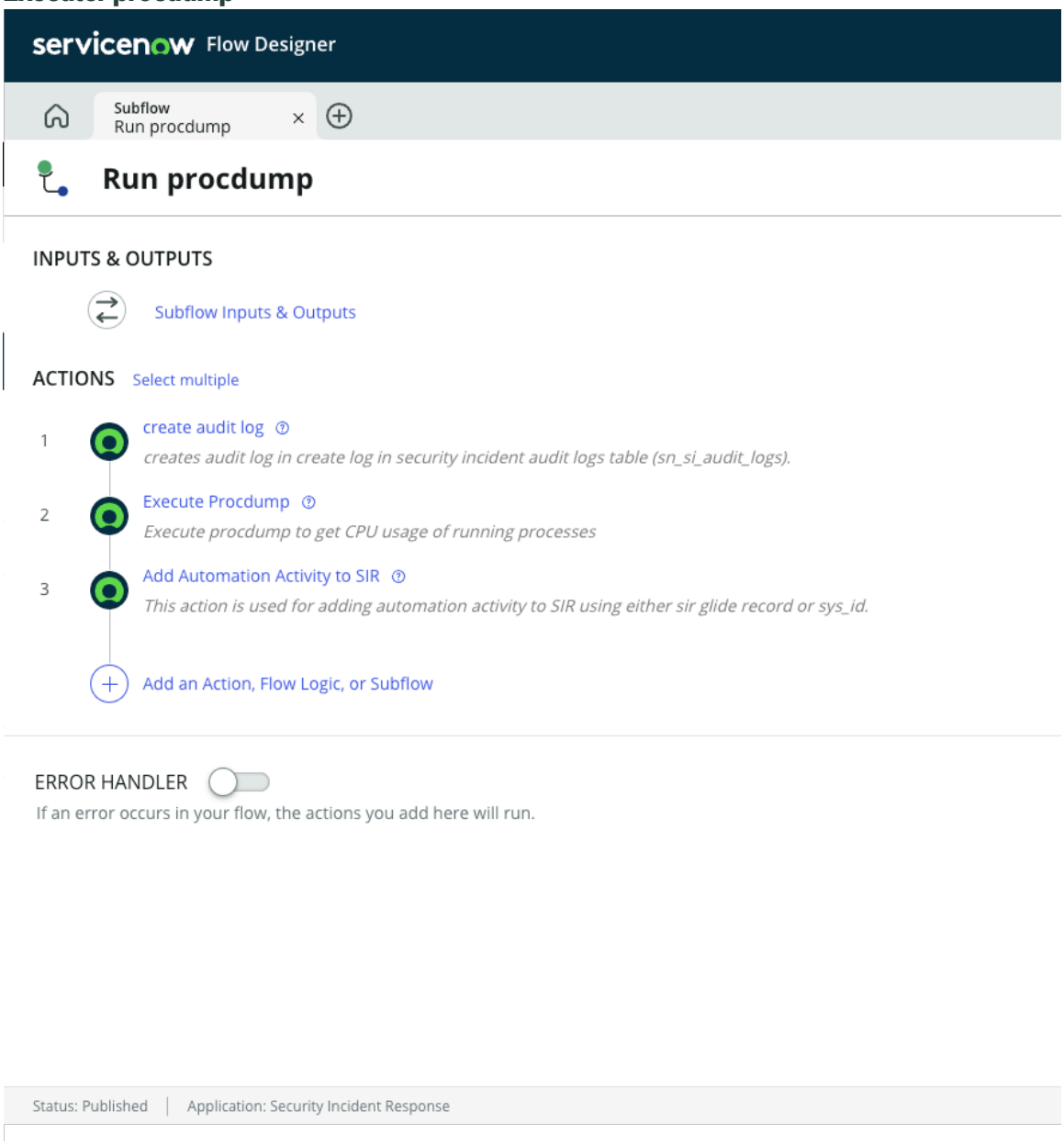
Rôle requis : sn_si.analyst

Ce flux est déclenché lorsque des processus enrichis sont sélectionnés et qu'une action d'interface utilisateur **Exécuter le procdump** est exécutée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exécuter procdump



Les raisons pour lesquelles le procdump peut échouer sont les suivantes :

- Chemin de vidage non valide
- Chemin de partage de fichier non valide
- Impossible d'extraire le nom de domination complet de l'ordinateur Windows sur lequel le procdump s'exécute
- Le nom du processus n'est pas spécifié
- Variable d'environnement PROCDUMP introuvable
- Une copie du fichier dump ne parvient pas à être copiée du chemin d'accès au partage de fichiers

Exécuter l'action procdump

Exécuter procdump est une action Powershell qui exécute le procdump sur les processus sélectionnés, vide les données dans un fichier et les publie sur un site partagé sur un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

réseau interne. Un analyste peut alors afficher un processus sur liste de refus, surligné en rouge dans un incident de sécurité, et effectuer une analyse supplémentaire du fichier.

Résultats

Les résultats possibles pour cette action sont les suivants :

Résultats

Résultat	Description
Réussite	Le procdump a été exécuté avec succès sur la process_name et les détails sont disponibles dans actionOutput.response.
Échec	Échec de l'exécution du procdump sur le process_name et les détails sont disponibles dans actionOutput.response.

Variables d'entrée

Les variables d'entrée sont utilisées pour créer les sorties demandées.

Variables d'entrée

Variable	Description
targetId	[Obligatoire] ID cible sur lequel exécuter le procdump.
process_name	[Obligatoire] Nom du processus pour le procdump.
dump_path	[Obligatoire] Chemin d'accès au fichier local dans lequel le fichier dump généré sera enregistré.
dump_filename	[Obligatoire] Nom de fichier du fichier généré par le procdump. Tous les caractères spéciaux seront remplacés par des traits d'union (-) du nom du fichier dump lors de la génération du fichier.
file_share_path	[Obligatoire] Chemin d'accès du partage de fichier vers lequel le fichier dump sera copié.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
share_path	Chemin d'accès du partage de fichier vers lequel le fichier dump a été copié.
réponse	Représentation JSON du résultat du procdump.
résultat	Résultat du procdump.

Incident de sécurité - Évaluer le workflow des résultats de tâche de réponse

Incident de sécurité - Évaluer le workflow de résultat de tâche de réponse détermine la tâche à utiliser, invoque un workflow choisi et un script d'évaluation en fonction de l'enregistrement de l'évaluateur de résultat fourni comme entrée dans le workflow choisi.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche
Ce workflow est destiné à s'exécuter en même temps que l'activité de création de tâche à évaluer. Le script d'évaluation interroge les artefacts (tels que les observations, les enregistrements de recherche ou les processus en cours d'exécution) de l'option configurée à l'aide des informations contextuelles de la tâche de réponse (telle que son incident de sécurité parent) pour déterminer le résultat approprié pour la tâche de réponse. Le résultat peut potentiellement dépendre de l'activité du workflow, mais est généralement **oui** ou **non**. Lors de la création d'un enregistrement d'évaluateur de résultats, seules les options qui ont un workflow configuré, avec la case **Est une option basée sur les tâches** cochée et un jeu de variables d'entrée de tâche sont disponibles à la sélection.

Les activités du processus de workflow comprennent :

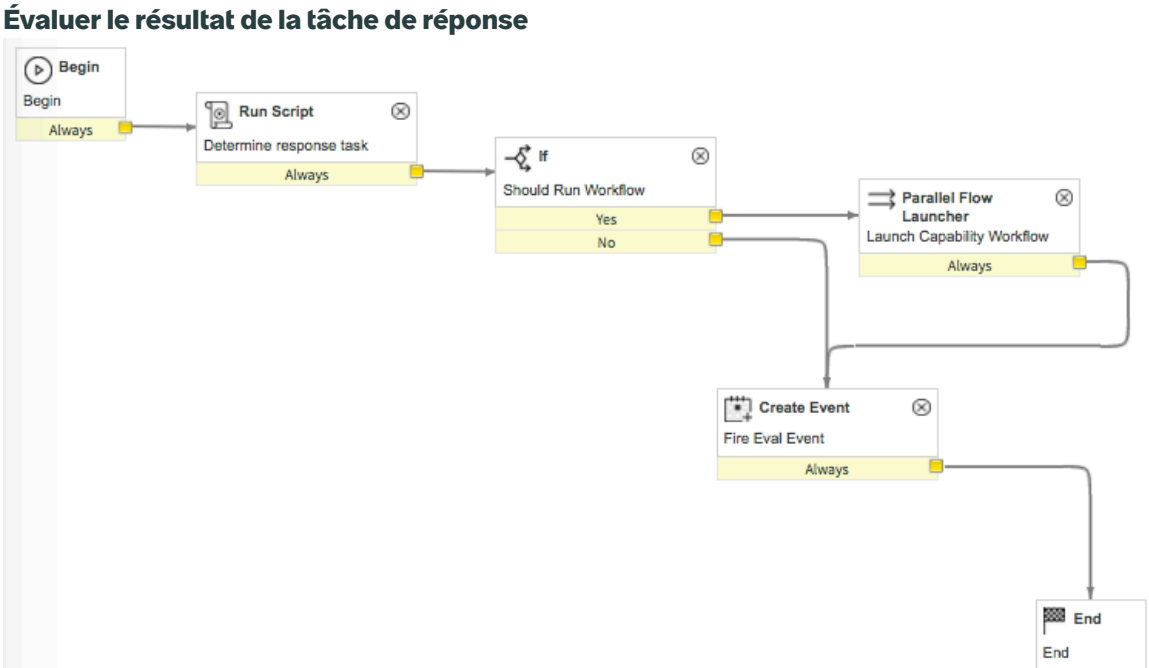
Exécuter un script pour déterminer la tâche de réponse

Doit exécuter le workflow

Workflow de l'aptitude de lancement de lanceur de flux parallèle

Créer un événement d'évaluation

Évaluer le résultat de la tâche de réponse



Modèles de workflows Réponse aux incidents de sécurité

Des modèles de workflow sont fournis pour Orchestration de la réponse aux incidents de sécurité vous permettre d'effectuer des procédures d'analyse de base liées à l'opération de sécurité. Les modèles peuvent être utilisés tels quels ou vous pouvez les personnaliser pour créer des workflows qui répondent mieux à vos besoins spécifiques. Les modèles de workflow sont désactivés par défaut.

Seuls les utilisateurs disposant du rôle sn_sec_cmn.admin peuvent accéder à l'éditeur de workflow .

Modèle de workflow d'exposition des données confidentielles des incidents de sécurité

Le modèle Incident de sécurité - Exposition de données confidentielles - vous permet d'effectuer une série de tâches conçues pour gérer l'exposition de données sensibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

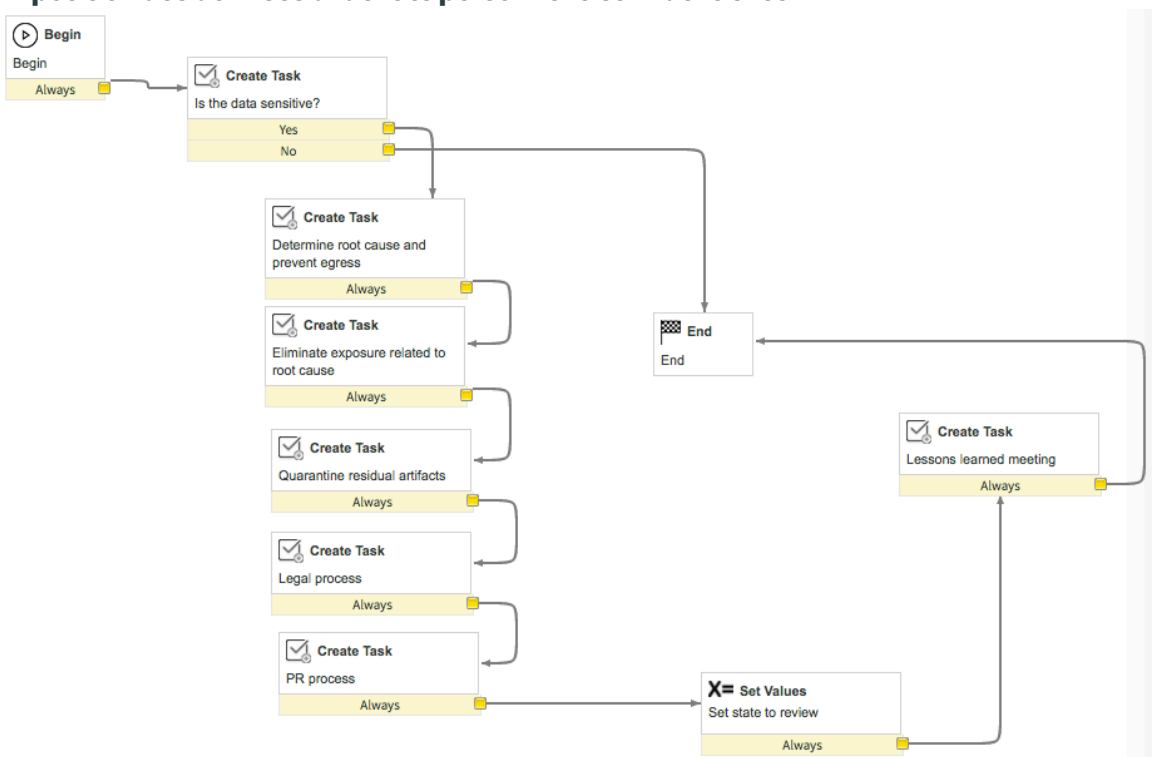
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie ou changée en **Exposition des données d'identité personnelle confidentielles**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Exposition des données d'identité personnelle confidentielles



Procédure

1. Ouvrez l'incident de sécurité pour lequel vous souhaitez gérer l'exposition aux données sensibles ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Exposition des données d'identité personnelle confidentielles**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du flux.

Tâches de réponse dans le modèle d'exposition de données confidentielles

Tâche de réponse	Description	Résultats
Les données sont-elles sensibles ?	Déterminez si les données associées à cet incident de sécurité sont sensibles ou confidentielles. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous avez sélectionné **Oui**, la tâche de réponse suivante est exécutée. Si vous avez sélectionné **Non**, le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Description	Résultats
Déterminer la cause première et empêcher la sortie	Déterminez la cause première de l'attaque et ajoutez un filtrage de sortie pour arrêter l'exfiltration, en mettant à jour le champ **État** dans la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Éliminer l'exposition liée à la cause première	En fonction de la cause première, effectuez les étapes pour éliminer l'exposition, en mettant à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Mettre en quarantaine les artefacts résiduels	Effectuez les étapes de mise en quarantaine de tous les artefacts résiduels, en mettant à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Processus juridique	Effectuez les étapes pour satisfaire aux exigences légales de cette analyse, en mettant à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Processus de PR	Effectuez les étapes pour satisfaire aux exigences de PR de cette analyse, en mettant à jour le champ **État** dans la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**.
Réunion sur les enseignements tirés	Organiser une réunion sur les enseignements tirés pour trier le travail effectué sur ces données sensibles, en mettant à jour le champ **État** de la tâche le cas échéant.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, l'incident de sécurité reste à l'état **Examen** jusqu'à ce que vous le fermiez.

Modèle de workflow Déni de service d'incident de sécurité

Le modèle Incident de sécurité - Déni de service - vous permet d'effectuer une série de tâches conçues pour gérer les attaques par déni de service (DOS).

Avant de commencer

Rôle requis : sn_si.write

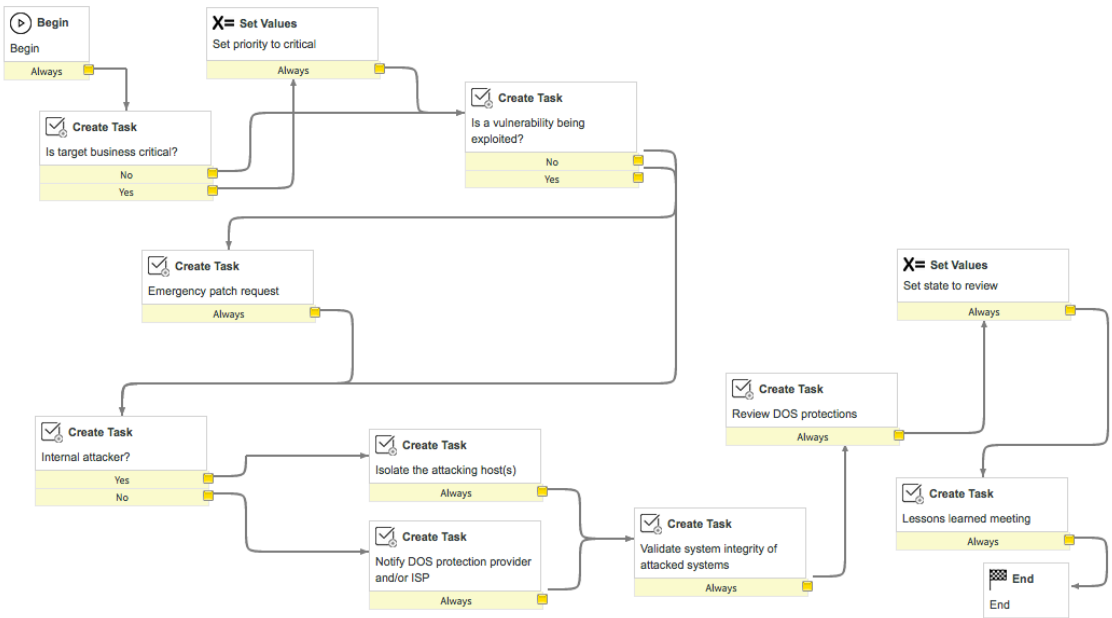
Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Déni de service**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déni de service (DOS)



Procédure

1. Ouvrez l'incident de sécurité pour cette occurrence de déni de service ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Déni de service**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du flux.

Tâches de réponse dans le modèle de déni de service

Tâche de réponse	Action	Résultats
Le business cible est-il critique ?	Déterminez si la cible de cette attaque DOS est critique pour l'entreprise. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, l'option **Définir la priorité sur** la tâche critique est exécutée. Si vous sélectionnez **Non**, la tâche **Une vulnérabilité est-elle exploitée ?** est exécutée.
Définir la priorité sur critique	Aucune action n'est requise.	La **priorité** de l'incident de sécurité passe automatiquement à **Critique** et la tâche **Une vulnérabilité est-elle exploitée ?** est exécutée.
Une vulnérabilité est-elle exploitée ?	Déterminez si cette attaque DOS exploite une vulnérabilité logicielle. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **de demande de correctif d'urgence** est exécutée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
		Si vous sélectionnez **Non**, la tâche **Attaquant interne ?** est exécutée.
Demande de correctif d'urgence	Émettez une demande d'application de correctif d'urgence pour le ou les systèmes attaqués. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez changé l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Attaquant interne ?	Déterminez si la source de cette attaque DOS est interne à votre organisation. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Isoler le ou les hôtes attaquants** est exécutée. Si vous sélectionnez **Non**, la tâche **Notification du fournisseur de protection DOS et/ou du FAI** est exécutée.
Isoler le ou les hôtes attaquants	Effectuez les étapes nécessaires pour isoler le ou les hôtes internes responsables de l'attaque. Mettez à jour le champ **État** dans la tâche comme il convient.	Une fois cette étape terminée, la tâche **Valider l'intégrité du système des systèmes attaqués** est exécutée.
Notifier le fournisseur de protection DOS et/ou le FAI	Effectuez les étapes nécessaires pour contacter votre fournisseur de protection contre le déni de service et/ou votre fournisseur d'accès Internet pour les informer de l'attaque. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez changé l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Valider l'intégrité du système des systèmes attaqués	Effectuez les étapes nécessaires pour évaluer et valider l'intégrité des ordinateurs attaqués. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez changé l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Réviser les protections DOS	Procédez à un examen de vos protections et procédures DOS existantes. Apportez les modifications nécessaires. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez changé l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**. La **tâche de réunion Leçons apprises** est exécutée.
Réunion sur les	Organiser une réunion sur les leçons apprises pour trier le travail effectué pour cet incident de déni de service.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
enseignements tirés	Mettez à jour le champ **État** dans la tâche comme il convient.	

Modèle de workflow d'incident de sécurité pour équipement perdu

Le modèle Incident de sécurité - Équipement perdu - vous permet d'effectuer une série de tâches conçues pour gérer l'équipement perdu.

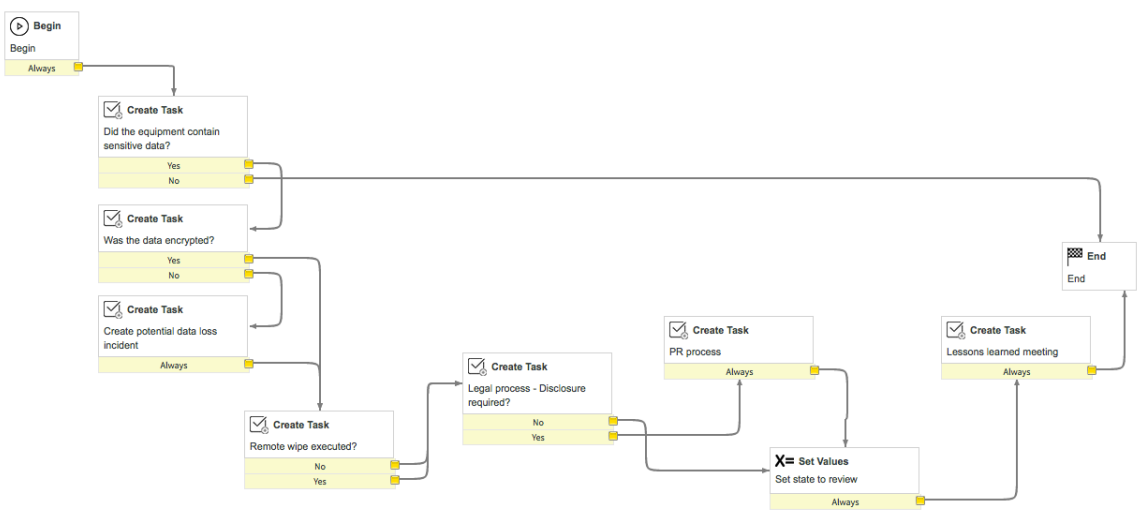
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Perte d'équipement**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Perte d'équipement



Procédure

1. Ouvrez l'incident de sécurité pour la perte d'équipement ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Perte d'équipement**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du flux.

Tâches de réponse dans le modèle d'équipement perdu

Tâche de réponse	Action	Résultats
L'équipement contenait-il des données sensibles ?	Déterminez si l'équipement associé à cet incident de sécurité contenait des informations sensibles ou confidentielles.	Si vous sélectionnez **Oui** , **la tâche Les données ont-elles été chiffrées ?** est exécutée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
	Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat** selon le cas.	Si vous sélectionnez **Non**, le flux s'arrête.
Les données ont-elles été chiffrées ?	Déterminez si les données sensibles de l'appareil perdu ont été chiffrées. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat** selon le cas.	Si vous sélectionnez **Oui**, la tâche **d'effacement à distance créée ?** est exécutée. Si vous sélectionnez **Non**, la tâche **Créer une réponse aux incidents avec perte potentielle de données**est exécutée.
Créer un incident de perte de données potentiel	Effectuez les étapes nécessaires pour créer un incident de perte de données potentiel. Une fois que vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet,** selon le cas.	La tâche **d'effacement à distance créée ?** est exécutée.
Effacement à distance créé ?	Effectuez les étapes nécessaires pour effectuer un effacement à distance de l'équipement perdu. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat** selon le cas.	La tâche **Processus juridique - Divulgation requise** est exécutée.
Processus juridique - Divulgation requise ?	Effectuez les étapes pour satisfaire aux exigences légales de cette analyse. Sélectionnez **Oui** si une divulgation légale est requise, **Non**si ce n'est pas le cas.	La **tâche de réunion Leçons apprises** est exécutée.
Processus de PR	Effectuez les étapes nécessaires pour satisfaire aux exigences de PR de cette analyse. Une fois que vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet,** selon le cas.	La tâche **Définir l'état sur Examiner** est exécutée.
Définir l'état sur Revue	Aucune action n'est nécessaire.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**.
Réunion sur les enseignements tirés	Organiser une réunion sur les leçons apprises pour trier le travail effectué pour cet incident d'équipement perdu.	Le flux s'arrête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
	Une fois que vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet,** selon le cas.	

Modèle de workflow d'incident de sécurité pour les logiciels malveillants

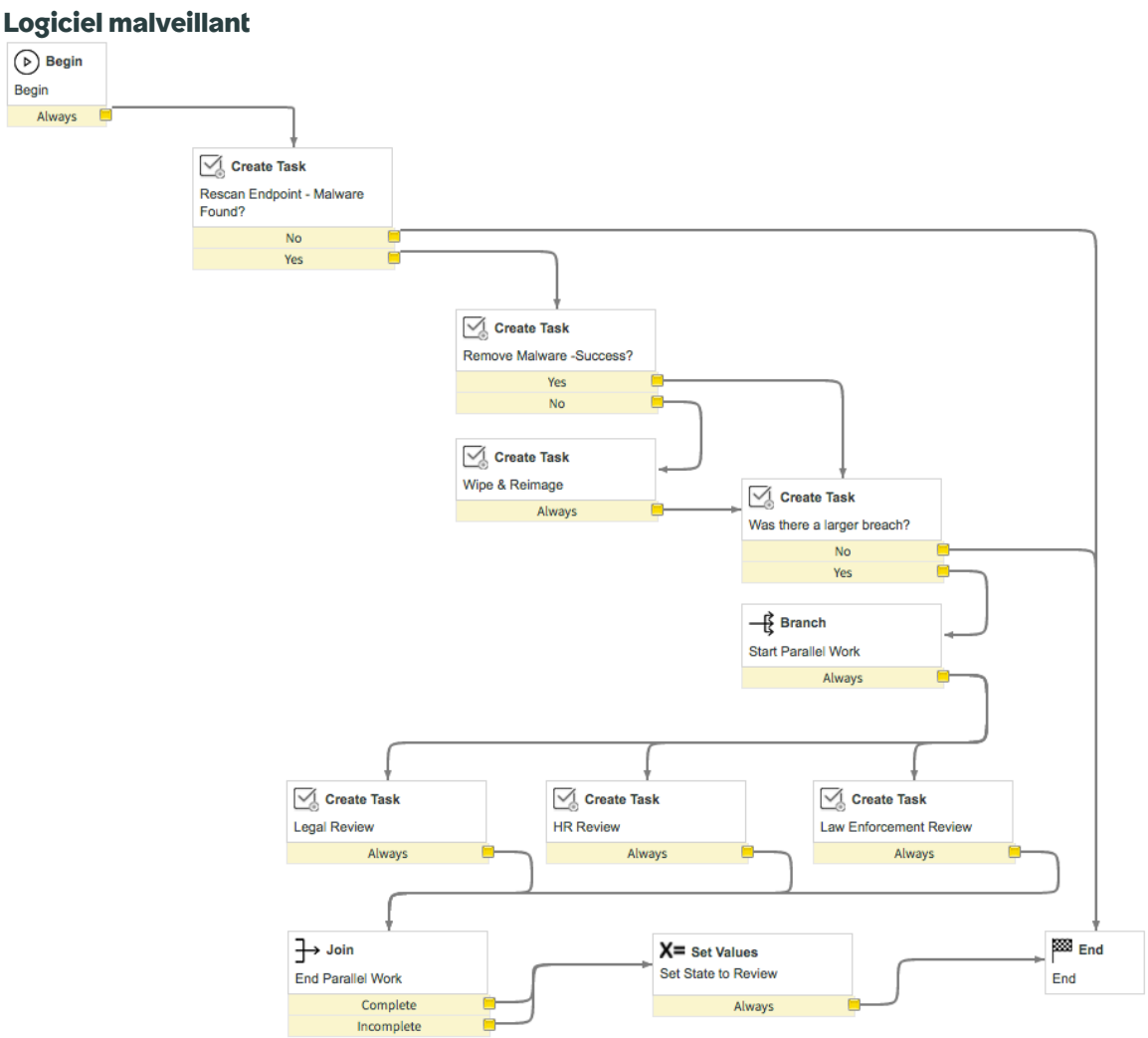
Le modèle Incident de sécurité - Logiciel malveillant - vous permet d'effectuer une série de tâches conçues pour gérer les logiciels malveillants sur votre réseau.

Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Logiciel malveillant**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez l'incident de sécurité pour cette attaque potentielle ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Activité du code malveillant**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du workflow.

Tâches de réponse dans le modèle de logiciel malveillant

Tâche de réponse	Action	Résultats
Point de terminaison de l'analyse : programme malveillant trouvé ?	Après avoir exécuté une analyse, déterminez si un programme malveillant a été trouvé. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Supprimer les programmes malveillants : réussite ?** est exécutée. Si vous sélectionnez **Non**, le flux s'arrête.
Supprimer les programmes malveillants : réussite ?	Déterminez si le programme malveillant a été supprimé. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Y a-t-il eu une violation plus importante ?** est exécutée. Si vous sélectionnez **Non**, la tâche **Effacer et réimager** est exécutée.
Effacer et réimager	Si vous n'avez pas réussi à supprimer le programme malveillant trouvé, cette tâche vous demande d'effectuer un effacement et une nouvelle image sur les ordinateurs infectés par le programme malveillant.	Une fois la tâche terminée, la tâche **Définir l'état sur Révision** est exécutée.
Y a-t-il eu une violation plus importante ?	Déterminez si la violation causée par le logiciel malveillant est plus importante qu'on ne le croyait au départ. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les tâches suivantes sont exécutées en parallèle : ○ Révision juridique ○ Revue RH ○ Examen de l'application de la loi Si vous sélectionnez **Non**, le flux s'arrête.
Révision juridique Revue RH	Effectuez les étapes nécessaires pour chacun de ces départements afin d'examiner le processus que vous avez suivi pour éradiquer le logiciel malveillant.	Lorsque les tâches sont terminées, la tâche **Définir l'état sur Révision** est exécutée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
Examen de l'application de la loi		
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen** et le flux s'arrête.

Modèle de workflow d'hameçonnage d'incidents de sécurité

Le modèle Incident de sécurité - Hameçonnage - vous permet d'effectuer une série de tâches conçues pour gérer les e-mails de spear phishing sur votre réseau.

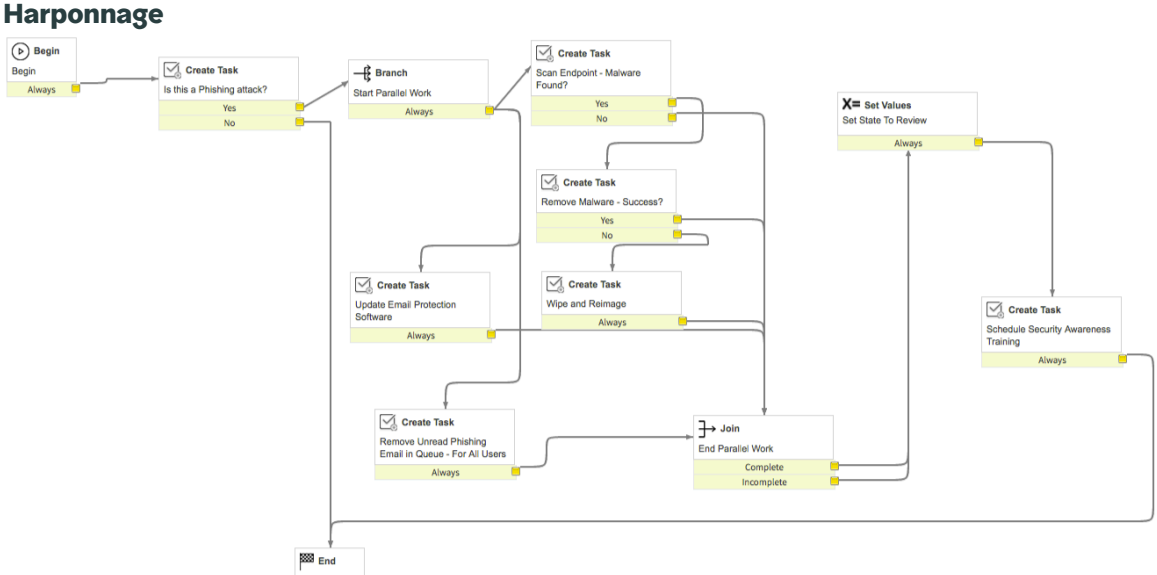
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Spear Phishing**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Harponnage



Procédure

1. Ouvrez l'incident de sécurité pour cette attaque potentielle de spear phishing ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Spear Phishing**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du workflow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâches de réponse dans le modèle de harponnage

Tâche de réponse	Action	Résultats
S'agit-il d'une attaque de phishing ?	Déterminez s'il s'agit d'une attaque de phishing. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les tâches suivantes sont exécutées en parallèle : ○ Point de terminaison de l'analyse : programme malveillant trouvé ? ○ Mettre à jour le logiciel de protection de la messagerie ○ Supprimer l'e-mail d'hameçonnage non lu de la file d'attente - Pour tous les utilisateurs Si vous sélectionnez **Non**, le flux s'arrête.
Point de terminaison de l'analyse : programme malveillant trouvé ?	Après avoir exécuté une analyse, déterminez si un programme malveillant a été trouvé. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Supprimer les programmes malveillants : réussite ?** est exécutée. Si vous sélectionnez **Non**, la tâche **Définir l'état sur Révision** est exécutée.
Supprimer les programmes malveillants : réussite ?	Déterminez si le programme malveillant a été supprimé. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Définir l'état sur Révision** est exécutée. Si vous sélectionnez **Non**, la tâche **Effacer et réimager** est exécutée.
Effacer et réimager	Si vous n'avez pas réussi à supprimer le programme malveillant trouvé, cette tâche vous demande d'effectuer un effacement et une nouvelle image sur les ordinateurs infectés par le programme malveillant.	Une fois la tâche terminée, la tâche **Définir l'état sur Révision** est exécutée.
Mettre à jour le logiciel de protection de la messagerie	S'il a été déterminé qu'il s'agit d'une attaque de phishing, vous êtes invité à mettre à jour votre logiciel de protection de la messagerie en conséquence.	Lorsque la tâche est terminée, la tâche **Définir l'état sur Révision** est exécutée.
Supprimer l'e-mail d'hameçonnage non lu de la file	Effectuez les étapes nécessaires pour supprimer l'e-mail d'hameçonnage toujours dans la file d'attente pour tous vos utilisateurs.	Lorsque la tâche est terminée, la tâche **Définir**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
d'attente - Pour tous les utilisateurs		**l'état sur Révision** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**. La tâche **Planifier une formation de sensibilisation** à la sécurité est exécutée.
Planifier une formation de sensibilisation à la sécurité	Planifiez une formation pour sensibiliser vos employés à la sécurité. Mettez à jour le champ **État** dans la tâche comme il convient.	Lorsque la tâche est terminée, le flux se termine.

Modèle de workflow de violation de la politique d'incident de sécurité

Le modèle Incident de sécurité - Violation de la politique - vous permet d'effectuer une série de tâches conçues pour gérer les violations de la politique de sécurité.

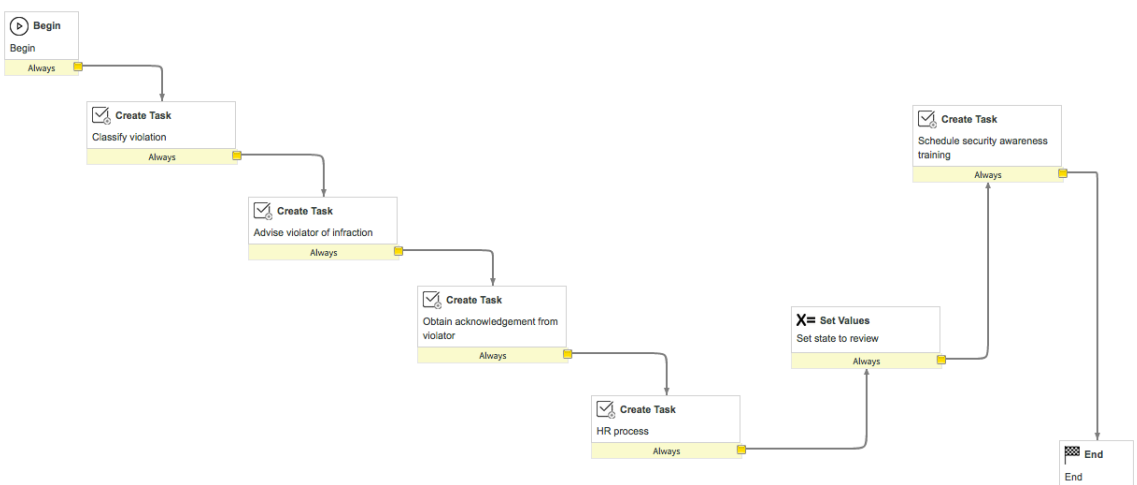
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Violation de la politique**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Violation de la politique



Procédure

1. Ouvrez l'incident de sécurité correspondant à la violation de la politique ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Violation de la politique**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du workflow.

Tâches de réponse dans le modèle de violation de la politique

Tâche de réponse	Action	Résultats
Classer la violation	Classez la façon dont cette infraction viole les politiques de sécurité de votre organisation. Mettez à jour le champ **État** dans la tâche une fois que vous l'avez terminée.	La tâche **Informer le contrevenant de l'infraction** est exécutée.
Aviser le contrevenant d'une infraction	Communiquez la nature de l'infraction au contrevenant. Mettez à jour le champ **État** dans la tâche après l'avoir communiqué.	La tâche **Obtenir la confirmation du contrevenant** est exécutée.
Obtenir la confirmation du contrevenant	Obtenir une confirmation de l'infraction de la part du contrevenant. Mettez à jour le champ **État** dans la tâche comme il convient.	La tâche de réponse du **processus RH** est exécutée.
Processus RH	Communiquez toutes les informations nécessaires concernant cette violation aux RH. Mettez à jour le champ **État** dans la tâche comme il convient.	La tâche **Définir l'état sur Examiner** la réponse est exécutée.
Définir l'état sur Revue	Aucune action n'est nécessaire.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**.
Planifier une formation de sensibilisation à la sécurité	Organisez une formation de sensibilisation à la sécurité pour éduquer le personnel sur la façon de prévenir des violations de sécurité similaires à l'avenir. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, le flux s'arrête.

Modèle de workflow de reconnaissance des incidents de sécurité

La reconnaissance est généralement une étape préliminaire vers une nouvelle attaque visant à exploiter un appareil ou un système. Le modèle Incident de sécurité - Reconnaissance - vous permet d'effectuer une série de tâches conçues pour gérer la reconnaissance sur votre réseau.

Avant de commencer

Rôle requis : sn_si.write

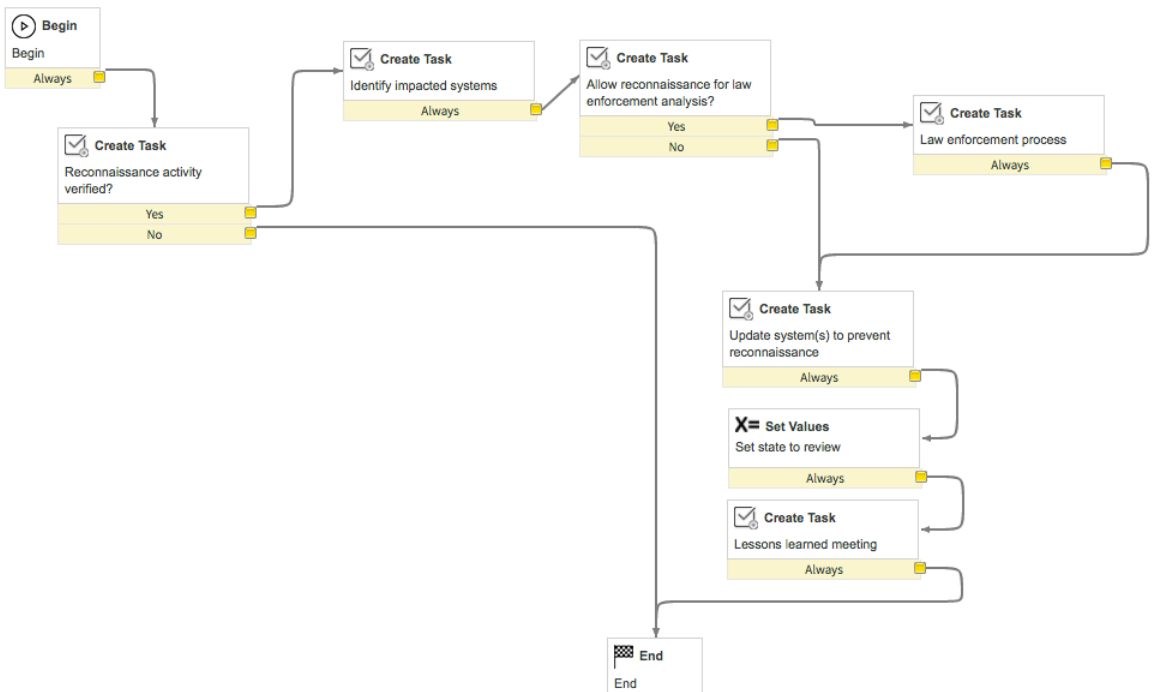
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Activité de reconnaissance**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Activité de reconnaissance



Procédure

1. Ouvrez l'incident de sécurité pour cette attaque potentielle ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Activité de reconnaissance**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du workflow.

Tâches de réponse dans le modèle de reconnaissance

Tâche de réponse	Action	Résultats
Activité de reconnaissance vérifiée ?	Déterminez si les reconnaissances observées ont été vérifiées. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Identifier les systèmes impactés** est exécutée. Si vous sélectionnez **Non**, le flux s'arrête.
Identifier les systèmes impactés	Déterminez les systèmes impactés par la reconnaissance.	Lorsque cette tâche est terminée, la tâche **Autoriser la reconnaissance pour l'analyse de l'application de la loi ?** est exécutée.
Autoriser la reconnaissance pour	Déterminez si vous souhaitez que la reconnaissance soit analysée par les forces de l'ordre.	Si vous sélectionnez **Oui**, la tâche Processus **d'application** de la loi est exécutée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
l'analyse des forces de l'ordre ?	Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Non**, la tâche **Mettre à jour le(s) système(s) pour empêcher la reconnaissance** est exécutée.
Processus d'application de la loi	Exécutez le processus d'application de la loi tel que défini par votre entreprise.	Lorsque cette tâche est terminée, la tâche **Mettre à jour le(s) système(s) pour empêcher la reconnaissance** est exécutée.
Mettre à jour le(s) système(s) pour empêcher la reconnaissance	Effectuez les étapes nécessaires pour mettre à jour les systèmes affectés par la reconnaissance.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur Révision** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen** et la **tâche de réunion Enseignements tirés** est exécutée.
Réunion sur les enseignements tirés	Tenir une réunion sur les leçons apprises afin de trier le travail effectué dans le cadre de cet incident de reconnaissance. Mettez à jour le champ **État** dans la tâche comme il convient.	Lorsque cette tâche est terminée, le flux s'arrête.

Modèle de workflow Serveur ou service non autorisé d'incident de sécurité

Le modèle Incident de sécurité - Serveur ou service non autorisé - vous permet d'effectuer une série de tâches conçues pour gérer l'activité des serveurs ou services non autorisés qui affectent votre réseau.

Avant de commencer

Rôle requis : sn_si.write

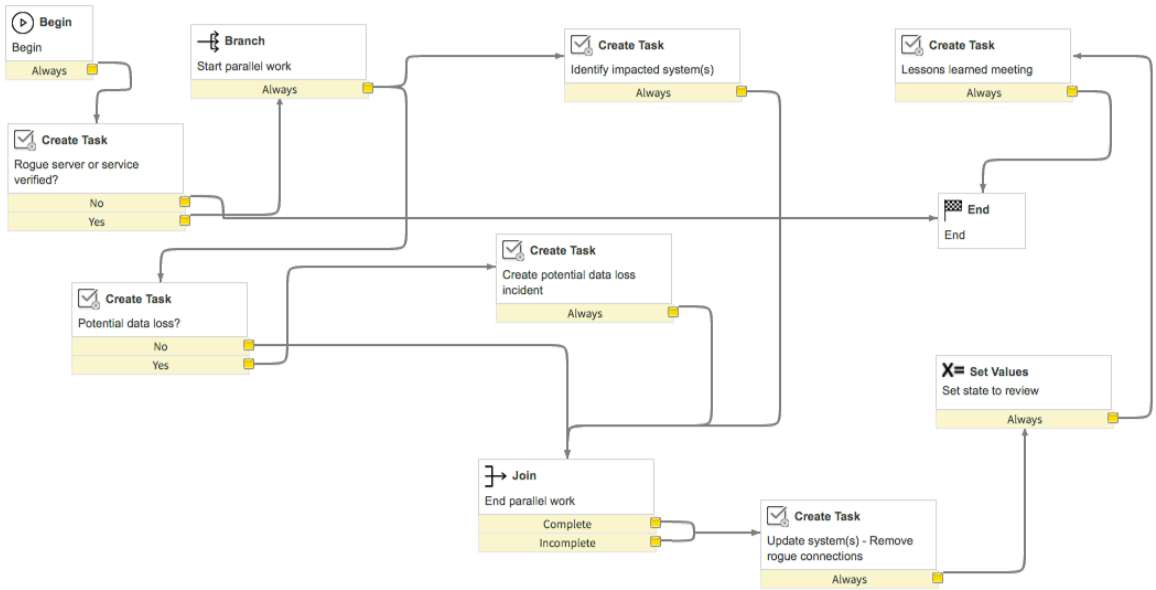
Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Serveur ou service non autorisé**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Serveur ou service non autorisé



Procédure

1. Ouvrez l’incident de sécurité pour cette attaque potentielle ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Activité de serveur ou de service non autorisée**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d’une série de tâches de réponse apparaît. Chaque fois que l’enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l’arrêt du workflow.

Tâches de réponse dans un serveur ou un modèle de service non autorisé

Tâche de réponse	Action	Résultats
Serveur ou service non autorisé vérifié ?	Déterminez si une connexion avec un serveur ou un service non autorisé a été vérifiée sur votre réseau. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les deux tâches suivantes sont exécutées en parallèle : ○ **Identifier le(s) système(s) impacté(s)** ○ **Perte de données potentielle ?** Si vous sélectionnez **Non**, le flux s’arrête.
Identifier le(s) système(s) impacté(s)	Déterminez les systèmes affectés par le contact avec le serveur ou le service non autorisé.	Lorsque cette tâche est terminée, la tâche **Mettre à jour le(s) système(s) - Supprimer les connexions non fiables** est exécutée.
Perte de données potentielle ?	Déterminez si la connexion avec le serveur ou le service non autorisé a causé une perte de données potentielle. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Créer un incident de perte potentielle de données** est exécutée. Si vous sélectionnez **Non**, la tâche **Mettre à jour le(s) système(s) -**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
		Supprimer les connexions non fiables est exécutée.
Créer un incident de perte de données potentiel	Effectuez les étapes nécessaires pour créer un incident de sécurité en vue de la perte potentielle de données.	Lorsque cette tâche est terminée, la tâche **Mettre à jour le(s) système(s) - Supprimer les connexions non fiables** est exécutée.
Mettre à jour le(s) système(s) - Supprimer les connexions non fiables	Effectuez les étapes nécessaires pour supprimer les connexions non autorisées.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur Révision** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen** et la **tâche de réunion Enseignements tirés** est exécutée.
Réunion sur les enseignements tirés	Organiser une réunion sur les leçons apprises pour trier le travail effectué pour cet incident de serveur ou de service non autorisé. Mettez à jour le champ **État** dans la tâche comme il convient.	Lorsque cette tâche est terminée, le flux s'arrête.

Modèle de workflow d'incidents de sécurité indésirables

Le modèle Incident de sécurité - Courrier indésirable - vous permet d'effectuer une série de tâches conçues pour gérer le courrier indésirable sur votre réseau.

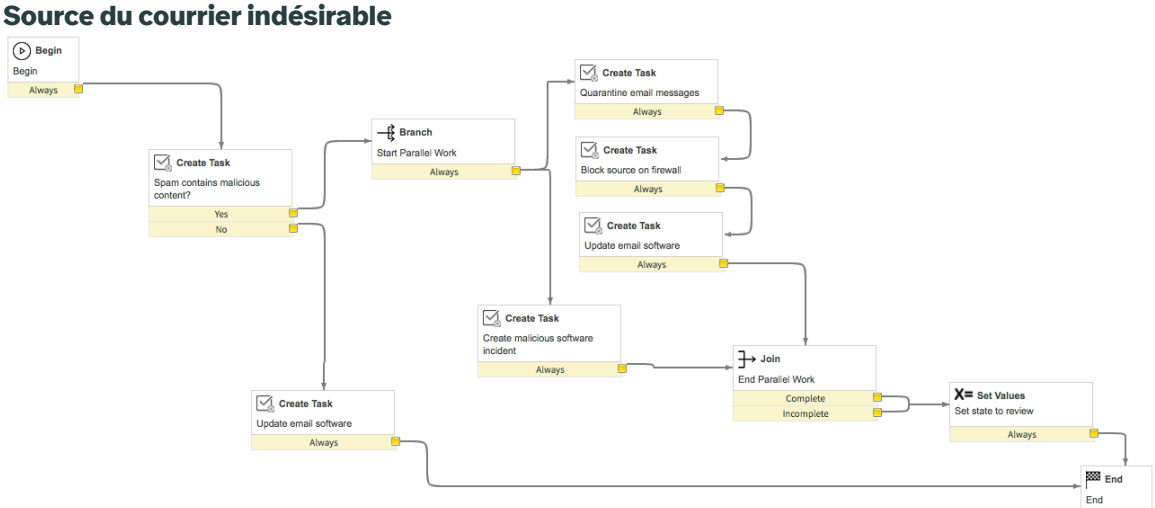
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie ou qu'elle devient **Source du courrier indésirable**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Source du courrier indésirable



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez l'incident de sécurité pour lequel vous souhaitez gérer le courrier indésirable ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Source du spam**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du workflow.

Tâches de réponse dans le modèle de courrier indésirable

Tâche de réponse	Action	Résultats
Le spam contient-il du contenu malveillant ?	Déterminez si le courrier indésirable contient des logiciels malveillants. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous avez sélectionné **Oui**, les tâches de réponse suivantes sont exécutées : ○ **Mettre en quarantaine le message électronique** ○ **Créer un incident lié au logiciel malveillant** Si vous avez sélectionné **Non**, Mettre **à jour le logiciel de messagerie** est exécuté.
Créer un incident lié au logiciel malveillant	Effectuez les étapes pour créer un incident de sécurité, en mettant à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, cette tâche de réponse attend jusqu'à ce que les trois tâches de réponse suivantes soient terminées. L'état de l'incident de sécurité passe alors à **l'état Réviser**.
Mettre en quarantaine le message électronique	Effectuez les étapes de mise en quarantaine du courrier indésirable, en mettant à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Source du bloc sur le pare-feu	Effectuez les étapes pour bloquer l'adresse e-mail sur le pare-feu, en mettant à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Mettre à jour le logiciel de messagerie	Ajoutez l'adresse e-mail à votre liste de blocs, en mettant à jour le champ **État** de la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée. **Remarque :** Cette tâche de réponse est également exécutée si vous avez répondu **Non** à la tâche de **réponse Le courrier indésirable contient-il du contenu malveillant ?**
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modèle de workflow d'accès non autorisé d'incident de sécurité

Le modèle Incident de sécurité - Accès non autorisé - vous permet d'effectuer une série de tâches conçues pour gérer les accès non autorisés à votre réseau.

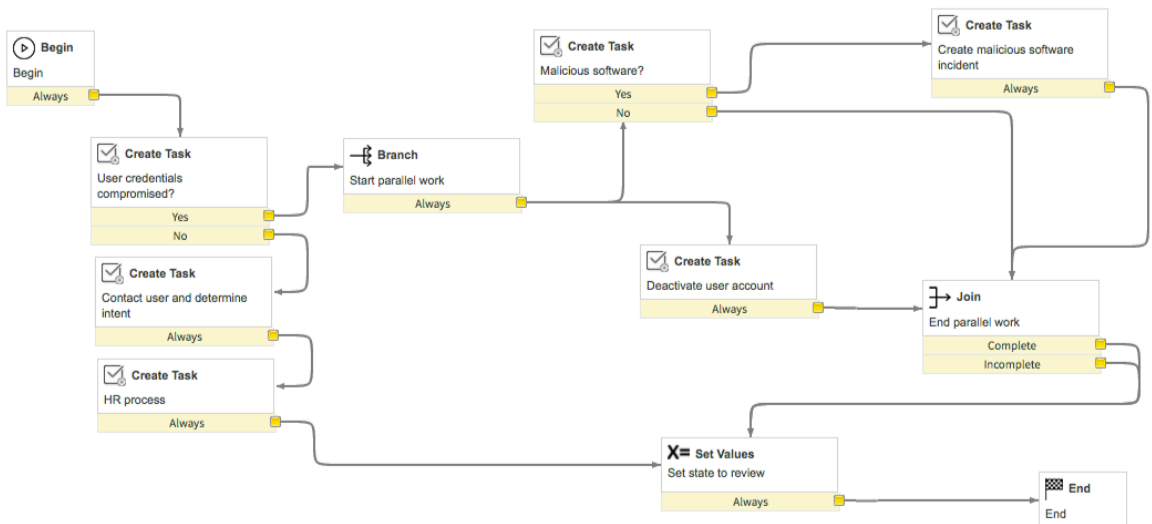
Avant de commencer

Rôle requis : sn_si.write

Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Accès non autorisé**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Accès non autorisé



Procédure

1. Ouvrez l'incident de sécurité pour cette attaque potentielle ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Accès non autorisé**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du workflow.

Tâches de réponse dans le modèle d'accès non autorisé

Tâche de réponse	Action	Résultats
Les informations d'identification de l'utilisateur compromises ?	Déterminez si des informations d'identification de l'utilisateur ont été compromises. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les deux tâches suivantes sont exécutées en parallèle : ○ **Logiciel malveillant ?** ○ **Désactiver un compte d'utilisateur** Si vous sélectionnez **Non**, la tâche **Contacter l'utilisateur**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
		et déterminer l'intention est exécutée.
Logiciel malveillant ?	Déterminez si l'accès non autorisé a entraîné l'introduction de logiciels malveillants. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, la tâche **Créer un incident de logiciel malveillant** est exécutée. Si vous sélectionnez **Non**, la tâche **Définir l'état sur Révision** est exécutée.
Créer un incident lié au logiciel malveillant	Effectuez les étapes nécessaires pour créer un incident de sécurité pour l'accès non autorisé.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur Révision** est exécutée.
Désactiver un compte d'utilisateur	Effectuez les étapes nécessaires pour désactiver le compte d'utilisateur compromis.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur Révision** est exécutée.
Contacter l'utilisateur et déterminer l'intention	Effectuez les étapes nécessaires pour contacter l'utilisateur responsable de l'accès non autorisé et déterminer le motif de la tentative d'accès.	Lorsque cette tâche est terminée, la tâche de **processus RH** est exécutée.
Processus RH	Effectuez les étapes nécessaires pour contacter les ressources humaines afin de mettre en œuvre des mesures disciplinaires si nécessaire.	Lorsque cette tâche est terminée, la tâche **Définir l'état sur Révision** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen** et le flux s'arrête.

Modèle de workflow de défiguration d'incident de sécurité Web/BBS

Le modèle Incident de sécurité - Altération de site web/BBS - vous permet d'effectuer une série de tâches conçues pour gérer le vandalisme dirigé contre l'un des sites Web ou BBS de votre organisation.

Avant de commencer

Rôle requis : sn_si.write

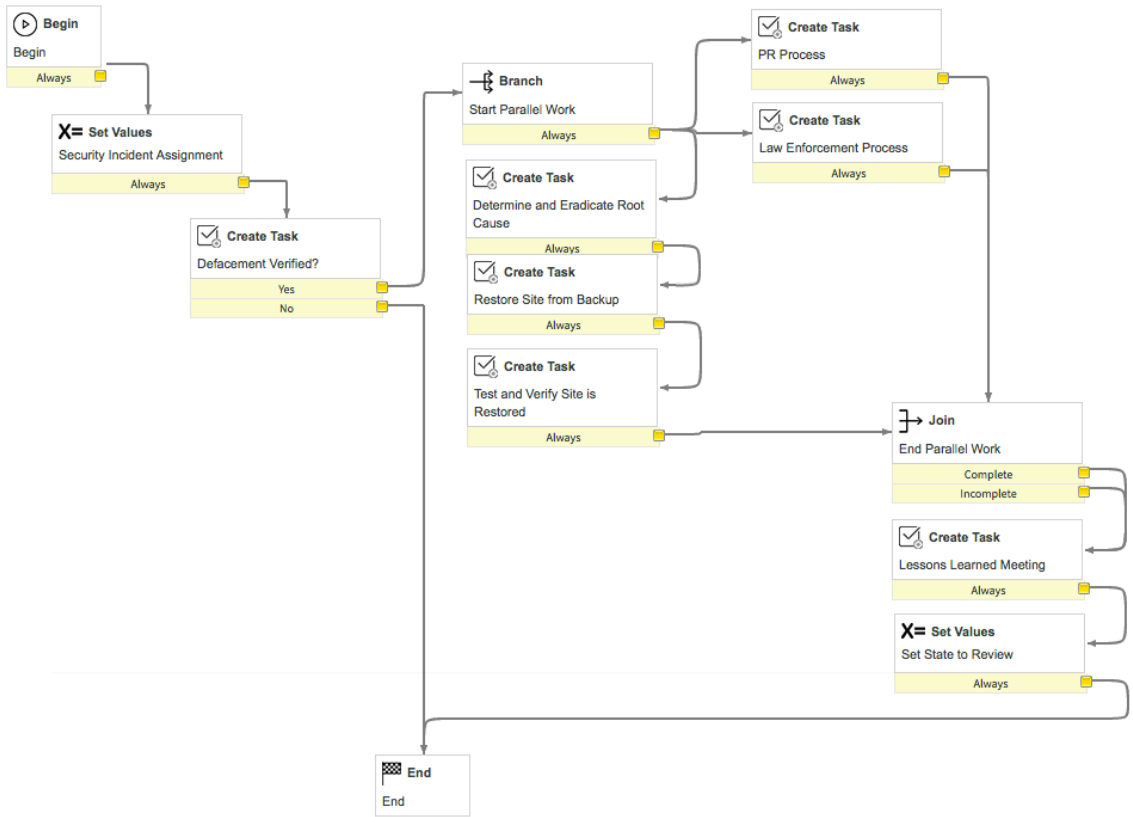
Pourquoi et quand exécuter cette tâche

Le workflow est déclenché lorsque la **catégorie** d'un incident de sécurité est définie sur **Altération de site web/BBS**. Cette action entraîne la création d'une tâche de réponse pour la première activité du workflow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Altération de site web/BBS



Procédure

1. Ouvrez l'incident de sécurité pour cette occurrence d'altération Web ou BBS, ou créez un nouvel incident de sécurité.
2. Dans **Catégorie**, sélectionnez **Altération de site web/BBS**.
3. Enregistrez l'enregistrement.
4. Faites défiler vers le bas et ouvrez la liste connexe **Tâches de réponse** .
   La première d'une série de tâches de réponse apparaît. Chaque fois que l'enregistrement est enregistré, votre réponse à la tâche précédente entraîne la création de la tâche de réponse suivante ou l'arrêt du workflow.

Modèle de défiguration des tâches de réponse dans le Web/BBS

Tâche de réponse	Action	Résultats
Affectation des incidents de sécurité	Créez un incident de sécurité pour chaque incident signalé d'altération d'un site Web ou d'un BBS.	La tâche de réponse suivante est exécutée.
Altération vérifiée ?	Déterminez si le site Web ou le BBS a effectivement été défiguré. Dans la tâche, sélectionnez **Oui** ou **Non** dans **Résultat**.	Si vous sélectionnez **Oui**, les tâches de réponse suivantes sont exécutées : ○ **Processus de PR** ○ **Processus d'application de la loi** ○ **Déterminer et éradiquer la cause première**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de réponse	Action	Résultats
		Si vous sélectionnez **Non**, le flux s'arrête.
Processus de PR	Effectuez les étapes nécessaires pour informer le public que le site Web ou le BBS a été dégradé. Lorsque vous avez terminé le processus de PR, définissez l'état de la tâche sur **Terminé** ou **Incomplet,** selon le cas.	La **tâche de réunion Leçons apprises** est exécutée.
Processus d'application de la loi	Effectuez les étapes nécessaires pour impliquer les forces de l'ordre appropriées concernant l'attaque. Lorsque vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet,** selon le cas.	La **tâche de réunion Leçons apprises** est exécutée.
Déterminer et éradiquer la cause première	Effectuez les étapes nécessaires pour découvrir et éliminer la cause première de l'altération. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez changé l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Restaurer le site à partir d'une copie de sauvegarde	Effectuez les étapes nécessaires pour sauvegarder et restaurer le site Web ou le BBS. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous avez changé l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche de réponse suivante est exécutée.
Le site de test et de vérification est restauré	Vérifiez que le site est restauré. Lorsque vous avez terminé, définissez l'état de la tâche sur **Terminé** ou **Incomplet,** selon le cas.	La **tâche de réunion Leçons apprises** est exécutée.
Réunion sur les enseignements tirés	Organiser une réunion sur les leçons apprises pour trier le travail effectué pour cet incident de défiguration du site Web/BBS. Mettez à jour le champ **État** dans la tâche comme il convient.	Si vous modifiez l'état de la tâche sur **Fermé terminé** ou **Annulé**, la tâche **Définir l'état sur Révision** est exécutée.
Définir l'état sur Revue	Aucune action n'est requise.	**L'état** de l'incident de sécurité passe automatiquement à **Examen**. Le flux s'arrête.

Renseignements sur les menaces

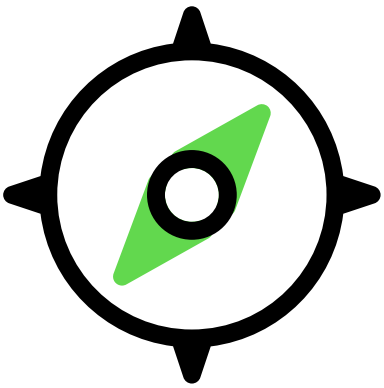
L'application ServiceNow® Renseignements sur les menaces vous permet de trouver des indicateurs de compromission (IoC) et d'enrichir les incidents de sécurité avec des données de renseignements sur les menaces.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

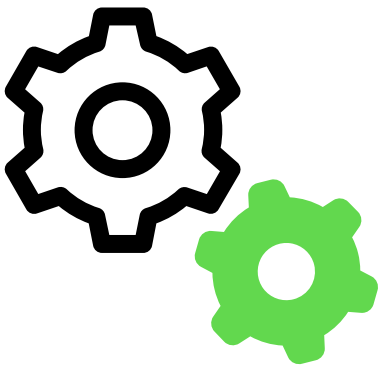
Premiers pas

Explorer



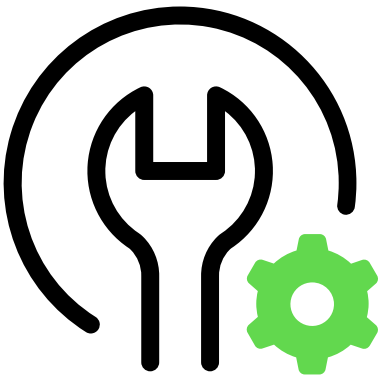
Découvrez les concepts de Threat Intelligence et leurs principales fonctionnalités.

Configurer



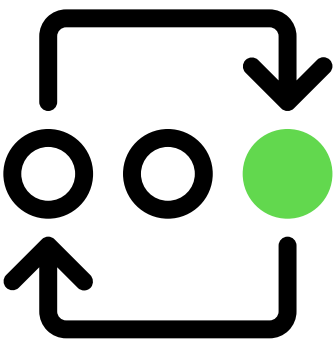
Configurez, découvrez les composants installés et les rôles d'utilisateur requis pour répondre à vos besoins professionnels.

Administrer



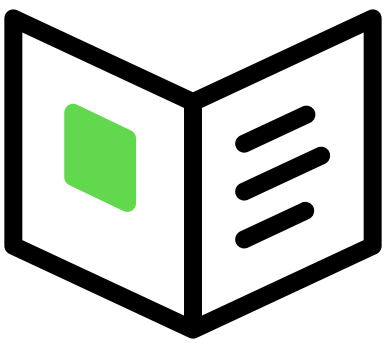
Définissez les propriétés de Renseignements sur les menaces.

Intégrer



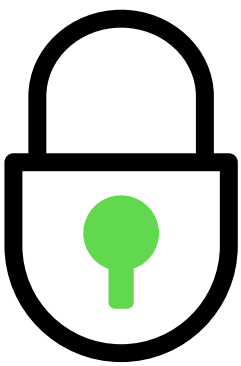
Étendez les options de Threat Intelligence en les intégrant à ServiceNow et à des applications tierces.

Utiliser



Gérez les indicateurs de compromis (IoC) et divers artefacts.

Cadre de travail MITRE ATT&CK



Gérez rapidement le cadre de travail MITRE-ATT&CK, identifiez les menaces et coordonnez les réponses aux cyberattaques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Security Case Management



Gérez la gestion des tickets de sécurité en recueillant des informations sur les activités suspectes.

Ressources d’apprentissage

- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Poser des questions et explorer d’autres ressources pour Renseignements sur les menaces dans le ServiceNow Community
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance
- Bibliothèque de ressources Security Operations
- Communauté Security Operations

Présentation de Renseignements sur les menaces

L’application Renseignements sur les menaces vous permet d’accéder aux données STIX (Structured™ Threat Information Expression) de votre entreprise et de fournir un point de référence pour celles-ci. L’application Gestion des tickets de sécurité est incluseRenseignements sur les menaces, qui fournit un moyen d’analyser les menaces pour votre organisation posées par des campagnes ciblées ou des acteurs étatiques.

STIX est un langage permettant de décrire les informations sur les cybermenaces de manière standardisée et structurée. Grâce aux données STIX et aux profils TAXII™ (Trusted Automated Exchange of Indicator Information), les professionnels de la menace peuvent utiliser des informations partagées sur les cybermenaces pour isoler les menaces précédemment identifiées par votre entreprise et provenant d’autres sources. TAXII rend possible l’échange automatisé généralisé d’informations sur les cybermenaces.

Renseignements sur les menaces prend en charge les versions 1.1, 2.0 et 2.1 de STIX.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

STIX™ et TAXII™ sont des marques commerciales de The MITRE Corporation.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Séparation de domaine et Renseignements sur les menaces

L'application Séparation de domaine est prise en charge dans le module disponible dans le Renseignements sur les menaces cadre de Réponse aux incidents de sécurité. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : basique

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Vue d'ensemble

Dans le module Renseignements sur les menaces (dans le cadre de l'application Réponse aux incidents de sécurité), Séparation de domaine permet aux fournisseurs de services de créer et de gérer le référentiel de renseignements sur les menaces comme suit :

- Profils de sources de menace et TAXII (Trusted Automated Exchange of Indicator Information)
- Observables
- Indicateurs de compromis
- Modes/méthodes d'attaque des menaces et gestion des cas sur l'ensemble de la base de clients qu'ils servent avec des coûts opérationnels réduits et une meilleure qualité de service

Le fait de disposer d'espaces de travail client distincts pour les workflows, les tableaux de bord, les rapports, etc., garantit que les données client sont séparées et ne sont jamais exposées à d'autres clients.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prise en charge de Domain Separation dans par Renseignements sur les menaces version

Séparation de domaine pour le module Threat Intelligence (dans le cadre de l'application Réponse aux incidents de sécurité) couvre les fonctionnalités de produit suivantes :

- Les observables d'incident de sécurité sont dirigés vers le domaine approprié de l'utilisateur dont l'ID/les informations d'identification ou le champ d'application génère l'incident. Les observables extraits de l'incident sont stockés dans le domaine de l'incident de sécurité.
- Configuration de profils de service TAXII pour télécharger une ou plusieurs collections TAXII qui offrent des flux d'informations sur les cybermenaces. La configuration est stockée dans le domaine sous lequel le profil est configuré.
- Configuration du téléchargement des flux de menaces dans le référentiel IOC dans le domaine sous lequel la configuration est effectuée.
- Création d'un ou de plusieurs modes/méthodes d'attaque dans le domaine de la source de renseignements sur les menaces qui fournit automatiquement les informations ou du domaine dans lequel un nouveau/une nouvelle méthode/mode d'attaque est ajouté manuellement par l'utilisateur
- Création de tickets pour une enquête à long terme sur les incidents, les observables, les CI, les utilisateurs et les indicateurs de compromis (IOC) associés au ticket. Le ticket est stocké dans le domaine créé par l'utilisateur.

Remarque : Dans tous les cas ci-dessus, les principes généraux de la visibilité dans des domaines séparés dans la NOW Platform s'appliquent. Comme toujours, un incident dans le domaine parent peut faire référence à des artefacts dans le domaine enfant, mais pas l'inverse.

Comment fonctionne Séparation de domaine dans Renseignements sur les menaces (dans le cadre de Réponse aux incidents de sécurité)

Threat Intelligence fait partie de Security Incident Response dans les niveaux Professional et Enterprise, mais pas avec le niveau Standard. Par conséquent, un plugin séparé est nécessaire. Le module Threat Intelligence (en tant que partie intégrante de l'application Réponse aux incidents de sécurité) crée et gère les informations de Threat Intelligence associées aux incidents de sécurité dans une organisation. Les cas d'utilisation suivants sont sensibles à la séparation de domaine :

- Création d'observables d'incident de sécurité au moment de la création de l'incident
  - À partir d'analyseurs d'e-mails (basés sur la plateforme, hameçonnage signalé par un utilisateur, personnalisés)
  - À partir d'applications dans des magasins SIEM (Security Information and Event Management) tiers
  - Saisie manuellement par l'analyste SOC
- Collecte d'observables à partir de sources de flux de menaces ; sources de veille sur les menaces à partir de collectes TAXII
- Gérer les observables d'incident de sécurité
  - Associer des observables à des indicateurs connexes
  - Associer des observables à des incidents de sécurité
  - Associer des observables à des observables enfants

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Associer l'observable à la source du flux de menaces
- Ajouter des annotations de sécurité aux observables

- Gérer les indicateurs de compromis
  - Associer des indicateurs à des observables associés
  - Associer des indicateurs au mode/méthode d'attaque
  - Associer des indicateurs à des types d'indicateurs
  - Associer des indicateurs à la source de flux de menaces
  - Ajouter des annotations de sécurité aux indicateurs
- Gérer les tickets
  - Créer un ticket (manuellement ou à partir d'un incident)
  - Modifiez un nouveau ticket pour ajouter des détails (choisir le type et la gravité du ticket, ajouter des incidents, des observables, des éléments de configuration, des utilisateurs, des indicateurs)
  - Supprimer un ticket

Configuration de Domain Separation

La configuration de Séparation de domaine pour Threat Intelligence ne nécessite aucune étape supplémentaire. Toutes les tables Threat Intelligence acquièrent la colonne Domaine une fois que l'instance a été séparée par domaine.

Données séparées par domaine

Les données peuvent être séparées par domaine, ce qui signifie :

- Les observables d'incident de sécurité dans un domaine ne peuvent pas être visualisés à partir du périmètre d'autres domaines.
- Les indicateurs de compromission dans un domaine ne peuvent pas être visualisés à partir du périmètre d'autres domaines.
- Les modes/méthodes d'attaque associés à un domaine ne peuvent pas être visualisés à partir du périmètre d'autres domaines.
- Les profils de service TAXII associés à un domaine ne peuvent pas être affichés à partir du périmètre d'autres domaines.
- Les sources de renseignements sur les menaces associées à un domaine ne peuvent pas être consultées à partir du périmètre d'autres domaines.
- Les tickets associés à un domaine ne peuvent pas être affichés à partir du périmètre d'autres domaines.

Les propriétés Threat Intelligence sont définies au niveau global et ne sont donc pas séparées par domaine. Les paramètres incluent :

- Nom du domaine pour récupérer des informations supplémentaires pour les adresses IP/URL
- Clé API à utiliser pour la récupération
- Recherche des tables IoC locales avant envoi au scanner distant
- Nombre de jours pendant lesquels les observables locaux sont pris en compte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Marquer un mode/une méthode d'attaque comme inactif lorsqu'il n'est pas reçu de sources de renseignements sur les menaces
- Marquage d'un indicateur comme inactif lorsqu'il n'est reçu d'aucune source pendant un nombre de jours spécifié

Configuration

Tous les aspects de la configuration de la fonctionnalité Threat Intelligence sont autonomes dans un environnement séparé par domaine.

Les tâches suivantes peuvent être configurées par domaine :

1. Création de profils de service TAXII
   - Choisir une configuration de service de découverte
   - Choisir une configuration de service de collecte : affecter des rôles aux utilisateurs et aux groupes d'utilisateurs
2. Création de sources Threat Intelligence
   - Configurer le service REST qui fournit les informations de Threat Intelligence
   - Planifier le téléchargement des informations de Renseignements sur les menaces
   - Choisir les informations sur les détails de la menace à affecter à la source
3. Création de modes/méthodes d'attaque (manuel)
   - Source, type de programme malveillant, mécanisme d'attaque, type d'acteur de menace, description, manipulation, effet souhaité, premier observé, dernier observé
   - Indicateurs connexes, mode/méthode d'attaque enfant, incidents de sécurité associés

   Remarque : Les modes/méthodes d'attaque sont également créés automatiquement à partir des sources de flux de menaces.

4. Définition de listes par défaut pour les catégories d'informations sur les menaces suivantes :
   - Mécanismes d'attaque
   - Méthodes de Découverte
   - Flux
   - Types d'indicateurs
   - Effets souhaités
   - Notifications
   - Types d'observables
   - Définitions de limite d'évaluation
   - Types d'acteurs de menace
   - Motivations de l'attaque
   - Types d'infrastructure
   - Options de logiciel malveillant
   - Types de malware
   - Types de rapports

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Rôles d’acteur de menace
- Types d’outil

Comment les domaines des locataires gèrent leurs propres données d’application

- Les propriétaires de domaines locataires peuvent créer leurs propres profils de service TAXII.
- Les propriétaires de domaines du locataire peuvent créer leurs propres sources de renseignements sur les menaces.
- Les propriétaires de domaines peuvent créer leurs propres modes/méthodes d’attaque.
- Les propriétaires de domaines du locataire peuvent créer leurs propres listes par défaut pour les catégories d’informations sur les menaces.

Remarque : La logique et les processus métier permettent de séparer par domaine les calendriers de téléchargement des sources de Renseignements sur les menaces par propriétaire d’instance.

Information associée

Séparation de domaine pour les fournisseurs de services

Configurer Renseignements sur les menaces

Avant de l’exécuter Renseignements sur les menaces dans votre instance, vous devez la télécharger à partir du .ServiceNow Store Vous pouvez également configurer des propriétés et définir une source de menace.

Installer Renseignements sur les menaces

Avant de l’exécuter Renseignements sur les menaces dans votre instance, vous devez la télécharger à partir du .ServiceNow Store

Avant de commencer
Effectuez la liste de vérification de configuration suivante avant l’installation. Ces tâches d’installation sont nécessaires pour une installation et une configuration fluides.

Tâches de configuration	Description
Vérifiez que vous disposez des rôles requis ServiceNow pour votre instance.	Les rôles suivants sont requis pour l’installation, la configuration et la vérification des résultats attendus : • Si ce n’est pas déjà fait, l’administrateur système [admin] installe l’application et affecte le rôle d’administrateur de menaces [sn_ti.admin]. • L’administrateur des menaces [sn_ti.admin] supervise la configuration et vérifie les résultats attendus.

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Suivez les instructions pour Télécharger une application à partir de ServiceNow Store.

Que faire ensuite

Définir les Renseignements sur les menaces propriétés.

Composants installés avec Renseignements sur les menaces

Plusieurs types de composants sont installés avec l'activation du module d'extension Renseignements sur les menaces, y compris les tables et les rôles d'utilisateur.

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Les données de démonstration sont disponibles pour cette fonctionnalité.

Rôles installés

Titre du rôle [name]	Description	Contient des rôles
Administrateur des menaces [sn_ti.admin]	Dispose d'un contrôle total sur toutes les propriétés de menace, les SLA et les notifications.	sn_ti.write
Lecteur de menace [sn_ti.lire]	Dispose d'un accès en lecture aux informations sur les menaces.	sn.sec_cmn.int_read
Auteur de menace [sn_ti.écrire]	Dispose d'un accès en écriture aux informations sur les menaces. Impossible de supprimer les modes d'attaque, les indicateurs ou les observables. Seul un administrateur des menaces peut les supprimer.	• sn_sec_cmn.int_write • sn_ti.lire
Analyste MITRE [sn_ti.mitre_analyst]	Ce rôle active l'accès MITRE-ATT&CK en lecture aux modules dans Renseignements sur les menaces et vers le SIR module.	• sn_ti.lire • sn_si.read

Tables installées

Table	Description
Mécanismes d'attaque [sn_ti_attack_mechanism]	Organise les schémas d'attaque de manière hiérarchique en fonction des mécanismes fréquemment utilisés lors de l'exploitation d'une vulnérabilité. Les catégories qui sont membres de cette vue représentent les différentes techniques utilisées pour attaquer un système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Modes/méthode d'attaque [sn_ti_attack_mode]	Les modes et méthodes d'attaque sont des représentations du comportement des cyberadversaires. Ils caractérisent ce que fait un adversaire et comment il le fait avec des niveaux de détail croissants.
Méthode de découverte [sn_ti_discovery_method]	Expression de la façon dont un incident a été découvert.
Groupe [sn_ti_feed]	Utilisé pour configurer le flux de menaces (RSS) dans la vue d'ensemble des menaces.
Indicateur : mode/méthode d'attaque [sn_ti_m2m_indicator_attack_mode]	Utilisé pour mapper les modes/méthodes d'attaque aux indicateurs.
Indicateur de compromis [sn_ti_indicator]	Utilisé pour transmettre des modèles observables spécifiques combinés à des informations contextuelles destinées à représenter des artefacts et/ou des comportements d'intérêt dans un contexte de cybersécurité.
Indicateur de compromis Métadonnées [sn_ti_indicator_metadata]	Utilisé pour remplir les enregistrements TAXII.
Source de l'indicateur [sn_ti_m2m_indicator_source]	Utilisée pour collecter toutes les sources générant des rapports sur un indicateur spécifique.
Type d'indicateur [sn_ti_indicator_type]	Caractérise un indicateur de cybermenace composé d'un modèle identifiant certaines conditions observables ainsi que des informations contextuelles sur la signification des modèles, comment et quand il est utilisé, etc.
Type d'indicateur connexe [sn_ti_m2m_indicator_indicator_type]	Lie les indicateurs à leurs types applicables
Nombre d'incidents [sn_ti_observable]	Nombre d'incidents de sécurité associés à un observable.
Effet souhaité [sn_ti_intended_effect]	Utilisé pour exprimer l'effet escompté d'un auteur de menace.
Résultat de l'analyse IP [sn_ti_ip_result]	Utilisé pour afficher les résultats d'une recherche d'adresses IP.
Limite de taux de programmes malveillants	Définit une limite de taux à utiliser sur une source de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_ti_rate_limit]	
Analyse anti-programme malveillant [sn_ti_scan]	Une recherche. Contient ce qu'il faut rechercher, avec la source de recherche et un résumé des résultats de la recherche.
Entrée de la file d'attente de l'analyse anti-programme malveillant [sn_ti_scan_q_entry]	Un enregistrement de recherche mis en file d'attente pour la recherche ou le traitement. Facilite les demandes dans les limites de débit indiquées.
Résultat de l'analyse anti-programme malveillant [sn_ti_scan_result]	Affiche le résultat d'une recherche.
Scanner de programme malveillant [sn_ti_scanner]	Définit les sources de recherche tierces à utiliser pour effectuer des recherches.
Limite de débit du scanner de programme malveillant [sn_ti_scanner_rate_limit]	Associe une source de recherche à une limite de taux.
Type de programme malveillant [sn_ti_malware_type]	Utilisé pour exprimer les types d'instances de programmes malveillants.
Observable [sn_ti_observable]	Les observables dans STIX représentent des propriétés d'état ou des événements mesurables pertinents pour le fonctionnement des ordinateurs et des réseaux.
Type de contexte de l'observable [sn_ti_observable_context_type]	Stocke le contexte (source, destination d'une adresse IP, etc.) d'un observable.
Indicateur observable [sn_ti_m2m_observable_indicator]	Utilisé pour relier les observables aux indicateurs
Source d'observable [sn_ti_observable_source]	Utilisé pour relier les observables aux sources de menace.
Type d'observable [sn_ti_observable_type]	Répertorie les différents types d'observables, tels que les adresses IP.
Catégorie de type de l'observable [sn_ti_observable_type_category]	Stocke la première catégorisation des observables (par exemple, les adresses IP et les URL). Il est utilisé pour déterminer plus précisément les types d'observables.
Mode/méthode d'attaque connexe [sn_ti_m2m_attack_mode_attack_mode]	Utilisé pour relier les modes d'attaque les uns aux autres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Observables associés [sn_ti_m2m_observables]	Utilisé pour relier les observables les uns aux autres.
Type d'analyse [sn_ti_scan_type]	Définition d’un type de recherche, avec des enregistrements initiaux pour le fichier, l’URL et l’adresse IP.
Ticket de sécurité [sn_ti_case]	Stocke les enregistrements de tickets de sécurité créés à l’aide de Gestion des tickets.
Ticket de sécurité IoC [sn_ti_case_ioc]	Utilisée pour gérer la relation entre les observables et les tickets.
Tâche associée au ticket de sécurité [sn_ti_m2m_case_task]	Utilisé pour gérer la relation entre les tâches (incidents de sécurité, demandes de changement, etc.) avec les tickets de sécurité.
Exclusion de relation des tickets de sécurité [sn_ti_case_relationship_exclusion]	Fournit la définition de l’inclusion et de l’exclusion des enregistrements connexes dans les tickets de sécurité.
Perception [sn_ti_sighting]	Lien m2m entre l’observable et le résultat détaillé de la recherche de perceptions utilisé dans l’exécution d’une demande de recherche de perception.
Éléments de configuration de perception [sn_ti_m2m_sighting_ci]	Mappe les éléments de configuration à une recherche de perceptions.
Détail de la recherche de perception [sn_ti_sighting_search_detail]	Détails d’une recherche d’observations, par exemple, le nombre d’éléments externes internes trouvés.
Résultat de la recherche de perception [sn_ti_sighting_search]	En-tête d’une exécution de recherche de perceptions.
Types d'observables pris en charge [sn_ti_m2m_ind_type_obs_type]	Associe les types d’indicateurs aux types d’observables valides.
Type d’analyse pris en charge [sn_ti_supported_scan_type]	Mappe le type de recherche à une implémentation spécifique à la source de recherche/au fournisseur. Indique qu’une source de recherche spécifique prend en charge le type.
Mode/méthode d’attaque de la tâche [sn_ti_m2m_task_attack_mode]	Relie les modes d’attaque aux tâches.
Indicateur de tâche [sn_ti_m2m_task_indicator]	Associe les indicateurs aux tâches.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Tâche Observable [sn_ti_m2m_task_observable]	Associe les observables aux tâches.
Perception de la tâche [sn_ti_m2m_task_sighting]	Stocke les enregistrements de tâches (incidents et tickets de sécurité) associés à un enregistrement d'observation.
Collecte TAXII [sn_ti_taxii_collection]	Définit un flux de renseignements sur les cyber-risques qui peut être importé par un serveur TAXII.
Profil TAXII [sn_ti_taxii_profile]	Définit un référentiel pour le partage des renseignements sur les cyber-risques. Contient les collections TAXII.
Type d'acteur de menace [sn_ti_threat_actor_type]	Fournit des caractérisations des acteurs malveillants (ou adversaires) représentant une menace de cyberattaque, y compris l'intention présumée et le comportement historiquement observé.
Source de renseignements sur les menaces [sn_ti_source]	Définit une source pour l'importation des données sur les menaces.
Motivation de l'attaque connexe [sn_ti_stix2_m2m_object_attack_motivation]	Collecte toutes les motivations d'attaque associées à un objet STIX.
Type d'infrastructure associée [sn_ti_stix2_m2m_infra_type]	Relie l'infrastructure à leurs types.
Phase de kill chain associée [sn_ti_stix2_m2m_indicator_kill_chain_phase]	Relie les phases de kill chain aux indicateurs.
Phase de kill chain associée [sn_ti_stix2_m2m_object_kill_chain_phase]	Relie les phases de kill chain aux objets STIX.
Aptitude de programme malveillant associée [sn_ti_stix2_m2m_malware_capability]	Relie les programmes malveillants à leurs options.
Type de logiciel malveillant associé [sn_ti_stix2_m2m_malware_malware_type]	Relie les programmes malveillants à leurs types.
Observable associé [sn_ti_stix2_m2m_malware_observable]	Collecte tous les observables associés à un programme malveillant.
Observable associé [sn_ti_stix2_m2m_observed_data_observable]	Collecte tous les observables associés à des données observées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Type de rapport associé [sn_ti_stix2_m2m_report_report_type]	Relie les rapports de menace à leurs types.
Rôle de l'acteur de menace associée [sn_ti_stix2_m2m_threat_actor_threat_actor_role]	Relie les auteurs de menace à leurs rôles.
Type d'acteur de menace associée [sn_ti_stix2_m2m_threat_actor_threat_actor_type]	Relie les auteurs de menace à leurs types.
Type d'outil associé [sn_ti_stix2_m2m_tool_tool_type]	Relie les outils à leurs types.
Motivation de l'attaque [sn_ti_stix2_attack_motivation]	La motivation de l’attaque façonne l’intensité et la persistance d’une attaque. Les acteurs de la menace et les ensembles d’intrusion agissent généralement d’une manière qui reflète leur émotion ou leur situation sous-jacente, ce qui informe les défenseurs de la manière dont ils attaquent.
Modèle d'attaque [sn_ti_stix2_attack_pattern]	Type de TTP qui décrit les méthodes utilisées par les adversaires pour tenter de compromettre des cibles.
Campagne [sn_ti_stix2_campaign]	Regroupement de comportements antagonistes qui décrivent un ensemble d’activités malveillantes ou d’attaques (parfois appelées vagues) qui se produisent sur une période contre un ensemble spécifique de cibles.
Déroulement de l'action [sn_ti_stix2_course_of_action]	Recommandation d’un producteur de renseignements à un consommateur sur les mesures qu’il pourrait prendre en réponse aux renseignements.
Référence externe [sn_ti_stix2_external_reference]	Pointeurs vers des informations représentées en dehors de STIX.
Perception d'identité [sn_ti_stix2_m2m_sighting_identity]	Collecte toutes les identités associées à une observation.
Identité [sn_ti_stix2_identity]	Personnes, organisations ou groupes réels (exemple : ACME, Inc.) ainsi que catégories d’individus, d’organisations, de systèmes ou de groupes (exemple : secteur financier).
Référence externe de l'indicateur [sn_ti_stix2_indicator_external_reference]	Représente les références externes associées aux indicateurs.
Perception de l'indicateur	Représente les perceptions des indicateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_ti_stix2_indicator_sighting]	
Type d'infrastructure [sn_ti_stix2_infrastructure_type]	Représente les différents types d’infrastructure.
Infrastructure [sn_ti_stix2_infrastructure]	Type de TTP qui décrit tous les systèmes, services logiciels et toutes les ressources physiques ou virtuelles associées, destinés à soutenir un but donné (par exemple, les serveurs C2 utilisés dans le cadre d’une attaque, les appareils ou les serveurs faisant partie de la défense, les serveurs de base de données ciblés par une attaque, entre autres).
Logiciel installé [sn_ti_stix2_m2m_malware_analysis_sw]	Collecte tous les logiciels (types de logiciels SCO) associés à une analyse de programme malveillant.
Ensemble d'intrusions [sn_ti_stix2_intrusion_set]	Un ensemble groupé de comportements et de ressources antagonistes avec des propriétés communes que l’on pense être orchestré par une seule organisation.
Phase de kill chain [sn_ti_stix2_kill_chain_phase]	Représente les phases de kill chain associées à une kill chain.
Chaîne de frappe [sn_ti_stix2_kill_chain]	Représente diverses chaînes de frappe.
Emplacement [sn_ti_stix2_location]	Représente un emplacement géographique fourni via STIX.
Analyse de programme malveillant [sn_ti_stix2_malware_analysis]	Métadonnées et résultats d’une analyse statique ou dynamique particulière effectuée sur une instance ou une famille de programmes malveillants.
Aptitude de logiciel malveillant [sn_ti_stix2_malware_capability]	Représente les options courantes d’une famille ou d’une instance de programme malveillant.
Système d'exploitation du logiciel malveillant [sn_ti_stix2_m2m_malware_operating_system]	Collecte tous les systèmes d’exploitation (types de logiciels SCO) associés aux programmes malveillants.
Programme malveillant [sn_ti_stix2_malware]	Un type TTP qui représente le code malveillant.
Définition de marquage [sn_ti_stix2_marking_definition]	Représente les besoins de gestion ou de partage des objets STIX.
Perception d'objets	Représente les observations d’objets STIX.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
[sn_ti_stix2_object_sighting]	
Relations objet-indicateur [sn_ti_stix2_m2m_object_indicator]	Collecte toutes les relations entre les objets STIX et les indicateurs STIX.
Relation objet-objet [sn_ti_stix2_m2m_object]	Collecte toutes les relations entre les objets STIX et d'autres objets STIX, à l'exception des indicateurs.
Relation objet-observable [sn_ti_stix2_m2m_object_observable]	Collecte toutes les relations entre les observables STIX et les objets STIX.
Perception de données observées [sn_ti_stix2_m2m_sighting_observed_data]	Collecte tous les objets de données observés associés à une observation.
Données observées [sn_ti_stix2_observed_data]	Transmet des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX.
Type de rapport [sn_ti_stix2_report_type]	Représente l'objectif ou le sujet principal des rapports de menace.
Observable rapporté [sn_ti_stix2_m2m_malware_analysis_observable]	Collecte tous les observables associés à l'analyse de programme malveillant.
Objet STIX V2 [sn_ti_stix2_object]	Table parente commune pour l'objet STIX.
Perception STIX V2 [sn_ti_stix2_sighting]	Table parente commune pour les tables de perception STIX.
Rôle d'acteur de menace [sn_ti_stix2_threat_actor_role]	Représente les rôles qui peuvent être joués par les acteurs de la menace.
Acteur de menace [sn_ti_stix2_threat_actor]	Les acteurs de la menace sont des individus, des groupes ou des organisations réels soupçonnés d'opérer avec des intentions malveillantes.
Regroupement des menaces [sn_ti_stix2_threat_grouping]	Regroupe tous les objets STIX qui partagent un contexte commun.
Note de menace [sn_ti_stix2_threat_note]	Fournit un contexte et une analyse supplémentaire qui ne sont pas contenus dans l'objet STIX correspondant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
Opinion sur la menace [sn_ti_stix2_threat_opinion]	Fournit une évaluation de l'exactitude des informations dans un objet STIX produit par une entité différente.
Rapport de menace [sn_ti_stix2_threat_report]	Les rapports sont des collections de renseignements sur les menaces axés sur une ou plusieurs rubriques, telles que la description d'un acteur malveillant, d'un programme malveillant ou d'une technique d'attaque, y compris le contexte et les détails connexes. Ils sont utilisés pour regrouper les renseignements sur les menaces liés à la communication afin de les publier sous forme d'article complet sur les cybermenaces.
Type d'outil [sn_ti_stix2_tool_type]	Catégories d'outils qui peuvent être utilisés pour effectuer des attaques.
Outil [sn_ti_stix2_tool]	Les outils sont des logiciels légitimes utilisés par les acteurs de la menace pour effectuer des attaques.
Vulnérabilité [sn_ti_stix2_vulnerability]	Représente une faiblesse ou un défaut dans les exigences, les conceptions ou les implémentations de la logique de calcul (exemple de code) trouvée dans le logiciel et certains composants matériels (exemple de micrologiciel). Elles peuvent être directement exploitées pour avoir un impact négatif sur la confidentialité, l'intégrité ou la disponibilité de ce système.

Définir les Renseignements sur les menaces propriétés

Renseignements sur les menaces les propriétés vous permettent de contrôler le fonctionnement de différents aspects du système, y compris le réglage des clés API.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration** > **Propriétés**.
2. Définissez les propriétés suivantes comme il convient.

Propriétés pour Renseignements sur les menaces

Propriété	Description
Nom du domaine pour récupérer des informations supplémentaires pour les adresses IP/URL sn_ti.recherche_ip.site_web	Nom du domaine à utiliser pour récupérer des informations supplémentaires dans votre base de données IoC. Cette propriété est utilisée par l'include de script ThreatAdditionalInfo pour renseigner

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	des informations supplémentaires sur le formulaire Observables. Valeur par défaut : http://api.ipinfodb.com/v3/ip-country/ **Remarque :** L'API tierce pinfodb.com est disponible sans frais supplémentaires et utilisée dans de nombreux logiciels commerciaux. Si vous le remplacez par un nom de domaine différent, vous devez également fournir la clé API dans le champ suivant.
Clé API à utiliser pour le domaine, le cas échéant sn_ti.ip_lookup.api_key	Clé API à utiliser pour récupérer des informations supplémentaires dans votre base de données IoC. Cette propriété est utilisée (avec la propriété sn_ti.ip_lookup.web_site) par l'include de script ThreatAdditionalInfo pour renseigner des informations supplémentaires sur le formulaire Observables.
N'exécutez pas de recherche automatisée de menaces sur un observable lorsque l'observable est associé à un IoC ou qu'il est malveillant. sn_ti.scan_ioc_before_sending **Remarque :** Vous devez définir la durée dans la propriété suivante (sn_ti.scan_ioc_num_days).	Option permettant d'arrêter l'exécution de la recherche automatisée de menaces sur un observable lorsqu'il s'avère que celui-ci est malveillant ou associé à un IoC pendant la durée configurée (en jours). Si vous devez toujours exécuter la recherche de menace pour l'observable, vous pouvez le faire manuellement. Valeur par défaut : oui
Durée (en jours) sn_ti.scan_ioc_num_days	Option permettant de définir la durée pendant laquelle la recherche automatisée de menace de l'observable est ignorée. Valeur par défaut (en jours) : 30
N'exécutez pas de recherche automatisée de menaces sur un observable si elle a déjà été exécutée. sn_ti.enable_threat_lookup_bypass	S'il existe un résultat de recherche de menace pour un observable déjà disponible, vous avez la possibilité d'ignorer la réexécution de la recherche de menace automatisée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Remarque : Vous devez définir la durée dans la propriété suivante (sn_ti.threat_lookup_bypass_times).	pour le même observable jusqu'à ce que la durée configurée soit écoulée. Valeur par défaut : non **Remarque :** Si vous activez cette propriété, assurez-vous d'ajouter une valeur appropriée.
Durée (en minutes) sn_ti.threat_lookup_bypass_time	Option permettant de définir la durée après laquelle la recherche automatisée de menace de l'observable peut être réexécutée. Valeur par défaut (en minutes) : 0
Définissez une durée de validité pour les remplacements d'utilisateur sur le résultat observable. sn_ti.enable_observable_finding_system_override **Remarque :** Vous devez définir la validité dans la propriété suivante (sn_ti.observable_finding_override_expiry).	Option permettant de définir une durée de validité pour les remplacements d'utilisateur sur les résultats observables. Le résultat de la recherche de menace de l'observable ne sera pas modifié par le système de base pendant cette durée de validité. Valeur par défaut : Non. **Remarque :** Si vous activez cette propriété, assurez-vous d'ajouter une valeur appropriée.
Validité (en minutes) sn_ti.observable_finding_override_expiry	Option permettant de définir la période de validité du résultat observable. Valeur par défaut (en minutes) : aucune
Lorsqu'un mode/une méthode d'attaque n'a été reçu d'aucune source pendant le nombre de jours spécifié, marquez-le comme inactif. sn_ti.attack_mode_inactivate_days	Nombre de jours à partir de la dernière réception d'un mode/méthode d'attaque pour que l'enregistrement soit marqué comme inactif. Valeur par défaut : 360 **Remarque :** La case **à cocher Actif** n'est pas visible sur le formulaire **Mode/méthode d'attaque** par défaut. Cependant, vous pouvez l'ajouter. Lorsque les modes/méthodes d'attaque sont inactifs, ils ne peuvent pas être sélectionnés sur d'autres formulaires.
Lorsqu'un indicateur n'a été reçu d'aucune source pendant le nombre de jours spécifié, marquez-le comme inactif.	Nombre de jours à partir de la dernière réception d'un indicateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
sn_ti.indicator_inactivate_days	pour que l'enregistrement soit marqué comme inactif. Valeur par défaut : 180 **Remarque :** La case **à cocher Actif** n'est pas visible sur le formulaire **Indicateur** par défaut. Cependant, vous pouvez l'ajouter. Lorsque les indicateurs sont inactifs, ils ne peuvent pas être sélectionnés sur d'autres formulaires.
Taille maximale de la charge utile (en Mo) d'une pièce jointe STIX pouvant être analysée. sn_ti.stix.max_taille_charge utile	Spécifie la taille maximale de la charge utile pour la pièce jointe STIX que vous pouvez analyser. Valeur par défaut : aucune Valeur maximale autorisée : aucune limite.
Délai maximal, en secondes, pendant lequel une connexion HTTP sortante attend pour récupérer les données de collecte TAXII sn_ti.taxii.http.max_timeout	Spécifie la durée maximale d'attente d'une connexion HTTP sortante avant d'extraire le paquet suivant de données de collecte TAXII. Valeur par défaut : 300
Nombre maximal d'objets récupérés dans un seul appel REST à partir d'un serveur TAXII (applicable uniquement pour les versions 2.0 et 2.1 de TAXII) sn_ti.taxii.max_taille_page	Spécifie le nombre maximal d'objets récupérés dans un seul appel REST à partir du serveur TAXII pour une page. Valeur par défaut : 5000 Valeur maximale autorisée : 50 000
Nombre maximal de nouvelles tentatives pour un échec d'appel REST TAXII 2.X sn_ti.taxii2.retry_count	Spécifie le nombre maximal de nouvelles tentatives pour un appel REST TAXII ayant échoué. Valeur par défaut : 3

3. Cliquez sur **Enregistrer**.

Définir une source de menace

Vous pouvez gérer une liste des sources de Renseignements sur les menaces menace. Chaque source inclut la possibilité de définir la fréquence à laquelle une source est interrogée. Vous pouvez également exécuter une source de menace sur demande pour importer les données STIX (Structured Threat Information eXpression) nécessaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_ti.admin

Pourquoi et quand exécuter cette tâche

Renseignements sur les menaces utilise deux technologies pour importer des informations relatives aux menaces : STIX et TAXII (Trusted Automated Exchange of Indicator Information).

STIX fournit un langage standardisé et structuré pour représenter un ensemble complet d'informations sur les cybermenaces qui comprend des indicateurs d'activité de compromission (IoC) (par exemple, les adresses IP et les hachages de fichiers), ainsi que des informations contextuelles concernant les menaces, telles que les modes/méthodes d'attaque, qui, ensemble, caractérisent plus complètement les motivations, les capacités et les activités d'un cyberadversaire. En tant que telles, les données STIX fournissent des informations précieuses sur la meilleure façon dont votre organisation peut se défendre contre les cybermenaces.

L'échange automatisé fiable d'informations d'indicateur (TAXII) est utilisé pour faciliter l'échange automatisé d'informations sur les cybermenaces. TAXII définit un ensemble de services et d'échanges de messages qui permettent le partage d'informations exploitables sur les cybermenaces au-delà des frontières des organisations et des produits/services pour la détection, la prévention et l'atténuation des cybermenaces. Les profils TAXII peuvent être configurés en tant que référentiels pour le partage d'informations au format STIX. Chaque profil contient une ou plusieurs collections ou flux TAXII.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Sources** > **Sources de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Le nom de la source de menace.
Application	L'application qui contient l'enregistrement.
Actif	Cochez cette case pour activer la source de menace.
Avancés	Cochez cette case pour afficher les scripts dans les champs **Script de l'instanciateur d'intégration** et **Processeur de rapport** .
Description	Description de cette source de menace.

4. Renseignez les champs de la section **Calendrier** , selon vos besoins.

Champ	Description
Exécuter	Fréquence à laquelle vous souhaitez que l'intégration s'exécute : Quotidien, Hebdomadaire, Périodiquement, etc. Comme indiqué, les champs suivants sont affichés en fonction de la configuration de ce champ.
Jour	Le jour où vous souhaitez que l'intégration s'exécute.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Si vous avez sélectionné **Hebdomadaire** dans le champ **Exécuter** , ce champ affiche les jours de la semaine. ○ Si vous avez sélectionné **Tous les mois** dans le champ **Exécuter** , ce champ affiche les jours du mois.
Heure	Heure à laquelle vous souhaitez que l'intégration commence.
Intervalle de répétition	Si vous avez sélectionné **Périodiquement** dans le champ **Exécuter** , ce champ affiche le nombre de jours et d'heures avant que l'intégration ne s'exécute à nouveau.
En cours de démarrage	Si vous avez sélectionné **Périodiquement** dans le champ **Exécuter** , ce champ affiche les dates et l'heure à utiliser comme point de départ pour les mises à jour périodiques.
Conditionnel	Sélectionnez ce champ si vous souhaitez ajouter des paramètres conditionnels.
Condition	Si vous avez coché la case **Conditionnel** , entrez les conditions ici.

5. Renseignez les champs de la section Détails de la **menace** , selon vos besoins.

Champ	Description
Indicateur	Indicateur à utiliser lorsque les données n'en fournissent pas explicitement. Pour les listes de blocs, si vide, un nouvel indicateur est créé pour chaque observable.
Type d'indicateur	Le type d'indicateur à utiliser pour les indicateurs qui sont créés et les données ne fournissent pas explicitement un type d'indicateur.
Modes/méthode d'attaque	Le mode/la méthode d'attaque à utiliser lorsque les données n'en fournissent pas explicitement.
Type d'observable	Type d'observable à utiliser pour les observables qui sont créés et les données ne fournissent pas explicitement un type d'observable.[SI1]
Pondération	Entrez une valeur de poids pour cette source à utiliser dans le calcul de confiance.

Remarque : L'utilisation des champs **Indicateur**, **Type d'indicateur**, **Mode/Méthode d'attaque** et **Type d'observable** est spécifique à l'implémentation. Le processeur par défaut, SimpleBlocklistProcessor, se comporte comme le décrivent les info-bulles. Toutefois, une source de menace TAXII est entièrement pilotée par les données. Tout processeur de source de menace personnalisé pourrait utiliser sa propre stratégie. Ces champs sont essentiellement des éléments à exposer à l'intégration/processeur et l'implémentation décide comment les utiliser.

6. Renseignez les champs de la section Détails de la **source** , le cas échéant.

Champ	Description
Point de terminaison	Entrez l'URL du point de terminaison de service Web à laquelle la source de menace est accessible Renseignements sur les menaces. Cliquez sur l'icône de verrou pour verrouiller l'URL.
Utiliser le message REST	Si vous avez besoin d'un message REST pour accéder à la source de menace, cochez cette case. Les champs **Message REST** et **Méthode REST** deviennent obligatoires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Message REST	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir un nouveau message REST .
Méthode REST	Cliquez sur l'icône de recherche et sélectionnez la méthode REST dans la liste ou cliquez sur **Nouveau** pour définir une nouvelle méthode REST.
Script d'intégration	Le script d'intégration par défaut est **SimpleRESTSecurityDataIntegration**. Il exécute un simple appel REST, enregistre la réponse sous forme de pièce jointe, puis renvoie la pièce jointe au processeur. Ce script répond aux besoins de la plupart des organisations. Mais si vous le souhaitez, vous pouvez cliquer sur l'icône de recherche et sélectionner un script d'intégration différent ou en définir un nouveau.
Script de l'instanciateur d'intégration	Si la case **à cocher Avancé** est sélectionnée, ce champ affiche le script réel de construction du script d'intégration. Vous pouvez modifier le script si nécessaire. Cette capacité est utile pour les implémentations personnalisées. Les intégrations dans le système de base n'ont généralement pas besoin de logique de constructeur personnalisée.
Script de processeur de rapport	Le script d'intégration par défaut est **SimpleBlocklistProcessor**. Ce script est un processeur simple qui accepte une liste de blocs simple (simple, c'est-à-dire un document à colonne unique avec des observables tels que des URL ou des adresses IP) et crée des observables. Elle utilise les différents champs Détails de la **menace** pour déterminer les champs à définir lors de la création d'observables.
Script de l'instanciateur de processeur	Si la case **Avancé** est cochée, ce champ affiche le script réel de construction du processeur. Vous pouvez modifier le script si nécessaire. Ce script est généralement utile pour les implémentations personnalisées. Les intégrations dans le système de base n'ont généralement pas besoin d'une logique de constructeur personnalisée.

7. Cliquez sur **Envoyer**.

Remarque : Pour plus d'informations sur la configuration de la pagination de la source de menace, consultez KB1213825 article.

Créer un profil TAXII

Vous pouvez gérer les profils TAXII pour partager des informations au format STIX. Chaque profil contient une ou plusieurs collections ou flux TAXII.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Sources** > **Profils TAXII**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs suivants comme il vous convient.

Champ	Description
Nom	Nom du profil TAXII
Application	L'application qui contient l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utiliser les messages REST comme modèle	Si vous avez besoin d'un message REST pour accéder au profil TAXII, cochez cette case.
Version TAXII	Spécifiez la version de TAXII. Les versions STIX prises en charge sont 1.1, 2.0 et 2.1.
Description	Description de ce profil TAXII.

4. Renseignez les champs de la section **Configuration du service Découverte** comme il convient.

Champ	Description
Point de terminaison du service de découverte	Le point de terminaison de découverte autorise les clients à obtenir des informations sur un serveur TAXII et une liste des racines d'API.
Utiliser le message REST	Sélectionnez cette option si vous avez besoin d'un message REST pour accéder au profil TAXII. Les champs **Message REST Service de découverte** et **Méthode REST Service de découverte** deviennent obligatoires.
Message REST du service de découverte	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir un nouveau message REST.
Méthode REST du service de découverte	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir une nouvelle méthode REST.

5. Renseignez les champs de la section **Configuration du service de collecte** , comme il convient.

Champ	Description
Point de terminaison du service d'information sur la collecte	Une collection TAXII est une interface vers un référentiel logique d'objets CTI fourni par un serveur TAXII et est utilisée par les clients TAXII pour envoyer des informations au serveur TAXII ou demander des informations au serveur TAXII. Un serveur TAXII peut héberger plusieurs collections par racine d'API, et les collections sont utilisées pour échanger des informations de manière demande-réponse.
Utiliser le message REST	Sélectionnez cette option si vous avez besoin d'un message REST pour accéder au profil TAXII. Les champs **Message REST Service d'informations de collecte** et **Méthode REST Service d'informations de collecte** deviennent obligatoires.
Message REST du service d'information sur la collecte	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir un nouveau message REST.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Méthode REST du service d'information sur la collecte	Cliquez sur l'icône de recherche et sélectionnez le message REST dans la liste ou cliquez sur **Nouveau** pour définir une nouvelle méthode REST.

6. Cliquez sur **Envoyer**.

Référentiel IoC

Le référentiel IoC contient des objets STIX, chacun de ces objets contient une information spécifique.

Lorsque vous combinez des objets STIX par le biais de relations, vous permettez des représentations faciles ou complexes de Cyber Threat Intelligence (CTI).

Renseignements sur les menaces prend en charge les versions 1.1, 2.0 et 2.1 de STIX.

Modes et méthodes d'attaque

Les modes et méthodes d'attaque, parfois appelés tactiques, techniques et procédures (TTP), sont des représentations du comportement des cyberadversaires. Ils caractérisent ce que font ces adversaires et comment ils le font, avec des niveaux de détail croissants. Les modes et méthodes d'attaque s'appliquent à STIX la version 1.1.

Par exemple, un mode/méthode d'attaque peut consister à utiliser des logiciels malveillants pour voler les informations d'identification des cartes de crédit. Ou une autre tactique connexe (à un niveau de détail inférieur) peut consister à envoyer des e-mails ciblés avec des pièces jointes contenant un code malveillant, qui s'exécute à l'ouverture, capture les informations de carte de crédit à partir des frappes clavier et utilise http pour communiquer avec un serveur de commande et de contrôle pour transférer des informations.

Les modes et méthodes d'attaque s'appliquent à STIX la version 1.1.

Définir un mode/méthode d'attaque

Les modes et méthodes d'attaque sont importés avec les données STIX, mais vous pouvez ajouter de nouveaux modes/méthodes, si nécessaire.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Modes/méthode d'attaque**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Sélectionner une balise de classification	Si vous configurez et activez des balises de classification pour ajouter des métadonnées à l'enregistrement, vous pouvez sélectionner une ou plusieurs balises pour spécifier le degré de sensibilité du mode/de la méthode d'attaque. Si vous n'avez pas configuré ou activé les balises de classification, cette liste déroulante ne s'affiche pas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Titre	Entrez un nom descriptif pour ce mode/méthode d'attaque.
Type de programme malveillant	Sélectionnez le type de programme malveillant pour ce mode/méthode d'attaque. Les types de programmes malveillants disponibles sont récupérés à partir du serveur du fournisseur en tant que données STIX.
Source	Sélectionnez la source de données de menace pour ce mode/méthode d'attaque. Certaines sources de données sont incluses dans le système de base. Vous pouvez créer de nouvelles sources de données selon vos besoins.
Mécanismes d'attaque	Sélectionnez le mécanisme d'attaque pour ce mode/méthode d'attaque. Les mécanismes d'attaque représentent les différentes techniques utilisées pour attaquer un système. Les mécanismes d'attaque disponibles sont récupérés sur le serveur du fournisseur sous forme de données STIX.
Premier observé	Cette date est récupérée à partir du serveur du fournisseur en tant que données STIX.
Dernier observé	Cette date est récupérée à partir du serveur du fournisseur en tant que données STIX.
Type d'acteur de menace	Sélectionnez le type d'acteur de menace pour ce mode/méthode d'attaque. Les types d'acteurs de menace caractérisent les acteurs malveillants (ou adversaires) représentant une menace de cyberattaque, y compris l'intention présumée et le comportement historiquement observé. Les types d'acteurs de menace disponibles sont récupérés sur le serveur du fournisseur en tant que données STIX.
Description	Entrez une description du mode/de la méthode d'attaque.
Gestion	Entrez des instructions sur la façon de gérer ce mode/méthode d'attaque.
Effet souhaité	Entrez l'effet escompté de ce type d'attaque.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
Vous pouvez consulter l'une des listes connexes suivantes pour afficher des informations supplémentaires.

Liste connexe	Description
Indicateurs connexes	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace.
Mode/méthode d'attaque enfant	Répertorie les modes/méthodes d'attaque enfants du mode/méthode d'attaque parent.
Tâches associées	Répertorie les changements associés au mode/méthode d'attaque parent.

Ajouter un IoC à un mode/méthode d'attaque

En plus d'importer des indicateurs en tant que données STIX, vous pouvez ajouter manuellement des IoC à un mode/méthode d'attaque.

Avant de commencer
Rôle requis : sn_ti.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Modes/méthode d'attaque**.
2. Cliquez sur le mode d'attaque auquel vous souhaitez ajouter un IoC.
3. Cliquez sur la liste connexe **Indicateurs connexes** .
4. Cliquez sur **Modifier**.
5. Au besoin, utilisez les filtres pour localiser l'IoC que vous souhaitez ajouter.
6. À l'aide de la zone de liste double, ajoutez l'IoC à la liste **des indicateurs connexes** .
7. Cliquez sur **Enregistrer**.

Ajouter une méthode de mode d'attaque connexe

En plus d'importer des modes/méthodes d'attaque en tant que données STIX, vous pouvez ajouter manuellement des modes/méthodes d'attaque connexes.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Modes/méthode d'attaque**.
2. Cliquez sur le mode d'attaque auquel vous souhaitez ajouter un mode/méthode d'attaque associé.
3. Cliquez sur la liste connexe **Mode/méthode d'attaque enfant** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser le mode/méthode d'attaque que vous souhaitez associer à celui en cours.
6. À l'aide de la zone de liste double, ajoutez le mode/la méthode d'attaque à la liste **des modes/méthodes d'attaque enfants** .
7. Cliquez sur **Enregistrer**.

Ajouter une tâche associée à un mode/une méthode d'attaque

En plus d'importer les tâches associées (telles que les changements et les incidents) en tant que données STIX, vous pouvez les ajouter manuellement à un mode/une méthode d'attaque.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Modes/méthode d'attaque**.
2. Cliquez sur le mode d'attaque auquel vous souhaitez ajouter une tâche associée.
3. Cliquez sur la liste connexe **Tâches associées** .
4. Cliquez sur **Modifier**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Si nécessaire, utilisez les filtres pour localiser les tâches que vous souhaitez associer au mode/méthode d'attaque.
6. À l'aide de la zone de liste double, ajoutez la tâche à la liste **des tâches associées** .
7. Cliquez sur **Enregistrer**.

Indicateurs de compromis

Les indicateurs de compromission (IoC) sont des artefacts observés sur un réseau ou un système d'exploitation qui sont susceptibles d'indiquer une intrusion. Les IoC typiques sont les signatures de virus et les adresses IP, les hachages MD5 de fichiers ou d'URL de logiciels malveillants ou les noms de domaine. L'IoC s'applique aux STIX versions 1.1 et 2.x.

Un IoC peut être un observable unique ou une collection d'observables (par exemple, une seule mauvaise URL connue ou la présence d'un fichier spécifique et de quelques valeurs de clé de registre spécifiques).

Une fois que les IoC ont été identifiés dans un processus de réponse aux incidents et d'expertise informatique, ils peuvent être utilisés pour la détection précoce de futures tentatives d'attaque à l'aide de systèmes de détection d'intrusion et de logiciels antivirus.

L'IoC s'applique aux STIX versions 1.1 et 2.x.

Voir un IoC

Les IoC, parfois appelés indicateurs, sont le plus souvent récupérés à partir d'une source de données sur les menaces sous le nom de données STIX. Si nécessaire, vous pouvez également créer des IoC.

Avant de commencer

Rôle requis : sn_ti.write

Procédure

1. Une fois que la tâche planifiée a récupéré les données IoC à partir de la source de données définie, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
   Les IoC récupérés sont répertoriés.
2. Cliquez sur l'IoC que vous souhaitez afficher.
3. Les informations suivantes s'affichent.

Champ	Description
Sélectionner une balise de classification	Si vous avez configuré et activé des balises de sécurité pour ajouter des métadonnées à l'enregistrement, vous pouvez sélectionner une ou plusieurs balises pour spécifier le degré de sensibilité de l'IoC. Si vous n'avez pas configuré ou activé les balises de sécurité, cette liste déroulante ne s'affiche pas.
Titre	Nom qui décrit cet indicateur.
Premier observé	Première date à laquelle cet indicateur a été observé dans le système.
Dernier observé	Date à laquelle cet indicateur a été observé le plus récemment dans le système.
Nombre rencontré	Nombre de fois que l'indicateur a été rencontré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nombre de sources	Nombre de fois où l'indicateur a été importé de sources de menace définies.
Notes	Toute remarque supplémentaire sur l'indicateur. Ce champ peut également contenir des paires clé/valeur JSON.

4. Vous pouvez cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Observables associés	Répertorie les observables liés à l'indicateur actuel.
Mode/ méthode d'attaque connexe	Répertorie les modes/méthodes d'attaque associés qui ont été identifiés comme associés à cet indicateur.
Type associé	Répertorie d'autres types d'indicateurs associés à cet IoC.
Sources d'indicateurs	Répertorie les sources de cet indicateur, ainsi que son niveau de confiance.
Tâches associées	Répertorie toutes les tâches, tous les changements et tous les incidents associés à l'IoC.
Métadonnées de l'indicateur	Si le champ **Notes** contient des paires clé/valeur JSON valides, elles sont analysées et affichées. Si aucune paire clé/valeur JSON n'est présente, ou si le JSON n'est pas valide, cette liste connexe ne s'affiche pas.
Annotations de sécurité	
Références externes de l'indicateur	
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.

Ajouter un observable connexe à un IoC

En plus d'importer des observables en tant que données STIX, vous pouvez ajouter manuellement des observables connexes à un IoC.

Avant de commencer
Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'indicateur auquel vous souhaitez ajouter un observable associé.
3. Cliquez sur la liste connexe **Observables connexes** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser l'observable que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez l'observable à la liste **Observables connexes** .
7. Cliquez sur **Enregistrer**.

Ajouter un mode/méthode d'attaque connexe à un IoC

En plus d'importer des modes/méthodes d'attaque connexes en tant que données STIX, vous pouvez ajouter manuellement des modes/méthodes d'attaque connexes à un IoC.

Avant de commencer
Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'indicateur auquel vous souhaitez ajouter un mode/méthode d'attaque connexe.
3. Cliquez sur la liste **connexe Mode/méthode d'attaque connexe** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser le mode/méthode d'attaque que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez le mode/la méthode d'attaque à la liste **Mode/méthode d'attaque connexe** .
7. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identifier les types d'indicateurs associés

Si aucun type d'indicateur associé n'est défini pour un IoC, il suit tous les types d'observables. Toutefois, si vous associez un ou plusieurs types d'indicateurs à un IoC, cela limite les types d'observables qui peuvent être associés à l'IoC.

Avant de commencer
Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'indicateur auquel vous souhaitez associer un type d'indicateur.
3. Cliquez sur la liste connexe **Type associé** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser le type d'indicateur que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez le type d'indicateur à la liste **Type associé** .
7. Cliquez sur **Enregistrer**.

Identifier les sources d'indicateurs

Les sources d'indicateurs sont normalement suivies automatiquement dans le cadre du processus d'importation des menaces, mais d'autres sources peuvent être ajoutées manuellement.

Avant de commencer
Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'indicateur auquel vous souhaitez ajouter des sources d'indicateurs.
3. Cliquez sur la liste connexe **Sources d'indicateurs** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser la source d'indicateur que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez la source d'indicateur à la liste **des sources d'indicateurs** .
7. Cliquez sur **Enregistrer**.

Ajouter des tâches associées à un IoC

En plus d'importer des tâches associées (telles que des changements et des incidents) en tant que données STIX, vous pouvez les ajouter manuellement à un IoC.

Avant de commencer
Rôle requis : sn_ti.write

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
2. Cliquez sur l'IoC auquel vous souhaitez ajouter une tâche associée.
3. Cliquez sur la liste connexe **Tâches associées** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser les tâches que vous souhaitez associer à l'IoC.
6. À l'aide de la zone de liste double, ajoutez la tâche à la liste **des tâches associées** .
7. Cliquez sur **Enregistrer**.

Observables

Les observables représentent des propriétés avec état (telles que le hachage MD5 d'un fichier ou la valeur d'une clé de registre) ou des événements mesurables (tels que la création d'une clé de registre ou la suppression d'un fichier) qui sont pertinents pour le fonctionnement des ordinateurs et des réseaux. Les observables s'appliquent pour STIX les versions 1.1 et 2.x.

Les ensembles de cyber-observables sont utiles pour identifier les indicateurs de compromission lorsqu'ils sont combinés à des informations contextuelles représentant les comportements des cybermenaces.

Les observables s'appliquent pour STIX les versions 1.1 et 2.x.

Définir un observable

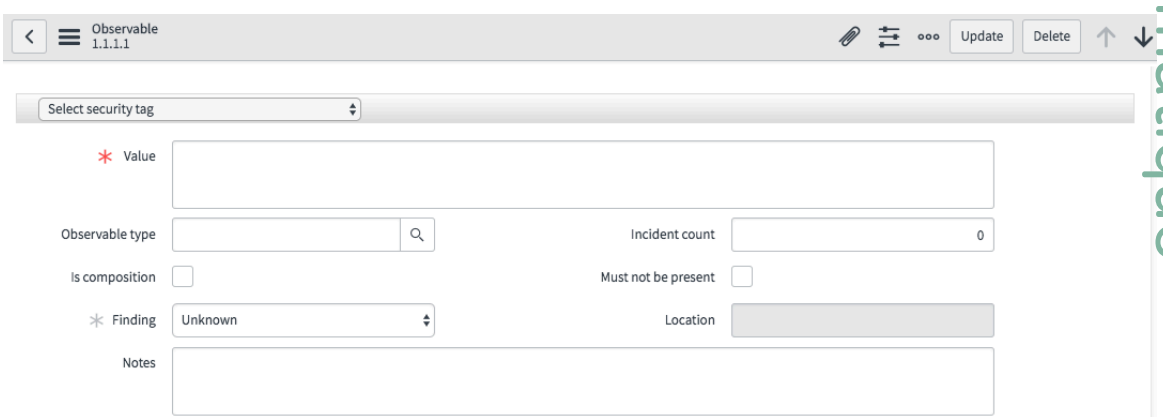
Les observables sont récupérés à partir du serveur du fournisseur en tant que données STIX. Toutefois, vous pouvez créer des observables selon vos besoins.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur **Nouveau**.



3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Sélectionner une balise de classification	Si vous avez configuré et activé des balises de sécurité pour ajouter des métadonnées à l'enregistrement, vous pouvez sélectionner une ou plusieurs balises pour spécifier le degré de sensibilité de l'observable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Si vous n'avez pas configuré ou activé les balises de sécurité, cette liste déroulante ne s'affiche pas.
Valeur	Valeur (par exemple, adresse IP ou hachage) associée à l'observable. **Remarque :** Si une analyse des menaces sur une adresse IP ou un hachage, renvoie un programme malveillant ou une autre défaillance, l'adresse IP ou la valeur de hachage est automatiquement ajoutée à la table Observable [sn_ti_observable]. En tant que tel, il peut être recherché à partir du formulaire Observables.
Type d'observable	Sélectionnez la classification de l'observable, telle qu'une adresse IP ou un hachage de fichier. Ces types d'observables sont définis dans le module **Types d'observables** .
Nombre d'incidents	Nombre de fois où la valeur de l'observable a été rencontrée.
Est une composition	Ce champ s'affiche uniquement après avoir sauvegardé l'enregistrement de l'observable. Si le **type d'observable** est défini sur autre chose que **Composition observable** et que ce nouvel observable est une composition, cochez cette case. Si le **type d'observable** est déjà défini sur **Composition de l'observable**, la case est cochée et en lecture seule. Une composition observable est un observable qui contient des observables enfants.
Résultat	Sélectionnez l'une des options suivantes : ○ **malveillant** : indique que l'observable est nuisible à l'organisation. ○ **Suspect** : indique que l'observable peut être dangereux pour l'organisation. ○ **Propre** : indique que l'observable n'est pas dangereux pour l'organisation. ○ **Inconnu** : indique que nous n'avons pas encore déterminé la conclusion de l'observable. ○ Valeur par défaut : inconnue. Pour plus d'informations, consultez Calculateurs de résultats de la recherche de menace. **Remarque :** Après une mise à niveau, les observables existants sont marqués comme malveillants.
Opérateur	Ce champ s'affiche uniquement si la case **Est la composition** est cochée. Selon votre configuration dans ce champ, les observables et leurs enfants sont pris en compte pour décider si un indicateur associé est présent. Définissez ce champ sur **ET** si tous les observables enfants doivent être présents pour qu'un indicateur associé soit considéré comme présent. Définissez-le sur **OU** si l'un des observables enfants est présent pour qu'un indicateur associé soit considéré comme présent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ne doit pas être présent	Ce champ s'affiche uniquement après avoir sauvegardé l'enregistrement de l'observable. Si ce champ est sélectionné, ce champ signifie que l'absence de l'observable est le problème potentiel (par exemple, une clé de Registre manquante).
Emplacement	Vous pouvez charger Charger plus de données IoC dans ce champ à l'aide des paramètres de deux propriétés et d'une définition d'include de script.
Notes	Saisissez toutes les remarques supplémentaires sur l'observable.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires.

Liste connexe	Description
Indicateurs connexes	Répertorie les indicateurs qui ont été identifiés par la source de menace.
Tâches associées	Répertorie les changements associés à l'observable.
Observables enfants	Répertorie les observables associés qui ont été identifiés par la source de menace.
Ressources correspondantes pour IP	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante.
Sources des observables	Répertorie les sources de cet observable, ainsi que le niveau de confiance de la source.
Annotations de sécurité	Répertorie les annotations de sécurité ajoutées à cet observable.

Ajouter un IoC connexe à un observable

En plus d'importer des observables en tant que données STIX, vous pouvez ajouter manuellement des observables connexes à un IoC.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'observable auquel vous souhaitez ajouter un IoC associé.
3. Cliquez sur la liste connexe **Indicateurs connexes** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser l'indicateur que vous voulez associer à l'observable.
6. À l'aide de la zone de liste double, ajoutez l'indicateur à la liste **des indicateurs connexes** .
7. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter des tâches associées à un observable

En plus d'importer des tâches associées (telles que des changements et des incidents) en tant que données STIX, vous pouvez les ajouter manuellement à un observable.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'observable auquel vous souhaitez ajouter une tâche associée.
3. Cliquez sur la liste connexe **Tâches associées** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser les tâches que vous souhaitez associer à l'observable.
6. À l'aide de la zone de liste double, ajoutez la tâche à la liste **des tâches associées** .
7. Cliquez sur **Enregistrer**.

Ajouter un observable connexe

En plus d'importer des observables en tant que données STIX, vous pouvez ajouter manuellement des observables connexes.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'observable auquel vous souhaitez ajouter un observable connexe.
3. Cliquez sur la liste connexe **Observables enfants** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser l'observable que vous voulez associer à l'observable actuel.
6. À l'aide de la zone de liste double, ajoutez l'observable à la liste **des observables enfants** .
7. Cliquez sur **Enregistrer**.

Charger plus de données IoC

En fonction des paramètres de deux propriétés et d'une définition d'include de script, vous pouvez charger des informations de géolocalisation pour les adresses IP et les sites web dans le formulaire Observables. Avec une personnalisation plus poussée, vous pouvez également ajouter d'autres informations, telles que les codes des pays, les noms de ville.

Avant de commencer
Les deux propriétés suivantes doivent être définies :

- **Nom du domaine permettant de récupérer des informations supplémentaires pour les adresses IP/URL** [sn_ti.ip_lookup.web_site]
- **Clé API à utiliser pour le domaine ci-dessus, le cas échéant** [sn_ti.ip_lookup.api_key]

Rôle requis : sn_ti.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'adresse IP ou l'URL de l'observable sur lequel vous souhaitez afficher plus de données IoC. Le champ **Emplacement** affiche la géolocalisation de l'IoC.
3. Cliquez sur le bouton **Enrichir les données** pour charger les données IoC supplémentaires.
4. Vous pouvez également configurer le formulaire Observable pour ajouter d'autres champs liés à l'emplacement, tels que le code du pays et le code de la ville.

> **Remarque :** Pour charger plus d'informations relatives à l'emplacement, modifiez l'include de script **ThreatAdditionalInfo** et fournissez la clé API appropriée à partir du site Web qui fournit les informations supplémentaires.

Identifier les sources d'observables

Si un observable n'a pas de sources définies, il utilise tous les types de sources. Toutefois, si vous ajoutez une ou plusieurs sources de menace à un observable, les sources utilisées sont limitées.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Cliquez sur l'observable auquel vous souhaitez ajouter des sources d'observables.
3. Cliquez sur la liste connexe **Sources observables** .
4. Cliquez sur **Modifier**.
5. Si nécessaire, utilisez les filtres pour localiser la source que vous souhaitez associer à l'observable.
6. À l'aide de la zone de liste double, ajoutez la source observable à la liste **Sources observables** .
7. Cliquez sur **Enregistrer**.

Effectuer des recherches sur les observables

Vous pouvez effectuer des recherches de connaissance des menaces sur un ou plusieurs observables pour déterminer s'ils sont associés à des menaces de sécurité connues. Les implémentations d'analyse qui s'exécutent dépendent de celles que vous avez activées.

Avant de commencer

Avant de pouvoir effectuer des recherches, vous devez activer le module d'extension Renseignements sur les menaces. Vous devez également installer le module d'extension pour une ou plusieurs des implémentations d'analyse :

- Intégration de CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Opérations de sécurité : ai-je été pwned ?
- VirusTotal

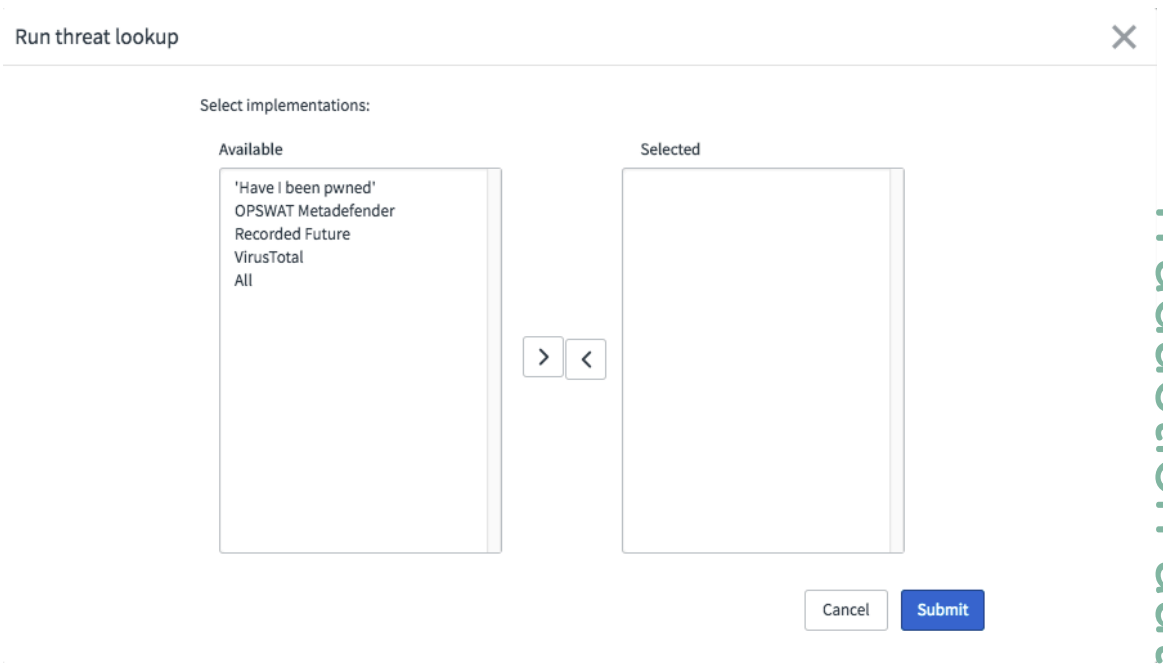
Rôle requis : sn_ti.write

Traduction automatique

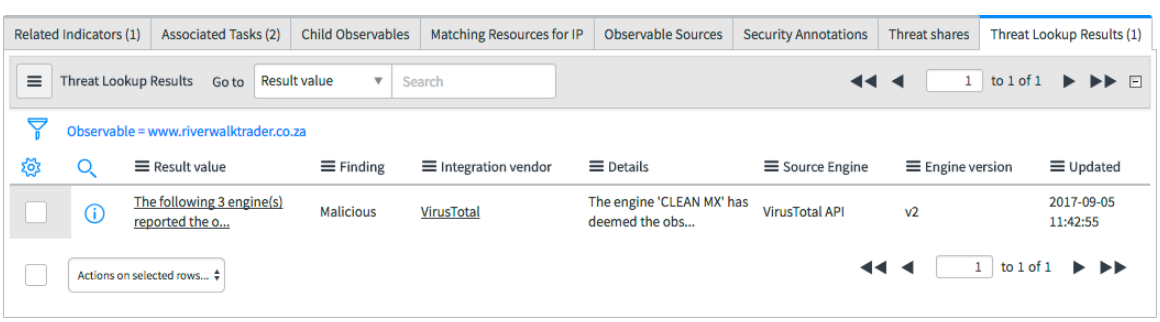
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Effectuez l'une des actions suivantes :
   - Pour effectuer une recherche sur plusieurs observables, sélectionnez les observables, cliquez sur **Actions sur les lignes sélectionnées**, puis sélectionnez **Exécuter une recherche de menace**.
   - Pour effectuer une recherche sur un seul observable, ouvrez l'enregistrement de l'observable, puis cliquez sur le lien connexe **Exécuter une recherche de menace** .



3. Sélectionnez les implémentations de recherche de menaces que vous souhaitez utiliser ou sélectionnez **Tout** pour effectuer des recherches à l'aide de toutes les implémentations actives, puis cliquez sur **Soumettre**. Un message indique que les recherches de menaces ont commencé. L'exécute Security Operations Integration - Flux de recherche de menaces et exécute également les workflows d'implémentation pour les implémentations de recherche de menaces que vous avez sélectionnées. Les recherches sont effectuées et les résultats sont générés.
4. Une fois les recherches terminées, vous pouvez cliquer sur **l'onglet Résultats de la recherche de menaces** pour afficher les résultats.



Résultat de la recherche de menaces récentes : vous pouvez également voir les résultats de recherche de menaces les plus récents ou les plus récents de chaque fournisseur d'intégration lorsque vous cliquez sur **l'onglet Résultat de la recherche de menaces récentes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : **L'onglet Résultat de la recherche de menaces récentes** ne fait pas partie du système de base.

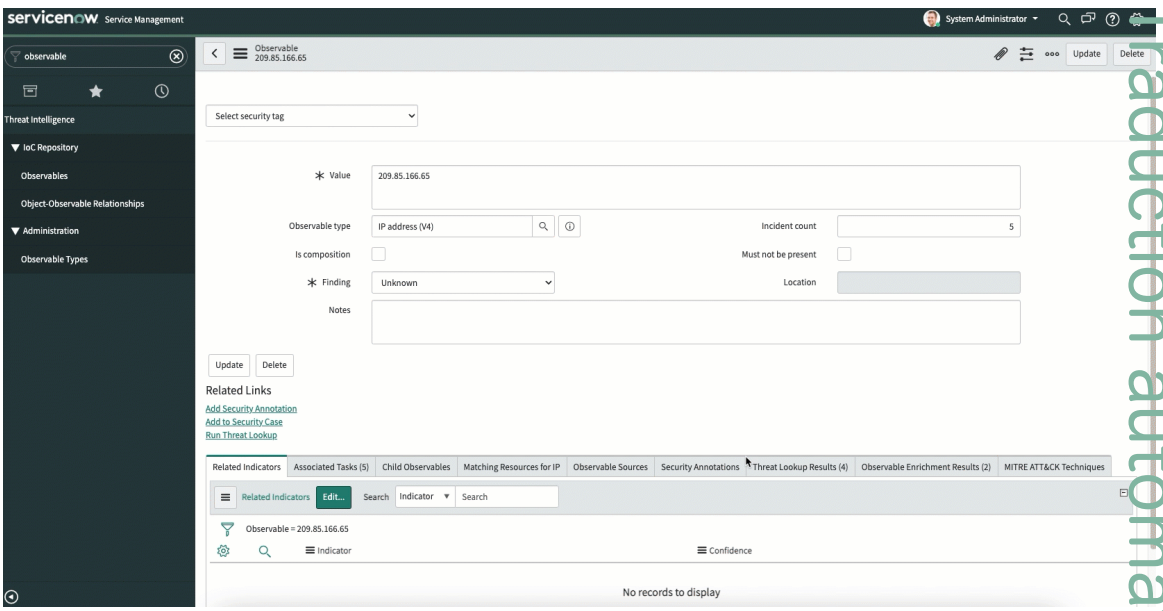
Pour activer cet onglet, procédez comme suit :

a. Cliquez avec le bouton droit sur l'en-tête du formulaire.

b. Accédez à la **Configurer** > **Listes connexes**.

c. Localisez les résultats de la **recherche de menaces récentes** dans la liste Disponible et déplacez-les vers la liste Sélectionné.

d. Cliquez sur **Enregistrer**.
Vous pouvez désormais afficher les résultats de la recherche de menaces récentes auprès de chaque fournisseur d'intégration dans **l'onglet Résultat de la recherche de menaces récentes** .

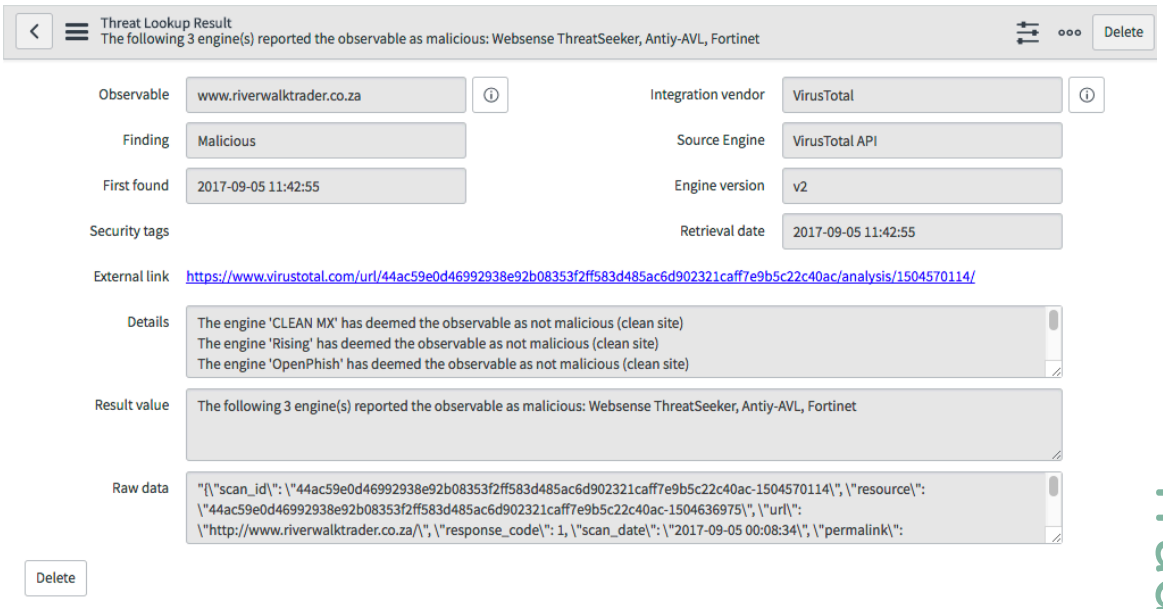


5. Pour afficher des détails supplémentaires, y compris les résultats bruts pour une recherche spécifique, cliquez sur la **valeur Résultat**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque les implémentations VirusTotal ou OPSWAT Metadefender sont utilisées, les détails sont consolidés, comme indiqué ci-dessous.



Effectuer un enrichissement des menaces sur les observables

Vous pouvez effectuer un enrichissement de la connaissance des menaces sur un ou plusieurs observables pour déterminer s'ils sont associés à des menaces de sécurité connues. Les implémentations qui s'exécutent dépendent de celles que vous avez activées.

Avant de commencer

Avant de pouvoir effectuer l'enrichissement, vous devez activer le module d'extension Threat Intelligence. Vous devez également installer le module d'extension pour une ou plusieurs des implémentations d'enrichissement :

- Intégration de CrowdStrike Falcon Intelligence
- OPSWAT Metadefender
- Opérations de sécurité : ai-je été pwned ?
- VirusTotal
- Qui est ?

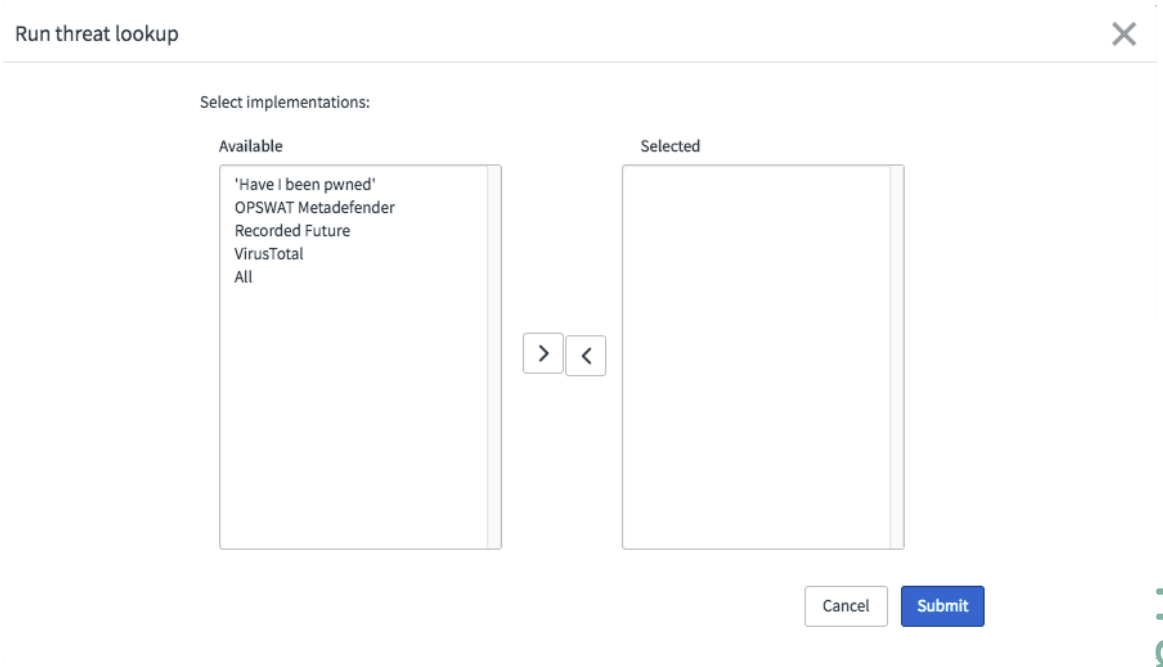
Rôle requis : sn_ti.admin

Procédure

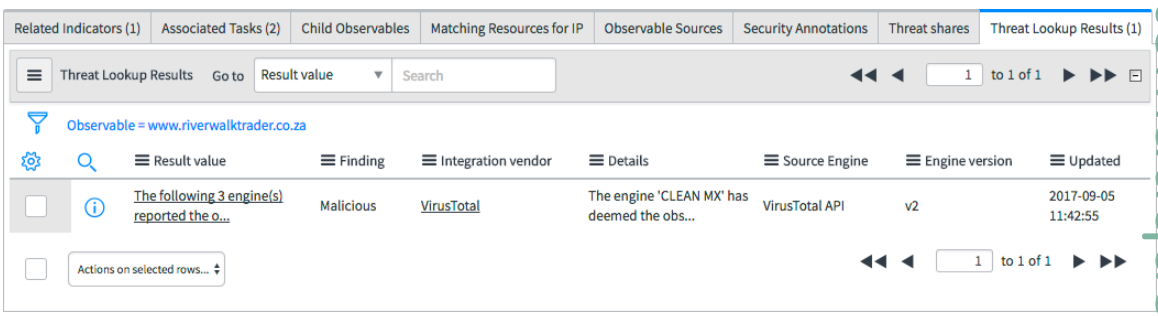
1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Effectuez l'une des actions suivantes :
   - Pour effectuer une recherche sur plusieurs observables, sélectionnez les observables, cliquez sur **Actions sur les lignes sélectionnées**, puis sélectionnez **Exécuter une recherche de menace**.
   - Pour effectuer une recherche sur un seul observable, ouvrez l'enregistrement de l'observable, puis cliquez sur le lien connexe **Exécuter une recherche de menace** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Sélectionnez les implémentations de recherche de menaces que vous souhaitez utiliser ou sélectionnez **Tout** pour effectuer des recherches à l'aide de toutes les implémentations actives, puis cliquez sur **Soumettre**. Un message indique que les recherches de menaces ont commencé. L'exécute Security Operations Integration - Flux de recherche de menaces et exécute également les workflows d'implémentation pour les implémentations de recherche de menaces que vous avez sélectionnées. Les recherches sont effectuées et les résultats sont générés.
4. Une fois les recherches terminées, vous pouvez cliquer sur **l'onglet Résultats de la recherche de menaces** pour afficher les résultats.

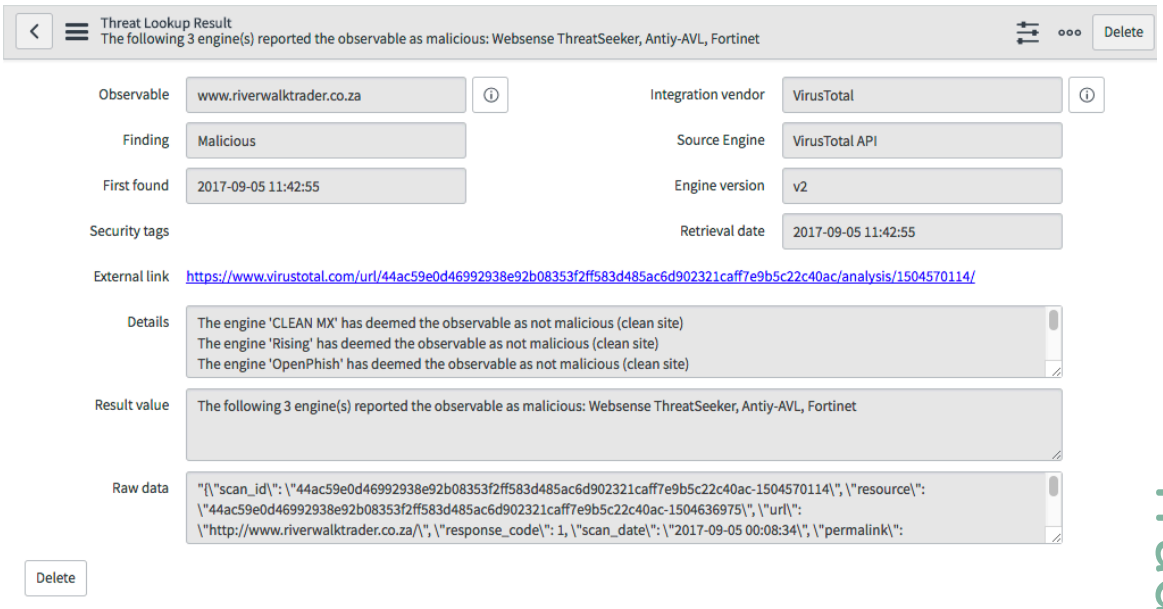


5. Pour afficher des détails supplémentaires, y compris les résultats bruts pour une recherche spécifique, cliquez sur la **valeur Résultat**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Lorsque les implémentations VirusTotal ou OPSWAT Metadefender sont utilisées, les détails sont consolidés, comme indiqué ci-dessous.



Modèles d'attaque

Les schémas d’attaque sont un type de tactiques, de techniques et de procédures (TTP) qui décrivent les méthodes par lesquelles les adversaires tentent de compromettre les cibles. Les schémas d’attaque s’appliquent à STIX 2.x.

Les schémas d’attaque sont utilisés pour faciliter la catégorisation des attaques. Ils généralisent des attaques spécifiques aux modèles qu’ils suivent et fournissent des informations détaillées sur la façon dont les attaques sont effectuées.

Par exemple, le spear phishing est un type d’attaque courant où un attaquant envoie un e-mail soigneusement conçu à une partie dans le but de l’amener à cliquer sur un lien ou à ouvrir une pièce jointe pour diffuser un logiciel malveillant. Les schémas d’attaque sont plus spécifiques, tels que le spear phishing par un acteur de menace particulier (par exemple, le fait que la cible ait gagné un concours) peuvent également être un modèle d’attaque.

Définir un modèle d’attaque

Définissez un modèle d’attaque pour faciliter la catégorisation des attaques.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Schémas d'attaque**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom descriptif pour ce modèle d’attaque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Entrez une description du modèle d'attaque.
Alias	Noms alternatifs pour identifier ce modèle d'attaque.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au modèle d'attaque.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Déroulement des actions	Répertorie le plan d'actions associé à cet objet qui sont des réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu) pour prévenir une attaque.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Campagnes

Une campagne est un regroupement de comportements contradictoires. Ces comportements décrivent un ensemble d'activités malveillantes ou d'attaques qui se produisent au fil du temps contre un ensemble spécifique de cibles. Les campagnes s'appliquent à STIX 2.x.

Les campagnes ont généralement des objectifs bien définis et peuvent faire partie d'un ensemble d'intrusions.

Les campagnes sont souvent attribuées à un ensemble d'intrusions et à des acteurs de la menace. Les acteurs de la menace peuvent réutiliser l'infrastructure connue de l'ensemble d'intrusion ou peuvent mettre en place une nouvelle infrastructure spécifique à la conduite de cette campagne.

Les campagnes ont un objectif commun dans les incidents qu'elles provoquent, les personnes ou les ressources qu'elles ciblent, et les ressources qu'elles utilisent.

Par exemple, un syndicat du crime attaque les dirigeants d'ACME Bank. Ils attaquent en utilisant une variante spécifique de logiciels malveillants et de nouveaux serveurs pour obtenir des informations secrètes sur une fusion à venir avec une autre banque.

Définir une campagne

Définissez une campagne pour regrouper les comportements antagonistes.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Campagnes**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Saisissez un nom descriptif pour cette campagne.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description qui fournit plus de détails et de contexte sur la campagne. Cela inclut son objectif et ses principales caractéristiques.
Alias	Noms alternatifs pour identifier cette campagne.
Objectif	Le but principal, l'objectif, le résultat souhaité ou l'effet recherché de la campagne. Ce que l'acteur de la menace ou l'ensemble de l'intrusion espère accomplir avec cette campagne.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la campagne.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Identités	Liste des identités associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Plan d'actions

Un plan d'action est une action prise soit pour empêcher une attaque, soit pour répondre à une attaque en cours. Plan d'action s'applique à STIX 2.x.

Plan d'actions décrit les réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu). Il peut également décrire des actions de niveau supérieur telles que la formation des employés ou des changements de politique.

Par exemple, un plan d'action pour atténuer une vulnérabilité pourrait décrire l'application du correctif qui la corrige.

Définir un plan d'action

Définissez un plan d'action pour prévenir une attaque ou pour répondre à une attaque en cours.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Déroulement des actions**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Entrez un nom descriptif pour cette ligne de conduite.
Action	Pour capturer des plans d'action structurés ou automatisés.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur le plan d'action, y compris potentiellement son objectif et ses principales caractéristiques.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au cours de l'action.

Liens connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identités

Les identités représentent des individus, des organisations ou des groupes réels (ACME, Inc.) et des catégories d'individus, de systèmes ou de groupes (le secteur financier). Les identités s'appliquent pour STIX 2.x.

Le SDO d'identité peut capturer des informations d'identification de base, des informations de contact et les secteurs auxquels l'identité appartient. L'identité représente les cibles des attaques, les sources d'information, les créateurs d'objets et les identités des acteurs de la menace.

Définir les identités

Définissez des identités qui représentent des individus, des organisations ou des groupes réels.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Identités**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour cette identité. Lorsqu'il s'agit d'une entité spécifique (un individu ou une organisation), cette pro–priété doit contenir le nom canonique de l'entité spécifique.
Classe d'identité	Type d'entité que cette identité décrit. Par exemple, une personne ou une organi–sation.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description qui fournit plus de détails et de contexte sur l'identité, y compris potentiellement son objectif et ses principales caractéristiques.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Infrastructure

Le SDO Infrastructure représente un type de tactiques, de techniques et de procédures (TTP). Ils décrivent tous les systèmes, services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'attaque. L'infrastructure s'applique à STIX 2.x.

Les éléments d'une attaque sont représentés par d'autres SDO ou SCO. Toutefois, le SDO d'infrastructure représente un groupe nommé de données qui constitue l'infrastructure.

Parmi les exemples d'infrastructure, citons les serveurs C2 utilisés dans une attaque, un appareil ou un serveur faisant partie d'une défense, ou les serveurs de base de données ciblés par une attaque.

Définir l'infrastructure

Définissez une infrastructure, c'est-à-dire tous les systèmes, services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'attaque.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Infrastructure**.
2. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom descriptif pour identifier l'infrastructure.
Premier observé	Moment auquel cette infrastructure a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette infrastructure a été vue pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description qui fournit plus de détails et de contexte sur l'infrastructure, y compris potentiellement son objectif, la façon dont elle est utilisée, son lien avec d'autres activités de renseignement saisies dans des objets connexes et ses principales caractéristiques.
Alias	Noms alternatifs pour identifier cette infrastructure.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires. Vous pouvez également associer d'autres objets à l'infrastructure.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Observables associés	Répertorie les observables associés à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Infrastructure associée	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Ensemble d’intrusions

Un ensemble d’intrusions est un ensemble groupé de comportements et de ressources antagonistes ayant des propriétés communes. Un ensemble d’intrusions implique généralement une seule organisation. L’ensemble d’intrusions s’applique à STIX 2.x.

Un ensemble d’intrusions peut capturer plusieurs campagnes ou d’autres activités. Ces activités ont en commun des attributs indiquant un auteur de menace connu ou inconnu.

Une nouvelle activité peut être attribuée à un ensemble d’intrusions, même si les acteurs de la menace à l’origine de l’attaque ne sont pas connus. Les acteurs de la menace peuvent passer d’un ensemble d’intrusion à un autre, ou ils peuvent prendre en charge plusieurs ensembles d’intrusion.

Un ensemble d’intrusion est l’ensemble de l’attaque et peut être utilisé sur une longue période dans plusieurs campagnes pour atteindre des objectifs potentiellement multiples.

Définir un ensemble d’intrusions

Définissez un ensemble d’intrusions, c’est-à-dire un ensemble groupé de comportements et de ressources adverses ayant des propriétés communes.

Avant de commencer
Rôle requis : sn_ti.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Ensemble de confiance**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour identifier l'ensemble d'intrusion.
Premier observé	Heure à laquelle cet ensemble d'intrusion a été vu pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cet ensemble d'intrusion a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Motivation principale	Raison principale, motivation ou but derrière cet ensemble d'intrusion. La motivation est la raison pour laquelle l'ensemble d'intrusion veut atteindre l'objectif (ce qu'il essaie d'atteindre). Par exemple, une intrusion dans le but de perturber le secteur financier d'un pays peut être motivée par une haine idéologique du capitalisme.
Niveau de ressource	Cette propriété spécifie le niveau organisationnel auquel cet ensemble d'intrusions fonctionne généralement, qui à son tour détermine les ressources disponibles pour une attaque.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'ensemble d'intrusion, y compris potentiellement son objectif et ses principales caractéristiques.
Alias	Noms alternatifs pour identifier cet ensemble d'intrusion.
Objectifs	Les objectifs de haut niveau de cette intrusion sont de savoir ce qu'ils essaient de faire. Par exemple, ils peuvent être motivés par un gain personnel, mais leur objectif est de voler des numéros de carte de crédit. Pour ce faire, ils peuvent exécuter des campagnes spécifiques qui ont des objectifs détaillés comme compromettre les systèmes de point de vente d'un grand détaillant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'ensemble d'intrusions.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Motivations de l'attaque connexe	Répertorie toutes les motivations secondaires recherchées par cet ensemble d'intrusions.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Emplacements

Un emplacement représente un emplacement géographique. Les emplacements sont principalement utilisés pour donner un contexte à d'autres organismes de statistique. Les emplacements s'appliquent à STIX 2.x.

L'emplacement peut contenir tout ou partie des éléments suivants : région (Amérique du Nord), adresse municipale (New York, États-Unis), latitude et longitude.

Le SDO d'emplacement peut se rapporter à un ensemble d'identité ou d'intrusion pour indiquer que l'identité ou l'ensemble d'intrusion se trouve à cet emplacement. Il peut également se rapporter à un logiciel malveillant ou à un modèle d'attaque pour indiquer que la victime cible se trouve à un endroit particulier.

Par exemple, un emplacement pourrait être utilisé dans une relation pour décrire que l'ensemble d'intrusion de l'hirondelle bourgeoise provient d'Europe de l'Est.

Au moins une des propriétés ou jeux de propriétés suivants doit être fourni :

- region
- pays
- Latitude et longitude

Définir l'emplacement

Définissez un emplacement géographique pour fournir plus de contexte aux autres SDO.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Emplacements**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour identifier l'emplacement.
Adresse (rue)	Adresse postale décrite par cet emplacement. Cette propriété comprend tous les aspects ou parties de l'adresse postale.
Ville	Ville dans laquelle se trouve cet emplacement.
Code postal	Code postal dans lequel se trouve cet emplacement.
Région	Région dans laquelle se trouve cet emplacement.
Pays	Pays dans lequel se trouve cet emplacement.
Latitude	Latitude de l'emplacement en degrés décimaux. Les nombres positifs décrivent les latitudes au nord de l'équateur et les nombres négatifs décrivent les latitudes au sud de l'équateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété doit être comprise entre -90,0 et 90,0 respectivement.
Longitude	Longitude de l'emplacement en degrés décimaux. Les nombres positifs décrivent les longitudes à l'est du méridien d'origine et les nombres négatifs décrivent les longitudes à l'ouest du méridien d'origine. La valeur de cette propriété doit être comprise entre -180,0 et 180,0 inclus.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'ensemble d'intrusion, y compris potentiellement son objectif et ses principales caractéristiques.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'emplacement.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Programme malveillant

Un logiciel malveillant est un type de TTP qui représente un code malveillant. Il s'agit d'un programme qui est secrètement inséré dans un système. Les programmes malveillants s'appliquent à STIX 2.x.

L'intention d'un logiciel malveillant est de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation (OS) de la victime.

L'ODD de programme malveillant caractérise, identifie et catégorise les instances et les familles de programmes malveillants à partir des données dérivées de l'analyse. Cette SDO capture des informations détaillées sur le fonctionnement du logiciel malveillant et ce qu'il fait.

Définir un programme malveillant

Définissez un programme malveillant qui représente un code malveillant.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Programme malveillant**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom pour identifier l'instance ou la famille de programme malveillant, tel que spécifié par le créateur du SDO. Pour une famille de logiciels malveillants, le nom doit être défini.
Premier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour la dernière fois en train d'effectuer des activités malveillantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description qui fournit plus de détails et de contexte sur l'instance ou la famille de programme malveillant, y compris potentiellement son objectif et ses principales caractéristiques.
Alias	Noms alternatifs pour identifier cette instance ou famille de programme malveillant.
ID source	Identificateur unique de cet objet dans la source de menace.
Est la famille	Spécifie si l'objet représente une famille de programmes malveillants ou une instance de programme malveillant.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au programme malveillant.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Options associées	Répertorie les options identifiées et associées à cet objet.
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Observables associés	Répertorie les observables associés à cet objet.
Logiciel malveillant associé	Répertorie les programmes malveillants associés identifiés à cet objet.
Systèmes d'exploitation associés	Les systèmes d'exploitation sur lesquels l'objet est exécutable. Cela s'applique aussi bien aux systèmes d'exploitation virtualisés qu'à ceux fonctionnant sur du matériel nu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Déroulement des actions	Répertorie le plan d'actions associé à cet objet qui sont des réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu) pour prévenir une attaque.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Analyse de programme malveillant	Répertorie les enregistrements d'analyse de programme malveillant associés à cet objet.
Observables rapportés	Répertorie les observables signalés comme faisant partie de cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

Analyse de programme malveillant

L'analyse des programmes malveillants capture les métadonnées et les résultats d'un programme malveillant. L'analyse des programmes malveillants s'applique à STIX 2.x.

L'analyse de programme malveillant comprend une analyse statique ou dynamique effectuée sur une instance ou une famille de programme malveillant.

Définir l'analyse de programme malveillant

Définissez une analyse de programme malveillant qui capture les métadonnées et les résultats d'une analyse statique ou dynamique particulière effectuée sur une instance ou une famille de programme malveillant.

Avant de commencer

Rôle requis : sn_ti.admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Analyse de programme malveillant**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour identifier l'ensemble d'intrusion.
Version du moteur d'analyse	Version du moteur d'analyse ou du produit (y compris les moteurs VA) utilisé pour effectuer l'analyse.
Version de la définition de l'analyse	Version des définitions d'analyse utilisée par l'outil d'analyse (y compris les outils VA).
Analyse démarrée	Date et heure de lancement de l'analyse de programme malveillant.
Analyse terminée	Date et heure auxquelles l'analyse de programme malveillant a été terminée.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Résultat	Résultat de classification tel que déterminé par le processus d'analyse du scanner ou de l'outil.
Nom des résultats	Résultat de classification ou nom attribué à l'instance de programme malveillant par l'outil de scanner.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'analyse de programme malveillant.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
	est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Logiciel malveillant associé	Répertorie les programmes malveillants associés identifiés à cet objet.
Observables rapportés	Répertorie les observables signalés comme faisant partie de cet objet.
Logiciel installé	Répertorie tout logiciel non standard installé sur le système d'exploitation utilisé pour l'analyse dynamique de l'instance ou de la famille de programme malveillant.

Données observées

Les données observées transmettent des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX. Les données observées s'appliquent à STIX 2.x.

Les données observées capturent à la fois une observation unique d'une seule entité (fichier, connexion réseau) et l'agrégation de plusieurs observations d'une entité.

Vous pouvez utiliser des données observées seules (sans relations) pour transmettre des données brutes collectées à partir de n'importe quelle source. Les sources comprennent des rapports d'analystes, des bacs à sable et des outils de détection basés sur le réseau et l'hôte.

Par exemple, les données observées peuvent capturer des informations sur une adresse IP, une connexion réseau, un fichier ou une clé de registre. Les données observées ne sont pas une affirmation de renseignement, ce sont simplement des informations brutes sans aucun contexte pour ce qu'elles signifient.

Définir les données observées

Définissez les données observées qui véhiculent des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Données observées**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Premier observé	Première fois où les données ont été vues.
Derniers observés	La dernière fois que les données ont été vues.
Nombre observé	Nombre de fois où chaque objet cyber-observable a été vu. La valeur doit être un nombre entier compris entre 1 et 999 999 999.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux données observées.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Observables associés	Répertorie les observables associés à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.

Acteurs de menace

Les auteurs de menace sont des personnes, des groupes ou des organisations qui agissent avec des intentions malveillantes. Les acteurs de la menace s'appliquent à STIX 2.x.

Un acteur de menace n'est pas un ensemble d'intrusion, mais peut soutenir ou être affilié à divers ensembles d'intrusion, groupes ou organisations au fil du temps.

Les acteurs de la menace utilisent leurs ressources, et les ressources d'un ensemble d'intrusions, pour mener des attaques et mener des campagnes contre des cibles.

Vous pouvez identifier les acteurs de menace par leurs motivations, leurs capacités, leurs objectifs, leur niveau de sophistication, leurs activités passées, les ressources auxquelles ils ont accès et leur rôle dans l'organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir les acteurs de menace

Définissez les acteurs de menace qui sont des individus, des groupes ou des organisations qui agissent avec des intentions malveillantes.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Acteurs de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom pour identifier l'instance ou la famille de programme malveillant, tel que spécifié par le créateur du SDO. Pour une famille de logiciels malveillants, le nom doit être défini.
Premier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour la dernière fois en train d'effectuer des activités malveillantes.
Motivation principale	La raison, la motivation ou le but principal derrière cet acteur de menace. La motivation est la raison pour laquelle l'acteur de la menace veut atteindre l'objectif (ce qu'il essaie d'atteindre). Par exemple, un acteur malveillant visant à perturber le secteur financier d'un pays peut être motivé par une haine idéologique du capitalisme.
Niveau de ressource	Niveau organisationnel auquel cet acteur de menace travaille généralement, qui détermine à son tour les ressources dont il dispose pour une attaque.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'auteur de la menace, y compris potentiellement son objectif et ses principales caractéristiques.
Alias	Une liste d'autres noms pour identifier cet acteur de menace.
Objectifs	Les objectifs de haut niveau de cet acteur de la menace, à savoir ce qu'il essaie de faire. Par exemple, ils peuvent être motivés par un gain personnel, mais leur objectif est de voler des numéros de carte de crédit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'auteur de la menace.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Rôles associés	Répertorie les rôles associés à l'acteur de menace.
Motivations de l'attaque connexe	Répertorie les motivations d'attaque associées à l'auteur de la menace.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Regroupements des menaces

Un objet Regroupement des menaces affirme explicitement que les objets STIX référencés ont un contexte commun. Le regroupement des menaces s'applique à STIX 2.x.

Un objet Regroupement des menaces représente un ensemble de données qui, avec une analyse suffisante, arrive à maturité pour transmettre un rapport d'incident ou de menace en tant qu'objet de rapport STIX. Par exemple, un regroupement peut être utilisé pour caractériser une enquête en cours sur un événement ou un incident de sécurité.

Un objet Regroupement des menaces peut également être utilisé pour déclarer que les objets STIX référencés sont liés à un processus d'analyse en cours. Par exemple, un analyste des menaces peut collaborer avec d'autres membres de sa communauté de confiance pour examiner une série de campagnes et d'indicateurs.

Le SDO Regroupement des menaces contient une liste de références aux SDO, aux SCO et aux OAR, ainsi qu'une déclaration explicite du contexte partagé par le contenu, une description textuelle et le nom du regroupement.

Définir les regroupements des menaces

Définissez les regroupements de menaces comme des objets qui ont un contexte commun.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Regroupements des menaces**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom pour identifier le regroupement de menaces.
Contexte	Description du contexte particulier partagé par le contenu référencé par le regroupement.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Description brève qui fournit des détails et le contexte du regroupement. Cela inclut son objectif et ses principales caractéristiques.
ID source	Identificateur unique de cet objet dans la source de menace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au regroupement de menaces.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Objets groupés	Répertorie les objets regroupés dans le cadre du regroupement de menaces.
Indicateurs groupés	Répertorie les indicateurs regroupés dans le cadre du regroupement de menaces.
Observables groupés	Répertorie les observables regroupés dans le cadre du regroupement de menaces.

Définitions de marquage

L'objet des définitions de marquage représente un marquage spécifique.

Les marquages de données représentent des restrictions, des autorisations et d'autres conseils sur la façon dont les données peuvent être utilisées et partagées.

Par exemple, les données peuvent être partagées avec la restriction qu'elles ne doivent pas être repartagées ou qu'elles doivent être cryptées au repos.

Dans STIX, les marquages de données sont spécifiés à l'aide de l'objet de définition de marquage. Ces définitions sont appliquées aux objets STIX à l'aide de marquages d'objets et aux propriétés individuelles des objets STIX via des marquages granulaires.

Définir des définitions de marquage

Définissez des définitions de marquage qui représentent un marquage de données spécifique.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Définitions de marquage**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Définition	Spécifiez l'objet de marquage (par exemple, TLP) ou une autre définition de marquage qui a été définie.
Type de définition	Identifie le type de définition de marquage - instruction ou TLP (Traffic Light Protocol).
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la définition de marquage.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Objets marqués	Listes des objets marqués avec la définition de marquage.
Indicateurs marqués	Listes des indicateurs marqués avec la définition de marquage.

Notes de menace

Une note sur les menaces transmet un texte informatif pour fournir une analyse supplémentaire qui n'est pas contenue dans les objets STIX, les objets de définition de marquage ou les objets de contenu linguistique auxquels la note se rapporte. Les notes de menace s'appliquent à STIX 2.x.

Par exemple, un analyste peut ajouter une note à un objet Campagne créé par une autre organisation. La note peut indiquer qu'ils ont vu des messages liés à cette campagne sur un forum de pirates.

Les notes sont généralement créées par des analystes humains et sont composées de texte orienté vers l'homme, elles contiennent une propriété supplémentaire pour capturer l'auteur qui a créé la note.

Définir les notes de menace

Définissez des notes sur les menaces qui transmettent des informations pour fournir un contexte ou une analyse supplémentaire qui n'est pas disponible dans les objets existants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Notes de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Abstrait	Spécifiez un bref résumé du contenu de la note.
Contenu	Spécifie le contenu de la note.
Auteurs	Spécifie le nom de l'auteur (par exemple, un analyste).
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite
Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux notes de menace.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Objets associés	Listes d'objets auxquels s'appliquent les notes sur les menaces.
Indicateurs associés	Listes d'indicateurs auxquels s'appliquent les notes sur les menaces.
Observables associés	Répertorie les observables associés à cet objet.

Opinions sur la menace

Un avis est une évaluation de l'exactitude des informations contenues dans un objet STIX produit par une entité différente. Les opinions sur la menace s'appliquent à STIX 2.x.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La propriété opinion capture le niveau d'accord ou de désaccord à l'aide d'une échelle fixe. L'échelle fixe prend également en charge une cartographie numérique pour permettre des opérations statistiques cohérentes entre les opinions.

Par exemple, un analyste d'une organisation consommatrice peut dire qu'il est « fortement en désaccord » avec un objet de campagne et expliquer pourquoi.

Les opinions sont subjectives et le cahier des charges n'aborde pas la meilleure façon de les interpréter.

Les analystes humains créent des opinions et sont composés de texte orienté vers l'homme, ils contiennent une propriété supplémentaire pour capturer l'auteur qui a créé l'opinion.

Définir les opinions sur la menace

Définissez les opinions sur une menace comme une évaluation de l'exactitude des informations contenues dans un objet STIX.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Opinions sur la menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Avis	L'avis du producteur sur l'objet STIX.
Explication	L'explication du producteur sur l'opinion.
Auteurs	Spécifie le nom de l'auteur (par exemple, un analyste).
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'opinion sur les menaces.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Objets associés	Liste des objets auxquels l'avis de menace s'applique.
Indicateurs associés	Liste des indicateurs auxquels l'avis sur la menace s'applique.
Observables associés	Répertorie les observables associés à cet objet.

Rapports de menace

Les rapports de menace sont des collections de renseignements sur les menaces axés sur une ou plusieurs rubriques. Les rapports de menace s'appliquent à STIX 2.x.

Les rapports de menace comprennent une description d'un auteur de menace, d'un programme malveillant, d'une technique d'attaque, y compris le contexte et des détails connexes. Ils sont utilisés pour regrouper les renseignements sur les menaces liés afin qu'ils puissent être publiés sous forme d'article complet sur les cybermenaces.

Le SDO Rapport de menace contient une liste de références aux objets STIX ainsi qu'une description textuelle et le nom du rapport.

Définir les rapports de menace

Définissez les rapports de menace décrivant un auteur de menace, un programme malveillant ou une technique d'attaque, y compris le contexte et les détails connexes.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Rapports de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Spécifiez un nom pour identifier le rapport de menace.
Publié	Date à laquelle ce rapport a été officiellement publié par l'auteur du rapport.
Description	Une description qui fournit des informations et un contexte supplémentaires sur le rapport.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identificateur unique de cet objet dans la source de menace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux rapports de menaces.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Objets signalés	Liste des objets signalés dans le rapport de menace.
Indicateurs signalés	Listes des indicateurs signalés dans le rapport de menace.
Observables rapportés	Listes des observables signalés dans le rapport de menace.

Perceptions

Les perceptions indiquent qu'un indicateur ou un objet a été vu. Les objets peuvent être un logiciel malveillant, un outil, un acteur de menace, etc.

Les observations permettent de suivre qui et quelle est la cible, comment les attaques sont menées et de suivre les tendances du comportement d'attaque.

L'objet de relation Perception contient des propriétés supplémentaires qui ne sont pas présentes dans les objets de relation génériques. Ces propriétés supplémentaires représentent des données spécifiques aux relations de perception.

Par exemple, un décompte ou représentant le nombre de fois où quelque chose a été vu.

La perception est capturée en tant que relation car vous ne pouvez pas avoir une observation à moins d'avoir quelque chose qui a été vu.

- Ce qui a été vu, comme le programme malveillant, la campagne ou un autre SDO
- Qui l'a aperçu et/ou où il a été aperçu, représenté comme une identité
- Ce qui a été vu sur les systèmes et les réseaux, représenté par des données observées

Définir les perceptions d'indicateur

Définissez les perceptions qui indiquent qu'un indicateur a été vu.

Avant de commencer

Rôle requis : sn_ti.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Perceptions d'indicateurs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Indicateur	Identifie l'indicateur. Recherchez et sélectionnez l'indicateur.
Nombre	Nombre de fois que l'objet a été vu.
Premier observé	Heure à laquelle cet objet a été vu pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cet objet a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur la perception de l'indicateur, y compris potentiellement son objectif et ses principales caractéristiques.
ID source	Identificateur unique de cet objet dans la source de menace.
Est une synthèse	
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la perception de l'indicateur.

Listes connexes	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Identités	Liste des identités associées à cet objet.
Données observées	Répertorie les données observées associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir les perceptions d'objets

Définissez la perception d'objets qui indique qu'un objet (programme malveillant, outil, acteur malveillant, entre autres) a été vu.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Détections d'objets**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Objet	Identifie l'objet. Recherchez et sélectionnez l'objet.
Nombre	Nombre de fois que l'objet a été vu.
Premier observé	Heure à laquelle cet objet a été vu pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cet objet a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'observation de l'objet, y compris potentiellement son objectif et ses principales caractéristiques.
ID source	Identificateur unique de cet objet dans la source de menace.
Est une synthèse	
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'observation d'objets.

Listes connexes	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Identités	Liste des identités associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes connexes	Description
Données observées	Répertorie les données observées associées à cet objet.

Outils

Les outils sont des logiciels légitimes utilisés par les acteurs de la menace pour effectuer des attaques. Les outils s'appliquent à STIX 2.x.

Les outils vous permettent de savoir comment et quand les acteurs de la menace les utilisent pour exécuter des campagnes. Contrairement aux logiciels malveillants, ces outils ou progiciels se trouvent souvent sur un système et ont des objectifs légitimes pour les utilisateurs avancés, les administrateurs, les administrateurs réseau ou même les utilisateurs normaux.

Par exemple, les outils d'accès à distance (RDP) et les outils d'analyse réseau (Nmap) sont des outils qu'un acteur malveillant utilise lors d'une attaque.

Définir des outils

Définissez les outils comme des logiciels légitimes utilisés pour effectuer des attaques.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Outils**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Entrez un nom descriptif pour identifier l'outil.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur l'outil, y compris potentiellement son objectif et ses principales caractéristiques.
Alias	Noms alternatifs pour identifier cet outil.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'objet d'outil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Phases de kill chain associées	Répertorie les phases de kill chain associées à cet objet.
Types associés	Répertorie les types d'indicateurs associés à cet objet.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Déroulement des actions	Répertorie le plan d'actions associé à cet objet qui sont des réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu) pour prévenir une attaque.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.

Vulnérabilités

Une vulnérabilité est une faiblesse ou un défaut d'un composant logiciel ou matériel exploité par des attaquants. Les vulnérabilités s'appliquent à STIX 2.x.

La faiblesse ou le défaut réside dans les exigences, les conceptions ou les implémentations du code trouvé dans un composant logiciel ou matériel. Cette faiblesse est directement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

exploitée pour avoir un impact négatif sur la confidentialité, l'intégrité ou la disponibilité de ce système.

CVE est une liste des vulnérabilités et des expositions en matière de sécurité de l'information qui fournit des noms communs pour les problèmes connus du public [CVE].

Par exemple, si un logiciel malveillant exploite CVE-2015-12345, un objet malveillant peut être lié à un objet de vulnérabilité faisant référence à CVE-2015-12345.

Définir les vulnérabilités

Définissez une vulnérabilité comme une faiblesse ou un défaut d'un composant logiciel ou matériel exploité par des attaquants.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Vulnérabilités**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Nom	Saisissez un nom descriptif pour identifier la vulnérabilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Description	Une description qui fournit plus de détails et de contexte sur la vulnérabilité, y compris potentiellement son objectif et ses principales caractéristiques.
Alias	Noms alternatifs pour identifier cet outil.
ID source	Identificateur unique de cet objet dans la source de menace.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

4. Cliquez sur **Envoyer**.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'objet de vulnérabilité.

Liens connexes et listes connexes	Description
Afficher toutes les relations	Ouvre le visualiseur STIX dans lequel vous pouvez afficher la relation de l'objet STIX. L'option Afficher les relations n'apparaît que lorsque l'objet est associé à un objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liens connexes et listes connexes	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Déroulement des actions	Répertorie le plan d'actions associé à cet objet qui sont des réponses techniques ou automatisées (application de correctifs, reconfiguration des pare-feu) pour prévenir une attaque.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Relations

Utilisez les objets de relation pour relier deux SDO ou objets cyber-observables (SCO) STIX afin de décrire leur relation l'un avec l'autre.

Les objets de relation STIX (SRO) représentent des types de relations entre divers objets STIX. Les objets de relation suivants sont disponibles :

- **Relation objet-objet** : cet objet définit les relations entre les SDO, à l'exception de l'objet indicateur. Un exemple de relation définie objet-objet est qu'un modèle d'attaque livre un logiciel malveillant.
- **Relation objet-indicateur** : cet objet définit les relations entre l'objet indicateur et d'autres SDO. Un exemple de relation définie objet-indicateur est qu'un indicateur détecte la preuve d'une campagne.
- **Relation objet-observable** : cet objet définit les relations entre les SDO et l'objet observable (SCO). Un exemple de relation définie objet-observable est qu'une infrastructure se compose d'objets cyber-observables qui fournissent des informations sur une attaque potentielle.

Relations d'objets STIX

Objet de relation	Exemple de source	Exemple de cible	Exemple de description
Relations objet-objet	Modèle d'attaque	Programme malveillant	Cette relation décrit que ce modèle d'attaque est

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Relations d'objets STIX (suite)

Objet de relation	Exemple de source	Exemple de cible	Exemple de description
			utilisé pour livrer cette instance (ou famille) de programme malveillant.
Relations objet-indicateur	Indicateur	Modèle d'attaque, Campagne, Infrastructure, Ensemble d'intrusion, Programme malveillant, Acteur de menace, Outil	Cette relation décrit que l'indicateur peut détecter des preuves du modèle d'attaque, de la campagne, de l'infrastructure, de l'ensemble d'intrusion, du programme malveillant, de l'acteur de menace ou de l'outil associés. Les preuves peuvent ne pas être directes. Par exemple, l'indicateur peut détecter des preuves secondaires de la campagne, telles que des logiciels malveillants couramment utilisés par cette campagne particulière.
Relations objet-observable	Infrastructure	Données observées	Cette relation indique que l'indicateur est créé en fonction des informations provenant d'un objet de données observé. Un exemple de relation définie objet-observable est qu'une infrastructure se compose d'objets cyber-observables qui fournissent des informations sur une attaque potentielle.

Traduction automatique

Définir les relations objet-objet

Définissez les relations entre les SDO, à l'exception de l'objet d'indicateur.

Avant de commencer

Rôle requis : sn_ti.admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Relations objet-objet**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Objet source	Sélectionnez et définissez l'objet source.
Type de l'objet source	Définit le type d'objet source.
Objet cible	Sélectionnez et définissez l'objet cible.
Type de l'objet cible	Définit le type d'objet cible.
Type de relation	Description qui fournit plus de détails et de contexte sur le type de relation.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identifie de manière unique l'objet source.

4. Cliquez sur **Envoyer**.

Définir les relations objet-indicateur

Définissez les relations entre l'objet d'indicateur et d'autres SDO.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Objet-Indicateur-Relations**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Objet	Sélectionnez et définissez l'objet.
Type	Spécifie le type d'objet en fonction de l'objet que vous avez sélectionné.
Indicateur	Sélectionnez les indicateurs de compromission.
Sens de la relation	Définissez le sens de la relation, qu'il soit direct ou inverse.
Type de relation	Description qui fournit plus de détails et de contexte sur le type de relation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identifie de manière unique l'objet source.

4. Cliquez sur **Envoyer**.

Définir les relations objet-observable

Définissez les relations entre les SDO et l'objet observable (SCO).

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel IoC** > **Relations objet-observable-objet**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Objet	Sélectionnez et définissez l'objet source.
Type	Entrez un nom descriptif pour identifier le type d'objet.
Observable	Sélectionnez et définissez l'observable.
Type de relation	Description qui fournit plus de détails et de contexte sur le type de relation.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
ID source	Identifie de manière unique l'objet source.

4. Cliquez sur **Envoyer**.

Visualiseur STIX

Le visualiseur STIX représente visuellement la structure de l'objet STIX et sa relation.

Vous pouvez obtenir plus d'informations sur l'objet ou la relation sélectionné dans le volet de détails.

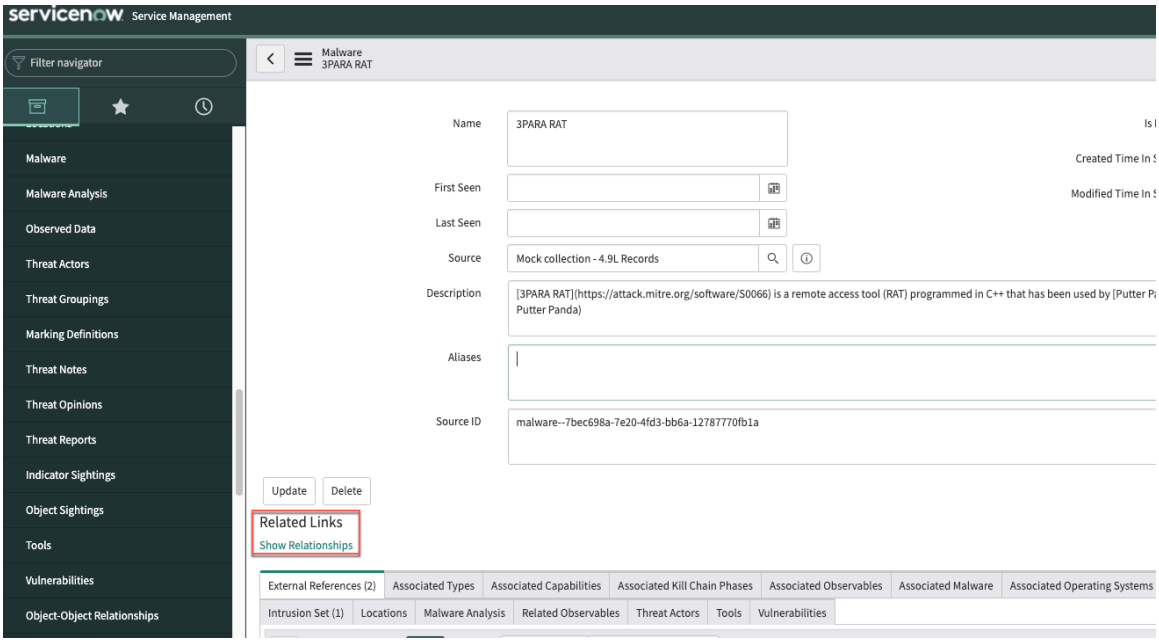
Le graphique des relations affiche les relations d'un objet et fournit un contexte que vous pouvez étudier. Vous pouvez cliquer sur n'importe quel nœud du graphique pour afficher plus de détails.

Remarque : Le visualiseur STIX est disponible pour tous les SDO, à l'exception des objets Rapport et Données observées.

Traduction automatique

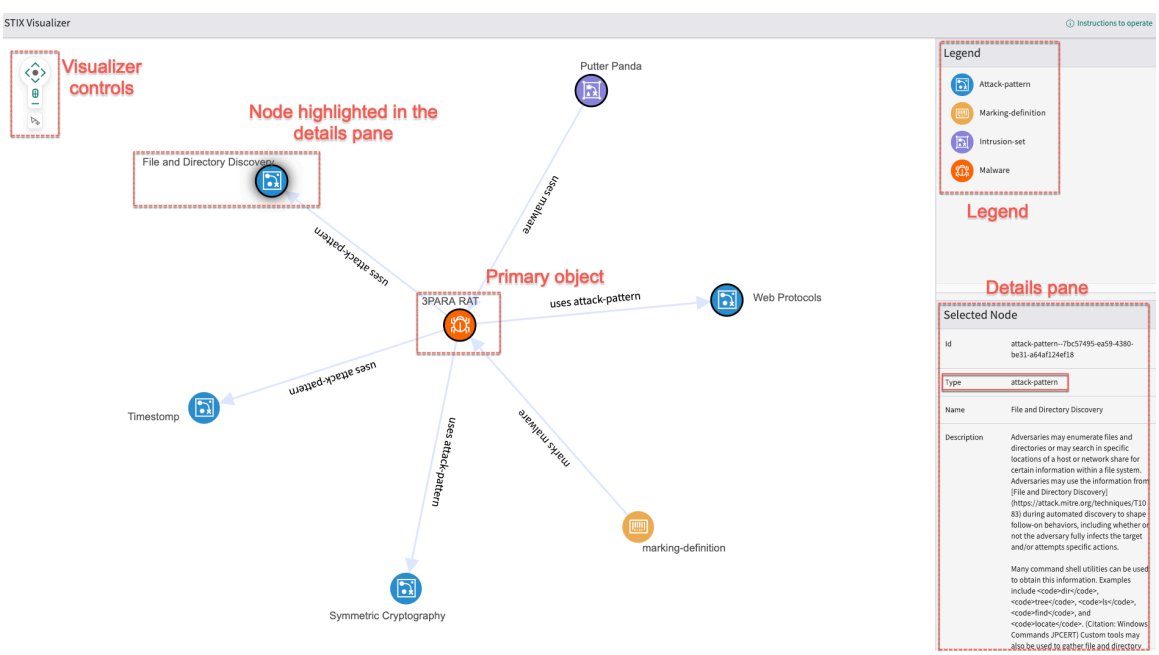
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accéder au visualiseur STIX



Cliquez sur Afficher les relations dans la section Liens connexes de l'un des SDO pour afficher le visualiseur STIX.

Afficher les détails dans STIX Visualizer



Dans le visualiseur, vous pouvez visualiser l'objet et sa relation, ce qui vous fournit un contexte pour une étude plus approfondie. Le visualiseur utilise des couleurs et des icônes pour illustrer diverses informations sur les objets.

Vous pouvez effectuer un zoom avant sur un objet, faire glisser les nœuds ou les épingler pour vous concentrer sur une relation particulière.

Cliquez sur n'importe quel objet pour ouvrir le volet de détails. Dans le volet de détails, vous pouvez obtenir plus d'informations associées à l'objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MITRE-ATT&CK™ Vue d'ensemble du cadre de travail

Le MITRE-ATT&CK cadre de travail est une base de connaissances des tactiques, des techniques et des procédures courantes (TTP) auxquelles votre organisation peut accéder pour développer des modèles de menaces et des méthodologies spécifiques contre les cyberattaques.

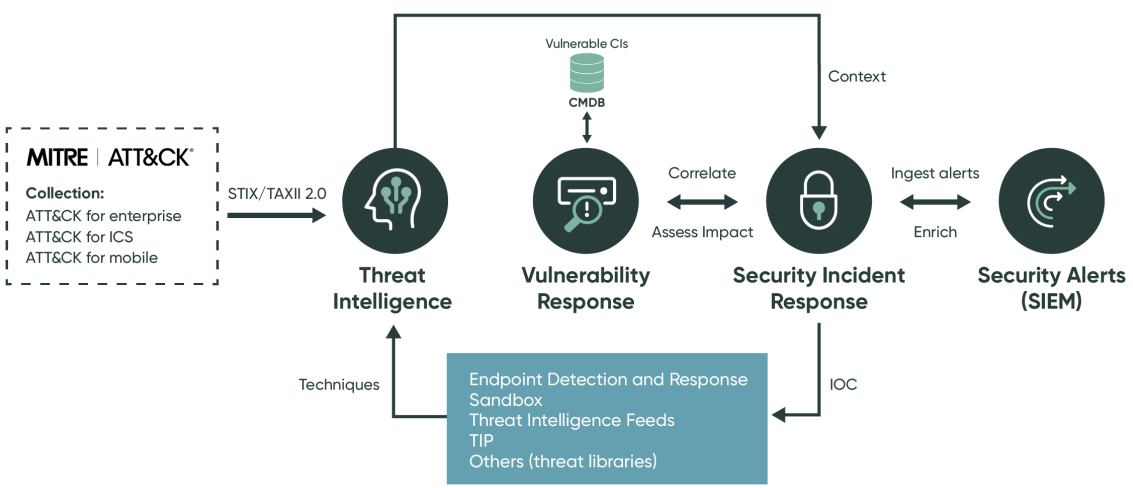
Vue d'ensemble

Le MITRE cadre de travail Tactiques, techniques et connaissances de base des adversaires (ATT&CK) documente et suit les différentes techniques des adversaires qui sont utilisées pendant les différentes étapes d'une cyberattaque.

En utilisant la base de connaissances du MITRE-ATT&CK framework, la communauté des renseignements sur les cybermenaces peut rapidement identifier les menaces et coordonner les réponses aux cyberattaques.

MITRE-ATT&CK et Opérations de sécurité

Consultez le diagramme suivant pour découvrir comment les informations circulent avec Opérations de sécurité les MITRE-ATT&CK applications.



- Le champ préchargé TAXII client se connecte au TAXII serveur pour ingérer les collections de données dans .Renseignements sur les menaces
- Les intégrations SIEM (Security Information and Event Manager) existantes ingèrent leurs données sur les menaces (alertes et événements), avec les TTP pertinents, et sont associées aux incidents de sécurité.
- Lorsqu'un IoC est associé à un incident de sécurité, Renseignements sur les menaces recherche automatiquement des informations pertinentes dans les flux de menaces et envoie les IoC à des sources tierces telles que EDR, Sandbox ou TIP pour une analyse supplémentaire.
- Si une source tierce contient l'information MITRE-ATT&CK , alors Renseignements sur les menaces Extrait les informations sur la technique et enrichit les données du référentiel à des Renseignements sur les menaces fins de corrélation et d'analyse.
- MITRE-ATT&CK partage également des informations de contexte CVE pour chaque technique. Votre équipe de sécurité peut examiner les techniques exploitées pour Réponse aux vulnérabilités déterminer si vos actifs critiques sont menacés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MITRE-ATT&CK Matrices, tactiques et techniques

Le cœur du MITRE-ATT&CK cadre est une matrice de tactiques et de techniques de l'adversaire. La séquence des tactiques représente ce qu'un adversaire essaie d'accomplir au stade d'un incident. Lorsque votre équipe de sécurité comprend cette séquence, vous avez la possibilité d'anticiper le prochain mouvement d'un adversaire et de briser la chaîne de frappe. ATT&CK se compose des matrices suivantes :

- ATT&CK d'entreprise : décrit les comportements et les actions qu'un adversaire entreprend pour compromettre et opérer dans un réseau et un cloud d'entreprise.

  Remarque : La matrice pré-ATT&CK a été déconseillée et a été fusionnée avec MITRE la matrice Enterprise.

- ICS ATT&CK : décrit les actions qu'un adversaire entreprend lorsqu'il opère au sein d'un réseau de systèmes de contrôle industriel (ICS).
- ATT&CK mobile : décrit les comportements et les actions des adversaires qui se concentrent sur les appareils mobiles.

La tactique représente le pourquoi d'une technique ATT&CK. C'est l'objectif tactique de l'adversaire pour effectuer une action.

Les techniques représentent la façon dont un adversaire atteint un objectif tactique en effectuant une action.

Les techniques peuvent être associées à plus d'une tactique. Par exemple, la manipulation des jetons d'accès est utilisée par un adversaire pour réaliser la tactique de l'élévation des privilèges ou de l'évasion de la défense.

Utilisation d'une approche basée sur l'intention pour les réponses aux incidents

Une réponse basée sur l'intention utilise un cadre de travail de chaîne de frappe dynamique et contextuelle qui peut aider votre organisation à corréler les incidents de sécurité et à identifier un large éventail d'attaques. Votre équipe de sécurité peut utiliser une réponse basée sur l'intention pour comprendre comment l'organisation est attaquée et ce que l'attaquant pourrait faire ensuite. Ce type de réponse vous permet de prédire le comportement d'un attaquant afin de concentrer efficacement vos ressources.

Grâce à Réponse aux incidents de sécurité, votre équipe de sécurité peut gérer le cycle de vie de chaque incident de sécurité, de l'analyse au confinement, en se concentrant sur les indicateurs de compromission (IOC) tels que les adresses IP, les hachages de fichiers et les domaines.

En s'intégrant Réponse aux incidents de sécurité au cadre de travail, les incidents de sécurité sont traités comme des liens dans une attaque plus large à l'échelle de l'entreprise MITRE-ATT&CK .

Les avantages dont votre organisation peut bénéficier MITRE-ATT&CK dans Security Operations



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'utilisation du cadre de MITRE-ATT&CK travail peut aider votre organisation à effectuer les opérations suivantes :

- Équipez les analystes de sécurité de MITRE-ATT&CK tactiques, de techniques et de procédures (TTP) pour mieux analyser les incidents de sécurité et y répondre.
- Automatisez les workflows d'incidents à l'aide du playbook pour détecter et contenir les MITRE-ATT&CK menaces dans le contexte du cadre de travail.
- Classer par ordre de priorité les indicateurs de compromission et la chasse aux menaces avec MITRE-ATT&CK des informations.
- Comprenez la posture de sécurité de haut niveau de votre organisation dans le contexte du cadre de MITRE-ATT&CK travail.

Administration MITRE-ATT&CK

Vous pouvez configurer, mapper des sources de données, mapper la couverture globale de détection de techniques et gérer le MITRE-ATT&CK référentiel dans le ServiceNow AI Platform.

Introduction au cadre de MITRE-ATT&CK travail

Examinez les informations suivantes avant de commencer à configurer votre MITRE-ATT&CK cadre de travail.

Liste de vérification

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles de ServiceNow AI Platform et Renseignements sur les menacesRéponse aux incidents de sécurité requis.	Les rôles suivants sont utilisés dans les MITRE-ATT&CK fonctionnalités : • L'administrateur (admin) installe les applications à partir de et affecte les rôles d'administrateur d'incident de sécurité (sn_si.admin) et d'administrateur ServiceNow Store de Renseignements sur les menaces (sn_ti.admin). • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.lire • sn_ti.write • sn_ti.mitre_analyst : le rôle d'analyste MITRE a été introduit pour permettre la navigation croisée pour les fonctionnalités entre Réponse aux incidents de sécurité et Support commun des renseignements sur les MITRE menaces. Avec ce rôle, vous pouvez afficher à la fois le Renseignements sur les menaces MITRE module et le Réponse aux incidents de sécurité module en mode lecture seule. • sn_si.read

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	Pour plus d'informations, consultez Configurer Threat Intelligence.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge le MITRE-ATT&CK module sont installées et activées.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. • Composants d'interface utilisateur courants (sn_ti_seismic) de Prise en charge de Threat Intelligence - Version 1.0 ou supérieure • Prise en charge de Threat Intelligence commun - Version 12.0 ou supérieure • Renseignements sur les menaces - Version 12.0 ou supérieure • Réponse aux incidents de sécurité - Version 12.0 ou supérieure Pour plus d'informations sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez obtenir une autorisation pour un produit ou une application Security Operations et activer une application ServiceNow Store.
Séparation de domaine	Vérifiez la section Séparation de domaine si vous avez l'intention de séparer les données, les processus et les tâches administratives.

Comprendre le modèle de MITRE données de destination STIX

Examiner la terminologie utilisée par MITRE le STIXMITRE-ATT&CK™ cadre de travail dans le ServiceNow AI Platform.

MITRE objets à STIX mapper

STIX est un langage permettant de décrire les informations sur les cybermenaces de manière normalisée et structurée. Les modèles de données parents du Renseignements sur les menaces module sont les STIX objets. Alors que les MITRE objets sont un sous-ensemble du modèle de données parent STIX . Dans le MITRE-ATT&CK cadre, MITRE fournit des informations similaires STIX avec certaines étiquettes et certains objets.

MITRE vers le mappage d'objets STIX

Terminologie de MITRE	Terminologie de STIX
Technique	Modèle d'attaque

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MITRE vers le mappage d'objets STIX (suite)

Terminologie de MITRE	Terminologie de STIX
Atténuation	Déroulement de l'action
Groupes	Ensembles d'intrusion
Programme malveillant	Programme malveillant
Outil	Outil

Extension des données dans le Renseignements sur les menaces module

Vous pouvez gérer une liste des sources de Renseignements sur les menaces menaces et importer les données nécessaires STIX , y compris un ensemble complet d'informations sur les cybermenaces. Vous pouvez également utiliser les profils pour faciliter l'échange automatisé d'informations sur les TAXII cybermenaces.

Remarque : Pour plus d'informations, consultez Définir une source de menace et créer un profil TAXII.

Extension des données dans le MITRE-ATT&CK module

Vous pouvez étendre les objets Malware, Group, Mitigation et Tool à une technique du MITRE-ATT&CK référentiel.

Vous pouvez créer un objet et établir une relation entre une technique et le nouvel objet dans le module Référentiel MITRE ATT&CK, mais vous ne pouvez pas définir le type de relation dans ce module. Pour définir un type de relation, accédez au **Renseignements sur les menaces** > **Référentiel IoC** > **Relations objet-objet** module.

Si vous mappez le type de relation entre une technique existante et un objet existant, vous devez définir la technique comme objet cible et l'objet comme objet source. Pour ce faire, accédez au **Référentiel IoC** > **Relations objet-objet** module.

Vous pouvez créer un groupe et l'associer à un modèle d'attaque, mais dans le référentiel MITRE ATT&CK, vous ne pouvez établir que la relation entre le groupe et le modèle d'attaque. Pour définir le type de relation objet-objet, vous devez le faire dans le référentiel IoC.

Remarque : Pour plus d'informations, consultez étendre MITRE-ATT&CK données et le référentiel IoC.

Séparation de domaine et MITRE-ATT&CK

Cette vue d'ensemble de Séparation de domaine se rapporte à MITRE-ATT&CK. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Prise en charge : Basique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment fonctionne Séparation de domaine avec MITRE-ATT&CK

Pour procéder à la séparation en domaines, procédez comme suit :

- Créez un utilisateur avec les rôles sn_ti.admin requis dans le domaine respectif.
- Répliquez ce qui suit pour chaque domaine :
  - TAXII Collectes

    Remarque :

    - N'activez pas les collections dans le domaine global. Activez uniquement les collections qui sont répliquées et disponibles dans votre domaine.
    - Modifiez le champ **Exécuter en tant que** dans les collections pour l'utilisateur ayant le rôle sn_ti.admin dans le domaine respectif.
  - Définition de la couverture de la technique
  - Règle d'extraction de la technique
  - Règles de détection : Mappages MITRE ATT&CK
  - Couverture de l'atténuation
    - Copiez tous les enregistrements de définition de couverture d'atténuation.
    - Copiez le calculateur de couverture d'atténuation ou créez un nouveau calculateur pour le domaine respectif.
  - Groupe de menaces : définitions de cartes thermiques de techniques

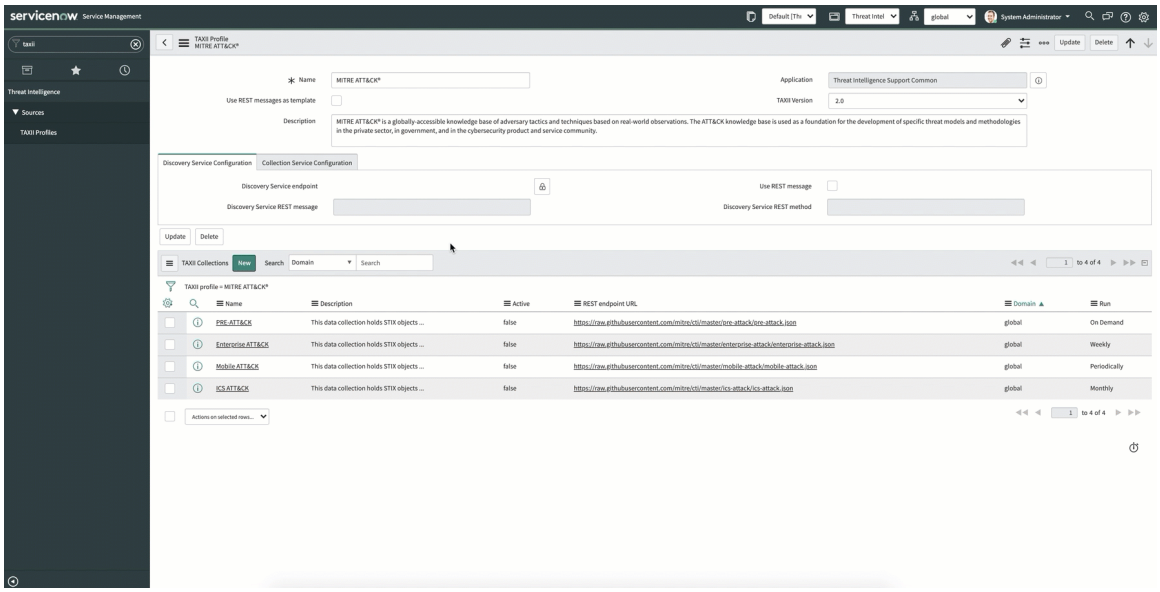
Répliquer la collection TAXII

1. Accédez à la **Renseignements sur les menaces** > **Sources** > **Profils TAXII**.
2. Dans la barre d'en-tête, utilisez le sélecteur de domaine pour sélectionner votre domaine.
3. Sélectionnez la collection TAXII pertinente pour votre organisation (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).
4. Cliquez avec le bouton droit dans la barre d'en-tête et sélectionnez **Insérer et rester**. La collection TAXII en double est créée sous le domaine sélectionné
5. Revenez au profil MITRE ATT&CK TAXII pour afficher la collection TAXII en double.

L'illustration suivante montre comment sélectionner le domaine TOP/Initech, répliquer la collection TAXII dans le domaine et vérifier la collection TAXII répliquée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Configurer le cadre de MITRE-ATT&CK™ travail

Activez le MITRE-ATT&CK profil et configurez une tâche planifiée afin de pouvoir configurer MITRE-ATT&CK des collections pour la détection des menaces dans votre organisation.

Avant de commencer

Rôle requis : sn_ti.admin

Pourquoi et quand exécuter cette tâche

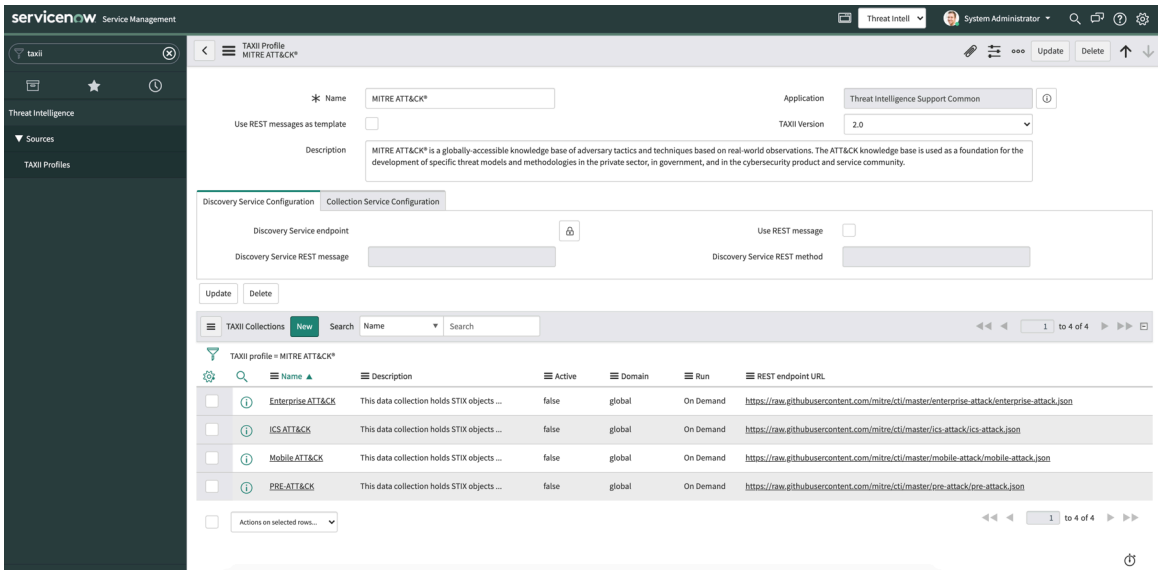
L'expression d'informations structurées sur les menaces (STIX™ en) est un langage permettant de décrire les informations sur les cybermenaces de manière normalisée et structurée. À l'aide des données STIX et de l'échange automatisé fiable d'informations d'indicateur (TAXII™), les équipes de sécurité peuvent utiliser les informations partagées sur les cybermenaces pour isoler les menaces précédemment identifiées par votre entreprise et provenant d'autres sources.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Sources** > **Profils TAXII**.
   Vous voyez les profils disponibles TAXII .
2. Cliquez sur le profil **MITRE ATT&CK** fourni avec le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour activer la TAXII collection, définissez l'option **Actif** sur vrai pour la TAXII collection pertinente pour votre organisation (Enterprise ATT&CK, Mobile ATT&CK ou ICS ATT&CK).

Collecte TAXII	Description
ATT&CK d'entreprise	Décrit les comportements et les actions qu'un adversaire entreprend pour faire des compromis et opérer dans un réseau d'entreprise et dans le cloud. **Remarque :** La matrice pré-ATT&CK a été déconseillée et a été fusionnée avec MITRE la matrice Enterprise.
ATT&CK mobile	Décrit les comportements et les actions de l'adversaire qui se concentrent sur les équipements mobiles.
ICS ATT&CK	Décrit les actions qu'un adversaire entreprend lorsqu'il opère au sein d'un réseau de systèmes de contrôle industriel (ICS).

4. Pour actualiser périodiquement la collection, définissez l'option **Exécuter** en fonction de votre organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, cette option est définie sur Sur demande.

Remarque :

a. Les collections sont fournies dans le cadre du module d'extension Renseignements sur les menaces Core. L'installation ou la mise à jour de Threat Intelligence Support Common (version 12.0 ou supérieure) et de Threat Intelligence (version 12.0 ou supérieure) garantit que les données de vos collections sont remplies automatiquement.

b. Activez la TAXII collection uniquement pour la collection que vous avez l'intention d'utiliser dans votre organisation et désactivez les autres collections. Par exemple, si vous avez l'intention d'utiliser la matrice Enterprise ATT&CK, activez Enterprise ATT&CK au niveau de la TAXII collection et des matrices . Désactivez les autres matrices Mobile ATT&CK et ICS ATT&CK à la TAXII collection et au niveau des matrices.

c. Dans les TAXII listes connexes Collections, si vous sélectionnez l'option Exécuter sur Quotidien, une erreur se produit et l'option est définie par défaut sur Sur demande. Cette erreur se produit car la planification quotidienne de l'actualisation MITRE-ATT&CK des données est restreinte afin d'optimiser la charge sur les MITRE serveurs. De plus, il MITRE ne met à jour les données ATT&CK que deux fois par an.

d. Les TAXII collections ne sont pas actualisées à moins que vous n'activiez la TAXII collection.

e. Les mises à jour des collectes existantes peuvent être récupérées à partir du MITRE serveur en planifiant la fréquence « run » dans chaque collection.

f. Les personnalisations que vous apportez aux données du MITRE-ATT&CK référentiel (logiciels malveillants, groupes, atténuations et objets d'outil pour une technique) sont enregistrées lors des mises à jour planifiées.

g. MITRE Met à jour la MITRE-ATT&CK base de connaissances dans laquelle certains objets sont identifiés comme révoqués ou déconseillés, de nouveaux objets sont ajoutés ou des objets existants sont modifiés. En cas MITRE de révocation d'une tactique ou d'une technique, ces objets sont marqués comme révoqués dans le ServiceNow AI Platform fichier . Les objets révoqués sont conservés dans le référentiel mais ne peuvent pas être utilisés dans le ServiceNow AI Platform fichier .

Que faire ensuite

Une fois la configuration du profil TAXII terminée, les données du MITRE-ATT&CK référentiel sont importées à intervalles réguliers vers le ServiceNow AI Platform®. Vous pouvez voir ces données en accédant à **Référentiel MITRE ATT&CK** > **Matrices** et **Référentiel MITRE ATT&CK** > **Techniques**.

Gérer les matrices

Gérez les matrices qui ont été importées à partir des MITRE TAXII collections. Les matrices sont un ensemble de tactiques et de techniques. Vous pouvez afficher les matrices pour vérifier si vos collections sont disponibles dans le MITRE-ATT&CK référentiel.

Avant de commencer

Remarque : Vérifiez que seule la matrice que vous avez l'intention d'utiliser dans votre organisation est activée et désactivez les autres matrices. Par exemple, si vous avez l'intention d'utiliser la matrice Enterprise ATT&CK, celle-ci est activée au niveau de la collection TAXII et des matrices. Désactivez les autres matrices Mobile ATT&CK et ICS ATT&CK à la TAXII collection et au niveau des matrices.

Rôle requis :

Traduction automatique

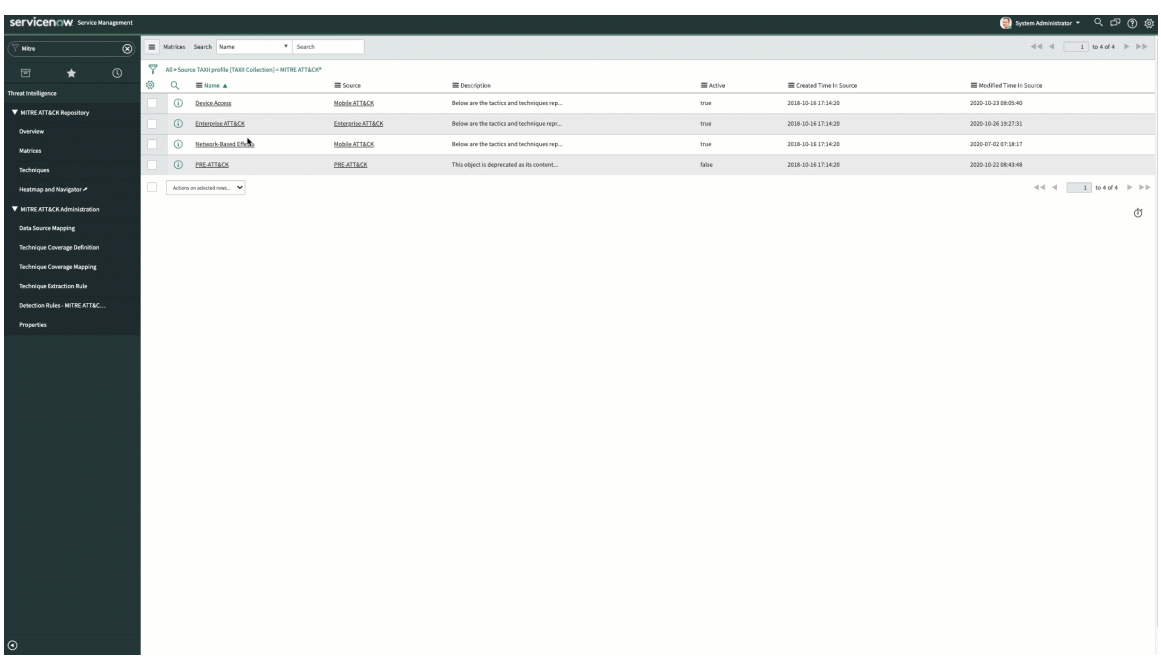
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_ti.admin : supprimer l’accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Matrices**.
   Toutes les matrices sont désactivées par défaut.
2. Pour activer une matrice, pointez sur **Actif**, double-cliquez et sélectionnez **vrai**.
3. Pour afficher toutes les informations associées, cliquez sur une matrice.
4. Pour afficher toutes les tactiques associées à cette collection, cliquez sur l’onglet **Tactiques MITRE** .
5. Pour afficher des détails supplémentaires et les techniques associées à une tactique sélectionnée, cliquez sur une tactique.
6. Sous l’onglet **Techniques MITRE ATT&CK** , sélectionnez une technique.
7. Dans les listes connexes, affichez les associations disponibles pour la technique que vous avez sélectionnée.

   Dans l’illustration suivante, vous pouvez voir le chemin de navigation depuis la matrice Enterprise ATT&CK vers la tactique d’accès initial (TA0001), puis vers la technique d’hameçonnage (T1566). Sur la page Modèle d’attaque - Technique d’hameçonnage, vous pouvez afficher la liste connexe : tactique, sous-technique, groupe, atténuation, références externes, programme malveillant et outils.



Que faire ensuite

Vous pouvez étendre les informations de certains de ces objets de liste connexes en fonction de la technique que vous avez sélectionnée. Par exemple, vous pouvez ajouter de nouvelles informations pour Groupe, Atténuation, Références externes, Programmes malveillants et Outils.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer les techniques

Gérez les techniques importées des MITRE TAXII collections. Les techniques contiennent différentes façons dont les attaquants se sont développés pour utiliser une tactique donnée. Vous pouvez examiner et désactiver les techniques qui ne sont pas pertinentes pour votre organisation. En STIX, les techniques sont connues sous le nom de schémas d'attaque.

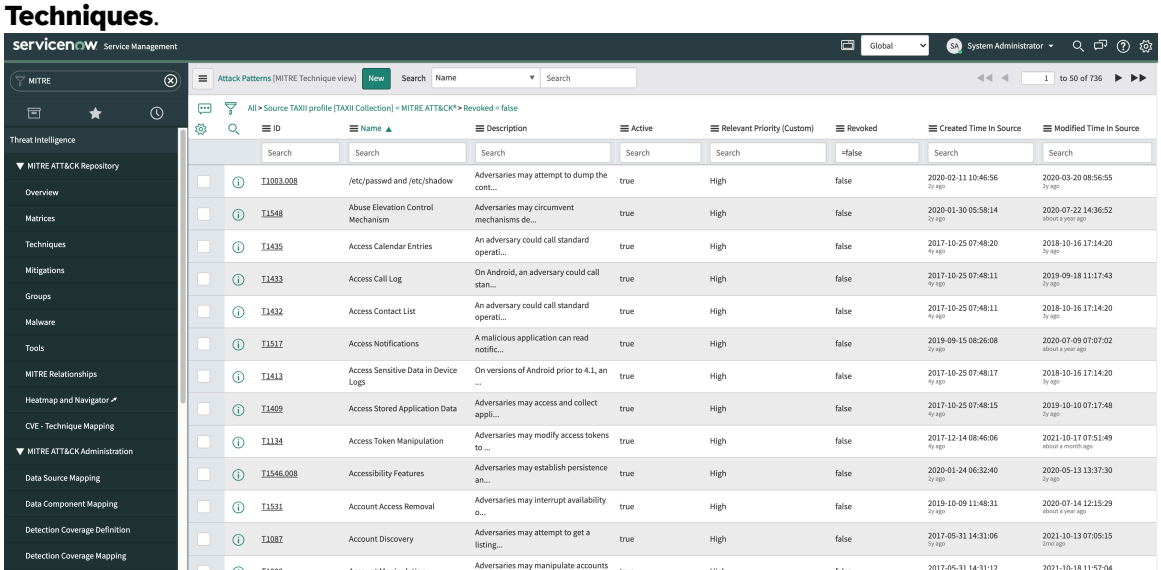
Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Techniques**.



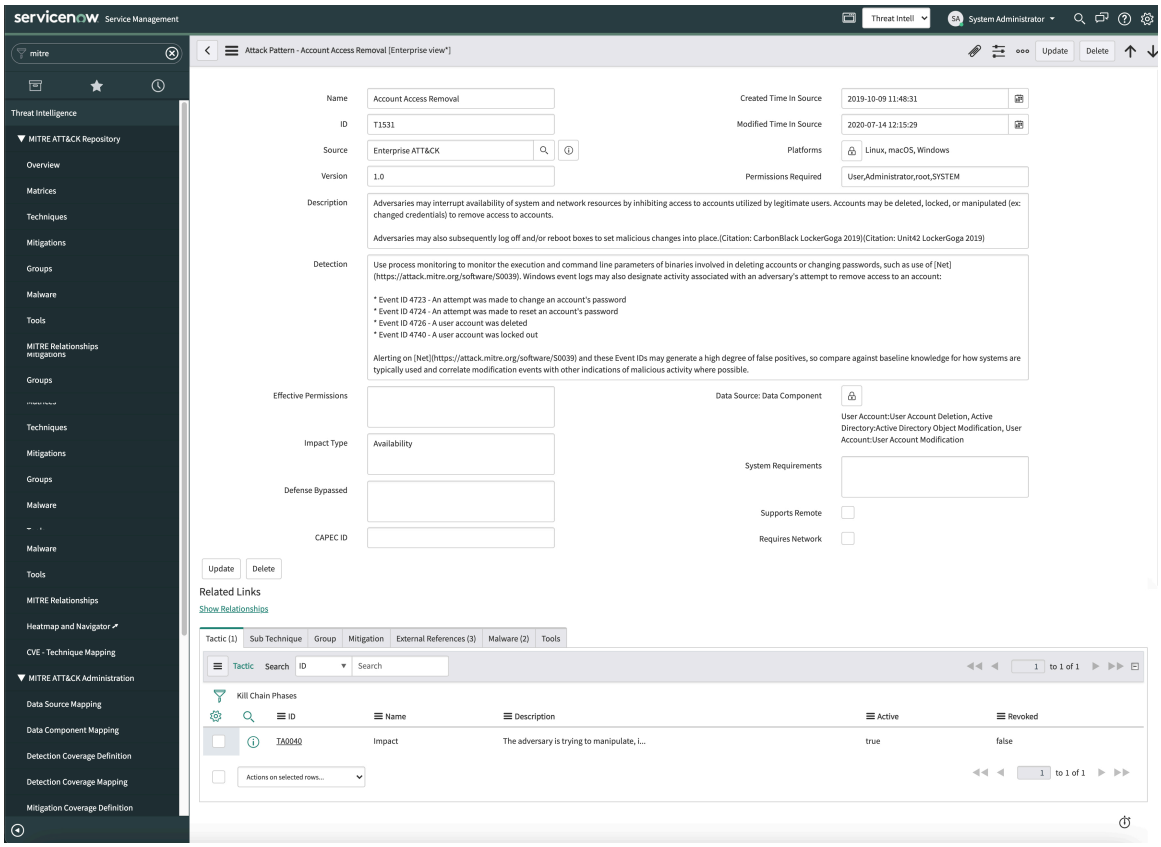
La liste des techniques et sous-techniques est maintenant répertoriée.

2. Pour examiner et désactiver des techniques qui ne sont pas pertinentes pour votre organisation, accédez à la vue de liste correspondant à la technique sélectionnée et, dans la colonne Actif, mettez à jour le paramètre sur **faux** et enregistrez le paramètre.
   Désactivez les techniques qui ne sont pas utilisées par les autres objets du MITRE-ATT&CK référentiel.
3. Pour classer une technique par ordre de priorité, affectez-lui une priorité dans le champ **Priorité pertinente (personnalisée).**
   La priorité pertinente pour le système de base est définie sur aucune. Le champ **Priorité pertinente (personnalisé)** n'est MITRE-ATT&CK TAXII pas importé à partir des collections, mais un champ personnalisé introduit dans le ServiceNow AI Platform. Vous pouvez utiliser les informations de priorité pertinentes pour filtrer et classer par ordre de priorité les techniques dans les tableaux de bord, pendant le mappage de la source de données ou lors de l'analyse de la carte thermique.
4. Cliquez sur une technique pour afficher toutes les informations associées à cette technique.

   Dans l'illustration suivante, vous pouvez afficher les détails de chaque technique de suppression d'accès au compte, son ID, sa source et d'autres informations connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque : L'élément Source de données : composant de données introduit par MITRE remplace le champ Source de données précédent. Le composant de données fournit une sous-couche supplémentaire de contexte aux sources de données. Si votre MITRE-ATT&CK référentiel contient les anciennes TAXII collections, vous pouvez afficher le champ Source de données. Dans le cas contraire, vous pouvez afficher les sources de données avec le contexte supplémentaire des composants de données dans le champ Source de données : composant de données. Vous pouvez afficher le nouveau champ de composant de données uniquement lorsque la source est Enterprise ATT&CK. Pour plus d'informations, consultez mappage des composants de données.

5. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Vous pouvez étendre les informations dans certains de ces objets de liste connexes. Par exemple, vous pouvez ajouter de nouvelles informations pour le groupe, l'atténuation et les références externes.

Gérer les atténuations

Gérez les atténuations qui ont été importées à partir des MITRE TAXII collections. Les atténuations vous permettent d'empêcher un adversaire d'exécuter avec succès des techniques ou des sous-techniques contre votre organisation. Dans STIX, les mesures d'atténuation sont appelées plan d'action.

Avant de commencer

Rôle requis :

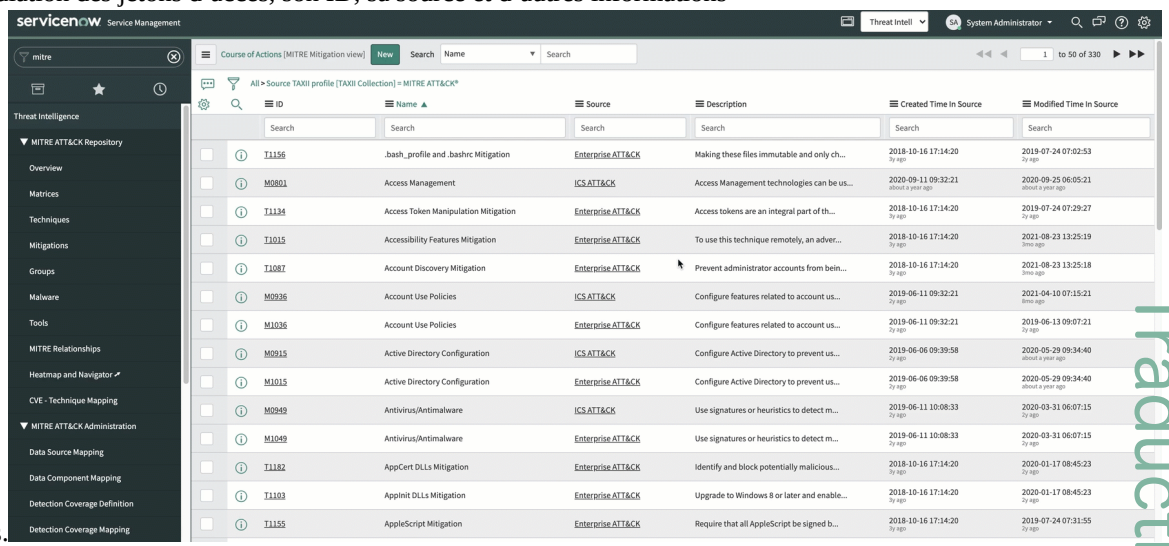
- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Atténuations**.
   Les atténuations sont maintenant répertoriées.
2. Cliquez sur une atténuation pour afficher toutes les informations associées.
   Dans l'illustration suivante, vous pouvez afficher les détails de l'atténuation de la manipulation des jetons d'accès, son ID, sa source et d'autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Utilisez le module des techniques pour ajouter ou modifier les données d'atténuation.

Gérer les groupes

Gérez les groupes qui ont été importés à partir des MITRE TAXII collections. Les groupes sont des ensembles d'activités d'intrusion connexes qui sont suivies par un nom commun dans la communauté de sécurité. Les analystes suivent les grappes d'activités à l'aide de divers termes tels que groupes de menaces, groupes d'activités, acteurs de menace, ensembles d'intrusion et campagnes. Dans STIX, les groupes sont appelés ensembles d'intrusion.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l'accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

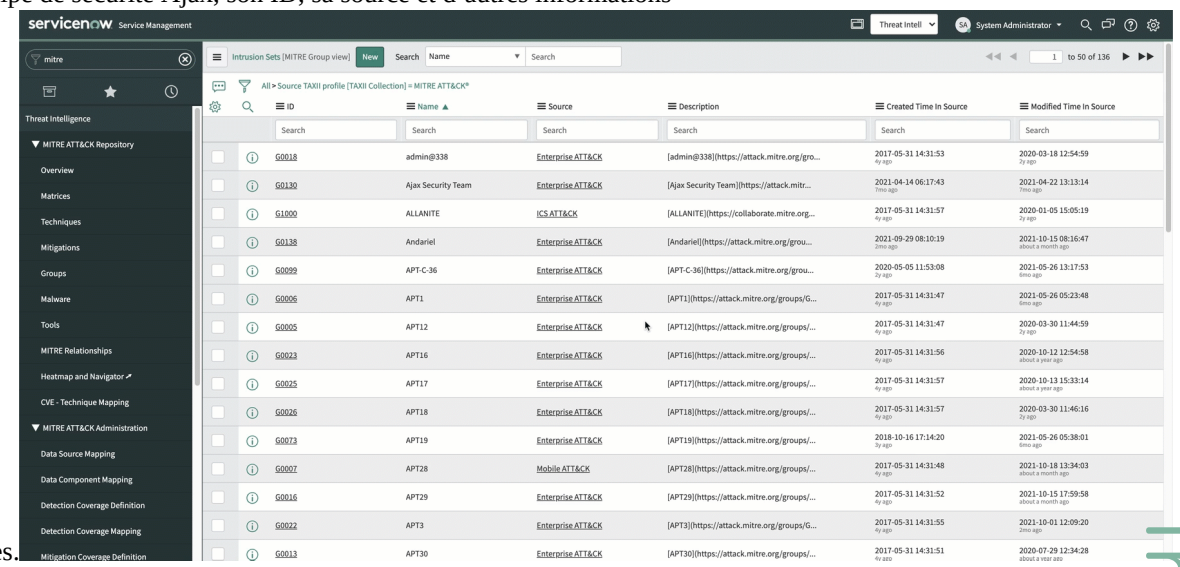
Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Groupes**.
   Vous pouvez afficher les groupes répertoriés.
2. Cliquez sur un groupe pour afficher toutes les informations associées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l’illustration suivante, vous pouvez afficher les détails du groupe de l’équipe de sécurité Ajax, son ID, sa source et d’autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

> **Remarque :** Pour associer les groupes de menaces à un ticket de sécurité en vue d’une enquête plus approfondie, cliquez sur **Ajouter au ticket de sécurité**.

Que faire ensuite

Utilisez le module des techniques pour ajouter ou modifier les données des groupes.

Gérer les programmes malveillants

Gérez les informations sur les programmes malveillants que vous avez importées à partir des MITRE TAXII collections. Un logiciel malveillant est un type de TTP qui représente un code malveillant. Il s’agit d’un programme qui est secrètement inséré dans un système. L’intention d’un logiciel malveillant est de compromettre la confidentialité, l’intégrité ou la disponibilité des données, des applications ou du système d’exploitation (OS) de la victime.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l’accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

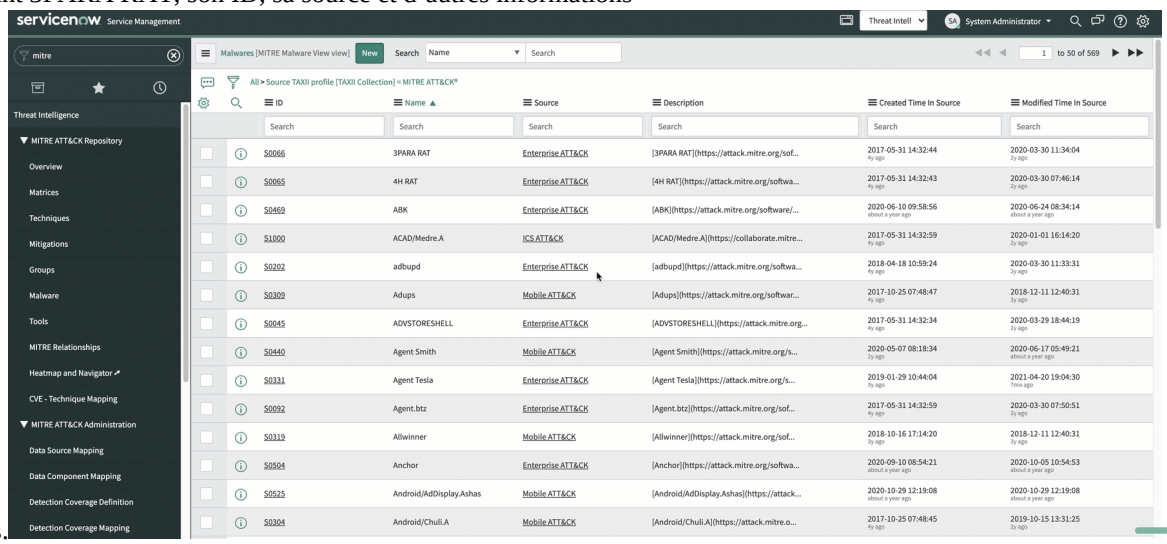
Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Programme malveillant**.
   Vous pouvez afficher les programmes malveillants répertoriés.
2. Cliquez sur un programme malveillant pour afficher toutes les informations associées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l’illustration suivante, vous pouvez afficher les détails du logiciel malveillant 3PARA RAT, son ID, sa source et d’autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Utilisez le module des techniques pour ajouter ou modifier les données relatives aux logiciels malveillants.

Gérer les outils

Gérez les informations sur les outils que vous avez importées à partir des MITRE TAXII collections. Les outils sont des logiciels légitimes utilisés par les acteurs de la menace pour effectuer des attaques.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l’accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Pourquoi et quand exécuter cette tâche

Les outils vous permettent de savoir comment et quand les acteurs de la menace les utilisent pour exécuter des campagnes. Contrairement aux logiciels malveillants, ces outils ou progiciels se trouvent souvent sur un système et ont des objectifs légitimes pour les utilisateurs avancés, les administrateurs, les administrateurs réseau ou même les utilisateurs normaux.

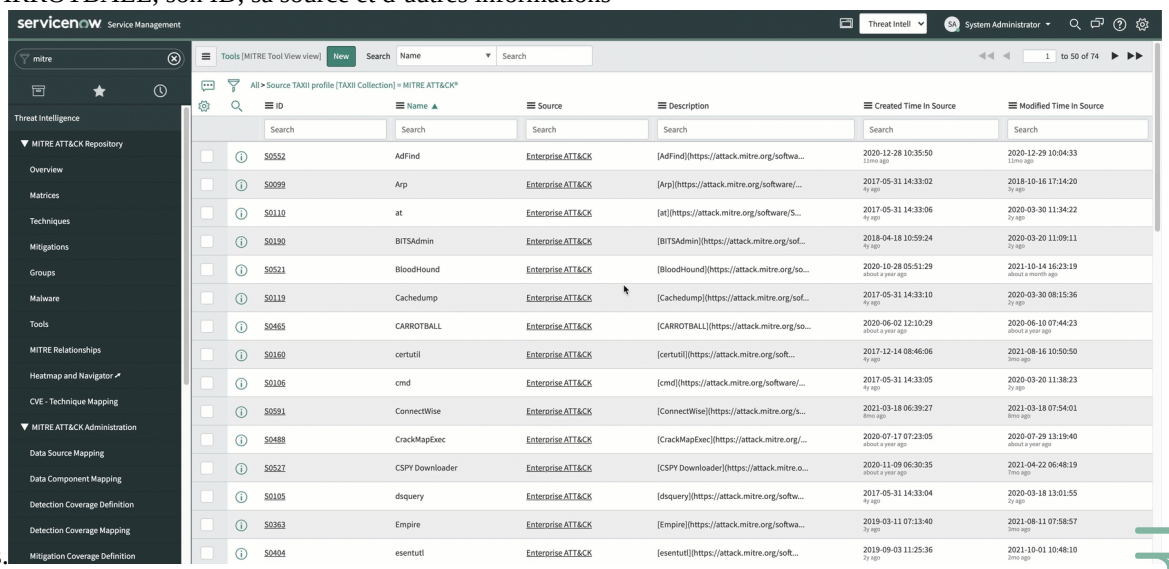
Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Outils**. Vous pouvez afficher les outils répertoriés.
2. Cliquez sur un outil pour afficher toutes les informations associées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l’illustration suivante, vous pouvez afficher les détails de l’outil CARROTBALL, son ID, sa source et d’autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Utilisez le module Techniques pour ajouter ou modifier les données des outils.

Gérer les MITRE relations

Gérez les MITRE informations de relations que vous avez importées à partir des MITRE TAXII collections.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l’accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

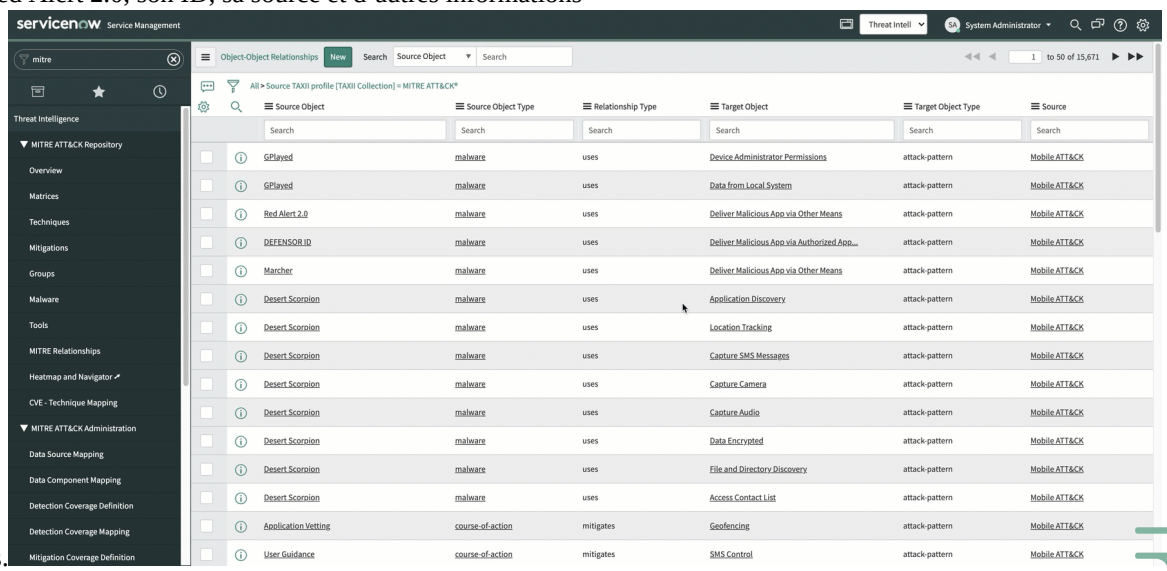
Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Relations MITRE**.
   Vous pouvez afficher les outils répertoriés.
2. Cliquez sur un objet source pour afficher toutes les informations associées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l’illustration suivante, vous pouvez afficher les détails de l’objet Red Alert 2.0, son ID, sa source et d’autres informations connexes.



3. Pour voir comment ces objets sont liés, cliquez sur **Afficher les relations**.

Que faire ensuite

Utilisez le module des techniques pour ajouter ou modifier les données de relations MITRE.

Gérer le CVE et le mappage des techniques

Gérez les informations CVE et techniques qui sont mappées après l’importation des MITRE TAXII collections.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l’accès
- sn_si.admin : créer, écrire, supprimer l’accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

Remarque : Le module **de mappage de technique CVE** n’est disponible que lorsque le produit Vulnerability Response est installé dans votre environnement.

Pourquoi et quand exécuter cette tâche

Une fois que vous importez les MITRE TAXII collections, vous pouvez afficher les CVE dans votre environnement et leur relation avec les techniques associées MITRE-ATT&CK . Vous pouvez également créer des associations avec les CVE et les schémas d’attaque.

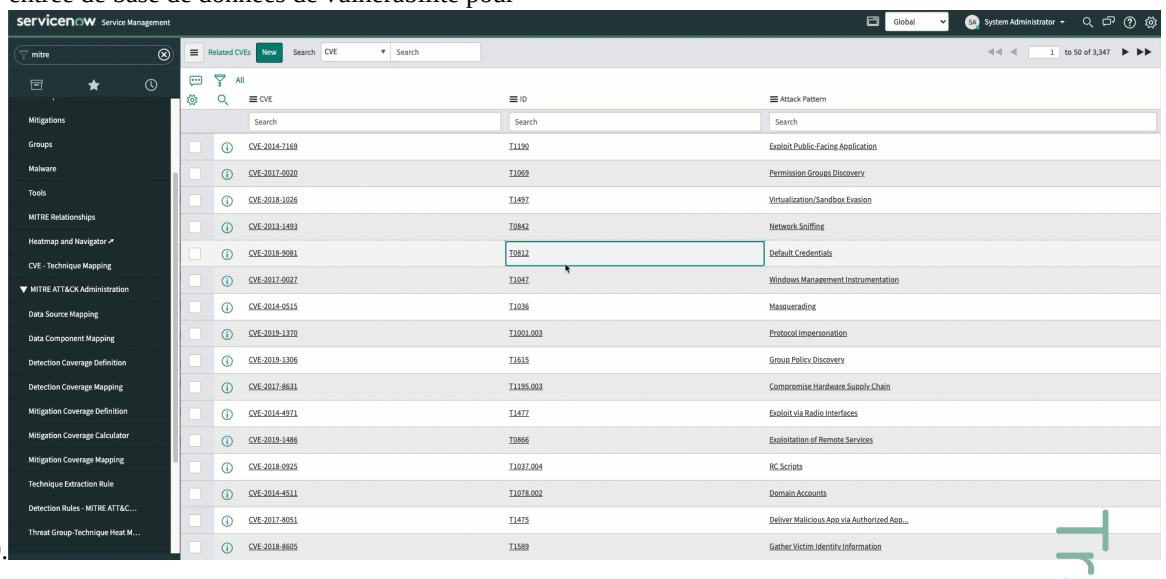
Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **CVE : mappage de technique**.
   Vous pouvez afficher les CVE et les techniques répertoriées.
2. Cliquez sur un CVE pour afficher l’entrée de la base de données des vulnérabilités.

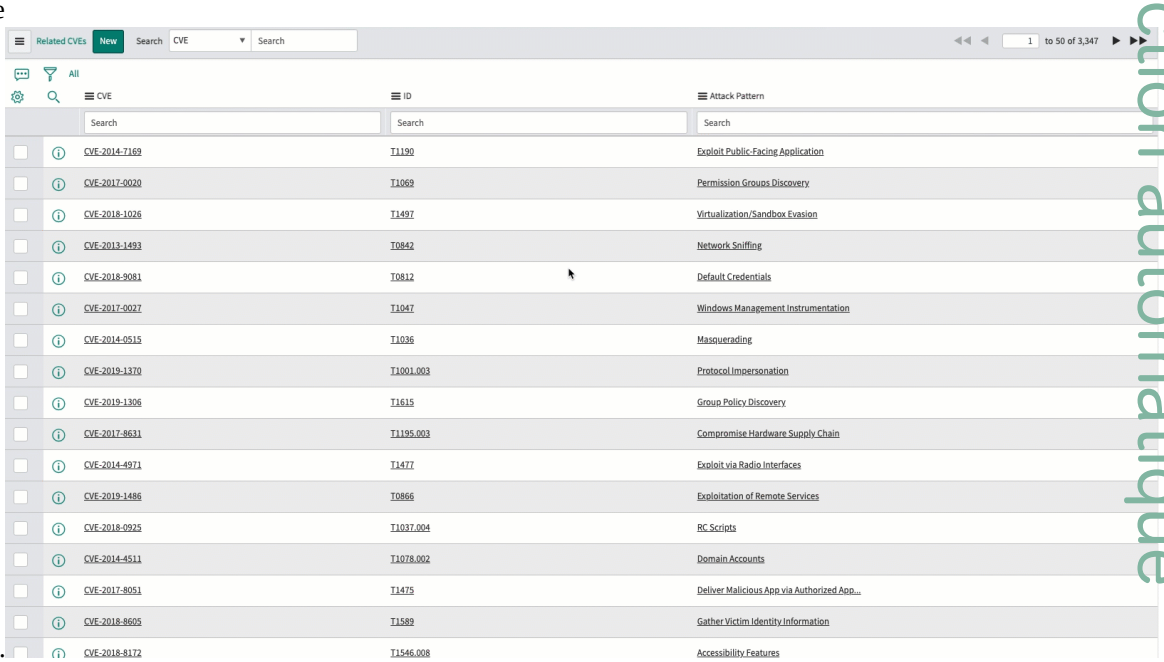
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l’illustration suivante, vous pouvez afficher les détails de la liste CVE et de l’entrée de base de données de vulnérabilité pour CVE-2014-7169.



3. Pour ajouter une entrée, cliquez sur **Nouveau**, mappez les CVE à un modèle d’attaque, puis cliquez sur **Soumettre**.
   Dans l’illustration suivante, une nouvelle entrée est créée en mappant CVE-2014-0515 avec le modèle d’attaque masquée.



Traduction automatique

Étendre les MITRE-ATT&CK données

Étendre les données du MITRE-ATT&CK référentiel en ServiceNow AI Platform les enrichissant.

Avant de commencer

Rôle requis :

- sn_ti.admin : supprimer l’accès
- sn_ti.read : accès en lecture
- sn_ti.write : créer, accès en écriture

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez étendre les objets Malware, Group, Mitigation et Tool à une technique du MITRE-ATT&CK référentiel.

Vous pouvez créer un nouvel objet et établir une relation entre une technique et le nouvel objet dans le module Référentiel MITRE ATT&CK, mais vous ne pouvez pas définir le type de relation dans ce module. Pour plus d'informations sur la définition des types de relation, consultez Relations objet à objet. Pour définir un type de relation, accédez au **Renseignements sur les menaces** > **Référentiel IoC** > **Relations objet-objet** module.

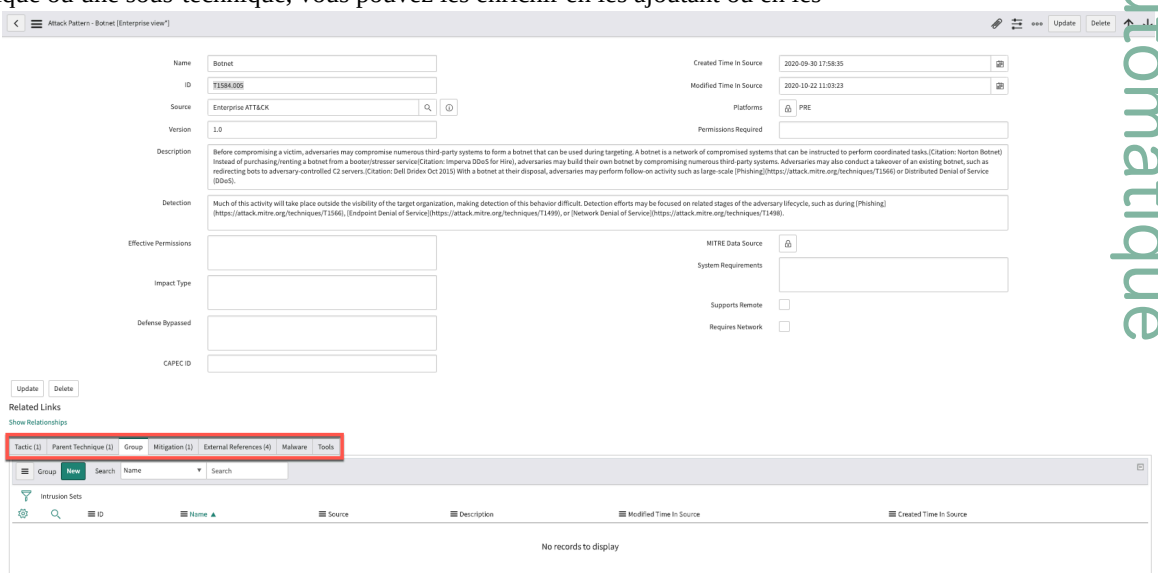
Si vous mappez le type de relation entre une technique existante et un objet existant, vous devez définir la technique comme objet cible et l'objet comme objet source. Pour ce faire, accédez au **Référentiel IoC** > **Relations objet-objet** module.

Vous pouvez créer un groupe et l'associer à un modèle d'attaque, mais dans le référentiel MITRE ATT&CK, vous ne pouvez établir que la relation entre le groupe et le modèle d'attaque. Pour définir le type de relation objet-objet, vous devez le faire dans le référentiel IoC.

Remarque : Toutes les personnalisations que vous apportez aux objets sont enregistrées lors des mises à jour planifiées.

Procédure

1. Accédez à la **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Techniques**.
2. Cliquez sur une technique ou une sous-technique pour afficher toutes les informations associées à cette technique.
   Dans l'illustration suivante, vous pouvez voir que la technique du botnet (T1584.005) n'est associée à aucun groupe. Si vous disposez d'informations supplémentaires sur une technique ou une sous-technique, vous pouvez les enrichir en les ajoutant ou en les modifiant.

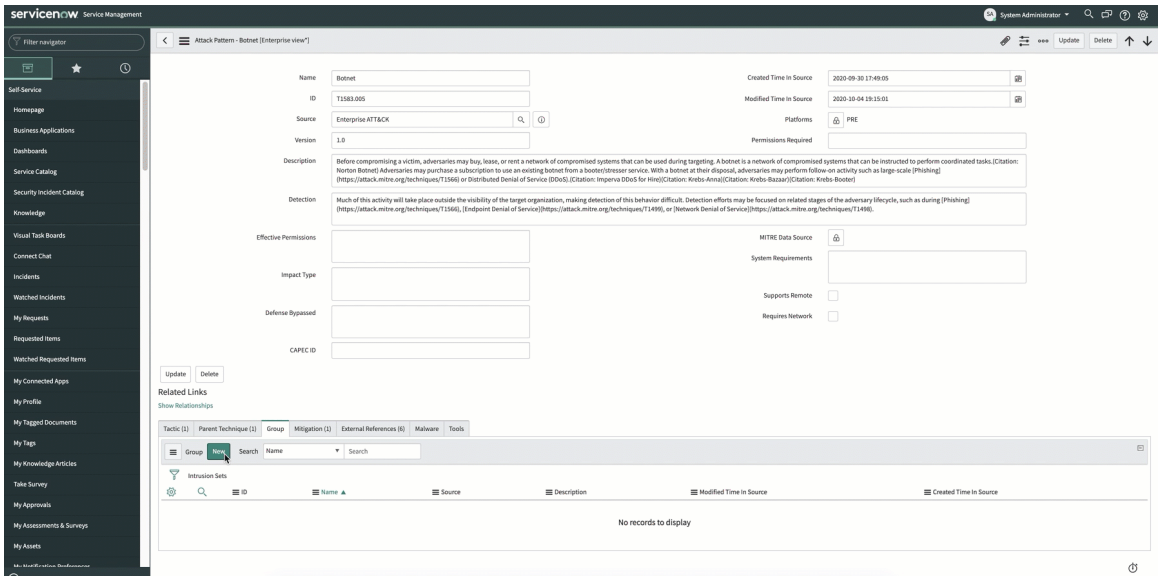


3. Cliquez sur une liste connexe pour enrichir ses données afin de l'associer à un nouveau groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans l'illustration suivante, un groupe, Custom1, a été associé à la sous-technique Botnet.



Définir le mappage de la source de données et de l'outil de détection

Définissez la source de données et le mappage de l'outil de détection pour MITRE-ATT&CK les tactiques et les techniques. Le mappage des sources de données vous donne un aperçu de la pertinence et de la disponibilité des sources de données et des outils de détection pour surveiller les sources de données dans votre environnement.

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : écriture, suppression de l'accès
- sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Vous pouvez identifier les sources de données et les outils de détection dont votre organisation a besoin pour détecter efficacement les techniques.

Par exemple, si votre organisation se concentre sur 5 techniques, vous aurez peut-être besoin de 10 sources de données et de 10 outils de détection pour surveiller ces sources. Supposons que vous identifiez que votre organisation ne dispose pas de deux sources de données et de cinq outils de détection. Cet exercice vous donne une visibilité sur les sources de données, leur pertinence pour votre organisation et pour identifier les lacunes dans la couverture. Vous pouvez également vous concentrer sur l'amélioration de votre environnement avec les bonnes sources de données et les bons outils de détection.

Toutes les tactiques, techniques, ID et sources de données actives sont automatiquement renseignées en fonction de votre TAXII Profil

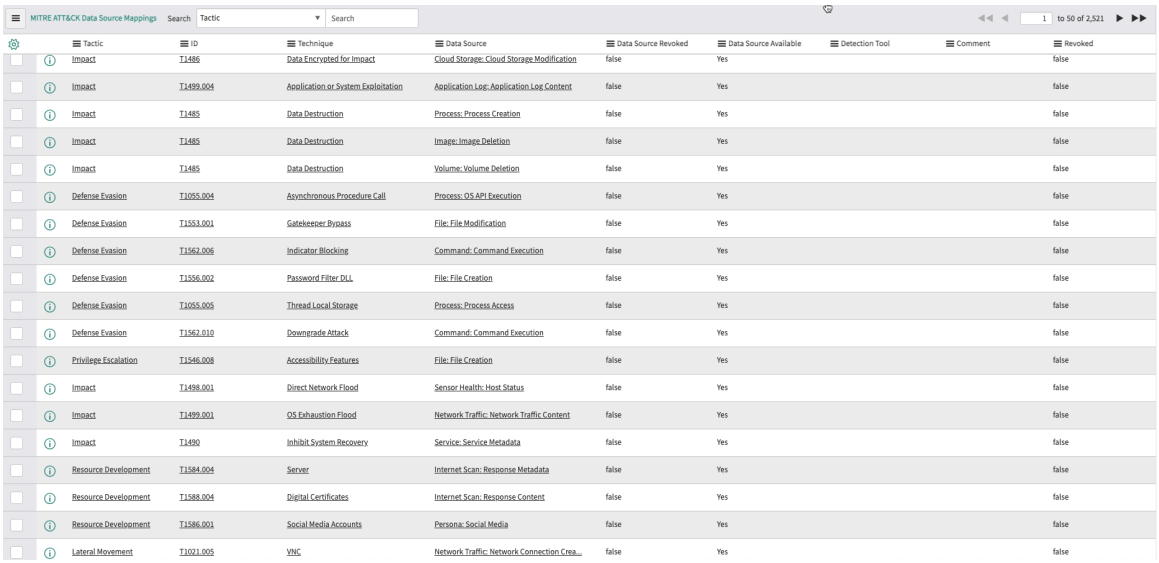
Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Mappage de source de données**.

   L'illustration suivante montre la liste des tactiques, techniques et de leurs ID qui ont été renseignées en fonction des mises à jour de votre collection.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champ	Description
Tactique	Objectif de l’adversaire ou motif de l’exécution d’une action.
ID	L’identité unique de Technique.
Technique	Comment un adversaire atteint un objectif tactique en effectuant une action.
Source de données	Source de données associée à la technique.
Source de données révoquée	La source de données est révoquée si elle est définie sur vrai, mais le mappage de source de données est toujours conservé. Si la valeur de la source de données est introuvable dans MITRE, la valeur Source de données révoquée est automatiquement marquée comme Vrai. Le mappage de source de données d’un enregistrement est révoqué si la technique et les relations de la source de données sont absentes des données mises à jour MITRE . Valeur par défaut : false
Source de données disponible	Disponibilité de la source de données.
Outil de détection	Outil qui complète la source de données en détectant les techniques utilisées. L’outil de détection est mappé avec le capteur d’alerte dans SIR.
Révoqué	Le mappage de source de données d’un enregistrement est révoqué si la technique et les relations de la source de données sont absentes des données mises à jour MITRE . Valeur par défaut : false

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Examinez les sources de données répertoriées et modifiez la valeur dans le champ **Source de données disponible** en fonction de votre environnement.

3. **Remarque :** Vous ne pouvez pas modifier cette entrée à partir de la vue de liste.

   Dans le champ **Outil de détection** , procédez comme suit :

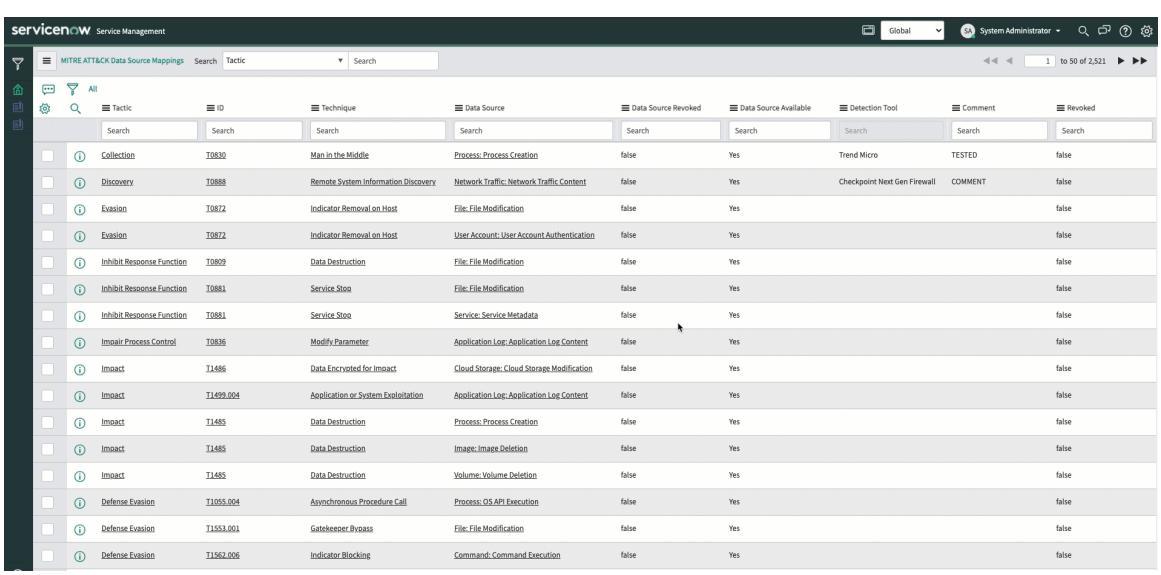
   a. Cliquez sur l'icône d'informations, puis sur **Ouvrir l'enregistrement**.

   b. Déverrouillez l'entrée **de l'outil de détection** .

   c. Utilisez la liste de recherche pour sélectionner un outil de détection. Vous pouvez sélectionner plusieurs outils de détection.

   d. Cliquez sur **Mettre à jour**.

   Dans l'illustration suivante, plusieurs outils de détection sont ajoutés pour surveiller la source de données.



Définir le mappage de la source de données et du composant de données

Utilisez le mappage des composants de données si vous utilisez les dernières TAXII collections et si vous souhaitez maintenir une relation entre les sources de données, les composants de données et les différentes techniques. Mappez les sources de données avec le contexte supplémentaire des composants de données qui fournit une sous-couche supplémentaire de contexte aux sources de données qui vous permettent de mieux comprendre les comportements des adversaires MITRE-ATT&CK .

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : écriture, suppression de l'accès
- sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Le mappage des sources de données et des composants de données fournit une visibilité sur les sources de données ou les composants et sur les techniques pertinentes pour votre organisation.

Par exemple, si votre organisation se concentre sur 7 techniques, vous aurez peut-être besoin de 5 sources de données et de 10 composants de données pour surveiller ces

Traduction automatique

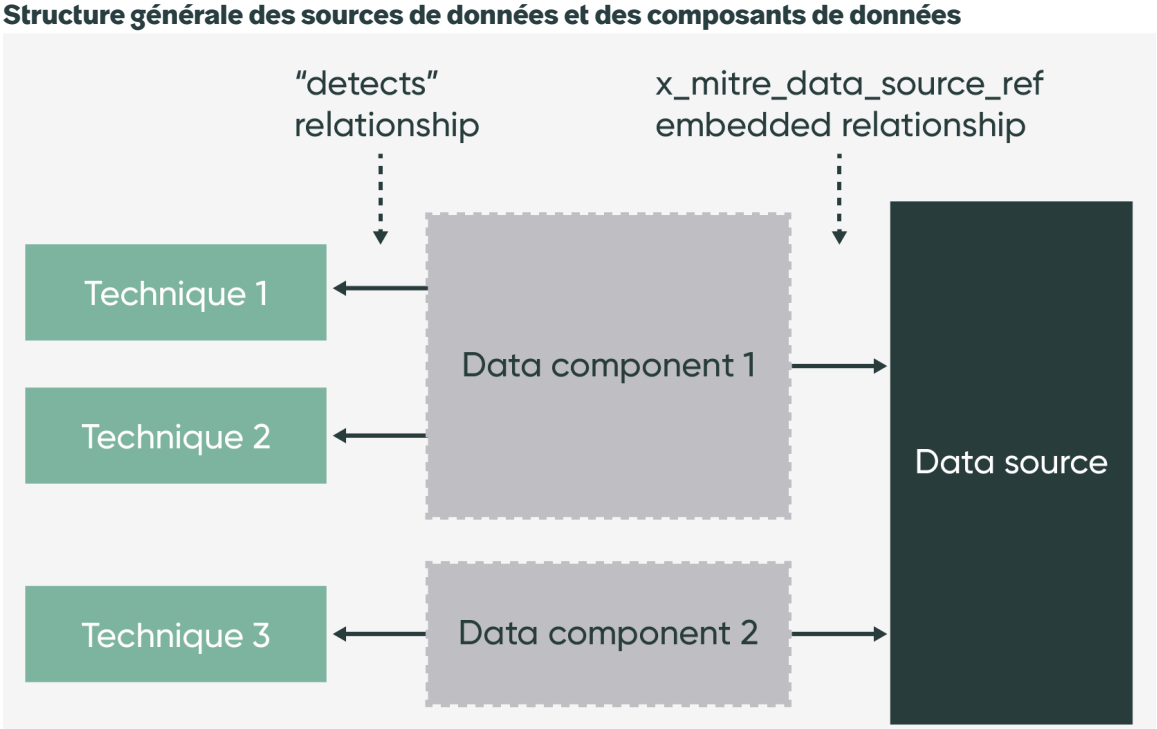
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sources. Votre évaluation des outils internes révèle que votre organisation ne dispose pas de deux sources de données et de quatre composants de données. Cet exercice de mappage fournit une visibilité sur les sources de données, les composants et les techniques, leur pertinence pour votre organisation et pour identifier les lacunes de couverture. Vous pouvez ainsi concentrer votre investissement sur les bonnes sources de données et les bons capteurs d'alerte pour détecter et atténuer les menaces adverses.

Le MITRE-ATT&CK cadre de travail contient une structure mise à jour pour les sources de données : Source de données : composant de données. Cette nouvelle forme de source de données fournit un contexte supplémentaire aux sources de données. L'objet source de données contient le nom de la source de données ainsi que des détails clés sur les données collectées (fichier, processus, trafic réseau, etc.) et des valeurs ou propriétés spécifiques requises pour détecter les comportements des adversaires.

L'illustration suivante montre la représentation de la structure pour les sources de données et les MITRE-ATT&CK STIX™ composants de données. Vous pouvez afficher à la fois les sources de données et les composants de données capturés en tant qu'objets personnalisés STIX™ . L'illustration montre que chaque source de données contient un ou plusieurs composants de données et que chaque composant de données détecte une ou plusieurs techniques.

Structure générale des sources de données et des composants de données



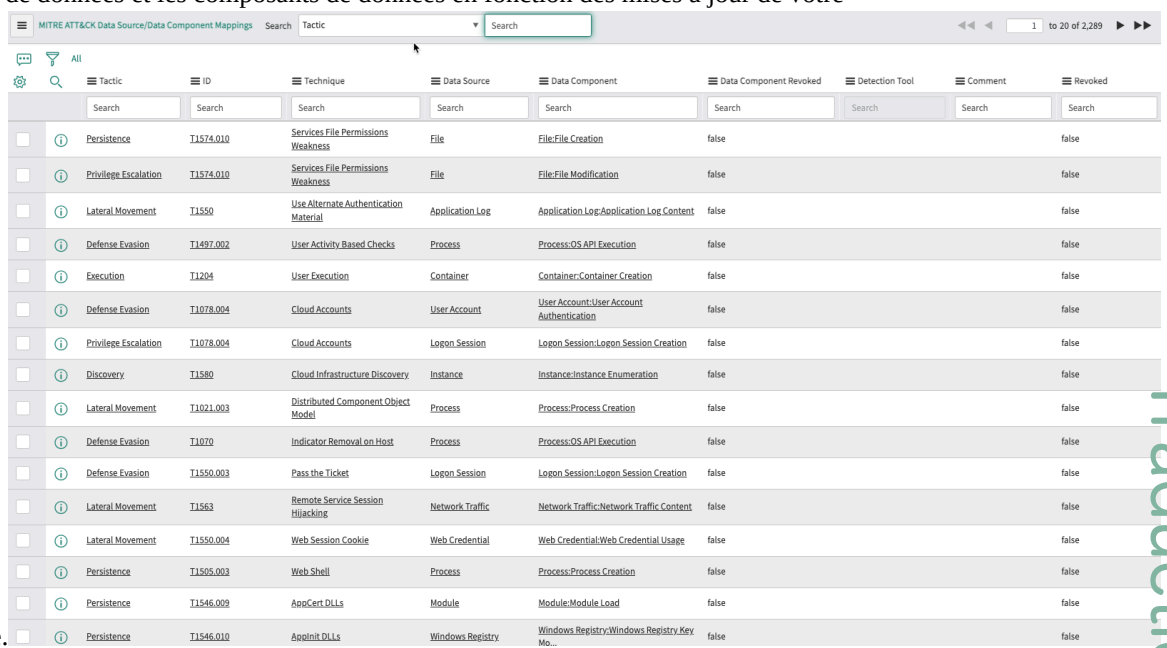
Vous pouvez continuer à utiliser le mappage de source de données si votre MITRE-ATT&CK référentiel contient les anciennes TAXII collections et que vous avez mappé vos sources de données à différentes techniques. Toutefois, utilisez le mappage des composants de données si vous utilisez les dernières TAXII collections et si vous souhaitez maintenir une relation entre les sources de données, les composants de données et les différentes techniques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Mappage des composants de données**.
   L'illustration suivante montre la liste des tactiques, des ID et des techniques, ainsi que les sources de données et les composants de données en fonction des mises à jour de votre collecte.



Champ	Description
Tactique	Objectif de l'adversaire ou motif de l'exécution d'une action.
ID	L'identité unique de Technique.
Technique	Comment un adversaire atteint un objectif tactique en effectuant une action.
Source de données	Source de données associée à la technique.
Composant de données	Composant de données associé à la source de données. Un composant de données ne peut avoir qu'une seule source de données parente.
Composant de données révoqué	Identifie si le composant de données a été révoqué dans la MITRE-ATT&CK base de connaissances.
Outil de détection	Outil qui complète la source de données en détectant les techniques utilisées. L'outil de détection est mappé avec le capteur d'alerte dans SIR.
Commentaire	Description du mappage de la source de données et du composant de données.
Révoqué	Identifie si le composant de données au mappage de technique est révoqué par MITRE-ATT&CK.

2. Examinez les sources de données et les composants de données répertoriés et modifiez les valeurs en fonction de votre environnement.
3. Suivez ces étapes pour ajouter un composant de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Techniques**.

b. Cliquez sur une technique dont vous souhaitez modifier la source de données : informations sur le composant de données.

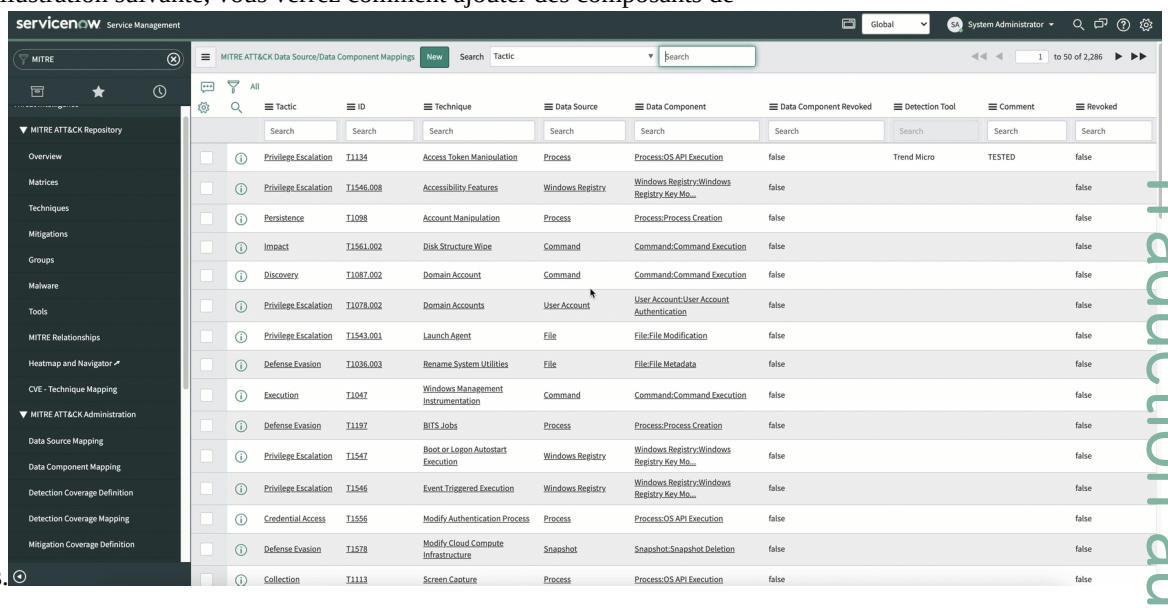
c. Déverrouiller la source de données : composant de données.

d. Utilisez la liste de recherche pour sélectionner MITRE-ATT&CK les composants de données.

e. Verrouiller la source de données : composant de données.

f. Cliquez sur **Mettre à jour**.

Dans l'illustration suivante, vous verrez comment ajouter des composants de données.



Définir la couverture de détection de technique

Définissez la couverture de détection de technique que votre organisation doit mesurer et détectez les techniques spécifiques des adversaires.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : accès en écriture
- Rôle requis : sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

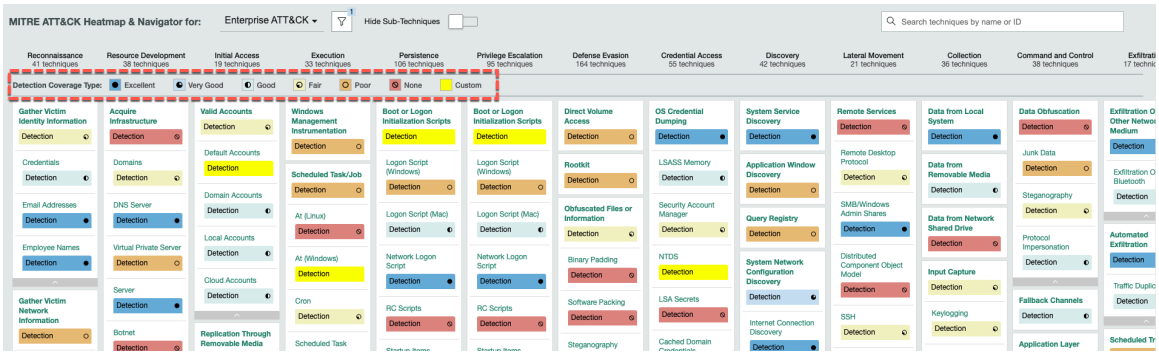
Les définitions de couverture de la technique sont utilisées dans le mappage global de détection de la technique. Vous pouvez utiliser la couverture de la technique du système de base. La couverture de la technique du système de base comprend les types de couverture Aucune, Médiocre, Passable, Bon, Très bon et Excellent. La couverture de la technique du système de base est également associée à des couleurs prédéfinies. Vous pouvez personnaliser les entrées et les couleurs du type de couverture ou créer vos propres entrées. Par exemple, vous pouvez remplacer les types de couverture du système de base par Non applicable, Couverture partielle et Couverture complète. Vous pouvez également créer des mesures numériques pour les types de couverture, par exemple 0-25 %, 25-50 % et 50-100 %. Le type de modifications apportées à la couverture du système de base ne se limite pas aux exemples partagés.

Les personnalisations que vous apportez au type de couverture et à la couleur sont utilisées dans le mappage de détection de technique global , ainsi que dans la carte thermique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous modifiez la définition de couverture du système de base, les icônes Type de couverture ne s'affichent pas avec les techniques de la carte thermique. La carte thermique fonctionne comme prévu lorsque vous modifiez les mêmes champs que la couverture de détection technique et les couleurs de couverture définies par le système de base. Toutefois, si vous supprimez les champs existants de la couverture globale de détection technique, la carte thermique n'affiche pas les icônes de type de couverture.



Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Définition de couverture de détection**.
2. Passez en revue les entrées de détection de la technique globales et personnalisez les entrées pour votre environnement.

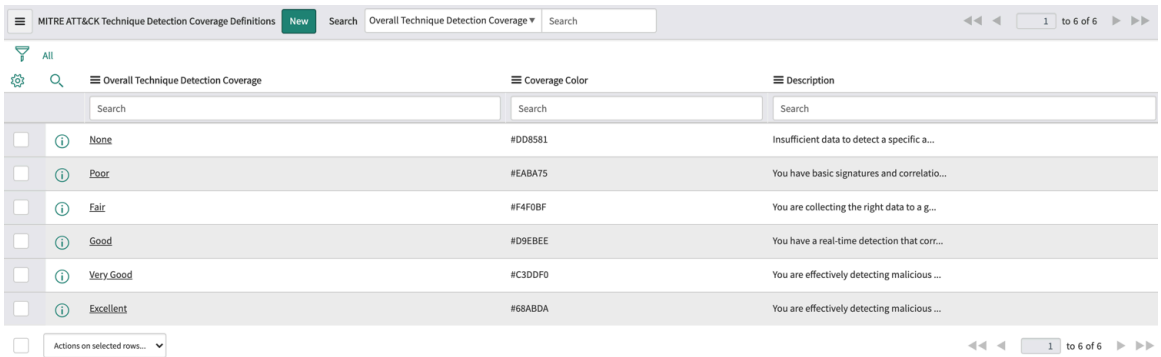
Définition de couverture de détection

Champ	Description
Couverture de détection de la technique globale	Nom de la couverture globale de détection de la technique. La couverture de la technique du système de base comprend Aucune, Médiocre, Passable, Bon, Très bon ou Excellent.
Couleur de couverture	Couleur affectée au score de couverture de détection. La couleur que vous définissez est utilisée pour la couverture de détection de technique dans la carte thermique. Vous pouvez personnaliser les couleurs à l'aide de codes HEX et de valeurs RVB(A).
Description	Couverture globale de la détection technique. Voir la définition du système de base dans la définition de notation.

L'illustration suivante montre la liste de définition de couverture de détection.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour ajouter une entrée, cliquez sur **Nouveau**, remplissez les entrées, puis cliquez sur **Soumettre**.

MITRE-ATT&CK Définition du score

Définissez le système de notation de MITRE-ATT&CK votre organisation afin de mesurer l'efficacité avec laquelle votre organisation peut détecter des techniques adverses spécifiques.

Définition du score

Score	Mappage de score	Description
Aucun	0	Données insuffisantes pour détecter une technique spécifique de l'adversaire.
Médiocre	1	Des signatures de base et des règles de corrélation sont en place pour détecter des techniques adverses spécifiques. La détection des menaces ne se fait pas en temps réel et ne couvre qu'un nombre minimal d'aspects d'une technique. Par exemple, la chasse n'a lieu que sur un seul point de terminaison à la fois. Votre organisation peut encore avoir des milliers ou des centaines d'événements que les chasseurs doivent examiner et corréler avec d'autres événements pour trouver des valeurs aberrantes. Le nombre de faux positifs est élevé.
Acceptable	2	Collecter les bonnes données dans une large mesure et la qualité des données est équitable. Par exemple, votre organisation commence peut-être à ajouter des journaux Sysmon, ETW, journaux PowerShell, etc. Cependant, la détection des menaces n'est toujours pas en temps réel. Votre organisation ne dispose peut-être pas de tous les bons outils pour regrouper et analyser efficacement les données. Les chasseurs doivent exécuter manuellement des requêtes et les corréler pour analyser les données avec précision. Le nombre de faux positifs est élevé.
Bien	3	Détection en temps réel qui met en corrélation et intègre plusieurs données sur vos terminaux. La détection des menaces couvre de nombreux aspects des procédures d'une technique. Vos adversaires pourraient éventuellement contourner la détection par l'évasion et l'obscurcissement. Votre organisation peut facilement identifier les faux positifs et les filtrer. Votre organisation utilise des techniques de science des données de base pour analyser les données dans le référentiel central.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définition du score (suite)

Score	Mappage de score	Description
Très bien	4	Détectez efficacement les techniques malveillantes en temps réel et couvrez la plupart des aspects des procédures d'une technique. La possibilité que vos adversaires contournent la détection avec des méthodes d'évasion et d'obscurcissement est plus difficile qu'au niveau Bien. Votre organisation peut facilement identifier les faux positifs et les filtrer. Votre organisation utilise des techniques avancées de science des données pour détecter les techniques adverses.
Excellent	5	Détectez efficacement les techniques malveillantes en temps réel et couvrez tous les aspects des procédures d'une technique. Votre organisation a une bonne compréhension de votre environnement avec la bonne automatisation et la bonne qualité des données. La possibilité pour vos adversaires de contourner la détection par des méthodes d'évasion et d'obscurcissement n'est pas possible à ce niveau. Le nombre de faux négatifs est faible.

Mapper votre couverture de détection de technique à une technique

Mappez votre couverture globale de détection de technique avec la technique qui permet à votre organisation de détecter des techniques adverses spécifiques.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : accès en écriture
- Rôle requis : sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la couverture de détection de technique pour obtenir une vue d'ensemble de la couverture globale de détection de technique de votre organisation. Par exemple, si un adversaire attaque votre organisation, vous voyez le type de couverture dont vous disposez pour détecter les techniques de l'attaquant.

La technique et l'ID sont automatiquement renseignés pour toutes les collections et techniques que vous avez activées. Le type de couverture et la définition de notation que vous avez définis sont disponibles en tant qu'option que vous pouvez sélectionner dans la couverture globale de détection de technique.

Vous pouvez mapper la couverture globale de détection de la technique avec la technique pour terminer le mappage. Vous ne pouvez associer une technique qu'à une seule couverture globale de détection de technique.

Le mappage de couverture de détection de technique que vous définissez est utilisé dans la visualisation de couverture dans la carte thermique.

Remarque : Vous pouvez obtenir la couverture globale de détection technique en utilisant les calculs spécifiques à votre organisation. Vous pouvez utiliser n'importe quel produit de simulation de violation et d'attaque (BAS), le référentiel de cyberanalyse (CAR) ou toute autre méthode nécessaire pour définir la définition du score, et l'utiliser dans cette procédure pour le mappage global de la couverture de détection technique.

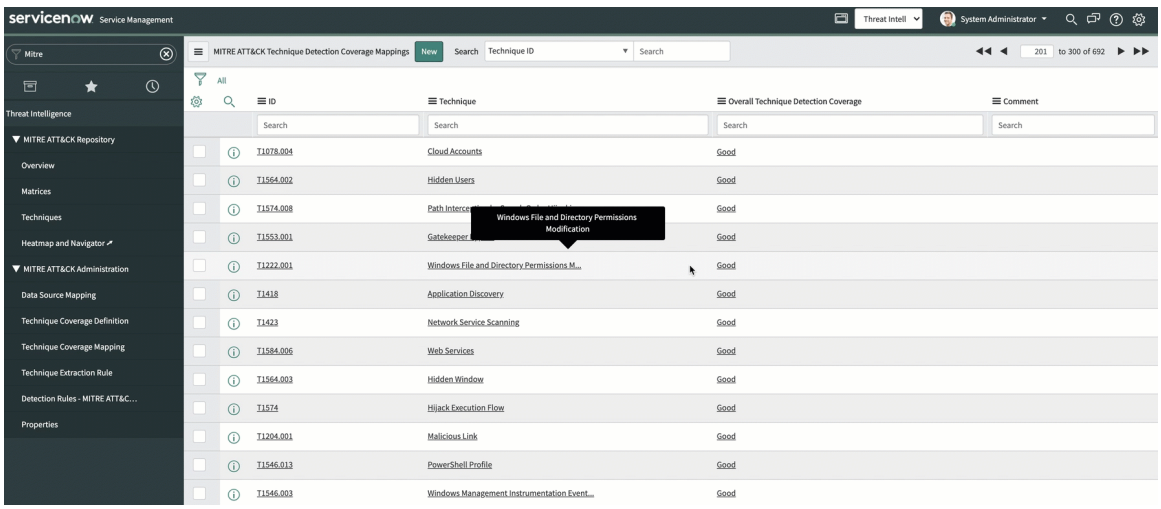
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Mappage de couverture de détection**.

   Dans cette illustration, vous verrez que la sous-technique Comptes dans le cloud (T1078.004) a une excellente couverture dans l'organisation et que la couverture globale de détection de la technique est mappée sur **Excellente**.



2. Passez en revue chaque technique et mappez votre couverture globale de détection technique en fonction de votre définition de couverture de détection et de la disponibilité de la couverture de votre organisation.

Définir la couverture d'atténuation

Définissez la couverture d'atténuation pour chaque atténuation associée à une technique afin d'avoir une visibilité sur la façon dont votre organisation peut prévenir les attaques qui se produisent en raison d'une technique particulière.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : créer, écrire, supprimer un accès
- Rôle requis : sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Les définitions de couverture d'atténuation sont utilisées dans le mappage global de couverture d'atténuation et de technique. Vous pouvez utiliser la couverture d'atténuation du système de base. La couverture d'atténuation du système de base comprend les types de couvertures Aucune, Médiocre, Passable, Bon, Très bon et Excellent. La couverture d'atténuation du système de base est également associée à des couleurs et des pourcentages de couverture prédéfinis. Vous pouvez personnaliser les types de couvertures (ajouter ou supprimer des types de couvertures), les pourcentages de couverture pour les limites inférieures et les limites supérieures, ainsi que les couleurs, ou créer votre couverture d'atténuation personnalisée.

Les personnalisations que vous apportez aux types de couverture, aux couleurs ou aux pourcentages sont utilisées dans le mappage de couverture d'atténuation ainsi que dans la carte thermique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

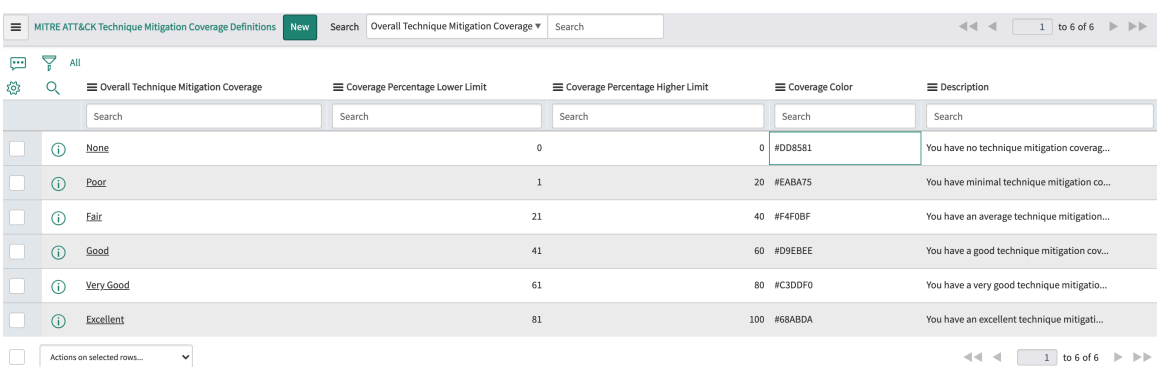
1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Définition de couverture d'atténuation**.
2. Examinez les entrées de détection d'atténuation et personnalisez les entrées pour votre environnement.

Définition de couverture d'atténuation de technique

Champ	Description
Couverture d'atténuation de la technique globale	Nom de la couverture d'atténuation de la technique. La couverture d'atténuation du système de base comprend Aucune, Médiocre, Passable, Bon, Très bon ou Excellent.
Limite inférieure du pourcentage de la couverture	Limite inférieure en pourcentage de la couverture d'atténuation. Définissez les valeurs numériques comprises entre 0 et 100.
Limite supérieure du pourcentage de la couverture	Limite de pourcentage supérieure de la couverture d'atténuation. Définissez les valeurs numériques comprises entre 0 et 100.
Couleur de couverture	Couleur affectée au score de couverture de détection. La couleur que vous définissez est utilisée pour la couverture d'atténuation de la technique dans la carte thermique. Vous pouvez personnaliser les couleurs à l'aide de codes HEX et de valeurs RVB(A).
Description	Couverture globale de détection d'atténuation. Consultez la définition du système de base dans la définition de couverture d'atténuation de la technique.

Remarque : Assurez-vous de ne pas chevaucher les plages de pourcentage de couverture si vous personnalisez les limites de pourcentage (inférieures ou supérieures). Par exemple, si un enregistrement de couverture a des plages de 0 à 20, alors l'enregistrement consécutif suivant doit avoir une plage de limite inférieure de 21 ou supérieure pour éviter de chevaucher la plage de pourcentage de couverture.

L'illustration suivante montre la liste des définitions de couverture d'atténuation.



3. Pour ajouter une entrée, cliquez sur **Nouveau**, remplissez les entrées, puis cliquez sur **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définitions de couvertures d'atténuation de technique

Définissez la couverture d'atténuation de votre organisation afin de pouvoir mesurer et détecter efficacement des techniques adverses spécifiques.

Définitions de la couverture de détection de la technique MITRE ATT&CK

Couverture d'atténuation de la technique globale	Limite inférieure du pourcentage de la couverture	Limite supérieure du pourcentage de la couverture	Couleur de couverture	Description
Aucun	0	0	#DD8581	Vous n'avez aucune couverture d'atténuation technique et vos contrôles de défense n'ont aucune capacité à empêcher une attaque dans n'importe quel scénario.
Médiocre	1	20	#EABA75	Vous disposez d'une couverture minimale de l'atténuation de la technique. Les chances d'une attaque sont très élevées et vos contrôles de défense peuvent empêcher une attaque dans 0 à 20 % des scénarios.
Acceptable	21	40	#F4F0BF	Vous disposez d'une couverture moyenne de l'atténuation de la technique. Les chances d'une attaque sont élevées et vos contrôles de défense peuvent empêcher une attaque dans 21 à 40 % des scénarios.
Bien	41	60	#D9EBEE	Vous disposez d'une bonne couverture technique d'atténuation. Cependant, les chances d'une attaque sont relativement élevées et vos contrôles de défense peuvent

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définitions de la couverture de détection de la technique MITRE ATT&CK (suite)

Couverture d'atténuation de la technique globale	Limite inférieure du pourcentage de la couverture	Limite supérieure du pourcentage de la couverture	Couleur de couverture	Description
				empêcher une attaque dans 41 à 60 % des scénarios.
Très bien	61	80	#C3DDF0	Vous avez une très bonne couverture technique d'atténuation. Les chances d'une attaque sont faibles et vos contrôles de défense peuvent empêcher une attaque dans 61 à 80 % des scénarios.
Excellent	81	100	#68ABDA	Vous disposez d'une excellente couverture d'atténuation des techniques et les chances d'une attaque utilisant cette technique sont très faibles et vos contrôles de défense peuvent empêcher une attaque dans 81 à 100 % des scénarios.

Traduction automatique

Mapper votre couverture d'atténuation à une technique

Mappez votre couverture d'atténuation avec la technique qui vous permet de détecter la stratégie d'atténuation globale de votre organisation.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : écriture, suppression de l'accès
- Rôle requis : sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Les atténuations vous permettent d'empêcher un adversaire d'exécuter avec succès des techniques ou des sous-techniques contre votre organisation. Chaque MITRE-ATT&CK technique contient des atténuations que vous pouvez déployer dans votre organisation pour réduire les risques d'attaque. Vous pouvez utiliser la couverture d'atténuation pour obtenir une vue d'ensemble de la stratégie d'atténuation globale de votre organisation. Par exemple, si un adversaire attaque votre organisation, vous voyez le type de couverture dont vous disposez pour atténuer les techniques de l'attaquant.

La technique et les informations d'atténuation sont automatiquement renseignées pour toutes les collections et techniques que vous avez activées. Vous pouvez sélectionner la

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

définition de couverture d'atténuation que vous avez définie dans la couverture d'atténuation de la technique.

Vous pouvez identifier les atténuations pertinentes pour votre organisation. Si une atténuation est pertinente, vous pouvez définir si les stratégies d'atténuation ont été déployées. Vous pouvez spécifier si les stratégies sont appliquées dans le cadre de la politique SOC de votre organisation. Vous pouvez également déterminer si votre organisation dispose d'outils préventifs pour atténuer les techniques d'un attaquant et vous pouvez mapper tous les contrôles de sécurité que votre organisation a déployés pour minimiser les risques de sécurité. Renseignez la couverture d'atténuation (pourcentage) pour chacun des enregistrements.

Après le mappage des informations pour chacune des techniques, le calculateur de couverture d'atténuation remplit automatiquement la couverture d'atténuation de la technique calculée. Pour calculer la couverture d'atténuation globale pour n'importe quelle technique, les enregistrements de mappage d'atténuation de technique doivent être actifs et pertinents pour l'organisation. Les enregistrements qui sont inactifs et non pertinents ne sont pas pris en compte pour calculer la couverture globale de l'atténuation de la technique. En fonction des valeurs de la couverture d'atténuation de la technique calculée et de la définition de couverture d'atténuation, votre couverture d'atténuation globale de la technique (calculée) est renseignée.

Les personnalisations que vous apportez aux types de couverture, aux couleurs ou aux pourcentages sont utilisées dans le mappage de couverture d'atténuation ainsi que dans la carte thermique.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Mappage de couverture d'atténuation**.
2. Passez en revue chaque technique de mappage d'atténuation et mettez à jour la **couverture d'atténuation (pourcentage)** pour calculer la disponibilité de la couverture de votre organisation.

Mappages de couvertures d'atténuation de technique

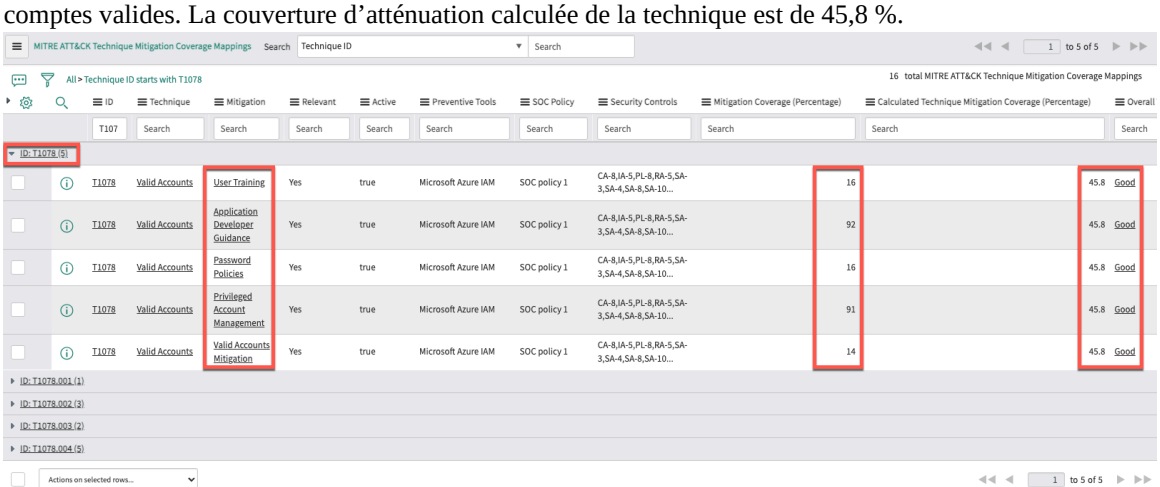
Champ	Description
ID	L'identité unique de Technique. Les ID sont automatiquement renseignés pour toutes les collections et techniques que vous avez activées.
Technique	Comment un adversaire atteint un objectif tactique en effectuant une action. Les informations sur les techniques sont automatiquement renseignées pour toutes les collections et techniques que vous avez activées.
Atténuation	Atténuations vous permettant d'empêcher un adversaire d'exécuter avec succès des techniques ou des sous-techniques contre votre organisation. Les informations relatives à l'atténuation sont automatiquement renseignées pour toutes les collections et techniques que vous avez activées.
Pertinent	Option permettant de spécifier si l'atténuation est pertinente pour votre organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Option permettant de spécifier si les stratégies d'atténuation sont déployées dans votre organisation. Il s'agit d'une option obligatoire requise pour calculer la couverture de l'atténuation de la technique.
Outils préventifs	Option permettant de spécifier si votre organisation a mis en place des outils préventifs pour atténuer les techniques d'un attaquant.
Politique SOC	Les politiques SOC qui définissent les stratégies d'atténuation de votre organisation.
Contrôles de sécurité	Les contrôles de sécurité de votre organisation contiennent les stratégies d'atténuation visant à minimiser les risques de sécurité.
Couverture d'atténuation (pourcentage)	Un système de notation pour calculer la couverture de l'atténuation de la technique. Définissez des valeurs numériques comprises entre 0 et 100. Il s'agit d'une option obligatoire requise pour calculer la couverture de l'atténuation de la technique.
Couverture d'atténuation de la technique calculée (pourcentage)	Couverture d'atténuation de la technique calculée en pourcentage. Cette valeur est déterminée en fonction de la formule définie dans le calculateur de couverture d'atténuation.
Couverture d'atténuation de la technique globale (calculée)	Couverture globale de l'atténuation de la technique. Cette valeur est déterminée en fonction de la couverture d'atténuation définie pour votre organisation.
Commentaire	Description de la technique et du mappage de couverture d'atténuation.
Révoqué	La technique de mappage de couverture d'atténuation est révoquée.

Dans cette illustration, vous voyez que la technique Comptes valides a cinq atténuations associées, chacune avec une couverture d'atténuation de 16 pour la formation des utilisateurs, 92 pour les conseils aux développeurs d'applications, et 16 pour les politiques de mot de passe, 91 pour la gestion des comptes privilégiés et 14 pour l'atténuation des comptes valides. La couverture d'atténuation calculée de la technique est de 45,8 %.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculateur de couverture d'atténuation de la technique globale

La couverture globale de la technique d'atténuation est déterminée en fonction de la formule définie dans le calculateur de couverture d'atténuation.

Avant de commencer

- Rôle requis : sn_ti.admin, sn_si.admin : créer, écrire, supprimer un accès
- Rôle requis : sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

- Vous ne pouvez définir comme actif qu'un seul calculateur de couverture d'atténuation par domaine.
- Le calculateur de couverture d'atténuation du système de base est un calculateur de moyenne.
- Toute personnalisation du script de la calculatrice doit garantir que la sortie finale est une valeur numérique comprise entre 0 et 100.
- La définition de couverture d'atténuation est appliquée en fonction de la plage de la sortie finale.

Procédure

Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Calculateur de couverture d'atténuation**.
L'illustration suivante montre le calculateur de couverture d'atténuation par défaut.



Créer et mapper des règles de détection

Créez des règles de détection et mappez-les par rapport aux tactiques et techniques. Avec ce mappage, vous pouvez voir la couverture des règles de détection dans votre organisation.

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture

Traduction automatique

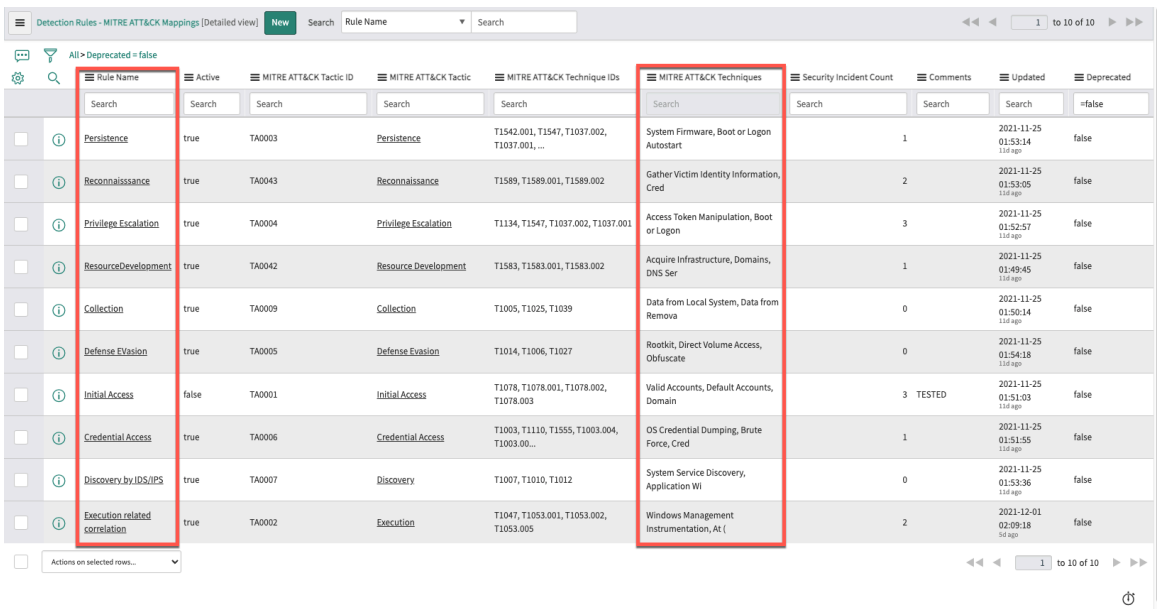
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Le mappage de règles de détection permet à votre organisation de voir quelles règles de détection sont disponibles pour identifier des techniques spécifiques.

L'objectif principal du mappage est de fournir une visibilité si votre organisation dispose des règles de détection nécessaires pour identifier quand une alerte ou un événement est déclenché à la suite d'une attaque par un adversaire à l'aide d'une technique spécifique.

Par exemple, consultez l'illustration suivante qui montre une liste des règles de détection mappées à diverses techniques. Vous pouvez également afficher ces informations dans le ou la MITRE-ATT&CK navigateur.



Si vous n'avez pas l'intention d'utiliser les règles d'extraction automatique SIEM du système de base, activez le déploiement automatique des TTP en fonction du mappage de règles de MITRE-ATT&CK détection. Vous pouvez renseigner l'alerte ou la règle d'événement qui déclenche l'incident de sécurité dans le champ Nom de la règle d'alerte . Vous pouvez également renseigner le champ Nom de la règle d'alerte à l'aide de l'intégration SIEM, de l'analyse des e-mails, de la création manuelle, et autres. Pour plus d'informations, consultez Informations sur le MITRE-ATT&CK déploiement à partir des règles de détection.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

La fonctionnalité de règles de détection a été mise à jour pour inclure le mappage d'une seule tactique à plusieurs techniques. Auparavant, vous pouviez cartographier une seule tactique avec une seule technique. Si vous mettez à niveau le module d'extension de la Renseignements sur les menaces version 12.0.4 vers une version supérieure, passez en revue les points suivants avant d'utiliser les règles de détection dans MITRE-ATT&CK le module.

- Vous trouverez plusieurs enregistrements fusionnés en un seul enregistrement si les champs Nom de la règle, Capteur d'alerte, Source, Catégorie, Sous-catégorie et MITRE-ATT&CK Tactique sont communs.
- Les anciens enregistrements sont marqués comme vrai dans la colonne déconseillée et faux dans la colonne active.
- Les nouveaux enregistrements fusionnés sont disponibles pour utilisation et sont marqués comme faux dans la colonne déconseillée et vrai dans la colonne active.
- Après avoir vérifié la mise à niveau et constaté que toutes vos règles de détection sont correctement migrées, vous pouvez supprimer les anciens enregistrements marqués comme vrais dans la colonne Déconseillée.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Règles de détection : Mappages MITRE ATT&CK**.
2. Utilisez l'une des méthodes suivantes pour créer votre règle de détection :
   Méthode 1 : créer manuellement des règles de détection.
   a. Cliquez sur **Nouveau** puis, renseignez les champs du formulaire.

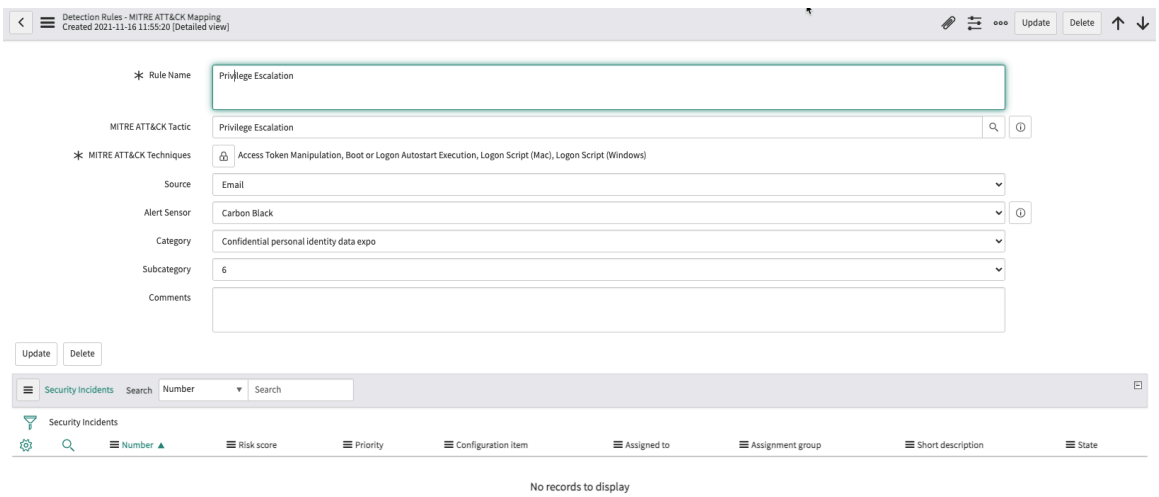
Règles de détection : MITRE-ATT&CK mappage

Champ	Description
Nom de la règle	Nom de la règle de détection.
MITRE-ATT&CK Tactique	Tactique pertinente MITRE-ATT&CK .
MITRE-ATT&CK Techniques techniques	Technique pertinente MITRE-ATT&CK . Vous pouvez sélectionner plusieurs techniques pour une seule tactique.
Source	Source de l'incident de sécurité, comme l'e-mail, le pare-feu, la surveillance du réseau, etc.
Capteur d'alerte	Intégration de sécurité par laquelle vous ingérez les données d'alerte ou d'événement, par exemple CarbonBlack, CrowdStrike, McAfee, etc.
Sous-catégorie	Sous-catégorie qui précise le problème.
Catégorie	Catégorie qui identifie le type de problème de sécurité.
MITRE-ATT&CK Technique	Technique pertinente MITRE-ATT&CK . Vous pouvez sélectionner plusieurs techniques pour une seule tactique.
Nombre d'incidents de sécurité	Nombre d'incidents de sécurité auxquels les techniques sont ajoutées. Ce nombre apparaît

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	lorsque vous avez activé le déploiement automatique des informations des règles d'alerte vers les incidents de MITRE-ATT&CK sécurité.
Déconseillé	Le mappage de règle de détection est obsolète.
Actif	Option permettant de spécifier si la règle de détection est active et déployée dans votre environnement.



b. Cliquez sur **Envoyer**.

Méthode 2 : importez et créez des règles de détection.

a. Cliquez avec le bouton droit sur l'en-tête de colonne Nom de la règle.

b. À partir de la liste, cliquez sur **Importer**.

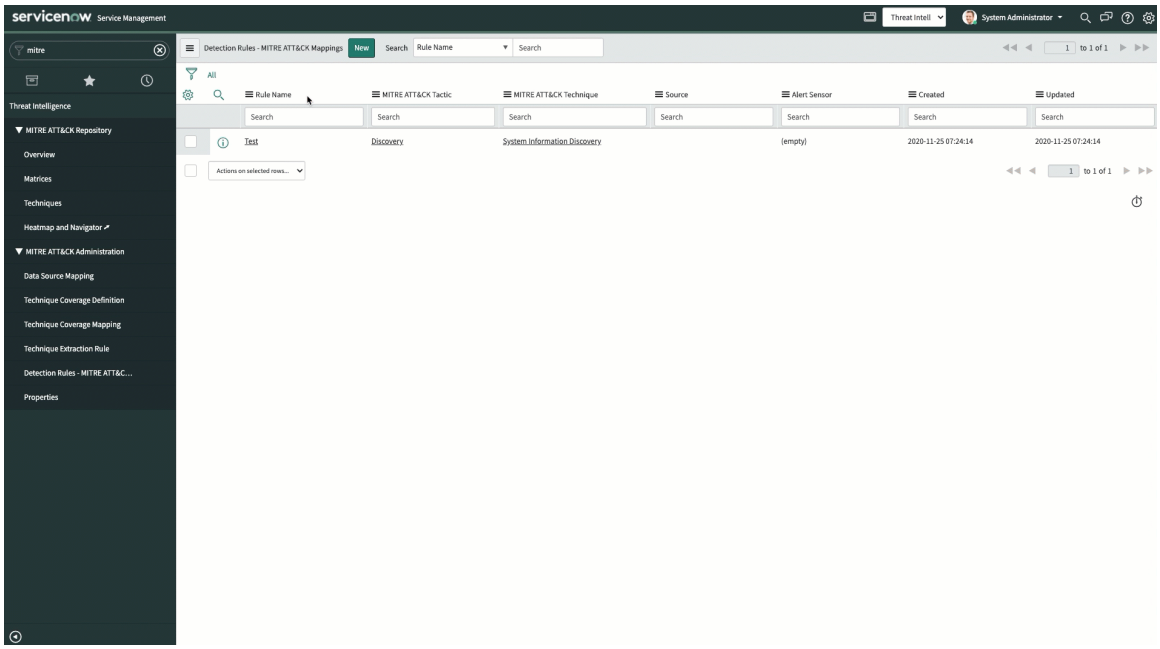
c. Cliquez sur **Créer un modèle Excel**.

d. Cliquez sur **Télécharger** une fois l'exportation terminée. Un modèle Excel contenant le nom de fichier sn_ti_alert_rules_mitre_attack_technique_mapping est téléchargé sur votre ordinateur.

Dans l'illustration suivante, vous verrez comment exporter le modèle Excel, renseigner les détails dans la feuille de calcul, charger le fichier, prévisualiser les champs et le réimporter dans le ServiceNow AI Platform.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



e. Ouvrez la feuille de calcul, sélectionnez le deuxième onglet de feuille et vérifiez ce que vous avez saisi. Renseignez les champs du formulaire, puis enregistrez votre fichier.

Importer un modèle

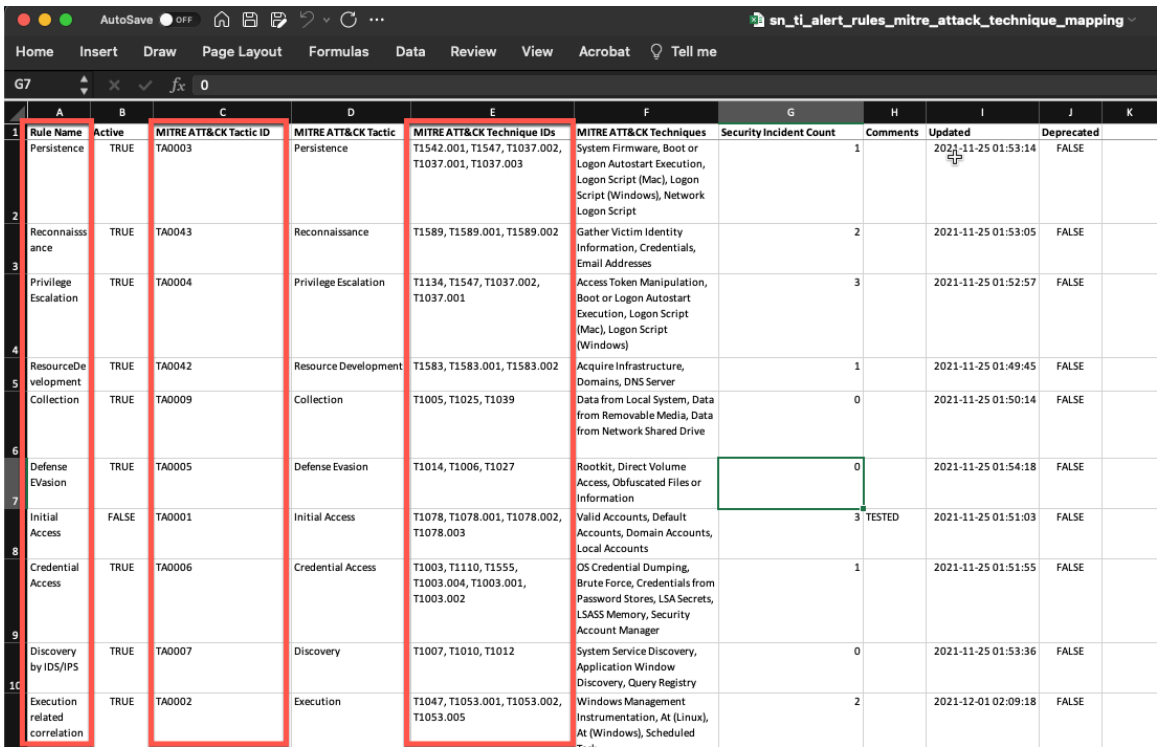
Champ	Description
Nom de la règle	Nom de la règle de détection.
Actif	Option permettant de spécifier si la règle de détection est active et déployée dans votre environnement.
Capteur d'alerte	Intégration de sécurité par laquelle vous ingérez les données d’alerte ou d’événement, par exemple CarbonBlack, CrowdStrike, McAfee, etc.
Catégorie	Catégorie qui identifie le type de problème de sécurité.
Commentaires	Description de la règle de détection.
Déconseillé	Le mappage de règle de détection est obsolète.
MITRE-ATT&CK ID de la technique	MITRE-ATT&CK ID de technique, tel que T1546.008, pour les fonctionnalités d’accessibilité.
MITRE-ATT&CK ID tactique	MITRE-ATT&CK ID tactique, tel que TA0003, pour Persistance.
Nombre d'incidents de sécurité	Nombre d’incidents de sécurité auxquels les techniques sont ajoutées. Ce nombre apparaît lorsque vous avez activé le déploiement automatique des informations des règles d’alerte vers les incidents de sécurité et que la règle de MITRE-ATT&CK détection est active.
Source	Source de l’incident de sécurité, comme l’e-mail, le pare-feu, la surveillance du réseau, etc.
Sous-catégorie	Sous-catégorie qui précise le problème.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
MITRE-ATT&CK Tactique	Tactique pertinente MITRE-ATT&CK .
MITRE-ATT&CK Technique	Technique pertinente MITRE-ATT&CK .

L'illustration suivante montre le modèle de feuille de calcul. Les champs requis sont surlignés en rouge : nom de la règle, MITRE-ATT&CK ID de tactique et MITRE-ATT&CK ID de technique.



Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated
Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE
Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE
Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE
ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE
Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE
Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE
Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE
Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE
Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE
Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE

f. Cliquez sur **Choisir un fichier** et sélectionnez la feuille de calcul sur votre ordinateur.

g. Cliquez sur **Charger**.

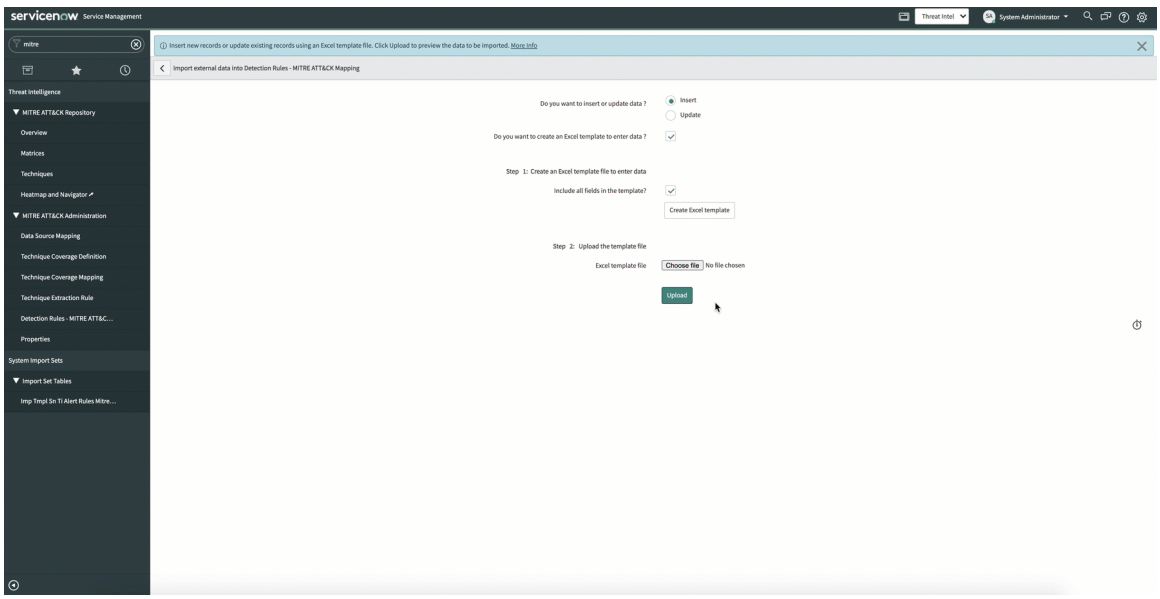
h. Cliquez sur **Afficher un aperçu des données importées**.

i. Prévisualisez les mappages et cliquez sur **Terminer l'importation**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'illustration suivante montre comment charger la feuille de calcul, prévisualiser les données, examiner les erreurs éventuelles et terminer le processus d'importation du mappage de règle de détection.



Règles de la technique d'extraction automatique pour l'importation d'informations MITRE-ATT&CK

Utilisez les règles d'extraction automatique du système de base pour importer les informations à partir de n'importe MITRE-ATT&CK quelle intégration tierce existante.

Utiliser les règles d'extraction automatique de la recherche de menaces

Utilisez les règles d'extraction automatique de la recherche de menaces pour importer les MITRE-ATT&CK informations à partir de toute intégration tierce existante Renseignements sur les menaces .

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

Lorsqu'une Renseignements sur les menaces intégration, telle que Sandbox ou TIP, prend en charge le cadre de MITRE-ATT&CK travail et si les informations sont analysées à chaque niveau d'intégration MITRE-ATT&CK , les informations sont affichées dans chaque enregistrement de résultat de recherche de menace. Cependant, toutes les Renseignements sur les menaces intégrations n'analysent pas les MITRE-ATT&CK informations. La règle d'extraction automatique globale de la recherche de menaces peut extraire MITRE-ATT&CK des informations de toutes les Renseignements sur les menaces intégrations.

Vous pouvez choisir de déployer automatiquement les MITRE-ATT&CK informations des résultats de la recherche de menaces vers un incident de sécurité. Pour le déploiement automatique des résultats de la recherche de menaces sur les incidents de sécurité, activez la propriété système. Vous pouvez également déployer les informations manuellement pour chaque recherche de menace.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le système Renseignements sur les menaces de base extrait automatiquement les informations de la MITRE-ATT&CK charge utile brute des intégrations tierces vers l'enregistrement de résultat de la recherche de menace, si l'intégration Renseignements sur les menaces vous fournit des MITRE-ATT&CK informations telles que la technique ou la tactique.

Si les MITRE-ATT&CK informations ne sont pas disponibles dans le champ de charge utile brute de l'enregistrement de recherche de menace, vous devez définir votre propre règle d'extraction automatique à partir de l'intégration tierce.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Règle d'extraction de la technique**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Règle d'extraction de technique

Champ	Description
Nom	Nom de la règle d'extraction automatique.
Type de règle	Type de règle d'extraction automatique. Sélectionnez **Recherche de menace**.
Ignorer l'extraction automatique	Le paramètre par défaut est effacé. Ce paramètre permet l'extraction automatique des MITRE-ATT&CK techniques.
Moteur source	Moteur source.
Global	Paramètre du moteur source. Lorsque vous définissez le moteur source sur **Global**, l'extraction s'exécute sur tous les résultats d'intégration de la recherche de menaces.
Description	Description de la règle d'extraction automatique.
Méthode de traitement	Regex ou méthode de script que vous spécifiez pour lier les informations de la technique à partir de la charge utile brute.
Extraction Regex	Option que vous spécifiez pour le **champ cible** lors de l'utilisation de la méthode d'extraction regex. Regex est la valeur par défaut.
Extraction de script	Processus que vous sélectionnez lors de l'exécution d'un script. Le script passe en revue les éléments suivants : ○ threatLookupResultSysId : sys_id de l'enregistrement du résultat de la recherche de menace ○ sourceName : nom de la source de recherche de menace.
Extraction tactique	Option que vous spécifiez pour extraire des informations liées à la tactique de la charge utile brute. Si une charge utile contient des informations spécifiques liées à des tactiques et à des techniques,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	vous pouvez extraire les informations et les annexer à l'incident de sécurité.

4. Cliquez sur **Envoyer**.

Utiliser les règles d'extraction automatique SIEM

Utilisez les règles d'extraction automatique SIEM pour importer les MITRE-ATT&CK informations à partir de toutes les intégrations tierces SIEM existantes Opérations de sécurité .

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture

Pourquoi et quand exécuter cette tâche

La règle d'extraction technique est disponible pour toutes les intégrations SIEM du système Opérations de sécurité de base telles que Splunk, IBM QRadar et ArcSight. Lorsque l'utilisateur ingère des données d'alerte ServiceNow AI Platform ou d'événement à partir de ces intégrations SIEM et qu'elles contiennent MITRE-ATT&CK des informations, traite ServiceNow AI Platform la charge utile brute et extrait automatiquement les MITRE-ATT&CK informations.

Si votre ServiceNow AI Platform contient des intégrations SIEM du système de base, cela signifie que les règles d'extraction de technique sont déjà créées dans le MITRE-ATT&CK module. Vous devez examiner et modifier les règles selon vos besoins.

Activer la règle d'extraction automatique SIEM ou la règle d'alerte à la fois.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Règle d'extraction de la technique**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

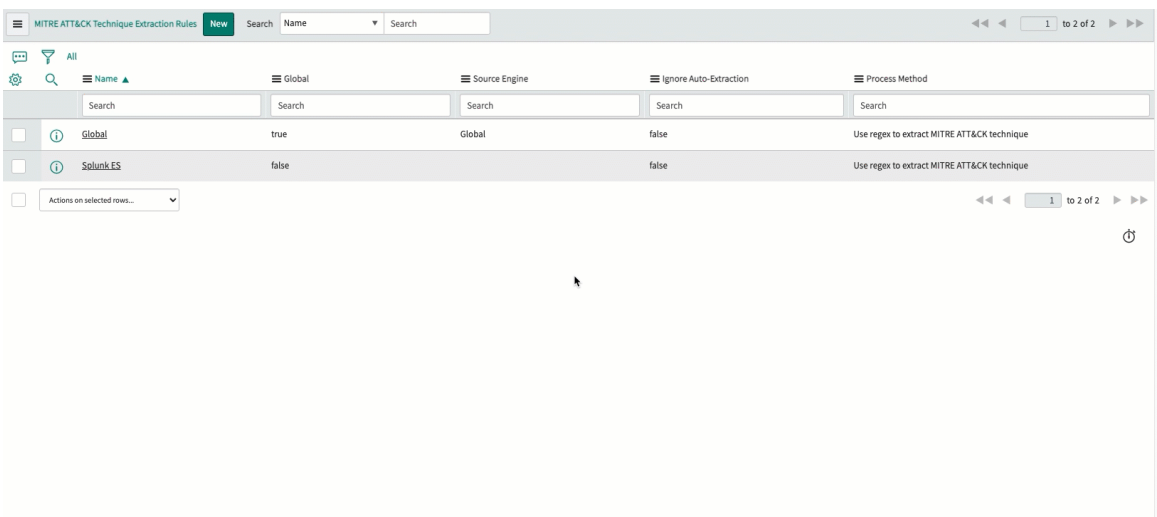
Formulaire Règle d'extraction de technique

Champ	Description
Nom	Nom de la règle d'extraction automatique.
Type de règle	Type de règle d'extraction automatique. Sélectionnez **SIEM**.
Ignorer l'extraction automatique	Le paramètre qui est effacé par défaut. Ce paramètre permet l'extraction automatique des MITRE-ATT&CK techniques.
Importer la table	Table d'importation automatiquement mappée pour les intégrations SIEM du système de base. Examinez ce champ pour d'autres intégrations SIEM pour obtenir des informations et mappez MITRE-ATT&CK en conséquence.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Champ d'importation	Champ d’importation automatiquement mappé pour les intégrations SIEM du système de base. Examinez ce champ pour d’autres intégrations SIEM pour obtenir des informations et mappez MITRE-ATT&CK en conséquence.
Description	Règle d’extraction automatique.
Méthode de traitement	Regex ou méthode de script que vous spécifiez pour lier les informations de la technique à partir de la charge utile brute.
Extraction Regex	Option que vous spécifiez pour le **champ cible** lors de l’utilisation de la méthode regex. L’extraction regex est la méthode de processus par défaut.
Extraction de script	Méthode de traitement de script que vous utilisez si vous souhaitez personnaliser la façon dont les MITRE-ATT&CK informations sont extraites.
Extraction tactique	Option que vous spécifiez pour extraire des informations liées à la tactique de la charge utile brute. Si une charge utile contient des informations spécifiques liées à des tactiques et à des techniques, vous pouvez extraire les informations et les annexer à l’incident de sécurité.

Dans l’illustration suivante, vous voyez un exemple de règle d’extraction de la Splunk Enterprise technique SIEM dans la vue de formulaire. Cette règle est similaire à toutes les autres règles d’extraction de technique SIEM.



4. Cliquez sur **Envoyer**.

Examiner le mappage des groupes de menaces et MITRE-ATT&CK des techniques

Passez en revue les informations de mappage des relations objet à objet des groupes de menaces et des techniques importées à partir des MITRE TAXII collections. Ce mappage vous permet d’afficher le groupe de techniques et le mappage de technique correspondant.

Avant de commencer

Rôle requis :

Traduction automatique

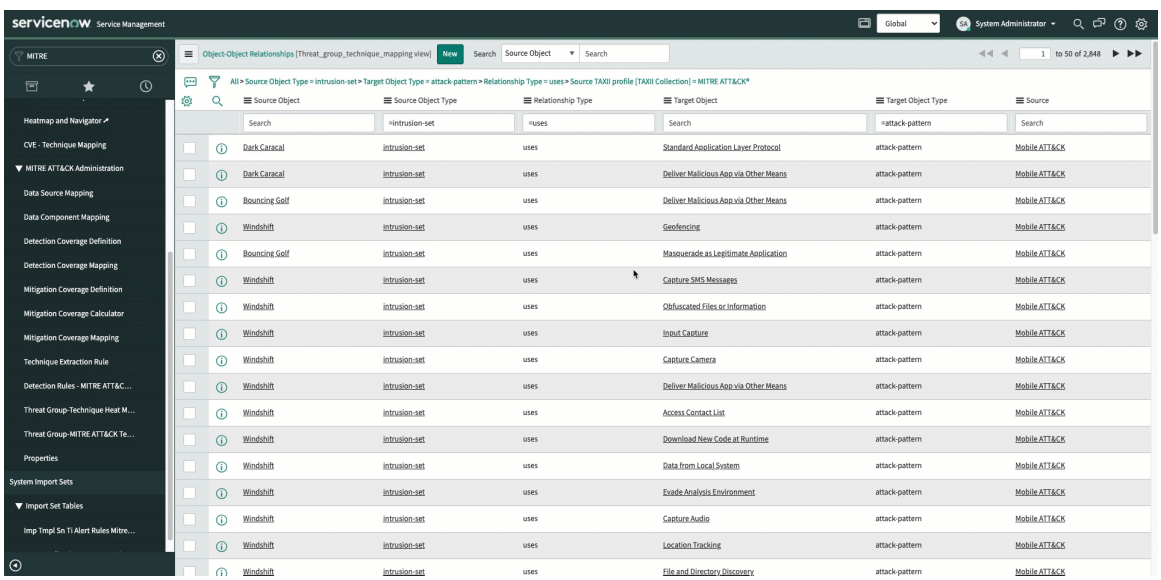
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_ti.admin, sn_si.admin : créer, écrire, supprimer l'accès
- sn_ti.read : accès en lecture

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Groupe de menaces : techniques MITRE ATT&CK**.
2. Cliquez avec le bouton droit sur **l'objet source** , puis sélectionnez **Grouper par objet source** pour afficher tous les schémas d'attaque associés à un groupe de menaces.

   L'illustration suivante montre le groupe de menaces admin@338 et les différents modèles d'attaque adoptés par ce groupe de menaces qui font partie de la source d'attaque de l'entreprise.



Groupe de menaces à définition de carte thermique de technique

Définissez le groupe de menaces par rapport à la définition de la carte thermique de la technique afin de pouvoir mesurer et détecter les schémas d'attaque que les groupes de menaces utilisent pour attaquer votre organisation. La probabilité d'une attaque utilisant une technique particulière augmente lorsque vous avez un nombre élevé d'attaquants.

Avant de commencer

Rôle requis :

- sn_ti.admin, sn_si.admin : accès en écriture
- sn_ti.read : accès en lecture

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Groupe de menaces : définition de la carte thermique de la technique**.
2. Passez en revue le groupe de menaces à la définition de la carte thermique de la technique et personnalisez les entrées pour votre environnement.

Traduction automatique

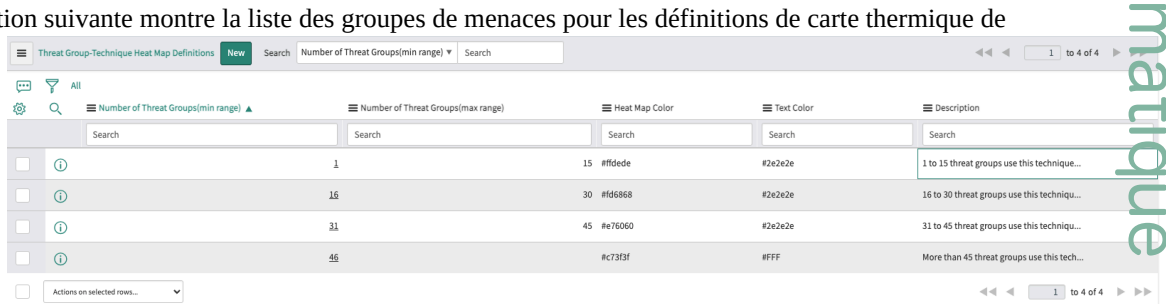
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Groupe de menaces : définitions de la carte thermique de la technique

Champ	Description
Nombre de groupes de menaces (plage minimale)	Le nombre minimal de groupes de menaces utilisant une technique particulière.
Nombre de groupes de menaces (plage maximale)	Nombre maximal de groupes de menaces utilisant une technique particulière. La probabilité d'une attaque utilisant une technique particulière augmente lorsque vous avez un nombre élevé d'attaquants.
Couleur de carte thermique	Couleur affectée à la catégorie de groupe de menaces. La couleur que vous définissez est utilisée pour mettre en surbrillance la catégorie de groupe de menaces dans la carte thermique. Vous pouvez personnaliser les couleurs à l'aide de codes HEX et de valeurs RVB(A).
Couleur du texte	Couleur affectée au texte du groupe de menaces. La couleur que vous définissez permet de mettre en évidence les groupes de menaces dans la carte thermique. Vous pouvez personnaliser les couleurs à l'aide de codes HEX et de valeurs RVB(A).
Description	Description de la portée et de la définition du groupe de menaces.

Remarque : Assurez-vous de ne pas chevaucher les plages de nombre de groupes de menaces si vous personnalisez la plage de groupes de menaces (minimale ou maximale).

L'illustration suivante montre la liste des groupes de menaces pour les définitions de carte thermique de technique.



3. Pour ajouter une entrée, cliquez sur **Nouveau**, remplissez les entrées, puis cliquez sur **Soumettre**.

Passer en revue les MITRE-ATT&CK propriétés système

Examinez les valeurs des propriétés système MITRE-ATT&CK .

Avant de commencer

Rôle requis : sn_ti.admin, sn_si.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration MITRE ATT&CK** > **Propriétés**.
2. Remplissez les champs du formulaire.

MITRE-ATT&CK Formulaire Propriétés

Champ	Description
Déployer automatiquement les informations MITRE ATT&CK à partir des observables vers l'incident de sécurité [sn_ti.rollup_mitre_att&ck_technique_observable_si]	Déploiement des MITRE-ATT&CK informations depuis les observables vers l'incident de sécurité. Pour plus d'informations, consultez Associer des informations MITRE ATT&CK à des observables. Valeur par défaut : oui
Déployer automatiquement les informations MITRE ATT&CK à partir des résultats de la recherche de menace vers l'incident de sécurité [sn_ti.rollup_mitre_att&ck_technique_threat_lookup_si]	Déploiement des informations depuis les résultats de MITRE-ATT&CK la recherche de menaces vers l'incident de sécurité. Pour plus d'informations, consultez Extraction automatique de la recherche de menaces. Valeur par défaut : oui
Déployer automatiquement les informations MITRE ATT&CK à partir des règles d'alerte vers les incidents de sécurité [sn_ti.rollup_mitre_att&ck_technique_alert_rule_si]	Déploiement automatique des informations TTP MITRE-ATT&CK des règles d'alerte vers les incidents de sécurité. Pour plus d'informations, consultez Règles de détection de carte. Valeur par défaut : non
Déployer automatiquement les informations MITRE ATT&CK à partir des incidents de sécurité enfants vers l'incident de sécurité parent [sn_ti.rollup_mitre_att&ck_technique_child_si_si]	Déployer automatiquement les informations des incidents de sécurité enfants vers l'incident MITRE-ATT&CK de sécurité parent. Valeur par défaut : oui
L'activation de cette propriété permet de mapper les champs d'incident de sécurité tels que la catégorie et la sous-catégorie avec les règles de détection dans la table « Règles de détection : mappage MITRE ATT&CK » [sn_ti.enable_category_mapping_with_alert_rule]	Catégorie et sous-catégorie sur la page de mappage Règles de détection - MITRE ATT&CK . Valeur par défaut : non
Temps (en heures) pour calculer « CVE : nombre de VUL » [sn_ti.time_to_calculate_cve_vits_count]	Temps planifié, en heures, pour calculer les informations CVE et VUL. Valeur par défaut : 24

3. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation MITRE-ATT&CK pour détecter et analyser les menaces

Utilisez le MITRE-ATT&CK cadre de travail dans le Renseignements sur les menaces module pour détecter et analyser les SIR menaces qui pèsent sur votre organisation.

Associer des MITRE-ATT&CK™ informations à des incidents de sécurité

Associez les MITRE-ATT&CK tactiques et techniques à l'incident de sécurité pour une meilleure analyse des incidents de sécurité et des menaces.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Ajoutez les MITRE-ATT&CK informations sur les tactiques et les techniques à l'incident de sécurité afin de pouvoir corréler vos informations sur l'incident de sécurité et les menaces pour une meilleure analyse. Par exemple, votre organisation peut recevoir des informations relatives aux tactiques, techniques et procédures (TTP) de la part de sources tierces, telles que Renseignements sur les menaces des rapports ou d'autres sources en dehors du Réponse aux incidents de sécurité. Vous ajoutez ensuite ces informations pour SIR améliorer la corrélation et l'analyse des menaces.

Vous pouvez choisir de déployer MITRE-ATT&CK les informations automatiquement à partir des résultats d'extraction automatique de la recherche de menaces, à partir d'observables ou d'un incident de sécurité enfant vers un incident de sécurité. Pour le déploiement automatique sur les incidents de sécurité, activez la propriété système. Vous pouvez également déployer les informations manuellement pour chaque recherche de menace ou observable.

Procédure

1. Accédez à la **Tous** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez enrichir avec les MITRE-ATT&CK informations.
3. Cliquez sur le lien connexe **Associer la technique MITRE ATT&CK** .
   Le volet Associer la technique MITRE ATT&CK s'affiche.

   Cette illustration montre comment accéder à la liste connexe et rechercher Associer MITRE-ATT&CK une technique, examiner l'ATT&CK d'entreprise source, ajouter un impact tactique et ajouter une technique d'arrêt/redémarrage du système.

   Associer des informations MITRE à un incident de sécurité
4. Sélectionnez **la source**.

   Remarque : Seules les collections et matrices activées apparaissent dans la liste source.

   Les tactiques et techniques associées à la source peuvent être sélectionnées. Vous pouvez également associer plusieurs sources.
5. Sélectionnez la **tactique** et les **techniques**.
6. **Facultatif :** Examinez les informations en fonction de leur pertinence par rapport à l'incident de sécurité et procédez comme suit :
   - Pour supprimer complètement l'association, cliquez sur l'icône de la corbeille. Cliquez sur cette icône pour supprimer la source et ses tactiques et techniques associées.
   - Pour supprimer une tactique, cliquez sur l'icône moins en regard de celle-ci.
   - Pour supprimer une technique, cliquez sur l'icône x en regard de la technique.
7. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Les MITRE-ATT&CK informations sont associées à l'incident de sécurité. Vous pouvez maintenant visualiser les informations associées dans la **carte MITRE ATT&CK**.

Associer des MITRE-ATT&CK informations à des incidents de sécurité clôturés

Vous pouvez désormais associer MITRE-ATT&CK des tactiques et des techniques aux incidents de sécurité fermés pour une meilleure analyse des incidents de sécurité et des menaces.

Associer des informations MITRE à un incident de sécurité

Utilisation de la carte pour afficher les MITRE-ATT&CK informations connexes dans un incident de sécurité

Vous pouvez utiliser la MITRE-ATT&CK carte pour afficher les MITRE-ATT&CK informations connexes dans un incident de sécurité.

Une fois que les informations ont été déployées à partir d'une recherche de menace, d'un observable ou d'une intégration SIEM, elles sont ajoutées à l'incident de sécurité. Ensuite, les informations agrégées sont présentées dans la MITRE-ATT&CK carte. La **carte MITRE ATT&CK** offre deux vues :

- Vue du navigateur : cette vue, qui est similaire au MITRE-ATT&CK navigateur, affiche toutes les techniques qui ont été ajoutées ou déployées manuellement à partir des tables de recherche d'observables ou de menaces. **Afficher l'origine des techniques** Affiche la source de la technique si elle a été déployée manuellement ou via une source. **Afficher l'ID** affiche l'ID de la technique.

  L'illustration suivante montre comment accéder à la vue **du navigateur de carte MITRE ATT&CK** . En cliquant sur l'un des liens disponibles, les informations s'ouvrent dans le Renseignements sur les menaces module.

  Carte MITRE ATT&CK : vue Navigateur et Vue Liste

- Vue de listes : cette vue affiche les données sous forme de liste ou de tableau. Vous pouvez afficher toutes les données réparties dans différentes tables et groupes dans cette vue.

  L'illustration suivante montre comment accéder à la vue de liste de cartes MITRE ATT&CK. En cliquant sur l'un des liens disponibles, les informations s'ouvrent dans le Renseignements sur les menaces module.

Associer des MITRE-ATT&CK informations à des observables

Associez MITRE-ATT&CK des tactiques et des techniques à un observable pour une meilleure analyse des incidents de sécurité et des menaces à un niveau granulaire.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Certains SIEM peuvent fournir des MITRE-ATT&CK informations avec des événements, des alertes ou des observables. Pour associer les MITRE-ATT&CK informations à un niveau granulaire, vous pouvez ajouter les informations avec un observable.

Vous pouvez choisir de déployer automatiquement les MITRE-ATT&CK informations des observables vers un incident de sécurité. Pour le déploiement automatique des observables dans les incidents de sécurité, activez la propriété système. Vous pouvez également déployer les informations manuellement pour chaque observable.

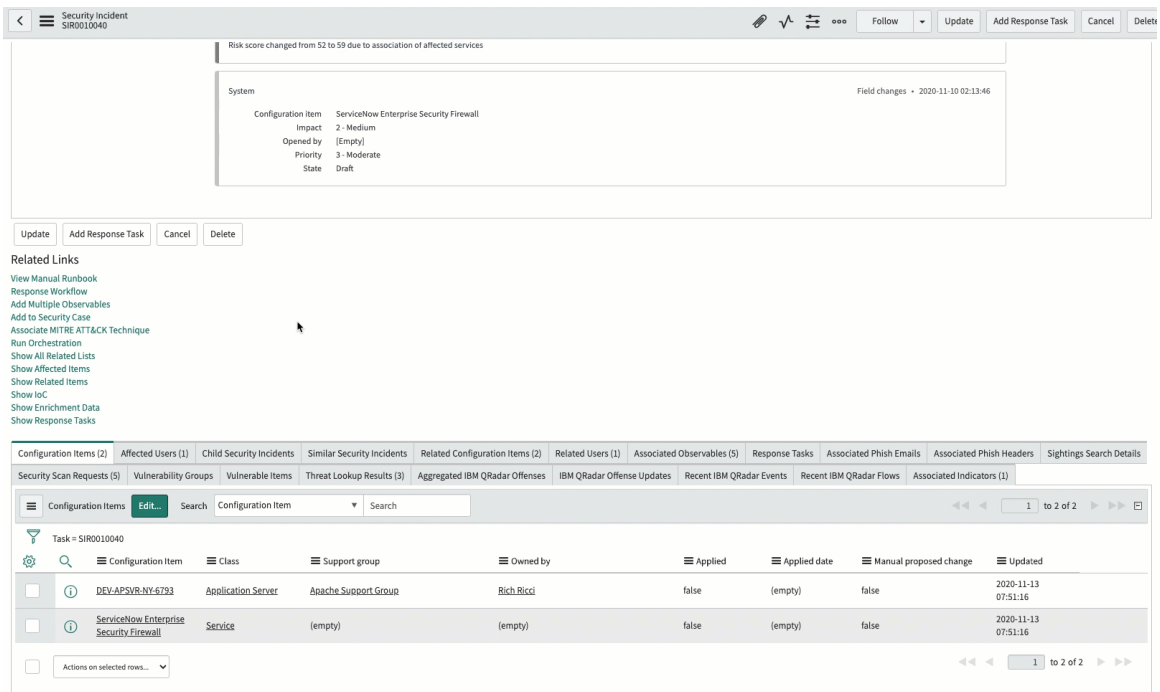
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez enrichir avec les MITRE-ATT&CK informations.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Pointez sur l'observable que vous souhaitez associer, cliquez avec le bouton droit de la souris et sélectionnez **Associer la technique MITRE ATT&CK**.

   Dans l'illustration suivante, vous pouvez voir comment naviguer à partir de la liste connexe pour **associer la technique MITRE ATT&CK**, examiner la source et ajouter une tactique et une technique.



5. Dans les listes de sources, examinez la **source**.

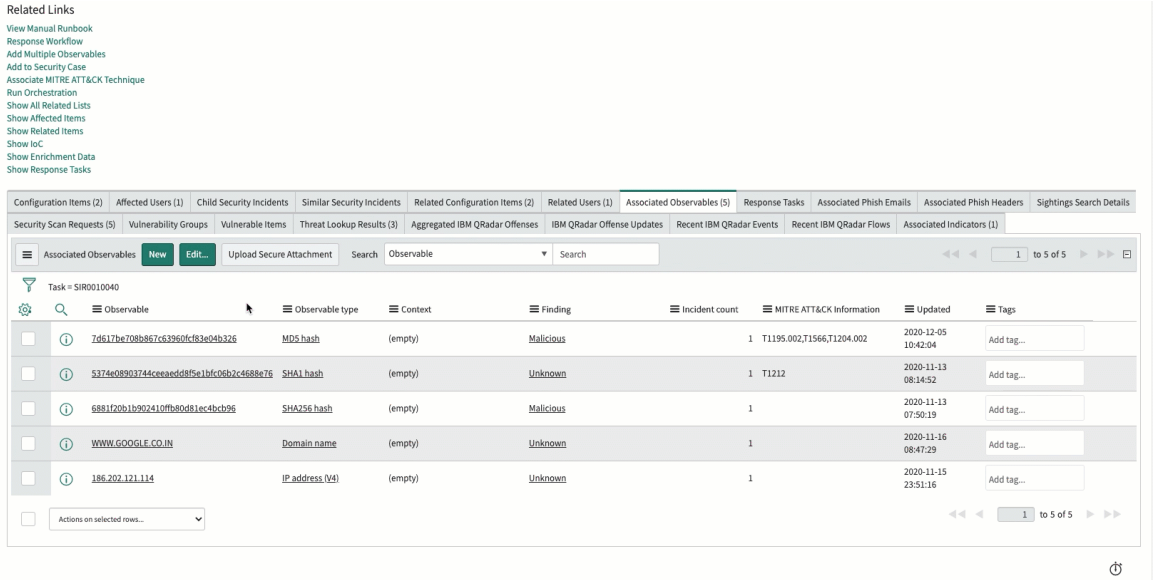
   Remarque : Seules les collections et matrices activées apparaissent dans la liste source.

6. Passez en revue la **tactique** et les **techniques**, et ajoutez-les ou supprimez-les en fonction de leur pertinence avec l'observable.
7. Cliquez sur **Enregistrer**.
   Les tactiques et techniques que vous avez ajoutées apparaissent dans la MITRE-ATT&CK colonne Informations de la liste connexe Observables.
8. Sélectionnez l'observable, puis dans le menu Actions, cliquez sur **Déployer les informations MITRE ATT&CK sur SI.**
   Si vous avez activé Déploiement automatique de MITRE-ATT&CK Informations des observables vers l'incident de sécurité, les informations sont automatiquement déployées. Si vous n'avez pas activé le déploiement automatique, vous devez le faire manuellement.

   L'illustration suivante montre comment sélectionner un observable et déployer les MITRE-ATT&CK informations dans un incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Pour afficher une vue agrégée des techniques associées aux observables, sélectionnez deux observables ou plus dans la liste, puis dans le menu **Actions** de la liste des lignes sélectionnées, cliquez sur **Afficher les informations MITRE ATT&CK**.

Résultats

Une vue agrégée des informations MITRE ATT&CK pour les observables sélectionnés s'affiche.

Associer les MITRE-ATT&CK informations au ticket de sécurité

Associez MITRE-ATT&CK des tactiques et des techniques à un ticket de sécurité pour une meilleure gestion des tickets de sécurité et une meilleure analyse des menaces à un niveau granulaire.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
2. Sélectionnez le ticket de sécurité que vous souhaitez enrichir avec les informations MITRE-ATT&CK.
3. Dans la liste connexe, cliquez sur **Associer la technique MITRE ATT&CK**.

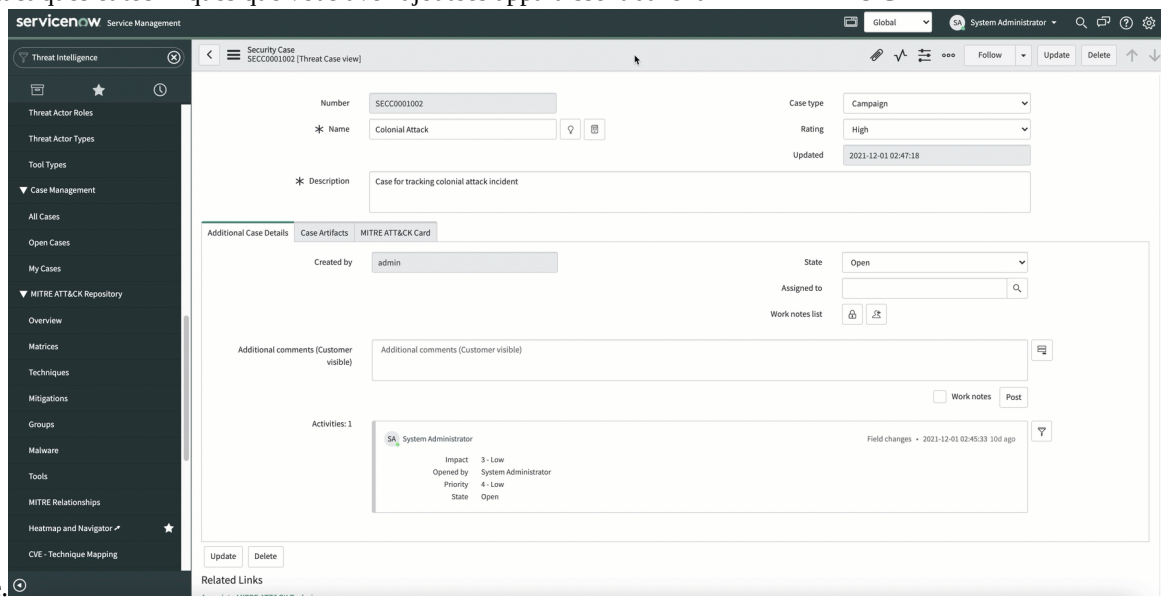
   Dans l'illustration suivante, vous pouvez voir comment naviguer à partir de la liste connexe pour **associer la technique MITRE ATT&CK**, examiner la source et ajouter une tactique et une technique.

4. Dans les listes de sources, examinez la **source**.
5. Passez en revue la **tactique** et les **techniques**, et ajoutez-les ou supprimez-les en fonction de leur pertinence avec le ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Enregistrer**.
   Les tactiques et techniques que vous avez ajoutées apparaissent dans la MITRE-ATT&CK carte.



Déployer les MITRE-ATT&CK informations à l'aide des résultats de la recherche de menace

Si vous n'avez pas activé le déploiement automatique des MITRE-ATT&CK informations, vous pouvez le faire manuellement.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Si vous avez activé Déploiement automatique de MITRE-ATT&CK informations issues des résultats de la recherche de menace vers l'incident de sécurité, les informations sont automatiquement déployées. Si vous n'avez pas activé le déploiement automatique, vous pouvez le faire manuellement.

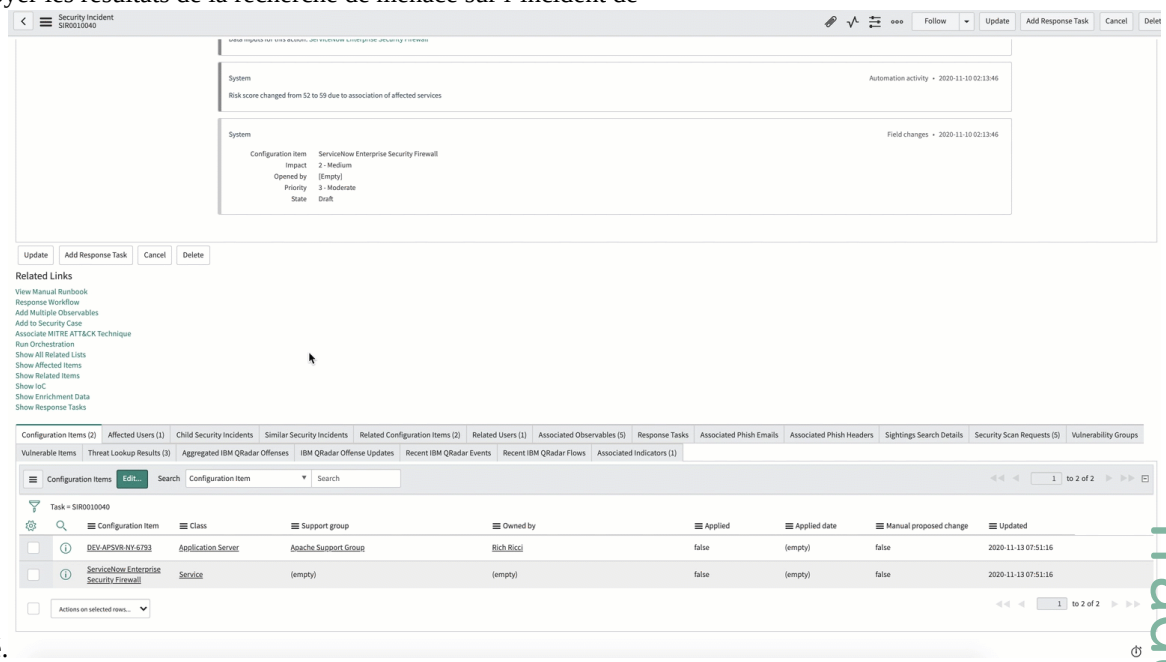
Procédure

1. Accédez à la **Tous** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez enrichir avec les MITRE-ATT&CK informations.
3. Cliquez sur **Afficher toutes les listes connexes** et sur **l'onglet Résultats de la recherche de menaces** .
4. Sélectionnez l'observable, puis dans le menu Actions, cliquez sur **Déployer les informations MITRE ATT&CK sur SI.**
   Vous pouvez sélectionner plusieurs observables et déployer les informations.
5. Cliquez sur **Recharger** pour confirmer les modifications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’illustration suivante montre comment sélectionner un observable et déployer les résultats de la recherche de menace sur l’incident de sécurité.



Vous pouvez afficher la MITRE-ATT&CK carte pour confirmer que les résultats de la recherche de menaces ont été déployés sur l’incident de sécurité.

Informations sur le MITRE-ATT&CK déploiement à partir des règles de détection

Activez le déploiement des informations des règles de détection vers les incidents de sécurité pour une meilleure analyse des incidents de sécurité et des MITRE-ATT&CK menaces.

Avant de commencer

Rôle requis : aucun.

Assurez-vous d’avoir effectué les actions suivantes :

- Activez automatiquement le déploiement des informations MITRE ATT&ACK des règles d’alerte vers la propriété Incidents de sécurité dans le module Propriétés . Par défaut, cette option est désactivée. Pour plus d’informations, consultez Examiner les propriétés système MITRE-ATT&CK.
- Effectuez le mappage des règles de détection sur MITRE-ATT&CK les TTP dans le module de mappage Règles de détection - MITRE ATT&CK TTP . Le nom de la règle de détection doit correspondre au nom de la règle d’alerte qui déclenche l’incident de sécurité. Pour plus d'informations, consultez Créer et mapper des règles de détection.

Pourquoi et quand exécuter cette tâche

Si vous n’avez pas l’intention d’utiliser les règles d’extraction automatique SIEM du système de base, activez le déploiement automatique des TTP en fonction du mappage de règles de MITRE-ATT&CK détection. Vous pouvez renseigner l’alerte ou la règle d’événement qui déclenche l’incident de sécurité dans le champ Nom de la règle d’alerte . Vous pouvez également renseigner le champ Nom de la règle d’alerte à l’aide de l’intégration SIEM, de l’analyse des e-mails, de la création manuelle, etc.

Procédure

1. Accédez à la **Administration MITRE ATT&CK** > **Propriétés**.
2. Activez la propriété Déployer automatiquement les informations MITRE ATT&ACK des règles d’alerte aux incidents de sécurité, puis cliquez **sur Enregistrer**.

Traduction automatique

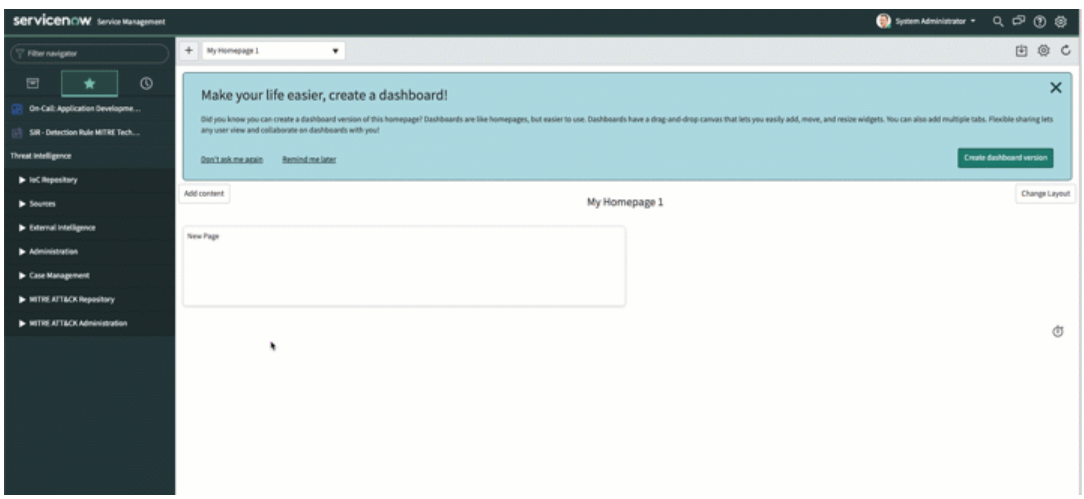
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, cette option est désactivée.

3. Vous devez renseigner le champ Nom de la **règle d'alerte** de l'incident de sécurité avec les règles d'alerte requises.

   Remarque : Assurez-vous d'ajouter le nom exact de la règle d'alerte . Pour ajouter plusieurs règles, vous devez les ajouter à l'aide d'un séparateur de virgules.

4. Cliquez avec le bouton droit sur le formulaire, puis cliquez sur **Enregistrer**.
   Si la valeur du nom de la règle d'alerte dans l'incident de sécurité correspond à un enregistrement dans le module de mappage Règle de détection - MITRE ATT&CK TTP, les techniques et tactiques correspondantes associées à la règle d'alerte sont automatiquement liées à l'incident de sécurité.



5. Ouvrez l'incident de sécurité, sélectionnez la **carte MITRE ATT&CK** et validez si les techniques sont déployées.
6. Activez **l'option Afficher l'origine des techniques** pour afficher l'origine des techniques.
   L'origine des techniques doit être la règle de détection.

Informations de MITRE-ATT&CK déploiement à partir des incidents de sécurité enfants

Si vous n'avez pas activé le déploiement automatique des MITRE-ATT&CK informations, vous pouvez le faire manuellement.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Si vous avez activé Déploiement automatique de MITRE-ATT&CK Informations provenant des incidents de sécurité enfants, les informations sont automatiquement déployées. Si vous n'avez pas activé le déploiement automatique, vous pouvez le faire manuellement.

Procédure

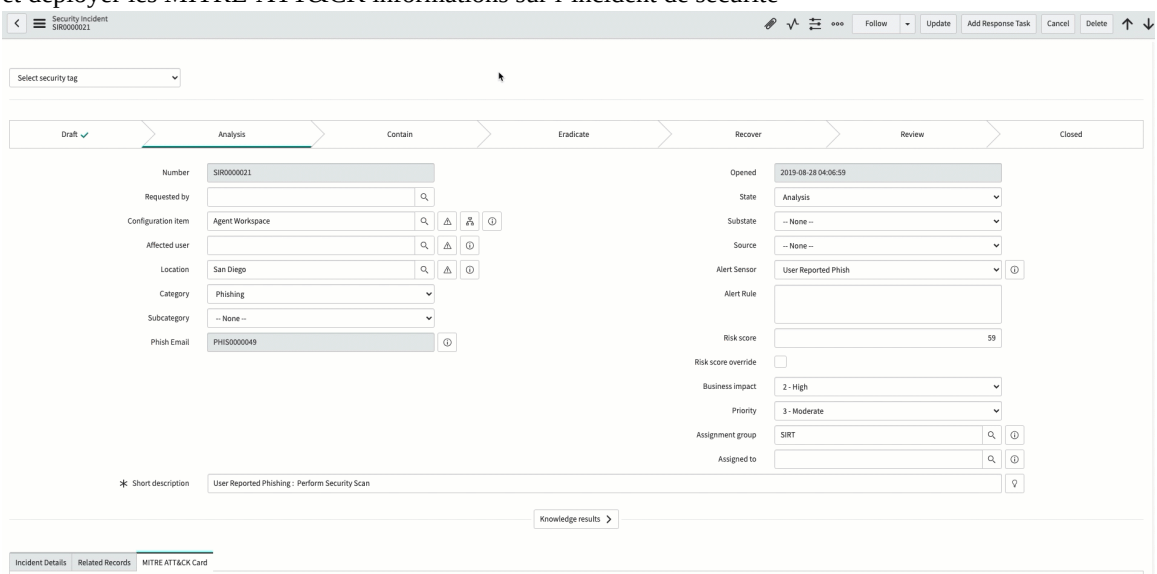
1. Accédez à la **Tous** > **Incidents** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité parent que vous souhaitez enrichir avec les informations enfants MITRE-ATT&CK .
3. Cliquez sur **Afficher toutes les listes connexes** et sur l'onglet **Incidents de sécurité enfants** .
4. Sélectionnez l'incident de sécurité enfant, puis, dans le menu Actions, cliquez sur **Déployer les informations MITRE ATT&CK sur** SI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez cliquer sur **Afficher les informations MITRE ATT&CK** pour afficher les informations MITRE de l'incident de sécurité enfant avant de déployer les informations MITRE ATT&CK.

5. Cliquez sur **Recharger** pour confirmer les modifications.
6. Cliquez sur la **carte MITRE ATT&CK** pour afficher l'origine des techniques. L'illustration suivante montre comment sélectionner un incident de sécurité enfant et déployer les MITRE-ATT&CK informations sur l'incident de sécurité parent.



Vous pouvez afficher la carte MITRE-ATT&CK pour confirmer que les informations relatives à l'incident MITRE-ATT&CK de sécurité enfant ont été déployées sur l'incident de sécurité parent.

Effectuez une analyse des liens et une chasse aux menaces à l'aide de MITRE-ATT&CK filtres spécifiques

Corrélez et analysez les liens des observables, des incidents de sécurité et MITRE-ATT&CK des informations connexes afin que votre organisation puisse commencer à rechercher les menaces.

Avant de commencer

Rôle requis : sn_ti.mitre_analyst, sn_si.read

Pourquoi et quand exécuter cette tâche

Une fois que vous avez associé les incidents de sécurité à MITRE-ATT&CK des informations, vous pouvez utiliser les filtres spécifiques pour la MITRE-ATT&CK chasse aux menaces. Utilisez les MITRE-ATT&CK filtres avec les filtres existants Réponse aux incidents de sécurité pour mettre en corrélation et effectuer une analyse de lien.

Procédure

1. Accédez à la **Tous** > **Incidents de sécurité** > **Afficher les incidents**.
2. Cliquez sur **Mettre à jour la liste personnalisée** pour ajouter les MITRE colonnes.
3. Sélectionnez une condition de filtre afin de pouvoir afficher MITRE les informations connexes et les associations avec les incidents de sécurité ou les observables :
   - MITRE-ATT&CK Groupe d'adversaires
   - MITRE-ATT&CK Source de données
   - MITRE-ATT&CK Procédure (programme malveillant)

Traduction automatique

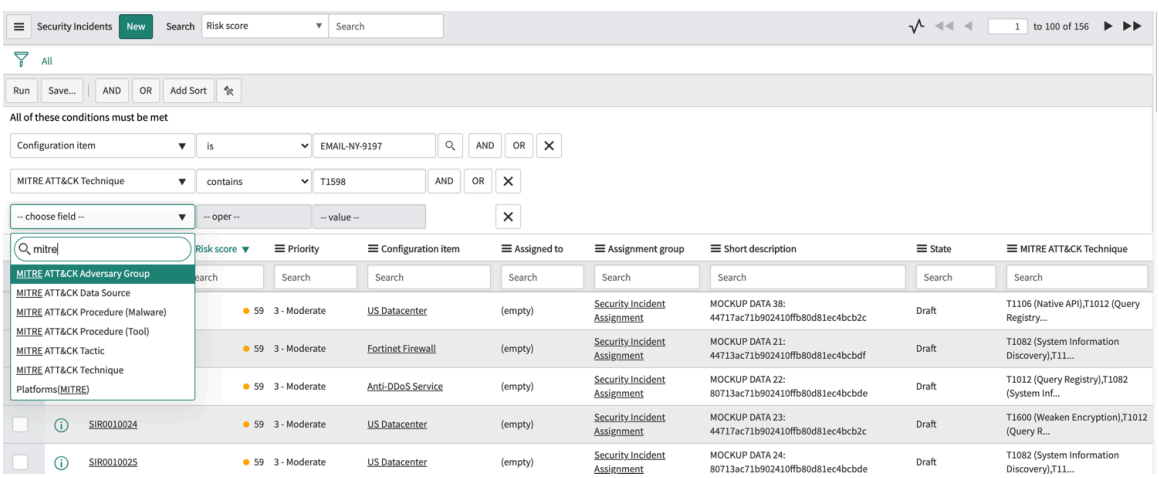
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- MITRE-ATT&CK Procédure (outils)
- MITRE-ATT&CK Tactique
- MITRE-ATT&CK Technique

4. Créez une condition de filtre basée sur les critères ci-dessus et cliquez sur **Exécuter** pour effectuer une analyse de lien ou une corrélation entre les incidents de sécurité, les observables et MITRE-ATT&CK les informations connexes.

   Remarque : Les MITRE-ATT&CK données sont stockées sous forme de chaîne et vous ne pouvez utiliser **« contient** » que comme opérateur pour les conditions de filtre.

   Par exemple, si vous souhaitez vérifier qu'un élément de configuration (CI) est compromis, vous sélectionnez un CI. Vous corrélez ensuite le CI avec les techniques présentes en ajoutant un MITRE-ATT&CK ID de technique. Vous pouvez ensuite continuer à créer vos critères de filtre pour corréler les informations et pour la chasse aux menaces.



MITRE-ATT&CK Carte thermique et navigateur

Vous pouvez utiliser la carte thermique et le MITRE-ATT&CK navigateur pour la navigation de base et pour visualiser votre couverture globale de détection technique.

Vue d'ensemble de la carte thermique et du MITRE-ATT&CK navigateur

Vous pouvez utiliser le navigateur avec les filtres primaires pour la navigation de base et l'observation des matrices ATT&CK. La carte thermique met en évidence le spectre de la couverture de détection, y compris les angles morts pour lesquels votre organisation n'a aucune couverture. Cette option est disponible après avoir mappé la couverture de détection technique .

Avec la carte thermique et le navigateur, vous pouvez :

- Identifiez rapidement et efficacement les options de détection de votre organisation et mettez en évidence les lacunes dans la couverture de la détection technique.
- Recherchez les menaces et effectuez une corrélation des menaces à l'aide des fonctionnalités associées.

Accéder à la carte thermique et au MITRE-ATT&CK navigateur

Accédez à la carte thermique et au MITRE-ATT&CK navigateur afin de visualiser la matrice qui vous permet d'utiliser ATT&CK.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_ti.read, sn_ti.mitre_analyst

Pourquoi et quand exécuter cette tâche

Vous pouvez examiner la carte thermique, utiliser les filtres pour établir une corrélation et effectuer une analyse de lien des informations, des observables et des incidents de sécurité au sein de MITRE-ATT&CK votre organisation.

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Carte thermique et navigateur**.
   La carte thermique et le navigateur s'ouvrent dans un nouvel onglet.
2. Sélectionnez la source pour remplir la carte thermique.

   Remarque : Seules les collections et matrices activées apparaissent dans la liste source.

   Dans l'illustration suivante, vous verrez comment accéder à la carte thermique et au navigateur, et comment sélectionner la source, qui est Enterprise ATT&CK dans cet exemple.

   Accéder à la source pour remplir la carte thermique et la sélectionner
3. Utilisez la zone de recherche pour trouver rapidement une tactique ou une technique particulière à l'aide de son nom ou de son ID.

   L'illustration suivante montre comment rechercher une tactique, une technique ou toute information qu'ils contiennent. Utilisez la recherche pour explorer rapidement une tactique ou une technique spécifique.
4. Cliquez sur **Filtres** et sélectionnez un filtre dans les filtres Primaire ou Avancé .
5. Cliquez sur **Appliquer et contrôlez** les filtres comme suit :
   - Pour enregistrer vos filtres, créez une vue personnalisée. Vous pouvez créer et enregistrer trois vues personnalisées.
   - Pour supprimer les filtres sélectionnés, cliquez sur **Restaurer les filtres par défaut** pour charger votre vue enregistrée par défaut.
   - Pour effacer tous les filtres et votre vue existante, cliquez sur **Effacer tous les filtres**.

   Remarque : Les vues que vous enregistrez sont spécifiques pour un utilisateur.
6. Cliquez sur **Masquer les sous-techniques** pour supprimer toutes les sous-techniques de la vue de la carte thermique.
   Si une technique comporte des sous-techniques, vous pouvez cliquer sur l'icône de développement pour afficher les sous-techniques.

Utilisation des vues personnalisées

Les vues personnalisées de la carte thermique et du MITRE-ATT&CK navigateur vous aident à enregistrer et à afficher vos filtres préférés la prochaine fois que vous atterrissez sur la carte thermique.

Remarque : Vous pouvez créer et enregistrer trois vues personnalisées pour chaque MITRE-ATT&CK collection par utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une vue

Une fois que vous avez sélectionné les filtres requis à partir des filtres Primaire ou Avancé , cliquez sur le bouton avec des points de suspension (...) dans l'en-tête Filtres et sélectionnez **Créer une vue**. Entrez le nom de la vue personnalisée et **enregistrez la vue**.

Vues par défaut

Cliquez sur **Enregistrer ceci en tant que vue par défaut** pour charger directement la vue la prochaine fois que vous atterrirez sur la carte thermique. Vous pouvez définir une vue par défaut pour chacune des collections.

Remarque : Si vous mettez à niveau le module d'extension Renseignements sur les menaces à partir d'une version antérieure, votre vue par défaut existante à partir de l'ancienne version s'affiche sous la forme d'une vue personnalisée.

L'illustration montre comment créer une vue personnalisée dans la carte thermique

Mettre à jour une vue

Vous pouvez apporter des mises à jour à une vue personnalisée existante en modifiant les filtres Primaire ou Avancé requis. Sélectionnez une vue personnalisée, mettez à jour les filtres selon vos besoins, puis cliquez sur le bouton représentant des points de suspension (...) dans l'en-tête Filtres et sélectionnez **Mettre à jour la vue** pour enregistrer les filtres.

Cette illustration montre comment mettre à jour une vue personnalisée.

Gérer les vues personnalisées

Utilisez les cases à cocher en regard de chaque vue personnalisée pour appliquer le filtre de vue personnalisé sélectionné.

Cliquez sur le bouton avec des points de suspension (...) en regard de chaque nom de vue personnalisée pour contrôler les vues personnalisées comme suit :

- Définissez une vue par défaut.
- Supprimez une vue personnalisée comme vue par défaut. Cela ne supprime pas la vue personnalisée.
- Renommez la vue personnalisée.
- Supprimez la vue personnalisée.

Cette illustration montre comment gérer les vues personnalisées.

Exporter une vue enregistrée

Pour exporter les vues personnalisées enregistrées vers des fichiers JSON, cliquez sur des points de suspension (...) dans l'en-tête Filtres et sélectionnez **Exporter les vues enregistrées**. Cliquez sur l'icône de téléchargement de la vue personnalisée que vous souhaitez télécharger sur votre ordinateur local.

Cette illustration montre comment exporter des vues personnalisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer une vue

Vous ne pouvez importer que des fichiers JSON. Pour importer les vues personnalisées, cliquez sur le bouton avec des points de suspension (...) dans l'en-tête Filtres et sélectionnez **Importer la vue (json).**

Vérifiez les conditions suivantes lors de l'importation des vues :

- Vous ne pouvez importer que le format de fichier JSON.
- Vous ne pouvez importer qu'une seule vue ou un seul fichier à la fois.
- Vous ne pouvez pas importer si vous avez déjà trois vues personnalisées dans vos filtres. Supprimez une vue personnalisée et importez une vue.
- Vous ne pouvez pas importer une vue avec un nom de vue personnalisée existant. Renommez une vue avant de l'importer.

Cette illustration montre comment importer une vue.

Navigateur avec filtres primaires

Utilisez les filtres primaires pour filtrer les techniques dans le MITRE-ATT&CK navigateur. Les informations contenues dans le MITRE-ATT&CK référentiel peuvent être sélectionnées.

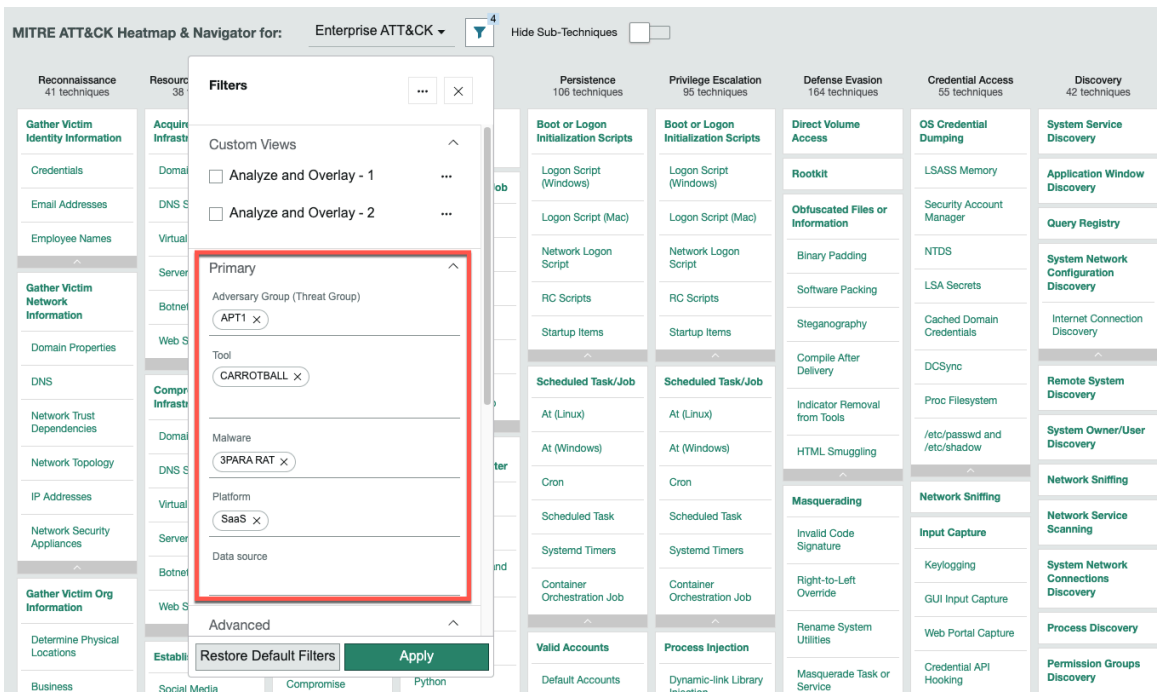
Filtre	Description
Groupe d'adversaires (groupe de menaces)	Ensembles d'activités d'intrusion connexes qui sont suivies par un nom commun dans la communauté de sécurité. Les groupes peuvent désigner divers groupes de menaces, groupes d'activités, acteurs de la menace, ensembles d'intrusion et campagnes. Vous pouvez ajouter plusieurs groupes au filtre **Groupe d'adversaires (groupe de menaces**). Par exemple, vous ajoutez APT1 et AT12 car les deux sont des groupes de menaces attribués à la Chine. Bien que les deux groupes puissent cibler des sources différentes, ils peuvent utiliser des techniques similaires.
Outil	Logiciel légitime utilisé par des acteurs de menace pour effectuer des attaques. Vous pouvez comprendre comment les acteurs de la menace exécutent les campagnes si vous savez comment et quels outils sont utilisés par les acteurs de la menace. Les outils comprennent à la fois les logiciels qui ne se trouvent pas sur un système d'entreprise et les logiciels disponibles dans le cadre d'un système d'exploitation déjà présent dans un environnement tel que les utilitaires Microsoft Windows. Par exemple, gsecdump est un dumper d'informations d'identification accessible au public que le groupe d'adversaires APT11 utilise pour obtenir des hachages de mot de passe et des secrets LSA (autorité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Filtre	Description
	de sécurité locale) à partir des systèmes d'exploitation Microsoft Windows.
Programme malveillant	Logiciel commercial, fermé personnalisé ou open source destiné à être utilisé à des fins malveillantes par des adversaires. Les exemples sont PlugX, CHOPSTICK, etc
Plateforme	Tactiques et techniques qui représentent MITRE-ATT&CK dans une plate-forme particulière. Par exemple, MITRE-ATT&CK prend en charge ces plateformes dans la matrice Enterprise ATT&CK : Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Réseau.
Source de données	Sources de données que vous collectez dans votre environnement et que vous utilisez pour détecter MITRE-ATT&CK des techniques. Par exemple, la surveillance des DLL et les extensions de navigateur.

L'illustration suivante montre tous les filtres primaires disponibles dans le MITRE-ATT&CK navigateur.



Utilisation d'une carte thermique avec des fonctionnalités primaires et avancées

Vous pouvez utiliser une carte thermique avec des filtres avancés pour effectuer une analyse en corrélant les incidents de sécurité avec MITRE-ATT&CK les informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les ID de la technique

Vous pouvez afficher les MITRE-ATT&CK ID de techniques avec les noms des techniques lorsque vous sélectionnez le filtre **Afficher les ID de techniques** .

Afficher les ID de techniques sur une carte thermique

Afficher les techniques pertinentes par priorité

Pour filtrer les techniques en fonction de leur priorité pertinente dans le navigateur, sélectionnez **Filtrer par filtre de priorité pertinent** de technique et sélectionnez la **priorité pertinente** dans le menu. Vous pouvez affecter plusieurs priorités au filtrage. Vous pouvez également pointer vers les techniques de la carte thermique pour connaître la priorité de la technique.

Les informations de priorité pertinentes sont basées sur la hiérarchisation que vous avez définie dans le champ Priorité pertinente des techniques .

Cette illustration montre le filtrage par priorité pertinente.

Afficher la couverture de détection technique

Pour afficher la couverture globale de détection de la technique dans la carte thermique, sélectionnez le filtre **Afficher la couverture de détection** de la technique. La carte thermique met en évidence le spectre visuel de la couverture de détection, y compris les angles morts où vous n'avez aucune couverture. La définition du score du système de base et les couleurs ont été définies dans la couverture de détection de technique. Les informations ont été extraites automatiquement de la couverture globale de détection technique.

Par exemple, les zones de la carte thermique marquées en rouge indiquent un manque de détection. Les zones marquées en bleu indiquent la présence de capacités de détection complètes. Les zones marquées en orange, jaune et bleu clair reflètent les options de détection partielle.

- La visualisation des couleurs est basée sur la définition de la technique et le codage couleur que vous définissez.
- La visualisation de la couverture est basée sur le mappage de couverture de détection de technique que vous définissez.
- Si vous modifiez la définition de couverture du système de base, les icônes Type de couverture ne s'affichent pas avec les techniques de la carte thermique.

> **Remarque :** La carte thermique fonctionne comme prévu lorsque vous modifiez les mêmes champs que la couverture de détection technique et les couleurs de couverture définies par le système de base.

Dans cette illustration, vous voyez la couverture de détection de technique pour toutes les techniques et sous-techniques et le type de couverture avec leurs couleurs et leurs icônes.

Couverture de détection technique de carte thermique

Afficher la couverture de l'atténuation de la technique

Pour afficher la couverture globale de l'atténuation de la technique dans la carte thermique, sélectionnez le filtre Afficher la couverture de l'atténuation de la technique. La carte thermique met en évidence le spectre visuel de la couverture d'atténuation, y compris les zones pour lesquelles vous n'avez aucune couverture. La couverture d'atténuation,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les couleurs et les plages de pourcentage ont été définies dans la définition de couverture d'atténuation. Les informations sont extraites de la couverture globale de l'atténuation de la technique.

Par exemple, les techniques surlignées en rouge indiquent qu'il n'y a pas de couverture d'atténuation, l'orange indique une mauvaise couverture d'atténuation et le bleu indique une excellente couverture d'atténuation.

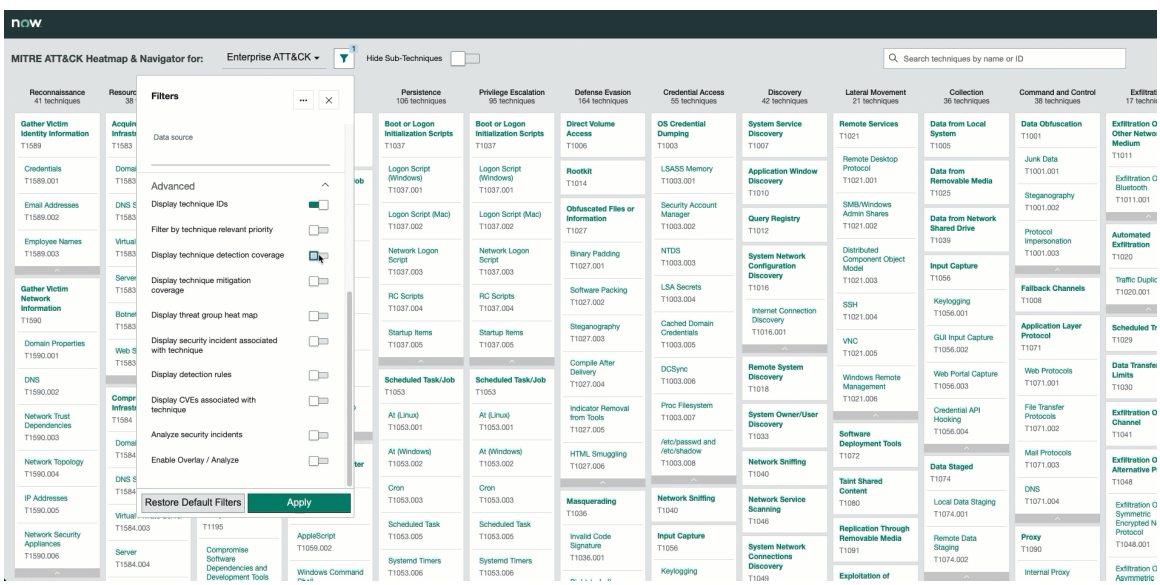
- La visualisation des couleurs est basée sur la définition d'atténuation de la technique et le code couleur que vous définissez.
- La visualisation de la couverture est basée sur le mappage de couverture d'atténuation technique que vous définissez.
- Si vous modifiez la définition de couverture d'atténuation du système de base, les icônes de type de couverture d'atténuation ne s'affichent pas avec les techniques de la carte thermique.

> **Remarque :** La carte thermique fonctionne comme prévu lorsque vous modifiez les mêmes champs que la technique, la couverture d'atténuation et les couleurs de couverture définies par le système de base.

Cette illustration montre la carte thermique de couverture d'atténuation de la technique

Afficher la couverture de détection et d'atténuation

Vous pouvez utiliser les filtres de détection de technique et de couverture d'atténuation de technique ensemble pour obtenir un aperçu de la pertinence de la détection de technique et de la couverture d'atténuation pour votre organisation.



Cette illustration montre comment utiliser le filtre de détection et le filtre d'atténuation.

Afficher le groupe de menaces

Pour afficher le groupe de menaces pour les informations de la technique sur la carte thermique, sélectionnez **Afficher la carte thermique du groupe de menaces**. Vous pouvez mesurer le nombre de groupes de menaces qui utilisent une technique particulière. La probabilité d'une attaque utilisant une technique particulière augmente lorsque vous avez un nombre élevé d'attaquants. Les plages de groupes de menaces et les couleurs de la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

carte thermique ont été définies dans la définition de la carte thermique Groupe de menaces - Technique.

- La visualisation des couleurs de la carte thermique et du texte est basée sur la définition du groupe de menaces à la carte thermique technique.
- La visualisation de la plage de groupes de menaces est basée sur le mappage du groupe de menaces à la technique.
- Vous ne pouvez pas utiliser le filtre **Afficher la carte thermique du groupe de menaces** lorsque la couverture de détection de technique ou la couverture d'atténuation de technique sont activées. Cette illustration montre les informations sur le groupe de menaces sur la carte thermique.

Afficher les incidents de sécurité associés à la technique

Pour afficher les techniques fréquemment exploitées dans votre organisation et qui ont entraîné des incidents de sécurité, cliquez sur **Afficher l'incident de sécurité associé à la technique**. Vous pouvez afficher plus d'informations sur chacun des incidents de sécurité associés lorsque vous cliquez sur le lien qui s'ouvre dans une nouvelle fenêtre d'analyse. Incidents de sécurité associés à une technique.

- Priorité : sélectionnez **Priorité d'incident de sécurité** pour filtrer par priorité d'incident de sécurité.
- Plage de dates : sélectionnez la **plage de dates de l'incident de sécurité** pour filtrer les problèmes de sécurité par plage de dates.
- Faux positifs : sélectionnez Filtrer les **incidents de sécurité faux positifs** pour supprimer les problèmes de faux positifs. La sélection de ce filtre réduit le nombre d'incidents de sécurité affichés sur la carte thermique.

Lorsque vous utilisez ce filtre avec le filtre **Afficher la couverture de détection** technique, vous obtenez un aperçu de la pertinence de la couverture de détection technique pour votre organisation jusqu'à la date sélectionnée.

Par exemple, lorsque vous activez les deux filtres, vous pouvez voir que sous la tactique d'évasion de défense, la technique de mascarade n'a aucune couverture. Si l'on regarde plus loin, la technique de mascarade est liée à la tâche ou au service de mascarade, qui est également associé à un incident de sécurité. Cela montre qu'il existe une lacune dans la couverture de la détection de technique pour la technique de masquage et que vous voudrez peut-être réviser la couverture globale de la détection de la technique.

Afficher les règles de détection

Pour afficher si les règles de détection sont définies pour une technique particulière, cliquez sur **Afficher les règles de détection**. Vous pouvez également consulter chaque règle de détection associée avec sa définition.

Ces informations sont basées sur le mappage de règles de détection que vous avez défini. Affichez les règles de détection associées.

Afficher les CVE associés à la technique

Pour afficher les informations CVE (Common Vulnerabilities and Exposures) associées à chacune des techniques, cliquez sur **Afficher les CVE associées à la technique**. Les informations sur les CVE à la technique sont basées sur les informations disponibles dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le module CVE - Technique Mapping. Cela vous donne un aperçu des vulnérabilités connues et vous permet de savoir si des adversaires peuvent potentiellement exploiter votre organisation.

Important : La carte thermique est améliorée pour afficher uniquement les CVE pertinents associés aux VIT

Pour afficher les VIT associés aux CVE et aux techniques, sélectionnez **Afficher les VIT associés aux CVE et aux techniques**. En outre, pour filtrer davantage les techniques sans VIT, sélectionnez **Masquer les techniques sans VIT**. Les informations CVE et VIT que vous affichez sont extraites du Réponse aux vulnérabilités produit dans votre environnement. Vous pouvez afficher la liste filtrée des CVE et des VIT dans la carte thermique et accéder à chaque CVE ou VIT pour chaque technique à partir de la carte thermique.

Remarque :

- **L'option Afficher les CVE associés à la technique** n'est disponible que lorsque le Réponse aux vulnérabilités produit est installé dans votre environnement.
- Les informations VIT et CVE sont calculées en fonction de la tâche planifiée que vous définissez dans le MITRE-ATT&CK Propriétés de. La tâche planifiée du système de base est définie sur 24 heures.

Lorsque vous utilisez ce filtre avec le filtre **Afficher l'incident de sécurité associé à la technique** , vous pouvez savoir si les vulnérabilités connues ont causé des incidents de sécurité dans votre organisation.

Vous pouvez afficher plus d'informations sur chaque CVE pour analyser si la CVE est pertinente pour votre organisation. Pour ce faire, affichez les éléments de vulnérabilité. Si des éléments de vulnérabilité sont créés, vous pouvez afficher plus d'informations sur toutes les informations de CI associées dans le Réponse aux vulnérabilités module. Vous pouvez également examiner la gravité et la priorité pour prendre des décisions éclairées. Examinez les CVE pour prendre des décisions éclairées.

Analyser les incidents de sécurité

Pour analyser les incidents de sécurité et examiner les techniques utilisées par un adversaire pour une attaque, cliquez sur **Analyser les incidents de sécurité**. Vous pouvez ajouter plusieurs incidents de sécurité à des fins d'analyse à l'aide de chaînes séparées par des virgules.

Ce filtre vous aide à analyser un incident de sécurité. Vous pouvez savoir pourquoi l'incident s'est produit, quelles techniques ont été exploitées, si des acteurs de menace connus étaient impliqués, si les acteurs de la menace ont utilisé une séquence particulière pour une attaque, etc. Étant donné que vous pouvez analyser plusieurs incidents de sécurité en même temps, vous pouvez corréler les informations pour voir s'ils sont liés ou s'il s'agit d'un incident isolé. Si les incidents de sécurité sont liés et que vous observez un schéma, vous pouvez examiner leur progression sur la chaîne de frappe pour arrêter l'attaque ou pour élaborer une stratégie de défense pour votre organisation.

Lorsque vous utilisez le filtre **Analyser les incidents de sécurité** avec des filtres primaires, tels qu'un **groupe d'adversaires**, vous pouvez corréler si des adversaires connus sont impliqués. Par exemple, lorsque plusieurs incidents de sécurité sont analysés, les techniques associées aux incidents de sécurité sont présentes sous la forme d'une chaîne de frappe. Lorsque vous chevauchez les informations avec l'adversaire, vous remarquerez un chevauchement entre les techniques associées à l'incident de sécurité et les techniques

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

associées à l'adversaire. Seules les informations sur la technique qui se chevauchent s'affichent si les deux filtres sont activés.

Analyser les incidents de sécurité

Utilisation de la superposition pour analyser les incidents de sécurité et les groupes d'adversaires

Utilisez le filtre **Activer la superposition/Analyser** pour visualiser le comportement de l'adversaire et analyser un ou plusieurs incidents de sécurité et corréler les informations pour voir si une attaque est un incident isolé ou une attaque coordonnée par un adversaire connu.

Par exemple, vous pouvez désormais afficher les incidents de sécurité et le comportement de la chaîne de frappe de l'adversaire dans la même vue. Cette vue fournit des informations de chevauchement qui vous informent de l'attaque et du comportement connu de l'adversaire. Cela vous permet de déterminer s'il s'agit d'une attaque isolée ou coordonnée par un adversaire connu.

L'activation du filtre d'analyse de superposition ignore tous les filtres primaires, à l'exception du filtre Groupe **d'adversaires** , et ignore le filtre avancé **Filtrer par priorité pertinente de technique** lors de la génération d'une vue.

Une fois que vous avez activé le filtre d'analyse de superposition, utilisez la palette de couleurs pour affecter des couleurs aux éléments suivants :

- Analyser l'incident de sécurité
- Groupe d'adversaires
- Superposition

L'illustration suivante montre que le groupe d'adversaires APT18 est réparti sur plusieurs techniques et tactiques dans la chaîne de frappe. L'analyse montre également qu'il existe trois techniques qui superposent le groupe d'adversaires et les incidents de sécurité que vous suivez. Cette illustration montre les informations de superposition de l'adversaire et de l'incident de sécurité.

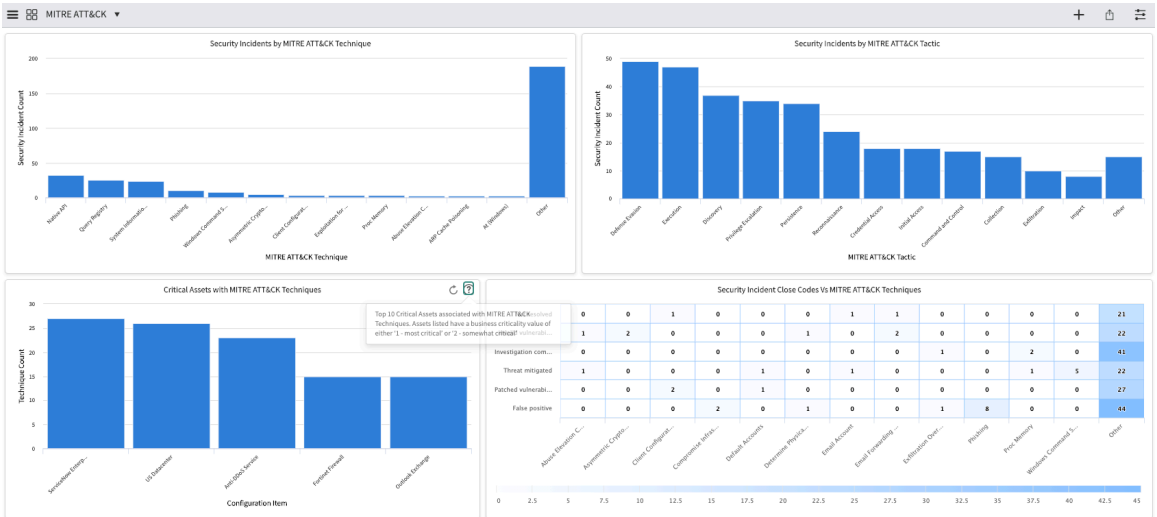
Utilisation du tableau de MITRE-ATT&CK bord

Le MITRE-ATT&CK tableau de bord fournit une vue exécutive de la couverture de la source de données, des tactiques et des techniques utilisées dans votre organisation.

Le MITRE-ATT&CK module Vue d'ensemble affiche MITRE-ATT&CK des informations sur les incidents de sécurité, y compris des tendances et des rapports. Vous pouvez cliquer sur n'importe quelle partie d'un widget (barre, point de données, table, etc.) pour afficher les données spécifiques à cette partie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Utilisez le tableau de bord pour afficher vos données liées à la MITRE-ATT&CK sécurité

Utilisez le MITRE-ATT&CK tableau de bord pour obtenir une vue d'ensemble de la couverture des sources de données, des tactiques et des techniques utilisées dans votre organisation.

Avant de commencer

Rôle requis : sn_si.ciso, sn_si.analyst, sn_si.manager, sn_ti.read

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Référentiel MITRE ATT&CK** > **Vue d'ensemble**.
2. Cliquez sur l'un des widgets suivants pour afficher des détails supplémentaires :
   - Incidents de sécurité par MITRE-ATT&CK technique
   - Incidents de sécurité par MITRE-ATT&CK tactique
   - Actifs critiques avec MITRE-ATT&CK techniques
   - Codes de fermeture des incidents de sécurité par rapport aux MITRE-ATT&CK techniques
   - Techniques MITRE-ATT&CK par couverture de détection
   - Techniques MITRE-ATT&CK par couverture d'atténuation
   - Groupes de menaces par technique MITRE-ATT&CK
   - CVE par technique MITRE-ATT&CK

Widgets MITRE-ATT&CK

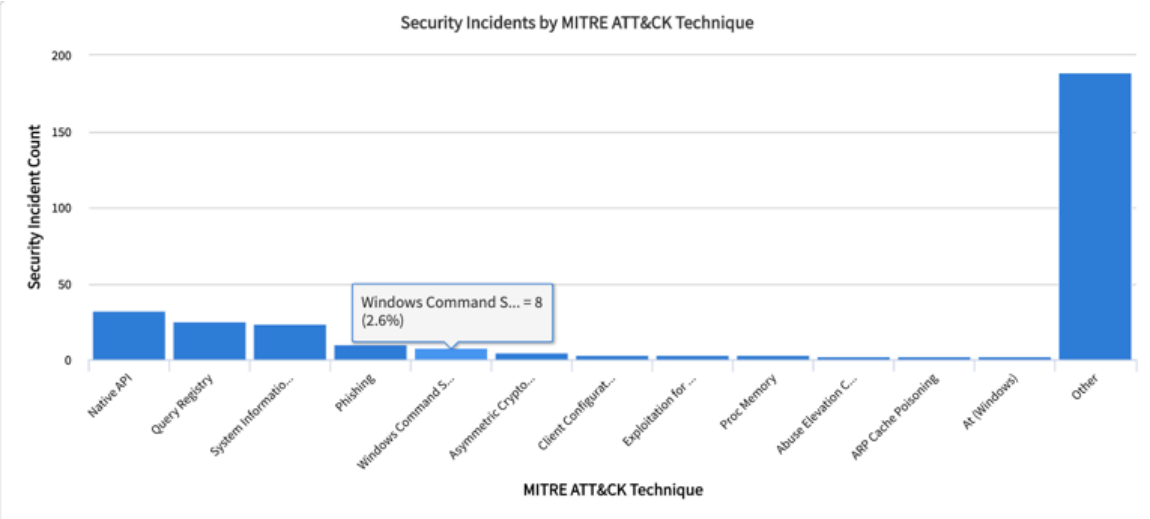
Le MITRE-ATT&CK module de vue d'ensemble se compose de widgets qui vous permettent de corréler les MITRE-ATT&CK informations avec les informations sur les incidents de sécurité de votre environnement.

Exemple d'incidents de sécurité par MITRE-ATT&CK technique

Dans cet exemple, le widget **Incidents de sécurité par technique MITRE ATT&CK** affiche les techniques par incident de sécurité dans l'environnement d'une organisation au cours des 90 derniers jours.

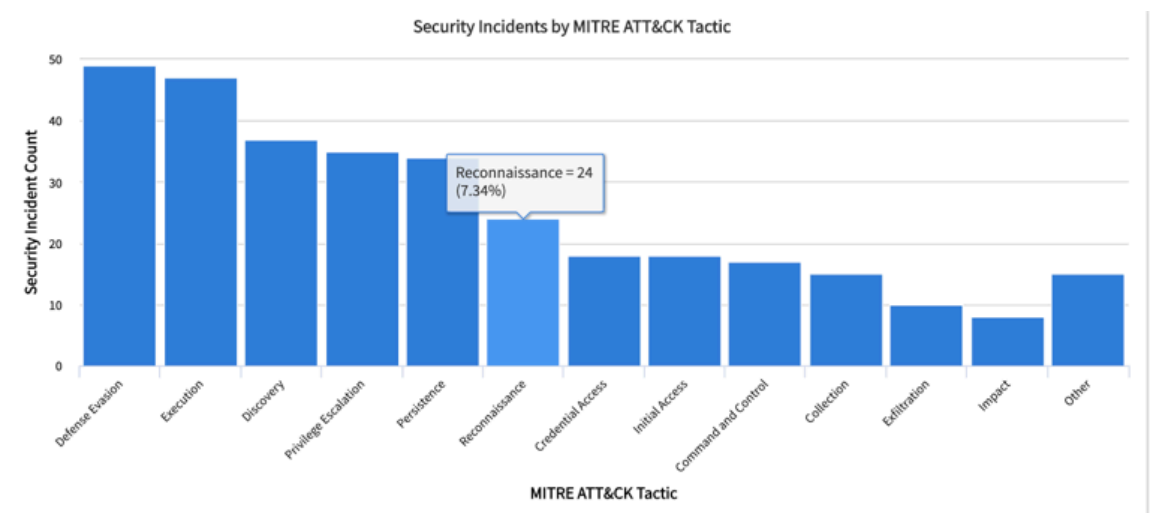
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple d'incidents de sécurité par MITRE-ATT&CK tactique

Dans cet exemple, le widget **Security Incidents by MITRE ATT&CK Tactic** affiche les principales tactiques par incident de sécurité dans l'environnement d'une organisation au cours des 90 derniers jours.



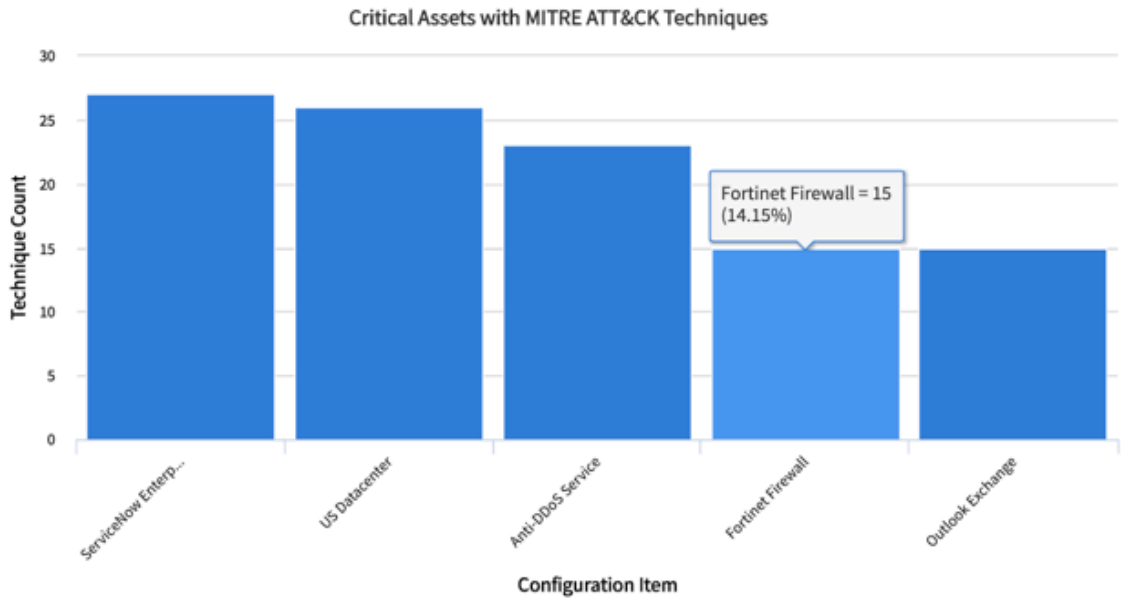
Exemple d'actifs critiques avec MITRE-ATT&CK techniques

Dans cet exemple, le widget **Actifs critiques avec techniques MITRE ATT&CK** affiche les 10 principaux actifs critiques associés aux MITRE-ATT&CK techniques. Les actifs ont une criticité opérationnelle de 1 (très critique) ou de 2 (assez critique).

Ce rapport permet à une organisation de voir les types et le nombre de techniques utilisées pour mener des attaques contre les actifs critiques.

Traduction automatique

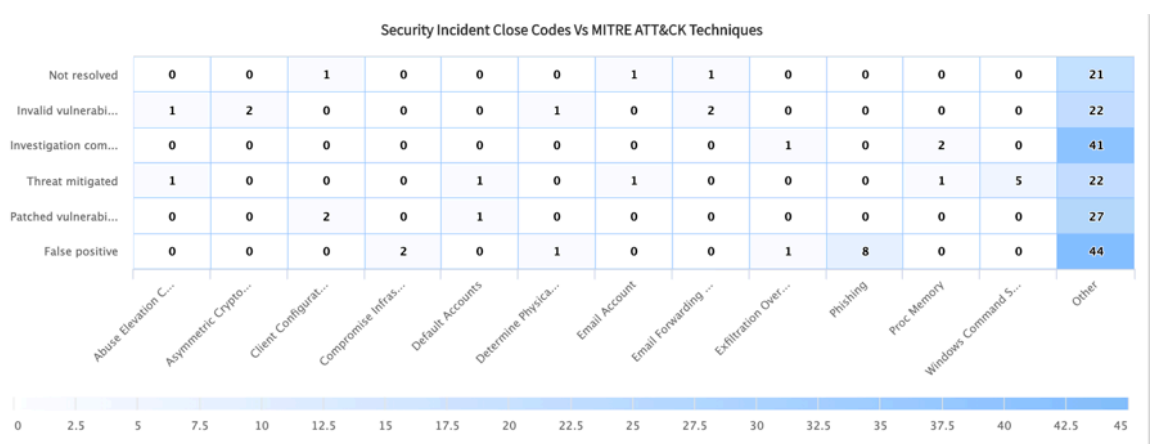
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple de codes de fermeture d'incidents de sécurité par rapport aux MITRE-ATT&CK techniques

Dans cet exemple, le widget **Codes de fermeture des incidents de sécurité par rapport aux techniques affiche les codes de fermeture des incidents de sécurité qui ont été mappés par rapport aux** *MITRE-ATT&CK* techniques principales identifiées dans l'environnement d'une organisation.

L'axe X affiche les principales techniques qui ont été utilisées pour mener des attaques contre l'entreprise et l'axe Y affiche les codes fermés.



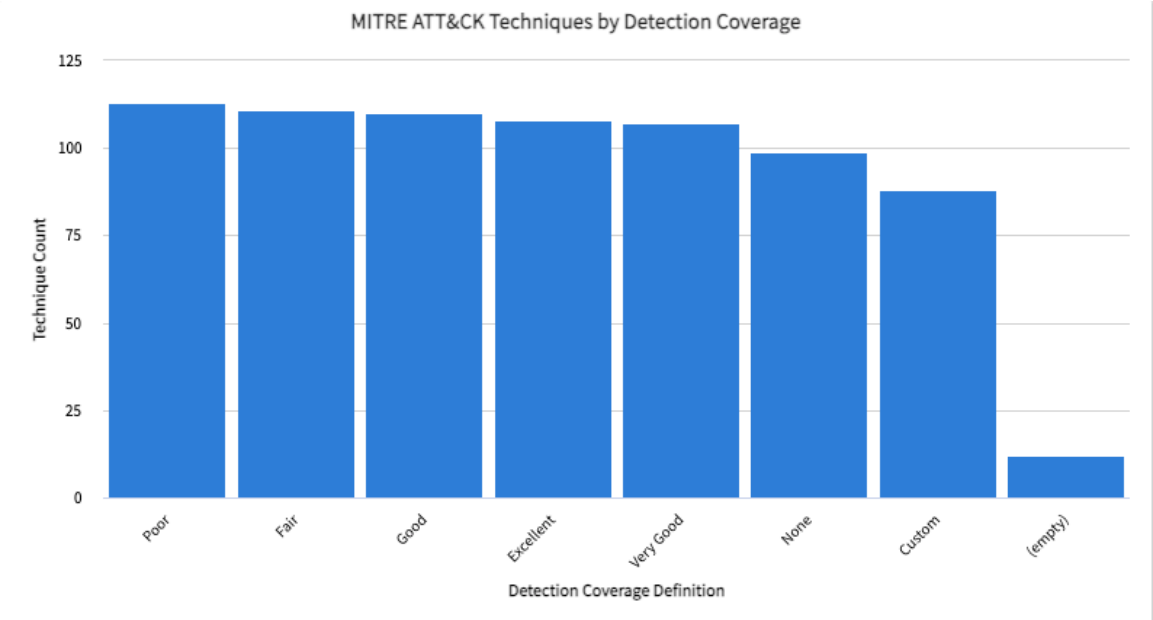
Exemple de couverture de détection par MITRE-ATT&CK techniques

Dans cet exemple, le widget **Techniques par couverture de détection MITRE-ATT&CK** affiche le nombre de techniques par couverture de détection dans votre environnement.

L'axe X affiche le nombre de techniques et l'axe Y affiche les types de couverture de détection.

Traduction automatique

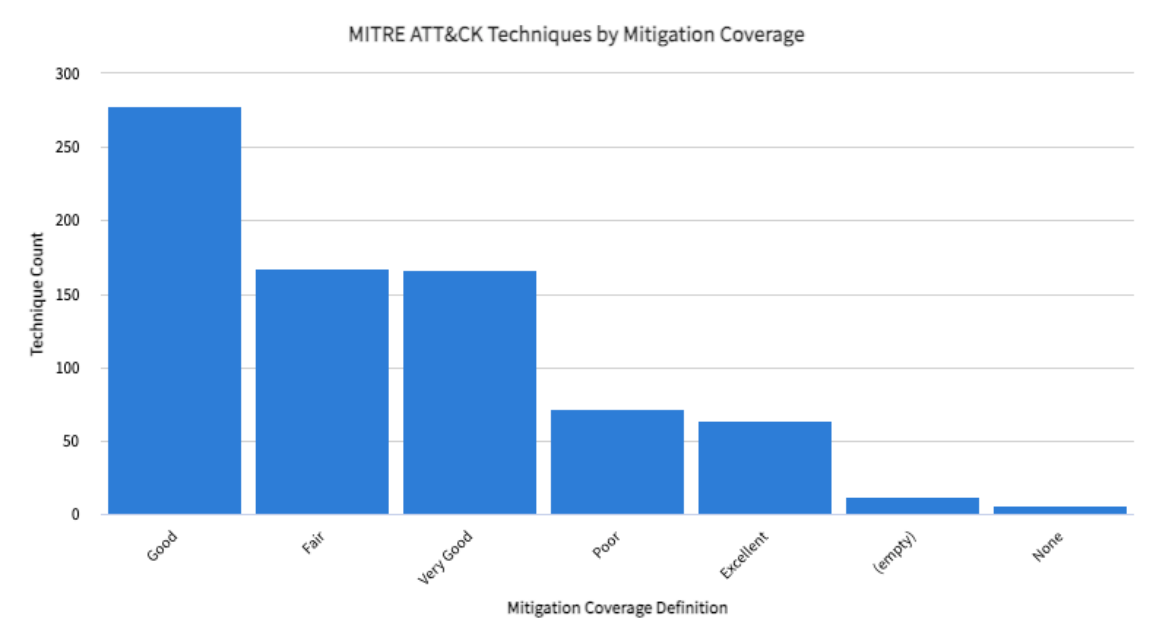
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple de couverture de l'atténuation par MITRE-ATT&CK techniques

Dans cet exemple, le widget **Techniques par couverture d'atténuation MITRE-ATT&CK** affiche le nombre de techniques par couverture d'atténuation dans votre environnement.

L'axe X affiche le nombre de techniques et l'axe Y affiche les types de couvertures d'atténuation.



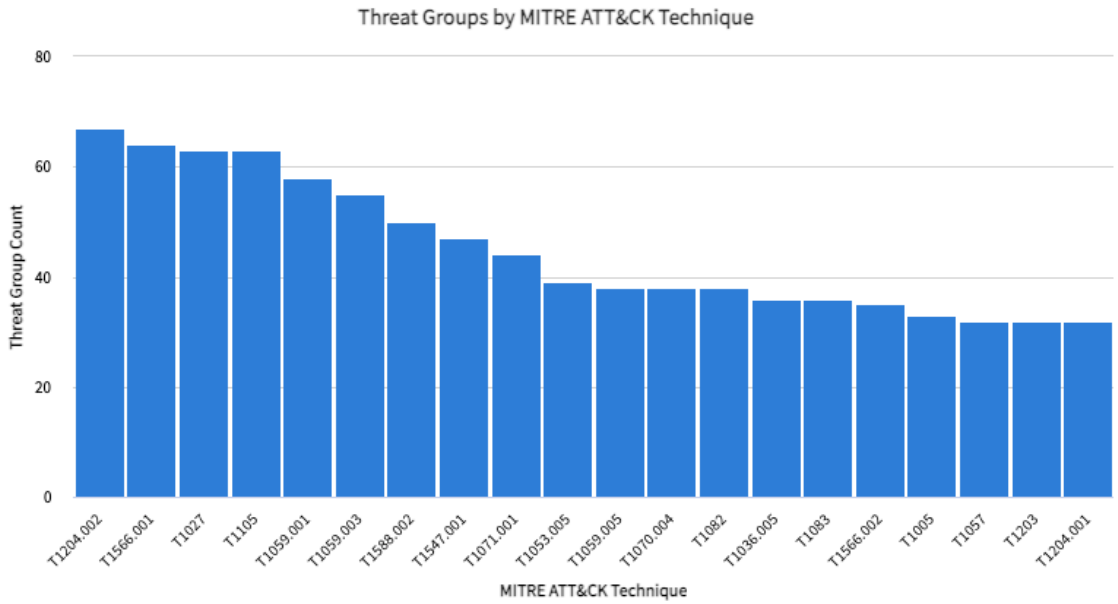
Exemple de groupes de menaces par MITRE-ATT&CK techniques

Dans cet exemple, le widget **Groupes de menaces par technique MITRE-ATT&CK** affiche les techniques en fonction du nombre de groupes de menaces. Ce widget affiche 20 techniques avec le nombre de groupes de menaces le plus élevé.

L'axe X affiche le nombre de groupes de menaces et l'axe Y affiche les MITRE-ATT&CK techniques.

Traduction automatique

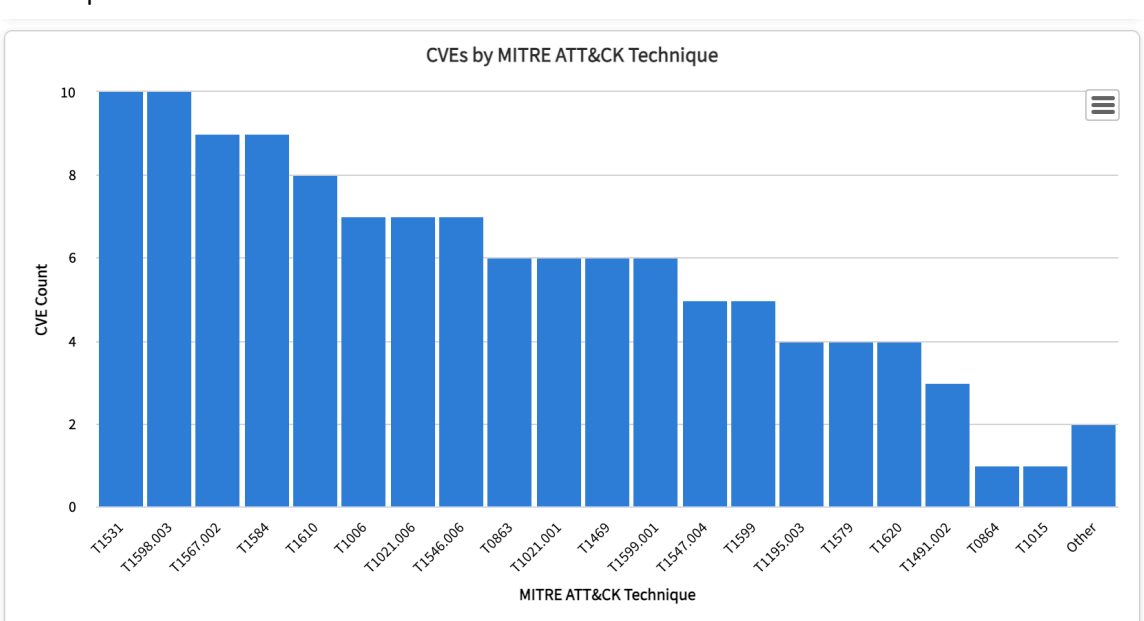
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Exemple de CVE par MITRE-ATT&CK techniques

Dans cet exemple, le widget **CVE by MITRE-ATT&CK Technique** affiche les techniques avec le nombre de CVE pertinent dans votre environnement.

L'axe X affiche le nombre de CVE pertinent et l'axe Y affiche les MITRE-ATT&CK techniques.



Administration Renseignements sur les menaces

Le Renseignements sur les menaces système de base est prêt à l'emploi lors de l'activation. Vous pouvez ajouter des enregistrements à certains modules dans le menu de l'application Administration, mais la plupart sont déjà renseignés avec des informations standard du secteur.

Les applications suivantes sont disponibles dans le module **Administration** de la Renseignements sur les menaces barre de navigation :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Applications d'administration de Threat Intelligence

Application	Description
Propriétés	Renseignements sur les menaces les propriétés vous permettent de contrôler le fonctionnement de différents aspects du système, y compris le réglage des clés API.
Mécanismes d'attaque	Ce module organise les schémas d'attaque de manière hiérarchique, en fonction des mécanismes fréquemment utilisés lors de l'exploitation d'une vulnérabilité.
Motivations de l'attaque	Ce module répertorie les motivations d'attaque possibles qui déterminent l'intensité d'une attaque par un acteur malveillant ou un ensemble d'intrusion.
Méthodes de Découverte	Ce module décrit comment les incidents de sécurité sont détectés.
Flux	Cette fonctionnalité a été déconseillée.
Types des indicateurs	Ce module est utilisé pour caractériser les indicateurs de cybermenace constitués de modèles qui identifient certaines conditions observables, ainsi que des informations contextuelles sur la signification des modèles, et comment et quand ils sont mis en œuvre.
Types d'infrastructure	Ce module répertorie les classifications possibles de l'infrastructure.
Effets souhaités	Cette application est utilisée pour exprimer l'effet escompté d'un auteur de menace.
Options de logiciel malveillant	Ce module répertorie les capacités possibles des logiciels malveillants.
Types de programmes malveillants	Ce module répertorie les classifications possibles des logiciels malveillants.
Notifications	Ce module permet de créer notifications par e-mail . Il s'agit de préciser quand ils sont envoyés, qui les reçoit et ce qu'ils contiennent.
Types des observables	Ce module répertorie les classifications possibles d'un observable, telles qu'une adresse IP ou un hachage de fichier.
Types de rapports	Ce module répertorie les classifications possibles des rapports de menace.
Rôles d'acteur de menace	Ce module répertorie les rôles joués par les acteurs de la menace.
Types d'acteurs de menace	Ce module caractérise les acteurs malveillants (ou adversaires) représentant une menace de cyberattaque, y compris l'intention présumée et le comportement historiquement observé.
Calculateurs de résultats de la recherche de menace	Ce module calcule les résultats en fonction des réponses reçues. Pour les intégrations tierces qui fournissent les résultats calculés, le calculateur de résultats de recherche de menaces mappe les résultats aux résultats pris en charge dans le système. Pour plus d'informations, consultez Calculateurs de résultats de la recherche de menace.
Types d'outil	Ce module répertorie la classification possible des outils.

Calculateurs de résultats de la recherche de menace

Le calculateur de résultats de la recherche de menace vous aide à calculer les résultats observables en fonction des réponses reçues.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez créer un calculateur de résultats de recherche de menaces pour votre intégration et utiliser un script pour déterminer comment vous souhaitez identifier les différents résultats observables. Le calculateur de résultats de recherche de menace comprend un exemple de script fourni avec le système de base, que vous pouvez utiliser pour identifier les résultats observables ou modifier ce script en fonction de vos besoins.

Pour les intégrations tierces qui fournissent les résultats calculés, le calculateur de résultats de la recherche de menace mappe les résultats aux conclusions prises en charge dans le système de base.

Résultats de la recherche de menace de déploiement

Lorsque vous disposez de plusieurs résultats de recherche de menaces pour un observable provenant des différents fournisseurs d'intégration, les résultats de la recherche de menaces récente de tous les fournisseurs sont pris en compte et les résultats globaux de l'observable sont marqués comme suit :

Déployer les conclusions de la recherche de menace

Dernier résultat observable	Résultat global de l'observable
Malveillant	Si l'un des fournisseurs de l'intégration signale l'observable comme malveillant, le résultat global de l'observable est marqué comme malveillant.
Suspect	Si aucun des fournisseurs d'intégration ne signale l'observable comme malveillant, l'un d'eux le signale comme suspect, puis le résultat observable global est marqué comme suspect.
Nettoyer	Si tous les fournisseurs de l'intégration signalent l'observable comme Propre, le résultat global de l'observable est marqué comme Propre.
Inconnu	Si aucun des fournisseurs d'intégration ne signale l'observable comme malveillant ou suspect et que l'un d'eux le signale comme inconnu, le résultat global de l'observable est marqué comme inconnu.

Utilisation des calculateurs de résultats de la recherche de menace

Utilisez le calculateur de résultats de la recherche de menace pour calculer les résultats observables pour votre intégration.

Avant de commencer

Rôle requis : sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Administration** > **Calculateurs de résultats de la recherche de menace**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Champ	Description
Fournisseur de la recherche de menace	Nom du fournisseur de recherche de menaces.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type d'observable	Spécifiez la classification du type d'observable auquel le script s'applique. Par exemple, adresse IP ou hachage de fichier, etc. Le script s'applique à tous les observables si vous ne sélectionnez aucun type d'observable.
Recherche du script	Éditeur de script pour déterminer comment vous souhaitez identifier les différents résultats observables. Le calculateur de résultats de recherche de menace contient un exemple de script avec le système de base. Vous pouvez utiliser ce script pour déterminer les résultats observables, ou vous pouvez modifier ce script en fonction de vos besoins.

4. Cliquez sur **Mettre à jour**.

Intégrations de Renseignements sur les menaces

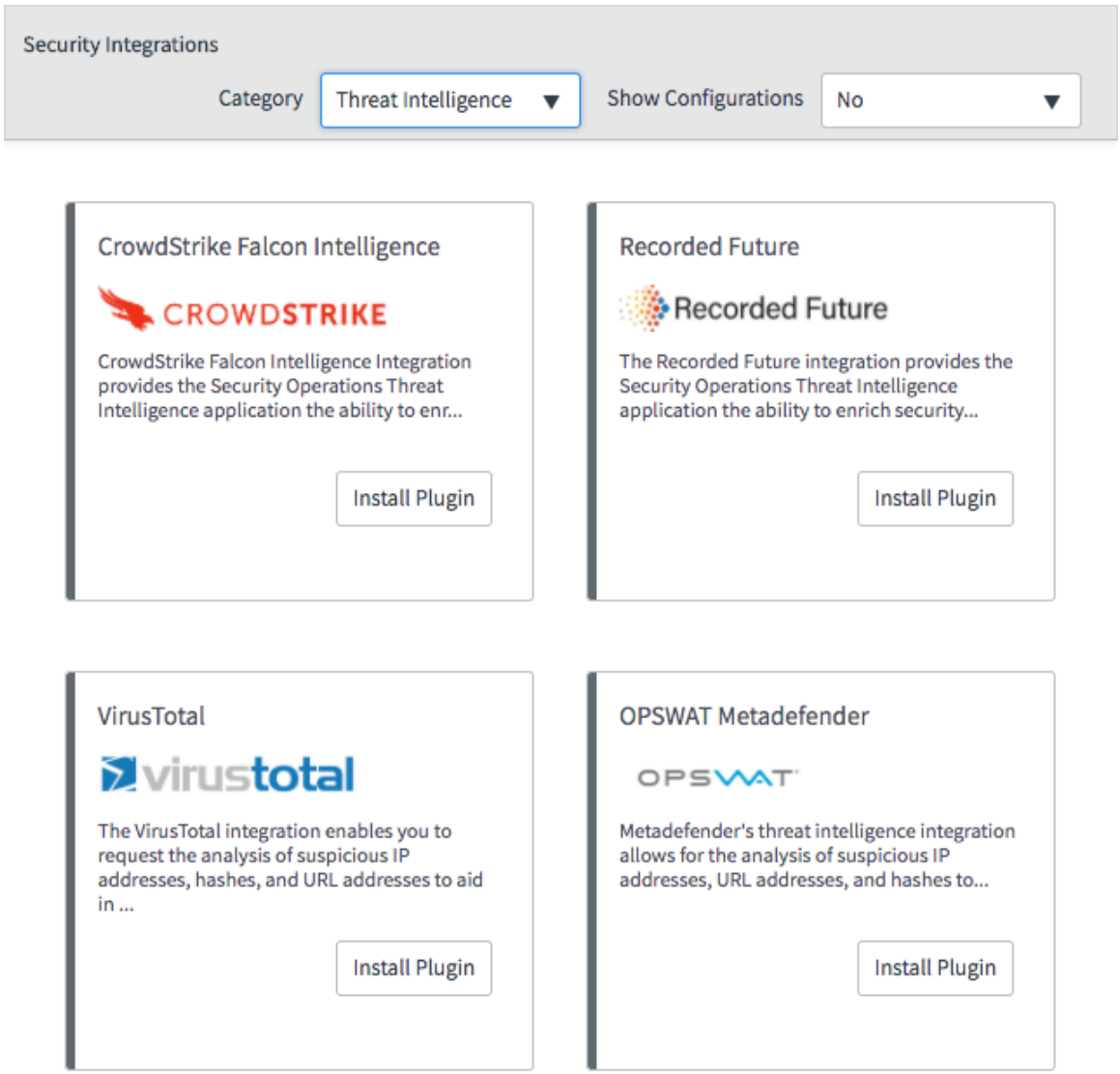
Le Renseignements sur les menaces système de base comprend des intégrations à des progiciels tiers de détection de logiciels malveillants. Cette section fournit des instructions pour activer les modules d'extension et configurer les intégrations ServiceNow tierces. Vous y trouverez également des instructions de base pour développer vos propres intégrations, ainsi que des détails sur des intégrations spécifiques incluses dans le système de base.

Configurations d'intégration

Le système de base comprend une série de « cartes » pour chacune des implémentations d'intégration que vous pouvez activer et utiliser. En outre, des cartes sont affichées pour toutes les intégrations publiées sur le ServiceNow Store qui ont des dépendances à Opérations de sécurité des modules d'extension. Les cartes d'intégration peuvent être affichées en sélectionnant **Security Operations** > **Configurations d'intégration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez filtrer les intégrations visibles à l'aide du menu déroulant **Catégorie** . Le menu déroulant **Afficher les configurations** vous permet de voir plusieurs instances d'implémentations qui autorisent leur création.

Boutons sur les cartes d'intégration

Les cartes d'intégration affichent différents boutons en fonction de l'état actuel de l'intégration et de la source de la carte.

Bouton	Description
Installer le module d'extension	Cliquez sur ce bouton pour installer le module d'extension applicable afin d'activer l'intégration. Une fois le module d'extension installé, le bouton passe à **Configurer**.
Configurer	Cliquez sur ce bouton pour entrer des informations sur la configuration de l'intégration. Pour certaines intégrations, vous devrez peut-être saisir des clés API ou des URL acquises à partir du site web de l'intégration tierce.
Nouveau	Certaines intégrations, telles que Carbon Black et IBM QRadar, vous permettent de définir plusieurs implémentations d'une même intégration. Pour ces intégrations, cliquez sur **Nouveau**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bouton	Description
	une fois le module d'extension activé. Les cartes vous permettent d'installer des modules d'extension (le cas échéant) et de configurer les implémentations à utiliser.
Ouvrir la page	Dans le système de base, votre instance interroge le ServiceNow Store pour toutes les applications qui ont des dépendances sur Opérations de sécurité des modules d'extension. Lorsque ces applications sont trouvées et que les modules d'extension d'application associés sont activés, des cartes d'intégration s'affichent avec les autres cartes d'intégration de sécurité. Cliquez sur **Ouvrir la page** pour accéder au site web de l'application tierce pour configurer l'intégration. Une fois la configuration terminée, le bouton **Ouvrir la page** devient **Configurer**.

Intégration de CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence Enrichit Renseignements sur les menaces en données relatives aux incidents de sécurité et aux observables associés.

Explorer

- Vue d'ensemble de l'intégration CrowdStrike Falcon Intelligence
- Intégrations de Réponse aux incidents de sécurité

Configurer

Activer et configurer l'intégration CrowdStrike Falcon Intelligence

Utiliser

- Effectuer des recherches sur les observables
- Recherche de menace : CrowdStrike Falcon Intelligence flux

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Vue d'ensemble de l'intégration CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence fournit des renseignements sur la cybersécurité qui s'intègrent facilement à Opérations de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

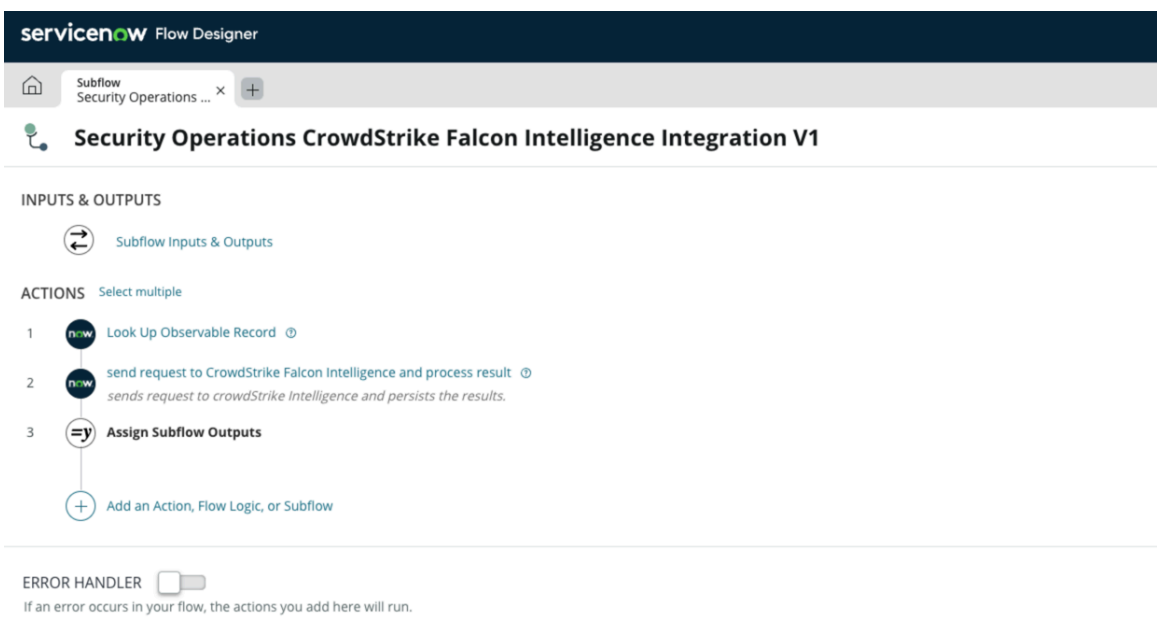
Remarque : Le Renseignements sur les menaces module d'extension est requis pour implémenter l'intégration CrowdStrike Falcon Intelligence .

Recherche de menace : CrowdStrike Falcon Intelligence flux

Le concepteur de flux Recherche de menace effectue CrowdStrike Falcon Intelligence une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par CrowdStrike Falcon Intelligence, ils sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés.

Ce flux est déclenché lorsque Security Operations Integration - Aptitude de recherche de menace vous publiez un ou plusieurs observables dans une liste de surveillance et que l'implémentation de CrowdStrike Falcon Intelligence est sélectionnée. Une fois publiées, les listes de suivi peuvent être consultées dans le logiciel CrowdStrike Falcon Host.

Rôle requis : admin



Pour plus d'informations sur les activités utilisées par ce concepteur de flux, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Activer et configurer l'intégration CrowdStrike Falcon Intelligence

La fonctionnalité Configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration CrowdStrike Falcon Intelligence . Avant de pouvoir utiliser le CrowdStrike Falcon Intelligence, vous devez le télécharger à partir de et ServiceNow Store ajouter la clé API et l'ID appropriés.

Avant de commencer

Rôle requis : admin

- Le Renseignements sur les menaces module d'extension doit être installé et activé avant de pouvoir utiliser l'intégration CrowdStrike Falcon Intelligence .
- Obtenez l'ID et le secret du client API sous votre CrowdStrike Falcon Intelligence profil.
- Si vous mettez à niveau CrowdStrike Falcon Intelligence l'intégration à partir d'une version précédente, vous devez supprimer la configuration existante et en configurer une nouvelle. L'intégration prend en charge l'authentification OAUTH2. Cette mise à jour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

nécessite que vous saisissiez **l'ID et** le **secret du client API** pour vous authentifier et terminer la configuration.

- Dans les **champs d'application de l'API** du CrowdStrike Falcon Intelligence portail, activez le paramètre **Lecture** pour les **indicateurs (Falcon X)** ou **les IOC (indicateurs de compromission).**

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configurations d'intégration**. Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la CrowdStrike Falcon Intelligence carte, cliquez sur **Configurer**.
4. Renseignez les champs du formulaire pour terminer la configuration :

Configuration CrowdStrike Falcon Intelligence

Champ	Description
Nom	Nom de l'intégration, par exemple `demo-1`.
ID client API	L'ID client que vous obtenez à partir de la section des paramètres de votre profil de compte dans CrowdStrike Falcon Intelligence le portail.
Secret client API	Clé secrète du client que vous obtenez à partir de la section des paramètres de votre profil de compte dans CrowdStrike Falcon Intelligence le portail.

5. Cliquez sur **Envoyer**.

Résultats

Une fois configuré, CrowdStrike Falcon Intelligence peut être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Intégration Have I been pwned?

L'intégration Opérations de sécurité Have I been pwned? vous permet de soumettre des recherches de noms de domaine et d'adresses e-mail afin de déterminer si les données personnelles des utilisateurs ont été compromises par des violations de données.

Explorer

Intégrations de Réponse aux incidents de sécurité

Configurer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

- Configuration de l’intégration Have I been pwned?
- Activer

Utiliser

Effectuer des recherches sur les observables
Recherche de menaces : Have I been pwned? flux

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l’écriture d’intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

- Dépannage de l’intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d’erreurs connues
- Contact Service client et assistance

Configuration de l’intégration Have I been pwned?

Have I been pwned? est une ressource gratuite utilisée pour évaluer si une personne a pu être mise en danger en raison de la compromission de son compte en ligne ou d’une violation de données. Il s’intègre facilement à Opérations de sécurité.

Avant de pouvoir utiliser l’intégration Have I been pwned? , vous devez activer le module d’extension. Si nécessaire, vous pouvez également mettre à jour votre certification SSL X509.

Les modules d’extension Réponse aux incidents de sécurité, Renseignements sur les menaces, et Opérations de sécurité Have I been pwned? sont nécessaires pour implémenter l’intégration Opérations de sécurité Have I been pwned? .

Recherche de menaces : Have I been pwned? flux

Le flux de recherche Have I been pwned? de menace effectue une recherche sur les observables sélectionnés. Si les observables sont d’un type reconnu par Have I been pwned?, ils sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés.

Rôle requis : sn_si_admin

Ce flux est déclenché lorsque Security Operations Integration - Aptitude de recherche de menace vous effectuez une recherche de menace sur un ou plusieurs observables et que l’implémentation Have I been pwned? est sélectionnée. Pour plus d'informations, consultez Effectuer des recherches sur les observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ai-je été pwned flow



Pour en savoir plus sur les activités utilisées par ce flux, reportez-vous à la rubrique Flux d'intégration et activités d'orchestration courants de Security Operations.

Activer

La fonctionnalité Configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration Opérations de sécurité Have I been pwned? . Avant de pouvoir utiliser l'intégration Have I been pwned? , vous devez la télécharger à partir du ServiceNow Store.

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être installé et activé avant de pouvoir utiliser l'intégration Opérations de sécurité Have I been pwned? .

Rôle requis : sn_si_admin

Procédure

Télécharger l'intégration à partir de ServiceNow Store.
Cette intégration prend en charge une API ouverte et ne nécessite pas de configuration supplémentaire. Have I been pwned? peut désormais être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Mettre à jour votre certificat X.509

Si vous avez besoin d'une connexion SSL pour l'intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou ait expiré. Cette tâche est facultative.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Obtenez le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

   b. Cliquez sur l'icône de verrou dans la ligne d'adresse.

   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

   e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

   f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
   Il doit commencer par `----- COMMENCER LE CERTIFICAT -----` et se terminer par `----- CERTIFICAT DE FIN -----`.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Ajoutez le certificat à l'enregistrement du fournisseur d'identité.
   a. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
   b. Sélectionnez le fournisseur d'identité par défaut actif pour lequel vous avez créé le nouveau certificat.
   c. Faites défiler jusqu'à la liste connexe des **certificats X.509** , puis cliquez sur **Modifier**.
   d. Déplacez le certificat nouvellement créé vers la colonne **Sélectionnée** .
6. Cliquez sur **Enregistrer**.
   Les autres champs de l'enregistrement sont générés automatiquement.

Remarque : Si vous avez un certificat qui a expiré, vous devez le supprimer. Pour plus d'informations sur la suppression du certificat expiré, consultez KB0691439 Remplacement d'un certificat SAML arrivant à expiration .

MISP integration for Security Operations

Avec MISP integration for Security Operations, vous pouvez enquêter sur les incidents de sécurité avec la recherche de perception, l'enrichissement des observables et créer ou mettre à jour des événements dans MISP. Grâce MISPà , vous pouvez enquêter plus rapidement sur les attaques ciblées, améliorer le taux de détection et réduire le nombre de faux positifs dans votre environnement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

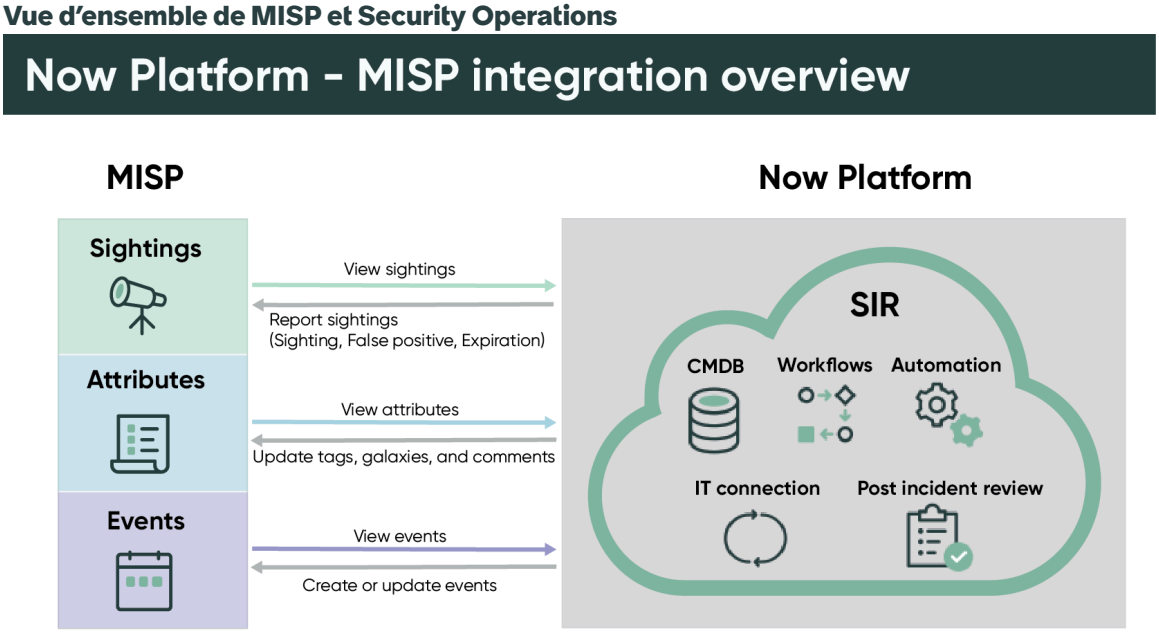
MISP Vue d'ensemble

MISP, qui signifie Malware Information Sharing Platform, vous permet d'échanger et de partager des renseignements sur les menaces et les indicateurs de compromission (IoC) sur les logiciels malveillants et les attaques ciblés au sein de votre communauté de membres de confiance. Vous pouvez également partager MISP des informations avec des communautés privées ou ouvertes. En échangeant des MISP informations, vous pouvez enquêter plus rapidement sur les attaques ciblées, améliorer le taux de détection et réduire le nombre de faux positifs dans votre environnement.

MISP et Opérations de sécurité

Consultez l'exemple suivant pour découvrir comment les informations circulent avec les MISP applications Security Operations.

Vue d'ensemble de MISP et Security Operations



Fonctionnalités principales

Cette intégration comprend les actions que vous pouvez effectuer avec les MISP fonctionnalités principales :

- Se connecter à une instance privée et publique MISP instances.
- Prise en charge de la recherche de perception manuelle et automatique des observables.
- Exécutez la recherche de perception à partir de la gestion des tickets.
- Signaler ou mettre à jour des observations sur un attribut :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

  - Signaler un observable en tant qu'observation (global)
  - Signaler un observable comme faux positif (global)
  - Signaler un observable comme expiré
- Prise en charge de l'enrichissement manuel et automatique des observables. Les résultats incluent les informations sur l'attribut et l'événement MISP associés aux observables.
- Enrichissement d'attributs qui MISP inclut l'ajout ou la mise à jour de balises, de galaxies ou de commentaires.
- Création d'événements dans MISP de SIR: prend en charge la création manuelle et automatique d'événements dans MISP à partir de SIR.
- Mettez à jour un MISP événement à partir duquel il peut ajouter ou mettre à jour des balises, des galaxies ou desSIRattributs.
- Ajouter des observables associés à un incident de sécurité en tant qu'attributs à un MISP event.
- Extraire automatiquement MITRE-ATT&CK™ informations provenant de MISP attributs et associer les informations à SIR des incidents de sécurité.
- Ajouter automatiquement SIR MITRE-ATT&CK™ sous forme de galaxies à un MISP event.

Concepts clés

Cette intégration comprend les concepts clés suivants que vous devez connaître :

- MISP est une plateforme de renseignements sur les menaces (TIP). Vous utilisez les TIP pour collecter, corréler, catégoriser, partager et intégrer des données sur les menaces de sécurité en temps réel afin de prendre en charge la hiérarchisation des actions et de contribuer à la prévention, à la détection et à la réponse aux attaques.
- MISP est une gestion des renseignements sur les menaces (TIM). Vous utilisez les TIM pour transformer les données sur les menaces en renseignements sur les menaces via le contexte et pour hiérarchiser automatiquement les menaces en fonction du score et de la pertinence définis par l'utilisateur.
- MISP Couche de données
  - Les événements sont des encapsulations d'informations liées contextuellement.
  - Les attributs sont des points de données individuels, qui peuvent être des indicateurs ou des données de support.
  - Les objets sont des compositions d'attributs de modèle personnalisées.
  - Les références d'objet sont les relations entre les autres blocs de construction.
  - Les observations sont des occurrences spécifiques dans le temps d'un point de données détecté.
- MISP Couche de contexte
  - Les balises sont des étiquettes attachées à des événements ou à des attributs et peuvent provenir de taxonomies.
  - Les amas de galaxies sont des éléments de la base de connaissances que vous pouvez utiliser pour étiqueter les événements ou les attributs provenant des galaxies.
  - Les relations de grappe désignent des relations prédéfinies entre les grappes.
- Les indicateurs contiennent un modèle que vous pouvez utiliser pour détecter les cyber-activités suspectes ou malveillantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les attributs peuvent être des MISP indicateurs réseau (adresse IP), des indicateurs système (une chaîne en mémoire) ou même des détails bancaires. Les attributs dans MISP sont appelés observables dans d'autres SIEM ou formats tels que STIX.
  - Un type décrit l'attribut. Par exemple, MD5 ou une URL.
  - La catégorie d'attribut décrit un attribut. Par exemple, une livraison de charge utile.
  - Une balise IDS détermine si un attribut peut être automatiquement utilisé pour la détection.

Remarque : Pour plus d'informations sur MISP les concepts, consultez le site web de la documentation MISP.

Comment votre organisation peut bénéficier de MISP integration for Security Operations

Les analystes de sécurité doivent acquérir et maintenir une connaissance situationnelle du paysage des menaces, ce qui signifie qu'ils doivent consolider et intégrer manuellement une quantité écrasante de données sur les menaces. La collecte, la consolidation et l'intégration de ces données prennent un temps précieux, ce qui ralentit la détection et l'analyse des menaces. MISP integration for Security Operations permet aux analystes de détecter davantage de menaces et de réagir plus rapidement en intégrant les renseignements de MISP sécurité dans une instance existante ServiceNow AI Platform .

À l'aide de , MISP integration for Security Operations votre organisation peut effectuer les actions suivantes :

- Permettez à vos analystes de sécurité de réagir rapidement et avec le bon contexte.
- Améliorez l'efficacité de votre équipe de sécurité en automatisant les flux d'incidents pour détecter et contenir les menaces.
- Réduisez le temps de recherche manuelle et permettez aux analystes de sécurité d'opérationnaliser et de gérer les indicateurs à partir du ServiceNow AI Platform.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
MISP Site web de la documentation	Site web de la documentation MISP
ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Administration MISP

Vous pouvez configurer l'intégration MISP dans le ServiceNow AI Platform pour effectuer une recherche de perception, un enrichissement d'observables, ainsi que pour créer et mettre à jour des événements dans MISP.

Premiers pas avec MISP integration for Security Operations

Consultez les informations suivantes avant de configurer votre MISP integration for Security Operations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles de ServiceNow AI Platform et Renseignements sur les menacesRéponse aux incidents de sécurité requis.	Les rôles suivants sont utilisés dans les MISP fonctionnalités de :ServiceNow AI Platform • L'administrateur (admin) installe les applications à partir de et affecte les rôles d'administrateur d'incident de sécurité (sn_si.admin) et d'administrateur ServiceNow Store de Renseignements sur les menaces (sn_ti.admin). • sn_si.admin et sn_ti.admin peuvent configurer l'intégration et configurer les profils de création automatique MISP d'événements. • sn_sec_misp.write : le rôle d'analyste dispose d'autorisations MISP de lecture et d'écriture pour MISP les données qui incluent les données d'événement et d'attribut. Pour plus d'informations, consultez Configurer Threat Intelligence.
Affectez les rôles d'utilisateur requis MISP .	Examiner le MISP rôles d'utilisateur et autorisations requises pour utiliser le MISP integration for Security Operations. **Remarque :** Pour plus d'informations sur les rôles d'utilisateur dans MISP, consultez la section Rôles sur le site Web de la documentation MISP .
Vérifiez que vous utilisez MISP la version 2.4.137 ou ultérieure.	Le MISP integration for Security Operations est testé avec un minimum de MISP Version 2.4.137 .
Vérifiez que les ServiceNow applications principales requises pour prendre en charge le MISP module sont installées et activées.	Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si elle n'est pas installée, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide. • Réponse aux incidents de sécurité • ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) • ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) Pour plus d'informations sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez obtenir

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	une autorisation pour un produit ou une application Security Operations et activer une application ServiceNow Store.
Séparation de domaine	Vérifiez la section Séparation de domaine si vous avez l'intention de séparer les données, les processus et les tâches administratives.

MISP Rôles et autorisations d'utilisateur

Passez en revue les rôles d'utilisateur requis dans l'intégration MISP integration for Security Operations .

Autorisations d'enrichissement des observables et de recherche de perception

Remarque :

- ***Toutes les* ServiceNow *options d'intégration MISP ont besoin des autorisations de base pour* gérer les événements de l'organisation *et* l'accès aux clés d'authentification*. Assurez-vous de disposer de ces autorisations de base avant de poursuivre.***
- ***Pour ajouter des galaxies locales, l'utilisateur qui configure l'intégration doit appartenir à l'organisation hôte du serveur MISP correspondant.***

Aptitude MISP	Tagueur	Éditeur de balises
Enrichissement des observables (lecture seule)	#	#
Recherche de perception (lecture seule)	#	#

Signaler des autorisations de perception

Aptitude MISP	Créateur de perception
Rapporter une observation	#

Autorisations d'attribut et d'événement

Aptitude MISP	Tagueur	Éditeur de balises
Modifier les balises d'événement/d'attribut	#	#
Modifier les galaxies d'événements/d'attributs	#	#
Modifier les commentaires d'attribut	#	#

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisations d'attribut et d'événement (suite)

Aptitude MISP	Tagueur	Éditeur de balises
Ajouter un nouvel attribut à l'événement	#	#
Créer un événement dans MISP	#	#

Installez et configurez le MISP integration for Security Operations

Installez et configurez le à partir de MISP integration for Security Operations sur ServiceNow Store votre ServiceNow AI Platform instance afin de commencer à enquêter sur les incidents de sécurité à l'aide des MISP données.

Avant de commencer

Assurez-vous d'avoir installé les certificats SSL valides sur le serveur MISP.

Rôle requis : sn_si.admin

Procédure

1. Téléchargez le MISP integration for Security Operations à partir de et ServiceNow Store installez-le.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la MISP tuile Intégration -SIR/TI et cliquez sur **Configurer**.
4. Remplissez les champs du formulaire.

MISP - Formulaire de configuration de l'intégration SIR/TI

Champ	Description
Nom	Nom de la configuration d'instance MISP .
MISP URL serveur	URL du MISP serveur qui sert de point de terminaison REST pour le MISP serveur.
Clé API	Clé API configurée pour votre compte d'utilisateur sur le MISP serveur. La clé API correspond à **l'Authkey** dans le MISP serveur.
Déploiement sur site	Option que vous pouvez sélectionner si votre MISP serveur est déployé dans une instance sur site. Lorsque vous sélectionnez l'option **Déploiement sur site** , vous devez utiliser le Serveur MID pour vous connecter au MISP serveur.
Application MID	Champ de chaîne qui identifie le nom de l'application MID utilisée pour communiquer avec MISP Ce champ est obligatoire lorsque vous sélectionnez l'option **Déploiement sur site** . Pour plus d'informations sur la configuration du Serveur MID pour votre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	application, voir Configurer un Serveur MID pour chaque application

5. Cliquez sur **Envoyer**.

Résultats

Une fois que vous avez validé et soumis la configuration, l'intégration MISP SIR/TI est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

Passer en revue les paramètres d'intégration MISP

Examinez les MISP integration for Security Operations paramètres et modifiez les propriétés système par défaut en fonction de votre environnement.

Avant de commencer

Rôle requis : sn_si.admin, sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Intégration de MISP** > **Paramètres d'intégration**.
2. Modifiez les paramètres suivants selon vos besoins.

Paramètres d'intégration MISP

Nom de la propriété		Description
Enrichissement des éléments observables	Temps (en heures) avant l'extraction de nouvelles données	Temps en heures avant de pouvoir extraire de nouvelles données. Type : nombre entier Valeur par défaut : 24
Recherche de perception	Exécuter automatiquement la recherche de perception lorsque de nouveaux observables sont associés à l'incident de sécurité	Recherche de perception qui s'exécute chaque fois qu'un nouvel observable est associé à un incident de sécurité. Valeur par défaut : oui
	Intervalle de recherche (en jours) pour la recherche sur la perception dans MISP	Nombre de jours dans MISP lesquels les données de recherche de perception sont recherchées. Utilisez cette option uniquement pour la fonction de recherche automatique de perception. Valeur par défaut : 90
Synchronisation des données	Période d'intervalle (en minutes) pour que les balises soient récupérées et synchronisées avec MISP	MISP Balises récupérées au moment de la configuration de l'intégration. Une fois les données dans la ServiceNow AI Platform, cette propriété définit la fréquence à laquelle les données avec le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété		Description
		MISP serveur sont synchronisées. La valeur est définie en minutes. Valeur par défaut : 1 440 (minutes ou 24 heures)
	Période d'intervalle (en minutes) pour actualiser les galaxies MISP à partir de sources configurées	MISP Galaxies qui sont extraites au moment de la configuration de l'intégration. Une fois les données dans la ServiceNow AI Platform, cette propriété définit la fréquence à laquelle les données avec le MISP serveur sont synchronisées. La valeur est définie en minutes. Valeur par défaut : 1 440 (minutes ou 24 heures)
	Période d'intervalle (en minutes) pour les organisations à extraire et à synchroniser avec MISP	MISP Organisations récupérées au moment de la configuration de l'intégration. Une fois les données dans la ServiceNow AI Platform, cette propriété définit la fréquence à laquelle les données avec le MISP serveur sont synchronisées. La valeur est définie en minutes. Valeur par défaut : 1 440 (minutes ou 24 heures)
MITRE™ Technique Extraction	Déployer automatiquement les techniques à partir des résultats de l'enrichissement de l'observable MITRE-ATT&CK MISP (balises) vers l'incident de sécurité	Déploiement des informations à partir des MISP résultats d'enrichissement des MITRE-ATT&CK observables (balises) vers l'incident de sécurité. Valeur par défaut : oui
	Déployer automatiquement les techniques à partir des résultats de l'enrichissement de l'observable MITRE-ATT&CK MISP (Galaxies) vers l'incident de sécurité	Déploiement des informations depuis les résultats de l'enrichissement de MITRE-ATT&CK l'observable MISP (galaxies) vers l'incident de sécurité. Valeur par défaut : oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Pour utiliser les fonctionnalités d'extraction technique MITRE™ dans MISP, vous devez Activez l'option MITRE-ATT&CK dans le Renseignements sur les menaces module.
- Il MISP integration for Security Operations introduit deux règles d'extraction de la technique du système MITRE-ATT&CK de base pour MISP les MISP galaxies et MISP les balises. Pour plus d'informations sur les règles d'extraction automatique dans , consultez MITRE-ATT&CKRègles de technique d'extraction automatique pour l'importation d'informations MITRE-ATT&CK.

3. Cliquez sur **Enregistrer**.

Résultats
Vos paramètres d'intégration modifiés sont enregistrés et appliqués.

Configurer MISP les recherches de perception

Configurez le ServiceNow AI Platform pour effectuer des recherches de perception pour les observables de l'instance MISP . Grâce à ces informations, vous pouvez déterminer la fréquence à laquelle les menaces se produisent.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations qui sont requises pour utiliser les fonctionnalités bidirectionnelles MISP .
- Rôle requis : sn_si.admin, sn_ti.admin

Pourquoi et quand exécuter cette tâche
Le workflow Security Operations Integration - Recherche de perceptions exécute les recherches de perception. Ce workflow accepte une liste d'observables, recherche toutes les options d'implémentation, crée les requêtes basées sur les configurations de recherche de perceptions et exécute les recherches basées sur le workflow configuré.

Le MISP integration for Security Operations fournit un profil de recherche de perception du système de base qui vous permet de configurer des recherches automatiques de perception. Avec ce profil, vous pouvez accéder aux informations d'observation observable connexes d'une organisation et également voir les observations externes d'autres organisations.

Procédure

1. Accédez à la **Tous** > **Intégration de MISP** > **Configuration de la recherche de détections**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Configuration de la recherche de perceptions

Champ	Description
Nom	Nom du profil d'aptitude.
Est une recherche enregistrée	Configuration de recherche enregistrée lorsque vous sélectionnez cette option. Les requêtes de configuration de recherche enregistrées sont des exemples de requêtes. Vous pouvez les remplacer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	par les paramètres de votre environnement et créer des configurations de recherche enregistrées supplémentaires si nécessaire.
Source de recherche de perceptions	Source pour la recherche d'observations. Sélectionnez le magasin de MISP journaux comme source.
Actif	Option permettant d'activer la configuration de recherche enregistrée. Seules les configurations de recherche actives peuvent effectuer une recherche de perceptions.
Type d'observable	Type d'observable tel que l'adresse IP, la valeur de hachage, l'URL et le nom de domaine.
Nombre maximum d'observables par recherche	Nombre maximal d'observables que vous pouvez afficher à partir d'une requête de recherche.
Rechercher	Chaîne de recherche par défaut `$(observable)`. Toutefois, vous définissez votre propre requête de recherche en spécifiant les paramètres pris en charge par le magasin de MISP journaux.

4. Cliquez sur **Envoyer**.

Résultats
Vous avez créé un profil de MISP configuration de recherche de perceptions.

Configurer la façon dont un événement automatique est créé

Configurer le ServiceNow AI Platform pour créer automatiquement des événements dans MISP.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations qui sont requises pour utiliser les fonctionnalités bidirectionnelles MISP .
- Rôle requis : sn_si.admin, sn_ti.admin

Procédure

1. Accédez à la **Tous** > **Intégration de MISP** > **Profils de création automatique d'événements**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de nom

Champ	Description
Nom	Nom du profil de création automatique d'événements.
Description	Brève description du profil. Une description plus détaillée est partagée par le biais des attributs à l'étape suivante de la création de l'événement.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ordre	Ordre du profil lorsque les conditions de déclenchement sont remplies. La valeur par défaut est 100. Laissez ce paramètre par défaut. Si vous créez plusieurs profils, cette valeur fournit une priorité d'exécution lorsque deux profils ou plus partagent des conditions de déclenchement. Le profil avec le numéro le plus bas a la priorité la plus élevée.
Source	MISP Source pour la création de l'événement.
Actif	Option qui indique si le profil est actif ou inactif. L'option est décochée par défaut pour indiquer que le profil est désactivé. Ce profil n'est pas actif tant que vous n'avez pas terminé toutes les étapes de configuration du profil et cliqué sur **Terminer**.

4. Cliquez sur **Continuer**.

Configurer les conditions de déclenchement d'événement

Configurez les conditions de déclenchement d'événement dans afin de ServiceNow AI Platform pouvoir déclencher automatiquement un événement lorsque MISP les conditions sont remplies.

Avant de commencer

Rôle requis : sn_sec_misp.write

Procédure

1. Dans le formulaire Conditions de déclenchement, renseignez les détails qui peuvent déclencher un événement.
   Vous pouvez créer une logique de composé en fournissant les conditions de déclenchement basées sur les champs d'incident de sécurité ou les champs observables. Vous pouvez également créer des événements dans MISP si les observables n'ont pas d'événement correspondant dans MISP. Vous pouvez choisir de créer une logique de composé à l'aide d'une combinaison des trois conditions de déclenchement : Déclencher en fonction des champs d'incident de sécurité, Déclencher en fonction des champs observables et Créer un événement MISP, si un observable n'a pas d'événements correspondants dans MISP. Si vous sélectionnez plusieurs déclencheurs, vous pouvez les joindre à l'aide de la condition ET. Envisagez de créer un profil avec de nouvelles conditions si vous devez utiliser la condition OU.

Formulaire Conditions de déclenchement d'événement

Champ	Description
Déclencher en fonction des champs d'incident de sécurité	MISP Événement que vous pouvez créer si toutes les conditions de déclenchement de l'incident de sécurité sont remplies.
Conditions de déclenchement des incidents de sécurité	Filtres de la première ligne que vous pouvez définir à l'aide des listes et des champs du générateur de

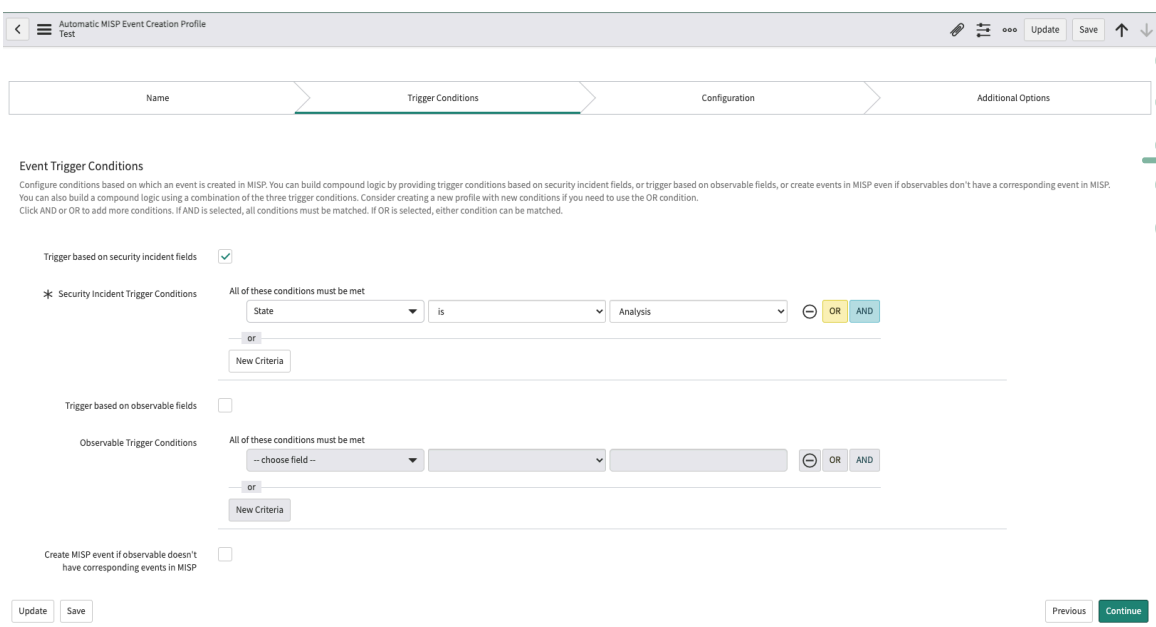
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	conditions. Pour ajouter d'autres conditions, cliquez sur ET ou OU. Si ET est sélectionné, toutes les conditions doivent être mises en correspondance. Si OU est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.
Déclencher en fonction des champs observables	MISP Événement que vous pouvez créer si toutes les conditions de déclenchement de l'observable sont remplies.
Conditions de déclenchement des observables	Filtres de la première ligne que vous pouvez définir à l'aide des listes et des champs du générateur de conditions. Pour ajouter d'autres conditions, cliquez sur ET ou OU. Si ET est sélectionné, toutes les conditions doivent être mises en correspondance. Si OU est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.
Créer un événement MISP en l'absence d'événements correspondants pour l'observable dans MISP	MISP Événement que vous pouvez créer si un observable n'a pas d'événements correspondants dans MISP.

Conditions de déclenchement de l'événement

L'exemple suivant montre les conditions de déclenchement d'événement lorsque vous configurez le profil de création d'événement MISP .



2. Cliquez sur **Continuer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mapper les champs d'événement MISP

Mappez les MISP champs d'événement afin que les informations sur les incidents de sécurité soient disponibles lors de la ServiceNow AI PlatformMISP création d'événements.

Avant de commencer

Rôle requis : sn_sec_misp.write

Procédure

1. Remplissez les champs du formulaire.

Formulaire par défaut du mappage de champs d'événements MISP

Champ	Description
Informations sur l'événement	Informations sur l'événement qui sont automatiquement créées à partir du ServiceNow AI Platform Réponse aux incidents de sécurité. Le champ **Informations sur l'événement** prend en charge les variables de substitution à l'aide de ${SIR FIELD LABEL}$. Lors de la création d'un événement, ces variables sont remplacées par les valeurs réelles des champs Incident de sécurité. La variable de substitution ${URL}$ est remplacée par l'URL de l'incident de sécurité.
Distribution	Option qui contrôle qui peut afficher cet événement après la publication de l'événement. Cette option contrôle également si l'événement est synchronisé avec d'autres serveurs. La distribution est héritée par les attributs, et le paramètre le plus restrictif l'emporte. Les options de distribution sont les suivantes : ○ Votre organisation uniquement : autorise uniquement les membres de votre organisation à afficher cet événement. L'événement peut être transféré vers une autre instance par l'un des membres de votre organisation, où seule votre organisation peut avoir accès pour l'afficher. Les événements avec ce paramètre ne sont pas synchronisés. ○ Cette communauté uniquement : permet aux utilisateurs qui font partie de votre MISP communauté d'afficher l'événement, y compris votre propre organisation, les organisations sur ce MISP serveur et les organisations qui exécutent MISP des serveurs qui se synchronisent avec ce serveur. Toute autre organisation qui se connecte à vos serveurs liés ne peut pas voir l'événement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

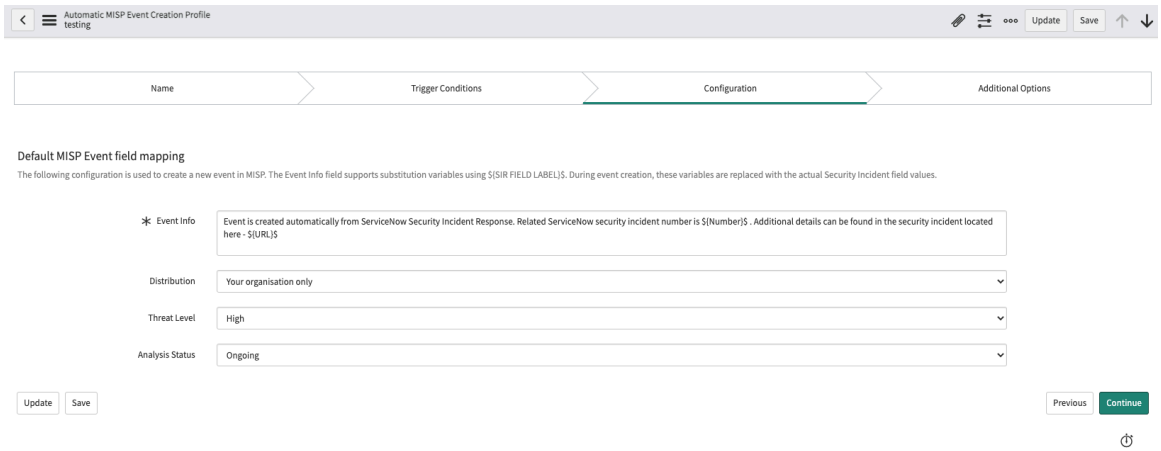
Champ	Description
	○ Communautés connectées : permet aux utilisateurs qui font partie de votre MISP communauté d'afficher l'événement, y compris toutes les organisations sur ce MISP serveur, toutes les organisations sur les MISP serveurs qui se synchronisent avec ce serveur et les organisations d'hébergement des serveurs qui se connectent à n'importe quel serveur situé à deux sauts de distance. Toutes les autres organisations connectées aux serveurs liés qui se trouvent à deux sauts de distance ne peuvent pas voir l'événement. ○ Toutes les communautés : partage l'événement avec toutes les MISP communautés.
Niveau de menace	Champ qui indique le niveau de risque de l'événement. Vous pouvez classer les incidents en trois catégories de menaces différentes (faible, moyenne, élevée). Ce champ peut également être laissé non défini. Les options sont les suivantes : ○ Faible : logiciel malveillant de masse général ○ Moyen : menaces persistantes avancées (APT) ○ Élevée : APT sophistiquées et attaques sur 0 jour
Statut de l'analyse	Étape actuelle de l'analyse de l'événement, avec les options possibles suivantes : ○ Initial : l'analyse ne fait que commencer ○ En cours : l'analyse est en cours ○ Terminé : l'analyse est terminée

L'exemple suivant montre le formulaire que vous pouvez utiliser pour créer un événement dans MISP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de champ d'événement MISP par défaut



2. Cliquez sur **Continuer**.

Mapper ou associer des SIR observables en tant qu'attributs à MISP des événements

Mappez les types d'observables Réponse aux incidents de sécurité aux types d'attributs MISP , car les types d'attributs MISP et les SIR observables peuvent être différents.

Avant de commencer

Rôle requis : sn_sec_misp.write

Pourquoi et quand exécuter cette tâche

fournit MISP integration for Security Operations un mappage du système de base que vous utilisez lorsque vous ajoutez SIR des observables en tant qu'attributs à un MISP événement.

Vous pouvez choisir de modifier le mappage du système de base en fonction de votre environnement. Par exemple, vous pouvez mapper plusieurs SIR observables à un seul type d'attribut MISP . Si des types d'observables ne sont pas mappés, **l'autre** MISP type d'attribut est sélectionné par défaut.

Procédure

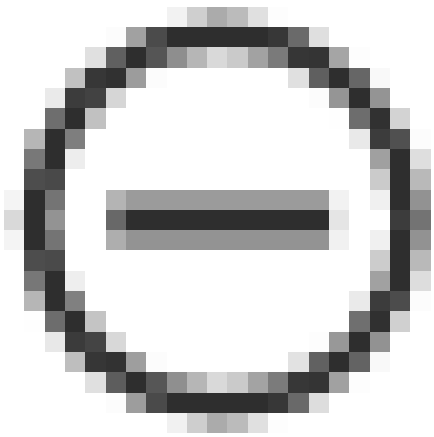
1. Dans le formulaire Options supplémentaires, mappez les types observable SIR et MISP attribut.
2. Mappez les types d'observables Réponse aux incidents de sécurité aux types d'attributs MISP , comme décrit dans la table suivante.

Correspondance entre les observables du SIR et les types d'attributs du MISP

Champ	Description
Ajouter tous les observables associés en tant qu'attributs	Option permettant d'ajouter des observables disponibles dans un incident de sécurité à un MISP événement en tant qu'attributs. Cette option active le mappage dans la section Mappage du type d'observable au type d'attribut.
Mappage type observable à type d'attribut	Option permettant de mapper les types d'observables SIR aux types d'attributs MISP . Par exemple, vous

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	pouvez mapper le numéro CVE à SIR l'attribut de vulnérabilité dans MISP. Vous pouvez ajouter un type d'observable SIR à un seul type d'attribut MISP . Le système de base fournit un mappage des types d'observables aux types d'attributs SIRMISP . Si des types d'observables SIR ne sont pas mappés à un type d'attribut MISP , l'observable est mappé à **l'autre** type d'attribut dans MISP. Pour ajouter un nouveau mappage, cliquez sur **Ajouter un type d'observable**, recherchez le type d'observable SIR , puis mappez-le au type d'attribut correspondant MISP . Cliquez sur l'icône Supprimer le  pour supprimer l'association de mappage d'attribut SIR et MISP . **Remarque :** Pour plus d'informations sur MISP les types d'attributs, consultez la documentation MISP .
Filtrer les éléments observables en fonction des balises de sécurité	Option permettant de filtrer les observables en fonction des balises de sécurité sélectionnées. **Balises de sécurité** : ajoutez des balises pour filtrer les observables. Par exemple, si vous ajoutez une balise appelée « Block from sharing » ou « TLP : White », si l'un des observables a l'une de ces balises associée, ces observables ne seront pas ajoutés en tant qu'attribut à l'événement

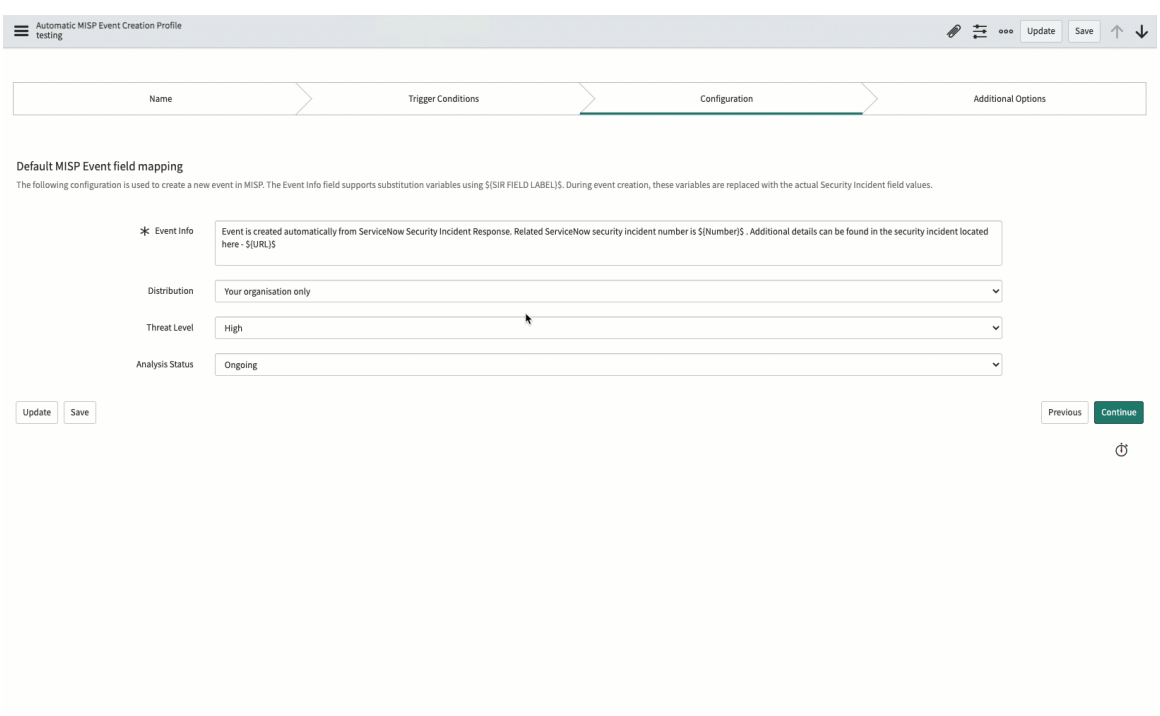
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	MISP lors de la création de l'événement MISP.
Définir le marqueur IDS d'attribut lorsque le résultat observable est malveillant	Option qui vous permet de savoir que si un observable est marqué comme malveillant dans SIR, le marqueur IDS est activé pour l'attribut MISP correspondant. Si le marqueur IDS n'est pas défini, l'attribut est considéré comme une information contextuelle et n'est pas utilisé pour la détection automatique des intrusions.

L'exemple suivant montre comment naviguer vers la page d'options supplémentaires. Sur cette page, vous pouvez activer le mappage des observables SIR et des types d'attributs MISP, ajouter de nouveaux SIR types d'observables, tels que le réseau IPV6 et le réseau IPV4, et le mapper à l'adresse IP du domaine de type d'attribut MISP .

Mappage des SIR observables et MISP des types d'attributs



Synchroniser les informations avec les MITRE-ATT&CKMISP événements

Synchronisez les informations avec MISP les MITRE-ATT&CK attributs pour une meilleure analyse des incidents de sécurité et des menaces.

Avant de commencer

Rôle requis : sn_sec_misp.write

Procédure

Dans le formulaire Options supplémentaires, examinez les options pour synchroniser les MITRE-ATT&CK informations avec les MISP attributs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Options avancées

Champ	Description
Synchroniser les techniques d'incident MITRE-ATT&CK™ de sécurité en tant que galaxies locales à l'événement MISP	Option permettant de synchroniser les techniques d'incident ServiceNow AI Platform SIRMITRE-ATT&CK™ de sécurité en tant que galaxies locales dans l'événement MISP . **Remarque :** Pour ajouter des galaxies locales, l'utilisateur qui a configuré l'intégration doit appartenir à l'organisation hôte du serveur correspondant MISP .
Synchroniser les techniques d'incident MITRE-ATT&CK™ de sécurité en tant que galaxies globales à l'événement MISP	Option permettant de synchroniser les techniques d'incident ServiceNow AI Platform SIRMITRE-ATT&CK™ de sécurité en tant que galaxies globales dans l'événement MISP .

Résultats

Vous avez créé un profil qui vous permet de créer automatiquement des événements dans MISP à partir de .ServiceNow AI Platform Vous pouvez maintenant afficher les événements dans la liste connexe Événements MISP associés.

Ajouter des balises MISP aux événements

Ajoutez des balises MISP aux événements MISP créés.

Avant de commencer

Rôle requis : sn_sec_misp.write

Procédure

1. Dans le formulaire Options supplémentaires, accédez à **Sélectionner les balises MISP à ajouter à la section événement** de la vue de formulaire.
2. Passez en revue les options permettant d'ajouter des balises aux événements créés.

Formulaire Options avancées

Champ	Description
Ajouter des balises à l'événement MISP créé	Option qui vous permet d'ajouter automatiquement des balises MISP aux événements créés à partir de ServiceNow.
Balises (locales)	Les balises sélectionnées seront ajoutées en tant que balises locales à l'événement MISP.
Balises (globales)	Les balises sélectionnées seront ajoutées en tant que balises globales à l'événement MISP.

3. Cliquez sur **Enregistrer**.

Résultats

L'ajout de balises MISP permet de classer l'événement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

MISP Données d'événement

Vous pouvez examiner les données d'événement MISP afin d'afficher des informations détaillées sur les MISP événements.

MISP Données d'événement dans la vue de liste

Accéder à la vue de liste à partir de **MISP** > **Données d'événements MISP**.

Utilisez la vue de liste pour obtenir une vue d'ensemble rapide des données de l'événement MISP .

Vue de liste d'événements MISP

Champ	Description
ID d'événement	ID d'événement attribué lors de MISP la première création ou importation de l'événement dans le MISP serveur.
Info	Brève description de l'événement.
Analyse	Étape actuelle de l'analyse de l'événement avec les options possibles suivantes : • Initial : l'analyse ne fait que commencer • En cours : l'analyse est en cours • Terminé : l'analyse est terminée
Niveau de menace	Niveau de risque de l'événement. Les incidents peuvent être classés en trois catégories de menaces différentes (faible, moyenne, élevée). Ce champ peut être laissé comme non défini. Les options sont les suivantes : • Faible : logiciel malveillant de masse général • Moyen : menaces persistantes avancées (APT) • Élevée : APT sophistiquées et attaques sur 0 jour
Balises MISP	Balises associées à l'événement MISP .
Galaxies MISP	Galaxies associées à l'événement MISP .
Org. du propriétaire	Organisation propriétaire de l'événement sur l'instance MISP . Ce champ n'est visible que par les administrateurs.
Org. du créateur	Organisation qui a créé l'événement sur l'instance MISP .
Distribution	Distribution de l'attribut individuel. Un attribut peut avoir un niveau de distribution différent de celui de l'événement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue de liste d'événements MISP (suite)

Champ	Description
Lien hypertexte d'événement MISP	Lien vers l'événement MISP qui est stocké sur le MISP serveur.
Source MISP	MISP Source où l'événement est créé.

MISP Données d'événement dans la vue de formulaire

Utilisez la vue de formulaire pour obtenir des informations détaillées sur les MISP événements.

Vue de formulaire d'événement MISP

Champ	Description
ID d'événement	ID d'événement attribué lors de MISP la première création ou importation de l'événement dans le MISP serveur.
UUID	ID qui identifie de manière unique les événements et les attributs.
Org. du créateur	Organisation qui a créé l'événement sur l'instance MISP .
Org. du propriétaire	Organisation propriétaire de l'événement sur l'instance MISP . Ce champ n'est visible que par les administrateurs.
Créateur	Utilisateur qui a créé l'événement dans MISP.
Dernier changement	Date de la dernière modification de l'événement.
Source MISP	MISP Source où l'événement est créé.
Date de création (dans MISP)	Date de création ou de première importation de l'événement sur le MISP serveur.
Niveau de menace	Niveau de risque de l'événement. Les incidents peuvent être classés en trois catégories de menaces différentes (faible, moyenne, élevée). Ce champ peut être laissé comme non défini. Les options sont les suivantes : • Faible : logiciel malveillant de masse général • Moyen : menaces persistantes avancées (APT) • Élevée : APT sophistiquées et attaques sur 0 jour
Analyse	Étape actuelle de l'analyse de l'événement avec les options possibles suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue de formulaire d'événement MISP (suite)

Champ	Description
	• Initial : l'analyse ne fait que commencer • En cours : l'analyse est en cours • Terminé : l'analyse est terminée
Distribution	Distribution de l'attribut individuel. Un attribut peut avoir un niveau de distribution différent de celui de l'événement.
Publié	État indiquant si l'événement a été publié ou non. La publication permet d'utiliser les attributs de l'événement pour toutes les exportations éligibles et notifie les utilisateurs qui se sont abonnés aux alertes d'événement.
Lien hypertexte d'événement MISP	Lien vers l'événement MISP qui est stocké sur le MISP serveur.
Info	Brève description de l'événement.
Balises (locales)	Balises disponibles sur l'instance de l'organisation hôte pour activer le balisage à des fins de MISP synchronisation et de filtrage des exportations. MISP Les événements ne sont pas modifiés lorsque vous utilisez des balises locales. Les balises locales sont toujours supprimées avant d'être synchronisées avec d'autres MISP instances et de partager des communautés.
Balises (globales)	Balises disponibles globalement pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des balises globales à MISP des instances, vous pouvez modifier les événements.
Galaxies (locales)	Galaxies disponibles sur l'instance de l'organisation hôte pour le filtrage de synchronisation et d'exportation. MISP Les événements ne sont pas modifiés lorsque vous utilisez des galaxies MISP locales. Ces galaxies locales sont toujours dépouillées avant d'être synchronisées avec d'autres MISP instances et communautés de partage.
Galaxies (globales)	Galaxies disponibles dans le monde entier pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des galaxies globales, MISP vous pouvez modifier les événements.

Événements associés MISP

Vous pouvez utiliser la vue de liste Événements associés MISP pour afficher les événements qui ont été créés manuellement ou automatiquement dans le contexte d'un incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Événements MISP associés

Champ	Description
Incident de sécurité	SIR Incident de sécurité. Cliquez sur l'incident de sécurité pour afficher l'incident de sécurité.
Événement MISP	MISP ID d'événement. Cliquez sur l'événement MISP pour l'afficher MISP dans le ServiceNow AI Platform.
Source MISP	MISP Source où l'événement est créé. Cliquez sur la MISP source pour afficher la source.
Mode de création d'événements	État indiquant si l'événement a été créé manuellement ou automatiquement avec le profil de création d'événement. Cliquez sur l'événement MISP pour afficher l'événement associé MISP .
Profil de création automatique d'événements	Profil de création d'événement utilisé pour créer l'événement automatique. Cliquez sur le profil pour afficher le profil de création automatique d'événements MISP.

MISP Informations utilisateur

Vous pouvez utiliser la MISP page Informations utilisateur pour afficher tous les utilisateurs associés pour le ServiceNow AI Platform MISP integration for Security Operations.

Informations sur l'utilisateur MISP

Champ	Description
Source	Source du MISP compte utilisateur.
ID d'utilisateur	ID d'utilisateur affecté par le serveur lors de la création d'un MISP compte utilisateur.
E-mail de l'utilisateur	Adresse e-mail d'un utilisateur. Seuls les administrateurs d'organisation peuvent voir les adresses e-mail des utilisateurs de leur propre organisation.
Organisation	Organisation à laquelle appartient un utilisateur.
Nom de rôle	Nom de rôle qui définit les privilèges utilisateur attribués à un utilisateur. Pour plus d'informations sur les rôles dans MISP, consultez la documentation MISP .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations sur l'utilisateur MISP (suite)

Champ	Description
ID de rôle	ID du rôle d'utilisateur dans MISP. Par exemple, Administrateur permanent, Audit permanent ou Tagueur permanent, etc.
Autorisation	Autorisations dont dispose un utilisateur. Les autorisations disponibles dans MISP sont les suivantes : • Lecture seule • Gérer ses propres événements • Gérer les événements de l'organisation • Gérer Publier les événements de l'organisation
Autorisation de perception	Autorisation qui permet à un utilisateur d'effectuer des recherches de perception.
Autorisation du tagueur	Autorisation qui permet à un utilisateur d'effectuer un balisage.

Séparation de domaine et MISP

L'application Séparation de domaine est prise en charge dans MISP. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Prise en charge : Basique.

Comment fonctionne Séparation de domaine avec MISP

Pour procéder à la séparation en domaines, procédez comme suit :

- Créez un utilisateur avec les rôles requis dans votre domaine.
- Effectuez les MISP integration for Security Operations procédures dans votre domaine.

Dépannage de l'intégration MISP

Cette section présente des conseils de dépannage importants qui peuvent vous aider à résoudre les problèmes courants que vous pouvez rencontrer lors de la configuration ou de l'exécution de l'intégration MISP.

Problèmes SSL

Lors de la connexion via l'intégration MISP, assurez-vous d'avoir installé un certificat CA valide sur le serveur MISP, qui n'a pas expiré. Vous pouvez importer RSA ou vos propres certificats dans la plateforme et vous assurer que le nom commun du certificat correspond au nom d'hôte. Pour plus d'informations, consultez Installez et configurez le MISP integration for Security Operations et MISP Rôles et autorisations d'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisation MISP pour enquêter et analyser les menaces

Vous pouvez utiliser les MISP données du module et du ServiceNow AI Platform Renseignements sur les menacesServiceNow AI Platform SIR module pour examiner et analyser les menaces qui pèsent sur votre organisation.

Recherches de perception dans MISP

Vous pouvez effectuer des recherches de perception sur les observables de l'instance MISP pour déterminer la fréquence à laquelle certains types d'attaques, tels que les attaques d'hameçonnage ou les communications avec une adresse IP ou une URL malveillante, se produisent sur votre réseau. Chaque occurrence est considérée comme une observation.

Perceptions dans MISP

Les observations indiquent qu'un indicateur, un objet ou un attribut a été vu et que sa validité est confirmée. Sightings in MISP est un système qui vous permet de répondre aux attributs d'un événement. Il est conçu pour fournir une méthode facile à vos utilisateurs pour confirmer qu'ils ont vu un attribut donné, ce qui lui donne plus de crédibilité. Vous pouvez voir un attribut plusieurs fois.

Remarque : Les observables sont appelés attributs dans MISP.

Certains attributs sont considérés comme des faux positifs, ce qui signifie qu'il ne s'agit pas d'observations valides. D'autres attributs ne sont valides que pendant une certaine durée, comme une campagne d'hameçonnage qui ne dure qu'une semaine. Vous pouvez affecter une date d'expiration aux attributs qui sont valides pour une certaine durée, mais chaque organisation ne peut affecter qu'une seule date d'expiration valide à un attribut.

Les perceptions créées MISP par les utilisateurs des organisations marquées comme locales dans le serveur MISP correspondant sont appelées perceptions internes. Les perceptions créées MISP par les utilisateurs des organisations marquées comme distantes dans le serveur correspondant MISP sont appelées perceptions externes.

Recherches de perception dans SIR

Le workflow Security Operations Integration - Sightings Search exécute la recherche de perceptions. Ce flux accepte une liste d'observables, recherche les options en cours d'implémentation, crée les requêtes basées sur les configurations de recherche de perceptions et exécute les recherches basées sur le flux configuré .

Les recherches de perception aident les analystes à déterminer la prévalence d'une menace au fil du temps. Vous pouvez sélectionner un ou plusieurs observables et la plage de dates de votre recherche à partir d'un incident de sécurité. Les résultats sont inclus dans les listes connexes Détections d'incidents de sécurité, Résultats de recherche de perception et Détails de recherche de perceptions .

Lorsque vous commencez à analyser un incident, vous pouvez configurer votre ServiceNow AI Platform pour effectuer automatiquement une recherche de perceptions ou effectuer manuellement une recherche de perceptions observables afin d'identifier les autres utilisateurs de votre organisation qui sont impactés par la même attaque de phishing.

Activer les recherches automatiques de perception dans MISP

Activez l'exécution automatique de la recherche de perception dans MISP afin que le workflow Security Operations Integration - Recherche de perceptions soit déclenché chaque fois que de nouveaux observables sont associés à un incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Vérifiez que le Profil de configuration de la recherche de perceptions pour MISP est actif.

Rôle requis : sn_si.analyst

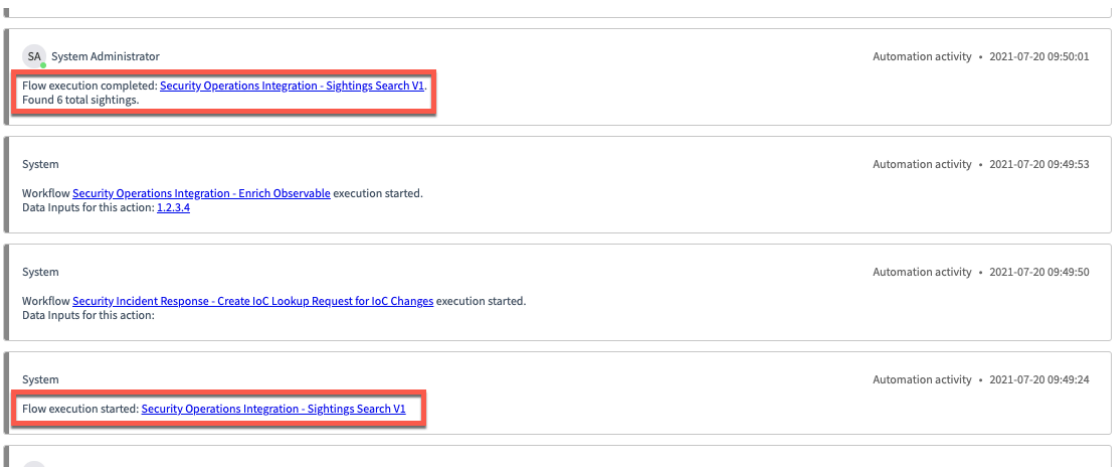
Pourquoi et quand exécuter cette tâche

Si vous activez l'aptitude de recherche de perception à exécuter automatiquement dans le MISP Configuration de l'intégration, la recherche de perception dans MISP se déclenche lorsque de nouveaux observables sont associés à un incident de sécurité. Par défaut, l'option **Exécuter automatiquement la recherche de perception lorsque de nouveaux observables sont associés à l'incident de sécurité** est activée.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables que vous souhaitez afficher dans les données de recherche d'observations MISP .
3. Examinez les notes de travail après que de nouveaux observables ont été associés à l'incident de sécurité. Une note de travail est publiée lorsque le workflow Security Operations Integration - Recherche de perceptions s'est déclenché.

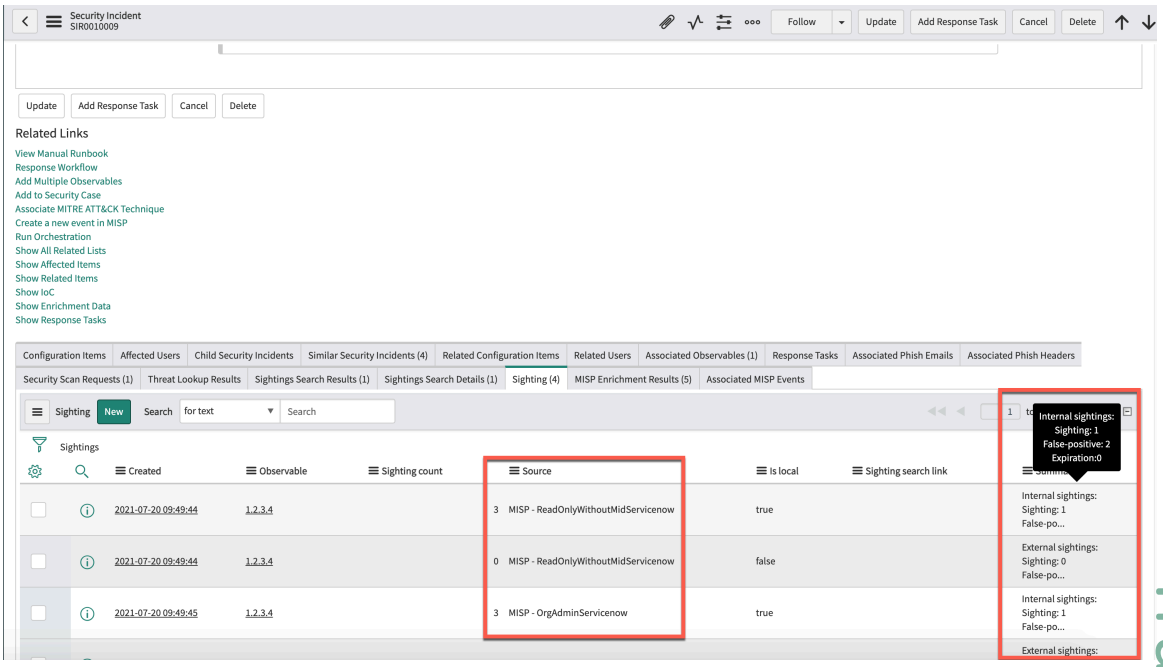
   L'exemple suivant montre la section des notes de travail.



4. Affichez les informations agrégées des observables qui sont vues dans tous les événements (globaux) et classées en fonction de leurs perceptions internes ou externes une fois l'exécution du workflow terminée. Affichez les informations contenues dans les listes connexes Perceptions, Résultats de recherche de perception et Détails de recherche de perception . L'exemple suivant montre l'enregistrement de recherche de perceptions qui a été créé dans la liste connexe Perceptions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Enregistrement de recherche de perceptions

Champ	Description
Créées	Date et heure de création de l'enregistrement de recherche d'observations.
Observable	Observable recherché par la requête.
Nombre de perception	Nombre de perceptions internes et externes.
Source	Source de l'observable. Si l'observable provient d'une MISP organisation, l'enregistrement est précédé des mots MISP.
Est local	État indiquant si l'observation a été signalée par un utilisateur interne.
Lien de recherche sur la perception	Lien de recherche de perception dans l'instance MISP .
Résumé	Type d'observations associées à l'enregistrement. Les trois types d'observations sont la perception, le faux positif et l'expiration. La colonne Résumé s'affiche uniquement lorsque le est MISP integration for Security Operations installé. Si des sources autres que MISP s'affichent, l'entrée de la colonne Résumé est vide pour cet enregistrement.

Effectuer une recherche de perception manuelle dans MISP

Sélectionnez un ou plusieurs observables et effectuez une recherche de perception manuelle dans l'application ServiceNow AI Platform MISP integration for Security Operations pour déterminer la prévalence d'une menace au fil du temps.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables dont vous souhaitez exécuter la recherche d'observations MISP .
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Sélectionnez l'observable, puis dans le menu Actions, cliquez sur **Exécuter la recherche de perceptions**.
   Vous pouvez sélectionner plusieurs observables pour une recherche d'observations.
   La boîte de dialogue Exécuter la recherche de perception s'ouvre.
5. Spécifiez la plage de dates pour rechercher les données de recherche d'observations.

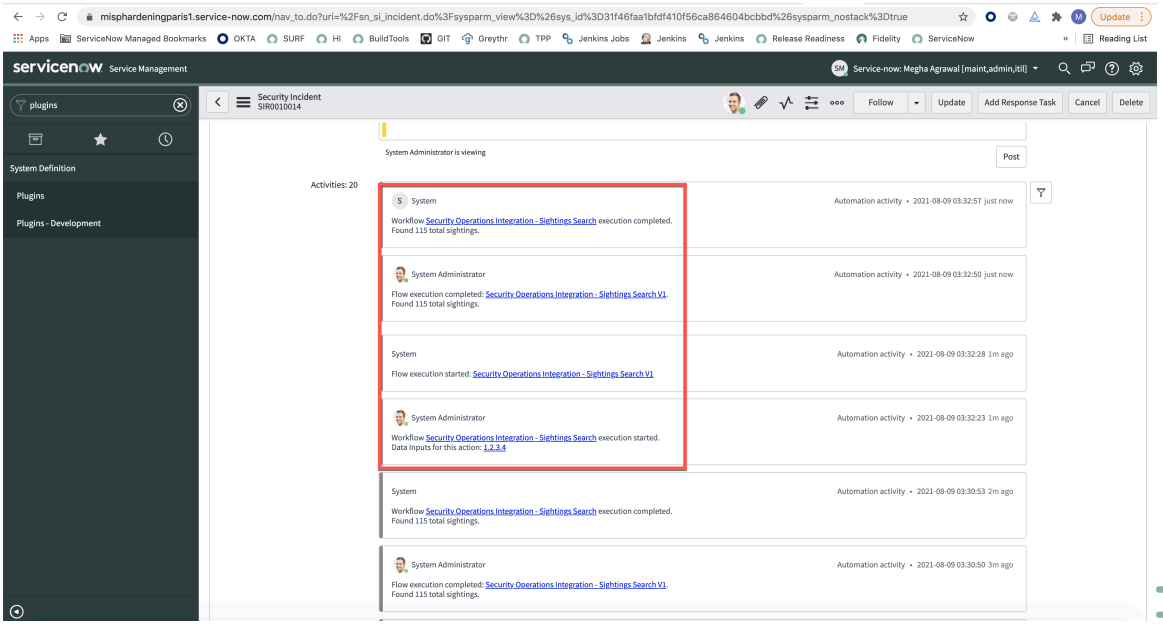
Boîte de dialogue Exécuter la recherche de perception

Champ	Description
Dernier	Nombre d'heures ou de jours avant la création de l'incident à rechercher. La valeur par défaut est de 7 jours. La limite est de 99 heures ou jours.
entre	Plage de dates à rechercher. Les dates par défaut sont les suivantes : ○ Date et heure de création de l'incident. ○ Date et heure qui précèdent de sept jours l'ouverture de l'incident.

6. Cliquez sur **Rechercher**.
   L'exemple suivant montre les résultats de la recherche de perception manuelle dans les notes de travail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Résultats

Un enregistrement de recherche de perceptions est créé. Une fois l'exécution du workflow terminée, vous pouvez afficher les informations agrégées des observables qui sont observées dans tous les événements (globaux) et classées en fonction de leurs perceptions internes ou externes. Les données d'agrégat et les observations associées sont affichées dans l'incident de sécurité dans les listes connexes Perceptions, Résultats de recherche de perceptions et Détails de recherche de perceptions .

Signaler des observations à MISP

Signalez les détections de données de menaces afin de pouvoir réagir aux faux positifs dans vos données et augmentez votre sensibilisation lorsqu'une menace réelle et positive se produit. Vous pouvez également ajouter une date d'expiration pour un observable ou un attribut particulier.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Cela MISP integration for Security Operations vous permet de rapporter globalement MISP des observations pour tous les événements. Pour signaler une observation à un événement spécifique, vous devez utiliser l'instance MISP et signaler l'observation localement.

Pour signaler une observation à MISP, l'observable ou l'attribut doit être disponible dans l'instance MISP .

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour MISP lesquels vous souhaitez signaler les observations.
3. Cliquez sur **Afficher toutes les listes connexes** et la liste connexe Observations.
4. Sélectionnez l'observable et, dans le menu Actions, sélectionnez l'une des options suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
MISP : signaler une observation observable	Signaler l'observable comme vu à MISP. Si l'observable est associé à plusieurs événements, il est mis à jour dans tous les événements.
MISP : signaler l'observable comme faux positif	Signalez l'observable comme faux positif à MISP.
MISP : signaler l'observable comme expiré	Signaler l'observable comme expiré à MISP.

Si vous sélectionnez des observables qui ne sont pas spécifiques à une MISP source, le menu Actions affiche le nombre de sources pertinentes MISP . L'exemple suivant montre quatre des huit observables comme étant pertinents pour MISP. L'exemple suivant montre le menu Actions et les observables pertinents pour la soumission.

Menu Actions affichant les observables pertinents pour la soumission



5. **Facultatif :** Si vous avez sélectionné l'option **MISP : signaler la perception observable** , vous devez remplir les champs de la boîte de dialogue Signaler la perception observable sur MISP.

Boîte de dialogue Signaler la perception observable dans MISP

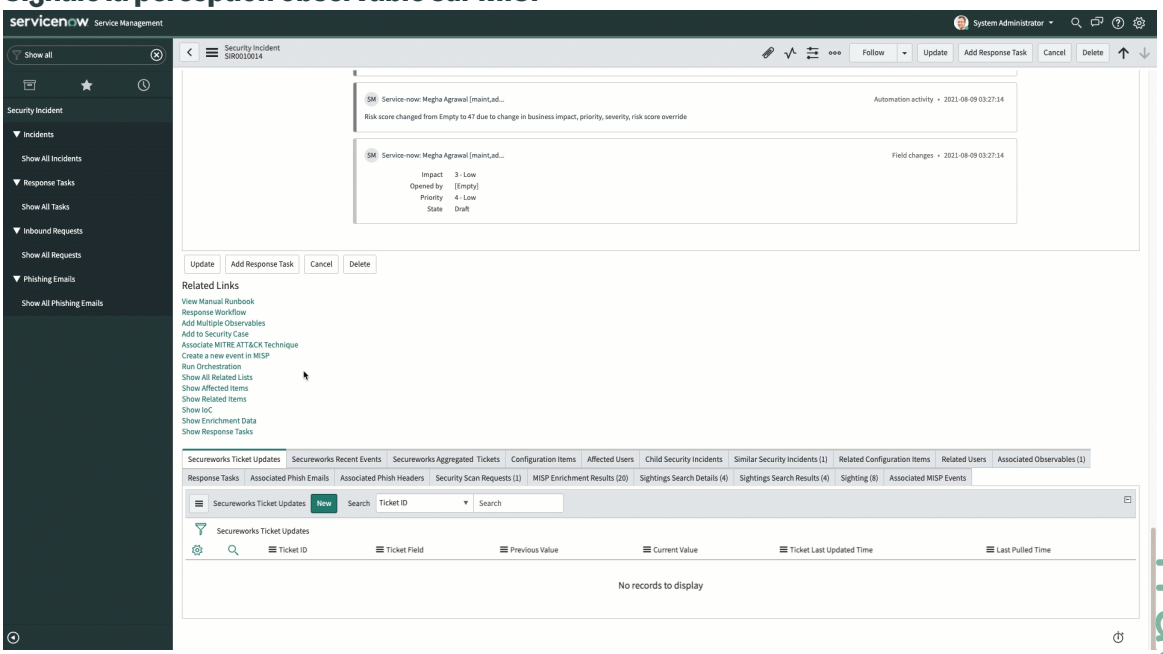
Champ	Description
Source	Champ source correspondant à la MISP source de l'observation.
Date	Champ de date correspondant à la date à laquelle l'observable est observé. Si la date est vide, la date et l'heure actuelles sont renseignées dans MISP.

L'exemple suivant montre comment accéder à la liste connexe Perceptions dans l'incident de sécurité. Dans cette liste, vous pouvez sélectionner un observable et signaler l'observation observable à MISP. Le message de réussite montre que l'observation a été soumise avec succès à MISP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signale la perception observable sur MISP



a. Cliquez sur **Signaler une observation**.

6. **Facultatif :** Si vous avez sélectionné l'option **MISP : signaler un observable comme faux positif** , vous devez remplir les champs de la boîte de dialogue Signaler l'observable comme faux positif à MISP .

Boîte de dialogue Signaler l'observable comme faux positif à MISP

Champ	Description
Source (facultatif)	Champ source correspondant à la MISP source. Utilisez ce champ pour déclarer l'observable comme faux positif.
Date	Champ de date correspondant à la date à laquelle il a été déterminé que l'observable est un faux positif. Si la date est vide, la date et l'heure actuelles sont renseignées dans MISP.

a. Cliquez sur **Signaler un faux positif**.

7. **Facultatif :** Si vous avez sélectionné l'option **MISP : signaler l'observable comme expiré** , vous devez remplir les champs de la boîte de dialogue Signaler l'expiration de l'observable à MISP .

Boîte de dialogue Signaler l'expiration de l'observable à MISP

Champ	Description
Source	Champ source correspondant à la MISP source. Utilisez ce champ pour définir un observable comme expiré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Date	Champ de date correspondant à la date à laquelle l'observable a expiré. Si la date est vide, la date et l'heure actuelles sont renseignées dans MISP.

a. Cliquez sur **Expiration du rapport**.

Résultats
Les perceptions ont été mises à jour avec succès vers le MISP serveur.

Enrichissement des observables dans MISP

En enrichissant les observables avec des informations supplémentaires provenant de diverses MISP sources au cours des enquêtes de réponse aux incidents, vous pouvez contenir les menaces identifiées.

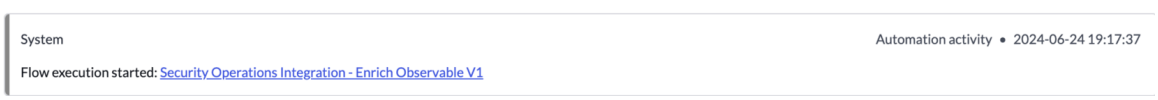
Activer l'enrichissement automatique des observables dans MISP

Activez l'enrichissement automatique des observables lorsque ServiceNow AI Platform MISP de nouveaux observables sont associés à l'incident de sécurité.

Avant de commencer
- Activez la Réponse aux incidents de sécurité propriété système pour l'option **Active ou désactive la tâche planifiée, Rechercher les observables d'incident de sécurité** pour déclencher l'aptitude d'enrichissement des observables dans SIR.
- Rôle requis : sn_si.analyst

Procédure
1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour MISP lesquels vous souhaitez enrichir les données observables.
3. Examinez les notes de travail après que de nouveaux observables ont été associés à l'incident de sécurité.

   L'exemple suivant montre qu'une note de travail est publiée lorsque le flux Security Operations Integration - Enrich Observable se déclenche .



4. Dans la liste connexe Résultats de l'enrichissement MISP de l'incident de sécurité, affichez les résultats de l'enrichissement une fois l'exécution du flux terminée.

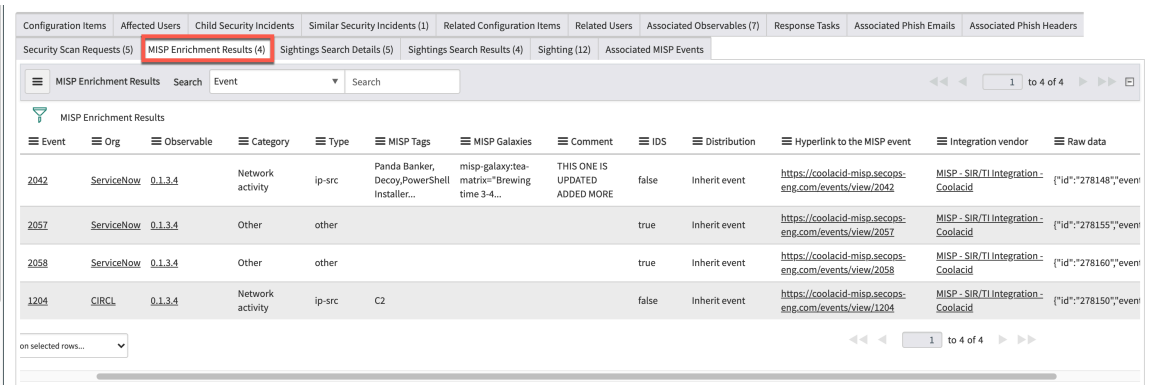


Remarque : Vous devez configurer la liste connexe des résultats de l'enrichissement MISP dans les listes connexes des incidents de sécurité. Pour plus d'informations, consultez la configuration de la liste connexe.

L'exemple suivant montre les résultats de l'enrichissement dans le MISP fichier .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La table suivante présente les résultats de l'enrichissement MISP.

Résultats de l'enrichissement MISP

Champ	Description
Événement	ID de l'événement. Cliquez sur Ouvrir pour afficher l'enregistrement dans l'instance ServiceNow AI Platform .
Org	Organisation qui a initialement créé l'événement.
Observable	Observable associé à l'événement.
Catégorie	Catégorie de l'attribut. Affichez la liste des catégories dans la documentation MISP .
Type	Type de l'attribut. Affichez la liste des types dans la documentation du MISP .
Balises MISP	Liste des balises associées à l'attribut MISP .
Galaxies MISP	Liste des galaxies associées à l'attribut MISP .
Commentaire	Commentaire contextuel permettant de décrire plus précisément l'attribut. Ces commentaires ne sont pas utilisés à des fins de corrélation et sont purement informatifs.
IDS	Indicateur de compromis, qui permet de l'inclure dans toutes les exportations éligibles.
Distribution	Distribution de l'attribut après sa publication. Un attribut peut avoir un niveau de distribution différent de celui de l'événement. Dans les deux cas, le niveau de distribution le plus bas est utilisé.
Lien hypertexte vers l'événement MISP	Lien vers l'événement MISP , qui est stocké sur le MISP serveur.
Fournisseur de l'intégration	Fournisseur d'intégration qui fournit les données pour l'enrichissement.
Données brutes	Données brutes associées à l'attribut MISP .

Traduction automatique

Effectuer un enrichissement manuel de l'observable dans MISP

Sélectionnez un ou plusieurs observables et procédez à un enrichissement manuel des observables afin de pouvoir enrichir les observables avec des informations supplémentaires provenant de diverses MISP sources.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour lesquels vous souhaitez effectuer l'enrichissement.
3. Cliquez sur **Afficher toutes les listes connexes** et l'onglet **Observables associés** .
4. Sélectionnez l'observable et, dans le menu Actions, cliquez sur **Exécuter l'enrichissement de l'observable**.
   Vous pouvez sélectionner plusieurs observables pour une recherche d'observations.
   La boîte de dialogue Exécuter l'enrichissement de l'observable s'affiche.
5. Sélectionnez une MISP source et, dans la colonne Sélectionné, sélectionnez une implémentation pour enrichir les observables sélectionnés.
6. Cliquez sur **Envoyer**.
   Une note de travail indique que le workflow Intégration de Security Operations - Enrichir les observables a été déclenché. Les workflows d'implémentation associés s'exécutent pour effectuer l'enrichissement. Vous pouvez consulter les notes de travail dans l'incident de sécurité pour afficher l'état.

   L'exemple suivant montre comment afficher les notes de travail pour un enrichissement manuel des observables.

Notes de travail pour l'enrichissement manuel des observables



Le message d'enrichissement répertorie l'événement créé. Vous pouvez afficher l'événement dans le ServiceNow AI Platform ou dans l'instance MISP et afficher les détails de l'enregistrement dans l'onglet Résultats de l'enrichissement MISP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter ou supprimer des balises aux MISP attributs

Ajoutez ou supprimez des balises MISP pour classer des événements ou des attributs. Vous pouvez utiliser le balisage globalement pour activer votre classification ou utiliser des balises localement lorsque vous ne souhaitez MISP pas que les événements soient modifiés pendant votre classification.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Vérifiez que l'attribut que vous modifiez appartient à la même organisation que l'utilisateur MISP .
- Notez que les balises et les galaxies disponibles sont basées sur la MISP source et ses autorisations de distribution.
- Rôle requis : sn_sec_misp.write

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables, les attributs ou les événements pour lesquels vous souhaitez ajouter les balises.
3. Cliquez sur **Afficher toutes les listes connexes** et la liste connexe Résultats de l'enrichissement MISP.
4. Cliquez sur l'icône ⓘ regard d'un enregistrement, puis cliquez sur **Ouvrir l'enregistrement**. L'exemple suivant montre comment examiner les **résultats d'enrichissement MISP** et comment ouvrir un MISP enregistrement d'enrichissement.

   Enregistrement du résultat de l'enrichissement MISP
   Ouverture de l'enregistrement du résultat de l'enrichissement MISP

5. Examiner l'enregistrement du résultat de l'enrichissement MISP.

Résultat de l'enrichissement MISP

Champ	Description
Observable	
Événement	ID d'événement affecté par le serveur lors de la MISP première création ou importation de l'événement dans MISP. Prévisualisez l'événement ou cliquez sur l'enregistrement pour afficher les données d'événement dans la page Données d'événement MISP .
Org	Organisation qui a créé l'attribut MISP .
Catégorie	Catégorie de l'attribut que vous ajoutez à l'événement spécifique dans MISP. Vous pouvez sélectionner une option telle qu'une référence interne, une activité réseau, une fraude financière, etc.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type	Type d’attribut MISP .
Fournisseur de l'intégration	Fournisseur d’intégration qui fournit les données d’enrichissement de l’observable.
Date de création (dans MISP)	Date à laquelle l’événement a été créé ou importé pour la première fois MISP.
IDS	État indiquant si un observable est marqué comme malveillant dans SIR. L’attribut correspondant dans MISP est également marqué comme vrai.
Distribution	Contrôles d’option de distribution, par exemple qui peut afficher cet événement après sa publication. Cette option contrôle également si l’événement est synchronisé avec d’autres serveurs. La distribution est héritée par les attributs, et le paramètre le plus restrictif l’emporte. Les options de distribution sont les suivantes : ○ Votre organisation uniquement : autorise uniquement les membres de votre organisation à afficher cet événement. L’événement peut être transféré vers une autre instance par l’un des membres de votre organisation, où seule votre organisation a accès pour l’afficher. Les événements avec ce paramètre ne sont pas synchronisés. ○ Cette communauté uniquement : permet aux utilisateurs qui font partie de votre MISP communauté d’afficher l’événement, y compris votre propre organisation, les organisations sur ce MISP serveur et les organisations qui exécutent MISP des serveurs qui se synchronisent avec ce serveur. Toute autre organisation connectée à ces serveurs liés ne peut pas voir l’événement. ○ Communautés connectées : permet aux utilisateurs qui font partie de votre MISP communauté d’afficher l’événement, y compris toutes les organisations sur ce serveur, toutes les organisations sur MISP les MISP serveurs qui se synchronisent avec ce serveur et les organisations d’hébergement des serveurs qui se connectent à n’importe quel serveur situé à deux sauts de distance. Toutes les autres organisations connectées aux serveurs liés qui se trouvent à deux sauts de distance ne peuvent pas voir l’événement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Toutes les communautés : partage l'événement avec toutes les MISP communautés, ce qui permet à l'événement d'être disponible gratuitement.
Lien hypertexte vers l'événement MISP	Lien vers l'événement MISP qui est stocké sur le MISP serveur.
Données brutes	Détails bruts pour l'enregistrement des données d'enrichissement des observables.
Commentaire	Commentaires que vous ajoutez pour les attributs. Ces commentaires sont fournis à titre informatif uniquement et ne sont pas utilisés à des fins de corrélation.
Balises (locales)	Balises disponibles sur l'instance de l'organisation hôte pour activer le balisage à des fins de MISP synchronisation et de filtrage des exportations. MISP Les événements ne sont pas modifiés lorsque vous utilisez des balises locales. Ces balises sont toujours supprimées avant d'être synchronisées avec d'autres instances et communautés de MISP partage.
Balises (globales)	Balises disponibles globalement pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des balises globales à MISP des instances, vous modifiez les événements.
Galaxies (locales)	Galaxies disponibles sur l'instance de l'organisation hôte pour le filtrage de synchronisation et d'exportation. MISP Les événements ne sont pas modifiés lorsque vous utilisez des galaxies MISP locales. Ces galaxies sont toujours dépouillées avant d'être synchronisées avec d'autres instances et communautés de MISP partage.
Galaxies (globales)	Galaxies disponibles dans le monde entier pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des galaxies globales, MISP les événements sont modifiés.

Traduction automatique

6. Pour modifier une balise locale ou globale, cliquez sur l'icône icône Modifier dans l'une des options suivantes :

   - **Balises (locales)**
   - **Balises (globales)**

7. Dans la boîte de dialogue Balises d'attribut MISP, entrez le nom de la balise à rechercher et pour l'ajouter.
8. Cliquez sur **Mettre à jour les balises sur l'attribut MISP**.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'exemple suivant montre qu'en cliquant sur l'icône de modification des balises locales, vous pouvez rechercher et ajouter les balises C3, Adware, C2 et Botnet 3101, et mettre à jour le serveur MISP avec les balises. Le message de confirmation indique que toutes les balises ont été mises à jour dans MISP.

Ajout de balises locales dans l'attribut MISP.
Les balises sont mises à jour avec succès dans le MISP serveur.

9. Pour afficher les changements dans l'enregistrement, cliquez sur **Recharger le formulaire** dans le message de réussite.

Ajouter ou supprimer des galaxies à un événement ou à un MISP attribut

Ajoutez ou supprimez des galaxies MISP afin de pouvoir classer ces objets en tant que cluster MISP et les attacher à des événements ou à MISP des attributs.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Pour ajouter des galaxies locales, l'utilisateur qui a configuré l'intégration doit appartenir à l'organisation hôte du serveur correspondant MISP .
- Notez que les balises et les galaxies disponibles sont basées sur la MISP source et ses autorisations de distribution.
- Rôle requis : sn_sec_misp.write

Procédure

1. Cliquez sur l'icône dans l'une des options suivantes.

- **Galaxies (locales)**
- **Galaxies (globales)**

2. Dans la boîte de dialogue Galaxies d'événements MISP, renseignez les détails.

Boîte de dialogue Galaxies d'événements MISP

Champ	Description
ID d'événement	ID d'événement affecté par le serveur lors de la MISP première création ou importation de l'événement dans MISP.
Espace de noms	Espace de noms où la galaxie est stockée. Vous pouvez utiliser des espaces de noms pour regrouper des galaxies similaires.
Galaxies	Galaxie dans laquelle vous stockez les informations du cluster.
Grappes	Informations sur les amas de la galaxie.

3. Cliquez sur **Mettre à jour les galaxies vers l'attribut MISP**.
L'exemple suivant montre qu'en cliquant sur l'icône d'édition des galaxies locales, vous pouvez sélectionner l'espace de noms obsolète, sélectionner la galaxie Enterprise Attack - Attack Pattern et ajouter les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

informations de cluster. Une fois les informations sur la galaxie mises à jour, vous pouvez afficher le message de réussite.

Ajout d'informations sur les galaxies dans MISP via la commande ServiceNow AI Platform

4. Pour afficher les changements dans l'enregistrement, cliquez sur **Recharger le formulaire** dans le message de réussite.

Résultats
Les informations sur les galaxies sont mises à jour avec succès dans le MISP serveur.

Ajouter des commentaires à l'attribut MISP

Ajoutez des commentaires pour les MISP attributs. Les commentaires que vous ajoutez le sont à des fins d'information uniquement et ne sont pas utilisés à des fins de corrélation de MISP données.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Vérifiez que l'attribut que vous modifiez appartient à la même organisation que l'utilisateur MISP .
- Rôle requis : sn_sec_misp.write

Procédure

1. Cliquez sur l'icône dans le champ Commentaire.
2. Saisissez votre commentaire dans le champ Commentaire d'attribut.
3. Cliquez sur **Mettre à jour un commentaire sur l'attribut MISP**.
   L'exemple suivant montre qu'en cliquant sur l'icône de modification en regard du champ de commentaire, vous pouvez ajouter un commentaire, puis mettre à jour l'attribut MISP . Une fois le commentaire mis à jour, vous pouvez afficher le message de réussite.

   Ajout d'informations sur les galaxies dans MISP via le ServiceNow AI Platform fichier .

4. Pour afficher les changements dans l'enregistrement, cliquez sur **Recharger le formulaire** dans le message de réussite.

Résultats
Le commentaire est mis à jour avec succès dans le MISP serveur.

Gestion des événements dans MISP

Vous pouvez créer des événements automatiquement ou manuellement à MISP partir de .ServiceNow AI Platform Vous pouvez également modifier les données d'événement dans MISP le ServiceNow AI Platform fichier .

Vérification des événements créés automatiquement dans MISP

Vous pouvez vérifier les événements créés automatiquement après avoir configuré le profil de création d'événements dans votre ServiceNow AI Platform instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Profil de création automatique d'événements

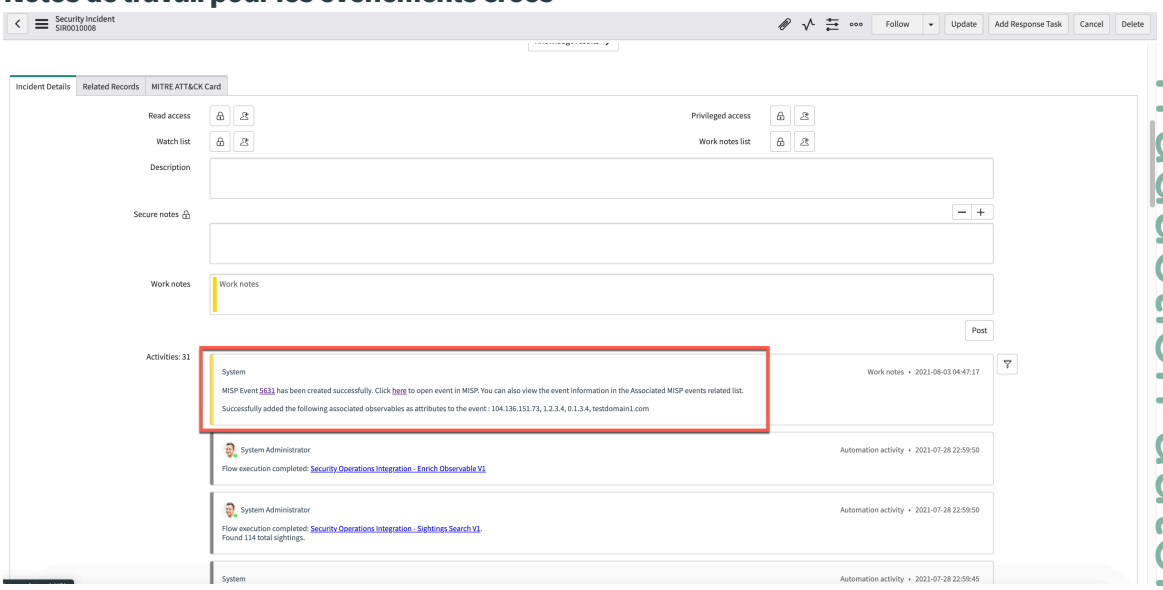
La configuration du profil de création automatique d'événements est effectuée par les rôles d'utilisateur sn_si.admin ou sn_ti.admin dans le **Intégration de MISP** > **Profils de création automatique d'événements** module.

Afficher les données de l'événement MISP

Vous pouvez afficher les événements créés des manières suivantes :

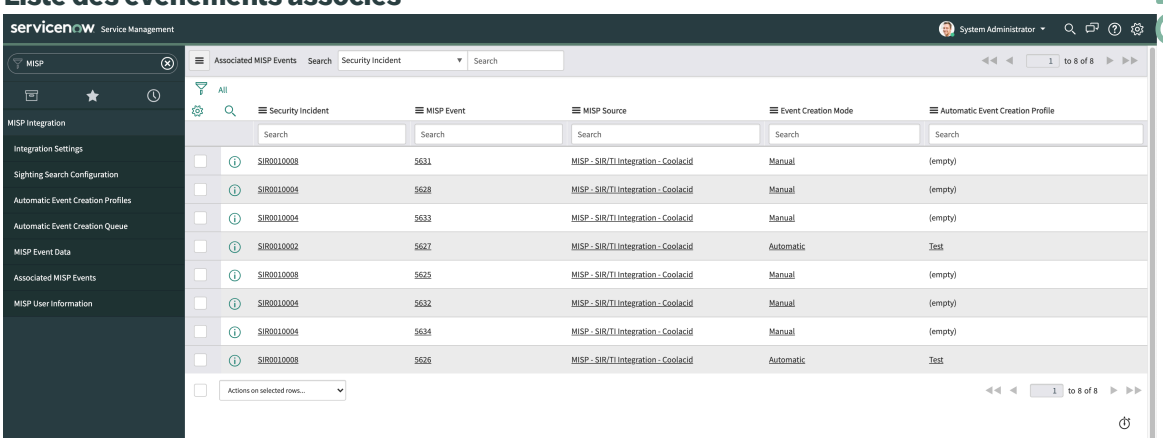
- Affichez les notes de travail pour les événements créés. Vous pouvez afficher les détails de l'événement dans l'instance ServiceNow AI Platform ainsi que tels qu'ils apparaissent sur le MISP serveur, comme indiqué dans l'exemple suivant.

Notes de travail pour les événements créés



- Cliquez sur la liste connexe Événements MISP associés . Ici, vous pouvez afficher l'événement par rapport à l'incident de sécurité et aux MISP ressources, comme illustré dans l'exemple suivant.

Liste des événements associés

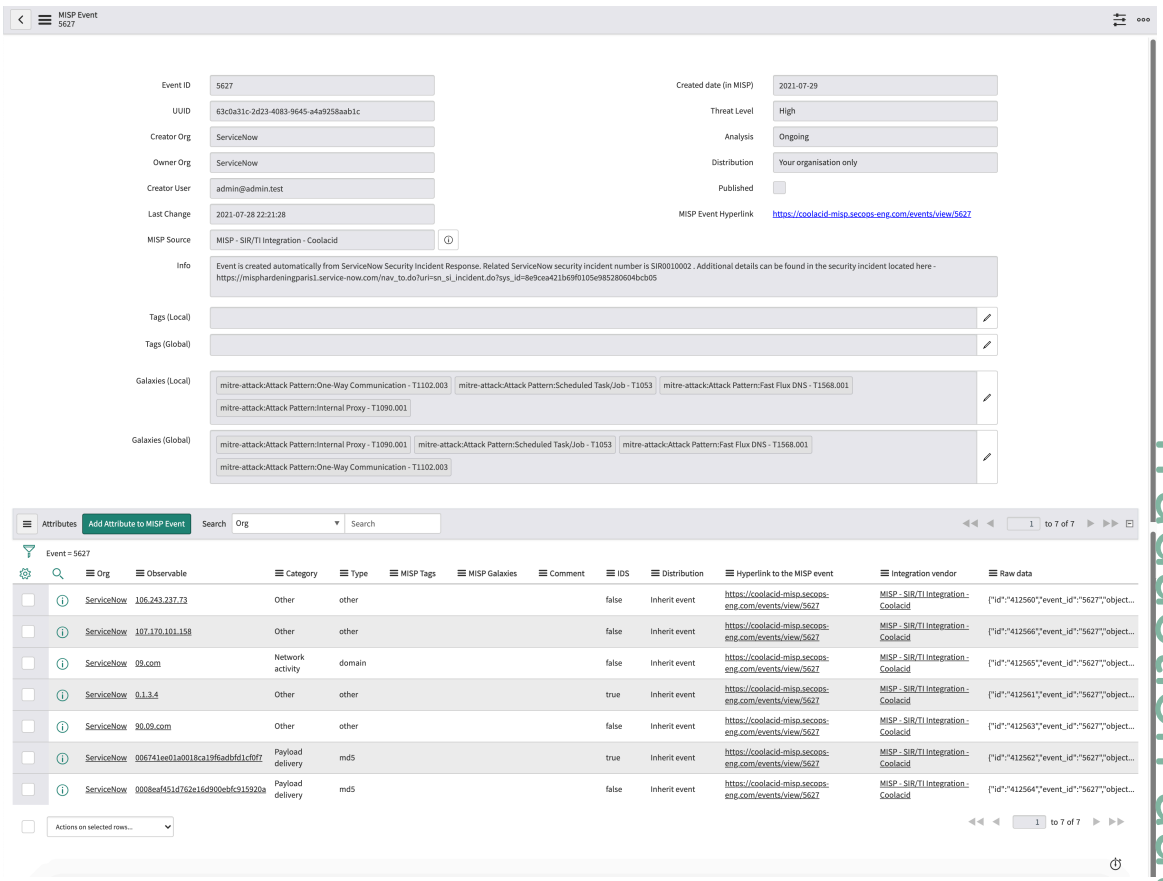


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Affichez les données d'événement MISP dans la vue de formulaire pour examiner les informations détaillées sur les MISP événements, comme indiqué dans l'exemple suivant.

Données d'événement dans la vue de formulaire



Créer manuellement un événement dans MISP

Créez manuellement des événements à MISP partir de pour capturer des informations contextuelles représentées sous forme d'attributs et d'objets ServiceNow AI Platform .

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Rôle requis : sn_sec_misp.write

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient les observables pour lesquels vous souhaitez créer un événement.
3. Cliquez sur **Créer un nouvel événement dans MISP**.
4. Dans la boîte de dialogue Créer un nouvel événement dans MISP, renseignez les détails.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un événement dans la boîte de dialogue MISP

Champ	Description
Date	Date de création de l'événement dans MISP.
Informations sur l'événement	Informations sur l'événement qui sont automatiquement créées à partir du ServiceNow AI Platform Réponse aux incidents de sécurité.
Niveau de menace	Niveau de risque de l'événement. Vous pouvez classer les incidents en trois catégories de menaces différentes (faible, moyenne, élevée). Ce champ peut également être laissé non défini. Les options sont les suivantes : ○ Faible : logiciel malveillant de masse général ○ Moyen : menaces persistantes avancées (APT) ○ Élevée : APT sophistiquées et attaques sur 0 jour
Source	MISP Source pour la création de l'événement.
Distribution	Option qui contrôle qui peut afficher cet événement après la publication de l'événement. Cette option contrôle également si l'événement est synchronisé avec d'autres serveurs. La distribution est héritée par les attributs. Le cadre le plus restrictif gagne. Les options de distribution sont les suivantes : ○ Votre organisation uniquement : permet uniquement aux membres de votre organisation de voir cet événement. L'événement peut être transféré vers une autre instance par l'un des membres de votre organisation, où seule votre organisation a accès pour l'afficher. Les événements avec ce paramètre ne sont pas synchronisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Cette communauté uniquement : permet aux utilisateurs qui font partie de votre MISP communauté d'afficher l'événement, y compris votre propre organisation, les organisations sur ce MISP serveur et les organisations qui exécutent MISP des serveurs qui se synchronisent avec ce serveur. Toutes les autres organisations connectées à des serveurs liés ne peuvent pas voir l'événement. ○ Communautés connectées : permet aux utilisateurs qui font partie de votre MISP communauté d'afficher l'événement, y compris toutes les organisations sur ce serveur, toutes les organisations sur MISP les MISP serveurs qui se synchronisent avec ce serveur et les organisations d'hébergement des serveurs qui se connectent à n'importe quel serveur situé à deux sauts de distance. Toute autre organisation connectée aux serveurs liés situés à deux sauts de ce serveur ne peut pas voir l'événement. ○ Toutes les communautés : partage l'événement avec toutes les MISP communautés.
Analyse	Étape actuelle de l'analyse de l'événement avec les options possibles suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ		Description
		○ Initial : l'analyse ne fait que commencer ○ En cours : l'analyse est en cours ○ Terminé : l'analyse est terminée
Options avancées	Ajouter les observables associés SIR en tant qu'attributs à l'événement MISP	Option permettant d'ajouter des observables disponibles dans un incident de sécurité à un MISP événement en tant qu'attributs. Cette option active **l'option Définir le marqueur IDS d'attribut lorsque le résultat observable est malveillant** .
	Définir le marqueur IDS d'attribut lorsque le résultat observable est malveillant	Observable marqué comme malveillant dans SIR. L'attribut correspondant dans MISP est également marqué comme vrai.
	Filtrer les éléments observables en fonction des balises de sécurité	Option permettant de filtrer les observables en fonction des balises de sécurité sélectionnées. Cette option permet de distinguer et de gérer les événements MISP dans Threat Intelligence. **Balises de sécurité** : ajoutez des balises pour filtrer les observables. Par exemple, si vous ajoutez une balise appelée « Block from sharing » ou « TLP : White », si l'un des observables a l'une de ces balises associée, ces observables ne seront pas ajoutés en tant qu'attribut à l'événement MISP lors de la création de l'événement MISP.
	Synchroniser les techniques d'incident de sécurité MITRE ATT&CK en tant que galaxies locales à l'événement MISP	Option permettant de synchroniser les techniques d'incident ServiceNow AI Platform SIRMITRE-ATT&CK™ de sécurité en tant que galaxies locales dans l'événement MISP .
	Synchroniser les techniques d'incident de sécurité ATT&CK MITRE en tant que galaxies globales à l'événement MISP	Option permettant de synchroniser les techniques d'incident ServiceNow AI Platform SIRMITRE-ATT&CK™ de

Traduction automatique

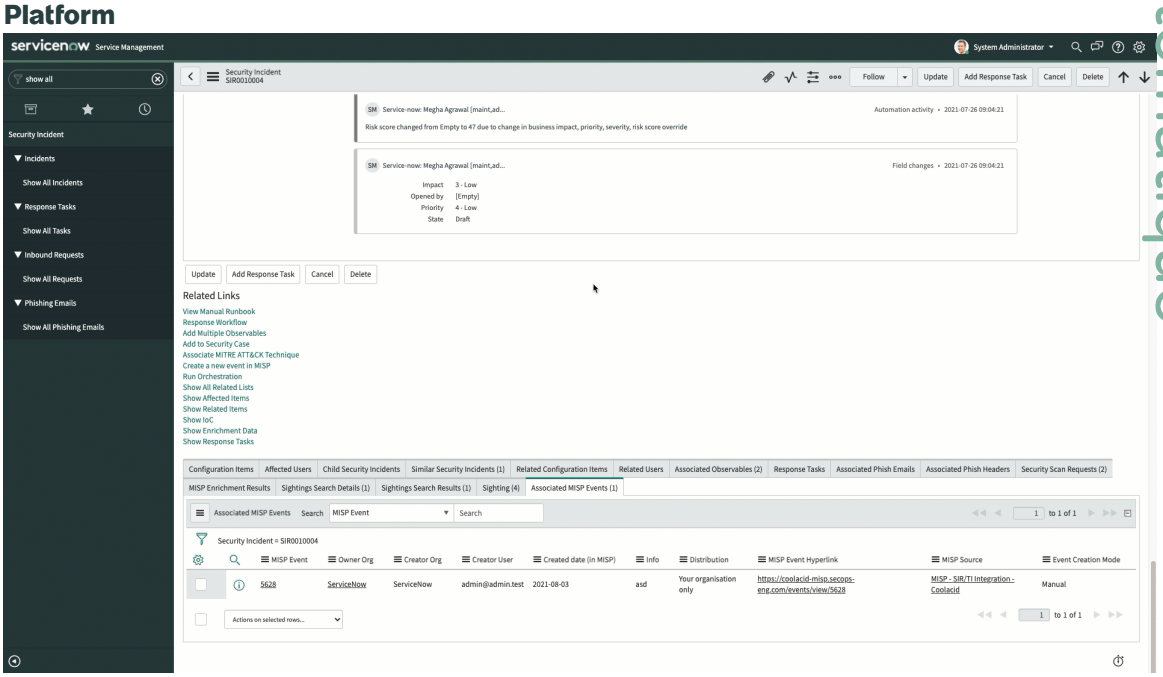
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ		Description
		sécurité en tant que galaxies globales dans l'événement MISP .
	Ajouter des balises à l'événement MISP	Option qui vous permet d'ajouter des balises MISP aux événements créés à partir de ServiceNow. Cette option affiche les options suivantes : ○ **Local (balises) :**Les balises sélectionnées seront ajoutées en tant que balises locales à l'événement MISP. ○ **Global (balises) :**Les balises sélectionnées seront ajoutées en tant que balises globales à l'événement MISP.

5. Cliquez sur **Créer un nouvel événement MISP**.

L'exemple suivant montre qu'en créant un événement dans MISP, vous pouvez afficher les résultats de l'incident de sécurité. Vous pouvez également afficher les notes de travail, l'événement dans l'instance ServiceNow AI Platform et l'événement sur le MISP serveur, comme illustré dans l'exemple suivant.

Créer manuellement un événement dans MISP à partir de ServiceNow AI Platform



Vous pouvez afficher les résultats de la manière suivante :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Un message de réussite apparaît en haut de la page de l'incident de sécurité. Vous pouvez afficher les détails de l'événement dans l'instance ServiceNow AI Platform ainsi que tels qu'ils apparaissent sur le MISP serveur.
- Dans les notes de travail, vous pouvez afficher le message de réussite avec plus de détails. Vous pouvez également afficher les détails de l'événement dans l'instance ServiceNow AI Platform ainsi que tels qu'ils apparaissent sur le MISP serveur.
- Dans la liste connexe des événements MISP associés , vous pouvez afficher l'événement par rapport à l'incident de sécurité et aux MISP ressources.

Ajouter des attributs à un MISP événement

Ajoutez des attributs à un événement, tels que le type, la catégorie et d'autres informations contextuelles sur l'événement.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Vérifiez que l'événement pour lequel vous ajoutez ou mettez à jour l'attribut appartient à la même organisation que l'utilisateur MISP .
- Rôle requis : sn_sec_misp.write

Procédure

1. Accédez à la **Tous** > **MISP** > **Événements MISP associés**.
   Vous pouvez également accéder à la liste connexe Événement MISP associé dans n'importe quel incident de sécurité.
2. Cliquez sur l'événement MISP pour lequel vous souhaitez ajouter un attribut.
3. Cliquez sur **Ajouter un attribut à l'événement MISP**.
4. Dans la boîte de dialogue Ajouter un attribut à l'événement, renseignez les détails.

Boîte de dialogue Ajouter un attribut à l'événement

Champ	Description
Valeur	Valeur réelle de l'attribut. Entrez des données sur la valeur en fonction de ce qui est valide pour le type d'attribut choisi. Par exemple, pour un attribut de type ip-src (adresse IP source), 11.11.11.11 est une valeur valide. **Remarque :** Vous ne pouvez sélectionner que des attributs ou des observables qui partagent un contexte avec l'événement. Les observables ne peuvent pas déjà avoir un attribut dans MISP.
Catégorie	Catégorie de l'attribut. La catégorie décrit l'aspect du programme malveillant pour cet attribut. Un exemple serait les mécanismes de persistance du logiciel malveillant ou l'activité du réseau.
Type	Type qui explique la catégorie. Par exemple, si un attaquant utilise une adresse IP pour une attaque,

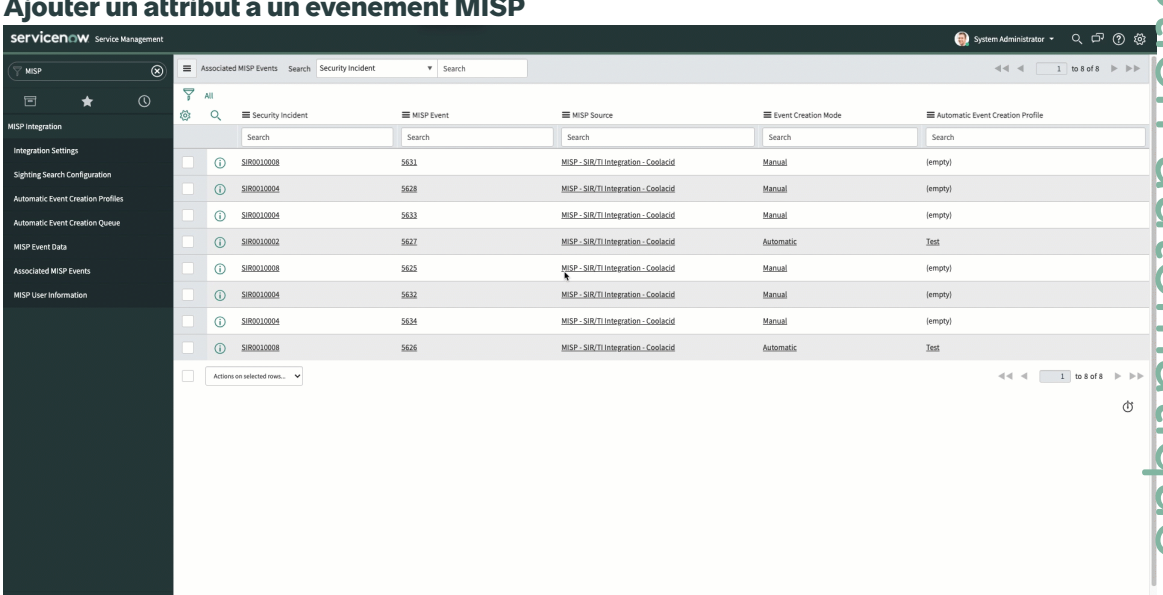
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	une adresse e-mail source ou un fichier envoyé via une pièce jointe peuvent tous décrire la livraison de la charge utile d'un logiciel malveillant. Ces types d'attributs ont la catégorie de livraison de charge utile.
Distribution	Utilisateurs qui peuvent afficher cet attribut. La distribution est héritée par attributs. Le cadre le plus restrictif gagne.
Utiliser l'attribut comme signature IDS	Observable marqué comme malveillant dans SIR. L'attribut correspondant dans MISP est également marqué comme vrai.
Commentaires	Commentaires que vous ajoutez pour les attributs.

L'exemple suivant montre qu'en naviguant à partir de la liste Événements MISP associés, vous pouvez afficher l'enregistrement d'événement 5627 et ajouter des attributs à l'événement. Les attributs incluent la valeur (testdomain.com), la catégorie en tant qu'analyse externe, le type en tant que domaine. Vous pouvez également activer IDS. Le message de réussite sur l'enregistrement d'événement montre que l'attribut est ajouté à l'événement, comme illustré dans l'exemple suivant.

Ajouter un attribut à un événement MISP



5. Cliquez sur **Ajouter un attribut à l'événement MISP**.

Résultats

Vous pouvez afficher l'attribut ajouté dans la section Attributs.

Ajouter des balises à un MISP événement

Ajoutez des balises ServiceNow AI Platform MISP pour classer des événements ou des attributs. Vous pouvez utiliser le balisage globalement pour activer votre classification ou utiliser des balises localement lorsque vous ne souhaitez MISP pas que les événements soient modifiés pendant votre classification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations pour l'utilisation des fonctionnalités bidirectionnelles MISP .
- Vérifiez que l'événement que vous modifiez appartient à la même organisation que l'utilisateur MISP .
- Notez que les balises et les galaxies disponibles sont basées sur la MISP source et ses autorisations de distribution.
- Rôle requis : sn_sec_misp.write

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité qui contient l'événement pour lequel vous souhaitez ajouter des balises.
3. Cliquez sur **Afficher toutes les listes connexes** et la liste connexe Résultats de l'enrichissement MISP.
4. Cliquez sur l'ID d'événement dans la liste des résultats d'enrichissement.
   Vous pouvez également naviguer à partir de **MISP** > **Événements MISP associés** module.
5. Passez en revue l'enregistrement de l'événement MISP.

Vue de formulaire d'événement MISP

Champ	Description
ID d'événement	ID d'événement attribué lors de MISP la première création ou importation de l'événement dans le MISP serveur.
UUID	ID qui identifie de manière unique les événements et les attributs.
Org. du créateur	Organisation qui a créé l'événement sur l'instance MISP .
Org. du propriétaire	Organisation propriétaire de l'événement sur l'instance MISP . Ce champ n'est visible que par les administrateurs.
Créateur	Utilisateur qui a créé l'événement dans MISP.
Dernier changement	Date de la dernière modification de l'événement.
Source MISP	MISP Source où l'événement est créé.
Date de création (dans MISP)	Date de création ou de première importation de l'événement sur le MISP serveur.
Niveau de menace	Niveau de risque de l'événement. Les incidents peuvent être classés en trois catégories de menaces différentes (faible, moyenne, élevée). Ce champ peut être laissé comme non défini. Les options sont les suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Faible : logiciel malveillant de masse général ○ Moyen : menaces persistantes avancées (APT) ○ Élevée : APT sophistiquées et attaques sur 0 jour
Analyse	Étape actuelle de l'analyse de l'événement avec les options possibles suivantes : ○ Initial : l'analyse ne fait que commencer ○ En cours : l'analyse est en cours ○ Terminé : l'analyse est terminée
Distribution	Distribution de l'attribut individuel. Un attribut peut avoir un niveau de distribution différent de celui de l'événement.
Publié	État indiquant si l'événement a été publié ou non. La publication permet d'utiliser les attributs de l'événement pour toutes les exportations éligibles et notifie les utilisateurs qui se sont abonnés aux alertes d'événement.
Lien hypertexte d'événement MISP	Lien vers l'événement MISP qui est stocké sur le MISP serveur.
Info	Brève description de l'événement.
Balises (locales)	Balises disponibles sur l'instance de l'organisation hôte pour activer le balisage à des fins de MISP synchronisation et de filtrage des exportations. MISP Les événements ne sont pas modifiés lorsque vous utilisez des balises locales. Les balises locales sont toujours supprimées avant d'être synchronisées avec d'autres MISP instances et de partager des communautés.
Balises (globales)	Balises disponibles globalement pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous ajoutez des balises globales à MISP des instances, vous pouvez modifier les événements.
Galaxies (locales)	Galaxies disponibles sur l'instance de l'organisation hôte pour le filtrage de synchronisation et d'exportation. MISP Les événements ne sont pas modifiés lorsque vous utilisez des galaxies MISP locales. Ces galaxies locales sont toujours dépouillées avant d'être synchronisées avec d'autres MISP instances et communautés de partage.
Galaxies (globales)	Galaxies disponibles dans le monde entier pour être partagées et synchronisées avec d'autres instances et communautés de MISP partage. Lorsque vous

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ajoutez des galaxies globales, MISP vous pouvez modifier les événements.

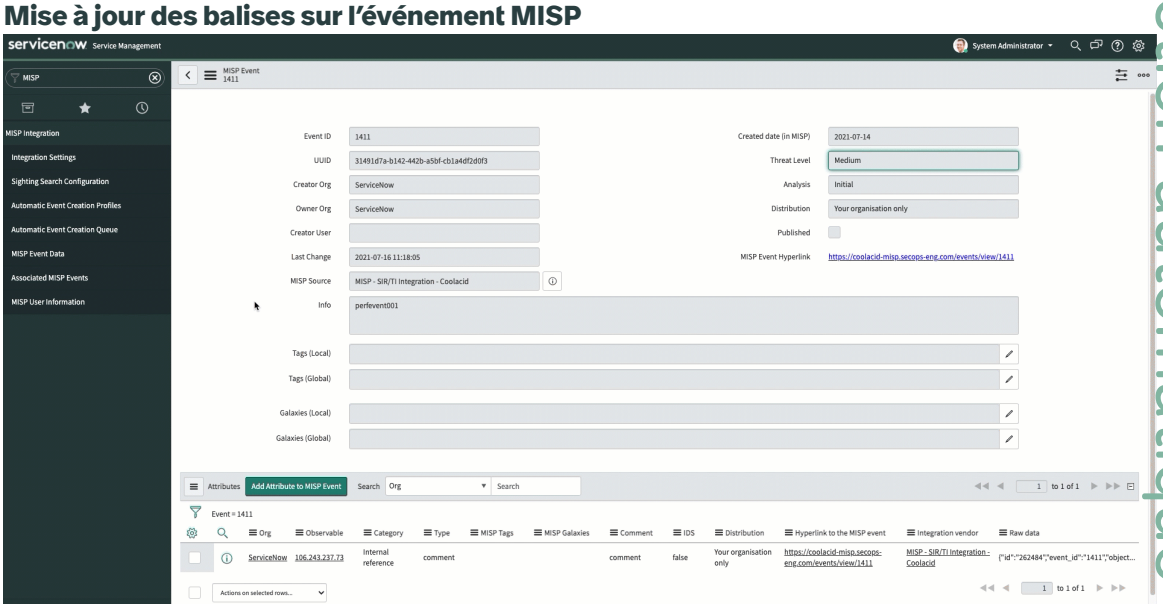
6. Pour modifier une balise locale ou globale, cliquez sur l'icône icône Modifier dans l'une des options suivantes :

   - **Balises (locales)**
   - **Balises (globales)**

7. Dans la boîte de dialogue Balises d'événements MISP, entrez le nom de la balise pour rechercher et ajouter les balises.
8. Cliquez sur **Mettre à jour les balises sur l'événement MISP**.

   L'exemple suivant montre qu'en cliquant sur l'icône de modification des balises locales, vous pouvez rechercher et ajouter les balises C3, Adware, C2 et Botnet 3101, et mettre à jour le serveur MISP avec les balises. Le message de confirmation indique que toutes les balises sont mises à jour dans MISP.

Mise à jour des balises sur l'événement MISP



9. Cliquez sur **Recharger le formulaire** dans le message de réussite pour afficher les changements dans l'enregistrement.

Résultats

Les balises sont mises à jour avec succès dans le MISP serveur.

Mettre à jour les galaxies en fonction d'un événement ou d'un MISP attribut

Ajoutez ou supprimez des galaxies ServiceNow AI Platform MISP afin de pouvoir classer ces objets en tant que cluster dans l'instance MISP et les attacher à des événements ou à MISP des attributs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Examiner le MISP Rôle d'utilisateur et autorisations requis pour utiliser les fonctionnalités bidirectionnelles MISP .
- Pour ajouter des galaxies locales, l'utilisateur qui a configuré l'intégration doit appartenir à l'organisation hôte du serveur correspondant MISP .
- Les balises et les galaxies disponibles sont basées sur la MISP source et ses autorisations de distribution.
- Rôle requis : sn_sec_misp.write

Procédure

1. Cliquez sur l'icône dans l'une des options suivantes.

   - **Galaxies (locales)**
   - **Galaxies (globales)**

2. Dans la boîte de dialogue Galaxies d'événements MISP, tapez et recherchez pour ajouter les balises.
3. Cliquez sur **Mettre à jour les galaxies sur l'événement MISP**.

   L'exemple suivant montre comment cliquer sur l'icône de modification des galaxies locales, sélectionner l'espace de noms obsolète, sélectionner la galaxie Enterprise Attack - Attack Pattern et ajouter des informations de cluster. Une fois les informations sur la galaxie mises à jour, vous pouvez afficher le message de réussite.

   Mettre à jour les informations sur les galaxies vers l'événement MISP

   Les galaxies sont mises à jour avec succès dans le MISP serveur.

4. Cliquez sur **Recharger le formulaire** dans le message de réussite pour afficher les changements dans l'enregistrement.

Déployer les MITRE-ATT&CK informations à l'aide des résultats de l'enrichissement MISP

Déployer manuellement les résultats de l'enrichissement MISP si vous n'avez pas activé le déploiement automatique des MISP informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

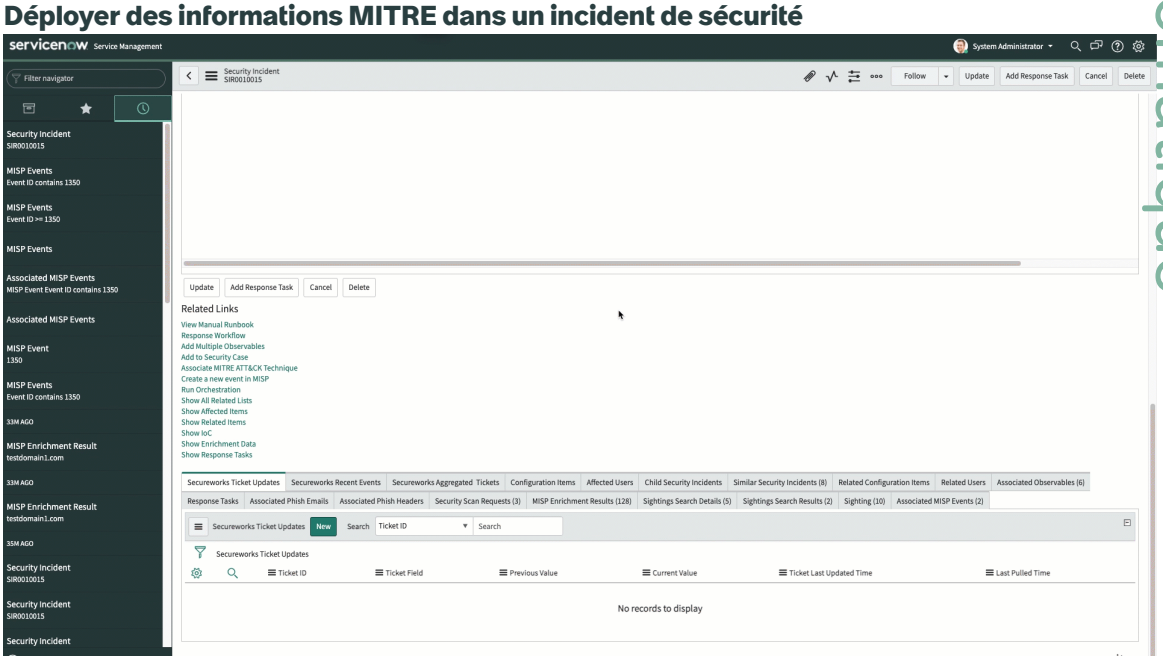
Utilisez les règles d'extraction automatique du système de base pour importer les MITRE-ATT&CK informations à partir de l'intégration MISP . Il MISP integration for Security Operations introduit deux règles d'extraction de la technique du système MITRE-ATT&CK de base pour MISP les MISP galaxies et MISP les balises. Pour plus d'informations sur les règles d'extraction automatique dans , consultez MITRE-ATT&CKRègles de technique d'extraction automatique pour l'importation d'informations MITRE-ATT&CK.

Si vous avez activé Déploiement automatique de MITRE-ATT&CK informations à l'aide de MISP Résultats de l'enrichissement En cas d'incident de sécurité, les informations sont automatiquement déployées. Si vous n'avez pas activé le déploiement automatique, vous pouvez effectuer cette tâche manuellement.

Procédure

1. Accédez à la **Tous** > **Incidents de sécurité** > **Afficher les incidents**.
2. Sélectionnez l'incident de sécurité que vous souhaitez enrichir avec les MITRE-ATT&CK informations.
3. Cliquez sur **Afficher toutes les listes connexes** et sur l'onglet **Résultats de l'enrichissement MISP** .
4. Sélectionnez l'observable et, dans le menu Actions, cliquez sur **Déployer les informations MITRE ATT&CK sur SI.**
   Vous pouvez sélectionner plusieurs observables, puis déployer les informations.
5. Pour confirmer les modifications, cliquez sur **Recharger**.
   L'exemple suivant montre comment sélectionner un observable et déployer les résultats de l'enrichissement MISP sur l'incident de sécurité.

Déployer des informations MITRE dans un incident de sécurité



Résultats

Vous pouvez afficher la MITRE-ATT&CK carte pour confirmer que les résultats de l'enrichissement MISP ont été déployés sur l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration de Metadefender OPSWAT

OPSWAT Metadefender permet de télécharger les données sur les menaces, détectées par le scanner tiers Metadefender, dans l'application pour le suivi, la hiérarchisation et la Renseignements sur les menaces résolution.

Explorer	Configuration
• Vue d'ensemble de l'intégration OPSWAT Metadefender • Intégrations de Renseignements sur les menaces	Activer et configurer l'intégration OPSWAT Metadefender
Utiliser	**Développer**
Effectuer des recherches sur les observables	• ServiceNow Opérations de sécurité Directives pour le développement des intégrations • Conseils pour l'écriture d'intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide	
• Dépannage de l'intégration • Poser des questions ou y répondre dans la communauté Security Operations • Rechercher des articles sur une erreur connue dans le portail d'erreurs connues • Contact Service client et assistance	

Vue d'ensemble de l'intégration OPSWAT Metadefender

OPSWAT Metadefender est une solution de sécurité qui donne accès à plusieurs machines anti-programme malveillant et s'intègre facilement à Opérations de sécurité.

Avant de pouvoir utiliser l'intégration OPSWAT Metadefender , vous devez activer le module d'extension et configurer l'intégration. Si nécessaire, vous pouvez également mettre à jour votre certification SSL X509.

Recherche de menace : flux OPSWAT Metadefender

Le flux Recherche de menace - OPSWAT Metadefender effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par OPSWAT Metadefender, ils sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés.

Ce flux est déclenché Security Operations Integration - Aptitude de recherche de menace lorsque vous effectuez une recherche de menace sur un ou plusieurs observables et que l'implémentation

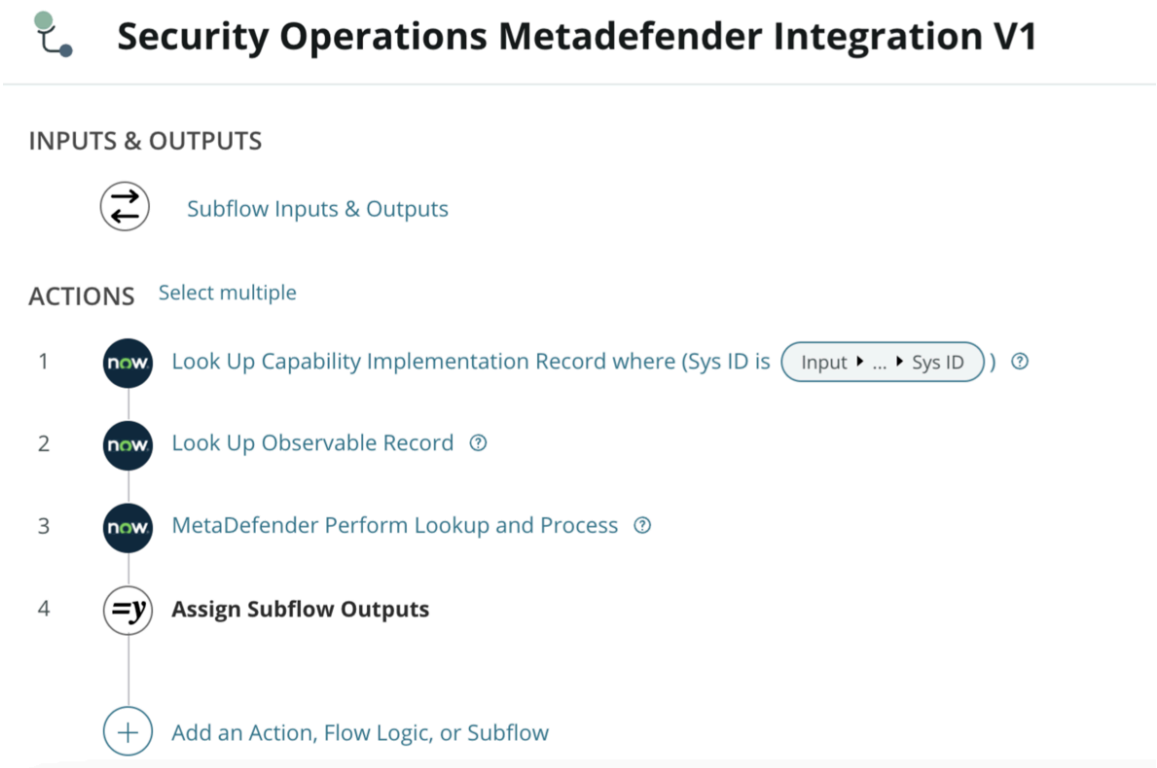
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

OPSWAT Metadefender est sélectionnée. Pour plus d'informations, consultez Effectuer des recherches sur les observables.

Rôle requis : sn_si.admin

Recherche de menace : flux OPSWAT Metadefender



Pour en savoir plus sur les activités utilisées par ce flux, reportez-vous à la rubrique Flux d'intégration et activités d'orchestration courants de Security Operations.

Activer et configurer l'intégration OPSWAT Metadefender

Avant de pouvoir utiliser l'intégration OPSWAT Metadefender , vous devez la télécharger à partir du ServiceNow Store.

Avant de commencer

Rôle requis : admin

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois l'intégration terminée, accédez au portail OPSWAT et obtenez la clé API Metadefender Cloud
3. Dans votre instance, accédez à **Security Operations** > **Intégrations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte OPSWAT Metadefender, cliquez sur **Configurer**.
5. Saisissez (ou collez) la **clé API** que vous avez acquise à partir du portail OPSWAT.
6. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Une fois configuré, OPSWAT Metadefender peut être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Mettre à jour votre certificat X.509

Si vous avez besoin d'une connexion SSL pour l'intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou ait expiré. Cette tâche est facultative.

Avant de commencer

Rôle requis : admin

Procédure

1. Obtenez le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.
   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
      Par exemple : `https://<3rdparty>/`.
   b. Cliquez sur l'icône de verrou dans la ligne d'adresse.
   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .
   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .
   e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.
   f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
      Il doit commencer par `----- COMMENCER LE CERTIFICAT -----` et se terminer par `----- CERTIFICAT DE FIN -----`.
2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Ajoutez le certificat à l'enregistrement du fournisseur d'identité.
   a. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
   b. Sélectionnez le fournisseur d'identité par défaut actif pour lequel vous avez créé le nouveau certificat.
   c. Faites défiler jusqu'à la liste connexe des **certificats X.509** , puis cliquez sur **Modifier**.
   d. Déplacez le certificat nouvellement créé vers la colonne **Sélectionnée** .
6. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les autres champs de l’enregistrement sont générés automatiquement.

Remarque : Si vous avez un certificat qui a expiré, vous devez le supprimer. Pour plus d’informations sur la suppression du certificat expiré, consultez KB0691439 Remplacement d’un certificat SAML arrivant à expiration .

Intégration de VirusTotal

L’intégration VirusTotal vous permet de demander l’analyse des adresses IP, des fichiers, des hachages de fichiers et des URL suspects afin d’aider à déterminer s’ils sont malveillants.

Explorer	Configurer
Intégrations de Renseignements sur les menaces	• Configuration de l’intégration VirusTotal • Activer et configurer l’intégration de VirusTotal
Utiliser	**Développer**
• Effectuer des recherches sur les observables • Recherche de menace - Workflow VirusTotal	• ServiceNow Opérations de sécurité Directives pour le développement des intégrations • Conseils pour l’écriture d’intégrations • Formation pour les développeurs • Documentation pour les développeurs • Rechercher les composants installés avec une application
Dépannage et demande d'aide	
• Dépannage de l’intégration • Poser des questions ou y répondre dans la communauté Security Operations • Rechercher des articles sur une erreur connue dans le portail d’erreurs connues • Contact Service client et assistance	

Configuration de l’intégration VirusTotal

VirusTotal est un service gratuit qui analyse les fichiers et les URL suspects et facilite la détection rapide des virus, vers, chevaux de Troie et toutes sortes de logiciels malveillants. Il s’intègre facilement avec Opérations de sécurité.

Avant de pouvoir utiliser l’intégration VirusTotal , vous devez activer le module d’extension et ajouter la clé API appropriée. Si nécessaire, vous pouvez également mettre à jour votre certification SSL X509.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si la source de recherche est utilisée et qu'un VirusTotal programme malveillant est rencontré, un observable est créé. Pour les recherches d'adresses IP, une liste supplémentaire d'URL qui partagent l'adresse IP est créée et des observables sont créés pour chacune des URL.

Remarque :

- Le Renseignements sur les menaces module d'extension est requis pour implémenter VirusTotal l'intégration.
- L'intégration VirusTotal a été mise à niveau vers la version 3 des API.

Activer et configurer l'intégration de VirusTotal

Avant de pouvoir utiliser l'intégration de VirusTotal, vous devez la télécharger à partir du ServiceNow Store.

Avant de commencer

Rôle requis : admin

Renseignements sur les menaces doit être installé et activé avant de pouvoir utiliser VirusTotal. L'intégration VirusTotal a été mise à niveau vers la version 3 des API.

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à VirusTotal et obtenez la clé API sous votre profil VirusTotal.
3. Dans votre instance, accédez à **Security Operations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
4. Dans la carte VirusTotal, cliquez sur **Configurer**.

VirusTotal Configuration

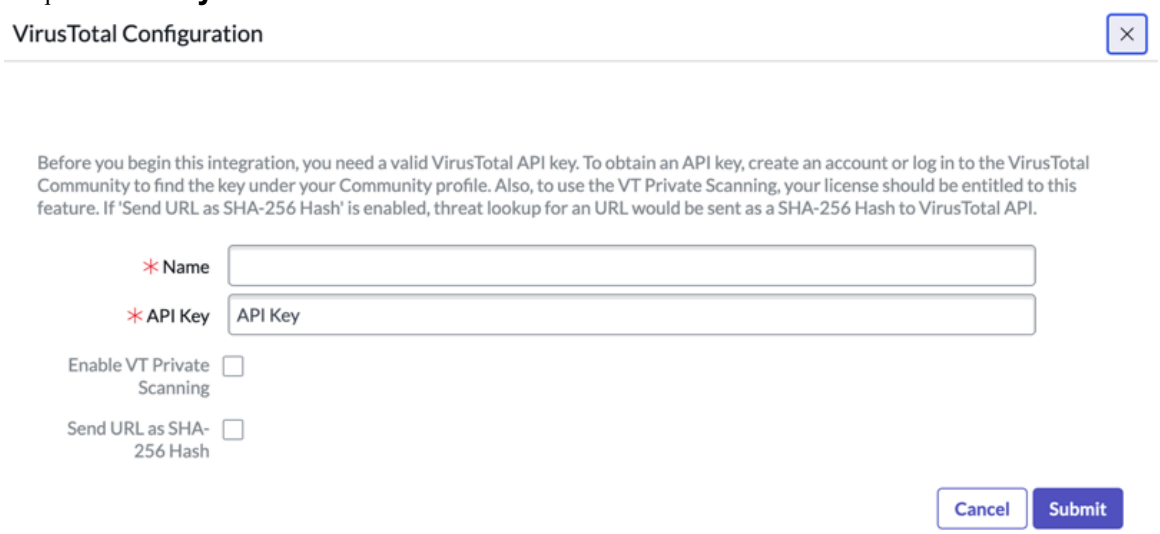
Champ	Description
Nom	Nom de l'intégration. Par exemple, VirusTotal.
Clé API	Saisissez (ou collez) la **clé API** que vous avez acquise sur le site VirusTotal.
Activer l'analyse privée VT	Cochez cette case pour analyser les fichiers avec VirusTotal en préservant la confidentialité. Les fichiers chargés via cette offre ne seront partagés avec personne en dehors de votre organisation et ne resteront dans VirusTotal que pendant une brève période. Les analyses résultantes seront également éphémères et ne seront visibles que par votre groupe VirusTotal. **Important :** Pour utiliser VT Private Scanning, votre licence VirusTotal doit autoriser cette fonctionnalité.
Envoyer l'URL comme hachage SHA-256	Cochez cette case pour envoyer les URL en tant que hachages pour la recherche de menaces et protéger la confidentialité des utilisateurs sur l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si elle est désactivée, l'URL est envoyée sous forme de codage Base64 à l'API VirusTotal.

5. Cliquez sur **Envoyer**.



Résultats

Une fois configuré, VirusTotal peut être sélectionné pour effectuer des recherches sur les observables dans Renseignements sur les menaces et sur les observables dans les incidents de sécurité.

Information associée

Effectuer des recherches sur les observables

Recherche de menace - Workflow VirusTotal

Le workflow Recherche de menace effectue VirusTotal une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par VirusTotal, ils sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés.

Avant de commencer

Rôle requis : admin

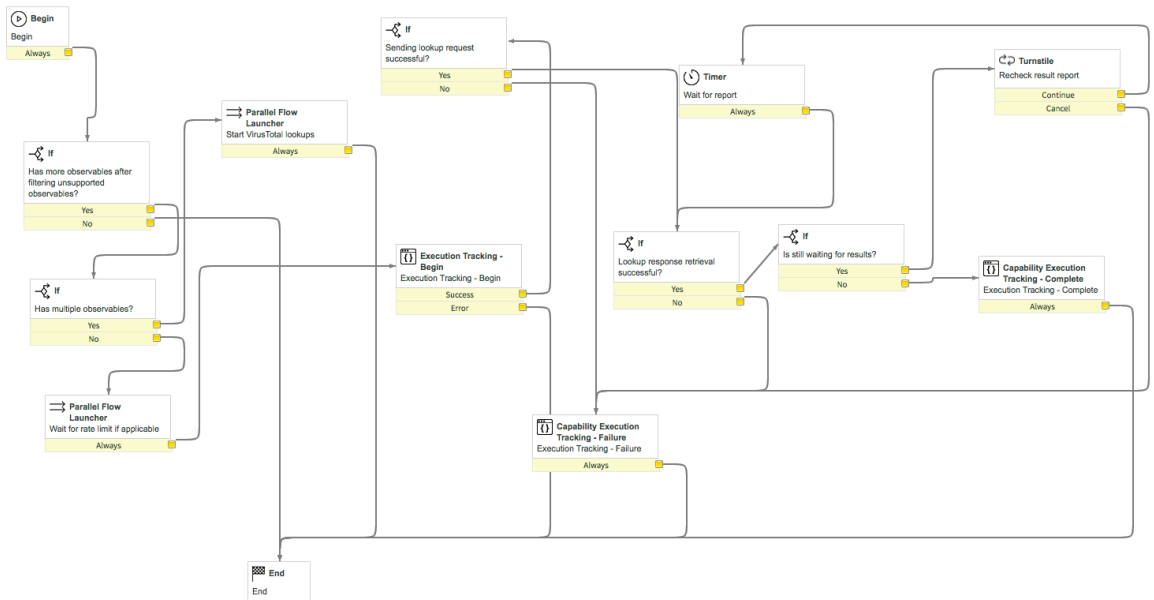
Pourquoi et quand exécuter cette tâche

Ce workflow est déclenché lorsque Security Operations Integration - Aptitude de recherche de menace vous effectuez une recherche de menace sur un ou plusieurs observables et que l'implémentation VirusTotal est sélectionnée. Pour plus d'informations, consultez Effectuer des recherches sur les observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche de menace - Workflow VirusTotal



Pour plus d'informations sur les activités utilisées par ce workflow, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Intégration de l'API WhoisXML

L'intégration de l'API WhoisXML vous permet de soumettre des recherches Whois sur les noms de domaine et les URL afin d'obtenir un contexte sur les observables d'URL et de mieux déterminer les menaces.

Explorer

Intégrations de Renseignements sur les menaces

Configurer

- Configuration de l'intégration de l'API WhoisXML
- Activer et configurer l'intégration Security Operations Whois

---

Utiliser

Renseignements sur les menaces - Exécuter le workflow de recherche IoC

Développer

- ServiceNow Opérations de sécurité Directives pour le développement des intégrations
- Conseils pour l'écriture d'intégrations
- Formation pour les développeurs
- Documentation pour les développeurs
- Rechercher les composants installés avec une application

Dépannage et demande d'aide

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(suite)

- Dépannage de l'intégration
- Poser des questions ou y répondre dans la communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Configuration de l'intégration de l'API WhoisXML

Avant de pouvoir utiliser l'intégration Whois, vous devez activer le module d'extension et ajouter les informations d'identification. Si nécessaire, vous pouvez également mettre à jour votre certification SSL X509.

Les modules d'extension Renseignements sur les menaces et WhoisXML API Integration sont requis pour implémenter l'intégration de l'API WhoisXML.

Activer et configurer l'intégration Security Operations Whois

La fonctionnalité Configuration de l'intégration vous permet d'activer et de configurer rapidement des intégrations de sécurité tierces, y compris l'intégration Whois des opérations de sécurité. Avant de pouvoir utiliser l'intégration Security Operations Whois, vous devez la télécharger à partir du , et vous devez disposer d'un compte valide à partir de l'API ServiceNow Store WhoisXML.

Avant de commencer

Renseignements sur les menaces doit être installé et activé avant de pouvoir utiliser l'intégration Security Operations Whois.

Rôle requis : admin

Procédure

1. Télécharger l'intégration à partir de ServiceNow Store.
2. Une fois l'installation terminée, accédez à **Security Operations** > **Configuration de l'intégration**. Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes.
3. Dans la carte API Whois, cliquez sur **Configurer**.
4. Entrez le nom d'utilisateur et le mot de passe de votre compte API WhoisXML.
5. Cliquez sur **Envoyer**.

Mettre à jour votre certificat X.509

Si vous avez besoin d'une connexion SSL pour l'intégration, il peut arriver que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou ait expiré. Cette tâche est facultative.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Obtenez le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

   b. Cliquez sur l'icône de verrou dans la ligne d'adresse.

   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

   e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

   f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
   Il doit commencer par `----- COMMENCER LE CERTIFICAT -----` et se terminer par `----- CERTIFICAT DE FIN -----`.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Ajoutez le certificat à l'enregistrement du fournisseur d'identité.
   a. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
   b. Sélectionnez le fournisseur d'identité par défaut actif pour lequel vous avez créé le nouveau certificat.
   c. Faites défiler jusqu'à la liste connexe des **certificats X.509** , puis cliquez sur **Modifier**.
   d. Déplacez le certificat nouvellement créé vers la colonne **Sélectionnée** .
6. Cliquez sur **Enregistrer**.
   Les autres champs de l'enregistrement sont générés automatiquement.

Remarque : Si vous avez un certificat qui a expiré, vous devez le supprimer. Pour plus d'informations sur la suppression du certificat expiré, consultez KB0691439 Remplacement d'un certificat SAML arrivant à expiration .

Enrichir le workflow WhoIs des observables

Le workflow **Enrichir l'observable WhoIs** effectue un enrichissement sur les observables sélectionnés. Si les observables sont d'un type reconnu par , WhoisXML API Integration les observables sont enrichis.

Avant de commencer

Rôle requis : admin

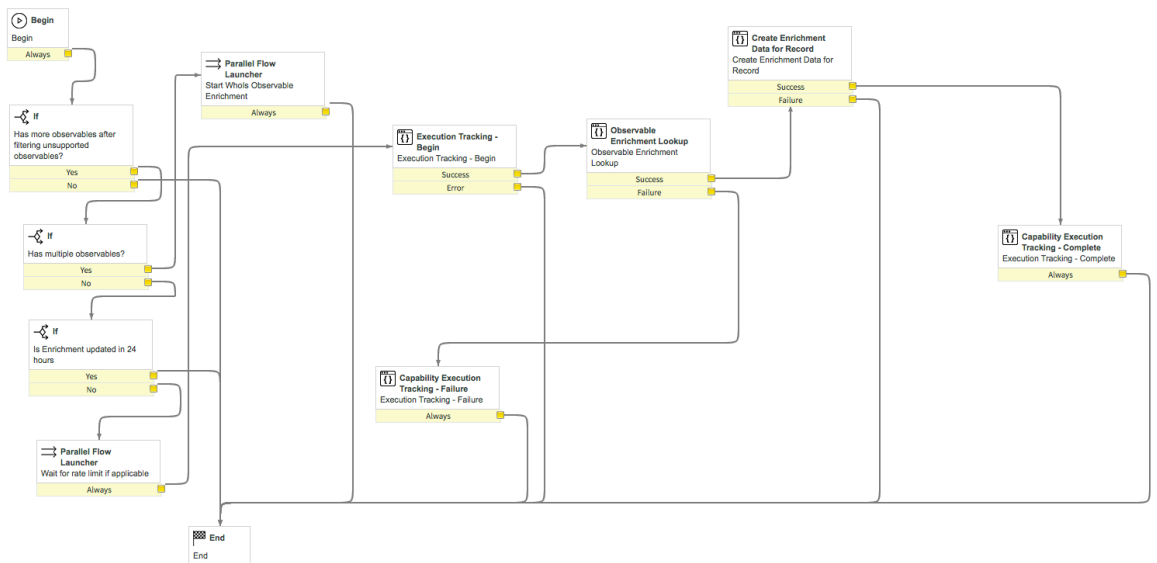
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Ce workflow est déclenché lorsque Security Operations Integration : enrichir l'aptitude des observables vous effectuez un enrichissement sur un ou plusieurs observables, et que l'implémentation WhoIs est sélectionnée.

Enrichir le workflow WhoIs des observables



Les activités spécifiques à cette intégration sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Activité de recherche d'enrichissement d'observable

L'activité de workflow **de recherche d'enrichissement d'observables** lance le processus d'enrichissement des observables.

L'activité Recherche d'enrichissement d'observables peut être utilisée avec n'importe quel workflow d'observables pour commencer l'enrichissement.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	La recherche a réussi.
Échec	Une erreur s'est produite lors de la tentative de recherche. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
implementation_id	Identificateur système de l'implémentation utilisée pour effectuer la recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
domain_id	L'identificateur du domaine dans lequel la recherche est effectuée.
observable_ids	Un ou plusieurs observables sur lesquels effectuer l'action souhaitée. Les ID sont utilisés comme entrée de workflow.
capabilityExcutionId	Identificateur système de l'option qui a lancé le workflow d'implémentation. Uniquement requis pour les workflows d'implémentation de l'option d'intégration tels que Splunk, Elasticsearch.
task_sys_id	Identificateur système pour toute tâche associée au workflow.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
response_data	Données brutes retournées par le point de terminaison d'API de l'implémentation pour le domaine donné.
mapping_id	Identificateur du mappage d'enrichissement. Par exemple, l'intégration WhoIs renvoie les données dans deux formats différents, IP et URL, avec un identifiant de mappage pour chacun.

Threat Intelligence Orchestration

Orchestration des renseignements sur les menaces Les activités permettent aux utilisateurs de déterminer si une menace a déjà été observée dans d'autres incidents de sécurité ou sur d'autres systèmes à l'aide de l'orchestration de workflow.

Pour plus d'informations sur la modification Orchestration de la réponse aux incidents de sécurité des workflows ou la création de workflows personnalisés, voir Introduction aux workflows et Éditeur de workflow Éditeur de workflow .

Configurer Threat Intelligence Orchestration

Avant d'utiliser Orchestration des renseignements sur les menaces, effectuez les étapes de configuration de diverses parties du système, notamment le remplissage de la CMDB, la configuration du serveur MID et la configuration des informations d'identification.

Avant de commencer

Rôle requis : admin

Pour l'utiliser Orchestration des renseignements sur les menaces , vous avez besoin d'une CMDB complète avec des noms de domaines. Pour plus d'informations, consultez Découverte .

Pourquoi et quand exécuter cette tâche

Procédure

1. Activez le module d'extension Renseignements sur les menaces .
2. Configurer le Serveur MID

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Configurer les informations d'identification de service de Serveur MID
   Vous êtes maintenant prêt à utiliser Orchestration des renseignements sur les menaces les activités dans un workflow.

Activités et workflows Threat Intelligence Orchestration

Le système de base inclut des workflows et des activités de workflow que vous pouvez utiliser pour automatiser les actions sur votre instance.

Renseignements sur les menaces - Exécuter le workflow de recherche IoC

Le workflow Renseignements sur les **menaces : exécuter la recherche d'IoC vérifie s'il** existe un observable non expiré et, le cas échéant, la recherche est définie sur **Terminée** et mise à jour avec les données de l'observable.

Avant de commencer
Rôle requis : sn_si.basic

Remarque : Ce workflow remplace Orchestration des renseignements sur les menaces les règles métier (**Remplir avec les tables IoC existantes**, **Mettre en file d'attente la recherche** et **Mettre à jour l'observable**) par des activités.

Si une recherche est insérée ou mise à jour et remplit les conditions, la règle métier de recherche déclenche ce workflow.

Pourquoi et quand exécuter cette tâche
Le workflow Renseignements sur les **menaces : exécuter la recherche d'IoC vérifie s'il** existe un observable non expiré et, le cas échéant, la recherche est définie sur **Terminée** et mise à jour avec les données de l'observable. Tous les indicateurs associés à l'observable sont réactivés.

Si l'observable a expiré, le workflow exécute les recherches et incrémente le **nombre de perceptions** dans l'observable existant et expiré.

S'il n'existe aucun observable corrélé, un nouvel observable avec indicateur est créé.

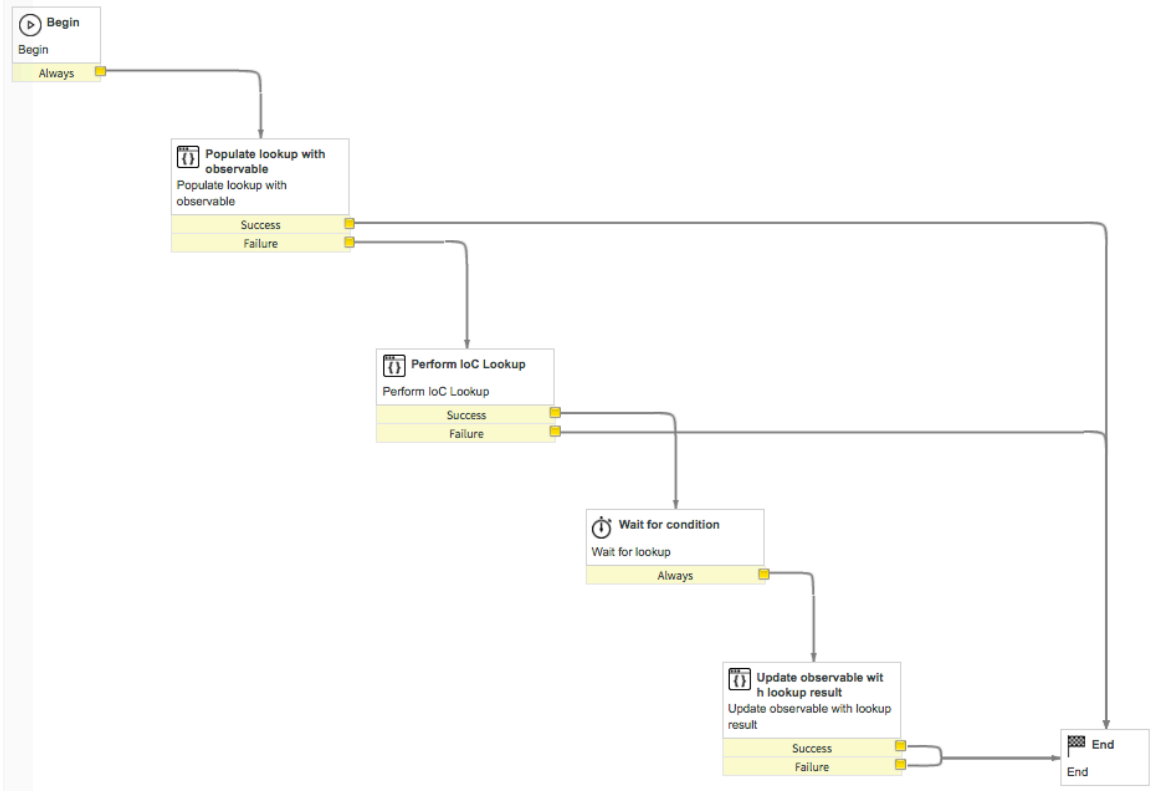
Les activités du processus de workflow comprennent :

- Remplir la recherche avec l'activité observable
- Effectuer une activité de recherche d'IoC
- Attendre la recherche (activité principale)
- Mettre à jour l'observable avec l'activité de résultat de la recherche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renseignements sur les menaces : exécuter le workflow de recherche d'IoC



Remplir la recherche avec l'activité observable

Si un observable non expiré est trouvé, l'activité de workflow **Orchestration pour la connaissance des menaces : remplir la recherche avec un observable fournit des données d'un** observable existant à une recherche. Cette activité peut accélérer le processus d'enquête et de correction.

Lorsqu'elle est déclenchée par un workflow **Remplir la recherche avec des observables** tente de trouver un observable existant pour une recherche qui correspond à la **valeur** et au **type** de la recherche fournie à l'activité en tant qu'entrée.

Si l'observable existe et n'a pas expiré, cette activité :

- Met à jour la recherche avec les informations trouvées dans l'observable
- Réactive un indicateur s'il est inactif, incrémente le **nombre de rencontres** et met à jour la date de **la dernière consultation**
- Définit **l'état** sur Terminé.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable d'entrée	Description
scanID[chaîne]	Identificateur de recherche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie	Description
Vrai	Observable valide trouvé et recherche mise à jour.
Faux	Observable introuvable valide. L'observable est manquant ou a expiré.

Effectuer une activité de recherche d'IoC

L'activité de workflow **Orchestration des renseignements sur les menaces : effectuer une recherche d'IoC** effectue une recherche donnée. Cette activité peut accélérer le processus d'enquête et de correction.

Lorsqu'elle est déclenchée par un workflow, **Effectuer une recherche IoC** prend un scanID, recherche l'enregistrement de recherche et ajoute la recherche à la file d'attente en créant une entrée de file d'attente de recherche.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
scanID[chaîne]	Identificateur de recherche

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Vrai	A déclenché la recherche.
Faux	N'a pas déclenché la recherche.

Mettre à jour l'observable avec l'activité de résultat de la recherche

L'activité de workflow **Orchestration des renseignements sur les menaces : mettre à jour l'observable avec le résultat de la recherche** met à jour l'enregistrement de l'observable. Si l'un n'existe pas, il crée un nouvel observable. Cette activité est utile pour enregistrer des informations.

Lorsqu'il est déclenché par un workflow, **mettre à jour l'observable avec le résultat** de la recherche met à jour un observable existant pour inclure le nouveau **nombre de perceptions**, ajoute une note et, s'il est inactif, réactive tous les indicateurs. Le **nombre de rencontres** et la date de **la dernière consultation** dans l'indicateur sont également mis à jour.

S'il n'existe aucun observable corrélé, le workflow crée un nouvel observable avec l'indicateur suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Exécute les recherches IoC
- Crée un nouvel observable
- Crée un indicateur pour l'observable
- Ajoute un **nombre de perceptions** à l'observable
- Ajoute un **nombre de rencontres** et la date de **la dernière consultation** à l'indicateur
- Ajoute un message indiquant à partir de quelle recherche elle a été créée

.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
scanID[chaîne]	Identificateur de recherche.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Vrai	La mise à jour ou la création d'observable est réussie.
Faux	Échec de la mise à jour ou de la création de l'observable.

Exécuter l'activité de sources de recherche d'IoC par défaut

Lorsqu'elles sont déclenchées par un workflow, Renseignements sur les menaces**l'option Exécuter les sources de recherche IoC par défaut prend en compte l'ID d'une** demande de recherche et crée plusieurs recherches en fonction des valeurs de données saisies.

Pour chaque type de données, la colonne **d'analyse include_in_bulk** de la table de type de recherche pris en charge de chaque source de recherche est évaluée. Si vrai, une recherche est ajoutée à la demande de recherche.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
scan_request_id	Rechercher l'identificateur système de la demande

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Nombre d'analyses créées	Entier

Security Case Management

Gestion des tickets de sécurité permet aux analystes de sécurité engagés dans la chasse aux menaces de recueillir des informations sur les activités suspectes dans leur environnement. Les enregistrements liés aux tickets, tels que les incidents de sécurité, les observables, les CI et les utilisateurs affectés peuvent être ajoutés aux tickets pour permettre une analyse large et spécifique.

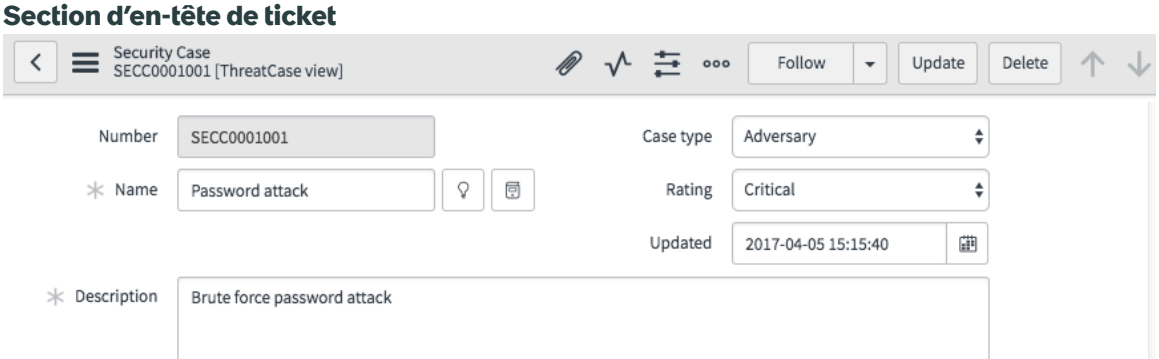
Grâce à la possibilité de parcourir facilement les enregistrements et les informations connexes, les analystes peuvent évaluer s'ils sont confrontés à une campagne ciblée, à une menace persistante avancée, etc.

Les tickets de sécurité peuvent être créés à partir de diverses sources sur votre instance, notamment Gestion des tickets de sécurité, Réponse aux incidents de sécurité et Renseignements sur les menaces. Vous pouvez également créer des tickets à partir d'éléments de configuration et d'utilisateurs affectés dans les tables Éléments de configuration [cmdb.ci] et Utilisateurs [sys.user], respectivement. Une fois les tickets créés, chacune de ces sources peut également être utilisée pour ajouter de précieuses ressources d'analyse aux tickets existants.

Chaque ticket de sécurité se compose de trois sections principales, une section d'en-tête, une section contenant des détails supplémentaires sur le ticket et une section d'artefacts de ticket contenant une collection d'enregistrements qui aident à construire un argument en faveur de l'identification et du traitement de menaces particulières.

En-tête de ticket

Section d'en-tête de ticket



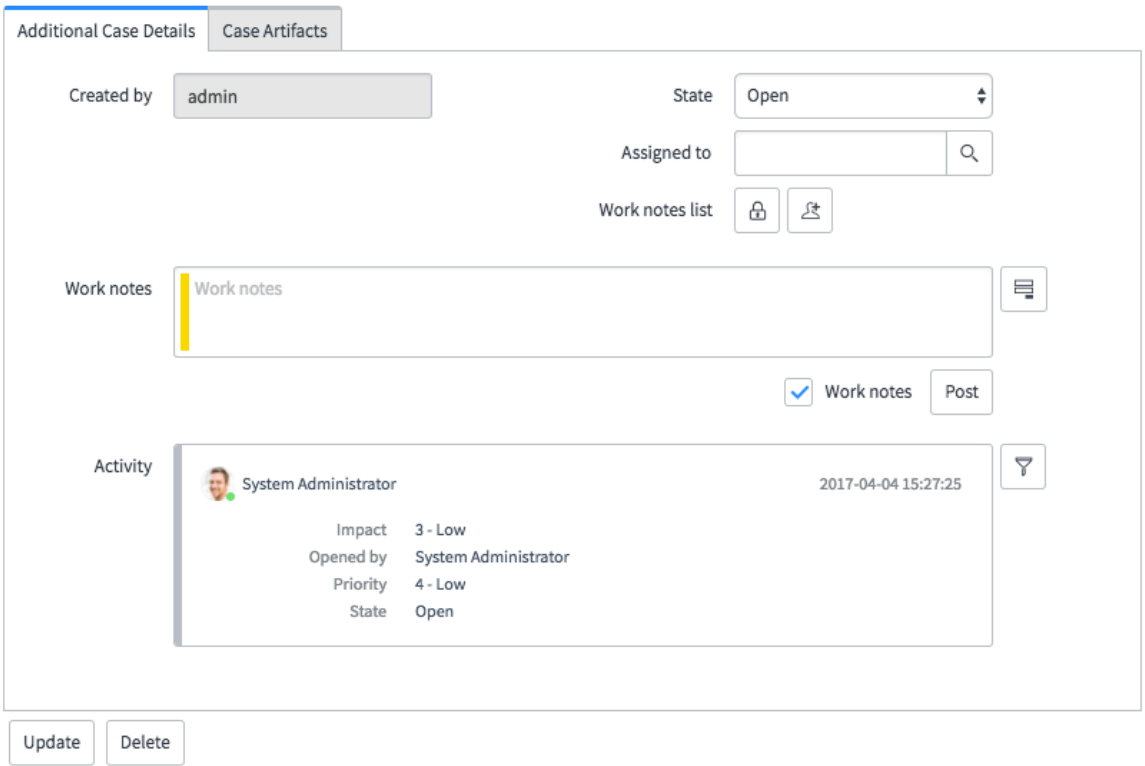
L'en-tête du ticket fournit des informations de base utilisées pour identifier et classifier le ticket de sécurité. Le numéro de dossier utilise le préfixe SECC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails supplémentaires du ticket

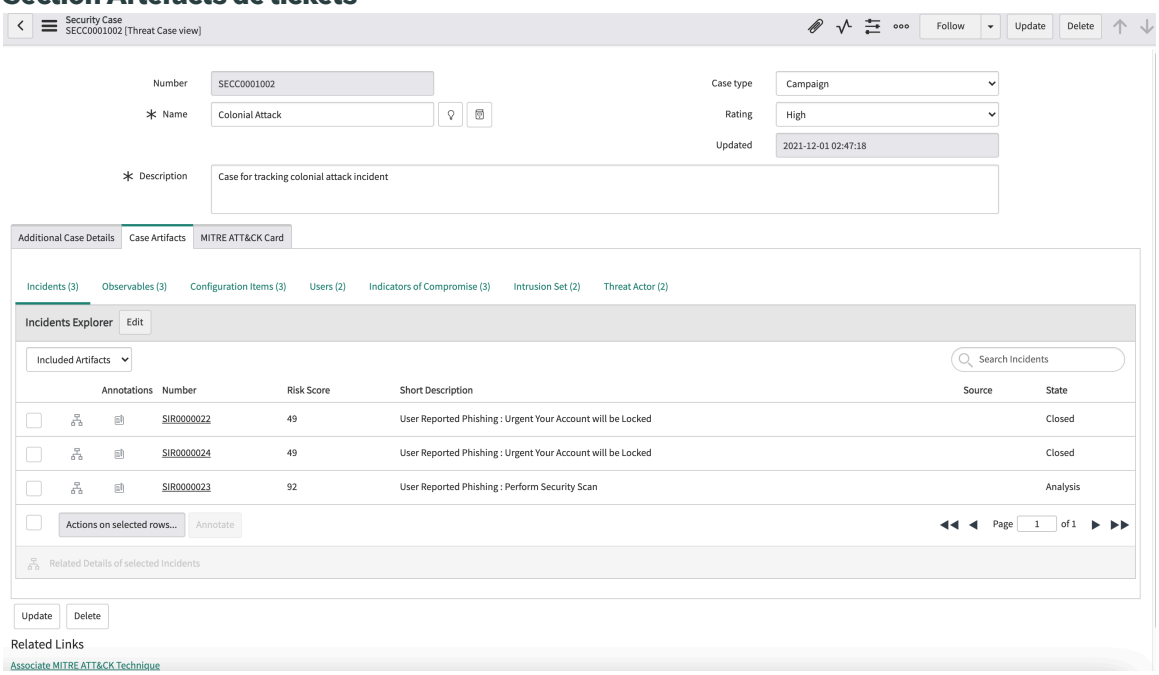
Section Détails supplémentaires du ticket



La section **Détails supplémentaires du ticket** fournit des informations spécifiques à l'analyse qui a déjà été effectuée sur le ticket, y compris son état actuel, ainsi que des notes de travail et des activités enregistrées pour le ticket.

Artefacts de ticket

Section Artefacts de tickets



Traduction automatique

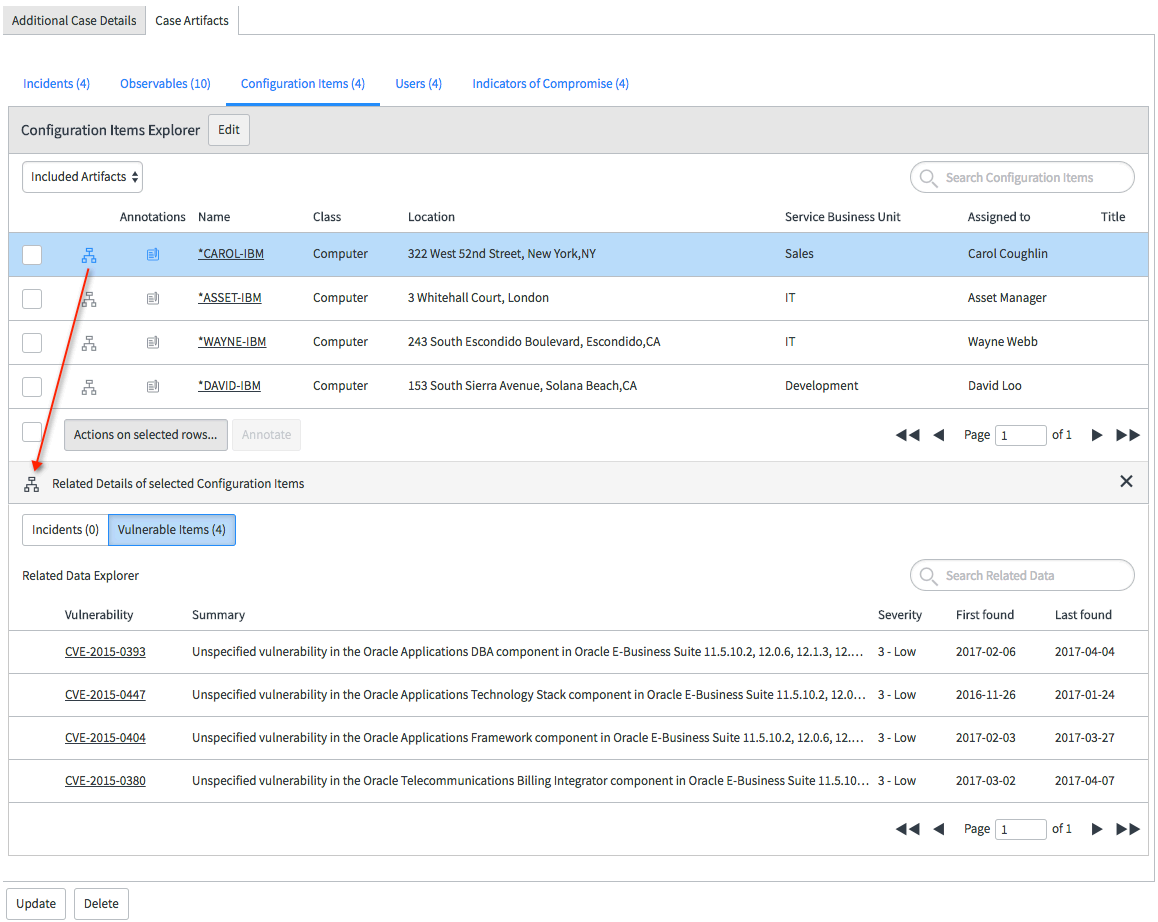
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La section **Artefacts du ticket** fournit une série d'onglets d'informations contenus dans le ticket de sécurité.

Vous pouvez effectuer des recherches dans le contenu de chaque onglet. Vous pouvez également exclure des enregistrements spécifiques que vous avez déjà évalués comme étant sûrs ou qui n'ont aucune valeur dans votre enquête. Les enregistrements exclus ne sont pas supprimés, mais sont masqués. Si nécessaire, vous pouvez afficher les enregistrements exclus et les ajouter à nouveau.

Dans chaque onglet, vous pouvez cliquer sur l'icône Détails supplémentaires pour afficher les informations connexes pour l'enregistrement sélectionné. Par exemple, si vous cliquez sur l'onglet **Éléments de configuration** pour afficher l'explorateur d'éléments de configuration et sur Détails supplémentaires pour un CI spécifique, vous pouvez afficher les incidents, les éléments vulnérables et les annotations associées à ce CI.

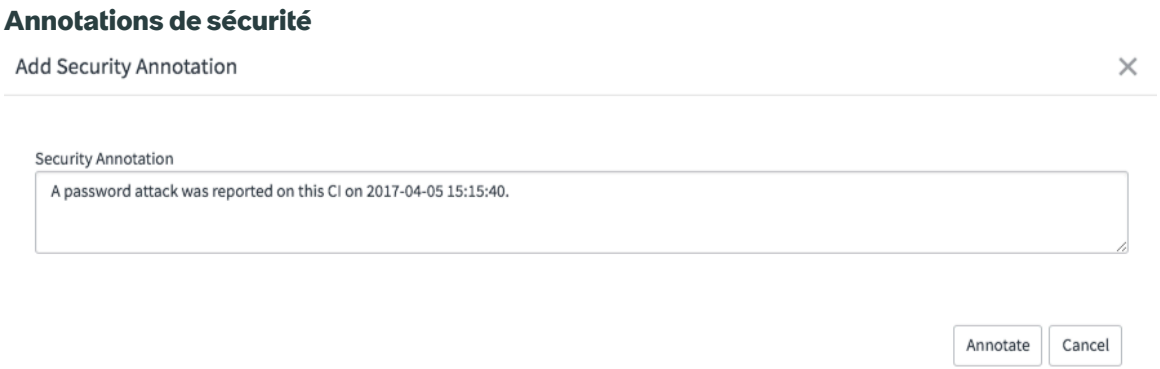
Artefacts de ticket : détails connexes



Vous pouvez également sélectionner un enregistrement et cliquer sur le bouton **Annoter** d'un artefact lié au ticket pour ajouter des annotations à l'enregistrement. Les annotations sont simplement des notes que chaque analyste peut faire sur un artefact particulier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



D’autres outils que l’analyste peut utiliser pour examiner les cas comprennent :

- Exécuter une recherche de perception sur les observables dans un ticket
- Rechercher des artefacts de sécurité

Créer des tickets dans Gestion des tickets de sécurité

Les tickets sont utilisés pour suivre les informations sur une campagne ou un acteur étatique menaçant votre organisation. Après la création d’un ticket, vous pouvez ajouter des artefacts qui vous permettent de passer en revue et d’analyser toutes les informations connexes dans un seul enregistrement de ticket.

Avant de commencer

Rôle requis : sn_ti.case_use

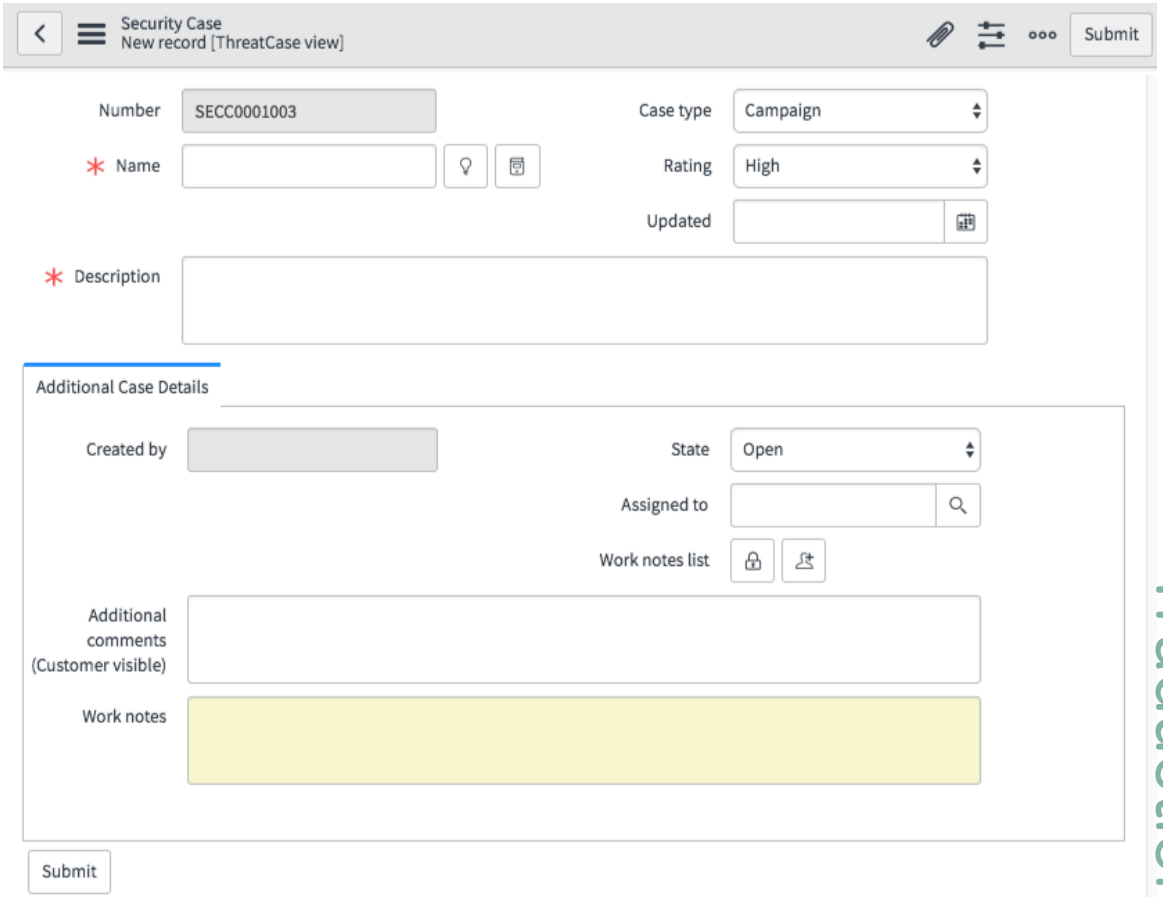
r

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
   La liste des tickets de sécurité s’ouvre.
2. Cliquez sur **Nouveau**.
   L’écran Tickets de sécurité s’ouvre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



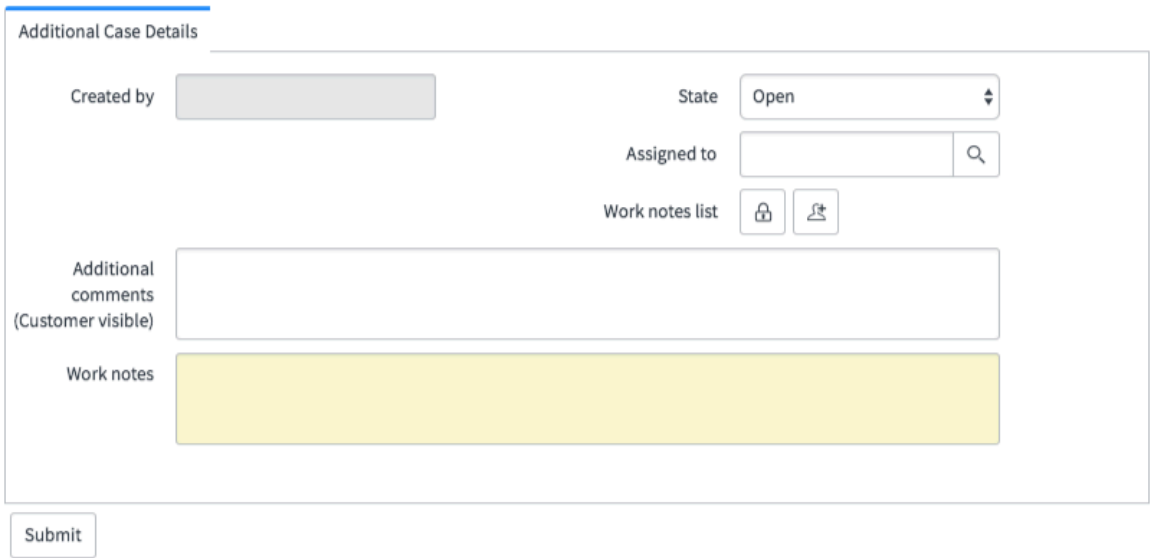
3. Renseignez les champs comme il convient.

Champ	Description
Numéro du ticket	[Lecture seule] Le numéro de ticket.
Nom du ticket	Saisissez un nom décrivant le ticket.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête.
Évaluation	Sélectionnez l'importance de ce ticket (de Critique à Faible).
Dernière mise à jour	[Lecture seule] Date et heure de la dernière mise à jour du ticket.
Description brève	Une brève description du ticket.

4. Cliquez sur l'onglet **Détails supplémentaires du ticket** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Renseignez les champs comme il convient.

Champ	Description
Créé par	[Lecture seule] Le nom de l'utilisateur qui a créé ce ticket.
État	État actuel du ticket. Lors de la création du ticket, l'état est défini par défaut sur Brouillon.
Affecté à	Cliquez sur l'icône de recherche et affectez le ticket à un analyste.
Liste de notes de travail	Cliquez sur l'icône de verrou et ajoutez des utilisateurs internes qui peuvent afficher les notes de travail.
Commentaires supplémentaires	Si nécessaire, saisissez des notes sur le ticket qui seront visibles par le client.
Notes de travail	Si nécessaire, saisissez une note de travail pour le ticket.

6. Cliquez sur **Envoyer**.
Une fois l'enregistrement sauvegardé, vous pouvez cliquer sur l'onglet **Artefacts du ticket** et ajouter des artefacts au ticket.

Ajouter des artefacts à un ticket

Une fois le ticket créé, vous pouvez y ajouter des artefacts, tels que des incidents de sécurité, des CI et des indicateurs de compromission. Ces artefacts servent d'indices pour résoudre l'affaire.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

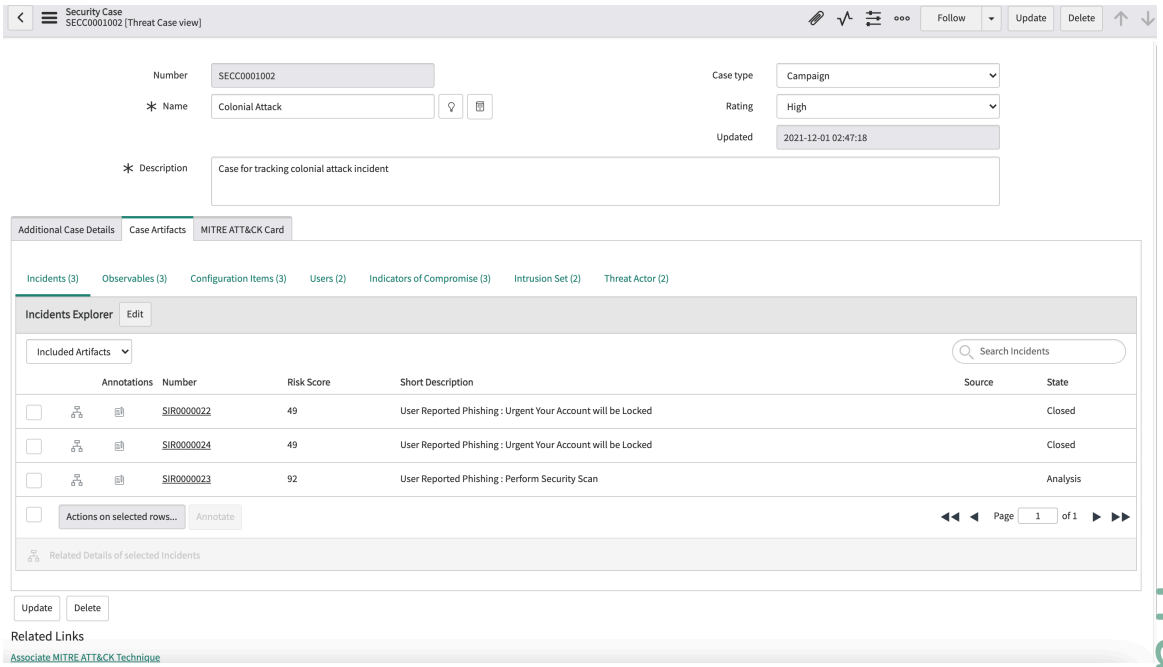
Procédure

1. Ouvrez un ticket auquel vous souhaitez ajouter des artefacts.

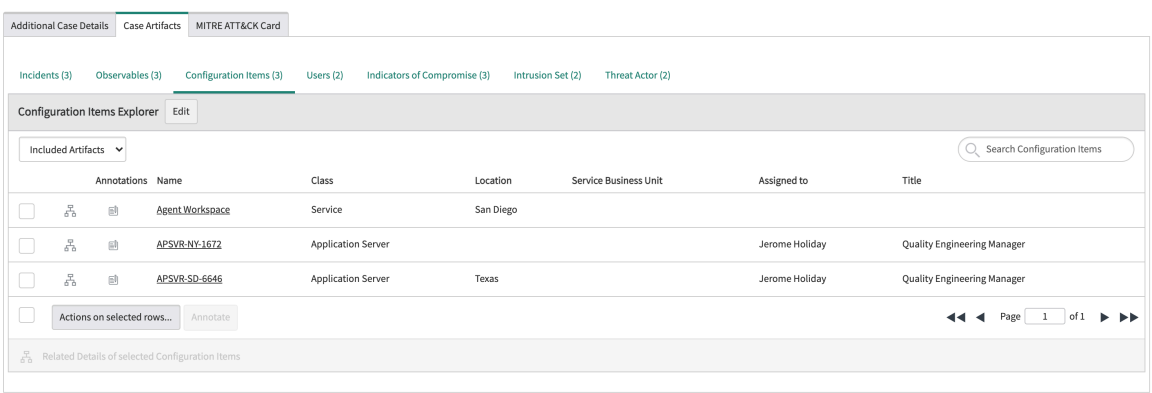
2. Cliquez sur la liste connexe **Artefacts de ticket** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



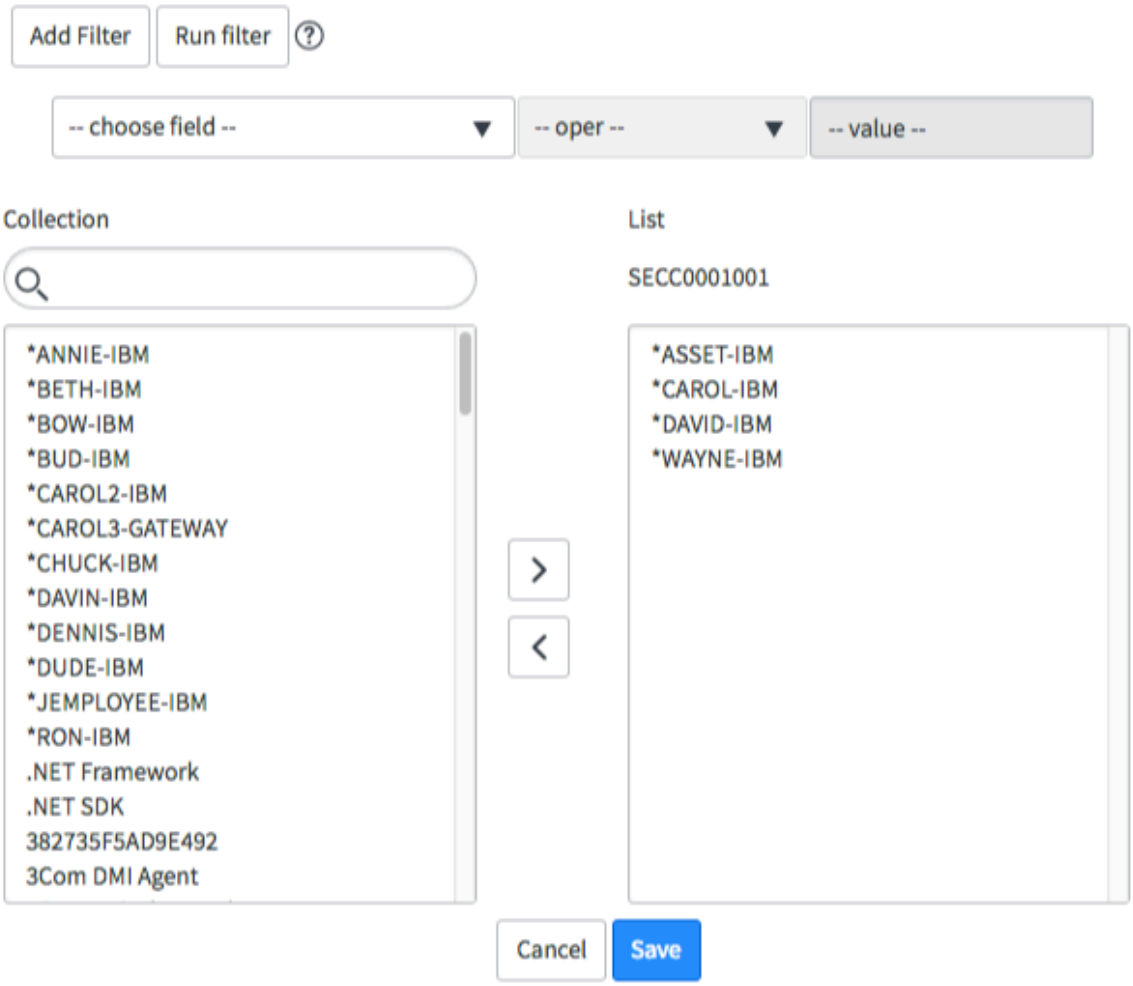
3. Cliquez sur l'onglet associé au type d'artefact que vous souhaitez ajouter au ticket.
Par exemple, cliquez sur **Éléments de configuration** pour ajouter un ou plusieurs CI au ticket.



4. Cliquez sur **Modifier**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. À l'aide de la zone de liste double et des filtres, localisez les enregistrements d'artefacts que vous souhaitez ajouter au ticket et déplacez-les de la catégorie Collection à la catégorie Liste, puis cliquez sur **Enregistrer**. La liste s'affiche dans l'onglet sélectionné et les artefacts sélectionnés sont ajoutés à la liste.

Information associée

Ajouter des IoC et des observables à un ticket existant

Ajouter des incidents de sécurité à un ticket existant

Ajouter des CI aux tickets existants

Ajouter des utilisateurs affectés aux tickets existants

Associer les MITRE-ATT&CK informations au ticket de sécurité

Associez MITRE-ATT&CK des tactiques et des techniques à un ticket de sécurité pour une meilleure gestion des tickets de sécurité et une meilleure analyse des menaces à un niveau granulaire.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
2. Sélectionnez le ticket de sécurité que vous souhaitez enrichir avec les informations MITRE-ATT&CK.

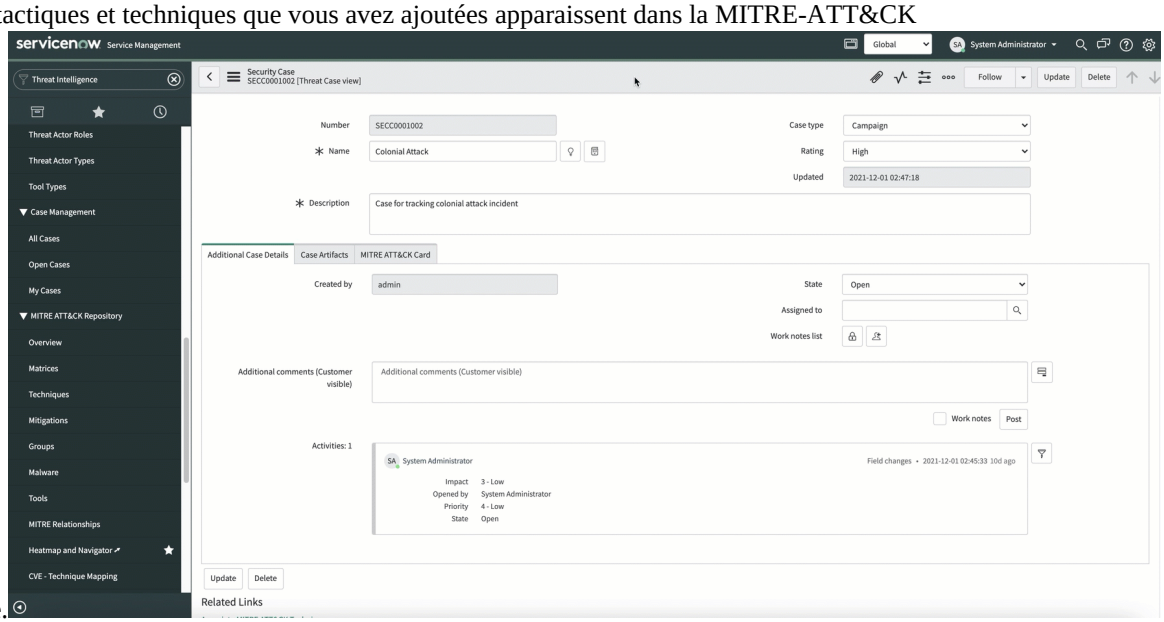
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la liste connexe, cliquez sur **Associer la technique MITRE ATT&CK**.

   Dans l'illustration suivante, vous pouvez voir comment naviguer à partir de la liste connexe pour **associer la technique MITRE ATT&CK**, examiner la source et ajouter une tactique et une technique.

4. Dans les listes de sources, examinez la **source**.
5. Passez en revue la **tactique** et les **techniques**, et ajoutez-les ou supprimez-les en fonction de leur pertinence avec le ticket.
6. Cliquez sur **Enregistrer**.
   Les tactiques et techniques que vous avez ajoutées apparaissent dans la MITRE-ATT&CK carte.



Création de ticket à partir d'artefacts de sécurité

En plus de créer des tickets manuellement à partir de Gestion des tickets de sécurité, vous pouvez également créer des tickets à partir d'artefacts de sécurité, tels que des incidents de sécurité, des indicateurs de compromission, des utilisateurs affectés et des éléments de configuration.

IoC et observables dans les tickets

Dans Renseignements sur les menaces, vous pouvez créer des cas à partir d'IoC et d'observables, ainsi qu'ajouter des IoC et des observables à des tickets existants. Vous pouvez également créer des observables directement à partir d'un ticket.

Créer un ticket à partir d'IoC ou d'observables

Dans Renseignements sur les menaces, vous pouvez créer un ticket à partir d'artefacts (IoC ou observables). Une fois que les IoC ou les observables ont été utilisés pour créer un ticket, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Traduction automatique

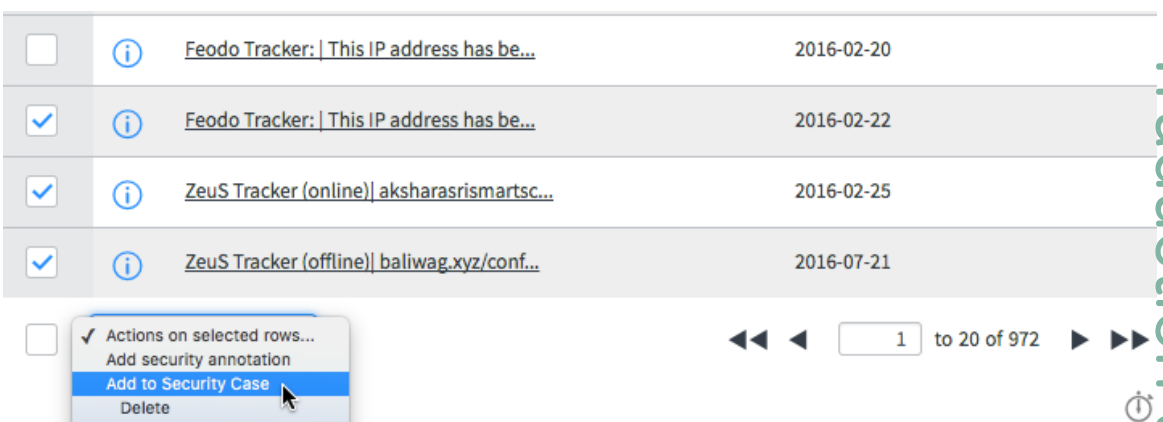
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

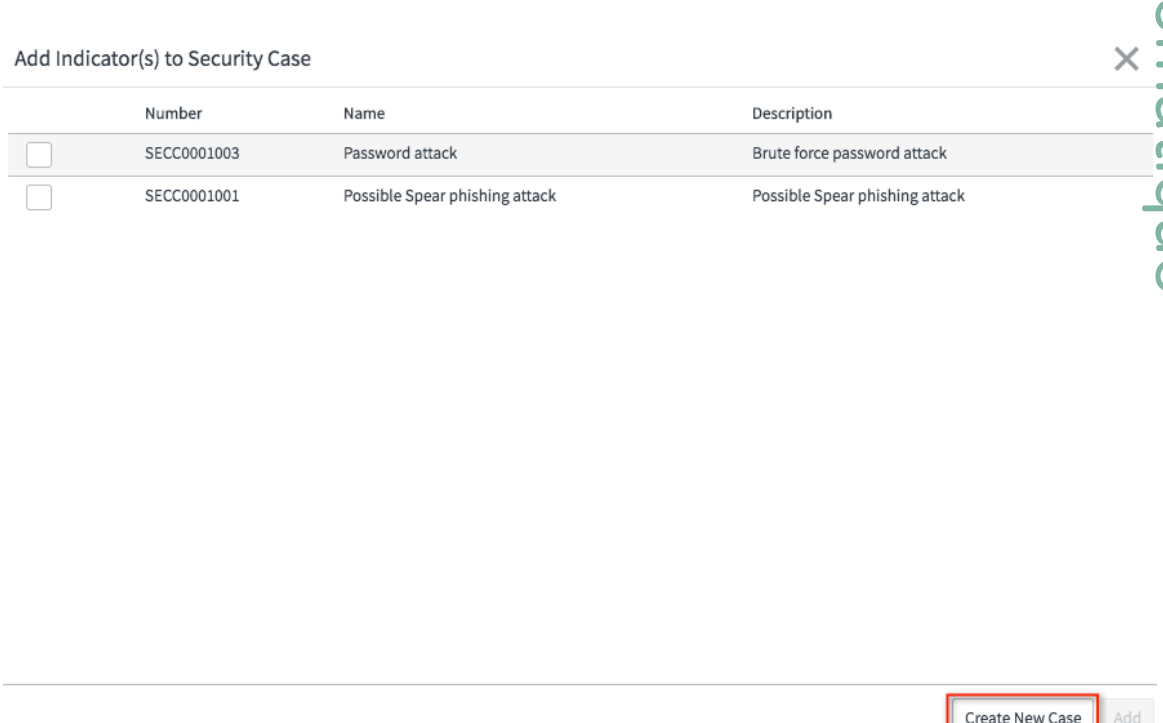
1. Accédez aux artefacts (IoC ou observables) que vous souhaitez utiliser pour créer un ticket.
   - Pour créer un ticket à partir d'IoC, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
   - Pour créer un ticket à partir d'observables, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Dans la liste, sélectionnez les artefacts que vous souhaitez ajouter à un nouveau ticket.

   Remarque : Si vous sélectionnez plusieurs IoC ou observables, ils sont tous ajoutés au ticket.

3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.



La boîte de dialogue **Ajouter au ticket de sécurité** s'ouvre. Si des tickets vous ont déjà été affectés, ils s'affichent dans la liste.



4. Cliquez sur **Créer un ticket**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Renseignez les champs.

Champ	Description
Nom du ticket	Entrez un nom pour ce ticket.
Description	Saisissez une description qui pourrait être utile à l'analyste du ticket.

6. Cliquez sur **Envoyer**.
   Un message en haut de la liste indique qu'un nouveau ticket a été créé, ainsi qu'un lien vers le ticket dans Gestion des tickets de sécurité.
7. Cliquez sur le lien pour afficher le nouveau ticket.

Ajouter des IoC et des observables à un ticket existant

Vous pouvez ajouter des IoC et des observables à des tickets existants. Une fois les incidents de sécurité ajoutés aux tickets, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Procédure

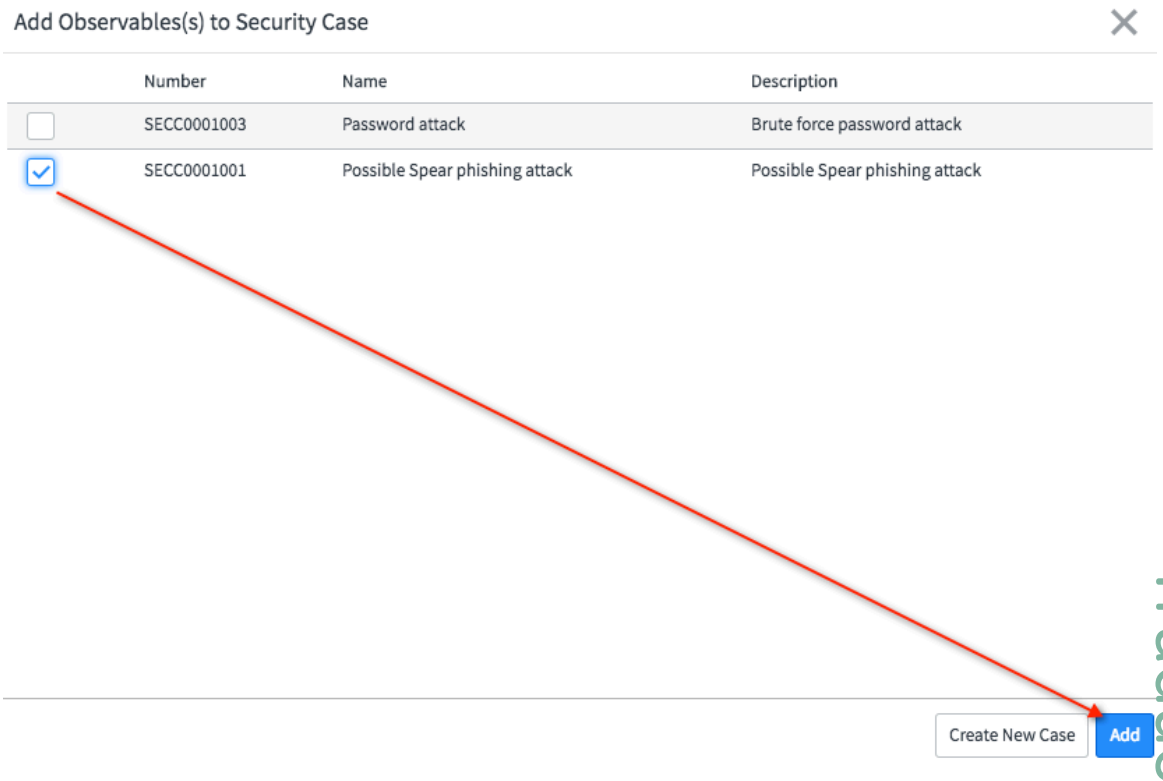
1. Accédez aux artefacts (IoC ou observables) que vous souhaitez ajouter aux tickets existants.
   - Pour ajouter des IoC à un ou plusieurs tickets, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Indicateurs**.
   - Pour ajouter des observables à un ou plusieurs tickets, accédez à **Renseignements sur les menaces** > **Référentiel IoC** > **Observables**.
2. Dans la liste, sélectionnez les enregistrements d'artefacts que vous souhaitez ajouter aux tickets existants.

   Remarque : Si vous sélectionnez plusieurs tickets, les IoC ou observables sélectionnés sont ajoutés à chacun des tickets sélectionnés.

3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.
   La boîte de dialogue **Ajouter au ticket de sécurité** s'ouvre. Si des tickets vous ont déjà été affectés, ils s'affichent dans la liste.
4. Sélectionnez les tickets dans lesquels vous souhaitez ajouter les IoC ou observables sélectionnés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Ajouter**.
   Un message indique que les enregistrements sélectionnés ont été ajoutés aux tickets, ainsi qu'un lien vers les tickets dans Gestion des tickets de sécurité.

Créer un observable à partir d'un ticket

De nouveaux observables peuvent être créés à partir des tickets dans Gestion des tickets de sécurité.

Avant de commencer

Rôle requis : sn_ti.case_user

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
   La liste des tickets de sécurité s'ouvre.
2. Ouvrez un ticket existant ou cliquez sur **Nouveau** pour créer un nouveau ticket.
3. Cliquez sur le lien connexe **Artefacts de ticket** , puis sur l'onglet **Observables** .
4. Cliquez sur **Nouveau** et saisissez les informations demandées.

Champ	Description
Valeur	[Lecture seule] Le numéro de ticket.
Type d'observable	Saisissez un nom décrivant le ticket.
Catégorie du type de l'observable	Sélectionnez le type de ticket faisant l'objet de l'enquête.
Nombre d'incidents	Sélectionnez l'importance de ce ticket (de Critique à Faible).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Résultat	[Lecture seule] Date et heure de la dernière mise à jour du ticket.
Notes	Une brève description du ticket.

5. Cliquez sur l'onglet **Détails supplémentaires du ticket** .
6. Renseignez les champs comme il convient.

Champ	Description
Créé par	[Lecture seule] Le nom de l'utilisateur qui a créé ce ticket.
État	État actuel du ticket. Lors de la création du ticket, l'état est défini par défaut sur Brouillon.
Liste de notes de travail	Cochez la case pour afficher les notes de travail dans la section Détails supplémentaires du ticket de l'enregistrement de ticket.
Notes de travail	Si nécessaire, saisissez une note de travail pour le ticket. Si la **liste** Notes de travail est sélectionnée, la note de travail s'affiche dans la section Détails supplémentaires du ticket de l'enregistrement du ticket.

7. Cliquez sur **Envoyer**.
   Si nécessaire, vous pouvez cliquer sur l'onglet **Artefacts du ticket** et ajouter des artefacts au ticket.

Exécuter une recherche de perception sur les observables dans un ticket

Vous pouvez rechercher des observables à l'aide de la fonctionnalité Recherche de perception pour déterminer leur fréquence. Chaque occurrence est considérée comme une *observation*. Vous pouvez limiter la recherche au nombre d'observations dans un nombre de jours ou une plage de dates sélectionné.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

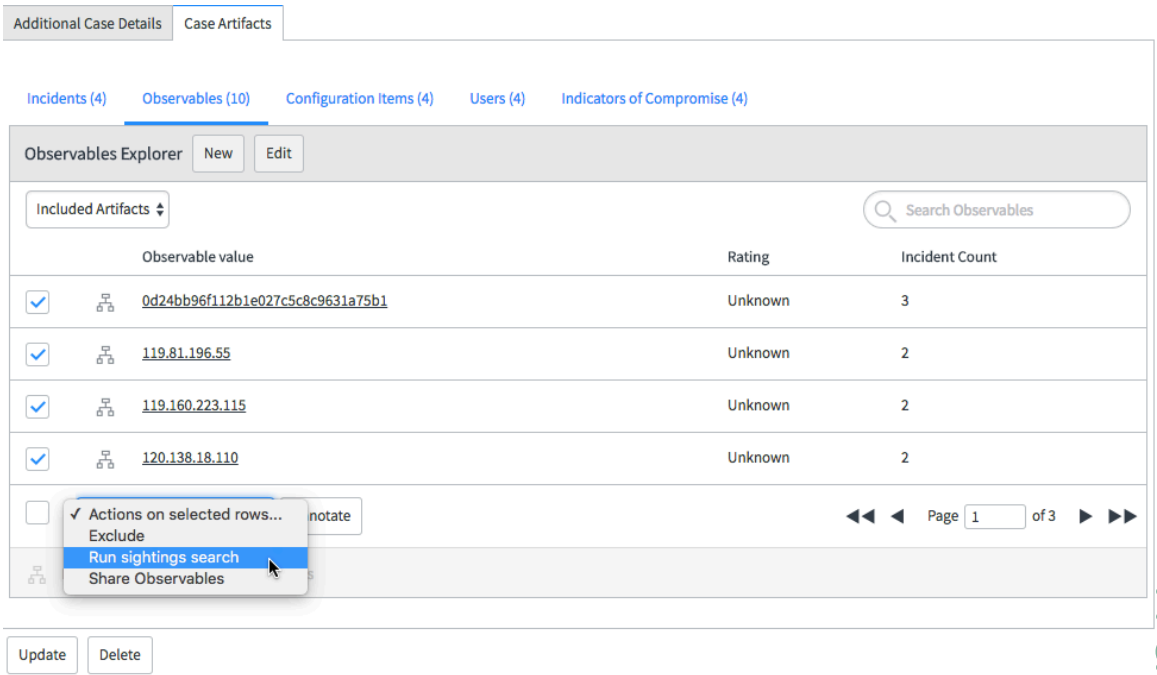
Rôle requis : sn_ti.case_user_write

Procédure

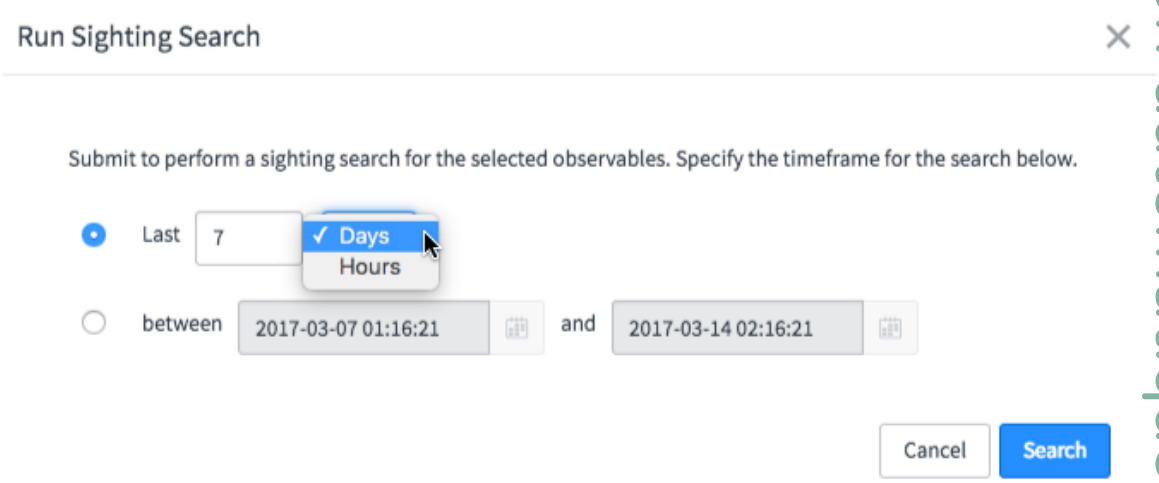
1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Gestion des tickets** > **Tous les tickets**.
2. Ouvrez le ticket qui contient les observables pour lesquels vous souhaitez exécuter une recherche d'observations.
3. Cliquez sur le lien connexe **Artefacts du ticket** .
4. Cliquez sur l'onglet **Observables** .
5. Sélectionnez un ou plusieurs observables pour lesquels vous souhaitez rechercher des observations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Exécuter la recherche d'observations**.
   La boîte de dialogue **Exécuter la recherche de perception** s'affiche.



7. Entrez le nombre de jours ou d'heures pendant lesquels vous souhaitez rechercher des observations des observables sélectionnés ou sélectionnez une plage de dates.
8. Cliquez sur **Rechercher**.

Incidents de sécurité dans les tickets

Dans Réponse aux incidents de sécurité, vous pouvez créer des tickets à partir d'incidents de sécurité, de CI et d'utilisateurs affectés, et ajouter ces artefacts aux tickets existants.

Créer un ticket à partir d'incidents de sécurité

Dans Réponse aux incidents de sécurité, vous pouvez créer des tickets à partir d'incidents de sécurité. Une fois que les incidents de sécurité ont été utilisés pour créer un nouveau ticket, vous pouvez l'utiliser Gestion des tickets de sécurité pour analyser les données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

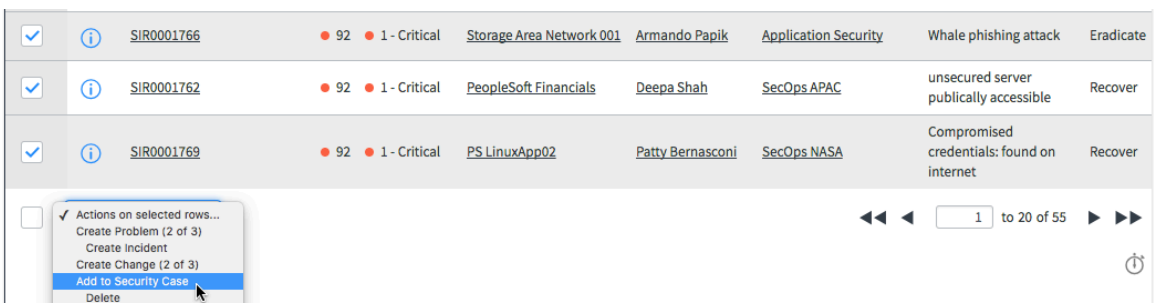
Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

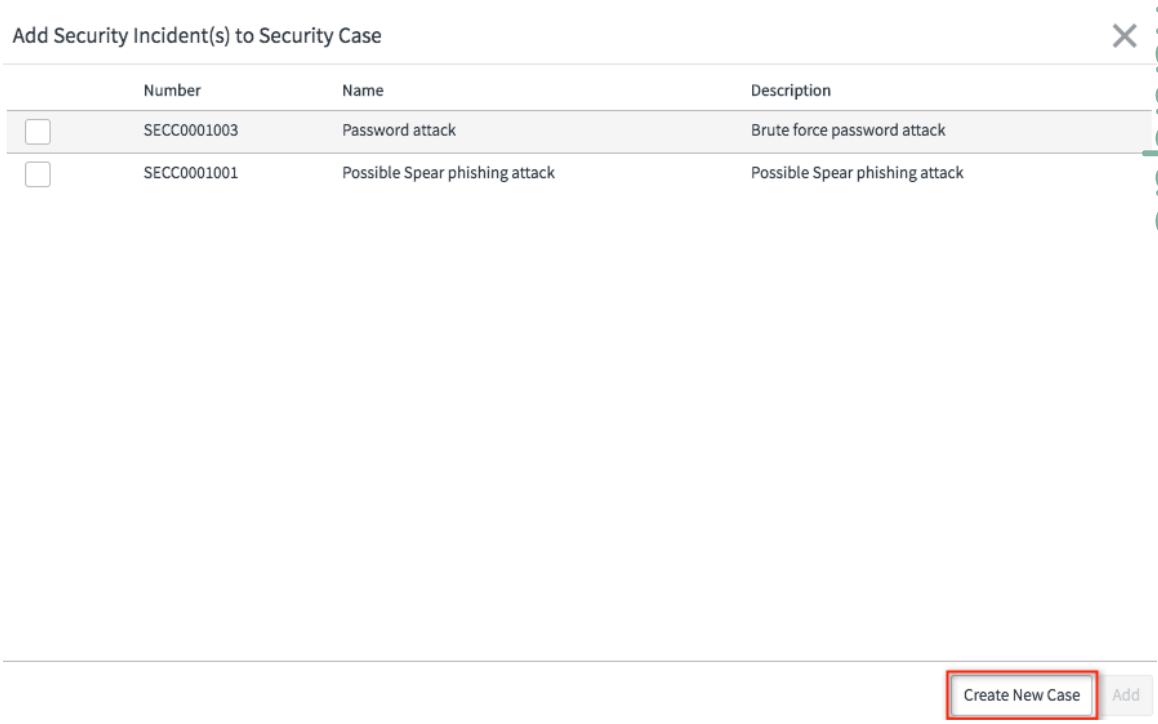
Vous devez accéder aux incidents de sécurité que vous souhaitez utiliser pour créer des tickets.

Procédure

1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents ouverts**.
   La liste des incidents de sécurité s'ouvre. Dans la liste, vous pouvez créer un cas à partir d'un ou de plusieurs incidents de sécurité, ou vous pouvez sélectionner un incident de sécurité spécifique et créer un nouveau ticket à partir du formulaire.
2. Pour créer un ticket dans la liste, sélectionnez les artefacts que vous souhaitez ajouter à un nouveau ticket.
3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.



La boîte de dialogue **Ajouter au ticket de sécurité** s'ouvre. Si des tickets vous ont déjà été affectés, ils s'affichent dans la liste.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Créer un ticket**.
5. Renseignez les champs.

Champ	Description
Nom du ticket	Entrez un nom pour ce ticket.
Description	Saisissez une description qui pourrait être utile à l'analyste du ticket.

6. Cliquez sur **Envoyer**.
   Un message en haut de la liste indique qu'un nouveau ticket a été créé, ainsi qu'un lien vers le ticket dans Gestion des tickets de sécurité.
7. Cliquez sur le lien pour afficher le nouveau ticket.

Ajouter des incidents de sécurité à un ticket existant

Vous pouvez ajouter des incidents de sécurité à un ou plusieurs tickets existants. Une fois les incidents de sécurité ajoutés aux tickets, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

Vous devez accéder aux incidents de sécurité que vous souhaitez ajouter aux tickets existants.

Procédure

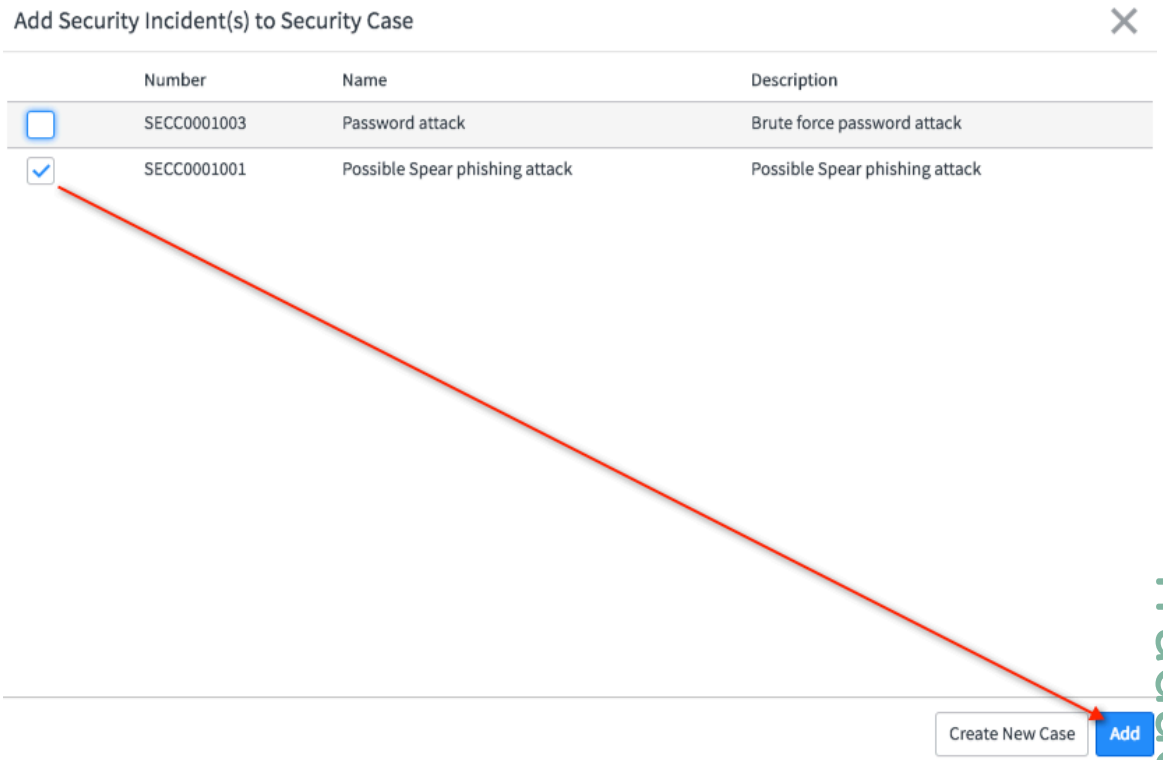
1. Accédez à la **Tous** > **Incident de sécurité** > **Incidents** > **Afficher les incidents ouverts**.
   La liste des incidents de sécurité s'ouvre.
2. Dans la liste, sélectionnez un ou plusieurs incidents de sécurité que vous souhaitez ajouter aux tickets existants.

   Remarque : Si vous sélectionnez plusieurs incidents de sécurité, les incidents de sécurité sélectionnés sont ajoutés à chacun des tickets sélectionnés.

3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.
   La boîte de dialogue **Ajouter au ticket de sécurité** s'ouvre et affiche les tickets qui vous sont affectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez les tickets dans lesquels vous souhaitez ajouter les incidents de sécurité sélectionnés.
5. Cliquez sur **Ajouter**.
   Un message indique que les enregistrements sélectionnés ont été ajoutés aux tickets, ainsi qu'un lien vers les tickets dans Gestion des tickets de sécurité.

Éléments de configuration dans les tickets

Vous pouvez créer un ticket à partir d'un ou de plusieurs éléments de configuration (CI) dans la table Élément de configuration [cmdb_ci]. Vous pouvez également ajouter des CI à des tickets existants.

Créer un ticket à partir de CI

Vous pouvez créer un ticket de sécurité à partir d'éléments de configuration dans la table Élément de configuration [cmdb_ci]. Une fois que les CI ont été utilisés pour créer un nouveau ticket, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

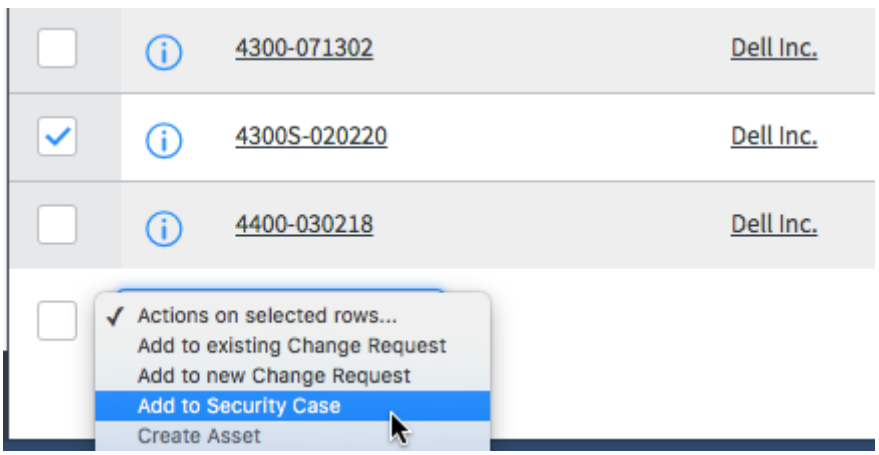
Vous devez accéder aux éléments de configuration que vous souhaitez utiliser pour créer un ticket.

Traduction automatique

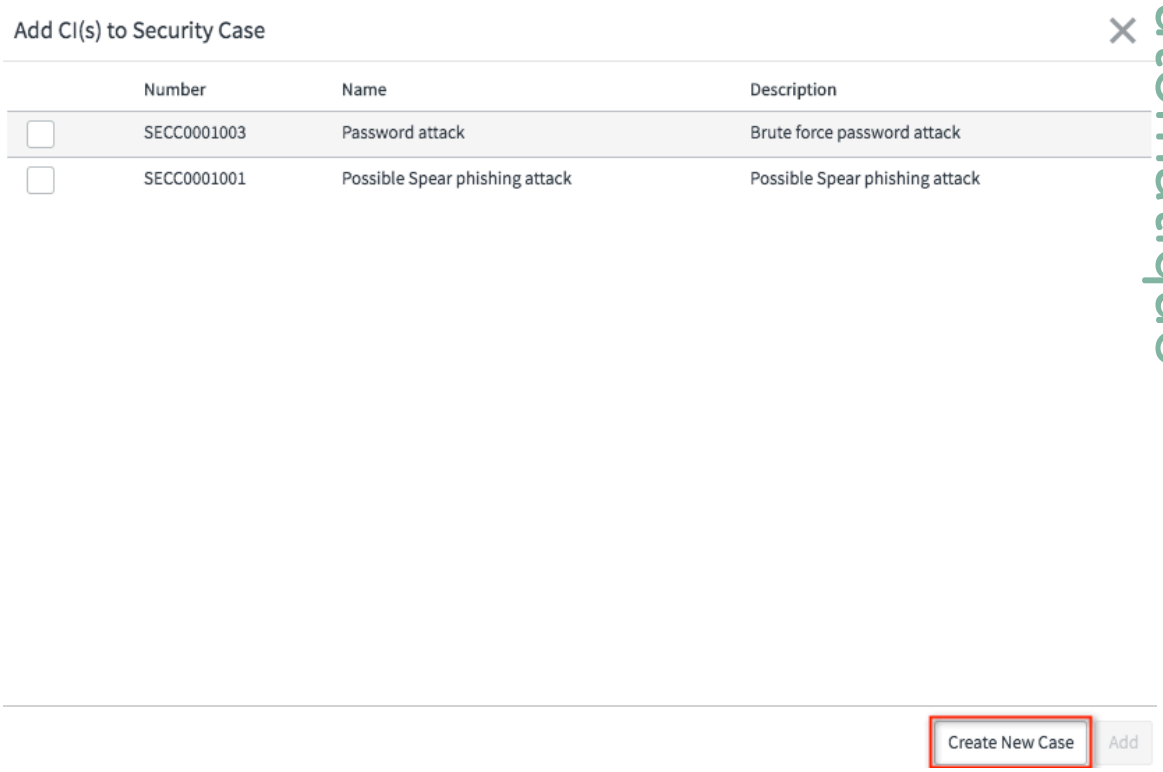
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Configuration** > **Éléments de base** > **Ordinateurs** pour afficher les CI des ordinateurs.
   La liste du type de CI sélectionné s'ouvre. Dans la liste, vous pouvez créer un nouveau ticket à partir d'un ou de plusieurs CI, ou vous pouvez sélectionner un CI spécifique et créer un nouveau ticket à partir du formulaire.
2. Dans la liste, sélectionnez les CI que vous souhaitez ajouter à un nouveau ticket.
3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.



La boîte de dialogue **Ajouter au ticket de sécurité** s'ouvre. Si des tickets vous ont déjà été affectés, ils s'affichent dans la liste.



4. Cliquez sur **Créer un ticket**.
5. Renseignez les champs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du ticket	Entrez un nom pour ce ticket.
Description	Saisissez une description qui pourrait être utile à l'analyste du ticket.

6. Cliquez sur **Envoyer**.
   Un message en haut de la liste indique qu'un nouveau ticket a été créé, ainsi qu'un lien vers le ticket dans Gestion des tickets de sécurité.
7. Cliquez sur le lien pour afficher le nouveau ticket.

Ajouter des CI aux tickets existants

Vous pouvez ajouter des éléments de configuration à un ou plusieurs tickets existants. Une fois les CI ajoutés aux tickets, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

Vous devez accéder aux CI que vous souhaitez ajouter aux tickets existants.

Procédure

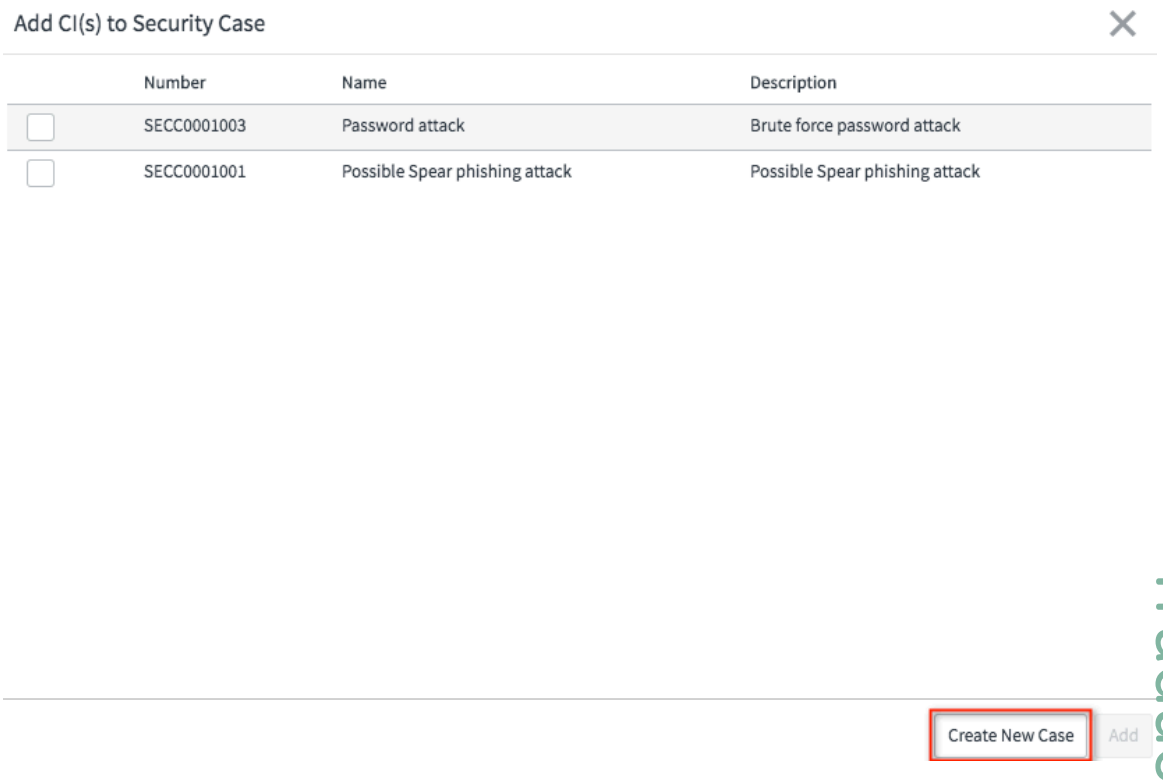
1. Accédez à la **Tous** > **Configuration** > **Éléments de base** > **Ordinateurs** pour afficher les CI des ordinateurs.
   La liste des CI sélectionnés s'ouvre.
2. Dans la liste, sélectionnez un ou plusieurs CI que vous souhaitez ajouter aux tickets existants.

   Remarque : Si vous sélectionnez plusieurs CI, les CI sélectionnés sont ajoutés à chacun des tickets sélectionnés.

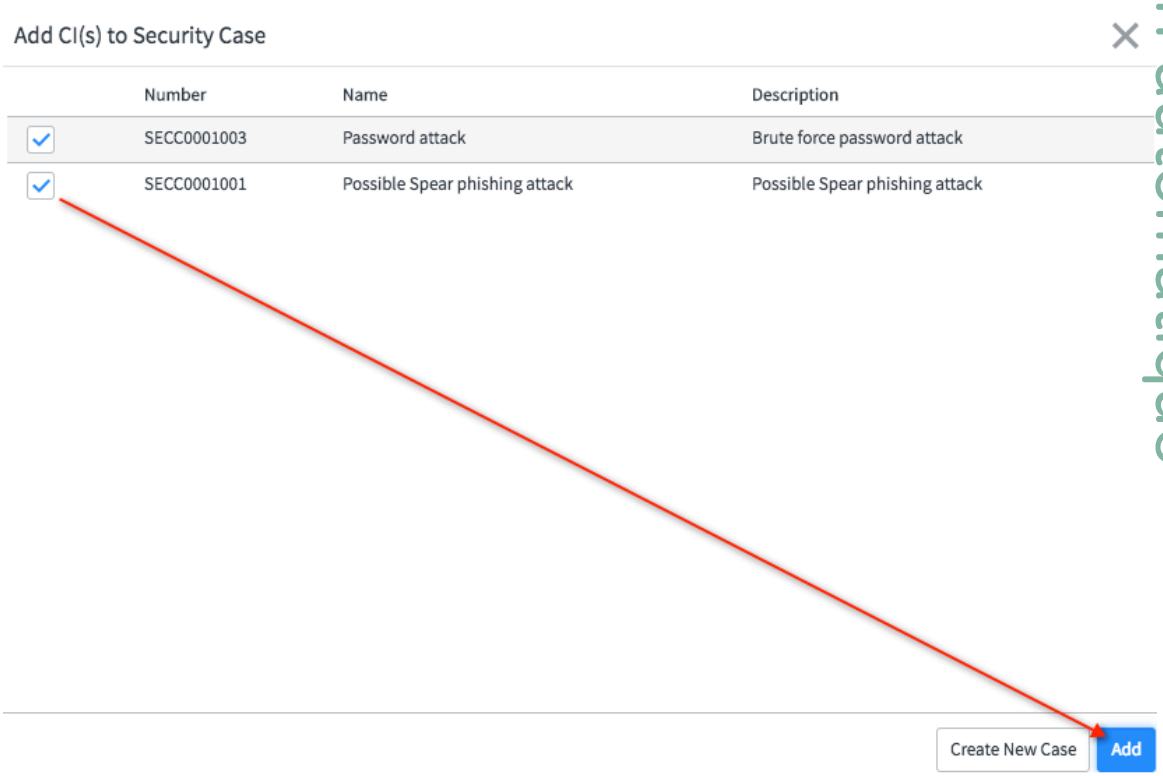
3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.
   La boîte de dialogue **Ajouter au ticket de sécurité** s'ouvre et affiche les tickets qui vous sont affectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez les tickets dans lesquels vous souhaitez ajouter les CI sélectionnés.



5. Cliquez sur **Ajouter**.
Un message indique que les enregistrements sélectionnés ont été ajoutés aux tickets, ainsi qu'un lien vers les tickets dans Gestion des tickets de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs affectés dans les tickets

Vous pouvez créer un ticket à partir d'un ou de plusieurs utilisateurs affectés dans la table Utilisateur [sys_user]. Vous pouvez également ajouter des utilisateurs à des tickets existants.

Créer un ticket à partir des utilisateurs affectés

Vous pouvez créer un ticket de sécurité à partir des utilisateurs affectés dans la table Utilisateur [sys_user]. Une fois que les utilisateurs affectés ont été utilisés pour créer un nouveau ticket, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

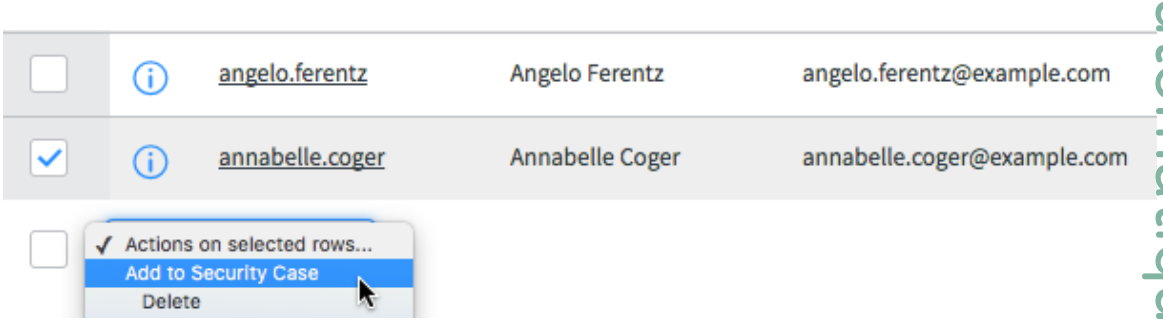
Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

Vous devez accéder aux utilisateurs que vous souhaitez utiliser pour créer un ticket.

Procédure

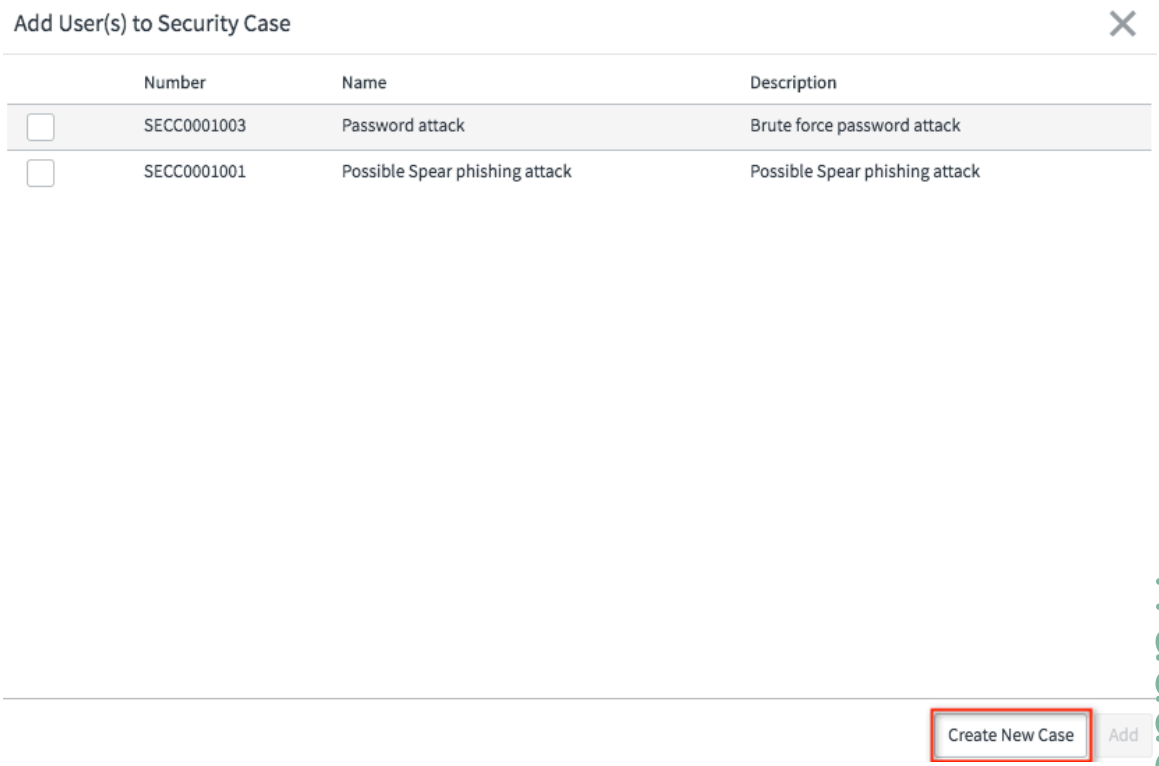
1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs**.
   La liste des utilisateurs sélectionnés s'ouvre. Dans la liste, vous pouvez créer un nouveau ticket à partir d'un ou de plusieurs enregistrements utilisateur, ou vous pouvez sélectionner un enregistrement utilisateur spécifique et créer un nouveau ticket à partir du formulaire.
2. Dans la liste, sélectionnez les utilisateurs que vous souhaitez ajouter à un nouveau ticket.
3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.



La boîte de dialogue **Ajouter au ticket de sécurité** s'ouvre. Si des tickets vous ont déjà été affectés, ils s'affichent dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Créer un ticket**.
5. Renseignez les champs.

Champ	Description
Nom du ticket	Entrez un nom pour ce ticket.
Description	Saisissez une description qui pourrait être utile à l'analyste du ticket.

6. Cliquez sur **Envoyer**.
   Un message en haut de la liste indique qu'un nouveau ticket a été créé, ainsi qu'un lien vers le ticket dans Gestion des tickets de sécurité.
7. Cliquez sur le lien pour afficher le nouveau ticket.

Ajouter des utilisateurs affectés aux tickets existants

Vous pouvez ajouter des utilisateurs affectés à un ou plusieurs tickets existants. Une fois les enregistrements d'utilisateur ajoutés aux tickets, vous pouvez les utiliser Gestion des tickets de sécurité pour analyser les données.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Pourquoi et quand exécuter cette tâche

Vous devez accéder aux enregistrements utilisateur que vous souhaitez ajouter aux tickets existants.

Traduction automatique

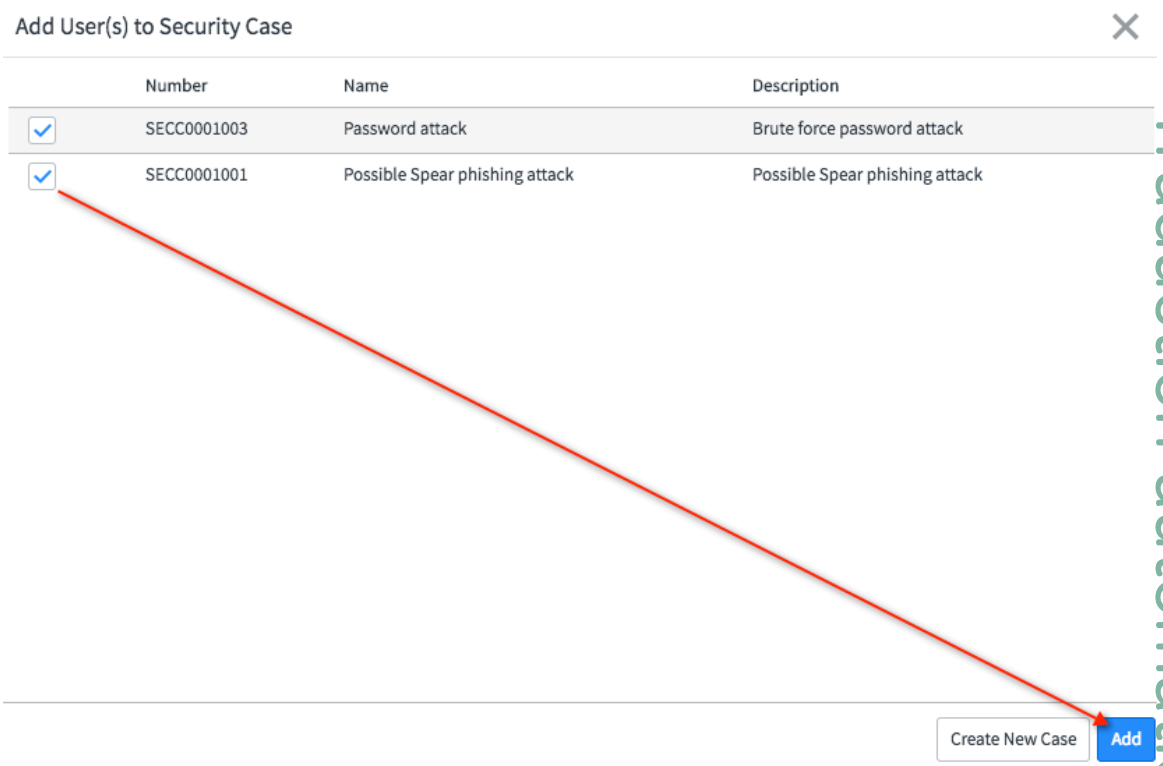
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs**.
   La liste des enregistrements d'utilisateurs s'ouvre.
2. Dans la liste, sélectionnez un ou plusieurs utilisateurs que vous souhaitez ajouter aux tickets existants.

   Remarque : Si vous sélectionnez plusieurs utilisateurs, les enregistrements des utilisateurs sélectionnés sont ajoutés à chacun des tickets sélectionnés.

3. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Ajouter au ticket de sécurité**.
   La boîte de dialogue **Ajouter au ticket de sécurité** s'ouvre et affiche les tickets qui vous sont affectés.



4. Sélectionnez les tickets dans lesquels vous souhaitez ajouter les utilisateurs sélectionnés.
5. Cliquez sur **Ajouter**.
   Un message indique que les enregistrements sélectionnés ont été ajoutés aux tickets, ainsi qu'un lien vers les tickets dans Gestion des tickets de sécurité.

Traduction automatique

Analyse des artefacts de sécurité

Après avoir créé des tickets, à l'aide Gestion des tickets de sécurité de , ou à partir d'artefacts tels que des IoC, des observables, des incidents de sécurité, etc., vous pouvez continuer à ajouter des artefacts pour faciliter l'analyse des menaces identifiées.

Détails connexes pour les artefacts de ticket

Lorsque vous ajoutez des artefacts à un ticket, des détails connexes supplémentaires pour chaque artefact peuvent également être ajoutés automatiquement. Par exemple, si vous ajoutez un incident de sécurité, il peut contenir des CI et des enregistrements d'utilisateurs affectés. Vous pouvez afficher rapidement les détails connexes pour un artefact sélectionné sans quitter la liste des artefacts.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les détails connexes d'un artefact d'incident de sécurité

Si votre ticket comprend des artefacts d'incident de sécurité, vous pouvez afficher tous les détails connexes contenus dans chaque incident de sécurité référencé par le ticket.

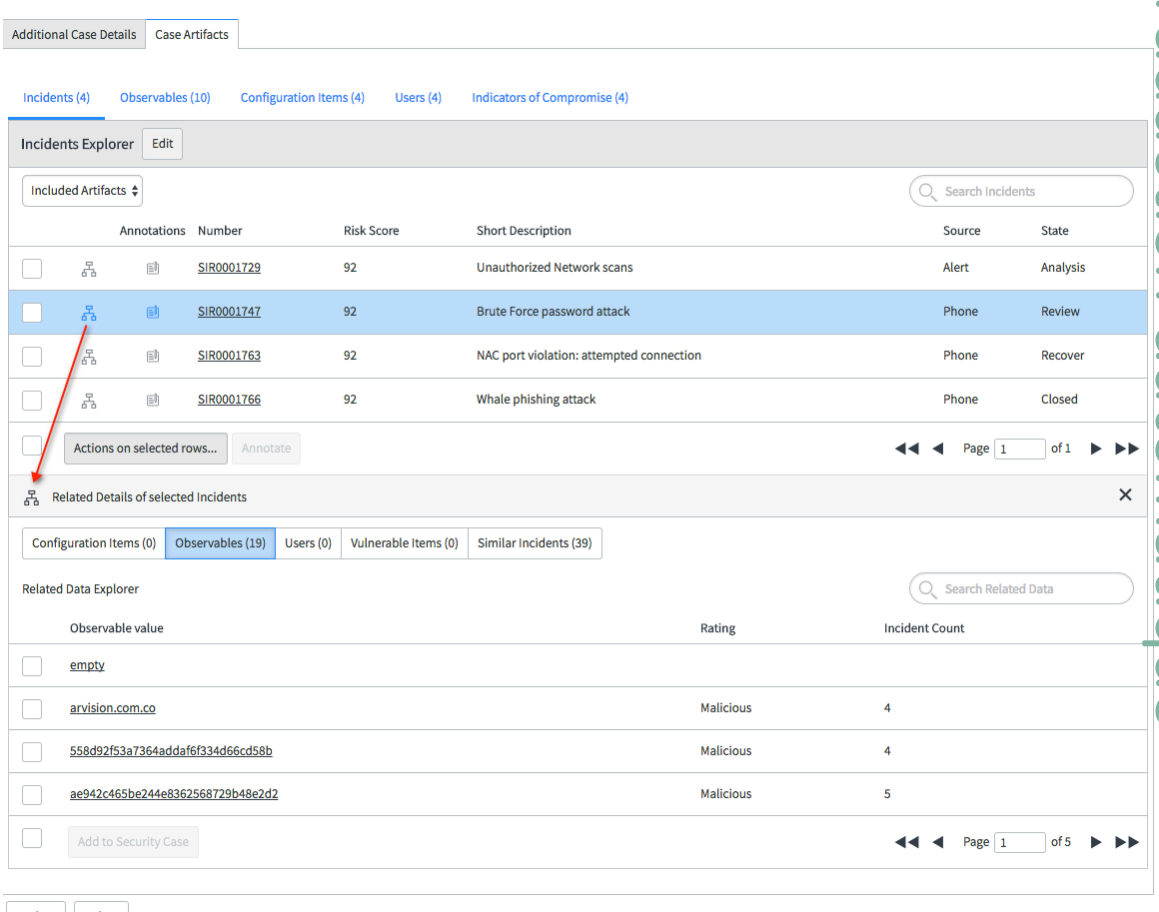
Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket contenant des artefacts d'incident de sécurité.
2. Cliquez sur l'onglet **Incidents** .
3. Cliquez sur l'icône Détails supplémentaires de l'incident de sécurité pour lequel vous souhaitez afficher les détails connexes.



4. Cliquez sur l'un des onglets pour afficher des types spécifiques de détails relatifs à l'artefact sélectionné.
5. Vous pouvez également cliquer sur l'onglet **Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Afficher les détails connexes d'un artefact d'élément de configuration

Si votre ticket comprend des artefacts d'élément de configuration, vous pouvez afficher tous les détails connexes contenus dans chaque CI référencé par le ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

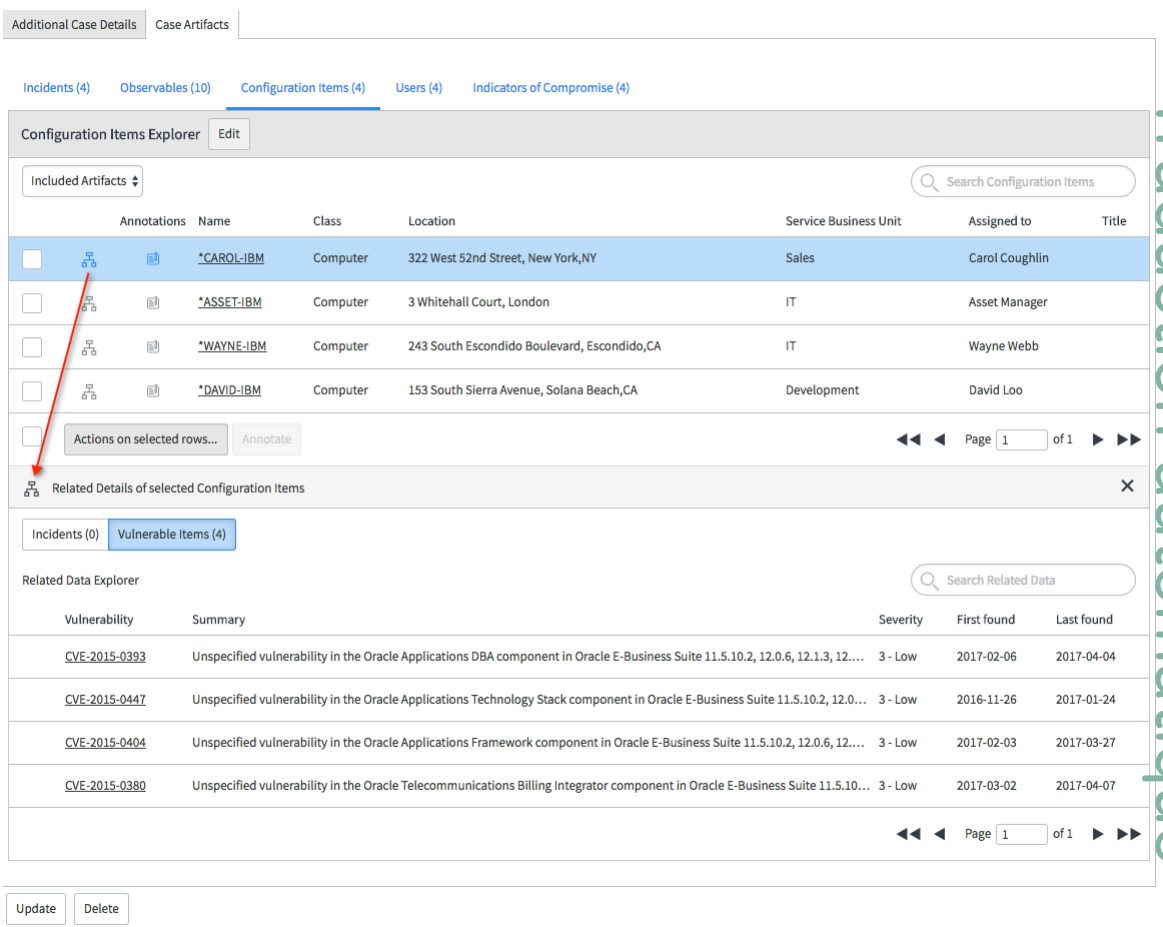
Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket contenant des artefacts de CI.
2. Cliquez sur l'onglet **Éléments de configuration** .
3. Cliquez sur Détails supplémentaires pour l'artefact CI pour lequel vous souhaitez afficher les détails connexes.



Traduction automatique

4. Cliquez sur l'un des onglets pour afficher des types spécifiques de détails relatifs à l'artefact sélectionné.
5. Vous pouvez également cliquer sur l'onglet **Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Afficher les détails connexes d'un artefact IoC

Si votre ticket comprend des artefacts d'indicateurs de compromission (IoC), vous pouvez afficher tous les détails connexes contenus dans chaque IoC référencé par le ticket.

Avant de commencer

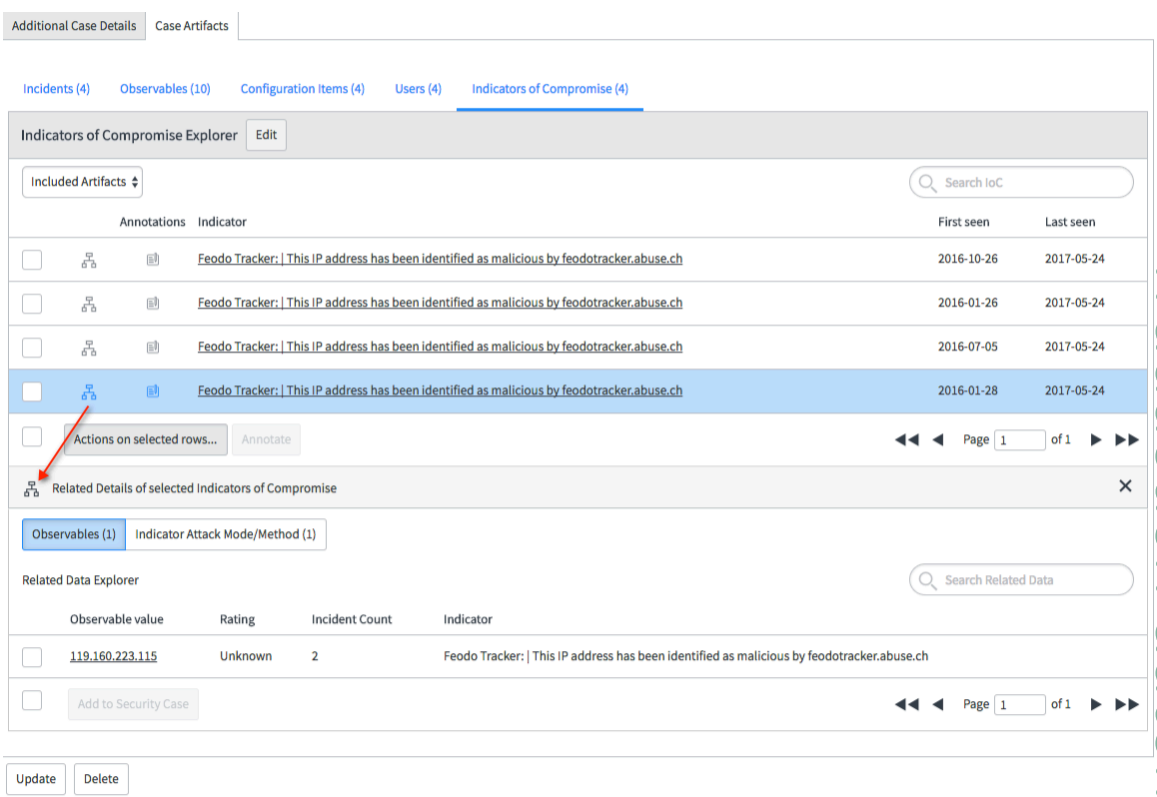
- Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket contenant des artefacts IoC.
2. Cliquez sur **l'onglet Indicateurs de compromission** .
3. Cliquez sur l'icône Détails supplémentaires pour l'artefact IoC pour lequel vous souhaitez afficher les détails connexes.



4. Cliquez sur l'un des onglets pour afficher des types spécifiques de détails relatifs à l'artefact sélectionné.
5. Vous pouvez également cliquer sur l'onglet **Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Afficher les détails connexes d'un artefact utilisateur affecté

Si votre ticket inclut des artefacts d'utilisateur affectés, vous pouvez afficher tous les détails connexes contenus dans chaque utilisateur affecté référencé par le ticket.

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

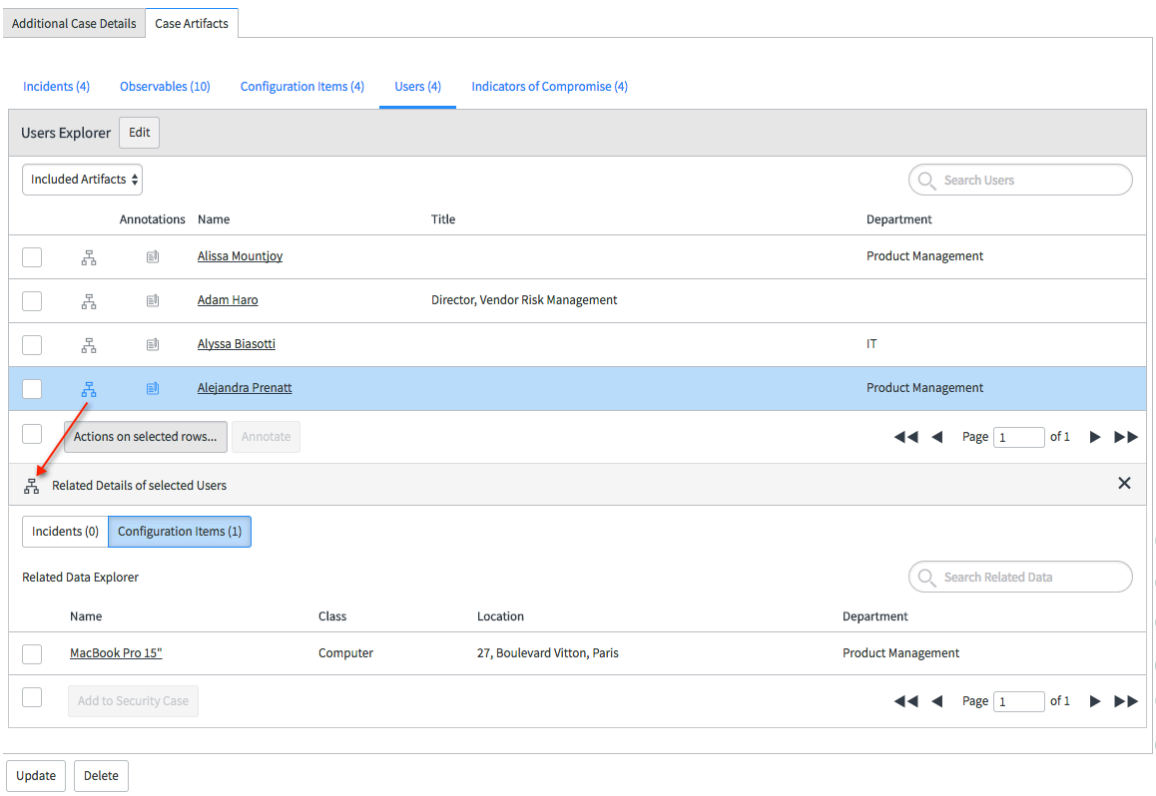
Procédure

1. Ouvrez un ticket contenant des artefacts utilisateur affectés.
2. Cliquez sur l'onglet **Utilisateurs** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur Détails connexes pour l'artefact de l'utilisateur affecté pour lequel vous souhaitez afficher les détails connexes.



4. Cliquez sur l'un des onglets pour afficher des types spécifiques de détails relatifs à l'artefact sélectionné.
5. Vous pouvez également cliquer sur l'onglet **Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Afficher les détails connexes d'un artefact observable

Si votre ticket inclut des artefacts observables, vous pouvez afficher tous les détails connexes contenus dans chaque observable référencé par le ticket.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

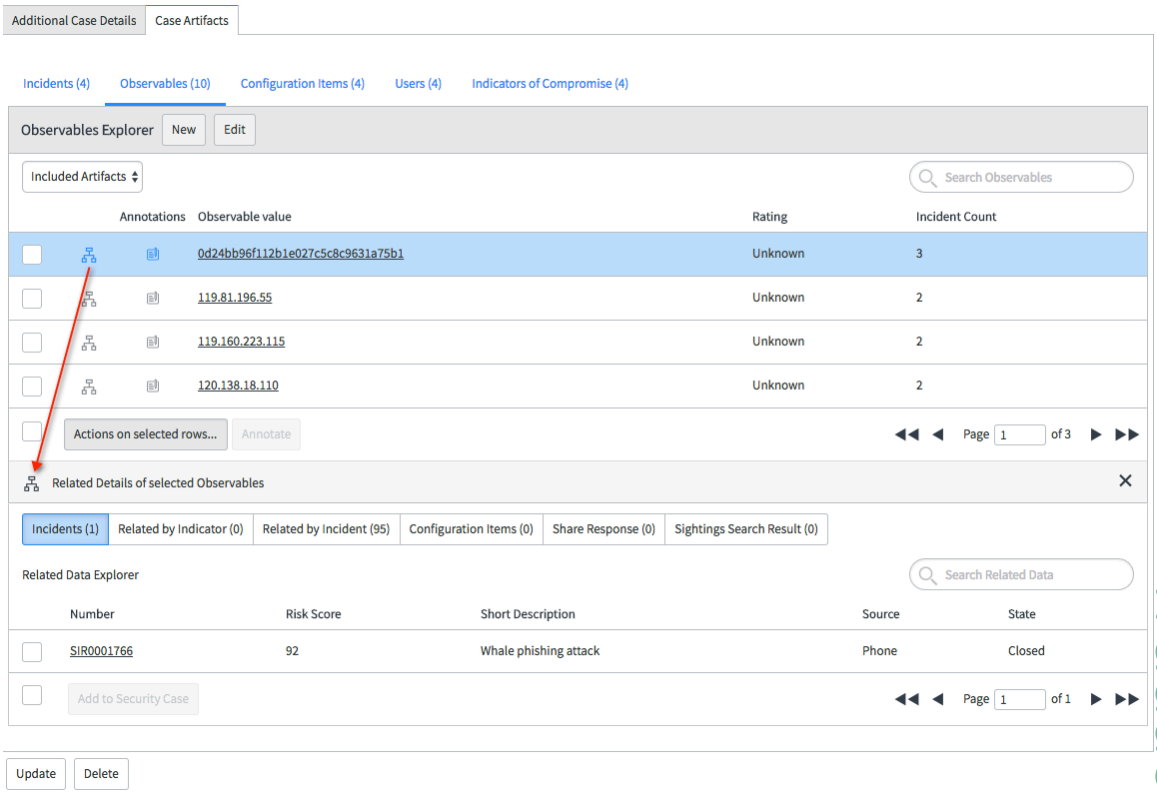
Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket contenant des artefacts observables.
2. Cliquez sur l'onglet **Observables** .
3. Cliquez sur l'icône Détails supplémentaires pour l'artefact observable pour lequel vous souhaitez afficher les détails connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur l'un des onglets pour afficher des types spécifiques de détails relatifs à l'artefact sélectionné.
5. Vous pouvez également cliquer sur l'onglet **Annotation de sécurité** pour afficher les annotations de l'artefact sélectionné.

Exclusion et inclusion des artefacts de sécurité

Les listes d'artefacts de prise en charge affectés à un ticket peuvent parfois être longues et il peut arriver que vous souhaitiez supprimer des artefacts particuliers d'une liste. Plutôt que de supprimer définitivement les artefacts, vous pouvez les exclure de la liste et, si nécessaire, les réintégrer ultérieurement à la liste.

Exclure les artefacts de sécurité d'un ticket

Vous pouvez supprimer des artefacts des listes d'artefacts de prise en charge. Ils ne sont pas retirés de façon permanente et peuvent être remis dans l'étui au besoin.

Avant de commencer

- Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

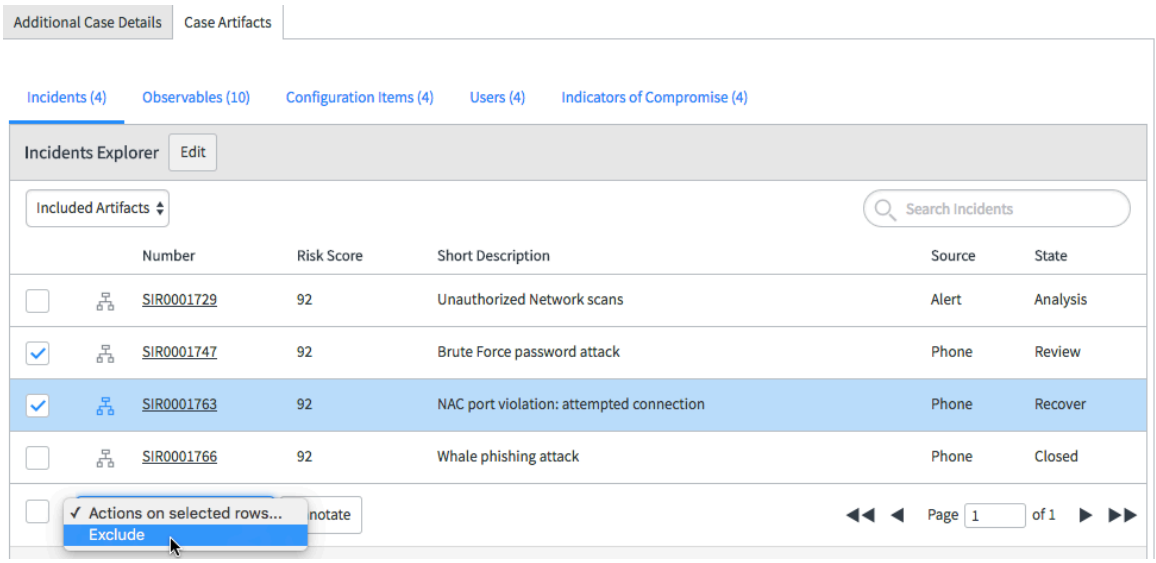
Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket qui contient des artefacts que vous souhaitez exclure d'une liste.
2. Cliquez sur la liste connexe **Artefacts de ticket** .
3. Cliquez sur l'onglet associé aux artefacts que vous souhaitez exclure.
   Par exemple, cliquez sur **Incidents** pour exclure les incidents de sécurité de la liste.
4. Sélectionnez un ou plusieurs enregistrements d'artefacts que vous souhaitez exclure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Exclure**.
6. Cliquez sur Exclure dans la zone **de** confirmation.
   Les artefacts sélectionnés sont supprimés de la liste.

Renvoyer les artefacts de sécurité exclus dans un ticket

Une fois que vous avez exclu les artefacts d'une liste dans un ticket, vous pouvez les renvoyer dans le ticket sur lequel vous pouvez continuer à travailler.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

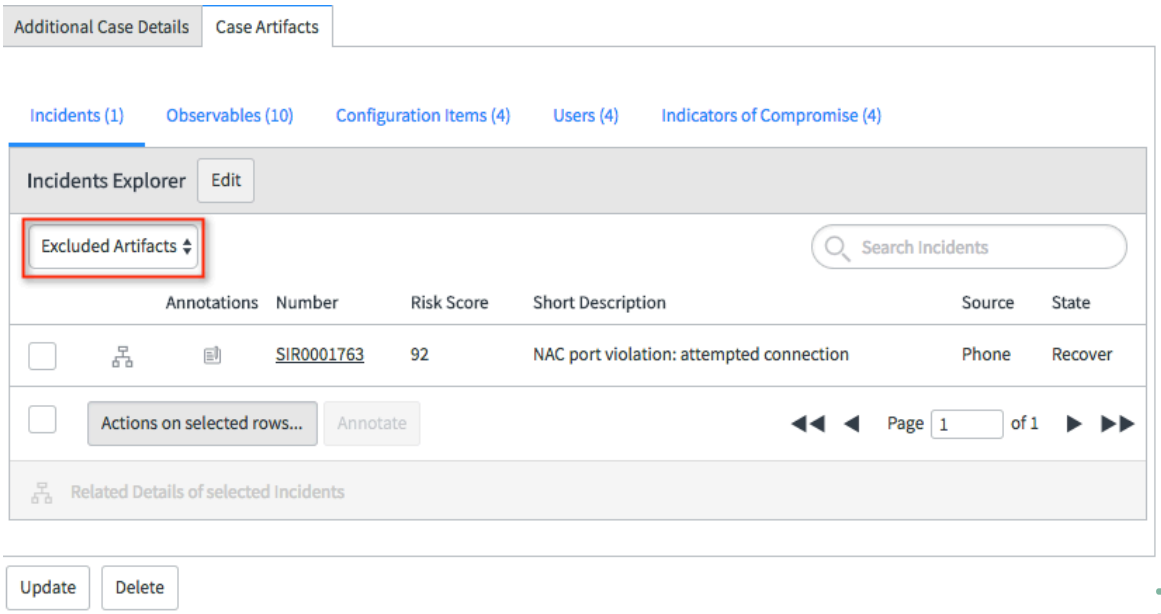
Rôle requis : sn_ti.case_user_write

Procédure

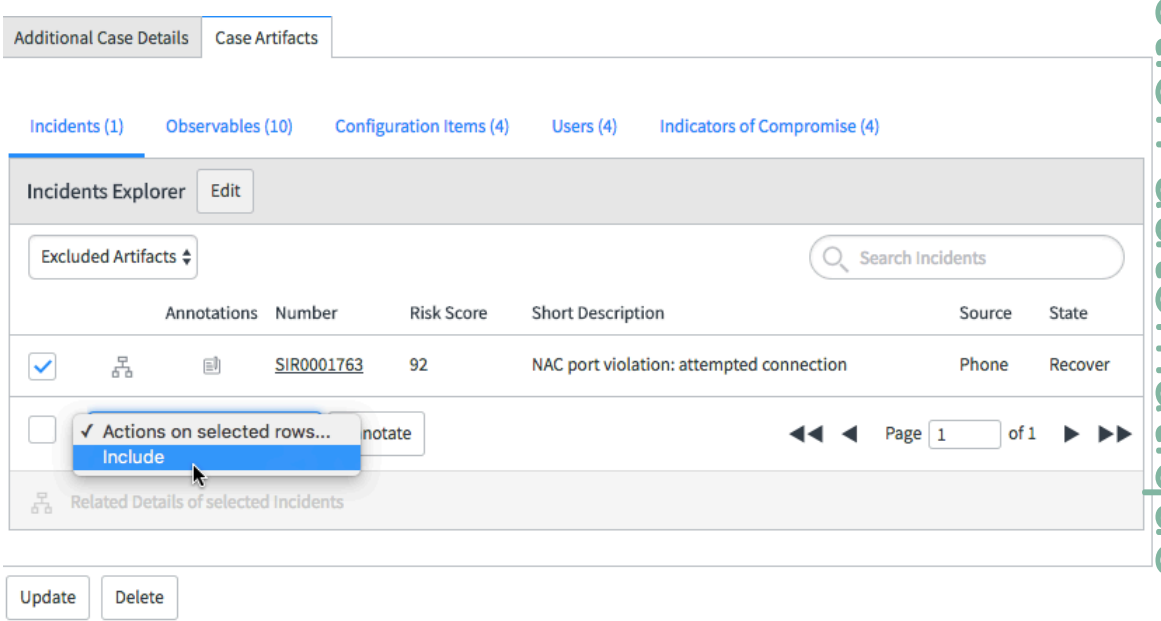
1. Ouvrez un ticket qui contient des artefacts que vous avez précédemment exclus d'une liste que vous souhaitez remettre dans la liste.
2. Cliquez sur la liste connexe **Artefacts de ticket** .
3. Cliquez sur l'onglet associé aux artefacts pour revenir à la liste.
4. Cliquez sur la liste déroulante Filtre d'artefact et sélectionnez **Artefacts exclus**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez un ou plusieurs enregistrements d'artefacts que vous souhaitez renvoyer à la liste Inclure.
6. Dans la liste déroulante **Actions sur les éléments sélectionnés** , sélectionnez **Inclure**.



7. Cliquez sur **Inclure** dans la zone de confirmation.
   Les artefacts sélectionnés sont retirés de la liste des artefacts exclus et renvoyés dans la liste des artefacts inclus dans le ticket.

Annoter les artefacts de sécurité

Lorsque vous analysez un ticket, vous pouvez ajouter des annotations à n'importe quel artefact.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis :

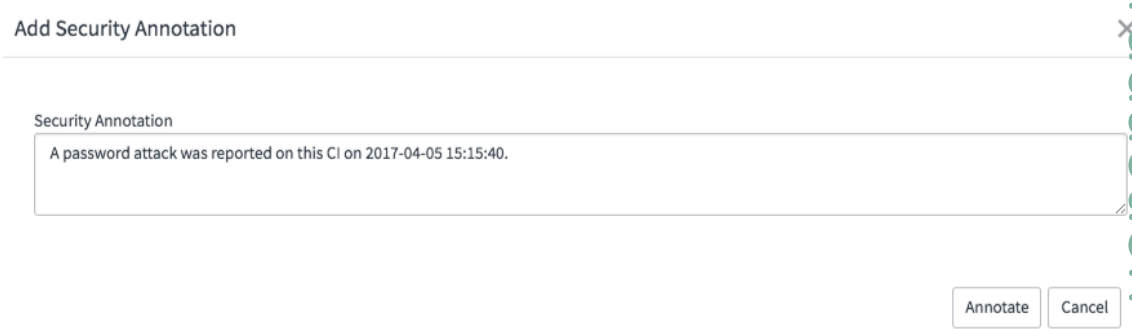
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_ti.case_user_write pour l'ajout d'annotations
- sn_ti.case_user_read pour afficher les annotations

Procédure

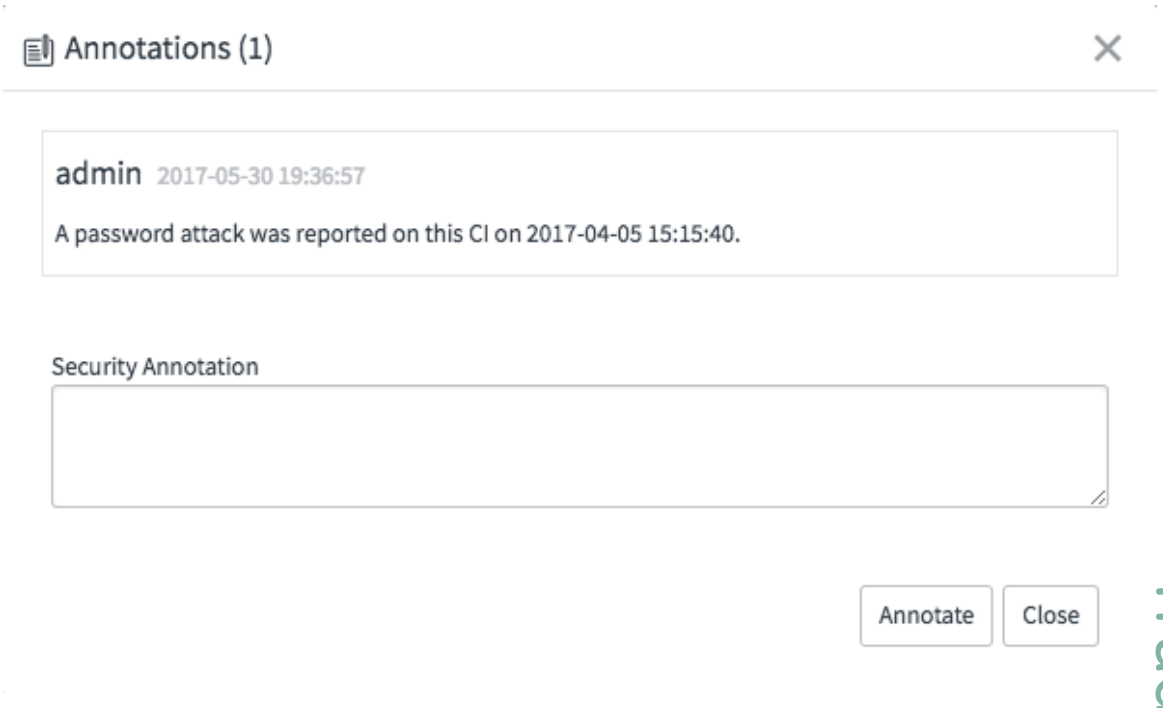
1. Ouvrez un ticket contenant des artefacts que vous souhaitez annoter.
2. Cliquez sur la liste connexe **Artefacts de ticket** .
3. Cliquez sur l'onglet associé aux artefacts que vous souhaitez annoter.
   Par exemple, cliquez sur **Indicateurs de compromis** pour ajouter des annotations aux IoC.
4. Pour ajouter une annotation à un ou plusieurs artefacts, procédez comme suit :
   a. Sélectionnez les artefacts auxquels vous souhaitez ajouter une annotation.
   b. Cliquez sur **Annoter**.



   c. Saisissez l'annotation et cliquez sur **Annoter**.
   L'annotation est ajoutée aux artefacts sélectionnés.
5. Pour afficher les annotations d'un artefact, cliquez sur l'icône Afficher les annotations ( ).
   Les annotations existantes apparaissent dans la boîte de dialogue Annotations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Vous pouvez également entrer une nouvelle annotation pour l'artefact dans la zone **Annotation de sécurité** et cliquer sur **Annoter**.

Rechercher des artefacts de sécurité

Vous pouvez effectuer une recherche par mot clé sur n'importe quelle liste d'artefacts de sécurité.

Avant de commencer

Le Renseignements sur les menaces module d'extension doit être activé pour être utilisé Gestion des tickets de sécurité.

Rôle requis : sn_ti.case_user_write

Procédure

1. Ouvrez un ticket contenant des artefacts de sécurité.
2. Cliquez sur l'onglet des artefacts de sécurité sur lesquels vous souhaitez effectuer une recherche par mot clé.
3. Dans la zone **de recherche Mot clé** , commencez à saisir le nom de l'artefact que vous souhaitez localiser. Lorsque des artefacts correspondant à votre entrée sont trouvés, ils sont affichés.

Contrôle de la posture de sécurité

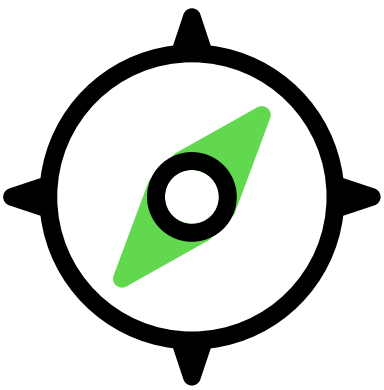
Gagnez en visibilité sur l'inventaire des actifs de votre entreprise et la couverture de vos outils de sécurité. Utilisez les politiques fournies avec le produit ou créez les vôtres pour identifier les actifs pour lesquels il manque des outils de sécurité clés, tels que la protection des points de terminaison, la gestion des configurations et l'analyse des vulnérabilités. Surveillez les actifs pour les configurations d'outils de sécurité spécifiques à votre environnement et automatisez le workflow de rattrapage des failles de sécurité dans l'application Conformité de la configuration .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

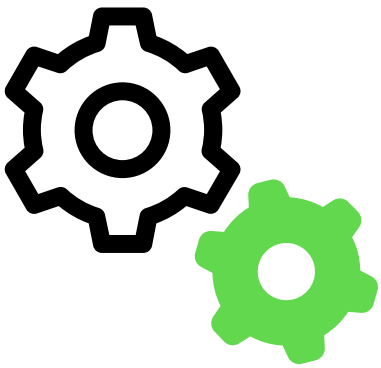
Premiers pas

Explorer



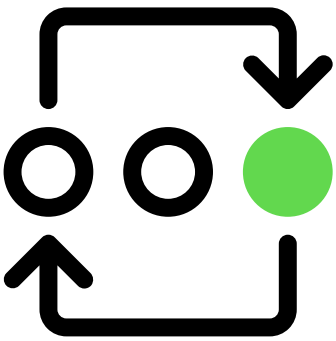
En savoir plus sur les concepts et les fonctionnalités de Security Posture Control

Installer



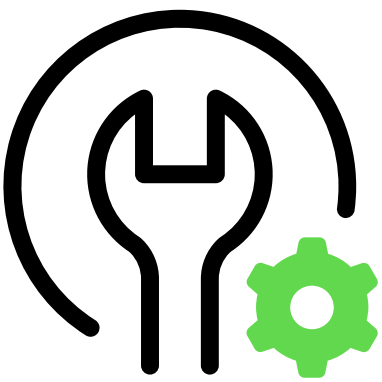
Installer les applications Contrôle de la posture de sécurité

Intégrer



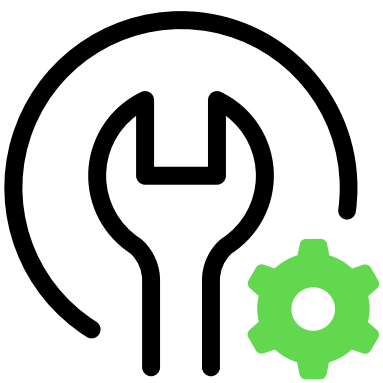
Intégrer Connecteurs du graphe de services au Contrôle de la posture de sécurité

Utiliser



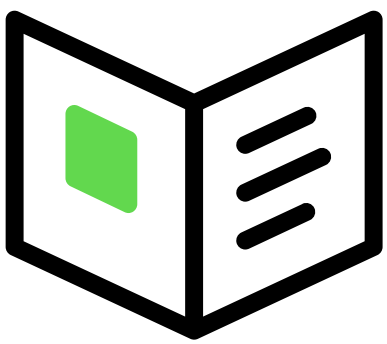
Découvrez comment utiliser l’espace de travail pour rechercher vos actifs et identifier les failles de sécurité

Atténuations Surveillance des contrôles



Découvrir quelles menaces pesant sur vos actifs sont atténuées par les contrôles d’atténuation disponibles

Référence



Obtenez des détails sur les scénarios qui vous aident à identifier des types spécifiques d’écarts de couverture d’outils. Consultez des exemples de politiques de base, enfant et clonées, et consultez une liste des connecteurs du graphe de services matériels et logiciels pris en charge.

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Explorer Contrôle de la posture de sécurité

Contrôle de la posture de sécurité permet aux équipes de cybersécurité d'obtenir une visibilité sur l'ensemble de leur inventaire d'actifs d'entreprise et de déterminer leur posture de sécurité globale.

Les analystes de sécurité obtiennent un aperçu de la façon dont les outils de sécurité sont déployés et couvrent leurs actifs en fonction de leur inventaire des actifs et des données importées à partir de connecteurs du graphe de services et de produits ServiceNow tels que Gestion des actifs matériels (HAM) et ITOM Discovery.

Les analystes de sécurité peuvent également créer des politiques personnalisées et configurer des aperçus pour surveiller la conformité des actifs aux normes de sécurité internes. Les gestionnaires de vulnérabilité peuvent utiliser les aperçus de Contrôle de la posture de sécurité (SPC) pour hiérarchiser le rattrapage des vulnérabilités sur les actifs à haut risque.

Le produit SPC est basé sur Cloud Security Posture Management (CSPM) et Cyber Asset Hygiene Management (CAHM). Contrôle de la posture de sécurité se compose de deux applications disponibles par abonnement distinct du ServiceNow® Store.

Version de mise en production	Notes de publication
Security Posture Control Core : v6.2, v6.1, v6.0.	Pour plus d'informations sur la compatibilité, consultez KB0856498 Changements de matrice de compatibilité et de schéma de mise en production de Vulnerability Response Notes de publication Contrôle de la posture de sécurité
Gestion de la posture de sécurité des actifs: v5.3, v5.1, v5.0	
Surveillance des contrôles d'atténuation v4.0, v3.0, v2.0	

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Avec le SPC produit, les équipes Info-Sec peuvent effectuer les tâches suivantes :

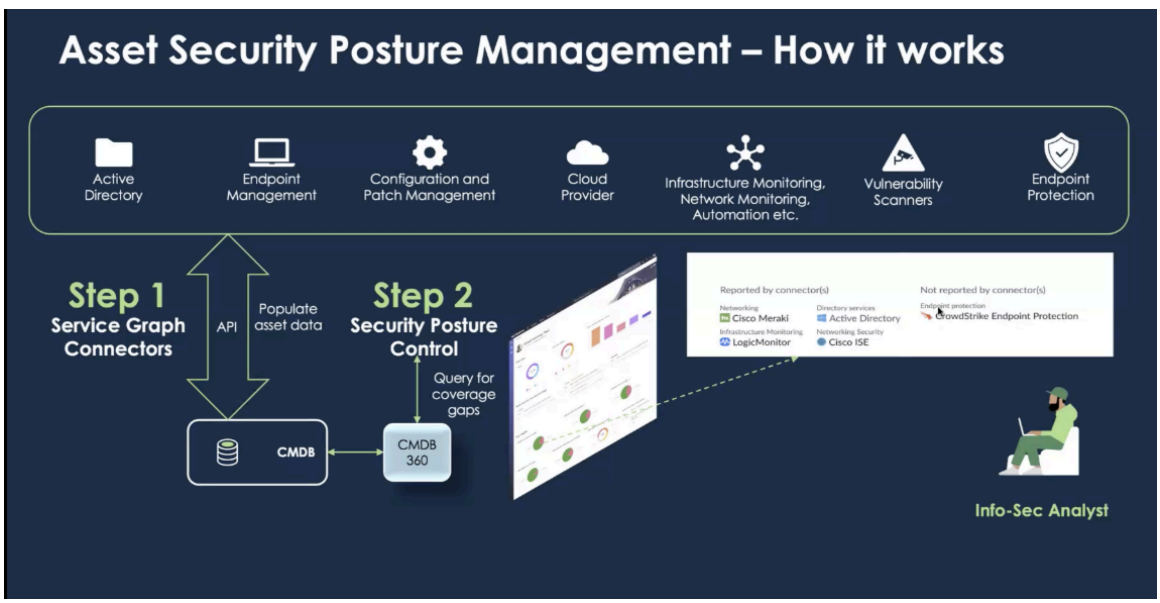
- Consultez des aperçus de la posture de sécurité pour vos actifs sur site et dans le cloud. SPC aide vos équipes de sécurité de l'information à identifier les actifs qui ne disposent pas d'une protection des points de terminaison, les actifs non gérés, les actifs exposés à Internet et toute combinaison à haut risque impliquant des vulnérabilités.
- Surveillez la conformité de vos actifs aux normes internes de configuration des outils de sécurité. Par exemple, assurez-vous que la dernière version d'un produit de protection des points de terminaison est utilisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Automatisez votre workflow de rattrapage des lacunes de posture de sécurité que vous trouvez avec l'application ServiceNow Configuration Compliance.
- Créez des politiques et des aperçus personnalisés basés sur les métadonnées des actifs, les données de couverture de l'outil de sécurité et les données de vulnérabilité.
- Découvrez quelles menaces pesant sur vos actifs sont atténuées par les contrôles d'atténuation disponibles, en fonction de la façon dont les différents outils de sécurité sont configurés avec la surveillance des contrôles d'atténuation.

Mode de fonctionnement de Gestion de la posture de sécurité des actifs



Gestion de la posture de sécurité des actifs (ASPM) identifie les lacunes de couverture des outils de sécurité dans les actifs à l'aide d'intégrations d'API avec divers outils tiers (connecteurs du graphe de services) ainsi qu'avec des produits ServiceNow.

ASPM s'appuie sur les données renseignées dans votre CMDB au sujet de vos actifs. Les données des actifs sont importées par différentes catégories d'outils de surveillance et comparées pour identifier toute faille de sécurité potentielle.

Par exemple, supposons que des données d'actif remplies dans la CMDB sont signalées par des outils qui couvrent les outils de surveillance de l'infrastructure et les outils de mise en réseau. Toutefois, ces données relatives à ces mêmes actifs ne sont pas renseignées ni signalées par les outils de protection des points de terminaison. Si vous comparez les données d'actif signalées par ces différents outils, vous pouvez voir qu'il existe des actifs sans agent de protection du point de terminaison.

Gestion de la posture de sécurité des actifs identifie les écarts de couverture des outils de sécurité dans les actifs à l'aide d'intégrations d'API avec divers outils (connecteurs du graphe de services) et produits ServiceNow. Les catégories comprennent, sans s'y limiter, les éléments suivants :

- Expérience numérique de l'employé
- Découverte
- Gestion des points de terminaison
- Gestion des actifs IT
- Surveillance de l'infrastructure

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Réseau
- Sécurité réseau
- Surveillance des performances du réseau
- Configuration et gestion des correctifs
- Protection du point de terminaison
- Fournisseur de cloud
- Surveillance de la performance des applications
- Services du répertoire
- Évaluation de la vulnérabilité

Le Contrôle de la posture de sécurité workflow

L'identification des lacunes des outils de Security implique les étapes suivantes :

1. Configurez et activez les connexions d'API avec l'un des outils que vous utilisez dans différentes catégories. Vous pouvez utiliser Service Graph Connector pour les produits disponibles dans le ServiceNow Store pour les connexions d'API requises. Pour plus d'informations sur les connecteurs du graphe de services pris en charge, reportez-vous à la section Connecteurs du graphe de services . Les connecteurs du graphe de services pris en charge sont disponibles auprès de avec ServiceNow® Store des abonnements distincts.
2. Activez les politiques expédiées avec l'application Contrôle de la posture de sécurité . Le Contrôle de la posture de sécurité produit détecte les lacunes de l'outil de Security en effectuant les tâches suivantes :
   a. Identifie la liste de tous les actifs uniques renseignés par divers connecteurs du graphe de services dans la CMDB.
   b. Identifie les actifs qui ne sont pas signalés par des catégories spécifiques à partir de cette réserve d'actifs (par exemple, Protection des points de terminaison). Les actifs sont identifiés en fonction de la politique active évaluée.
   c. Les actifs identifiés comme non signalés par des catégories spécifiques sont signalés comme « Constatations » ou « Résultats des tests » dans l'application Conformité de la configuration .
3. Affectez automatiquement des « résultats » à différentes équipes pour un rattrapage avec l'application Configuration Compliance.

Combinaisons à haut risque

Avec Gestion de la posture de sécurité des actifs, vous pouvez également identifier les actifs qui ont des combinaisons à haut risque. Un exemple de combinaison à haut risque peut montrer des actifs qui n'ont pas d'outils de sécurité, qui présentent des vulnérabilités critiques et qui sont exposés à Internet.

Certaines des politiques fournies avec l'application Contrôle de la posture de sécurité recherchent ces combinaisons à haut risque de vulnérabilités critiques et de lacunes dans la couverture des outils de sécurité. Toutefois, pour que ces stratégies de combinaison fonctionnent, vous devez avoir l'application Réponse aux vulnérabilités et au moins un produit d'intégration de scanner de vulnérabilité tel que Qualys, Rapid7 ou l'application Tenable Vulnerability Integration installée. Ces applications sont disponibles avec des abonnements distincts du ServiceNow Store.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Surveillance des contrôles d'atténuation

Depuis l'espace de travail (SPC), découvrez quelles menaces pesant sur vos actifs sont atténuées par les contrôles d'atténuation disponibles, en fonction de la Contrôle de la posture de sécurité configuration des différents outils de sécurité. Voir Surveillance des contrôles d'atténuation pour plus d'informations.

Installer les applications prises en charge pour Contrôle de la posture de sécurité

Les applications requises pour cette intégration sont disponibles sur le .ServiceNow Store Certaines applications ont des dépendances que vous devez télécharger et installer séparément.

Avant de commencer

Rôle requis : admin pour le téléchargement, l'installation et l'activation de toutes les applications.

Procédure

1. Téléchargez les applications requises à partir de dans ServiceNow Store votre ServiceNow instance.

   L'application Contrôle de la posture de sécurité (SPC Core) fournit le cadre de travail de base et est requise pour Gestion de la posture de sécurité des actifs (ASPM). L'application Conformité de la configuration et ses dépendances vous permettent de créer des tâches de rattrapage pour les failles de contrôle de sécurité que vous constatez à l'aide Gestion de la posture de sécurité des actifs de .

Applications Gestion de la posture de sécurité des actifs

Application	ID d'application
Gestion de la posture de sécurité des actifs	(ID de module d'extension : sn_sec_caasm)
Licence Découverte ITOM	(ID du module d'extension : com.snc.itom.discovery.license)
Base pour le contrôle de la posture de sécurité	(ID de module d'extension : sn_sec_spc_core)
Surveillance des contrôles d'atténuation	(ID de module d'extension : sn_sec_mit_ctr)
Configuration Compliance (inclut l'application enfant secops_shared_components)	(ID de module d'extension : sn_vulc)
Gestion des licences et utilisation de Vulnerability Response	(ID de module d'extension : sn_vul_licensing)

Applications Gestion de posture de sécurité cloud

Application	ID d'application
Module d'extension Discovery	(ID de module d'extension : com.snc.discovery)
Cloud Configuration Governance	(ID de module d'extension : sn_itom_ccg)
Pack de contenu CCG	(ID de module d'extension : sn_itom_ccg_cp)
CMDB CI Class Models	(ID de module d'extension : sn_cmdb_ci_class)
Bibliothèque d'actions dans le cloud	(ID du module d'extension : com.sn.itom.cal)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur le téléchargement et l'activation des applications, consultez les rubriques suivantes :

- Télécharger une application à partir de ServiceNow Store pour la première fois.
- Activer une ServiceNow Store application.

2. Une fois les applications téléchargées, accédez à **Tous** > **Applications système** > **Toutes les applications disponibles** > **Tous**.
3. Localisez les applications que vous avez téléchargées et sélectionnez **Installer** pour les activer ainsi que leurs dépendances.
   Toutes les applications dépendantes qui sont également installées automatiquement en même temps qu'une application s'affichent dans la boîte de dialogue d'installation de l'application. Toutefois, si vous êtes invité à installer des modules d'extension de dépendance pendant l'installation, suivez les invites fournies. Vérifiez que toutes les applications et dépendances répertoriées dans la table précédente sont installées et activées.

   Une boîte de dialogue s'affiche après l'activation réussie d'une application.

   Pour plus d'informations sur le téléchargement et l'installation d'applications à partir de :ServiceNow Store

   - Pour vous abonner aux ServiceNow produits, suivez les étapes de la section S'abonner auxServiceNow Store produits .
   - Pour installer une application que vous avez achetée à partir du , suivez les étapes de la ServiceNow Store section Installer une ServiceNow Store application .
   - Si vous souhaitez également gérer votre autorisation pour les applications sur d'autres ServiceNow AI Platform instances, procédez comme suit Gérer les autorisations de votre ServiceNow instance dans .
4. Après avoir installé et activé les applications, affectez les utilisateurs aux groupes Contrôle de la posture de sécurité suivants :

   Ces groupes héritent de tous les rôles nécessaires pour lire et modifier les enregistrements SPC.

   Groupe d'administrateurs SPC

   Les utilisateurs de ce groupe disposent d'un accès complet en lecture et en écriture à tous les enregistrements du produit, y compris les informations de gestion des licences. Les rôles granulaires de ce groupe comprennent : [sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin et sn_sec_spc_core.configure].

   Groupe d'analystes SPC

   Les utilisateurs de ce groupe disposent d'un accès complet en lecture et en écriture à tous les enregistrements du produit, mais ne peuvent pas afficher les informations de gestion des licences. Les rôles granulaires de ce groupe comprennent [pa_power_user et sn_sec_spc_core.analyst].

   Groupe en lecture seule d'analyste SPC

   Les utilisateurs de ce groupe disposent d'un accès en lecture complet à tous les enregistrements du produit, mais ne peuvent pas afficher les informations de gestion des licences. Les rôles granulaires de ce groupe comprennent [pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read et cmdb_ms_user].

   Rôles de l'application de soutien

   Les rôles suivants sont requis par les applications répertoriées dans le tableau précédent qui prennent en charge SPC et Gestion de la posture de sécurité des actifs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Conformité de la configuration Administrateur [sn_vulc.admin] : configure l'application, a une visibilité sur tous les enregistrements et peut modifier les Conformité de la configuration propriétés. Affecte des rôles dans l'application Conformité de la configuration .
- Réponse aux vulnérabilités Administrateur [sn_vulc.admin] : configure l'application Vulnerability Response et les calculateurs de risque de vulnérabilité.
- Serveur MID [mid_server] : configure un Serveur MID.

5. **Facultatif :** Définissez la propriété système **ignoreCIClass** [sn_sec_cmn.ignoreCIClass] pour ignorer certaines classes d'éléments de configuration (CI) lors de l'exécution de règles de recherche de CI.

   (Optional) En tant qu'administrateur SPC et analyste SPC, vous devrez peut-être ignorer certaines classes matérielles ou virtuelles afin de ne pas ingérer d'informations sur des actifs que vous ne souhaitez pas contrôler. Voir Créer une règle de recherche de CI de réponse aux vulnérabilités et Ignorer les classes CI pour plus d'informations.

6. Modifiez les sources de données CMDB de réconciliation et recalculez pour définir la source de vérité pour les valeurs d'attribut.

   Le tableau de bord CMDB 360 fournit des agrégations et une analyse des données CMDB 360. CMDB 360 collecte des données sur toutes les sources de découverte générant des rapports sur les valeurs d'attribut pour les CI. Utilisez la vue CMDB 360 dans l'espace de travail CMDB (Configuration Management Database) pour suivre les activités et identifier les problèmes potentiels des sources de découverte. Consultez Vue CMDB 360 dans l'espace de travail CMDB pour plus d'informations.

Connecteurs du graphe de services pour Contrôle de la posture de sécurité

Contrôle de la posture de sécurité s'appuie sur les intégrations d'API ou les connecteurs du graphe de services comme source clé pour les données d'actif utilisées pour identifier les failles de sécurité.

Contrôle de la posture de sécurité prend actuellement en charge les connecteurs du graphe de services (SGC), qui peuvent vous fournir une grande variété de données sur vos actifs. Ces applications d'intégration sont disponibles à partir du ServiceNow Store.

Choisissez les connecteurs que vous souhaitez utiliser et téléchargez les applications, puis activez-les. La liste des connecteurs pris en charge dans le magasin s'allonge à mesure que Contrôle de la posture de sécurité d'autres connecteurs sont pris en charge.

Pour profiter pleinement des Contrôle de la posture de sécurité fonctionnalités, vous pouvez télécharger et activer les produits Connecteur du graphe de services suivants pour prendre en charge les catégories énumérées ci-dessous.

Les connecteurs du graphe de services pris en charge par Contrôle de la posture de sécurité comprennent actuellement les catégories suivantes :

- Expérience numérique de l'employé
- Découverte
- Endpoint Management : Microsoft Intune ou Jamf Device and Endpoint Management.
- Gestion des actifs IT
- Surveillance de l'infrastructure

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Réseau
- Sécurité réseau
- Surveillance des performances du réseau
- Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.
- Endpoint Protection : CrowdStrike ou SentinelOne.
- Fournisseur cloud : Amazon AWS Cloud, Microsoft Azure, GCP.

> **Remarque :** Si Découverte dans le cloud est activé, ces produits Service Graph Connector ne sont pas requis.

- Surveillance de la performance des applications
- Services du répertoire (Active Directory) Microsoft Active Directory
- Évaluation de la vulnérabilité : Qualys, Rapid7 ou Tenable.

Après les avoir installés, vous pouvez afficher les connecteurs et leurs catégories sur la table des connecteurs [sn_sec_spc_core_connector] de votre instance.

Vous pouvez afficher les types d'actifs et la façon dont ils sont mappés aux classes CI et aux connecteurs dans la table [sn_sec_spc_core_asset_type_connector].

Voir Connecteurs du graphe de services matériels pris en charge pour Contrôle de la posture de sécurité et Connecteurs du graphe de services logiciels pris en charge pour Contrôle de la posture de sécurité pour plus d'informations et d'exemples de ces tableaux. Bien qu'il ne s'agisse pas de listes exhaustives, vous pouvez voir comment les connecteurs pris en charge fournissent une grande variété de données.

Contrôle de la posture de sécurité prend en charge les produits ServiceNow tels que Gestion des actifs logiciels (SAM) et Gestion des actifs matériels (HAM) que vous pouvez utiliser avec les connecteurs du graphe de services pour vous aider à rechercher toute discordance entre le logiciel installé signalé par vos produits de scanner de vulnérabilité et le logiciel signalé par les scanners qui est déjà pris en compte dans SAM et d'autres produits ServiceNow.

Pour plus d'informations sur le téléchargement, la configuration et l'activation des applications prises en charge pour Connecteur du graphe de services, consultez les rubriques suivantes :

- Connecteurs du graphe de services .
- Télécharger une application à partir de ServiceNow Store pour la première fois.
- Activer une ServiceNow Store application.

Politiques pour Contrôle de la posture de sécurité

Les politiques auditent vos actifs en fonction des données importées de vos connecteurs du graphe de services pour vous aider à identifier les violations potentielles.

Politiques

Contrôle de la posture de sécurité Les politiques sont basées sur un modèle de données Actif-Relations-Propriétés. Certaines politiques sont incluses dans l'application. Vous pouvez créer vos propres politiques pour rechercher des critères spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les critères des politiques peuvent être spécifiés sous la forme de conditions portant sur les propriétés de cet actif ou sur les propriétés d'une entité connexe. Dans le créateur de politique du module Politique et résultats de l'espace de travail, vous pouvez définir des politiques pour rechercher un type d'actif (matériel, logiciel) et une connexion (signalé par, non signalé par) ou une entité (source d'actif, produit Service Graph Connector ou métadonnées CMDB), ou vous pouvez faire correspondre d'autres types de critères spécifiques.

Pour vous aider à modifier ou à créer des politiques :

- Définissez vos conditions dans le module Recherche d'actifs et recherchez des actifs par produits Service Graph Connector spécifiques ou par des actifs dont des données spécifiques sont signalées par un connecteur. Vous pouvez enregistrer vos recherches en tant que politiques.
- Clonez les politiques incluses dans l'application pour créer des stratégies plus étendues. Vous copiez puis affinez les conditions d'une politique existante sans avoir à les saisir à nouveau.
- Créez de nouvelles politiques (politiques enfants) à l'aide des politiques de base que vous sélectionnez comme point de départ pour les nouvelles politiques.

Types d'actifs et politiques

Vous utilisez ces types d'actifs de niveau primaire ou supérieur comme point de départ pour définir des politiques.

Actif matériel

L'actif matériel est une abstraction qui représente tout appareil qui comprend des appareils informatiques personnels, des serveurs, des appareils réseau, des ordinateurs virtuels dans le cloud et d'autres matériels. Les politiques auditent vos actifs pour détecter les violations potentielles en fonction des données importées des produits Service Graph Connector et ServiceNow® des produits tels que Software Asset Management (SAM) et ITOM Discovery.

Actifs Logiciels

L'actif logiciel vous permet de rechercher toutes les divergences qui existent entre les logiciels installés signalés par les données importées de Connecteur du graphe de services, vos produits de scanner de vulnérabilité et le logiciel signalé par les scanners qui est déjà pris en compte dans Gestion des actifs logiciels (SAM) et d'autres produits ServiceNow.

Les entités et leurs relations avec les entités secondaires

Entité	Relation	Entité cible	Description
Actif matériel	Reporté par	Source d'actif	Représente une source qui a signalé cet actif dans la CMDB.
Actif matériel	Signalé uniquement par	Source d'actif	Représente la seule source générant des rapports sur cet actif dans la CMDB.
Actif matériel	Non signalé par	Source d'actif	Représente une source qui n'a pas signalé cet actif dans la CMDB.
Actif matériel	Avec exception IRM	IRM Exception	Représente un enregistrement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les entités et leurs relations avec les entités secondaires (suite)

Entité	Relation	Entité cible	Description
			d'exception dans Gestion intégrée des risques.
Actif matériel	Avec vulnérabilité	Vulnérabilité	Représente une vulnérabilité trouvée sur cet actif.
Actif matériel	A un résultat de configuration	Configuration	Représente un problème de configuration et de conformité trouvé sur cet actif.
Actif matériel	Avec métadonnées CMDB	Métadonnées CMDB	Représente la collection des propriétés de CI CMDB sur cet actif.
Actif matériel	Avec les données du connecteur	Connecteur du graphe de services	Représente la collection de propriétés signalées par le connecteur du graphe de services sélectionné pour cet actif.
Actif matériel	Avec données agrégées	Données agrégées	Collection de propriétés avec des valeurs agrégées signalées par différentes sources pour un actif donné. Un exemple est le système d'exploitation.
Actif matériel	À partir de la classe CI	Classe CI CMDB	Utilisé pour définir des conditions sur des propriétés de classe CI spécifiques.
Actif matériel	A des métadonnées dans le cloud	Métadonnées dans le cloud	Représente les métadonnées dans le cloud (applicables aux ordinateurs virtuels dans le cloud).
Actif matériel	A un port exposé à Internet	Port ouvert	Représente un port ouvert sur Internet (applicable aux ordinateurs virtuels dans le cloud).
Logiciel	Reporté par	Source d'actif	Représente une source qui a signalé ce logiciel.
Logiciel	Signalé uniquement par	Source d'actif	Représente la seule source générant des rapports sur ce logiciel.
Logiciel	Non signalé par	Source d'actif	Représente une source qui n'a pas signalé ce logiciel.
Logiciel	Avec détails du logiciel	Logiciel	Représente l'ensemble des propriétés logicielles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les entités et leurs relations avec les entités secondaires (suite)

Entité	Relation	Entité cible	Description
			telles que l'éditeur et la version, par exemple.

Exemple d'audit de politique et de remplissage de données : classes CI dans la CMDB

Si une politique tente de récupérer une classe d'actifs signalée ou non par un connecteur du graphe de services spécifique, Contrôle de la posture de sécurité mappe toutes les classes d'éléments de configuration (CI) pertinentes qui sont associées à cette classe d'actifs dans la CMDB, renseignées ou non par ce connecteur du graphe de services ou cette catégorie de connecteur.

Par exemple, supposons qu'une politique recherche tous les actifs matériels signalés par le connecteur du graphe de services Jamf Pro. La logique suivante s'applique.

1. Contrôle de la posture de sécurité identifie quelles classes CI dans la CMDB sont mappées à la classe « Actif matériel » pour Jamf Pro.

   Remarque : Différents connecteurs du graphe de services renseignent différentes classes CI dans la CMDB, et le mappage aux classes CI à partir de « Actif matériel » varie d'un connecteur du graphe de services à l'autre.

2. Contrôle de la posture de sécurité détermine que les classes CI, l'ordinateur, le serveur et l'imprimante dans la CMDB sont mappés à la classe d'actifs « Actif matériel » pour le Jamf Pro de Connecteur du graphe de services.
3. Contrôle de la posture de sécurité interroge ensuite tous les enregistrements d'actifs renseignés dans l'une de ces trois classes de CI : Serveur, Ordinateur et Imprimante par le connecteur du graphe de services Jamf Pro dans la CMDB et renvoie ces actifs.

   La colonne « Classes CI prises en charge par SPC » dans la table suivante indique quelles classes d'enregistrements CI sont prises en compte lors d'une requête par le produit Contrôle de la posture de sécurité dans le cadre d'une évaluation de politique. Cette table n'est pas une liste exhaustive, mais vous pouvez l'utiliser pour voir comment les données ingérées provenant de différentes catégories et sources sont généralement mappées et interrogées.

Politiques incluses dans l'application

Activez les profils d'actifs et les politiques dans l'espace de Contrôle de la posture de sécurité travail qui sont inclus dans l'application afin de pouvoir identifier les lacunes dans la configuration ou la couverture des outils de sécurité.

Création de vos propres politiques

Consultez la rubrique Création de vos propres politiques dans l'application Contrôle de la posture de sécurité pour plus d'informations sur la création de vos propres stratégies.

Pour obtenir des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfant et clonées pour Contrôle de la posture de sécurité.

Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes requises pour créer une politique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

SGC pris en charge

Pour obtenir la liste de certains des connecteurs du graphe de services pris en charge, consultez Connecteurs du graphe de services matériels pris en charge pour Contrôle de la posture de sécurité et Connecteurs du graphe de services logiciels pris en charge pour Contrôle de la posture de sécurité.

Politiques de contrôles d'atténuation

Depuis l'espace de travail (SPC), découvrez quelles menaces pesant sur vos actifs sont atténuées par les contrôles d'atténuation disponibles, en fonction de la Contrôle de la posture de sécurité configuration des différents outils de sécurité. Consultez Politiques de contrôles d'atténuation pour plus d'informations.

Politiques incluses dans l'application Contrôle de la posture de sécurité

Quelques politiques incluses dans l'application sont liées à des Contrôle de la posture de sécurité cas d'utilisation importants et sont finalement affichées comme des aperçus clés sur le tableau de bord sur la page de destination (module d'accueil) de l'espace SPC de travail.

Affichage des politiques

Pour afficher ces politiques, accédez à **Espaces de travail** > **Contrôle de la posture de sécurité** > **Politiques et résultats** > **Tous**.

Ces politiques sont désactivées par défaut. Vous devez les activer avant de pouvoir afficher les résultats renvoyés (résultats). Vous ne pouvez pas modifier ces stratégies, mais vous pouvez les utiliser pour vous aider à créer d'autres stratégies en clonant leurs conditions comme point de départ. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité pour plus d'informations.

Vous pouvez cloner ces politiques pour créer vos propres politiques personnalisées, mais notez que les politiques que vous clonez ne sont pas reflétées en tant qu'aperçus clés sur le tableau de bord de la page de destination d'accueil avec les aperçus clés inclus avec l'application. Toutefois, vous pouvez configurer les résultats pour ces stratégies clonées et afficher les résultats renvoyés par ces stratégies.

Vous pouvez configurer des aperçus ou des rapports personnalisés pour les politiques clonées, ou configurer les résultats de ces politiques clonées afin de gérer le rattrapage. Vous pouvez également créer vos propres politiques personnalisées à partir de zéro pour surveiller la couverture des contrôles de sécurité en fonction de vos besoins internes.

Les politiques expédiées avec l'application comprennent les catégories suivantes :

- Politiques qui surveillent la couverture des contrôles de sécurité (protection des points de terminaison et scanner de vulnérabilité).
- Politiques qui identifient les appareils non gérés.
- Politiques qui surveillent les combinaisons toxiques impliquant des combinaisons critiques telles que l'absence de contrôles de sécurité, l'exposition à Internet, etc.
- Politiques pour SPC les intégrations d'API pour la surveillance des contrôles d'atténuation.

Après avoir cloné et activé toutes les politiques que vous créez, vous devez créer votre propre enregistrement d'aperçu personnalisé dans le module Générateur d'aperçus personnalisés de l'espace de travail (le dernier module du panneau de navigation). Ce n'est qu'alors que vous pouvez afficher les données de vos politiques sur le tableau de bord Aperçus personnalisés (la deuxième icône en partant du haut de l'espace de travail).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politiques et profils d'actifs inclus avec l'application

Obtenez un aperçu de votre posture de sécurité globale et des lacunes de configuration de vos outils de sécurité à l'aide des politiques et des profils d'actifs inclus dans l'application. Activez ces profils d'actifs et politiques dans l'espace de travail afin de pouvoir identifier les lacunes dans la Contrôle de la posture de sécurité configuration ou la couverture des outils suivants :

- CrowdStrike
- Microsoft Intune, Defender et SCCM
- Gros correctif HCL
- Qualys
- Rapid7

Création de vos propres politiques

Consultez la rubrique Création de vos propres politiques dans l'application Contrôle de la posture de sécurité pour plus d'informations sur la création de vos propres stratégies.

Pour obtenir des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfant et clonées pour Contrôle de la posture de sécurité.

Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes requises pour créer une politique.

Pour plus d'informations sur les politiques utilisées pour la surveillance des contrôles d'atténuation, reportez-vous à la section Politiques de contrôles d'atténuation pour en savoir plus.

Création de vos propres politiques dans l'application Contrôle de la posture de sécurité

Vous pouvez créer vos propres politiques personnalisées pour surveiller les données spécifiques aux ressources de votre environnement. Vous basez ces politiques sur les données que vous importerez à partir des différents connecteurs du graphe de services que vous avez installés et activés.

Comment commencer

Vous pouvez cloner les politiques existantes et y ajouter d'autres conditions ou créer une politique à partir de zéro. Pour vos politiques personnalisées, vous pouvez inclure des critères pour les propriétés CMDB communes renseignées par divers connecteurs du graphe de services.

Vous pouvez également utiliser une politique de base comme point de départ et inclure des conditions pour les exceptions approuvées avec des politiques pour l'application Gouvernance, risque et conformité (GRC), par exemple. Ces exceptions concernent les actifs que vous ne souhaitez pas surveiller et inclure dans vos nombres d'actifs.

Pour vos stratégies personnalisées, vous pouvez inclure des conditions pour les métadonnées telles que le système d'exploitation, la version du système d'exploitation et le nom de domaine complet, par exemple pour vous aider à surveiller les actifs dotés de logiciels plus anciens. Notez que ces propriétés sont des propriétés CMDB communes renseignées par divers connecteurs du graphe de services pour un actif donné.

Consultez Politiques incluses dans l'application Contrôle de la posture de sécurité pour plus d'informations sur les types d'actifs de niveau supérieur et leurs relations dans les politiques du créateur de conditions de politique pour vous.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour obtenir des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfant et clonées pour Contrôle de la posture de sécurité.

Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes requises pour créer une politique.

Utilisation des décorateurs AND, OR dans le générateur de conditions

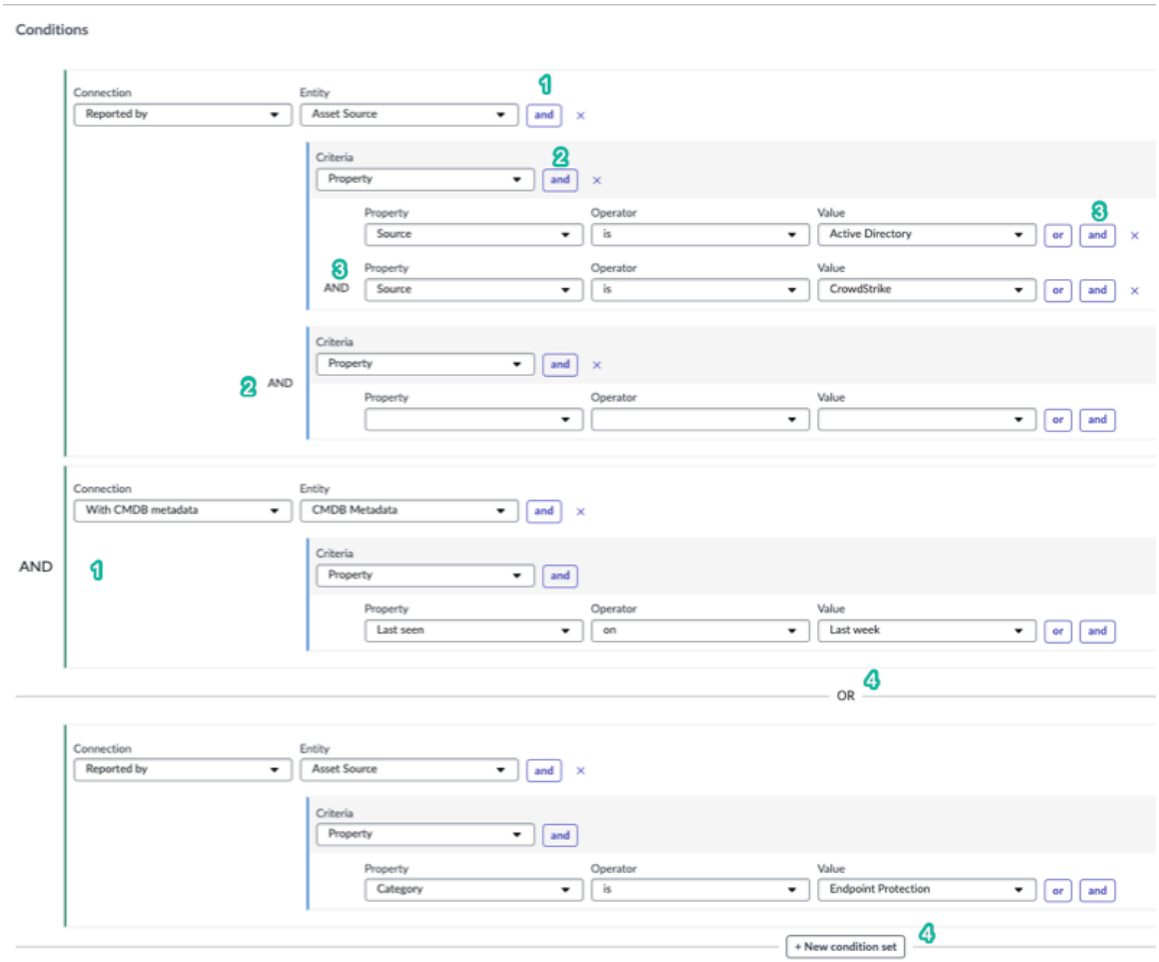
Vous naviguez des types d'actifs de niveau supérieur pour le matériel et les logiciels vers leurs entités secondaires à l'aide du générateur de conditions du module Politiques et résultats de l'espace de travail. En fonction de vos choix, des champs s'affichent pour vous et vous modifiez ou ajoutez des critères.

Les décorateurs AND, OR du générateur de conditions vous permettent de configurer la logique pour les données renvoyées que vous souhaitez renvoyer pour la politique.

Décorateur	Description	Numéro référencé dans l'image
Sélectionnez **ET** à côté des champs Connexion et Entité en haut pour le nouvel ensemble de conditions.	Ajoute un ET logique entre les critères d'entité de connexion actuels et de nouveaux critères d'une autre entité de connexion.	1
Sélectionnez **ET** à droite d'un champ Critère ou Propriété pour un nouvel ensemble de critères et de conditions de propriété.	Ajoute un ET logique entre les critères d'entité de connexion actuels et un nouveau critère sous la même entité de connexion.	2
Sélectionnez **OU/ET** à droite d'un champ de propriété pour le nouvel ensemble de conditions de propriété.	Ajoute un OU/ET logique entre la propriété actuelle et une nouvelle propriété des mêmes critères de connexion-entité.	3
Sélectionnez **+ Nouvel ensemble de conditions** pour un nouvel ensemble de conditions.	Ajoute un OU logique entre l'ensemble de conditions de tous les critères actuels et un nouvel ensemble de conditions.	4

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Utilisation des politiques de base, du clonage et des politiques enfants

Vous pouvez utiliser plusieurs politiques pour évaluer vos actifs et créer vos propres aperçus personnalisés. Vous disposez des options suivantes pour vous aider à créer des politiques personnalisées ou modifier rapidement des politiques existantes :

- Cloner la politique : créer une copie d'une politique. Le nom de la politique et ses conditions sont affichés avec une « copie » dans le titre. Les conditions s'affichent et vous pouvez les modifier. Consultez Modifier une politique activée dans Contrôle de la posture de sécurité.
- Créer une politique enfant : le nom de la politique à partir de laquelle vous avez commencé s'affiche sous la forme « Politique de base » dans le nouvel enregistrement. Les conditions de votre politique de base sont héritées dans la nouvelle politique et un nouvel ensemble de conditions vide s'affiche. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité.
- Politiques d'exclusion : ajoutez des politiques à vos politiques personnalisées afin que les résultats relatifs aux actifs des politiques que vous sélectionnez soient exclus de vos résultats. Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité.

Métadonnées et filtrage CMDB

Il peut être important pour vos équipes de sécurité de surveiller les actifs dotés de logiciels plus anciens. Vous pouvez spécifier des critères de politique commençant par la connexion « Avec métadonnées CMDB » après le type d'actif matériel pour inclure les propriétés communes énumérées ci-dessous. Il ne s'agit pas d'une liste exhaustive. Afin de collecter ces métadonnées, les propriétés doivent être disponibles à partir de la connexion de métadonnées CMDB renseignée par vos connecteurs du graphe de services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- RAM
- Nom d'hôte
- Numéro de série
- Domaine SE
- Version de SE
- Espace disque
- Dernier observé
- Systèmes d'exploitation
- Premier observé
- Nombre de processeurs
- Fabricant de MAC
- Carte réseau
- Adresse IP
- Emplacement
- FQDN
- Masque réseau
- Version IP
- Type de numéro de série
- Service Pack du système d'exploitation

À partir de la v3.0 de Contrôle de la posture de sécurité:

La connexion « Avec métadonnées CMDB » vous permet d'ajouter la propriété de nom d'hôte et d'utiliser l'opérateur regex de correspondances pour vous aider à saisir des expressions régulières dans vos conditions pour le type d'actif matériel. Par exemple, si vous entrez « lp », vous pouvez rechercher tous les ordinateurs portables avec « lp » comme deuxième et troisième caractères dans le nom d'hôte.

« Premier observé » : actifs qui ont été découverts pour la première fois par n'importe quelle source dans la période que vous sélectionnez avec la propriété d'horodatage « Premier observé ».

« Dernier observé » : actifs qui ont été « observés pour la dernière fois au cours des n derniers jours » par n'importe quelle source. Entrez le nombre de jours jusqu'à 30 comme valeur. Par exemple, entrez 3 comme valeur pour surveiller les actifs par « dernière connexion » à partir d'Active Directory au cours des trois derniers jours.

Type d'actif logiciel : recherchez des éditeurs de logiciels ou utilisez des SGC que vous avez installés et qui importent les données et métadonnées logicielles souhaitées si vous commencez par la connexion « Avec les détails du logiciel ».

Pour les types d'actifs matériels, vous pouvez utiliser la connexion « A des informations de modèle » avec la connexion « Avec les métadonnées CMDB » pour les appareils basés sur des modèles et des informations de modèle spécifiques.

Les types d'actifs matériels vous permettent également de rechercher tous les actifs signalés par une source, Qualys, par exemple, mais qui ne sont pas signalés par ServiceNow Découverte ITOM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voir Politiques pour Contrôle de la posture de sécurité pour plus d'informations sur le schéma de Contrôle de la posture de sécurité politique.

Exceptions avec l'application Governance, Risk, and Compliance (GRC)

Une exception de Gestion intégrée des risques (IRM) est un actif avec une exception approuvée du produit Gouvernance, risque et conformité (GRC). Une politique vous permet d'ajouter une condition pour une exception afin de ne pas surveiller ces actifs et de les inclure dans vos décomptes.

Par exemple, certains actifs peuvent avoir des exceptions approuvées pour certains objectifs de contrôle avec IRM. Pour réduire le nombre de correspondances renvoyées, les équipes de sécurité des informations peuvent exclure ces actifs de la surveillance des contrôles de sécurité avec des exceptions IRM qui sont déjà approuvés.

Aperçus clés et aperçus configurés pour Contrôle de la posture de sécurité

Les aperçus clés et configurés (personnalisés) vous fournissent des rapports visuels qui sont créés et mis à jour en fonction des critères d'évaluation qui correspondent à vos actifs. Les aperçus vous aident à surveiller les mesures des contrôles de sécurité sur un tableau de bord.

Aperçus clés

Les critères utilisés pour les évaluations de vos actifs sont fournis par les politiques incluses dans l'application.

- Les aperçus clés utilisent les politiques incluses dans l'application.
- Les aperçus configurés peuvent être créés à l'aide des politiques incluses dans l'application, de vos propres politiques personnalisées ou d'une combinaison des deux.

Dans l'accueil (page de destination) de l'espace de travail Contrôle de la posture de sécurité, la section Aperçus clés sous la vue d'ensemble affiche des rapports visuels créés et mis à jour par les politiques incluses dans l'application. Ces aperçus sont également inclus dans l'application et affichent les informations suivantes :

- Agent de protection du point de terminaison installé : nombre total d'actifs qui ont ou ne disposent pas d'une protection de point de terminaison.
- Couverture de l'appareil géré : nombre d'actifs gérés par rapport à ceux qui ne sont pas gérés.
- Couverture de l'analyse des vulnérabilités : nombre total d'actifs analysés par rapport à ceux qui ne sont pas analysés pour détecter les vulnérabilités connues par un scanner de vulnérabilité tiers.
- Actifs avec des vulnérabilités critiques : nombre d'actifs par rapport au nombre total d'actifs qui ont des vulnérabilités critiques.
- Éléments vulnérables par criticité : nombre total d'éléments vulnérables répartis par gravité. Une vulnérabilité connue qui correspond à un actif de votre CMDB entraîne la génération d'un élément vulnérable. Pour obtenir cet aperçu, vous devez installer l'application Vulnerability Response et au moins une intégration de scanner : Qualys, Rapid7 ou Tenable Vulnerability Integration. Toutes ces applications sont disponibles sur le .ServiceNow® Store
- 3 principales politiques par résultats : politiques qui renvoient le plus de résultats (correspondances) sur vos actifs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus configurés

Vous pouvez créer vos propres aperçus si vous souhaitez plus d'informations qui ne se trouvent pas dans les aperçus clés. Vous pouvez créer ces aperçus configurés et utiliser les politiques existantes ou vos propres politiques personnalisées pour l'évaluation. Vos aperçus configurés sont affichés dans le module Tableau de bord des aperçus configurés, la deuxième icône en partant du haut de l'espace de travail.

Les types d'aperçus suivants peuvent être configurés.

- Tableau comparatif : comparez les résultats entre plusieurs politiques à l'aide d'histogrammes.
- Widget du nombre de correspondances de politique : affichez le nombre d'appareils qui correspondent à une politique.
- Graphique des pourcentages de correspondance de politique : affichez le pourcentage d'appareils qui correspondent à une politique dans un graphique à secteurs. Vous pouvez choisir le pool d'actifs total comme tous les actifs surveillés par SPC ou les actifs qui correspondent à la politique de base à partir de laquelle la politique sélectionnée actuelle est créée.
- Graphique de tendance des polices : affichez les tendances des actifs qui correspondent à différentes politiques.

Consultez Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes de création d'un aperçu configuré.

Groupes

Vous devez créer ou affecter des groupes à vos aperçus configurés lorsque vous créez de nouveaux enregistrements dans le module Générateur d'aperçus personnalisés. Les groupes vous permettent d'organiser vos rapports sur le tableau de bord Aperçus configurés.

Les aperçus peuvent être organisés en groupes. Chaque groupe peut avoir 21 widgets ou aperçus.

Utilisation de l'espace de Contrôle de la posture de sécurité travail

L'espace Contrôle de la posture de sécurité de travail contient les modules que vous utilisez pour configurer, utiliser et surveiller les données importées sur vos actifs.

Rôles

Groupe d'administrateurs SPC

Les utilisateurs de ce groupe disposent d'un accès complet en lecture et en écriture à tous les enregistrements du produit, y compris les informations de gestion des licences. Les rôles granulaires de ce groupe comprennent : [sn_sec_caasm.analyst, sn_sec_caasm.caasm_security_admin et sn_sec_spc_core.configure].

Groupe d'analystes SPC

Les utilisateurs de ce groupe disposent d'un accès complet en lecture et en écriture à tous les enregistrements du produit, mais ne peuvent pas afficher les informations de gestion des licences. Les rôles granulaires de ce groupe comprennent [pa_power_user et sn_sec_spc_core.analyst].

Groupe en lecture seule d'analyste SPC

Les utilisateurs de ce groupe disposent d'un accès en lecture complet à tous les enregistrements du produit, mais ne peuvent pas afficher les informations de gestion des licences. Les rôles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

granulaires de ce groupe comprennent [pa_power_user, sn_sec_spc_core.analyst_read, sn_sec_caasm.read et cmdb_ms_user].

Rôles de l'application de soutien

Les rôles suivants sont requis par les applications qui prennent en charge SPC et Gestion de la posture de sécurité des actifs.

- Conformité de la configuration Administrateur [sn_vulc.admin] : configure l'application, a une visibilité sur tous les enregistrements et peut modifier les Conformité de la configuration propriétés. Affecte des rôles dans l'application Conformité de la configuration .
- Réponse aux vulnérabilités Administrateur [sn_vulc.admin] : configure l'application Vulnerability Response et les calculateurs de risque de vulnérabilité.
- Serveur MID [mid_server] : configure un Serveur MID.

Les modules de l'espace de travail

Pour accéder à l'espace de travail, accédez à **Espaces de travail** > **Contrôle de la posture de sécurité** L'accueil (page de destination) s'affiche. L'espace Contrôle de la posture de sécurité de travail contient les modules suivants.

Modules

Module	Description
Accueil	Affichez les visualisations de données et d'autres informations dans les sections Vue d'ensemble, Aperçus clés et Couverture du cas d'utilisation clé pour vous aider à surveiller vos actifs. Les informations fournies sur cette page vous permettent de rendre compte de l'état de votre posture de sécurité globale aux responsables informatique, informatique et sécurité, et à d'autres personnes concernées clés. Consultez Aperçus clés et aperçus configurés pour Contrôle de la posture de sécurité et Politiques pour Contrôle de la posture de sécurité.
Aperçus configurés	Affichez les visualisations de données sur vos actifs que vous créez, configurez et activez. Consultez Aperçus clés et aperçus configurés pour Contrôle de la posture de sécurité.
Recherche d'actifs	Recherchez rapidement des actifs dans votre environnement en fonction des conditions que vous définissez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modules (suite)

Module	Description
	Vérifiez que vous pouvez localiser les actifs avec un ensemble de conditions avant d'intégrer ces conditions à une politique. Vous pouvez affiner ces recherches afin d'obtenir un aperçu des ressources qui répondent à vos critères de recherche. Lorsque vous êtes prêt, vous pouvez enregistrer vos conditions en tant que politique. Consultez Créer une recherche d'actifs dans Contrôle de la posture de sécurité.
Profils d'actifs	Créez et définissez des profils d'actif pour surveiller différentes catégories d'appareils avec vos politiques SPC. Incorporez vos profils d'actifs dans vos politiques afin de pouvoir exécuter des politiques pour des types d'actifs spécifiques. Filtrez les aperçus dans le tableau de bord Aperçus configurés afin qu'ils soient basés sur vos profils d'actifs. Voir Créer un profil d'actif dans Contrôle de la posture de sécurité.
Politiques et résultats	Créez, clonez, modifiez et activez des politiques. Certaines politiques sont incluses dans l'application, et vous pouvez créer les vôtres. Les politiques auditent vos actifs pour trouver des correspondances avec les violations potentielles. Les aperçus, les visualisations et les cas d'utilisation dépendent des politiques. Consultez Politiques pour Contrôle de la posture de sécurité. Les actifs qui correspondent aux conditions de la politique sont signalés comme résultats et sont mappés à l'application pour correction Conformité de la configuration . Consultez Contrôle de la posture de sécurité : configuration et affichage de vos résultats.
Configuration des connecteurs et des tickets d'utilisation	Activez et affichez l'état des intégrations de connecteurs du graphe de services (SGC) et d'API installés. Les Connecteurs du graphe de services et les intégrations d'API sont des sources que vous utilisez pour importer des données relatives à vos actifs. Une grande variété de (SGC) sont pris en charge et sont disponibles auprès du ServiceNow® Store.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modules (suite)

Module	Description
	Configurez et surveillez les cas d'utilisation clés. Les cas d'utilisation sont différents scénarios que vous configurez pour vous aider à identifier des types spécifiques d'écarts de couverture d'outils. Chaque cas d'utilisation nécessite une ou plusieurs politiques pour auditer vos actifs afin de détecter d'éventuelles violations. Consultez Cas d'utilisation, exemples de politiques et connecteurs du graphe de services pris en charge dans Contrôle de la posture de sécurité.
Générateur d'aperçus personnalisés	Créez vos propres visualisations de données. Les aperçus personnalisés vous fournissent des rapports visuels qui sont mis à jour en fonction des résultats d'audit de vos politiques et des données importées. Une fois que vous les avez activés, vos aperçus personnalisés s'affichent sur le tableau de bord dans le module Aperçus configurés. Vous pouvez déterminer où les données d'un aperçu sont affichées sur le tableau de bord à l'aide de Groupes. Consultez Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité.

Utilisation des modules de l'espace de travail pour identifier les écarts dans la couverture de l'outil

L'identification des lacunes des outils de Security nécessite les étapes suivantes.

1. Configurez et activez les connexions d'API avec l'un des outils que vous utilisez dans différentes catégories. Vous pouvez utiliser Service Graph Connector pour les produits disponibles dans le ServiceNow Store pour les connexions d'API requises. Pour plus d'informations sur les connecteurs du graphe de services pris en charge, consultez Connecteurs du graphe de services pour Contrôle de la posture de sécurité et Connecteurs du graphe de services . Les connecteurs du graphe de services pris en charge sont disponibles auprès de avec ServiceNow® Store des abonnements distincts.
2. Effectuez une ou plusieurs recherches d'actifs basées sur des critères spécifiques pour obtenir un inventaire.
3. Activez les politiques expédiées avec l'application Contrôle de la posture de sécurité. Vous pouvez également créer vos propres politiques et les activer en fonction des résultats de vos recherches d'actifs.
4. Créez et activez vos propres aperçus configurés pour vous aider à surveiller vos actifs.
5. Pour savoir quelles menaces pesant sur vos actifs sont atténuées par les contrôles d'atténuation disponibles en fonction de la configuration des différents outils de sécurité,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

reportez-vous à la section Utilisation de la surveillance des contrôles d'atténuation avec Contrôle de la posture de sécurité.

6. Configurez des règles pour automatiser le workflow de rattrapage dans l'application Configuration Compliance.

L'identification des lacunes des outils de Security implique les étapes suivantes :

1. Activez les politiques expédiées avec l'application Contrôle de la posture de sécurité . Le Contrôle de la posture de sécurité produit détecte les lacunes de l'outil de Security en effectuant les tâches suivantes :
   a. Identifie la liste de tous les actifs uniques renseignés par divers connecteurs du graphe de services dans la CMDB.
   b. Identifie les actifs qui ne sont pas signalés par des catégories spécifiques à partir de cette réserve d'actifs (par exemple, Protection des points de terminaison). Les actifs sont identifiés en fonction de la politique active évaluée.
   c. Les actifs identifiés comme non signalés par des catégories spécifiques sont signalés comme « Constatations » ou « Résultats des tests » dans l'application Conformité de la configuration .
2. Affectez automatiquement des « résultats » à différentes équipes pour un rattrapage avec l'application Configuration Compliance.

Création de vos propres politiques

Consultez la rubrique Création de vos propres politiques dans l'application Contrôle de la posture de sécurité pour plus d'informations sur la création de vos propres stratégies.

Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour en savoir plus sur les étapes requises pour créer une politique.

Pour obtenir des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfant et clonées pour Contrôle de la posture de sécurité.

Activer une politique incluse dans l'application Contrôle de la posture de sécurité

Les politiques incluses dans l'application doivent être activées avant Contrôle de la posture de sécurité de pouvoir surveiller les actifs qui correspondent à cette politique. Par défaut, aucune des stratégies incluses dans l'application n'est activée.

Avant de commencer

Vous devez vérifier que toutes les conditions préalables requises sont remplies avant d'activer les politiques incluses dans l'application.

- Vérifiez que les connecteurs du graphe de services requis sont activés.
- Vérifiez que toutes les applications requises, telles que Réponse aux vulnérabilités, sont installées et activées, le cas échéant.
- Pour plus d'informations sur les stratégies utilisées pour la surveillance des contrôles d'atténuation, reportez-vous à la section Politiques de contrôles d'atténuation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Vous ne pouvez pas modifier les stratégies incluses dans l'application, mais vous pouvez créer de nouvelles stratégies en fonction de leurs critères avec les fonctionnalités **Cloner la stratégie** et **Créer une stratégie enfant** . Ces fonctionnalités sont disponibles dans le menu Autres options (trois points verticaux).

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Politiques et résultats** > **Tous**.

   Pour déterminer si une politique est activée, confirmez son état (vrai ou faux) dans la colonne Actif.

2. Sélectionnez un enregistrement de politique pour l'ouvrir.
3. Vous disposez des options suivantes sur les enregistrements de police inclus avec l'application :

Option	Description
Activer la politique	Activez une politique si vous souhaitez surveiller tous les actifs qui correspondent aux conditions de la politique et générer des résultats. Le cas échéant, sélectionnez Désactiver la politique pour arrêter les évaluations d'actifs et la génération de résultats pour cette politique.
Configurer les résultats	Sélectionnez **Oui** dans le modal pour générer des résultats pour la politique. Sélectionnez le lien **Configurer les règles d'affectation** pour configurer des règles d'affectation dans l'application Conformité de la configuration afin d'affecter tous les résultats à votre politique pour résolution. **Remarque :** Pour les politiques que vous créez avec « Logiciel » comme type d'actif, vous pouvez enregistrer la politique et créer des aperçus personnalisés, mais vous ne pouvez pas configurer les conclusions à partir de l'enregistrement de politique.
Cloner la politique	Créez une nouvelle politique avec toutes les conditions de la politique affichée comme point de départ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour plus d'informations.
Créer une politique enfant	Créez une politique enfant qui hérite des conditions de la politique actuelle. Les conditions actuelles de la politique s'affichent dans le champ « Politique de base » du nouvel enregistrement, et vous ajoutez d'autres conditions.
Désactiver la politique (affiché uniquement sur les politiques activées)	Désactivez une politique active si vous ne souhaitez pas que les actifs soient surveillés ou évalués par rapport à cette politique. Cette option de modification n'est visible que sur les enregistrements de politique activés.
Afficher les résultats	Ouvrez un nouvel onglet et affichez les actifs correspondants s'ils sont disponibles. Les résultats sont également renvoyés aux CTR, ou enregistrements de résultats de test pour la police.

Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité

Créez vos propres politiques personnalisées pour surveiller les actifs pour la couverture des outils et d'autres combinaisons à haut risque.

Avant de commencer

Pour vous aider à comprendre les étapes requises pour créer une politique avec plus de détails, reportez-vous à .Exemples de politiques de base, enfant et clonées pour Contrôle de la posture de sécurité Les exemples vous guident à travers les étapes requises pour créer une politique de base, utiliser la politique de base pour créer une politique enfant et cloner une politique.

Pour obtenir des exemples de stratégies, reportez-vous à la section Exemples de politiques de base, enfant et clonées pour Contrôle de la posture de sécurité.

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Liste** > **Politiques** > **Tous**.
2. Sélectionnez **Nouvelle politique**.
3. Sélectionnez l'icône en forme de crayon à côté du nom en haut pour modifier les métadonnées.

   Remplissez les champs.

Champ	Description
Nom	Nom unique pour votre politique.
Criticité	Sélectionnez-en un dans la liste.
Description brève	Une description unique pour votre police.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Enregistrer les métadonnées**.
5. Pour Type d'actif, sélectionnez « Actif » dans la liste.

Option de l'entité	Description de l'entité
Matériel	Localisez les périphériques IP qui incluent des appareils de calcul personnel, des machines virtuelles dans le cloud, des serveurs, des périphériques réseau et d'autres matériels.
Logiciel	Localisez les logiciels installés sur les appareils signalés par les SGC et vos scanners de vulnérabilité.

6. **Facultatif :** Choisissez aucun, un ou les deux.

Option	Description
Politique de base	Les conditions de votre choix de politique de base sont héritées dans la nouvelle politique.
Politiques d'exclusion	Sélectionnez toutes les politiques que vous souhaitez exclure des résultats d'actifs pour cette politique. Les conclusions de ces politiques sont ignorées.

(Optional) Les champs Connexion et Entité s'affichent.

7. Sélectionnez-en un dans la liste du champ Connexion.
   Le champ Entité cible est renseigné automatiquement en fonction de votre choix. Un nouveau champ Critère s'affiche avec les champs Propriété, Opérateur et Valeur. Pour plus d'informations sur les types d'actifs et le schéma des relations, reportez-vous à la section Politiques pour Contrôle de la posture de sécurité.
8. Sélectionnez-en un dans la liste pour la propriété.
9. **Sélectionnez une catégorie** ou **une source**.
10. Sélectionnez un opérateur et entrez une catégorie de connecteur, par exemple, Gestion des points de terminaison ou un nom de produit de catégorie (source).
11. **Facultatif :** Utilisez le générateur de conditions et ajoutez d'autres conditions ou ensembles de conditions.

(Optional) Vous naviguez des types d'actifs de niveau supérieur pour le matériel et les logiciels vers leurs entités secondaires à l'aide du générateur de conditions. En fonction de vos choix, des champs s'affichent pour vous et vous modifiez ou ajoutez des critères.

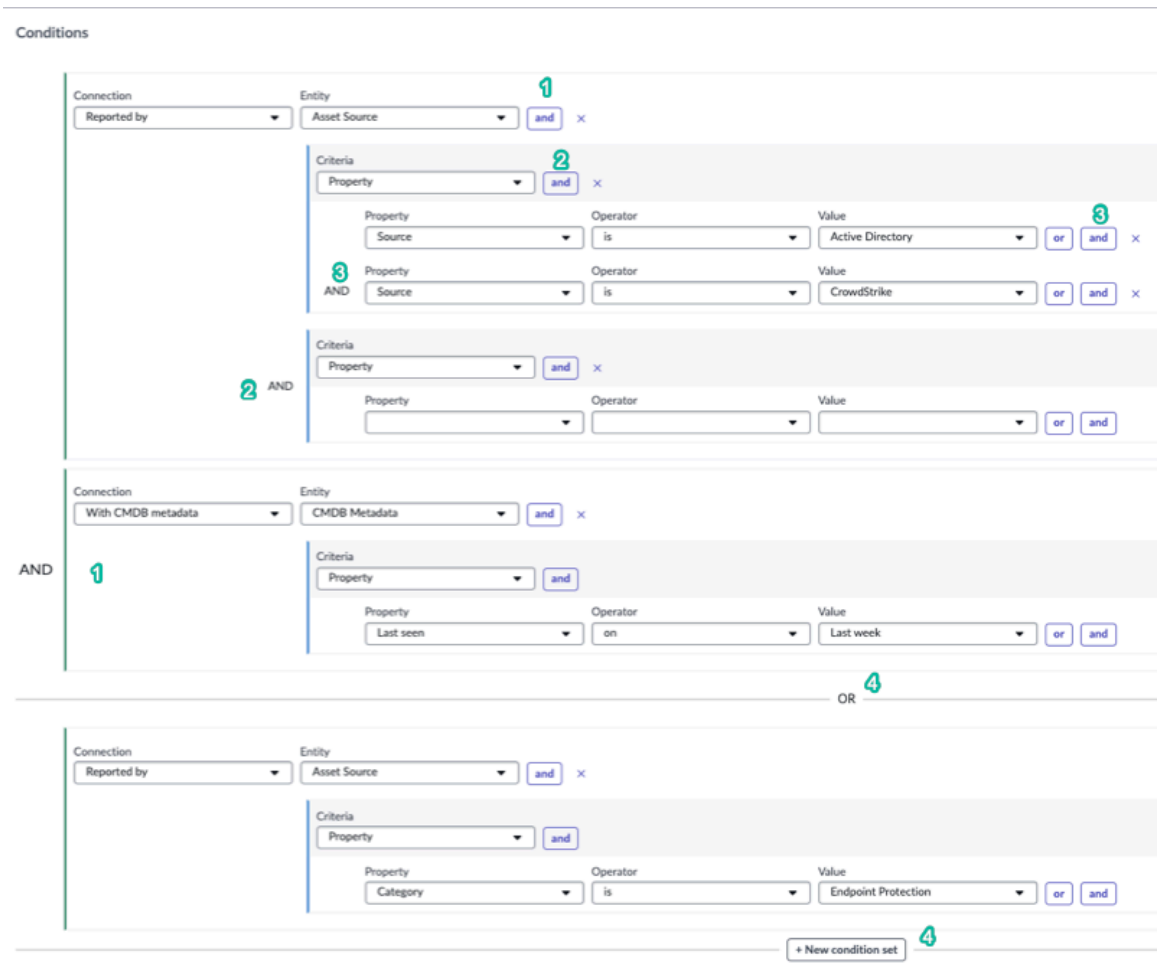
Les décorateurs AND, OR du générateur de conditions vous permettent de configurer la logique pour les données renvoyées que vous souhaitez renvoyer pour la politique. Reportez-vous au tableau et à l'image suivants pour plus d'informations.

Décorateur	Description	Numéro référencé dans l'image
Sélectionnez **ET** à côté des champs Connexion et Entité en haut pour le nouvel ensemble de conditions.	Ajoute un ET logique entre les critères d'entité de connexion actuels et de nouveaux critères d'une autre entité de connexion.	1
Sélectionnez **ET** à droite d'un champ Critère ou Propriété pour un nouvel ensemble de critères et de conditions de propriété.	Ajoute un ET logique entre les critères d'entité de connexion actuels et un nouveau critère sous la même entité de connexion.	2

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Décorateur	Description	Numéro référencé dans l'image
Sélectionnez **OU/ET** à droite d'un champ de propriété pour le nouvel ensemble de conditions de propriété.	Ajoute un OU/ET logique entre la propriété actuelle et une nouvelle propriété des mêmes critères de connexion-entité.	3
Sélectionnez **+ Nouvel ensemble de conditions** pour un nouvel ensemble de conditions.	Ajoute un OU logique entre l'ensemble de conditions de tous les critères actuels et un nouvel ensemble de conditions.	4



12. Sélectionnez **Enregistrer la politique** une fois que vous avez terminé la modification.
    Votre police est enregistrée. Vous pouvez choisir de l'activer maintenant ou de revenir plus tard pour l'activer.
13. Dans le menu Autres options en regard de **Enregistrer la politique**, sélectionnez Configurer les résultats.
14. Renseignez les champs.

Option	Description
Générer des conclusions pour cette politique ?	Choisissez **Oui** pour générer des résultats pour les actifs correspondants. Une fois les données importées, sélectionnez Afficher les résultats est affiché dans l'enregistrement de politique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Choisissez **Non** si vous ne souhaitez pas générer de résultats.
Configurer les règles d'affectation	Sélectionnez le lien pour configurer des règles d'affectation pour affecter des résultats à corriger dans l'application Configuration Compliance. Il existe une règle d'affectation par défaut dans la table [sn_vulc_assignment_rule_list] que vous pouvez utiliser dans Configuration Compliance.

15. Sélectionnez **Enregistrer la configuration**.

Une fois que vous avez enregistré et activé une politique, elle évalue les données importées à partir du connecteur du graphe de services planifiées lors de la prochaine exécution. Si vous souhaitez afficher les données sur le tableau de bord des aperçus configurés dans l'espace de travail, vous devez créer un nouvel aperçu dans le module Générateur d'aperçus personnalisés. Une fois que vous avez activé l'aperçu configuré, ses données s'affichent sur le tableau de bord des aperçus configurés dans l'espace de travail.

Modifier une politique activée dans Contrôle de la posture de sécurité

Vous pouvez modifier les politiques activées pour vous aider à personnaliser leurs conditions afin qu'elles correspondent mieux à vos actifs.

Avant de commencer

Vous ne pouvez pas modifier les stratégies incluses dans l'application, mais vous pouvez les cloner et créer des stratégies enfants à partir de celles-ci. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité.

Si vous modifiez des politiques et publiez vos changements, les versions sont suivies et les numéros de version sont affichés sur l'enregistrement de politique et ses résultats de test associés.

Avant de modifier une stratégie activée, vous préférerez peut-être la désactiver afin que la stratégie ne continue pas à évaluer vos actifs pendant que vous modifiez.

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Liste** > **Politiques** > **Tous**.
2. Sélectionnez un enregistrement de politique pour l'ouvrir.
3. Sélectionnez **Modifier la politique**.
   Si vous modifiez pour la première fois, deux boutons désactivés s'affichent à côté du bouton actif **Quitter le mode d'édition** : **Enregistrer les modifications** et **Publier les modifications**. Si vous avez déjà modifié cette politique et l'avez enregistrée en tant que brouillon, la notification, Vous avez une modification non publiée s'affiche également.
4. Apportez vos modifications et choisissez-en une pour continuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Enregistrer les changements	Enregistrez vos modifications en tant que brouillon et revenez au mode d'édition. Vos changements ne sont pas publiés pour l'instant. Vous pouvez revenir à la politique et continuer à les modifier plus tard.
Publier les changements	Publiez vos changements en tant que nouvelle version de la stratégie et quittez automatiquement le mode édition. L'affichage des résultats dans votre nouvelle version de la stratégie peut prendre un certain temps sur le bouton Afficher les conclusions de la stratégie. Si vous publiez une nouvelle version d'une politique, vous avez la possibilité de fermer tous les résultats existants pour la politique que vous avez modifiée. Vous préférez peut-être fermer les résultats existants de la politique d'origine si vous souhaitez uniquement afficher les résultats de votre politique modifiée. Si vous annulez à ce stade ou quittez le mode d'édition, un message s'affiche indiquant que vous avez une modification non publiée pour cette politique. Si vous choisissez de fermer ses résultats des tests associés existants (conclusions), les états de résultat des tests et de tâche de rattrapage passent conformément aux processus de transition d'état de l'application Configuration Compliance. Consultez Transitions d'états des résultats des tests et des tâches de rattrapage dans l'application Contrôle de la posture de sécurité pour plus d'informations.
Afficher l'historique des versions	Pour les changements publiés, les versions sont suivies et les numéros de version sont affichés sur l'enregistrement de politique et ses résultats de test associés.
Quitter le mode Édition	Quittez sans enregistrer vos changements ou enregistrez vos changements et quittez sans publier. Si vous enregistrez vos changements et ne les publiez pas, vous devez publier votre nouvelle version avant qu'elle puisse créer des conclusions.
Désactiver la politique (affiché uniquement sur les politiques activées)	Désactivez une politique active si vous ne souhaitez pas que les actifs soient surveillés ou évalués par rapport à cette politique. Cette option de modification n'est visible que sur les enregistrements de politique actifs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Afficher les résultats	Ouvrez un nouvel onglet et affichez les actifs correspondants s'ils sont disponibles. Les résultats sont également renvoyés aux CTR ou aux enregistrements de résultats de test pour la police.

5. Une fois que vous avez enregistré la politique en tant que brouillon et quitté le mode d'édition, sélectionnez l'une des options suivantes :

Option	Description
Modifier la politique	Revenez au mode d'édition.
Désactiver la politique (affiché uniquement sur les politiques activées)	Désactivez une politique active si vous ne souhaitez pas que les actifs soient surveillés ou évalués par rapport à cette politique. Cette option est uniquement visible sur les enregistrements de politique actifs.
Menu Autres options	
Configurer les résultats	Sélectionnez **Oui** dans le modal pour générer des résultats pour la politique. Consultez Contrôle de la posture de sécurité : configuration et affichage de vos résultats.
Cloner la politique	Créez une copie de l'enregistrement de la politique. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité.
Créer une politique enfant	Créez une nouvelle politique en utilisant cette politique comme base. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité.
Supprimer la politique	Supprimez l'enregistrement de politique de la liste de politiques.
Afficher les résultats	Ouvrez un nouvel onglet et affichez les actifs correspondants s'ils sont disponibles. Les résultats sont également renvoyés aux enregistrements de résultats de test (CTR) pour la police.
Afficher les enregistrements liés	Pour les politiques publiées, affichez les aperçus personnalisés, le cas échéant. Reportez-vous à la rubrique Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité.

Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité

Clonez une politique existante et ajoutez-y des conditions pour créer votre propre politique personnalisée. Vous pouvez également créer des politiques enfants à partir de stratégies existantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Vous pouvez cloner des politiques pour créer vos propres politiques personnalisées. Vous pouvez cloner une politique ou créer une politique enfant en utilisant n'importe quelle stratégie comme base pour vous aider à étendre les politiques existantes sans avoir à entrer à nouveau les conditions. Toutes les conditions de la politique de base sont également héritées de la politique enfant. Consultez Cloner une politique ou créer une politique enfant dans Contrôle de la posture de sécurité pour plus d'informations.

Vous pouvez cloner toutes les politiques incluses dans l'application, mais les correspondances de politiques ne sont pas reflétées en tant qu'aperçus clés sur le tableau de bord de la page de destination d'accueil. Seuls les aperçus clés des politiques incluses dans l'application sont affichés sur la page de destination de la page de destination.

Après avoir cloné et activé toutes les politiques que vous créez, vous devez créer votre propre enregistrement d'aperçu configuré dans le module Générateur d'aperçus personnalisés de l'espace de travail (le dernier module du panneau de navigation). Ce n'est qu'ensuite que vous pouvez afficher les données de vos politiques sur le tableau de bord des aperçus configurés (la deuxième icône en partant du haut de l'espace de travail).

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Liste** > **Politiques** > **Tous**.
2. Sélectionnez l'enregistrement de politique que vous souhaitez cloner.
3. Sélectionnez-en un dans le menu Autres options en regard de **Activer la politique**.

Option	Description
Cloner la politique	Sélectionnez cette option si vous souhaitez utiliser les conditions d'une politique exis–tante comme point de départ pour votre nouvelle politique. Un nouvel onglet avec l'enregistrement de politique cloné s'affiche avec « copie » dans le nom. (Facultatif) Sélectionnez une politique de base et ajoutez-en une dans la liste pour votre nouvelle politique.
Créer une politique enfant	Sélectionnez cette option si vous souhaitez créer une nouvelle politique en utilisant la politique actuelle comme point de départ. Un nouvel onglet avec un enregistrement de politique vide avec une politique de base que vous choisissez s'affiche.

4. **Facultatif :** Sélectionnez **Stratégie de base** et sélectionnez une stratégie comme base de votre nouvelle politique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

(Optional) Vous pouvez choisir cette option si vous souhaitez hériter des conditions d'une stratégie existante comme point de départ de votre nouvelle stratégie.

5. **Facultatif :** Sélectionnez **Politiques d'exclusion** et sélectionnez les politiques que vous souhaitez exclure des résultats de cette politique.
   Les résultats de votre nouvelle politique qui correspondent à des politiques exclues ne sont pas inclus dans vos résultats.
6. Pour une politique clonée, modifiez les conditions.
   Pour plus d'informations sur les relations ressource-connexion-entité dans le générateur de conditions, reportez-vous à la section Politiques pour Contrôle de la posture de sécurité. Pour plus d'informations sur les décorateurs du générateur de conditions, reportez-vous à la section Création de vos propres politiques dans l'application Contrôle de la posture de sécurité.
7. Modifier et enregistrer votre politique avec **Enregistrer les changements**.
   Votre politique s'affiche dans la liste Tout du module Liste de l'espace de travail.
8. Pour activer une stratégie, suivez les étapes décrites à la section Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité.
9. **Facultatif :** Sélectionnez Supprimer la politique pour supprimer une politique.
   L'option de suppression n'est pas prise en charge pour les politiques fournies avec l'application ou pour les politiques qui ont généré des résultats. Vous ne pouvez désactiver que des politiques avec des résultats.

Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité

Vous pouvez créer vos propres aperçus. Les aperçus configurés sont des aperçus que vous pouvez créer à l'aide de politiques existantes ou de vos propres politiques personnalisées.

Avant de commencer

Vous devez créer un enregistrement d'aperçu et l'activer avant de pouvoir afficher vos données sur le tableau de bord des aperçus configurés. Vous pouvez avoir jusqu'à six aperçus et 21 graphiques sur le module Tableau de bord des aperçus configurés de l'espace de travail.

Toutes les politiques que vous utilisez pour un aperçu personnalisé doivent être activées.

Pour les politiques que vous créez avec « Logiciel » comme type d'actif, vous pouvez enregistrer la politique et créer des aperçus personnalisés, mais vous ne pouvez pas configurer les conclusions à partir de l'enregistrement de politique.

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Générateur d'aperçus**.

   Sur cette page de destination, il y a trois onglets :

   Actif

   Vos aperçus personnalisés activés. Les aperçus personnalisés activés s'affichent sur la page de destination Aperçus configurés (deuxième icône en partant du haut de l'espace de travail).

   Inactif

   Vos aperçus personnalisés inactifs. Les aperçus désactivés ne s'affichent pas sur la page de destination des aperçus configurés tant que les aperçus et les politiques de prise en charge ne sont pas activés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tous

Tous vos aperçus configurés actifs et inactifs.

2. Sélectionnez **Nouvel aperçu** à droite de la page pour créer un enregistrement.
3. Dans le champ Type, sélectionnez un aperçu dans la liste de choix.

Option	Description
Tableau comparatif	Comparez les nombres d'actifs correspondants pour un maximum de cinq polices.
Widget du nombre de correspondances de politique	Nombre total de vos actifs qui correspondent à une ou plusieurs politiques.
Graphique des pourcentages de correspondance avec les politiques	Pourcentage de vos actifs totaux qui correspondent ou non à une police.
Graphique des tendances de correspondance avec les politiques	Tendance historique des actifs qui correspondent à une ou plusieurs politiques.

4. Sélectionnez-en un.
   - Actif matériel ou ordinateur virtuel dans le cloud
   - Logiciel
5. Sélectionnez des groupes pour votre aperçu.
   Un aperçu doit appartenir à au moins un groupe. Vous devez créer ou affecter des groupes à vos aperçus configurés lorsque vous créez de nouveaux enregistrements dans le module Générateur d'aperçus personnalisés. Les groupes vous permettent d'organiser vos rapports sur le tableau de bord Aperçus configurés.
6. Sélectionnez les politiques et les étiquettes correspondantes que vous souhaitez pour vos données d'aperçu.
7. Sélectionnez **Enregistrer**.
   Votre aperçu est enregistré dans l'onglet Aperçu inactif.
8. Pour activer votre nouvel aperçu, ouvrez l'enregistrement de la liste Inactive et sélectionnez **Activer**.
   Les données sont collectées à partir de la prochaine importation planifiée pour les connecteurs du graphe de services associés aux politiques de l'aperçu, et les données sont affichées dans le module Tableau de bord des aperçus personnalisés dans l'espace de travail.

Créer un profil d'actif dans Contrôle de la posture de sécurité

Créez un profil d'actif avec des conditions pour regrouper les actifs. Vous pouvez utiliser ces profils d'actifs dans vos stratégies.

Avant de commencer

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Tous** > **Espace de travail Contrôle de la posture de sécurité** > **Profils d'actifs**.
2. Sélectionnez **Nouveau**.
   Le générateur de conditions s'affiche. Notez que le nom inclut la date et l'heure de création du profil.
3. Sélectionnez l'icône du stylet pour modifier le nom du profil avec un nom unique.
4. Sélectionnez **Enregistrer les métadonnées**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez-en un dans la liste pour la connexion :

   Le profil d'actif prend en charge trois types de connexion.

   - **Avec métadonnées CMDB** : collection des propriétés de CI CMDB telles que le nom d'hôte, le système d'exploitation, la version du système d'exploitation, le premier et le dernier observé, par exemple, ou les connexions auxquelles des cartes réseau ou des logiciels sont installés.
   - **Avec données agrégées** : collection de propriétés avec des valeurs agrégées signalées par différentes sources pour un actif donné. Par exemple, les différentes façons dont les sources peuvent signaler une version de système d'exploitation : windows11, Win11, Windows 11, etc.
   - **À partir de la classe CI** : collection des classes CI qui inclut l'ordinateur, le serveur, l'instance d'ordinateur virtuel et d'autres.

   Les opérateurs et la logique de ce créateur de stratégie de profil d'actif sont similaires à ceux décrits dans Création de vos propres politiques dans l'application Contrôle de la posture de sécurité.

6. Sélectionnez **Créer**.
   Votre profil est affiché dans la liste Profils d'actifs.

   Vous pouvez associer des profils d'actifs à n'importe quelle politique.

7. Accédez à la **Tous** > **Espace de travail Contrôle de la posture de sécurité** > **Politiques et résultats**.
8. Sélectionnez une politique.
9. Dans la section Politiques et profils, sélectionnez un ou plusieurs profils d'actif.
10. Sélectionnez **Enregistrer les modifications**.
    La politique audite vos actifs en fonction des données importées à partir de vos connecteurs du graphe de services et inclut les conditions des profils d'actifs que vous avez ajoutés. Vous pouvez Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité ajouter des profils d'actif en tant que filtre.
11. Accédez à la **Tous** > **Espace de travail Contrôle de la posture de sécurité** > **Aperçus configurés**.
    Vous devez Créer et activer un aperçu configuré pour Contrôle de la posture de sécurité avant que les données ne s'affichent sur cette page.

    Étant donné que les visualisations de cette page sont configurées par politiques, vous pouvez les filtrer avec des profils d'actif. Filtrez les données des visualisations en procédant comme suit :

12. Sélectionnez l'icône de filtre.
13. Sélectionnez **Sélectionner**.
14. Sélectionnez et déplacez l'un des profils d'actif de la colonne Disponible vers la colonne Appliqué.
15. Sélectionnez **Appliquer**.
    Les visualisations d'aperçus personnalisés sont filtrées pour afficher les données des politiques qui incluaient les profils d'actifs que vous avez choisis. Un message dans le volet Filtre indique combien d'aperçus configurés sont filtrés à la suite des profils d'actifs que vous avez ajoutés. Les mises à jour des données de tendance peuvent être retardées, car la tâche planifiée Exécuter la politique SPC doit être terminée pour mettre à jour les données de tendance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supprimer un profil d'actif dans Contrôle de la posture de sécurité

Vous pouvez supprimer des profils d'actif. Vous supprimez les profils d'actif s'ils sont associés à des politiques, de sorte que les conditions du profil d'actif ne soient pas incluses dans le prochain audit de politique.

Avant de commencer

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Tous** > **Espace de travail Contrôle de la posture de sécurité** > **Profils d'actifs**.
2. Sélectionnez un enregistrement de profil.
3. Sélectionnez l'icône de menu Plus ⋮) et sélectionnez **Supprimer le profil d'actif**.
4. **Facultatif :** Dans la boîte de dialogue, sélectionnez **Examiner les politiques** pour afficher toutes les politiques auxquelles ce profil est lié.
   Les politiques qui contiennent le profil d'actif sont répertoriées dans l'onglet Politiques liées.
5. Sélectionnez l'onglet avec le profil d'actif que vous souhaitez supprimer.
6. Sélectionnez l'icône de menu Actions supplémentaires, puis **Supprimer le profil d'actif**.
   Il s'agit d'une suppression définitive. Les conditions du profil d'actif sont supprimées de toutes les politiques et ne sont pas incluses dans les audits de politique nocturnes suivants pour obtenir les derniers résultats.

Contrôle de la posture de sécurité : configuration et affichage de vos résultats

Vous pouvez afficher les résultats générés par l'évaluation des politiques dans Contrôle de la posture de sécurité dans l'espace de travail Contrôle de la posture de sécurité.

Vue d'ensemble des résultats

Tous les actifs correspondants sont signalés comme « Résultats ». Vous pouvez configurer les résultats à générer à partir de l'exécution des politiques afin que ces résultats puissent être affectés à différentes équipes pour le rattrapage ou utilisés pour la génération de rapports. Contrôle de la posture de sécurité publie ces résultats sous forme de « Résultats des tests » dans le module Conformité de la configuration. Tous les contrôles administratifs dans l'application Configuration Compliance qui sont liés à l'affectation, au regroupement (génération de tâche de rattrapage), aux cibles de rattrapage et aux exceptions sont pris en charge pour les résultats générés par Contrôle de la posture de sécurité.

Types de résultats :

Couverture de l'outil

Ce type représente un écart de couverture de l'outil de sécurité. Ce type de résultat s'applique aux politiques utilisant des relations « Signalé par le connecteur » et « Non signalé par le connecteur ».

Exposition Internet

Ce type représente l'exposition Internet d'un actif dans le cloud. Ce type de résultat s'applique aux politiques utilisant la relation « Has-internet-exposed-port » sur CloudVM.

Combinaison à risque élevé

Ce type représente un problème ayant plusieurs facteurs de risque associés, c'est-à-dire des actifs avec des vulnérabilités critiques et un agent de protection de point de terminaison manquant.

Selon les relations utilisées dans les politiques, les types de résultats disponibles sont visibles lorsque vous sélectionnez **Configurer les résultats**. Par exemple, si vous sélectionnez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les résultats d'une politique qui a plusieurs facteurs de risque, tels que « Actifs dans le cloud avec des vulnérabilités critiques, Protection des points de terminaison manquante et Port SSH 22 ouvert à Internet », les options suivantes s'affichent comme types de résultats qui peuvent être générés.

1. Combinaison à risque élevé
2. Couverture de l'outil
3. Exposition Internet

Vous pouvez choisir de générer des résultats de type « Combinaison à risque élevé » qui crée un résultat pour chaque actif correspondant à cette police. Vous pouvez également choisir de créer des résultats du type « Couverture de l'outil » et « Exposition Internet », ce qui entraînera la création de deux résultats pour chaque actif correspondant à la police : un du type « Couverture de l'outil » et un du type « Exposition Internet ».

En utilisant le type de résultats ou le résultat des tests, vous pouvez écrire des règles d'affectation dans Configuration Compliance pour acheminer ces problèmes aux équipes respectives pour correction. Par exemple, vous pouvez envoyer les résultats « Couverture de l'outil » à l'équipe des opérations IT et « Exposition Internet » à l'équipe chargée de l'application.

Toutefois, si l'un des propriétaires de rattrapage résout le problème, l'autre résultat est automatiquement fermé, car ces résultats sont générés par une politique recherchant la combinaison. Par exemple, si l'équipe des opérations informatiques ferme le résultat « Couverture de l'outil » en installant l'agent de protection du point de terminaison, le résultat « Exposition Internet » généré par cette politique est automatiquement fermé, même si l'actif est orienté vers Internet, car ce résultat est généré par une politique qui recherche une combinaison de problèmes. Si vous souhaitez suivre le problème d'exposition à Internet sur les actifs, il est recommandé de créer une autre police qui recherche uniquement l'exposition à Internet sur les actifs et non aucun autre facteur de risque.

Où consulter les résultats

Ces options vous permettent d'afficher les résultats générés par l'évaluation des politiques.

- Accédez à la **Espace de travail Contrôle de la posture de sécurité** > **Listes** > **Conclusions** > **Tout.**
- Sur un enregistrement de politique, sélectionnez **Afficher les résultats**.
- Dans l'application Configuration Compliance, sélectionnez Résultats des **tests** et filtrez les enregistrements par **Source est ServiceNow SPC**.

Le tableau de bord

Dans l'espace de travail Contrôle de la posture de sécurité, l'accueil (page de destination) affiche les visualisations suivantes :

Vue d'ensemble

- Actifs : nombre d'actifs surveillés sur site et dans le cloud.
- Résultats par criticité : nombre de résultats critiques sur le total de vos actifs.
- Actifs surveillés par les 5 principales sources : les cinq principaux connecteurs du graphe de services générant des rapports sur les actifs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Comptes dans le cloud : nombre de comptes dans le cloud surveillés par AWS et Azure.
- Résultats ouverts par rapport aux résultats fermés : comparaison des enregistrements encore en cours ou en attente de résolution et de ceux qui sont résolus.

Aperçus clés

- Agent de protection du point de terminaison installé : nombre total d'actifs avec ou sans protection de point de terminaison.
- Couverture de l'appareil géré : nombre d'actifs gérés par rapport à ceux qui ne sont pas gérés.
- Couverture de l'analyse des vulnérabilités : nombre total d'actifs analysés par rapport au nombre d'actifs qui ne sont pas analysés pour détecter les vulnérabilités connues par un scanner de vulnérabilité tiers.
- Actifs avec des vulnérabilités critiques : nombre d'actifs par rapport au nombre total d'actifs qui ont des vulnérabilités critiques.
- Éléments vulnérables par criticité : nombre total d'éléments vulnérables répartis par gravité. Une vulnérabilité connue qui correspond à un actif de votre CMDB entraîne la génération d'un élément vulnérable.
- 3 principales politiques par résultats : les politiques qui renvoient le plus de résultats (correspondances) sur vos actifs.

Couverture du cas d'utilisation clé

Sélectionnez une visualisation et **contribuez à l'améliorer** pour voir quels connecteurs et politiques du graphe de services sont activés pour les cas d'utilisation clés.

Transitions d'états des résultats des tests et des tâches de rattrapage dans l'application Contrôle de la posture de sécurité

Les états des résultats (enregistrements des tests de configuration) et leurs tâches de rattrapage associées sont impactés si vous modifiez vos politiques dans l'application Contrôle de la posture de sécurité.

Scénarios de transition d'état entre les résultats des tests et les tâches de rattrapage

À quelques exceptions près, les états font généralement la transition entre vos résultats (résultats des tests) et leurs tâches de rattrapage associées dans Contrôle de la posture de sécurité, de la même manière qu'ils passent des résultats des tests aux tâches de rattrapage dans l'application Conformité de la configuration . Toutefois, si vous modifiez vos politiques dans Contrôle de la posture de sécurité, vos changements ont un impact sur la transition des états de vos résultats et de leurs tâches de rattrapage associées.

Les tableaux suivants illustrent la transition des états sur vos résultats si vous modifiez et publiez une nouvelle version (modifier), désactivez ou supprimez vos stratégies.

Pour plus d'informations sur les changements d'état dans , reportez-vous Transitions d'états des résultats des tests et des tâches de rattrapage dans l'application Conformité de la configurationà Conformité de la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : À partir de la version 14.9 de Conformité de la configuration, les termes suivants ont été renommés :

Changements dans la terminologie

Terminologie antérieure à la version 14.9	Terminologie v14.9 et ultérieures
Groupe de résultats des tests	Tâche de remédiation
Règles de groupe	Règles de la tâche de rattrapage
Politique	Groupe de test

Les améliorations apportées aux audits de stratégie garantissent que les actifs mis hors service ne sont pas évalués par des stratégies activées. Si l'état d'un actif passe de **Mis hors service** à **Actif**, il est inclus dans la prochaine évaluation de la politique.

Si une politique est...	Valeurs de champ sur des enregistrements de résultats existants pour...	Transition vers...
Désactivé	Résultat	Conserver les valeurs d'origine
	État	Fermé
	Résolution	Expiré

Si une politique est...	Valeurs de champ sur des enregistrements de résultats existants pour...	Transition vers...
Modifié avec la possibilité de fermer tous les résultats existants sélectionnés	Résultat	Conserver les valeurs d'origine
	État	Fermé
	Résolution	Résultat non valide

Si une politique est...	Valeurs de champ sur des enregistrements de résultats existants pour...	Transition vers...
Modifié avec la possibilité de conserver les résultats existants sélectionnés	Résultat	Les scénarios de tests valides (réussis) conservent les valeurs d'origine et les scénarios de tests non valides (échecs) sont fermés.
	État	Fermé
	Résolution	Résultat non valide

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si une politique est...	Valeurs de champ sur des enregistrements de résultats existants pour...	Transition vers...
Supprimé	Résultats	Conserver les valeurs d'origine
	État	Fermé
	Résolution	Résultat non valide

Créer une recherche d'actifs dans Contrôle de la posture de sécurité

Définissez vos conditions et recherchez des actifs par produits Service Graph Connector spécifiques ou par des actifs dont des données spécifiques sont signalées par un connecteur.

Avant de commencer

À titre d'exemple de recherche, supposons que vous souhaitiez identifier vos actifs qui ont des serveurs Windows et une version spécifique trouvée dans CrowdStrike les détails des métadonnées.

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Recherche d'actifs**.
2. Choisissez-en un.

Option	Description
Actif matériel	Recherchez n'importe quel appareil, y compris des appareils informatiques personnels, des serveurs, des périphériques réseau, des machines virtuelles dans le cloud et d'autres matériels.
Logiciel	Recherchez les logiciels installés sur vos actifs signalés par Connecteur du graphe de services, vos produits de scanner de vulnérabilité et les logiciels signalés par les scanners qui sont déjà comptabilisés dans Gestion des actifs logiciels (SAM) et d'autres produits ServiceNow.

   Pour cet exemple, sélectionnez **Actif matériel pour Type d'actif** .
3. **Facultatif :** Sélectionnez **Politique de base** et **Politiques d'exclusion** si vous souhaitez utiliser les conditions d'une politique existante comme point de départ et exclure les actifs qui correspondent aux politiques existantes, respectivement.
   Les politiques que vous sélectionnez s'affichent.
4. Sélectionnez **Avec données de connecteur** pour le champ Connexion.
5. Sélectionnez **les détails de l'appareil CrowdStrike** pour l'entité.
6. Pour Propriété, Opérateur et Valeur, sélectionnez **[Version de l'agent][est]** et entrez la version, par exemple, **6.26.14003.0**.
7. Sélectionnez l'opérateur ET à droite du champ Entité avec CrowdStrike Détails de l'appareil comme valeur pour une autre condition.
8. Sélectionnez **Avec les métadonnées CMDB** pour le champ Connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le champ Entité est renseigné avec les métadonnées CMDB.

9. Sélectionnez la **propriété** pour le champ Critères.
10. Pour Propriété, Opérateur et Valeur, sélectionnez **[Système d'exploitation][contient]** et entrez **Serveur Windows**.
11. Sélectionnez **Afficher les actifs**.
    Après quelques instants, les résultats s'affichent dans l'onglet Actifs correspondants. Si vous ne voyez aucune correspondance, vous pouvez affiner votre recherche. Lorsque vous êtes satisfait d'avoir correctement défini les conditions, vous pouvez enregistrer la recherche en tant que politique et l'activer. Comme les autres stratégies, il recherche vos actifs avec une tâche en arrière-plan en continu après son activation.

Résolution des éléments de configuration en double dans Contrôle de la posture de sécurité

La résolution des entrées en double pour les éléments de configuration (CI) dans votre base de données de gestion des configurations vous assure d'obtenir des audits précis avec vos SPC politiques.

Vue d'ensemble des éléments de configuration en double

Dans certains cas, vos sources de découverte d'actifs, c'est-à-dire vos produits Service Graph Connector (SGC), importent des données d'actif susceptibles de créer des entrées en double dans votre Base de données de gestion des configurations (CMDB) pour les actifs (éléments de configuration). Ces enregistrements de CI en double se produisent lorsque deux actifs ou plus sont répertoriés dans votre CMDB avec les mêmes noms, mais que les références CMDB sont différentes.

Par exemple, une ressource nommée par son adresse IP, 10.0.2.11, qui est répertoriée deux fois dans la table Données CMDB 360 [cmdb_multisource_data]. Une entrée pour 10.0.2.11 est répertoriée dans la colonne de référence CMDB sous le numéro 10.0.2.11, et une autre sous le numéro 10.0.65.159. Ces actifs peuvent provenir de la même source de découverte, d'un produit SGC ou de deux sources de découverte ou plus. Dans les deux cas, pour éviter les problèmes liés aux politiques SPC et à vos inventaires d'actifs, vous devez supprimer les CI en double.

Identification et suppression des éléments de configuration en double

Vous pouvez identifier les CI en double en filtrant la colonne Nom de la table [sn_sec_spc_core_asset_cache] et en notant quels actifs portent le même nom.

Si vous identifiez des doublons, le processus de déduplication de CI intègre un modèle de déduplication que vous devez publier, une propriété système que vous activez et une tâche planifiée qui supprime les CI en double dans la table Actifs SPC mis en cache [sn_sec_spc_core_asset_cache]. Le processus supprime les doublons et préserve l'enregistrement de CI maître ou canonique qui contient le plus d'éléments connexes.

Résoudre les éléments de configuration en double dans Contrôle de la posture de sécurité

Utilisez ce processus pour supprimer les éléments de configuration en double dans la table Actifs SPC mis en cache [sn_sec_spc_core_asset_cache]. Ce processus supprime les enregistrements en double et préserve l'enregistrement d'actif maître ou canonique qui contient le plus d'éléments connexes.

Avant de commencer

Rôles requis : sn_cmdb_user pour accéder à l'espace de travail CMDB et sn_sec_spc_core.admin pour lancer la tâche planifiée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Propriétés système** > **Toutes les propriétés**.
2. Localisez la propriété système sn_sec_spc-core.is_ci_name_unique.

   Il s'agit d'une valeur configurable sur la propriété qui spécifie si tous les éléments de configuration répertoriés dans votre table CMDB ou Cache d'actifs ont des noms uniques.

   Consultez Résolution des éléments de configuration en double dans Contrôle de la posture de sécurité pour plus d'informations sur l'identification des CI en double.
3. Sélectionnez l'enregistrement pour l'ouvrir et définissez le champ Valeur sur **vrai**.
4. Mettez à jour l'enregistrement
5. Accédez à la **Espace de travail CMDB** > **Gestion** et sélectionnez le lien Bibliothèque de modèles de déduplication sous Outils de gestion à droite.

   Remarque : Le rôle sn_cmdb_user est requis pour accéder à l'espace de travail CMDB.
6. Dans le volet Modèles de déduplication, développez **les modèles de déduplication SPC** et sélectionnez **Bascule Nom** pour l'ouvrir.
7. Sélectionnez **Publier**.
8. Sélectionnez **Publier** dans la fenêtre modale.

   Vous avez publié le modèle de déduplication et activé la propriété système sn_sec_spc-core.is_ci_name_unique. Vous devez exécuter la tâche planifiée Générer la tâche de déduplication pour générer les tâches qui résolvent les CI en double.
9. Accédez à la **Tous** > **Définition du système** > **Travaux planifiés** > **Générer une tâche de déduplication** et sélectionnez l'enregistrement pour l'ouvrir.
10. Sélectionnez **Exécuter maintenant**.
    Vérifiez que la tâche en arrière-plan est en file d'attente et en cours de traitement.
11. Accédez au **Tâche en arrière-plan [sn_sec_cmn_background_job]** table pour surveiller la tâche planifiée Générer la tâche de déduplication.
    Une fois la tâche planifiée terminée (Terminé), vous pouvez lancer le modèle que vous avez publié.
12. Accédez à la **Espace de travail CMDB** > **Gestion** et sélectionnez **Afficher le tableau de bord de déduplication**.
13. Sélectionnez **En cours d'exécution** pour charger le modèle.
14. Sélectionnez l'onglet **Terminé** pour afficher les tâches terminées.

    Vous devez vérifier que les tâches de déduplication sont terminées avant de vérifier la présence de doublons dans la table Actifs SPC mis en cache [sn_sec_spc_core_asset_cache].

    Vous devrez peut-être actualiser votre écran pour afficher les tâches effectuées.
15. Lorsque la tâche planifiée est terminée avec succès et que vous avez vérifié que les tâches de déduplication sont terminées, accédez à la table Actifs SPC mis en cache [sn_sec_spc_core_asset_cache], filtrez la colonne Nom et vérifiez les doublons.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le principal, ou canonique, est l'enregistrement de CI qui contient le plus d'éléments connexes. Il est conservé sur la table. S'il n'y a pas de doublons, vérifiez s'il y a des doublons dans la table de données CMDB 360 [cmdb_multisource_data].

16. Accédez à la table Données CMDB 360 [cmdb_multisource_data].
17. Regroupez par Col0 et vérifiez s'il existe différentes références CMDB pour les actifs qui correspondent à la colonne Nom de la table Actifs SPC mis en cache [sn_sec_spc_core_asset_cache].
    Si vous trouvez des doublons, exécutez à nouveau la tâche planifiée Générer la tâche de déduplication.

Utilisation de la surveillance des contrôles d'atténuation avec Contrôle de la posture de sécurité

Depuis l'espace de travail (SPC), découvrez quelles menaces pesant sur vos actifs sont atténuées par les contrôles d'atténuation disponibles, en fonction de la Contrôle de la posture de sécurité configuration des différents outils de sécurité.

Surveillance des contrôles d'atténuation

Pour connaître les applications prises en charge pour Contrôle de la posture de sécurité la surveillance des contrôles d'atténuation, reportez-vous à la section Explorer Contrôle de la posture de sécurité.

L'application Contrôle de la posture de sécurité se concentre sur trois problèmes principaux :

- Inventaire des actifs : identification de tous les actifs de votre entreprise, y compris des actifs non gérés ou inconnus.
- Couverture et intégrité des contrôles de sécurité : identification de toute lacune de couverture avec vos contrôles de sécurité
- Visibilité de la vulnérabilité et de l'atténuation des menaces : identification des menaces ou des vulnérabilités de vos actifs qui sont atténuées par les contrôles d'atténuation applicables.

La surveillance des contrôles d'atténuation décrit les fonctionnalités Contrôle de la posture de sécurité qui relèvent de la visibilité de la vulnérabilité et de l'atténuation des menaces.

Rôles requis :

- admin : installe les applications à partir de et active les modules d'extension ServiceNow® Store (ITOM Discovery).
- SPC Groupe d'administrateurs et SPC groupe d'analystes : les utilisateurs de ce groupe disposent d'un accès complet en lecture et en écriture à tous les enregistrements du produit et de l'espace de travail.
- SPC Groupe d'analystes en lecture seule : les utilisateurs de ce groupe ont un accès en lecture complet à tous les enregistrements du produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles d'atténuation surveillant les utilisateurs et les avantages

Utilisateurs

Utilisateur	Description
Équipes de cybersécurité, analystes et responsables de la sécurité	• Gagnez en visibilité sur tous les actifs de votre entreprise, y compris des actifs non gérés ou inconnus. • Identifiez les lacunes de couverture de vos contrôles de sécurité, les combinaisons toxiques de problèmes tels que les vulnérabilités critiques et l'exposition à Internet sur vos actifs, ainsi que les écarts par rapport à vos normes de sécurité internes.
Équipes de gestion de la vulnérabilité	Obtenez un aperçu des mesures d'atténuation disponibles pour les vulnérabilités sur les actifs et ajustez dynamiquement le score de risque pour ces vulnérabilités.
Équipes de défense contre les menaces	Obtenez un aperçu des lacunes dans la configuration des atténuations ou des contrôles de sécurité par rapport à des techniques d'attaque spécifiques.

Contrôle de la posture de sécurité et le workflow de surveillance des contrôles d'atténuation

Contrôle de la posture de sécurité utilise des intégrations d'API avec des outils de sécurité tels que des pare-feu d'application Web et des outils de protection des points de terminaison pour importer des données de configuration supplémentaires sur vos actifs et les analyser afin d'identifier les contrôles d'atténuation applicables à un actif donné. Ces intégrations d'API sont distinctes des intégrations de connecteur du graphe de services qui sont prises en charge par SPC des données différentes et importent différentes. Vous configurez ces intégrations d'API à partir de l'espace de SPC travail.

Les intégrations de connecteur du graphe de services ou ITOM Découverte sont toujours nécessaires pour la surveillance des contrôles d'atténuation. Par exemple, le connecteur du CrowdStrike graphe de services et l'intégration de l'API CrowdStrike prise en charge par SPC doivent être activés pour importer des informations supplémentaires sur les contrôles d'atténuation activés par la configuration de protection CrowdStrike du point de terminaison.

Politiques de contrôles d'atténuation

Les Contrôle de la posture de sécurité applications et Contrôles d'atténuation sont requises pour afficher les contrôles d'atténuation et les politiques de contrôles d'atténuation dans le SPC. Les deux applications sont disponibles dans le ServiceNow Store.

Reportez-vous aux rubriques suivantes pour plus d'informations sur le téléchargement et l'installation d'applications à partir du ServiceNow® Store.

- Télécharger une application à partir de ServiceNow Store pour la première fois
- Installer une Opérations de sécurité intégration

Pour afficher les politiques de contrôles d'atténuation, les utilisateurs du groupe d'administrateurs SPC et du groupe d'analystes SPC peuvent accéder à **Espaces de travail**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

> **Contrôle de la posture de sécurité** > **Politiques et résultats** > **Tous** dans le panneau de navigation de l'espace SPC de travail.

Les politiques de contrôle d'atténuation suivantes sont incluses dans l'application et s'affichent avec les autres SPC politiques :

- Remplacement SEH
- Pulvérisation en tas
- CrowdStrike NULL Page Allocation
- CrowdStrike Forcer DEP
- CrowdStrike Forcer l'ASLR
- Microsoft Protection du flux de contrôle Defender
- Microsoft ASLR de force du défenseur
- Microsoft ASLR obligatoire de Defender et ASLR ascendante
- Contrôle d'application SentinelOne
- Fichiers de données SentinelOne
- Exécutables SentinelOne
- SentinelOne Exploits
- SentinelOne IDR
- Détection des menaces interactives SentinelOne
- SentinelOne Détecter les mouvements latéraux
- IA statique SentinelOne
- IA statique SentinelOne : suspect
- Applications potentiellement indésirables SentinelOne
- Shell à distance SentinelOne
- Réputation de SentinelOne

Catégories de contrôles d'atténuation

Les catégories suivantes de contrôles d'atténuation sont actuellement prises en charge avec le SPC.

- Contrôles et politiques d'atténuation requis pour la protection contre les exploits (EDR) Contrôles d'atténuation.
- Contrôles d'atténuation de la protection contre les exploits (WAF). Vous devez créer des politiques pour AWS WAF. Consultez Créer une politique pour l'intégration WAF afin de surveiller les AWS contrôles d'atténuation pour plus d'informations.

Contrôles et politiques d'atténuation requis pour la protection contre les exploits (EDR) Contrôles d'atténuation

Cette catégorie de contrôles d'atténuation couvre les mesures d'atténuation disponibles sur vos actifs sous la forme d'une configuration de l'agent de protection du point de terminaison. Cela s'applique aux agents de protection des terminaux tels que CrowdStrike et SentinelOne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les paramètres d'atténuation des exploits tels que « Forcer la randomisation de la disposition de l'espace d'adressage » et « Forcer DEP » peuvent être activés dans les outils de protection des points de terminaison tels que CrowdStrike. SPC détecte automatiquement cette configuration sur les appareils à l'aide des politiques incluses dans l'application et de l'intégration de l'API avec les outils de protection des points de terminaison.

Rôles requis : SPC Groupe d'administration et SPC Groupe d'analystes.

Conditions préalables à CrowdStrike la détection des contrôles d'atténuation de la protection des exploits (EDR)

1. Vérifiez que vous avez activé le CrowdStrike connecteur du graphe de services. Cette application est disponible dans le ServiceNow Store. Les informations d'installation et de configuration sont incluses dans la liste des applications. Consultez Installer et configurer les intégrations pour la surveillance des contrôles d'atténuation CrowdStrike pour plus d'informations.
2. Vérifiez que l'intégration de l'API CrowdStrike est activée dans l'espace Contrôle de la posture de sécurité de travail.

Conditions préalables à Microsoft la détection des contrôles d'atténuation de la protection des exploits (EDR)

Microsoft Informations d'identification SCCM incluant le rôle d'auteur de script. Le rôle d'auteur de script fournit les autorisations requises pour créer un script nécessaire pour importer des informations d'atténuation sur le serveur SCCM.

Vous devez activer l'intégration SCCM pour identifier les contrôles d'atténuation configurés dans Microsoft Defender.

Consultez Installer et configurer le connecteur du graphe de services pour Microsoft SCCM et l'intégration du contrôle d'atténuation de Microsoft Defender pour plus d'informations.

- Defender – Atténuation des exploits – CFG

  Microsoft Protection du flux de contrôle Defender.

- Defender – Atténuation des exploits – DEP

  Microsoft Prévention de l'exécution des données Defender.

- Defender – Atténuation des exploits – ASLR obligatoire et ASLR ascendante

  Microsoft Défenseur force ASLR.

- MITRE Tactiques abordées : accès initial, exécution, accès aux informations d'identification, évasion de la défense, escalade de privilèges, mouvement latéral.

1. Vérifiez que vous avez activé le connecteur du graphe de services SentinelOne.

   Cette application est disponible dans le ServiceNow Store. Les informations d'installation et de configuration sont incluses dans la liste des applications. Consultez Installez et configurez le Connecteur du graphe de services pour SentinelOne et l'intégration du contrôle d'atténuation SentinelOne pour plus d'informations.

2. Vérifiez que l'intégration de l'API SentinelOne est activée dans l'espace de travail Contrôle de la posture de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer et configurer les intégrations pour la surveillance des contrôles d'atténuation CrowdStrike

Le CrowdStrike connecteur du graphe de services et les intégrations d'API nécessitent des étapes de configuration distinctes. Vous configurez le connecteur du graphe de services pour importer les détails des CrowdStrike actifs. Vous configurez l'intégration d'API pour collecter des données d'atténuation CrowdStrike sur les actifs surveillés par CrowdStrike.

Avant de commencer

- Vérifiez que vous avez installé et activé les applications Contrôle de la posture de sécurité et Surveillance des contrôles d'atténuation dans votre instance. Ces applications sont disponibles dans le ServiceNow Store.
- Connecteur CrowdStrike du graphe de services doit être installé et configuré avant de configurer l'intégration de l'API CrowdStrike .

Rôles requis : administrateur pour l'installation des modules d'extension, et Groupe d'administrateurs SPC et Groupe d'analystes SPC pour la configuration des intégrations dans l'espace de travail.

Procédure

1. Pour installer et configurer l'intégration de Connecteur du CrowdStrike graphe de services, procédez comme suit :

   Remarque : Si vous avez installé Connecteur du graphe de services pour CrowdStrike, passez à l'étape 2 pour savoir comment configurer l'intégration de l'API CrowdStrike .

   a. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Onglet Connecteurs du graphe de services**.

   b. Localisez le connecteur du graphe de services Protection du point de CrowdStrike terminaison.

   c. Sélectionnez le lien qui vous redirige vers la liste d'applications pour Connecteur du graphe de services pour CrowdStrike dans le ServiceNow® Store.

   d. Suivez les invites pour installer l'application.

   e. Téléchargez le guide d'installation à partir de la section Liens et documents de support de la liste des applications avant de quitter pour vous aider dans la configuration et l'activation.

   f. Accédez à la **CrowdStrike** > **Configuration** dans votre instance.

   g. Suivez les invites de la configuration guidée et reportez-vous à la documentation pour configurer et activer le SGC.

2. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Intégrations d'API SPC**.

   Cet onglet répertorie les sources de contrôles d'atténuation (CrowdStrike, F5 Big IP et SCCM), et l'onglet n'est affiché dans l'espace de travail que si vous avez installé l'application Monitoring des contrôles d'atténuation.

   Sur les cartes sources, vous pouvez afficher l'état de la source d'atténuation (active ou inactive) et le nombre de contrôles d'atténuation et de leurs politiques associées qui sont surveillés par CrowdStrike (6). Vous pouvez sélectionner le nombre pour afficher la liste.

   Notez que la colonne Actif dans Sources affiche Actif. Cela indique que la source (CrowdStrike SGC) est active, mais vous devez configurer l'intégration de l'API avant de pouvoir surveiller les contrôles d'atténuation CrowdStrike .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **Suivant**.
4. Sélectionnez CrowdStrike dans la colonne Nom.
5. Sélectionnez Modifier et remplissez les champs.

> **Remarque :** Entrez les mêmes informations de compte et de serveur CrowdStrike pour l'intégration d'API que vous avez fournies pour Connecteur du CrowdStrike graphe de services. Ces informations vous assurent d'importer des données d'atténuation qui correspondent aux données d'actif que vous avez importées avec Connecteur du graphe de services.

Champ	Description
Nom	Nom d'instance. Vous pouvez modifier ce nom pour vous aider à enregistrer les informations d'identification sans les tester. Si vous modifiez des champs sous le champ Nom, vous devez tester la connexion avant d'enregistrer et de quitter.
Limite de taille de l'actif	Nombre d'actifs surveillés.
ID client	ID CrowdStrike
Secret client	CrowdStrike Secret
URL D'API	URL d'API, par exemple, https://api.crowdstrike.com

6. Lorsque vous êtes prêt, sélectionnez **Tester la connexion**.
   Un message s'affiche si la connexion aboutit.
7. Sélectionnez **Enregistrer et quitter**.
8. Sélectionnez **Afficher les détails** sur la CrowdStrike carte dans l'onglet Intégrations d'API SPC et notez que la source et l'API sont activées et que la barre de progression de la configuration est terminée.
9. **Facultatif :** Si le test des informations d'identification échoue, vous pouvez sélectionner **Revenir aux informations d'identification précédentes** pour insérer les informations d'identification que vous avez précédemment validées.
10. Suivez ces étapes pour exécuter les CrowdStrike intégrations.

    a. Accédez à la **Contrôle d'atténuation de CrowdStrike** > **Intégrations**.
    Il existe trois intégrations :

    - CrowdStrike Intégration de la politique de prévention
    - CrowdStrike Intégration de la politique de contrôle des appareils
    - CrowdStrike Intégration des aperçus des actifs

    Les intégrations sont enchaînées et s'exécutent dans un ordre spécifique. La réussite d'une intégration initie la suivante.

    b. Sélectionnez l'intégration de la CrowdStrike politique de prévention dans la colonne Nom pour lancer les exécutions d'intégration.

    c. Sur l'enregistrement, cochez la case **Actif** , puis sélectionnez **Exécuter maintenant**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez afficher l'état de l'exécution de l'intégration dans l'onglet Exécution de l'intégration à partir des enregistrements d'intégration.

L'intégration est planifiée pour s'exécuter quotidiennement par défaut.

L'intégration CrowdStrike de l'aperçu des actifs importe uniquement les informations sur les actifs qui ont changé depuis la dernière exécution de l'intégration. L'intégration CrowdStrike de la politique de contrôle des appareils et l'intégration de la CrowdStrike politique de prévention importent toutes les données pour chaque exécution.

Installer et configurer le connecteur du graphe de services pour Microsoft SCCM et l'intégration du contrôle d'atténuation de Microsoft Defender

Le connecteur du graphe de services pour SCCM et l'intégration du contrôle d'atténuation de Microsoft Defender nécessitent des étapes de configuration distinctes.

Avant de commencer
Vous devez installer, activer et configurer Service Graph Connector for SCCM pour importer les détails des actifs. Vous configurez l'intégration des contrôles d'atténuation de Microsoft Defender, qui utilise également SCCM, pour collecter des données supplémentaires sur les contrôles d'atténuation configurés sur les actifs surveillés par Service Graph Connector for SCCM.

Rôles requis :

- administrateur pour l'installation et l'activation des modules d'extension
- Groupe d'administrateurs SPC et groupe d'analystes SPC pour la configuration des intégrations dans l'espace de travail
- Informations d'identification Microsoft SCCM incluant le rôle Auteur de script. Le rôle d'auteur de script fournit les autorisations requises pour créer un script nécessaire pour importer des informations d'atténuation sur le serveur SCCM.

Remarque : Ce rôle doit être créé et affecté avec les autorisations suivantes :

Rôle d'auteur de script

Catégorie	Autorisation	État
Collection	Exécuter le script	Non
Site	Lire	Oui
SMS Scripts	Créer	Oui
SMS Scripts	Lire	Oui
SMS Scripts	Supprimer	Oui
SMS Scripts	Modifier	Oui

- Informations d'identification Microsoft SCCM incluant le rôle d'approbateurs de script. Le script créé pour importer les informations d'atténuation nécessite une approbation dans votre console Microsoft SCCM par l'utilisateur disposant du rôle Approbateurs de script.

Remarque : Ce rôle doit être créé et affecté avec les autorisations suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Approbateur de script

Catégorie	Autorisation	État
Collection	Exécuter le script	Non
Site	Lire	Oui
SMS Scripts	Lire	Oui
SMS Scripts	Approuver	Oui
SMS Scripts	Modifier	Oui

Procédure

1. Pour installer et configurer Connecteur du graphe de services pour Microsoft SCCM Integration, procédez comme suit :

   Remarque : Si vous avez installé Connecteur du graphe de services pour l'intégration Microsoft SCCM, passez à l'étape 2 pour configurer l'intégration du contrôle d'atténuation de Microsoft Defender.

   a. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Onglet Connecteurs du graphe de services**.

   b. Localisez Connecteur du graphe de services pour Microsoft SCCM Integration.

   c. Sélectionnez le lien qui vous dirige vers la liste des applications dans le ServiceNow® Store.

   d. Suivez les invites pour installer l'application.

   e. Téléchargez le guide d'installation à partir de la section Liens et documents de support de la liste des applications avant de quitter pour vous aider dans la configuration et l'activation.

   f. Accédez à la **Configuration** dans votre instance.

   g. Suivez les invites de la configuration guidée et reportez-vous à la documentation pour configurer et activer le SGC.

2. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Intégrations d'API SPC** pour configurer l'intégration du contrôle d'atténuation de Microsoft Defender.

   Cet onglet répertorie les sources de contrôles d'atténuation (CrowdStrike, F5 Big IP et Defender), et l'onglet s'affiche dans l'espace de travail uniquement si vous avez installé l'application Surveillance des contrôles d'atténuation.

   Sur les cartes sources, vous pouvez afficher l'état de la source d'atténuation (active ou inactive).

   Notez que la colonne Actif dans Sources affiche Actif. Cela indique que la source (Connecteur du graphe de services pour Microsoft SCCM) est active pour récupérer les données d'actif, mais vous devez configurer l'intégration du contrôle d'atténuation de Microsoft Defender qui récupère les données supplémentaires sur les configurations de Defender sur ces actifs à l'aide de SCCM avant de pouvoir surveiller les contrôles d'atténuation.

3. Sélectionnez **Suivant**.
   La page Configuration SCCM s'affiche avec un lien d'instance de contrôle d'atténuation Microsoft SCCM.

4. Sélectionnez le lien d'instance fourni dans la colonne Nom.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Renseignez les champs de configuration des informations d'identification SCCM Modal d'intégration du contrôle d'atténuation SCCM Microsoft.

Champ	Description
Nom	Le champ est renseigné automatiquement avec le nom de l'instance.
Connexion	Champ renseigné automatiquement avec les informations de connexion.
Hôte	Nom d'hôte du serveur SCCM dans les informations de connexion fournies dans le champ précédent.
Nom d'utilisateur	Nom d'utilisateur permettant d'accéder au serveur SCCM.
Mot de passe	Mot de passe permettant d'accéder au serveur SCCM.
Serveur MID	Sélectionnez un serveur MID géré par ServiceNow dans la liste.
État de validation	Champ renseigné après tentative de validation. Si la connexion réussit, l'état de l'instance d'intégration est **Valide**.
Connexion du connecteur SG	Sélectionnez une option Alias de connexion et d'informations d'identification dans la liste pour Connecteur du graphe de services pour Microsoft SCCM. Vous avez configuré cette connexion pendant les étapes de configuration guidée pour Microsoft SCCM SGC.
Détail de validation	Détails de la tentative de validation.

6. Sélectionnez **Enregistrer et tester les informations d'identification**.
   Une réponse valide pour une connexion réussie est requise pour passer à l'étape suivante.
7. Sélectionnez **Suivant**.
   Un script PowerShell est créé automatiquement pour récupérer les détails de l'atténuation. Une fenêtre modale s'affiche avec l'option Valider l'approbation de script.
8. Pour approuver le script, connectez-vous à votre console Microsoft SCCM avec le rôle d'approbateur de script.

   Un script PowerShell a été généré dans votre gestionnaire de configuration SCCM pour récupérer les détails de l'atténuation. Vous devez vous connecter avec les informations d'identification appropriées avec un rôle d'utilisateur qui a l'autorisation d'approbateur de script afin d'approuver le script. Une fois approuvé, vous pouvez le valider dans votre ServiceNow AI Platform instance.

9. Dans votre console, recherchez le script **[ServiceNow Secops] : Get System Mitigations** et approuvez-le.

Traduction automatique

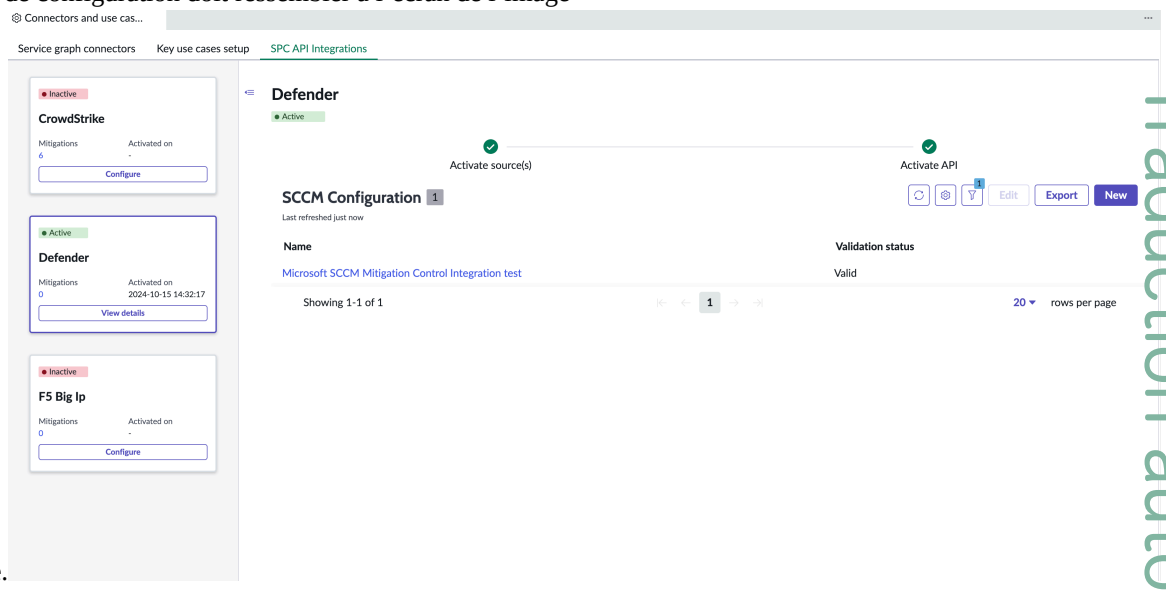
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Dans votre gestionnaire de configuration SCCM, la section Script se trouve sous la bibliothèque de logiciels. Localiser : [ServiceNow Secops] : obtenez l'approbation du script d'atténuations du système.

Ce script reste à l'état **En attente d'approbation** jusqu'à ce que vous l'approuviez.

Vous pouvez valider le script dans votre ServiceNow AI Platform instance sans l'approuver comme décrit ci-dessus, mais le message d'erreur Le script n'est pas approuvé s'affiche.

10. Pour valider l'approbation, revenez à votre ServiceNow AI Platform instance et, dans le modal de script Approuver PowerShell, sélectionnez **Valider l'approbation de script**.
11. Sélectionnez **Terminé**.
    La page de configuration doit ressembler à l'écran de l'image suivante.



Créer plusieurs instances pour l'intégration du contrôle d'atténuation de Microsoft Defender

Vous pouvez configurer plusieurs instances pour l'intégration du contrôle d'atténuation de Microsoft Defender.

Avant de commencer

Rôles requis :

- Groupe d'administrateurs SPC et groupe d'analystes SPC pour la configuration de nouvelles instances d'intégration dans l'espace de travail
- Informations d'identification Microsoft SCCM incluant le rôle Auteur de script. Le rôle d'auteur de script fournit les autorisations requises pour créer un script nécessaire pour importer des informations d'atténuation sur le serveur SCCM.

Remarque : Ce rôle doit être créé et affecté avec les autorisations suivantes :

Rôle d'auteur de script

Catégorie	Autorisation	État
Collection	Exécuter le script	Non
Site	Lire	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catégorie	Autorisation	État
SMS Scripts	Créer	Oui
SMS Scripts	Lire	Oui
SMS Scripts	Supprimer	Oui
SMS Scripts	Modifier	Oui

- Informations d'identification Microsoft SCCM incluant le rôle d'approbateurs de script. Le script créé pour importer les informations d'atténuation nécessite une approbation dans votre console Microsoft SCCM par l'utilisateur disposant du rôle Approbateurs de script.

Remarque : Ce rôle doit être créé et affecté avec les autorisations suivantes :

Approbateur de script

Catégorie	Autorisation	État
Collection	Exécuter le script	Non
Site	Lire	Oui
SMS Scripts	Lire	Oui
SMS Scripts	Approuver	Oui
SMS Scripts	Modifier	Oui

Procédure

1. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Intégrations d'API SPC**.
2. Sélectionnez **Nouveau**.
   Le modal Nouvelle instance de Defender s'affiche.
3. Donnez un nom à votre nouvelle instance et sélectionnez **Créer une instance**.
   La page Intégrations d'API SPC s'affiche avec l'instance fournie avec l'application et votre nouvelle instance.
4. Sélectionnez le lien de votre nouvelle instance.
5. Renseignez les champs du modal de configuration des informations d'identification SCCM pour votre nouvelle instance.

Champ	Description
Nom	Le champ est renseigné automatiquement avec le nom de l'instance.
Connexion	Créez une nouvelle connexion. a. Sélectionnez **Créer une connexion et un alias** en haut de la fenêtre modale. b. Dans le formulaire Alias de connexion et d'informations d'identification, renseignez les champs obligatoires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ **Nom** : nom unique ▪ **Type** : connexion et informations d'identification ▪ **Type de connexion** : de base **Remarque :** Ne sélectionnez pas **Soumettre** pour l'instant. **c.** Cliquez avec le bouton droit n'importe où dans l'en-tête gris et sélectionnez **Enregistrer**. La page s'actualise et les liens et onglets connexes s'affichent en bas de la page après son enregistrement. **d.** Une fois l'onglet Connexions sélectionné, sélectionnez **Nouveau** à droite de l'onglet. Le formulaire Connexion s'affiche. Remplissez les champs. ▪ **Nom** : nom unique ▪ Informations d'identification : sélectionnez l'icône de recherche. Recherchez les informations d'identification Windows et sélectionnez le lien. Renseignez les champs du formulaire Informations d'identification Windows. ▪ **Nom** : nom unique ▪ Nom d'utilisateur : nom d'utilisateur correspondant aux informations d'identification. Il s'agit du nom d'utilisateur qui sera référencé pour le champ Nom d'utilisateur dans le modal de configuration des informations d'identification SCCM après son enregistrement sur cette page. ▪ Mot de passe : mot de passe pour les informations d'identification. Il s'agit du mot de passe qui sera référencé pour le champ Mot de passe dans la fenêtre modale de configuration des informations d'identification SCCM après son enregistrement sur cette page. ▪ Hôte : il s'agit de l'hôte du serveur SCCM qui sera référencé dans le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	champ Hôte de la fenêtre modale de configuration des informations d'identification SCCM après son enregistrement sur cette page. **e.** Cochez la case **Utiliser Serveur MID** . Sélectionnez un serveur MID spécifique pour la **sélection de MID** et sélectionnez-en un dans la liste de Serveur MID. **f.** Cliquez avec le bouton droit n'importe où dans l'en-tête gris et sélectionnez **Enregistrer**. Il s'agit des informations d'identification que vous entrez sur le formulaire de connexion décrit ci-dessus à l'étape d.
Hôte	Il s'agit de l'hôte du serveur SCCM référencé dans le champ Hôte après l'avoir enregistré sur la page Connexion, comme décrit ci-dessus.
Nom d'utilisateur	Il s'agit du nom d'utilisateur référencé à partir du champ Nom d'utilisateur après l'avoir enregistré sur la page Connexion, comme décrit ci-dessus.
Mot de passe	Il s'agit du mot de passe référencé dans le champ Mot de passe après l'avoir enregistré sur la page Connexion comme décrit ci-dessus.
Serveur MID	Il s'agit du serveur MID référencé à partir des champs de serveur MID après son enregistrement sur la page Connexion, comme décrit ci-dessus.
État de validation	Champ renseigné après tentative de validation. Si la connexion réussit, l'état de l'instance d'intégration est **Valide**.
Connexion du connecteur SG	Sélectionnez une option Alias de connexion et d'informations d'identification dans la liste pour Connecteur du graphe de services pour Microsoft SCCM. Vous avez configuré cette connexion pendant les étapes de configuration guidée pour Microsoft SCCM SGC.
Détail de validation	Détails de la tentative de validation.

Traduction automatique

6. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Intégrations d'API SPC**.
7. Sélectionnez le lien de votre nouvelle instance.
8. Dans la fenêtre modale de configuration des informations d'identification SCCM, sélectionnez la connexion dans la liste que vous avez créée à l'étape 5 pour le champ Connexion.

   Notez que les champs répertoriés ci-dessous sont renseignés automatiquement en fonction des informations que vous avez saisies pour votre nouvelle connexion.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Hôte	Il s'agit de l'hôte du serveur SCCM référencé dans le champ Hôte après l'avoir enregistré sur la page Connexion, comme décrit ci-dessus.
Nom d'utilisateur	Il s'agit du nom d'utilisateur référencé à partir du champ Nom d'utilisateur après l'avoir enregistré sur la page Connexion, comme décrit ci-dessus.
Mot de passe	Il s'agit du mot de passe référencé dans le champ Mot de passe après l'avoir enregistré sur la page Connexion comme décrit ci-dessus.
Serveur MID	Il s'agit du serveur MID référencé à partir des champs de serveur MID après son enregistrement sur la page Connexion, comme décrit ci-dessus.
État de validation	Champ renseigné après tentative de validation. Si la connexion réussit, l'état de l'instance d'intégration est **Valide**.
Connexion du connecteur SG	Sélectionnez une option Alias de connexion et d'informations d'identification dans la liste.
Détail de validation	Détails de la tentative de validation.

9. Sélectionnez **Enregistrer et tester les informations d'identification**.
   Une réponse valide pour une connexion réussie est requise pour passer à l'étape suivante.
10. Sélectionnez **Suivant**.
    Le script PowerShell est créé comme décrit dans .Installer et configurer le connecteur du graphe de services pour Microsoft SCCM et l'intégration du contrôle d'atténuation de Microsoft Defender Suivez les étapes de cette rubrique pour approuver les scripts de vos nouvelles instances.

Installez et configurez le Connecteur du graphe de services pour SentinelOne et l'intégration du contrôle d'atténuation SentinelOne

L'intégration Connecteur du graphe de services pour SentinelOne et l'intégration SentinelOne pour l'intégration du contrôle d'atténuation nécessitent des étapes de configuration distinctes. Vous installez et configurez le pour importer les détails de l'actif Connecteur du graphe de services pour SentinelOne . Vous configurez SentinelOne Integration for Mitigation Control Integration pour collecter des données d'atténuation sur les actifs surveillés par le Connecteur du graphe de services pour SentinelOne.

Avant de commencer

Rôles requis :

- Administrateur pour l'installation et l'activation des modules d'extension.
- Groupe d'administrateurs SPC et groupe d'analystes SPC pour la configuration des intégrations dans l'espace de travail.
- Informations d'identification SentinelOne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour installer et configurer l'intégration Connecteur du graphe de services pour SentinelOne , procédez comme suit :

   Remarque : Si vous avez installé Service Graph Connector for SentinelOne, passez à l'étape 2 pour configurer l'intégration SentinelOne pour l'intégration du contrôle d'atténuation.

   a. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Onglet Connecteurs du graphe de services**.

   b. Localisez l'intégration Connecteur du graphe de services pour SentinelOne .

   c. Sélectionnez le lien qui vous dirige vers la liste des applications dans le ServiceNow® Store.

   d. Suivez les invites pour installer l'application.

   e. Téléchargez le guide d'installation à partir de la section Liens et documents de support de la liste des applications avant de quitter pour vous aider dans la configuration et l'activation.

   f. Accédez à la **Configuration** dans votre instance.

   g. Suivez les invites de la configuration guidée et reportez-vous à la documentation pour configurer et activer le SGC.

2. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Intégrations d'API SPC** pour configurer l'intégration SentinelOne pour l'intégration du contrôle d'atténuation.

   Cet onglet répertorie les sources de contrôles d'atténuation : CrowdStrike, F5 Big IP, Defender, SentinelOne. L'onglet s'affiche dans l'espace de travail uniquement si vous avez installé l'application Surveillance des contrôles d'atténuation.

   Sur les cartes sources, vous pouvez afficher l'état de la source d'atténuation (active ou inactive).

   Notez que la colonne Actif dans Sources affiche Actif. Cela indique que la source, dans ce cas, est Connecteur du graphe de services pour SentinelOne active pour récupérer les données d'actif, mais vous devez configurer l'intégration SentinelOne pour l'intégration du contrôle d'atténuation avant de pouvoir surveiller les contrôles d'atténuation sur les actifs importés.

3. Sélectionnez **Suivant**.
   La page de configuration SentinelOne s'affiche avec un lien d'instance d'intégration SentinelOne pour le contrôle d'atténuation.

4. Sélectionnez le lien d'instance fourni dans la colonne Nom.

5. Renseignez les champs de l'intégration SentinelOne pour l'intégration du contrôle d'atténuation.

   Remarque :

   Saisissez les mêmes informations de compte SentinelOne et les mêmes détails du serveur pour l'intégration SentinelOne pour l'intégration du contrôle d'atténuation que vous avez fournis pour le Connecteur du graphe de services pour SentinelOne. Ces informations vous assurent d'importer des données d'atténuation qui correspondent aux données d'actif que vous avez importées avec Connecteur du graphe de services.

   Sélectionnez l'icône du stylo si vous devez modifier les champs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom d'instance	Le champ est renseigné automatiquement avec le nom de l'instance.
Clé API	Champ renseigné automatiquement avec les informations de clé API.
URL D'API	Nom d'hôte du serveur SentinelOne, par exemple : https//usea1-na.sentinelone.net

6. Sélectionnez **Enregistrer et tester les informations d'identification**.
   Une réponse valide pour une connexion réussie est requise pour passer à l'étape suivante.
7. Sélectionnez **Enregistrer et quitter**.
8. Sélectionnez **Afficher les détails** sur la carte SentinelOne dans l'onglet Intégrations d'API SPC.
   Notez que la source et l'API sont activées et que la barre de progression de la configuration est terminée.
9. **Facultatif :** Sélectionnez **Revenir aux informations d'identification précédentes** pour insérer les informations d'identification que vous avez précédemment validées.
10. Suivez ces étapes pour exécuter l'intégration d'importation d'actifs SentinelOne.

    a. Accédez à la **Contrôle d'atténuation de SentinelOne** > **Intégrations**.
    Il existe une intégration : SGC SentinelOne Asset Import.

    b. Sélectionnez l'intégration de la **politique de prévention SentinelOne** dans la colonne Nom pour lancer l'intégration.

    c. Sur l'enregistrement, cochez la case **Actif** , puis sélectionnez **Exécuter maintenant**.

    Vous pouvez afficher l'état de l'exécution de l'intégration dans l'onglet **Exécution de l'intégration** à partir des enregistrements d'intégration.

    L'intégration est planifiée pour s'exécuter quotidiennement par défaut.

    L'intégration d'importation d'actifs SentinelOne importe uniquement les informations sur les actifs qui ont changé depuis la dernière exécution de l'intégration.

Contrôles d'atténuation de la protection contre les exploits (WAF)

Cette catégorie de contrôles d'atténuation couvre les mesures d'atténuation disponibles sous la forme d'un pare-feu d'application Web.

Protection contre les exploits (WAF)

Contrôle de la posture de sécurité détecte les serveurs qui s'exécutent derrière le pare-feu d'application Web (WAF) à l'aide de l'intégration de l'API avec des outils WAF tels que F5 BIG-IP (F5) et les données de trafic réseau de Discovery basée sur IP ITOM, si nécessaire.

Contrôle d'atténuation importe les règles ACL Web et tous les équilibreurs de charge associés pour déterminer quelles règles protègent vos ordinateurs virtuels à l'aide des modèles Détection et Mappage des services.

Rôles requis : SPC Groupe d'administration et SPC Groupe d'analystes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions préalables à la protection contre les exploits (WAF) avec F5 BIG-IP

1. Vérifiez que vous avez activé la découverte basée sur IP ITOM dans l'environnement où F5 BIG-IP F5 WAF et les serveurs d'applications associés sont installés.
2. Vérifiez que l'intégration de l'API pour F5 BIG-IP F5 est activée dans l'espace Contrôle de la posture de sécurité de travail.

Conditions préalables à la protection contre les exploits (WAF) avec Amazon Web Services AWS

Les données de cette intégration sont importées par les applications Modèles de découverte et de mappage des services [sn_itom_pattern] et Surveillance des contrôles d'atténuation [sn_sec_mit_ctrl]. Les deux applications sont requises. Suivez les étapes ci-dessous dans l'ordre dans lequel elles sont répertoriées afin de pouvoir importer toutes les ACL Web, les règles ACL Web et les données d'atténuation requises pour vous aider à confirmer qu'un ordinateur virtuel est protégé. Reportez-vous à la section AWS Découverte à l'aide de schémas pour plus d'informations sur les modèles de AWS détection.

1. Définissez les ACL et les règles Web dans le compte de service que vous AWS souhaitez utiliser. Pour plus d'informations, consultez Utilisation d'ACL Web dans AWS WAF .

   Remarque : Vous pouvez créer vos propres règles d'ACL Web, mais vous préférez peut-être utiliser les AWS règles gérées qui sont conçues spécifiquement pour fonctionner avec leurs ACL Web. Si vous choisissez de créer vos propres règles personnalisées pour les ACL Web, notez que cette intégration à AWS WAF ne prend en charge que les types d'attaques qui correspondent aux attaques par injection Contient SQL et aux attaques par injection Contient XSS (script de site à site). Les équilibreurs de charge sont les actifs (ressources) pris en charge par cette intégration.

2. Installez et activez l'application Schémas de détection et de mappage des services [sn_itom_pattern] dans votre instance afin que les noms et les actions par défaut des ACL Web que vous avez définis à l'étape 1 puissent être détectés. Pour plus d'informations, consultez Installer les applications prises en charge pour Contrôle de la posture de sécurité.
3. Vérifiez que la propriété système du serveur MID sn_itom_pattern.discover_aws_app_pool_members est définie sur vrai. Pour activer cette propriété, accédez à **Tous** > **Serveur MID** > **Propriétés**.
4. Vérifiez que vous avez installé et activé l'application Surveillance des contrôles d'atténuation [sn_sec_mit_ctrl]. Cette application inclut une extension de modèle, des règles ACL Web et des ressources associées. Cette extension de modèle vous permet d'importer les règles ACL Web réelles et leurs associations (relations) à vos ressources (actifs) dans votre instance.

Configurer les intégrations pour la surveillance des contrôles d'atténuation F5 BIG-IP

L'application Découverte basée sur IP ITOM et les intégrations d'API F5 BIG-IP nécessitent des étapes de configuration distinctes. Vous configurez l'application Découverte basée sur IP ITOM pour importer les détails des actifs. Vous configurez l'intégration d'API pour recueillir des données d'atténuation F5 BIG-IP sur les actifs qui sont surveillés par la découverte basée sur IP ITOM.

Avant de commencer

- La découverte basée sur IP ITOM doit être opérationnelle dans l'environnement où F5 BIG-IP tous les serveurs d'applications associés sont configurés.
- Pour les actifs sur site, vous devez fournir un Serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez la source (ITOM) pour collecter des données sur les actifs surveillés.
- Activez l'intégration d'API pour collecter des données d'atténuation sur les actifs.

Rôles requis : administrateur pour l'installation des modules d'extension et la création des propriétés système, et SPC Groupe d'administrateurs et SPC Groupe d'analystes pour la configuration des intégrations dans l'espace de travail.

Procédure

1. Pour installer et configurer l'intégration, procédez comme suit :

   Remarque : Si vous avez installé et activé ITOM, passez à l'étape 2 pour savoir comment configurer l'intégration de l'API F5 BIG-IP (F5).

   a. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Onglet Connecteurs du graphe de services**.

   b. Sélectionnez la F5 BIG-IP carte.

   c. Sélectionnez le lien du **module d'extension ITOM pour** activer le module d'extension ITOM.

   d. Suivez les instructions.

2. Accédez à la **Configuration des connecteurs et des tickets d'utilisation** > **Intégrations d'API SPC**.

   Cet onglet répertorie les sources de contrôles d'atténuation (CrowdStrike et F5 Big IP et SCCM), et l'onglet n'est affiché dans l'espace de travail que si vous avez installé l'application Surveillance des contrôles d'atténuation.

   Sur les cartes sources, vous pouvez afficher l'état de la source d'atténuation (active ou inactive).

3. Sélectionnez **Suivant**.

   Notez que la source (ITOM) est active, mais vous devez configurer et activer l'intégration de l'API avant de pouvoir surveiller les contrôles d'atténuation F5 BIG-IP .

4. Sélectionnez F5 BIG-IP dans la colonne Nom.

5. Sélectionnez Modifier et remplissez les champs.

Champ	Description
Nom	Nom d'instance. Vous pouvez modifier ce nom pour vous aider à enregistrer les informations d'identification sans les tester. Si vous modifiez des champs sous le champ Nom, vous devez tester la connexion avant d'enregistrer et de quitter.
Nom d'utilisateur	Nom d'utilisateur F5 BIG-IP
Mot de passe	F5 BIG-IP mot de passe.
Serveur MID	Sélectionnez un serveur MID dans la liste.
URL D'API	URL d'API avec le port 8443, par exemple, https://bigip.example.com:8443.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Lorsque vous êtes prêt, sélectionnez **Tester la connexion**.
   Un message s'affiche si la connexion aboutit.

   Si l'erreur suivante résulte du test de la connexion pendant les étapes de configuration, la session ne contient aucun certificat - Non approuvé : La session ne contient aucun certificat - Non approuvé, définissez les propriétés système suivantes sur `faux` :

   - com.glide.communications.httpclient.verify_hostname
   - com.glide.communications.httpclient.verify_revoked_certificate

   Un utilisateur disposant du rôle administrateur doit créer ces propriétés système dans le champ d'application global si elles ne sont pas répertoriées dans la table Propriétés système [sys_properties]. Les propriétés système sont Type, Vrai/Faux (booléen).

7. Sélectionnez **Enregistrer et quitter**.
8. Sur la F5 BIG-IP carte dans l'onglet Intégrations d'API SPC et notez que la source et l'API sont activées et que la barre de progression de la configuration est terminée.
9. **Facultatif :** Si le test des informations d'identification échoue, vous pouvez sélectionner **Revenir aux informations d'identification précédentes** pour insérer les informations d'identification que vous avez précédemment validées.
10. Pour exécuter les intégrations d'API, procédez comme suit :

    a. Accédez à la **Contrôle d'atténuation de F5 Big-IP** > **Intégrations**

       Il y a cinq intégrations. Les intégrations sont enchaînées et s'exécutent dans un ordre spécifique. La réussite d'une intégration lance la suivante :

       - Intégration d'appareil F5 Big IP
       - Intégration de la politique F5 Big IP
       - Intégration de signature d'attaque F5 Big IP
       - Intégration de serveur virtuel F5 Big IP
       - Intégration de membre du pool F5 Big IP

    b. Pour lancer la chaîne d'intégration, sélectionnez **l'intégration de l'appareil F5 Big IP** dans la colonne Nom.

    c. Sur l'enregistrement, cochez la case **Actif** , puis sélectionnez **Exécuter maintenant**.

    d. Affichez l'état des exécutions d'intégration dans l'onglet Exécution de l'intégration à partir des enregistrements d'intégration.
       L'intégration est planifiée pour s'exécuter quotidiennement par défaut.

Configurer l'intégration WAF pour la surveillance des contrôles d'atténuation AWS

Déterminez si vos machines virtuelles sont protégées avec l'intégration WAF pour la surveillance des contrôles d'atténuation AWS .

Avant de commencer
Les données sont importées par deux applications distinctes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'application Schémas de détection et de mappage des services importe les noms et les actions par défaut, autoriser ou bloquer, des ACL Web que vous définissez dans votre AWS compte de service. Le modèle de détection Amazon AWS - Web ACL (LP) est activé avec l'application.
- L'application Surveillance des contrôles d'atténuation importe les règles ACL Web réelles et les relations entre les ressources associées, à l'instar d'un équilibreur de charge d'application. Cette extension est incluse dans le cadre de l'application Surveillance des contrôles d'atténuation.

Vérifiez que vous avez terminé les étapes de définition des ACL et des règles Web et que vous avez activé les applications requises pour l'intégration AWS WAF décrites dans Contrôles d'atténuation de la protection contre les exploits (WAF) avant d'activer les applications.

Rôles requis :

- administrateur pour l'installation des modules d'extension dans votre ServiceNow AI Platform® instance.
- SPC Groupe d'administrateurs pour la configuration des intégrations dans l'espace de travail.
- AWS Informations d'identification AWS du compte de service que vous souhaitez utiliser.

Procédure

1. Accédez à la **Tous** > **Espace de travail Contrôle de la posture de sécurité** > **Configuration des connecteurs et des tickets d'utilisation** > **Onglet Intégrations d'API SPC**.
2. Sélectionnez la vignette **AWS WAF** .
3. Sélectionnez-en un.

Option	Description
Afficher les comptes de services	Affichez les comptes de service disponibles AWS configurés dans votre instance. Pour créer un nouveau compte : **a.** Sélectionnez **Afficher les comptes de services**. **b.** Sélectionnez **Nouveau**. **c.** Renseignez les champs. ▪ Nom : nom de votre AWS compte de service. Il s'agit du compte que vous utilisez pour votre calendrier de découverte et vos informations d'identification. ▪ ID de compte : ID de compte pour votre AWS compte de service. ▪ Type de centre de données : sélectionnez **Centre de données AWS [cmdb_ci_aws_datacenter]** **d.** Sélectionnez **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Configurer le compte de service	Configurez un compte de AWS service dans votre instance.

4. Créez le calendrier de découverte pour le AWS compte de service que vous souhaitez utiliser.

   a. Accédez à la **Tous** > **Découverte** > **Accueil**.

   b. **Sélectionnez Afficher les calendriers actifs**.

   c. Sélectionnez **Ajouter un calendrier**.

   d. Sélectionnez **Ajouter un calendrier dans le cloud** et renseignez les champs.

Champ	Description
Fournisseur	AWS
Nom de calendrier	Saisissez un nom unique pour votre calendrier afin de le distinguer des autres AWS calendriers.
Ajouter un compte	Sélectionnez cette option pour créer un compte de service.
Sélectionner un compte	Sélectionnez cette option pour modifier un compte de service existant.
ID du compte	ID de compte pour votre AWS compte de service.
Type de sélection de MID	Vous devez fournir un Serveur MID. Sélectionnez l'une des options : ▪ Sélectionner automatiquement Serveur MID ▪ Grappe MID spécifique ▪ Serveur MID spécifique Pour importer des données de règles pour des ordinateurs virtuels individuels avec votre serveur MID, vous devez activer une propriété de serveur MID. Pour vérifier ou définir cette propriété, accédez à **Tous** > **Serveur MID** > **Propriétés** > **sn_itom_pattern.discover_aws_app_pool_members**. Définissez la valeur sur vrai.
Informations d'identification	Il s’agit des informations d’identification Discovery pour votre compte de service.
URL	
Nom du rôle d'accès	
Sélectionner un compte pour l'accès	

   e. Sélectionnez **Compte de test**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous devez avoir réussi la validation avant de pouvoir continuer.

f. Sélectionnez **Suivant**.

g. Sélectionnez les centres de données que vous souhaitez détecter.

h. Sélectionnez le bouton bascule **Découvrir les ordinateurs virtuels par adresse IP** et sélectionnez le serveur MID que vous avez sélectionné à l'étape d dans la liste.

i. Sélectionnez **Suivant**.

j. Sélectionnez la fréquence et le moment où vous souhaitez exécuter votre découverte.

k. Sélectionnez **Terminer, puis exécuter**.

Une fois le calendrier de détection que vous définissez exécuté, le modèle **de détection Amazon AWS - Web ACL (LP)** s'exécute et les données des deux applications sont importées.

Créer une politique pour l'intégration WAF afin de surveiller les AWS contrôles d'atténuation

Créez une politique afin de pouvoir auditer vos actifs en fonction des données importées depuis l'intégration.

Avant de commencer

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Politiques et résultats** > **Tous**.
2. Sélectionnez **Actif matériel** pour le type d'actif.

   Les propriétés fonctionnent également pour la recherche d'actifs et les profils d'actifs.
3. Pour Connexion, sélectionnez **Configuration du contrôle de sécurité**.
4. Pour Entité, sélectionnez **AWS Insight**.

   Un champ Critères s'affiche, renseigné automatiquement avec la connexion.
5. Pour le nouveau champ Connexion, sélectionnez **Avec la règle gérée par AWS**.

   Le champ Entité est renseigné automatiquement avec la règle gérée et un champ Critère s'affiche et renseigné automatiquement avec la propriété. Les champs Propriété, Opérateur et Valeur vides s'affichent.

   Si vous avez créé une règle AWS personnalisée, sélectionnez **Avec instruction de correspondance personnalisée**. Le champ Entité est renseigné avec l'instruction de correspondance.
6. Sélectionnez des propriétés dans la liste.

   Vous pouvez en ajouter plusieurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, pour une ACL Web pour la base de données SQL dans votre compte de service AWS, les règles suivantes peuvent s'afficher :

- SQLiExtendedPatterns_QUERYARGUMENTS
- SQLiQUERYARGUMNETS
- SQLi_BODY
- SQLi_COOKIE
- SQLi_URIPATH

Dans le créateur de stratégie, cette propriété s'affiche comme suit : SQLRuleSet-SQLi_BODY est Autorisé. Vous pouvez sélectionner **Autoriser** ou **Bloquer** dans la liste.

7. Sélectionnez **ou** pour ajouter des propriétés.
   Consultez Créer et activer des politiques personnalisées pour Contrôle de la posture de sécurité pour plus d'informations sur l'utilisation du créateur de politique pour créer des politiques.
8. Sélectionnez **Enregistrer les changements** une fois que vous avez terminé votre police.
9. **Activez** la politique si vous souhaitez afficher les résultats.
10. Consultez la section Contrôle de la posture de sécurité : configuration et affichage de vos résultats pour plus d'informations sur l'affichage des résultats de votre police.
11. Ouvrez un enregistrement de la liste et sélectionnez les onglets Contrôles d'atténuation Éléments vulnérables atténués.

    L'onglet Éléments vulnérables atténués répertorie tous les éléments vulnérables atténués qui incluent des informations sur les CVE qui sont atténuées en raison des règles d'atténuation trouvées sur vos actifs.

    - Source(s) vérifiée(s) : API AWS, ITOM Discovery
    - Protégé par un pare-feu d'application Web (WAF) : oui
    - Type WAF : AWS
    - Éléments vulnérables entièrement atténués : nombre d'éléments vulnérables associés atténués.
    - Éléments vulnérables partiellement atténués : nombre d'éléments vulnérables associés en cours de traitement.
    - Règles gérées classées par actions : règles gérées avec des actions « Bloquer » et « Autoriser ».

      Vous pouvez voir plus de règles que vous n'en avez saisies pour votre police. Ces règles sont identifiées avec CommonRuleSet (CRS) dans la règle.

    - Règles personnalisées : toutes vos règles personnalisées classées par actions « Bloquer » et « Autoriser ».
    - Sur le tableau de bord de la page d'accueil, la vignette Actifs avec atténuations répertorie les actifs protégés par WAF dans la visualisation Exploit Protection (WAF).

Afficher les atténuations détectées

Vous devez activer les politiques avant de pouvoir voir quelles menaces pour vos actifs sont atténuées par les contrôles d'atténuation disponibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Vérifiez que vous avez satisfait aux exigences énumérées dans Installer et configurer les intégrations pour la surveillance des contrôles d'atténuation CrowdStrike, Installer et configurer le connecteur du graphe de services pour Microsoft SCCM et l'intégration du contrôle d'atténuation de Microsoft Defender et Configurer les intégrations pour la surveillance des contrôles d'atténuation F5 BIG-IP.

Rôles requis : groupe d'administrateurs SPC et groupe d'analystes SPC.

Procédure

Pour afficher les actifs avec des atténuations détectées par Contrôle de la posture de sécurité avec le widget « Actifs avec atténuations MITRE » sur le tableau de bord, procédez comme suit.

a. Accédez à la **Espaces de travail** > **Contrôle de la posture de sécurité** > **Accueil**.

b. Dans la section Aperçus clés, passez en revue le widget Actifs avec atténuations MITRE.

c. Sélectionnez une catégorie d'atténuation, **Protection contre les exploits (EDR)** ou **Protection contre les exploits (WAF)** dans le widget.

d. Vous pouvez afficher la liste des actifs avec des atténuations détectées dans cette catégorie d'atténuation.

e. Sélectionnez un actif.

f. Sélectionnez l'onglet **Contrôles d'atténuation** pour afficher les détails du contrôle d'atténuation détecté.

g. Sélectionnez l'onglet **Éléments vulnérables atténués** pour afficher la liste des éléments vulnérables atténués par ce contrôle d'atténuation.

> **Remarque :** Pour que cet onglet soit rempli, l'application Réponse aux vulnérabilités doit être installée et activée.

Contrôles d'atténuation du mappage des éléments vulnérables

Les données des contrôles d'atténuation sont mappées aux éléments vulnérables. Vous pouvez afficher la liste des contrôles d'atténuation utilisés pour atténuer les vulnérabilités et les vulnérabilités et expositions courantes (CVE) sous-jacentes associées aux éléments vulnérables.

Après avoir identifié un contrôle d'atténuation spécifique sur une ressource, Contrôle de la posture de sécurité identifie automatiquement tous les éléments vulnérables atténués par ce contrôle. Par exemple, tous les éléments vulnérables avec des CVE qui font partie des signatures dans les politiques de pare-feu d'application Web (WAF) sont marqués comme éléments vulnérables atténués. Cette identification peut être utile aux équipes de gestion de la vulnérabilité pour les aider à réduire automatiquement les scores de risque pour les éléments vulnérables atténués.

Table des contrôles d'atténuation des éléments vulnérables

La table Contrôles d'atténuation des éléments vulnérables [sn_vul_vulnerable_item_mitigation_control] a été créée pour mapper les données de contrôle d'atténuation aux éléments vulnérables atténués (VIT). Ce tableau répertorie les VIT atténués et les contrôles d'atténuation détectés qui ont été utilisés pour atténuer les vulnérabilités et leurs CVE sous-jacentes associées aux éléments vulnérables. Les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

enregistrements CVE atténués contiennent des références au contrôle d'atténuation utilisé pour les actifs, par exemple, la protection contre les exploits (EDR).

Le tableau suivant présente des exemples de données.

Données des contrôles d'atténuation des éléments vulnérables

Un contrôle d'atténuation existe	Efficacité du contrôle d'atténuation	Type de contrôle d'atténuation détecté	CVE atténués	Élément vulnérable
Oui/Non	Modéré	Protection contre les exploits (EDR)	CVE-2009-3373	VIT0018323

Ouvrez un enregistrement de contrôle d'atténuation (type de contrôle d'atténuation détecté) sur la table pour examiner les détails de la façon dont une CVE et sa vulnérabilité CWE (Common Weakness Enumeration) connexe sont atténuées par le contrôle d'atténuation associé à un actif. L'enregistrement de contrôle d'atténuation contient des détails sur les CWE qui ont été atténuées, par exemple, la façon dont un paramètre d'atténuation satisfait les vulnérabilités spécifiées dans une CWE.

Calculateur de risque et règles du calculateur de risque

Les informations sur l'atténuation peuvent être utilisées pour vous aider à configurer des règles de calcul de risque personnalisées afin de vous aider à recalculer les scores de risque sur les VIT auxquels sont associés des types spécifiques de vulnérabilités et des contrôles d'atténuation. Pour cet exemple de règle, qui est basé sur la table précédente, le calculateur de risque par défaut calcule un score de risque de 60 pour les VIT qui ont le type de contrôle d'atténuation, Protection contre l'exploit (EDR) sur les actifs détectés. Ce score de calcul est dû au risque modéré associé à la vulnérabilité avec cette atténuation en place.

Exemple de règle du calculateur de risque avec les conditions suivantes :

[Détails des contrôles d'atténuation] [n'est pas] [vide] ET [Détails des contrôles d'atténuation, type de contrôle d'atténuation détecté] [est] [Protection des exploits (EDR)].

Valeurs :

[Score du risque][est][60]

Consultez Définir les champs et les poids de la règle de risque pour les calculateurs de risque de Vulnerability Response pour plus d'informations.

Cas d'utilisation, exemples de politiques et connecteurs du graphe de services pris en charge dans Contrôle de la posture de sécurité

Les cas d'utilisation sont différents scénarios que vous configurez pour vous aider à identifier des types spécifiques d'écarts de couverture d'outils. Chaque cas d'utilisation nécessite une ou plusieurs politiques pour auditer vos actifs afin de détecter d'éventuelles violations. Vous pouvez également définir vos propres politiques pour vous aider à répondre aux exigences de vos normes de sécurité internes spécifiques.

Cas d'utilisation

L'application Contrôle de la posture de sécurité prend en charge divers cas d'utilisation inclus dans l'application. Les cas d'utilisation vous aident à identifier des types spécifiques

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de lacunes de couverture d'outils dans vos actifs, l'exposition Internet des actifs dans le cloud et les combinaisons avec des vulnérabilités. Les politiques dont vous avez besoin pour les cas d'utilisation pris en charge sont également incluses dans le produit.

Vous pouvez afficher l'état de la couverture pour certains des cas d'utilisation clés sur la page d'accueil (de destination) de l'espace de travail Contrôle de la posture de sécurité à l'adresse **Espaces de travail** > **Contrôle de la posture de sécurité** > **Accueil** dans le module Accueil (page de destination).

Vous pouvez également afficher les connecteurs du graphe de services pris en charge et l'état de la couverture pour certains des cas d'utilisation clés dans les onglets « Connecteurs du graphe de services pris en charge » et « Configuration du cas d'utilisation clé » à l'adresse suivante : **Tous** > **Espaces de travail** > **Contrôle de la posture de sécurité** > **Configuration des connecteurs et des tickets d'utilisation** (l'icône d'engrenage).

Remarque :

L'onglet Cas d'utilisation clés des pages de destination d'accueil ne répertorie pas tous les cas d'utilisation possibles. Il vous fournit quelques cas d'utilisation importants que vous pouvez activer pour vous aider à démarrer le déploiement du produit Contrôle de la posture de sécurité.

Avant d'activer les politiques pour les cas d'utilisation pris en charge fournis avec l'application, vérifiez que vous avez effectué les tâches suivantes.

- Vous avez installé et configuré toutes les applications requises décrites à la section Installer les applications prises en charge pour Contrôle de la posture de sécurité.
- Vous avez satisfait à un ou plusieurs des prérequis suivants pour chaque cas d'utilisation.

1. Vous utilisez actuellement ou vous installez et activez Connecteurs du graphe de services pour différentes catégories.

   Les catégories des cas d'utilisation comprennent Connecteurs du graphe de services que vous devez activer pour obtenir des aperçus initiaux, et Connecteurs du graphe de services que vous avez la possibilité d'activer pour une meilleure couverture des actifs surveillés par Contrôle de la posture de sécurité.

2. Vous utilisez actuellement ou vous installez et activez l'application Vulnerability Response.
3. Vous utilisez actuellement ou vous configurez l'analyse de compte cloud pour vos comptes AWS et Azure sous « Gestion de la posture de sécurité cloud ».

Les exigences spécifiques à chaque cas d'utilisation pris en charge sont décrites dans les sections suivantes. En outre, vous devez activer une ou plusieurs des politiques expédiées avec Contrôle de la posture de sécurité pour un cas d'utilisation. Ce concept est également abordé dans les sections suivantes.

Exemples de politiques de base, enfant et clonées

Découvrez Exemples de politiques de base, enfant et clonées pour Contrôle de la posture de sécurité comment réutiliser les conditions d'une stratégie de base lorsque vous créez d'autres stratégies. Créez des politiques de base et enfants et clonez des politiques existantes dans ces exemples. Ces exemples vous aident également à voir comment le créateur de stratégie fonctionne dans le module Politiques et résultats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services pris en charge

Consultez les tables des connecteurs du graphe de services pris en charge, leurs catégories d'outils et les types de données qu'ils importent dans Connecteurs du graphe de services matériels pris en charge pour Contrôle de la posture de sécurité et Connecteurs du graphe de services logiciels pris en charge pour Contrôle de la posture de sécurité.

Contrôle de la posture de sécurité Cas d'utilisation : Détection des actifs avec une protection de point de terminaison manquante

Pour détecter les actifs sans agent Endpoint Protection, les prérequis suivants sont requis.

En fonction de votre cas d'utilisation, vous pouvez choisir d'activer uniquement les connecteurs requis.

1. Activez au moins un connecteur du graphe de services à partir de la catégorie Protection du point de terminaison.
2. Activez au moins un connecteur du graphe de services pour UNE des catégories suivantes.
   a. Services de répertoires (Microsoft Active Directory).
   b. Endpoint Management : Microsoft Intune ou Jamf Device and Endpoint Management.
   c. Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.
   d. Fournisseur cloud : Amazon AWS Cloud, Microsoft Azure, GCP.

   Remarque : Si Découverte dans le cloud est activé, ces produits Service Graph Connector ne sont pas requis.

3. [Facultatif] Vous pouvez activer les connecteurs du graphe de services pour l'une des catégories suivantes afin d'améliorer la couverture globale, c'est-à-dire le nombre d'actifs qui sont signalés et surveillés par Contrôle de la posture de sécurité.
   a. Sécurité réseau
   b. Surveillance de l'infrastructure
   c. Réseau
   d. Surveillance de la performance des applications .

Après avoir vérifié que vous remplissez ces conditions préalables, vous devez activer la politique suivante, Protection des actifs manquants contre les points de terminaison . Pour plus d'informations sur les politiques, consultez .Politiques pour Contrôle de la posture de sécurité

Contrôle de la posture de sécurité Cas d'utilisation : Détection des actifs manqués par les outils d'évaluation des vulnérabilités

Pour détecter les actifs manqués par les outils d'évaluation de la vulnérabilité, les conditions préalables suivantes sont requises.

Pour chaque connecteur du graphe de services de la liste, vous pouvez voir si ce connecteur est nécessaire pour surveiller les actifs sur site ou les actifs dans le cloud. En fonction de votre cas d'utilisation, vous pouvez choisir d'activer uniquement les connecteurs requis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Activez au moins un connecteur du graphe de services à partir de la catégorie d'évaluation de vulnérabilité.
2. Activez au moins un connecteur du graphe de services pour UNE des catégories suivantes.
   a. Services de répertoires (Microsoft Active Directory).
   b. Endpoint Management : Microsoft Intune ou Jamf Device and Endpoint Management.
   c. Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.
   d. Fournisseur cloud : Amazon AWS Cloud, Microsoft Azure, GCP.

   Remarque : Si Découverte dans le cloud est activé, ces produits Service Graph Connector ne sont pas requis.

3. [Facultatif] Vous pouvez activer les connecteurs du graphe de services pour l'une des catégories suivantes afin d'améliorer la couverture globale, c'est-à-dire le nombre d'actifs qui sont signalés et surveillés par Contrôle de la posture de sécurité.
   a. Sécurité réseau .
   b. Réseautage.
   c. Surveillance de l'infrastructure.
   d. Surveillance de la performance des applications .

Une fois que vous avez vérifié que vous remplissez ces conditions préalables, vous devez activer la politique suivante, Actifs non analysés pour détecter les vulnérabilités. Pour en savoir plus sur les stratégies, consultez .Politiques pour Contrôle de la posture de sécurité

Contrôle de la posture de sécurité Cas d'utilisation : Détection des actifs non gérés

Ce cas d'utilisation comprend deux parties, la détection des actifs pour lesquels il manque des agents de configuration et de gestion des correctifs.

Pour détecter les actifs sans outils de configuration et de gestion des correctifs, les conditions préalables suivantes sont requises.

Pour chaque connecteur du graphe de services de la liste, vous pouvez voir si ce connecteur est nécessaire pour surveiller les actifs sur site ou dans le cloud.

En fonction de votre cas d'utilisation, vous pouvez choisir d'activer uniquement les connecteurs requis.

1. Activez au moins un connecteur du graphe de services à partir des catégories Configuration et Gestion des correctifs.
2. Au moins un connecteur du graphe de services doit être activé pour UNE des catégories suivantes.
   a. Services de répertoires (Microsoft Active Directory).
   b. Endpoint Protection : CrowdStrike ou SentinelOne.
   c. Évaluation de la vulnérabilité : Qualys, Rapid7 ou Tenable.
   d. Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. [Facultatif] Vous pouvez activer les connecteurs du graphe de services pour l'une des catégories suivantes afin d'améliorer la couverture globale, c'est-à-dire le nombre d'actifs qui sont signalés et surveillés par Contrôle de la posture de sécurité.
   a. Réseautage.
   b. Surveillance de l'infrastructure
   c. Sécurité réseau
   d. Surveillance de la performance des applications .

Après avoir vérifié que vous remplissez ces conditions préalables, vous devez activer au moins une des politiques suivantes. Pour toute politique commençant par « Actifs dans le cloud », Connecteurs du graphe de services sous la catégorie « Fournisseur dans le cloud » doivent être activés. Pour plus d'informations sur les politiques, consultez Politiques pour Contrôle de la posture de sécurité.

- Configuration et gestion des correctifs manquants pour les actifs.
- Configuration et gestion des correctifs manquants pour les actifs dans le cloud.

Contrôle de la posture de sécurité Cas d'utilisation : détection des actifs sans solution de gestion des points de terminaison

Pour détecter les actifs sans solution de gestion des points de terminaison, les conditions préalables suivantes sont requises.

En fonction de votre cas d'utilisation, vous pouvez choisir d'activer uniquement les connecteurs requis.

1. Activez au moins un connecteur du graphe de services à partir de la catégorie Gestion des points de terminaison.
2. Au moins un connecteur du graphe de services doit être activé pour UNE des catégories suivantes.
   a. Services de répertoires (Microsoft Active Directory).
   b. Endpoint Protection : CrowdStrike ou SentinelOne.
   c. Évaluation de la vulnérabilité : Qualys, Rapid7 ou Tenable.
   d. Configuration et gestion des correctifs : Microsoft SCCM ou IBM Bigfix.

Après avoir vérifié que vous remplissez ces conditions préalables, vous devez activer la politique suivante, Actifs manquants Solution de gestion des points de terminaison. Pour en savoir plus sur les stratégies, consultez .Politiques pour Contrôle de la posture de sécurité

Contrôle de la posture de sécurité Cas d'utilisation : Détection des actifs présentant des vulnérabilités et des lacunes dans la couverture de l'outil de sécurité

Vous pouvez identifier les actifs présentant des vulnérabilités critiques et des outils de sécurité critiques manquants, tels que la protection des points de terminaison, afin de classer ces actifs par ordre de priorité pour le rattrapage. Security Posture Control fournit quelques politiques incluses avec le produit pour prendre en charge ce cas d'utilisation.

Ce cas d'utilisation nécessite l'installation de l'application Vulnerability Response et d'une intégration avec au moins un produit d'évaluation de la vulnérabilité tel que , Rapid7 ou Qualys Tenable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les politiques suivantes sont incluses dans le produit Contrôle de la posture de sécurité pour prendre en charge ce cas d'utilisation pour les actifs présentant des vulnérabilités critiques qui ne couvrent pas non plus l'outil de sécurité.

1. Actifs avec des vulnérabilités critiques et une protection de point de terminaison manquante.
2. Actifs avec des vulnérabilités critiques et une configuration et une gestion des correctifs manquantes.
3. Actifs avec vulnérabilités critiques et gestion des points de terminaison manquante.

Contrôle de la posture de sécurité Cas d'utilisation : Détection de l'exposition Internet des ressources cloud et des combinaisons à haut risque

Il est essentiel de surveiller l'exposition potentielle à Internet des ressources cloud (machines virtuelles) sur différents ports pour s'assurer que les vulnérabilités de ces ressources ne sont pas exploitées à distance. Ce cas d'utilisation vous aide à identifier ces actifs.

Contrôle de la posture de sécurité vous permet d'évaluer la configuration des ressources dans le cloud pour vous aider à identifier les ressources qui sont ouvertes sur Internet, c'est-à-dire celles qui sont accessibles de n'importe où sur Internet et à partir de quels ports elles sont exposées.

Security Posture Control combine ces informations avec les lacunes de couverture des outils de sécurité et les données de vulnérabilité provenant d'analyseurs tiers tels que Qualys, Rapid7 ou Tenable pour identifier les combinaisons à haut risque.

Actuellement, ce cas d'utilisation prend en charge AWS et nécessite les conditions préalables suivantes.

1. Connecteur du graphe de services pour AWS est activé pour les mêmes comptes AWS que ceux que vous avez configurés.
2. Vous avez activé une ou plusieurs des politiques incluses dans le produit dans Contrôle de la posture de sécurité.
   - Actifs dans le cloud avec le port SSH 22 ouverts à Internet.
   - Actifs dans le cloud avec le port SSH 22 ouvert à Internet et sans protection des points de terminaison.
   - Actifs dans le cloud avec le port HTTP 80 ouvert à Internet et sans protection des points de terminaison.
   - Actifs dans le cloud avec vulnérabilités critiques et port SSH 22 ouvert à Internet (nécessite Vulnerability Response).
   - Actifs dans le cloud avec vulnérabilités critiques, protection des points de terminaison manquante et port SSH 22 ouvert à Internet (nécessite Vulnerability Response).
   - Actifs dans le cloud avec ports HTTP ouverts à Internet, vulnérabilités critiques et protection des points de terminaison manquante (nécessite Réponse aux vulnérabilités).

Connecteurs du graphe de services matériels pris en charge pour Contrôle de la posture de sécurité

Connecteurs du graphe de services matériels pris en charge avec la classe CI, la source (produit) et les catégories d'outils. Cette liste n'est pas complète et est susceptible d'être modifiée avec l'ajout d'autres produits.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour la source de découverte d'un connecteur répertorié, « SG », « SGO » ou « SGC » précède le nom de produit pour les produits tiers, par exemple, SG-AWS, SGO-Datadog ou SGC-AD (Active Directory). Pour les produits ServiceNow, « SN » ou « ServiceNow » précède le nom du produit, par exemple, SNAssetManagement for ServiceNow Hardware Asset Management.

Après les avoir installés, vous pouvez afficher les connecteurs et leurs catégories sur la table des connecteurs [sn_sec_spc_core_connector] de votre instance.

Vous pouvez afficher les types d'actifs et la façon dont ils sont mappés aux classes CI et aux connecteurs dans la table [sn_sec_spc_core_asset_type_connector].

Connecteurs du graphe de services matériels

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_computer	Active Directory	Services du répertoire
Actif matériel	cmdb_ci_server	AppDynamics	Surveillance de la performance des applications
Actif matériel	cmdb_ci_server	Automox	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_computer	Automox	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_computer	BigFix	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_server	BigFix	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_printer	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_server	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_iot	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_hc_device	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_netgear	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_computer	Cisco Meraki	Réseau
Actif matériel	cmdb_ci_server	CrowdStrike	Protection du point de terminaison
Actif matériel	cmdb_ci_server	Datadog	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_server	Dynatrace	Surveillance de la performance des applications
Actif matériel	cmdb_ci_computer	Dynatrace	Surveillance de la performance des applications
Actif matériel	cmdb_ci_computer	Révélation ExtraHop(x)	Sécurité réseau
Actif matériel	cmdb_ci_hc_device	Révélation ExtraHop(x)	Sécurité réseau

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services matériels (suite)

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_server	Révélation ExtraHop(x)	Sécurité réseau
Actif matériel	cmdb_ci_iot	Révélation ExtraHop(x)	Sécurité réseau
Actif matériel	cmdb_ci_printer	Révélation ExtraHop(x)	Sécurité réseau
Actif matériel	cmdb_ci_iot	Avant-scout	Sécurité réseau
Actif matériel	cmdb_ci_hc_device	Avant-scout	Sécurité réseau
Actif matériel	cmdb_ci_computer	Avant-scout	Sécurité réseau
Actif matériel	cmdb_ci_server	Avant-scout	Sécurité réseau
Actif matériel	cmdb_ci_printer	Avant-scout	Sécurité réseau
Actif matériel	cmdb_ci_server	Intune	Gestion des points de terminaison
Actif matériel	cmdb_ci_computer	Intune	Gestion des points de terminaison
Actif matériel	cmdb_ci_printer	Jamf Pro	Gestion des points de terminaison
Actif matériel	cmdb_ci_server	Jamf Pro	Gestion des points de terminaison
Actif matériel	cmdb_ci_computer	Jamf Pro	Gestion des points de terminaison
Actif matériel	cmdb_ci_server	Balayeur de lanière	Gestion des actifs IT
Actif matériel	cmdb_ci_computer	Balayeur de lanière	Gestion des actifs IT
Actif matériel	cmdb_ci_printer	Balayeur de lanière	Gestion des actifs IT
Actif matériel	cmdb_ci_hc_device	LogicMonitor	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_printer	LogicMonitor	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_server	LogicMonitor	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_vm_instance	LogicMonitor	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_iot	LogicMonitor	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_computer	LogicMonitor	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_netgear	LogicMonitor	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_server	Microsoft Defender	Protection du point de terminaison

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services matériels (suite)

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_server	New Relic	Surveillance de la performance des applications
Actif matériel	cmdb_ci_computer	Nexthink	Expérience numérique de l'employé
Actif matériel	cmdb_ci_computer	Netskope	Prévention de la perte de données
Actif matériel	cmdb_hardware_product_model	Netskope	Prévention de la perte de données
Actif matériel	cmdb_ci_network_adapter	Netskope	Prévention de la perte de données
Actif matériel	cmdb_software_instance	Netskope	Prévention de la perte de données
Actif matériel	cmdb_sam_sw_install	Netskope	Prévention de la perte de données
Actif matériel	sn_sec_sgc_netskop_client_attribute	Netskope	Prévention de la perte de données
Actif matériel	cmdb_ci_server	Ouvrir la télémétrie	Surveillance de la performance des applications
Actif matériel	cmdb_ci_computer	Puppet	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_server	Puppet	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_computer	Qualys	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_server	Qualys	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_vm_instance	Qualys-ServiceNow	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_server	Qualys-ServiceNow	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_hardware	Rapid7	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_computer	SCCM	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_server	SCCM	Configuration et gestion des correctifs
Actif matériel	cmdb_ci_printer	ScienceLogic	Surveillance de l'infrastructure

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services matériels (suite)

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_iot	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_server	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_computer	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_hc_device	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_vm_instance	ScienceLogic	Surveillance de l'infrastructure
Actif matériel	cmdb_ci_hardware	ServiceNow HAM	Gestion des actifs matériels
Actif matériel	cmdb_ci_hardware	ServiceNow Découverte ITOM	Découverte
Actif matériel	cmdb_ci_aws_datacenter	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_azure_datacenter	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_availability_zone	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_google_datacenter	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_cloud_service_account	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_cloud_subnet	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_compute_template	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_network	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_vm_instance	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_key_value	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_os_template	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_server	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_computer	SentinelOne	Protection du point de terminaison

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services matériels (suite)

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Actif matériel	sn_sec_sgc_sntlone_asset_tags	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_ip_address	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_network_adapter	SentinelOne	Protection du point de terminaison
Actif matériel	sn_sec_sgc_sntlone_additional_attributes	SentinelOne	Protection du point de terminaison
Actif matériel	cmdb_ci_server	Actif Tanium	Gestion des points de terminaison
Actif matériel	cmdb_ci_computer	Actif Tanium	Gestion des points de terminaison
Actif matériel	cmdb_ci_ups	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_industrial_sensor	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_cnc	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_hardware	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_netgear	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_industrial_actuator	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ip_switch	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_hub_network	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_security	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_server	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_rtu	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_ews	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_plc	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_control	Tenable	Évaluation de la vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services matériels (suite)

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_ot_dcs	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_storage_server	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_hmi	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_control_module	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_industrial_robot	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_historian	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_industrial_drive	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_iot	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ip_firewall	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_computer	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_unclassed_hardware	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ids_network	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_ot_ied	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_printer	Tenable	Évaluation de la vulnérabilité
Actif matériel	cmdb_ci_computer	Espace de travail VMware ONE UEM	Gestion des points de terminaison
Actif matériel	cmdb_ci_server	Espace de travail VMware ONE UEM	Gestion des points de terminaison
Actif matériel	cmdb_ci_printer	Espace de travail VMware ONE UEM	Gestion des points de terminaison
Actif matériel	cmdb_ci_vm_instance	Wiz	Plateforme de protection des applications native dans le cloud
Actif matériel	cmdb_ci_server	Wiz	Plateforme de protection des applications native dans le cloud

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services matériels (suite)

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Actif matériel	cmdb_ci_linux_server	Wiz	Plateforme de protection des applications native dans le cloud
Actif matériel	cmdb_ci_win_server	Wiz	Plateforme de protection des applications native dans le cloud

Connecteurs du graphe de services logiciels pris en charge pour Contrôle de la posture de sécurité

Connecteurs du graphe de services logiciels pris en charge avec la classe CI, la source (produit) et les catégories d'outils. Cette liste n'est pas complète et est susceptible d'être modifiée avec l'ajout d'autres produits.

Après les avoir installés, vous pouvez afficher les connecteurs et leurs catégories sur la table des connecteurs [sn_sec_spc_core_connector] de votre instance.

Vous pouvez afficher les types d'actifs et la façon dont ils sont mappés aux classes CI et aux connecteurs dans la table [sn_sec_spc_core_asset_type_connector].

Connecteurs du graphe de services logiciels

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Logiciel	cmdb_ci_spkg	BigFix	Configuration et gestion des correctifs
Logiciel	cmdb_ci_spkg	Dynatrace	Surveillance de la performance des applications
Logiciel	cmdb_ci_spkg	Avant-scout	Sécurité réseau
Logiciel	cmdb_ci_spkg	Intune	Gestion des points de terminaison
Logiciel	cmdb_ci_spkg	Jamf Pro	Gestion des points de terminaison
Logiciel	cmdb_ci_spkg	New Relic	Surveillance de la performance des applications
Logiciel	cmdb_ci_spkg	Nexthink	Expérience numérique de l'employé
Logiciel	cmdb_ci_spkg	Netskope	Prévention de la perte de données
Logiciel	cmdb_ci_spkg	Qualys-ServiceNow	Évaluation de la vulnérabilité
Logiciel	cmdb_ci_spkg	SCCM	Configuration et gestion des correctifs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connecteurs du graphe de services logiciels (suite)

Type d'actif	Classe CI	Source d'actif	Catégorie de connecteur
Logiciel	cmdb_ci_spkg	ServiceNow Découverte ITOM	Découverte
Logiciel	cmdb_ci_spkg	Actif Tanium	Gestion des points de terminaison
Logiciel	cmdb_ci_spkg	Espace de travail VMware ONE UEM	Gestion des points de terminaison

Exemples de politiques de base, enfant et clonées pour Contrôle de la posture de sécurité

Vous pouvez créer vos propres politiques de base qui disposent de vastes ensembles de conditions que vous pouvez utiliser comme points de départ pour des stratégies plus complexes.

Exemples

Les exemples suivants vous aideront à voir comment réutiliser les conditions d'une stratégie de base lorsque vous créez d'autres stratégies en créant des stratégies enfants ou en clonant des stratégies existantes. Ces exemples vous aident également à voir comment le créateur de stratégie fonctionne dans le module Politiques et résultats.

Commençons par le premier exemple, la politique de base. Les autres exemples utilisent la politique de base comme point de départ.

Remarque : Le connecteur du graphe de services CrowdStrike est utilisé comme connecteur du graphe de services dans ces exemples, mais vous pouvez utiliser n'importe quel connecteur que vous avez installé. Ces exemples vous permettent de créer et d'activer les polices pour rechercher des correspondances d'actifs. Vous pouvez supprimer ces politiques à tout moment du module Politiques et résultats après leur activation.

Créer une politique de base pour Contrôle de la posture de sécurité (exemple)

Un exemple de la façon de créer une politique de base que vous pouvez utiliser pour créer d'autres politiques.

Avant de commencer

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Procédure

1. Accédez à la **Tous** > **Espace de travail Contrôle de la posture de sécurité** > **Politiques et résultats**.
2. Sélectionnez **Nouvelle politique**.
3. Sélectionnez l'icône du stylet en haut à gauche, puis renseignez les champs dans la fenêtre modale Modifier les métadonnées.

Champ	Description
Nom	Tapez : politique de base : appareils Windows 10.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Criticité	Sélectionnez **Faible**.
Description brève	**Tapez : Localiser les appareils sur lesquels Windows 10 est installé.**

4. Sélectionnez **Enregistrer les métadonnées**.
5. Dans le générateur de conditions, sélectionnez **Actif matériel** pour Type d'actif.

   Pour cette politique, laissez les options Politique de base et Politiques d'exclusion dans leurs paramètres par défaut (désactivés).
6. Pour Connexion, sélectionnez **Avec données agrégées**.

   Pour cette stratégie, les données agrégées vous aident à localiser les ressources dans votre CMDB sur lesquelles Windows 10 est installé. Par exemple, certains enregistrements peuvent présenter de légères variations sur la façon dont les différents scanners signalent « Windows 10 ». Les données agrégées garantissent que toutes ces légères variations sur « Windows 10 » correspondront à cette politique.

   Les champs Entité et Critères sont renseignés automatiquement en fonction de votre sélection dans le champ Connexion.
7. Pour Propriété**, sélectionnez OS.**
8. Pour Valeur, tapez dans Windows 10.
9. Sélectionnez **Enregistrer les modifications**.
   Votre politique de base s'affiche dans la liste Tous du module Politiques et résultats, mais elle n'est pas activée.
10. Sélectionnez **Activer la politique** afin que votre politique de base surveille tous les actifs qui correspondent aux conditions de la politique et génère des résultats.

Créer une politique enfant à partir d'une politique de base pour Contrôle de la posture de sécurité (exemple)

Un exemple de la façon de créer une politique enfant à l'aide des conditions d'une politique de base.

Avant de commencer

Cette police enfant hérite des conditions d'une politique de base, et vous allez ajouter d'autres conditions à votre police enfant pour vous permettre de vous concentrer sur des détails d'actifs plus spécifiques. Vous souhaitez une nouvelle politique pour surveiller tous vos appareils sur lesquels Windows 10 est installé et qui sont signalés par le connecteur du CrowdStrike graphe de services, et vous souhaitez exclure tous les appareils qui correspondent à une autre politique. Pour cet exemple, vous allez exclure de vos conclusions les actifs qui ont été approuvés pour les exceptions de la Gestion intégrée des risques (IRM).

Remarque : Si vous n'avez pas installé le connecteur du CrowdStrike graphe de services, vous pouvez en utiliser un qui est installé.

Rôles requis : groupe d'administrateurs SPC ou groupe d'analystes SPC

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Espace de travail Contrôle de la posture de sécurité** > **Politiques et résultats**.
2. Dans la liste Actif, localisez la politique de base - Appareils Windows 10 que vous avez créée dans le premier exemple et sélectionnez-la pour ouvrir l'enregistrement.
3. Sélectionnez le menu Autres options (trois points verticaux), puis Créer **une politique enfant**.
   Un nouvel onglet s'ouvre avec un nouvel enregistrement et la politique de base - Appareils Windows 10 s'affiche dans le champ Politique de base.
4. Sélectionnez l'icône du stylo en haut à gauche et renseignez les champs dans la fenêtre modale Modifier les métadonnées.

Champ	Description
Nom	Tapez : Stratégie enfant - Appareils Windows avec CrowdStrike.
Criticité	Sélectionnez **Moyen**.
Description brève	Tapez : Localisez tous les appareils avec Windows 10 signalé par CrowdStrike.

5. Sélectionnez **Enregistrer les métadonnées**.
6. Dans le générateur de conditions, sélectionnez **Actif matériel** pour Type d'actif.
7. Sélectionnez le bouton bascule de la politique de base.
8. Sélectionnez la stratégie que vous avez créée pour l'exemple 1, **Stratégie de base : appareils Windows 10** dans la liste.

   Cette politique enfant hérite automatiquement des conditions de la politique de base.
9. Sélectionnez le bouton bascule Politiques d'exclusion.
10. Sélectionnez Actifs avec exception IRM approuvée dans la liste.

    Remarque : Si vous ne disposez pas de cette politique, vous pouvez sélectionner dans la liste une autre politique que vous souhaitez exclure de celle-ci.

    Les actifs qui correspondent à cette police seront exclus de votre police enfant. Notez que vous pouvez ajouter d'autres polices.
11. Sélectionnez **Signalé par**.
12. Sélectionnez **CrowdStrike** dans la liste.
13. Sélectionnez **Enregistrer les modifications**.
    Votre nouvelle politique s'affiche dans la liste Tous du module Politiques et résultats, mais elle n'est pas activée.
14. Sélectionnez **Activer la politique** afin que votre politique de base surveille tous les actifs qui correspondent aux conditions de la politique et génère des résultats.

Traduction automatique

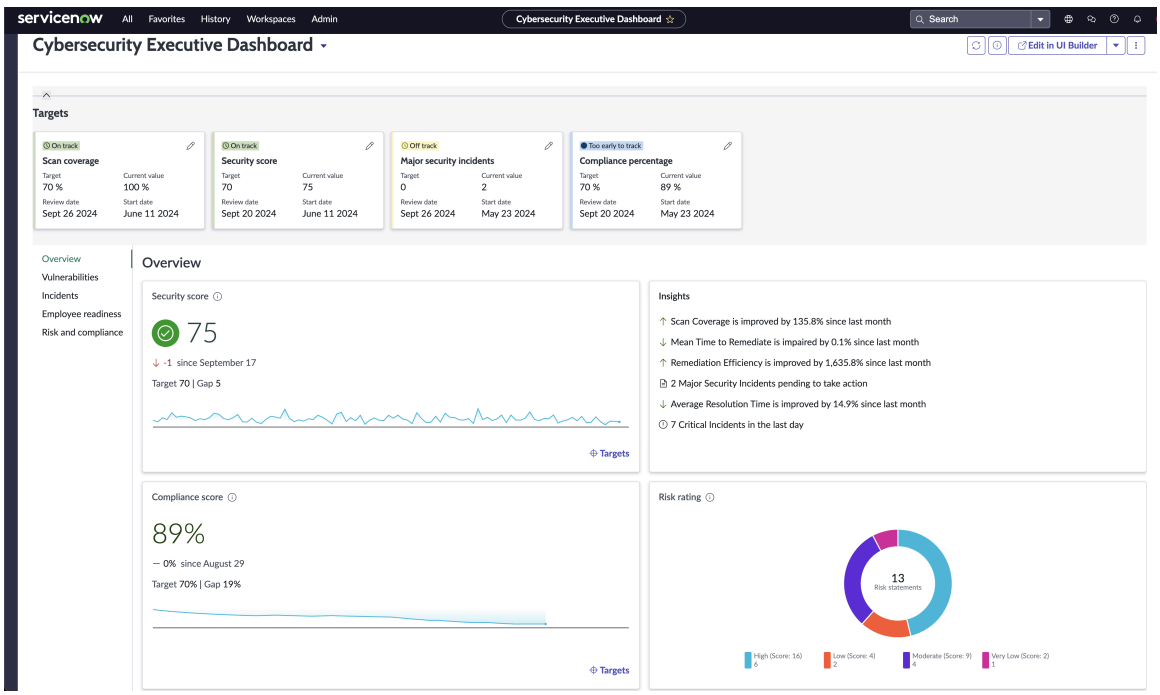
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord de direction de cybersécurité

Le tableau de bord de la cybersécurité est une solution complète qui permet aux responsables de la sécurité de l'information (RSSI) et aux responsables de la cybersécurité d'avoir une visibilité sur la posture et les initiatives de sécurité de l'organisation. Le tableau de bord consolide les données de divers produits de la suite Security Operations et de ServiceNow Governance, Risk and Compliance (GRC).

Le tableau de bord fournit les fonctionnalités suivantes :

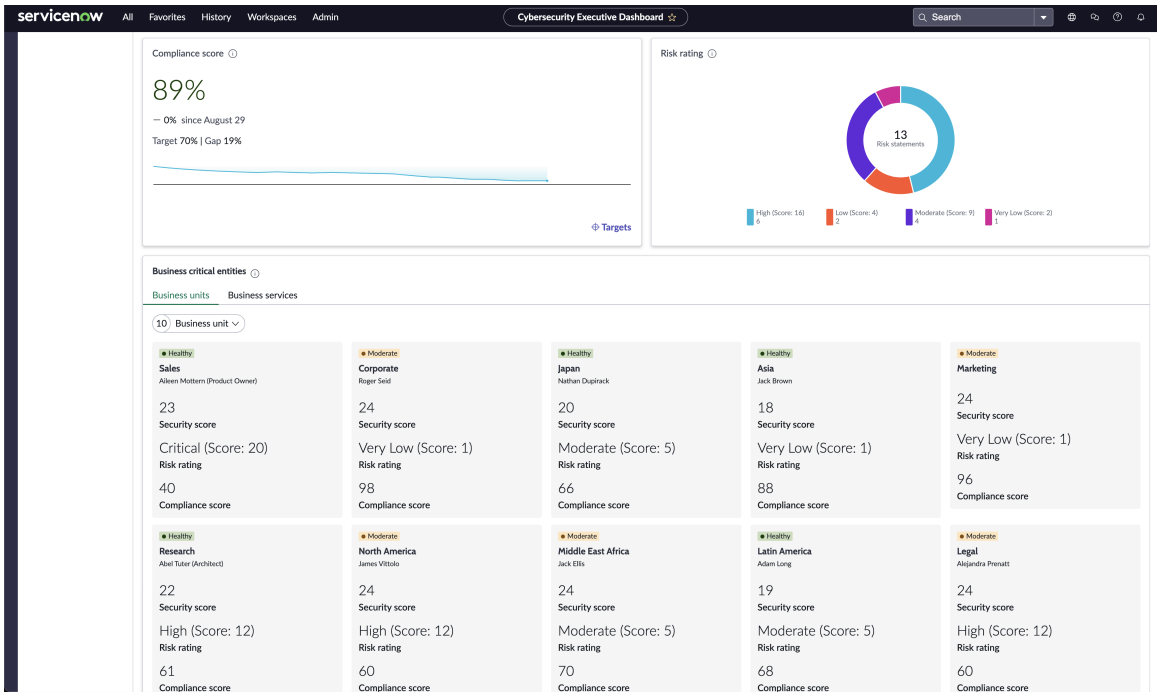
- Score de la posture de sécurité à l'échelle de l'organisation
- Scores de sécurité, risque et conformité par unité business
- Surveillance personnalisable
- Vue unifiée du paysage de sécurité d'une organisation
- Benchmarking
- Interface conviviale
- Visibilité sur les mesures de simulation d'hameçonnage de KnowBe4 et Microsoft Defender pour Office 365



Ces fonctionnalités permettent une prise de décision proactive en fournissant un accès rapide aux mesures de sécurité critiques. Ce qui en fait un outil indispensable pour améliorer la résilience et la préparation globales en matière de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Rôles ServiceNow AI Platform requis

- CISO (sn_bod.ciso) pour afficher et partager le tableau de bord.
- sn_bod.ciso_admin pour afficher, partager le tableau de bord, configurer les pondérations de l'évaluation de la posture de sécurité.
- Utilisateur CISO GRC (sn_grc_dashboards.grc_ciso_user) pour afficher les rapports de conformité et de risque.

Accéder au tableau de bord de direction de cybersécurité

Pour ouvrir le tableau de bord, accédez à **Tous** > **Tableau de bord de direction de cybersécurité** > **Tableau de bord de direction de cybersécurité**.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Responsables de la sécurité de l'information (CISO)	Les RSSI obtiennent des informations sur la gestion des vulnérabilités, la gestion des incidents, la posture de sécurité de l'organisation, les mesures de simulation d'hameçonnage, etc., pour leur organisation.

Visualisation des données

Remarque : Pour en savoir plus sur un widget, sélectionnez l'icône ⓘ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cibles

Mesures	Type	Description
Cibles	Pourcentage	Affiche la cible définie à couvrir pour une mesure. L'état des cibles est indiqué par un code couleur. Il affiche toutes les cibles dont la date d'examen se situe dans les 30 derniers jours ou à venir. Vous pouvez définir le nombre de jours d'affichage des cibles à l'aide de la *sn_bod.show_targets_from* propriété système. De plus, ces cibles peuvent être modifiées. Consultez Définir des cibles pour plus d'informations.

Mesures	Type	Description
Score de sécurité	Score unique	Score global de la posture de sécurité de l'organisation en tenant compte des éléments vulnérables, des incidents de sécurité, des incidents de sécurité majeurs et des erreurs de configuration.
Aperçus	Points forts	Points forts de l'ensemble du tableau de bord.
Score de conformité	Score unique	Fournit la posture de conformité de l'organisation à l'aide du score de conformité calculé en fonction du pourcentage de contrôles conformes par rapport au nombre total de contrôles.
Score du risque	Score unique	Fournit le nombre de déclarations de risque en fonction des évaluations de risque. Elle aide les organisations à comprendre l'impact potentiel et la probabilité de divers risques, ce qui leur permet de hiérarchiser et de gérer ces risques.
Entités critiques pour l'entreprise		
Unités business	Score unique	Score de sécurité global des unités business en

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures	Type	Description
		tenant compte du risque associé aux vulnérabilités, aux erreurs de configuration, aux vulnérabilités de technologie opérationnelle (OT), aux incidents de sécurité et aux incidents de sécurité majeurs. L'étiquette d'intégrité des unités business est basée uniquement sur le score de sécurité. Pour savoir comment ces étiquettes sont affectées, accédez à la table Poids du score de risque [sn_sec_cmn_risk_score_weight_list.do] et recherchez l'entité d'entreprise. Des étiquettes telles que « Intègre » sont attribuées en fonction de plages de valeurs prédéfinies. Par exemple, un score de sécurité compris entre 0 et 39 est étiqueté comme sain. Le code couleur de ces étiquettes est spécifié dans l'include de script UnifiedCISOutils . Vous pouvez configurer la plage de valeurs ainsi que les couleurs des étiquettes. Pour voir comment les noms d'unité business et de tête d'unité business sont attribués, accédez à **Tous** > **Organisation** > **Unités business**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures	Type	Description
		Remarque : Selon les modules d'extension que vous avez activés, vous pouvez accéder au score de conformité, au score de risque et au score de sécurité. Pour afficher le score de conformité et de risque, vous devez activer les modules d'extension GRC. Pour afficher le score de sécurité, vous devez activer les modules d'extension associés à Security Operations. Voir la section Applications à actif pour plus d'informations.
Services d'entreprise	Score unique	Score de sécurité global des services d'entreprise en tenant compte du risque associé aux vulnérabilités, aux erreurs de configuration, aux vulnérabilités de technologie opérationnelle (OT), aux incidents de sécurité et aux incidents de sécurité majeurs. Pour savoir comment ces étiquettes sont affectées, accédez à la table Poids du score de risque [sn_sec_cmn_risk_score_weight_list.do] et recherchez l'entité d'entreprise. Les étiquettes telles que « Intègre », « Modéré » et « Critique » sont attribuées en fonction de plages de valeurs prédéfinies. Par exemple, un score de sécurité compris entre 0 et 39 est étiqueté comme sain. Le code couleur de ces étiquettes est spécifié dans l'include de scriptUnifiedCISOutils . Vous pouvez configurer la plage de valeurs ainsi que les couleurs des étiquettes. Pour voir comment l'unité business et le nom du responsable de l'unité business sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures	Type	Description
		affectés, accédez à **Tous** > **Organisation** > **Unités business**. **Remarque :** Selon les modules d'extension que vous avez activés, vous pouvez accéder au score de conformité, au score de risque et au score de sécurité. Pour afficher le score de conformité et de risque, vous devez activer les modules d'extension GRC. Pour afficher le score de sécurité, vous devez activer les modules d'extension associés à Security Operations. Voir la section Applications à actif pour plus d'informations.

Vulnérabilités

Mesures	Type	Description
Délai moyen de résolution (mensuel)	Ligne	Temps moyen nécessaire pour fermer les vulnérabilités et les résultats des tests échoués sur tous les actifs (hôtes, conteneurs et applications) en un mois. Il fournit également les mesures suivantes : • Cible : cible définie en jours pour corriger les vulnérabilités. • Écart : différence entre les jours entre la cible et le temps réel nécessaire pour corriger les vulnérabilités. • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence mondial : moyenne des mesures des pairs sur le marché mondial

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

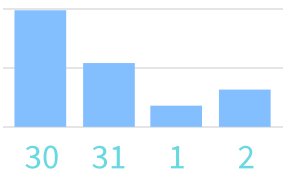
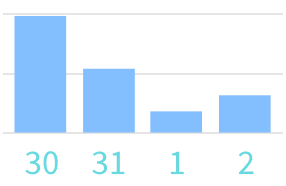
Vulnérabilités (suite)

Mesures	Type	Description
		Consultez la section S'abonner aux scores de point de référence Comment afficher les scores de point de référence.
Âge moyen des vulnérabilités actives (mensuel)	Score unique	Âge moyen mensuel des trois types d'éléments vulnérables. Il fournit également une comparaison de l'âge du mois en cours avec le mois précédent. Il fournit également les mesures suivantes : • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence mondial : moyenne des mesures des pairs sur le marché mondial • Cible : cible définie en jours pour corriger les vulnérabilités.
Efficacité de la résolution (mensuelle)	Score unique	Pourcentage d'éléments vulnérables fermés chaque mois par rapport aux éléments vulnérables actifs mensuels. Il fournit également les mesures suivantes : • Variation en pourcentage par rapport au mois précédent. • Cible : cible définie en pourcentage pour corriger les vulnérabilités. • Écart : écart entre le score cible et le score actuel. • Point de référence du secteur : moyenne des mesures des pairs du même secteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

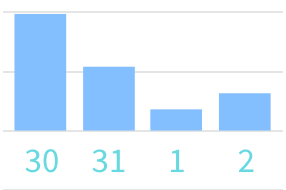
Vulnérabilités (suite)

Mesures	Type	Description
		• Point de référence mondial : moyenne des mesures des pairs sur le marché mondial
Âge moyen des vulnérabilités actives par groupe d'affectation	Ligne multiple	Âge moyen des vulnérabilités actives pour chaque groupe d’affectation.
Vulnérabilités par cote de risque et âge	Carte thermique	Répartition des vulnérabilités actives entre les hôtes, les conteneurs et les applications par cote de risque et par âge.
Respect de la cible de résolution par groupe d'affectation	 verticale	Rapport entre le nombre de vulnérabilités et d’erreurs de configuration fermées avec la cible de correction et le nombre totalde vulnérabilités et d’erreurs de configuration fermées.
Couverture de l'analyse	Pourcentage	Pourcentage des actifs analysés au cours des 90 derniers jours sur l’ensemble des actifs du CMDB.
Actifs numérisés et non numérisés	Barre horizontale	Répartition des actifs analysés au cours des 90 derniers jours et actifs totaux par CMDB classe CI
Actifs numérisés	Barre horizontale	Actifs analysés au cours des 90 derniers jours pour détecter les vulnérabilités par rapport à la conformité de la configuration.
Tendance des résultats de vulnérabilités critiques et élevées actives	à plusieurs lignes	Tendance quotidienne des vulnérabilités et des mauvaises configurations ayant une cote de risque critique et élevé.
Vulnérabilités par catégorie d'actifs et cote de risque	 verticale	Répartition des vulnérabilités actives et des mauvaises configurations par catégorie d’actifs et cote de risque (critique, élevé et moyen).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vulnérabilités (suite)

Mesures	Type	Description
Résultats différés par motif et groupe d'affectation	 verticale	Répartition des vulnérabilités actives et des erreurs de configuration différées par motif de report et groupe d'affectation.
Technologie opérationnelle (OT)		
Tendance des vulnérabilités critiques et élevées actives	de ligne	Tendance quotidienne des vulnérabilités OT actives avec cote de risque critique et élevé.
Délai moyen de résolution (mensuel)	Score unique	Délai moyen nécessaire pour fermer les vulnérabilités OT. Rapport entre l'âge total des vulnérabilités OT fermées et le nombre total de vulnérabilités OT. Il fournit également les mesures suivantes : • Variation en pourcentage par rapport au mois précédent. • Cible : cible définie en jours pour corriger les vulnérabilités. • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence mondial : moyenne des mesures des pairs sur le marché mondial Consultez la section S'abonner aux scores de point de référence Comment afficher les scores de point de référence.
Vulnérabilités par cote de risque et âge	Carte thermique	Répartition des vulnérabilités OT actives par cote de risque et par âge.
Âge moyen des vulnérabilités actives (mensuel)	Graphique en courbes	Âge moyen mensuel des éléments vulnérables OT. Il fournit

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vulnérabilités (suite)

Mesures	Type	Description
		également une comparaison de l'âge du mois en cours avec le mois précédent.
Vulnérabilités par état et âge	Carte thermique 	Répartition des vulnérabilités OT actives par état et par âge.

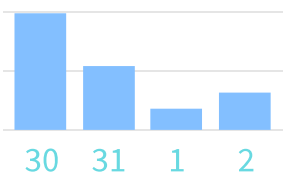
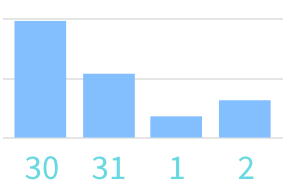
Incidents

Mesures	Type	Description
Incidents de sécurité majeurs	Score unique	Nombre d'incidents de sécurité majeurs actuellement actifs
Délai moyen de résolution des incidents de sécurité (mensuel)	Score unique	Délai de résolution mensuel moyen, en jours, des incidents de sécurité fermés. Il fournit également les mesures suivantes : • Variation en pourcentage par rapport au mois précédent. • Cible : cible définie en jours pour corriger les incidents de sécurité. • Écart : écart entre les jours réels nécessaires à la résolution et l'ensemble de cibles à corriger. • Point de référence du secteur : moyenne des mesures des pairs du même secteur. • Point de référence mondial : moyenne des mesures des pairs sur le marché mondial
Délai moyen pour éradiquer (mensuel)	Graphique en courbes	Résolution moyenne mensuelle en jours pour éradiquer les incidents de sécurité.
Délai moyen pour identifier (mensuel)	Score unique	Résolution moyenne mensuelle en jours pour identifier les incidents de sécurité.

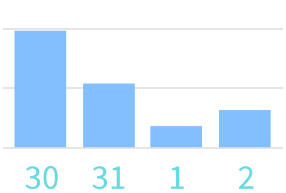
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Incidents (suite)

Mesures	Type	Description
Délai moyen pour contenir (mensuel)	Score unique	Résolution mensuelle moyenne en jours pour contenir les incidents de sécurité.
Incidents actifs par priorité et catégorie	Carte thermique	Nombre d'incidents de sécurité actifs, classés par priorité et par catégorie.
Tendance des incidents fermés et ouverts	 verticale	Répartition des incidents fermés et ouverts.
Incidents actifs par états	 verticale	Répartition des incidents actifs en fonction de leur état.

Préparation des employés

Mesures	Type	Description
Vue d'ensemble mensuelle de la simulation d'hameçonnage	 verticale	Somme des utilisateurs qui ont effectué les actions telles que ouverture, clic et signalement dans la simulation d'hameçonnage, ainsi que la somme du nombre total d'utilisateurs de chaque simulation au cours des six derniers mois.

Risque et conformité

Pour afficher les widgets de risque et de conformité, vous devez activer les modules d'extension GRC. Pour en savoir plus sur les modules d'extension GRC, consultez la section Applications à activer. Pour en savoir plus sur les widgets GRC, reportez-vous à la section Tableau de bord de risque et conformité pour GRC : Mesures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateurs

SLA hôte – Fermé

Cet indicateur est calculé quotidiennement. Il prend en compte l'âge total de toutes les vulnérabilités d'hôte qui ont été fermées le jour précédent au moment du calcul.

SLA de conteneur : fermé

Cet indicateur est calculé quotidiennement. Il prend en compte toutes les vulnérabilités de conteneurs qui ont été fermées le jour précédent au moment du calcul.

SLA de l'application – Fermé

Cet indicateur est calculé quotidiennement. Il tient compte de l'âge total de toutes les vulnérabilités d'applications qui ont été fermées le jour précédent au moment du calcul.

SLA de résultat de test : réussi

Cet indicateur est calculé quotidiennement. Il prend en compte toutes les vulnérabilités des résultats des tests qui ont été transmises la veille au moment du calcul.

SLA hôte : nombre de fermetures

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre de vulnérabilités de l'hôte qui ont été fermées le jour précédent au moment du calcul.

SLA de conteneur : compte fermé

Cet indicateur est calculé quotidiennement. Il prend en compte le nombre de toutes les vulnérabilités de conteneurs qui ont été fermées le jour précédent au moment du calcul.

SLA de l'application : nombre de fermetures

Cet indicateur est calculé quotidiennement. Il tient compte du nombre de vulnérabilités d'applications qui ont été fermées le jour précédent au moment du calcul.

SLA de résultat de test : compte réussi

Cet indicateur est mesuré quotidiennement. Il tient compte du nombre de vulnérabilités des résultats des tests qui ont été transmises pour la dernière fois le jour précédent au moment du calcul.

Actifs analysés

Cet indicateur est calculé quotidiennement. Il prend en compte la somme des CI analysés à partir de la table sn_vul_analytics_scan_coverage_config, qui inclut ceux qui ont été analysés pour la dernière fois au cours des 90 derniers jours, dans toutes les classes de CI CMDB.

Actifs analysables

Cet indicateur est calculé quotidiennement. Il prend en compte la somme des CI totaux de sn_vul_analytics_scan_coverage_config table pour toutes les classes CI CMDB présentes.

Éléments vulnérables

Cet indicateur est calculé quotidiennement. Il tient compte du nombre d'éléments vulnérables actifs au moment du calcul.

Élément vulnérable de l'application

Cet indicateur est calculé quotidiennement. Il tient compte du nombre d'éléments vulnérables actifs de l'application au moment du calcul.

Élément vulnérable de conteneur

Cet indicateur est calculé quotidiennement. Il tient compte du nombre d'éléments vulnérables de conteneurs actifs au moment du calcul.

Âge cumulé des éléments vulnérables

Cet indicateur est calculé quotidiennement. Il tient compte de l'âge cumulé des éléments vulnérables actifs au moment du calcul.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Âge cumulé des éléments vulnérables de l'application

Cet indicateur est calculé quotidiennement. Il tient compte de l'âge cumulé des éléments vulnérables actifs de l'application au moment du calcul.

Éléments vulnérables ouverts

Cet indicateur est calculé quotidiennement. Il tient compte des éléments vulnérables ouverts au moment du calcul.

Éléments vulnérables du conteneur ouverts

Cet indicateur est calculé quotidiennement. Il tient compte des éléments vulnérables du conteneur ouvert au moment du calcul.

Éléments vulnérables de l'application ouverts

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables de l'application ouverts au moment du calcul.

Résultats des test actifs

Cet indicateur est calculé quotidiennement. Il tient compte des résultats des tests ouverts au moment du calcul.

VIT différés

Cet indicateur est calculé quotidiennement. Il a une source d'indicateur en tant qu'élément vulnérable d'hôte.

AVIT différés

Cet indicateur est calculé quotidiennement. Il dispose d'une source d'indicateur en tant qu'élément vulnérable de l'application.

CVIT différés

Cet indicateur est calculé quotidiennement. Il a une source d'indicateur en tant qu'élément vulnérable de conteneur.

Résultats des tests différés

Cet indicateur est calculé quotidiennement. Il prend en compte les résultats des tests qui étaient dans un état différé.

Problèmes de configuration ouverts : résultats des tests

Cet indicateur est calculé quotidiennement. Il dispose d'une source d'indicateur comme résultat de test pour le tableau de bord Vulnerability Response unifié

SI - Délai moyen d'identification

Cet indicateur est calculé quotidiennement. Il prend en compte l'incident de sécurité pour lequel il est temps d'identifier l'incident de sécurité au moment du calcul.

SI : durée moyenne

Cet indicateur est calculé quotidiennement. Elle prend en compte l'incident de sécurité lorsque la définition est une durée d'état d'incident au moment du calcul.

Nombre d'incidents de sécurité majeurs ouverts

Cet indicateur est calculé quotidiennement. Il prend en compte les incidents de sécurité majeurs ouverts au moment du calcul.

Nombre d'incidents de sécurité clôturés

Cet indicateur est calculé quotidiennement. Il prend en compte les incidents de sécurité fermés au moment du calcul.

Éléments vulnérables d'application clôturés

Cet indicateur est calculé quotidiennement. Il tient compte des éléments vulnérables de l'application fermée au moment du calcul.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Éléments vulnérables du conteneur fermés

Cet indicateur est calculé quotidiennement. Il tient compte des éléments vulnérables du conteneur fermé au moment du calcul.

Éléments vulnérables clôturés

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables fermés au moment du calcul.

Obtenir le score de risque maximal pour les éléments vulnérables

Cet indicateur est calculé quotidiennement. Il tient compte du score de risque maximal pour les éléments vulnérables au moment du calcul.

Obtenir le score de risque maximal pour l'élément vulnérable du conteneur

Cet indicateur est calculé quotidiennement. Il tient compte du score de risque maximal pour les éléments vulnérables du conteneur au moment du calcul.

Obtenir le score de risque maximal pour les éléments vulnérables de l'application

Cet indicateur est calculé quotidiennement. Il tient compte du score de risque maximal pour les éléments vulnérables de l’application au moment du calcul.

Score de risque cumulé des VIT

Cet indicateur est calculé quotidiennement. Il tient compte de la somme des scores de risque des éléments vulnérables au moment du calcul.

Score de risque cumulé des AVI

Cet indicateur est calculé quotidiennement. Il tient compte de la somme des scores de risque des éléments vulnérables de l’application au moment du calcul.

Score de risque cumulé des CVI

Cet indicateur est calculé quotidiennement. Il tient compte de la somme des scores de risque des éléments vulnérables du conteneur au moment du calcul.

Score de risque cumulé d'erreurs de configuration

Cet indicateur est calculé quotidiennement. Il tient compte de la somme des scores de risque des résultats des tests au moment du calcul.

Obtenir le score de risque maximal pour les incidents SI

Cet indicateur est calculé quotidiennement. Il tient compte des scores de risque maximal des incidents de sécurité au moment du calcul.

Obtenir le score du risque maximal pour les résultats des tests de configuration incorrecte

Cet indicateur est calculé quotidiennement. Il tient compte des scores de risque maximal pour mauvaise configuration des résultats des tests au moment du calcul.

Obtenir le score du risque moyen pour les résultats des tests de configuration incorrecte

Cet indicateur est calculé quotidiennement. Il tient compte des scores de risque moyen pour mauvaise configuration des résultats des tests au moment du calcul.

Nombre d'incidents de sécurité ouverts

Cet indicateur est calculé quotidiennement. Il prend en compte les incidents de sécurité ouverts au moment du calcul.

Vue d'ensemble de l'hameçonnage

Cet indicateur est calculé quotidiennement. Il tient compte du nombre de mesures de simulation de sécurité au moment du calcul.

Regrouper MTTR

Calcule le temps moyen nécessaire pour fermer les vulnérabilités (hôtes, conteneurs et applications) et le temps nécessaire pour fermer les résultats des tests en jours. [[SLA hôte -

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

fermé]] + [[SLA de l’application - fermé]] + [[SLA conteneur - fermé]] + [[SLA de résultat de test - réussi]]) / ([[SLA hôte - nombre fermé]] + [[SLA de l’application - nombre fermé]] + [[SLA de résultat de test - nombre réussi]] + [[SLA conteneur - nombre fermé]])

Couverture de l'analyse actuelle

Calcule le pourcentage en utilisant le rapport entre le nombre d’éléments analysés et le nombre total d’éléments éligibles à la numérisation au cours de la même période. var scannedItems =[[Actifs analysés]] ; var scannableItems = [[Actifs analysables]] ; var res ; if (scannedItems == 0)res = 0 ; elseres = scannedItems / scannableItems * 100 ; si (res > 100)res = 100 ; Res;

Âge moyen des éléments vulnérables actifs

Calcule l’âge moyen de tous les éléments vulnérables actifs (hôtes, conteneurs et applications) en jours. ([[Âge cumulé des éléments vulnérables]] + [[Âge cumulé des éléments vulnérables de l’application]] + [[Âge cumulé des éléments vulnérables du conteneur]]) / ([[Éléments vulnérables]] + [[Éléments vulnérables de l’application]] + [[Éléments vulnérables de conteneur]])

VIT actives par âge et cote de risque

Calcule le nombre total de tous les éléments vulnérables actifs (hôtes, conteneurs et applications) classés par âge et niveau d’évaluation des risques. [[Éléments vulnérables ouverts]] + [[Éléments vulnérables conteneurs ouverts]] + [[Éléments vulnérables de l’application ouverts]]

Problèmes différés

Calcule le nombre total de tous les éléments vulnérables (hôtes, conteneurs, applications et résultats des tests) avec l’état « Différé ». [[VIT différés]] + [[AVIT différés]] + [[Résultats des tests différés]] + [[CVIT différés]]

Délai moyen de résolution des incidents de sécurité clôturés

Calcule le délai moyen nécessaire pour fermer les incidents de sécurité en jours. ([[Durée cumulée d’incidents de sécurité fermés]] / [[Nombre d’incidents de sécurité fermés]]) /24

Score de sécurité

Calcule quotidiennement les évaluations de sécurité globales. Elle est calculée en fonction du score de risque déployé. var secPostureRating = 100 - [[Score de sécurité]] ; secPostureRating ;

Score de sécurité (unités business)

Calcule le score de risque cumulé final où le score de risque cumulé des éléments vulnérables, des erreurs de configuration, des incidents de sécurité et des incidents de sécurité majeurs est multiplié avec les poids respectifs extraits de la table de déploiement de la posture de sécurité. var numMajorIncidents = [[Nombre d’incidents de sécurité majeurs ouverts]], majorSIRiskScore, rollUpRiskScore ; if(numMajorIncidents > 0) majorSIRiskScore = 100 ; sinon majorSIRiskScore = 0 ; rollUpRiskScore = ([[Score de risque déployé de vulnérabilité et d’erreur de configuration]] * 20 + [[Score de risque déployé de vulnérabilité OT]] * 20 + [[Obtenir le score de risque maximal pour les incidents SI]] * 20 + majorSIRiskScore * 40)/100 ; rollUpRiskScore ;

Score de sécurité (services d’entreprise)

Calcule le score de risque cumulé final où le score de risque cumulé des éléments vulnérables, des erreurs de configuration, des incidents de sécurité et des incidents de sécurité majeurs est multiplié avec les poids respectifs extraits de la table de déploiement de la posture de sécurité. var numMajorIncidents = [[Nombre d’incidents de sécurité majeurs ouverts - Services]], majorSIRiskScore, rollUpRiskScore ; if(numMajorIncidents > 0) majorSIRiskScore = 100 ; sinon majorSIRiskScore = 0 ; rollUpRiskScore = ([[Score de risque déployé de vulnérabilité et d’erreur de configuration - Services]] * 20 + [[Score de risque déployé de vulnérabilité OT - Services]] * 20 + [[Obtenir le score de risque maximal pour les incidents SI - Services]] * 20 + majorSIRiskScore * 40)/100 ; rollUpRiskScore ;

Score de risque déployé de vulnérabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calcule le score de risque déployé de vulnérabilité où le score de risque maximal, le score de risque moyen des éléments vulnérables et le nombre d'éléments vulnérables sont multipliés par leurs poids respectifs. var maxRiskScore = 100 ; nombre de var = [[VIT actives par âge et cote de risque]] ; var countRiskScore ; si (0 == nombre) countRiskScore = 0 ; else if (nombre > 10000) countRiskScore = maxRiskScore ; sinon si (nombre > 1000) countRiskScore = (maxRiskScore * 0,80) ; sinon si (nombre > 100) countRiskScore = (maxRiskScore * 0,60) ; sinon si (nombre > 10) countRiskScore = (maxRiskScore * 0,40) ; sinon countRiskScore = (maxRiskScore * 0,20) ; var vulRiskScore = ([[Obtenir le score maximal de tous les éléments vulnérables]] * 0 + [[Score de risque moyen de tous les éléments vulnérables]] * 100 + countRiskScore * 0)/100 ; Score de risque de vulnérabilité ;

Obtenir le score maximal pour tous les éléments vulnérables

Calcule le score de risque déployé de vulnérabilité où le score de risque maximal, le score de risque moyen des éléments vulnérables et le nombre d'éléments vulnérables sont multipliés par leurs poids respectifs. var maxScoreForVI = [[Obtenir le score de risque maximal pour les éléments vulnérables]], maxScoreForCVI = [[Obtenir le score de risque maximal pour l'élément vulnérable du conteneur]], maxScoreForAVI = [[Obtenir le score de risque maximal pour les éléments vulnérables de l'application]], maxScore ; if (maxScoreForVI >= maxScoreForCVI && maxScoreForVI >= maxScoreForAVI) maxScore = maxScoreForVI ; else if (maxScoreForCVI >= maxScoreForVI && maxScoreForCVI >= maxScoreForAVI) maxScore = maxScoreForCVI ; sinon maxScore = maxScoreForAVI ; maxScore ;

Scores de risque moyen de tous les éléments vulnérables

Calcule le score de risque moyen de tous les éléments vulnérables (hôtes, conteneurs et applications). var summedRiskScore = [[Score de risque cumulé des VIT]] + [[Score de risque cumulé des AVI]] + [[Score de risque cumulé des CVI]], avgRiskScore ; var totalVulCount = [[Éléments vulnérables ouverts]] + [[Éléments vulnérables de l'application ouverts]] + [[Éléments vulnérables conteneurs ouverts]] ; if(summedRiskScore == 0) avgRiskScore = 0 ; sinon if(totalVulCount .=0) avgRiskScore = summedRiskScore / totalVulCount ; score de risque moyen ;

Score de risque déployé des mauvaises configurations

Calcule le score de risque déployé d'erreur de configuration à l'aide des résultats des tests classés comme Échec, Erreur ou Inconnu. var maxRiskScore = 100 ; nombre de variables = [[Problèmes de configuration ouverts - Résultats des tests]] ; var countRiskScore ; si (0 == nombre) countRiskScore = 0 ; else if (nombre > 10000) countRiskScore = maxRiskScore ; sinon si (nombre > 1000) countRiskScore = (maxRiskScore * 0,80) ; sinon si (nombre > 100) countRiskScore = (maxRiskScore * 0,60) ; sinon si (nombre > 10) countRiskScore = (maxRiskScore * 0,40) ; sinon countRiskScore = (maxRiskScore * 0,20) ; var misRiskScore = ([[Obtenir le score du risque maximal pour les résultats des tests de configuration incorrecte]] * 0 + [[Obtenir le score de risque moyen pour les résultats des tests de configuration incorrecte]] * 100 + countRiskScore * 0)/100 ; misRiskScore ;

Délai moyen pour éradiquer

Calcule la durée moyenne nécessaire pour supprimer les incidents de sécurité en jours [[SI - Durée moyenne > l'état de l'incident de sécurité = éradiquer]] / 1 440

Délai moyen pour identifier

Calcule le temps moyen nécessaire pour identifier les incidents de sécurité en jours. [[SI - Durée moyenne d'identification]] / 1440

Délai moyen pour contenir

Calcule le temps moyen nécessaire pour contenir les incidents de sécurité en jours. [[SI : durée moyenne > l'état de l'incident de sécurité = maîtriser]] / 1 440

Respect de l'objectif de remédiation

Calcule le pourcentage mensuel de respect de la cible de rattrapage à partir des résultats des tests, des éléments vulnérables, des éléments vulnérables de conteneurs et des éléments vulnérables

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d’applications. Le respect de l’objectif est déterminé par le nombre d’éléments qui ont atteint l’objectif fixé. ([[SLA de résultat de test : compte réussi > état du rattrapage (unifié) = cible atteinte]] + [[SLA de conteneur : nombre de fermetures > état du rattrapage (unifié) = cible atteinte]] + [[SLA de l’application : nombre de fermetures > état du rattrapage (unifié) = cible atteinte]] + [[SLA hôte : nombre de fermetures > état de rattrapage (unifié) = cible atteinte]]) / ([[SLA de résultat de test : nombre de réussites]] + [[SLA de conteneur : nombre de fermetures]] + [[SLA de l’application : nombre de fermetures]] + [[SLA hôte : nombre de fermetures]]) * 100

Efficacité de la remédiation mensuelle (Tous les éléments vulnérables)

Calcule le pourcentage mensuel d’éléments vulnérables fermés, d’éléments vulnérables de conteneurs et d’éléments vulnérables d’applications, par opposition aux éléments nouvellement identifiés. var closedItems = [[SLA hôte - Nombre de fermetures]] + [[SLA de conteneur - Nombre de fermetures]] + [[SLA de l’application - Nombre de fermetures]] + [[SLA de résultat de test - Nombre de réussites]] ;

var newItems = [[VIT d’hôte ouverts/rouverts hier]] + [[VIT de conteneur ouverts/rouverts hier]] + [[VIT d’application ouverts/rouverts hier]] + [[Résultats des tests ouverts/rouverts hier]] ;

var res = 0 ; if (closedItems == 0) res = 0 ; else if (newItems .=0)res = closedItems / newItems * 100 ; si (res > 1000) res = 1000 ; Res;

VIT d'hôte ouverts/rouverts hier

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables de l’hôte qui ont été ouverts pour la dernière fois la veille au moment du calcul.

VIT d'application ouverts/rouverts hier

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables de l’application qui ont été ouverts pour la dernière fois le jour précédent au moment du calcul.

VIT de conteneur ouverts/rouverts hier

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables de conteneurs qui ont été ouverts pour la dernière fois le jour précédent au moment du calcul.

Résultats des test ouverts/rouverts hier

Cet indicateur est calculé quotidiennement. Il prend en compte les résultats des tests qui ont été observés pour la dernière fois la veille au moment du calcul.

Éléments vulnérables OT

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables OT actifs présents au moment du calcul.

Durée cumulée des éléments vulnérables OT fermés

Cet indicateur est calculé quotidiennement. Il prend en compte l’âge total de toutes les vulnérabilités OT qui sont fermées le jour du calcul.

Éléments vulnérables OT fermés

Cet indicateur est calculé quotidiennement. Il prend en compte les éléments vulnérables OT qui sont fermés le jour du calcul.

Âge moyen des éléments vulnérables actifs OT

Calcule l’âge moyen des éléments vulnérables OT ([[Âge cumulé des éléments vulnérables OT]] / [[Éléments vulnérables OT]])

Répartitions

- Unité business
- Services d'entreprise

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cotes de risque
- Tranche d'âges
- Groupe d'affectation (unifié)
- État de la cible de rattrapage (fermé)
- classe d'actifs
- Catégorie d'actif
- Évaluation du risque (unifiée)
- Raison de l'ajournement (unifiée)
- État de l'incident de sécurité
- Priorité de l'incident de sécurité
- Catégorie d'incident de sécurité
- Événement d'hameçonnage
- Raison de l’ajournement Non fermé (unifié)

Applications à activer

Vous devez activer les applications suivantes pour renseigner le score dans les widgets. En fonction de l’application que vous utilisez, vous devez activer les applications dépendantes.

Si vous utilisez	Activer
Réponse aux vulnérabilités	• Performance Analytics pour Vulnerability Response • Structure commune de Réponse aux vulnérabilités • Réponse aux vulnérabilités • Vulnerability Response et Configuration Compliance pour les conteneurs • Configuration Compliance
Operational Technology	Vulnerability Response pour Operational Technology
Intégrations de l'hameçonnage	• Intégration de la simulation et de la formation de sécurité pour SecOps • Intégration KnowBe4 pour SecOps • Intégration de Microsoft Defender pour Office 365 pour SecOps
Security Incident Response	• Analyse des performances pour Réponse aux incidents de sécurité • Security Incident Response • Gestion des incidents de sécurité majeurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous utilisez	Activer
Gouvernance, risque et conformité	• GRC : éléments communs du tableau de bord • GRC : Espace de travail de gestion des risques • GRC: Advanced Risk • GRC : Espace de travail pour la gestion de Compliance

Travaux planifiés pour la collecte de données

Les travaux planifiés suivants sont exécutés pour collecter automatiquement des scores sur de nouvelles données.

Tâche planifiée	Fréquence	Description
Charger les scores de point de référence	Sur demande	Collecte les scores de l'instance et les publie sur l'instance centrale. Les algorithmes de référence calculent les meilleurs scores du secteur.
Télécharger les scores de point de référence	Sur demande	Télécharge les scores de point de référence. Il est disponible dans le tableau des scores de point de référence [sn_bm_client_score_list].

S'abonner aux scores de point de référence

Obtenez les scores de point de référence en inscrivant votre instance à l'instance ServiceNow centrale. Ce dernier conserve des informations sur plusieurs industries pour fournir le score de référence.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur le benchmarking, reportez-vous à la section Explorer Benchmarks .

Procédure

1. Pour enregistrer votre instance auprès de l'instance centrale, procédez comme suit :

   a. Accédez à la **Tous** > **Propriétés système** > **Toutes les propriétés**.

   b. Sélectionnez la `sn_bm_client.central_instance_url` propriété système.

   c. Dans le champ **Valeur** , entrez l'URL de l'instance centrale de point de référence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si l'instance est mise en service, vos informations sont transmises automatiquement à l'instance centrale.

d. Sélectionnez **Opt-in** dans le widget pour valider et établir une connexion avec l'instance centrale.

2. Pour charger votre score dans l'instance centrale, procédez comme suit :

a. Accédez à la **Tous** > **Planificateur système** > **Travaux planifiés**

b. Sélectionnez la *`Upload the benchmark scores`* tâche planifiée.

c. Sélectionnez **Mettre à jour**.
Les scores sont téléchargés sur l'instance centrale. Toutefois, les travaux planifiés par l'instance centrale s'exécutent une fois par mois pour mettre à jour les scores sur les widgets du tableau de bord.

3. Pour télécharger la partition à partir de l'instance centrale, procédez comme suit :

a. Accédez à la **Tous** > **Planificateur système** > **Travaux planifiés**

b. Sélectionnez la *`Download the benchmark scores`* tâche planifiée.

c. Sélectionnez **Exécuter maintenant**.
Les scores sont disponibles dans la table des scores de point de référence [sn_bm_client_score_list], qui est reflétée dans les widgets du tableau de bord.

Définir des cibles

Définissez des cibles en jours pour corriger les vulnérabilités, les incidents de sécurité et les erreurs de configuration.

Avant de commencer

Rôle requis : admin

Procédure

1. Sélectionnez **Cibles** sur le widget ou sélectionnez l'icône **Cibles** sur la page Détails des KPI.
2. Sélectionnez le bouton **Pour tout le monde** .
3. Dans le champ **Nouvelle valeur** , entrez le nombre de jours pendant lesquels vous souhaitez atteindre la cible.
4. Sélectionnez la date de début de la cible.
5. Sélectionnez la date d'examen cible.
6. Sélectionnez **Mettre à jour**.

Intégration de la simulation et de la formation de sécurité pour Security Operations

Renforcez la défense de votre organisation contre les menaces de cybersécurité importantes en intégrant des intégrations de phishing au tableau de bord de direction de la cybersécurité. Les intégrations d'hameçonnage améliorent le tableau de bord de direction

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de cybersécurité en intégrant de manière transparente les données provenant d'outils de simulation d'hameçonnage tiers tels que KnowBe4 et Microsoft Defender pour Office 365.

Les intégrations suivantes améliorent les capacités du tableau de bord de direction de cybersécurité, offrant une perspective unifiée sur la posture de sécurité de votre organisation, la préparation des employés et la vulnérabilité aux attaques d'hameçonnage :

- Intégration KnowBe4
- Intégration de Microsoft Defender pour Office 365

Configurer l'intégration Knowbe4

Obtenez des informations immédiates sur la vulnérabilité de votre personnel aux attaques de phishing en l'intégrant à KnowBe4, une plateforme de formation de sensibilisation à la cybersécurité de premier plan. Grâce à l'intégration de KnowBe4, identifiez les tendances et les domaines d'amélioration dans vos programmes de formation en cybersécurité, surveillez la résilience globale au phishing et renforcez de manière proactive les mesures de sécurité de votre organisation.

Avant de commencer

Rôle requis : sn_sec_phish.admin et sn_sec_phish_kb4.kb4_admin

Procédure

1. Accédez à la **Tous** > **Intégration KnowBe4** > **KnowBe4 Configurations**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs suivants du formulaire :

Formulaire de configuration KnowBe4

Champ	Description
Instance d'intégration	Nom de l'instance d'intégration. Sélectionnez l'instance d'intégration à l'aide de l'icône de recherche.
URL de base	URL à intégrer à KnowBe4.
Clé API	Clé API acquise à partir du compte KnowBe4.
Page	Numéro de page à partir duquel les simulations doivent être extraites.
Taille de page	Nombre de simulations à inclure.

a. Sélectionnez **Nouveau** si aucune instance d'intégration n'est disponible.

b. Renseignez les champs suivants du formulaire :

Formulaire Instance d'intégration

Champ	Description
Nom	Nom de l'instance d'intégration.
Application	Nom de l'application (KnowBe4 Integration for SecOps).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Intégration	KnowBe4 est la valeur par défaut.
Actif	La valeur par défaut est activée (sélectionnée). Si elle est décochée, l'instance n'est pas active.
Description	Brève description de l'instance d'intégration.

4. Sélectionnez **Soumettre**.
5. Accédez à la **Tous** > **Simulation et formation de sécurité** > **Intégrations**.
6. Sélectionnez l'intégration Knowbe4.
7. Sélectionnez **Exécuter maintenant** pour exécuter et collecter des données à partir de KnowBe4.

Configurer l'intégration de Microsoft Defender pour Office 365

Obtenez des informations précieuses sur les mesures de simulation d'hameçonnage directement dans le tableau de bord de direction de cybersécurité grâce à une intégration transparente avec Microsoft Defender pour Office 365.

Avant de commencer

Rôle requis : sn_sec_phish_msatk.ms_admin

Pourquoi et quand exécuter cette tâche

Pour en savoir plus sur la simulation d'une attaque de phishing et la configuration d'un locataire, consultez :

- Simuler une attaque de phishing avec la formation de simulation d'attaque
- Premiers pas avec la formation de simulation d'attaque
- Configurer un locataire

Procédure

1. Accédez à la **Tous** > **Intégration des attaques Microsoft** > **Configurations d'attaques Microsoft**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs suivants du formulaire :

Formulaire Configuration des attaques Microsoft

Champ	Description
Instance d'intégration	Nom de l'instance d'intégration. Sélectionnez l'instance d'intégration à l'aide de l'icône de recherche.
ID de locataire	ID de locataire de l'application créée sur le portail Microsoft Azure.
ID client	ID client de l'application créée sur le portail Microsoft Azure.
Secret client	Clé secrète client de l'application créée sur le portail Microsoft Azure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Signet	Date à partir de laquelle les simulations doivent être extraites.
URL de jeton	URL de base à partir de laquelle le jeton est créé pour accéder à l'API de simulation Microsoft.
Toutes les URL de simulation	URL de base de l'API de simulation Microsoft.

a. Sélectionnez **Nouveau** si aucune instance d'intégration n'est disponible.

b. Renseignez les champs suivants du formulaire :

Formulaire Instance d'intégration

Champ	Description
Nom	Nom de l'instance d'intégration.
Application	Nom de l'application (Microsoft Defender pour Office 365).
Intégration	Référence d'intégration tierce (intégration des attaques Microsoft).
Actif	La valeur par défaut est activée (sélectionnée). Si elle est décochée, l'instance n'est pas active.
Description	Brève description de l'instance d'intégration.

4. Sélectionnez **Soumettre**.
5. Accédez à la **Tous** > **Simulation et formation de sécurité** > **Intégrations**.
6. Sélectionnez l'intégration des attaques Microsoft.
7. Sélectionnez **Exécuter maintenant** pour exécuter et collecter des données à partir de Microsoft.

Tableau de bord de risque et conformité pour GRC : Mesures

Le tableau de bord Risque et conformité fournit aux utilisateurs de conformité et de risque une vue d'ensemble complète des informations relatives au risque et à la conformité dans un tableau de bord unique qui les aide à prendre des décisions clés.

Vous pouvez accéder au tableau de bord de risque et conformité à partir du tableau de bord unifié unique Tableau de bord de direction de cybersécurité pour afficher les mesures de risque et de conformité des Gouvernance, risque et conformité applications.

Le tableau de bord fournit des fonctionnalités telles que :

- Vue d'ensemble de la conformité
- Vue d'ensemble du risque
- Vue d'ensemble de la confidentialité
- Vue d'ensemble de la continuité d'activité
- Risque de tiers
- Vue d'ensemble de l'audit

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions préalables pour accéder au tableau de bord de risque et conformité

Important : Vous devez disposer de l'accès Tableau de bord de direction de cybersécurité primaire pour activer le module d'extension fonctionnel Cybersécurité et risque qui vous permet d'accéder au tableau de bord de risque et conformité.

Un nouveau domaine fonctionnel est introduit pour séparer les données relatives à la cybersécurité et aux risques. Vous pouvez activer le module d'extension Cybersécurité et risque en sélectionnant le bouton **Activer** l'action d'interface utilisateur. Par défaut, ce domaine fonctionnel est inactif.

Rôles ServiceNow AI Platform requis

Le rôle d'utilisateur principal GRC est le sn_grc_dashboards.grc_ciso_user qui peut afficher les rapports sur le tableau de bord de risque et conformité. Ce rôle comprend :

- sn_compliance.reader
- sn_risk.reader

Remarque : Toutefois, vous devez disposer du rôle sn_bod.ciso pour vous connecter, afficher et partager le tableau de bord de direction de cybersécurité à partir duquel vous pouvez naviguer vers le tableau de bord de risque et conformité.

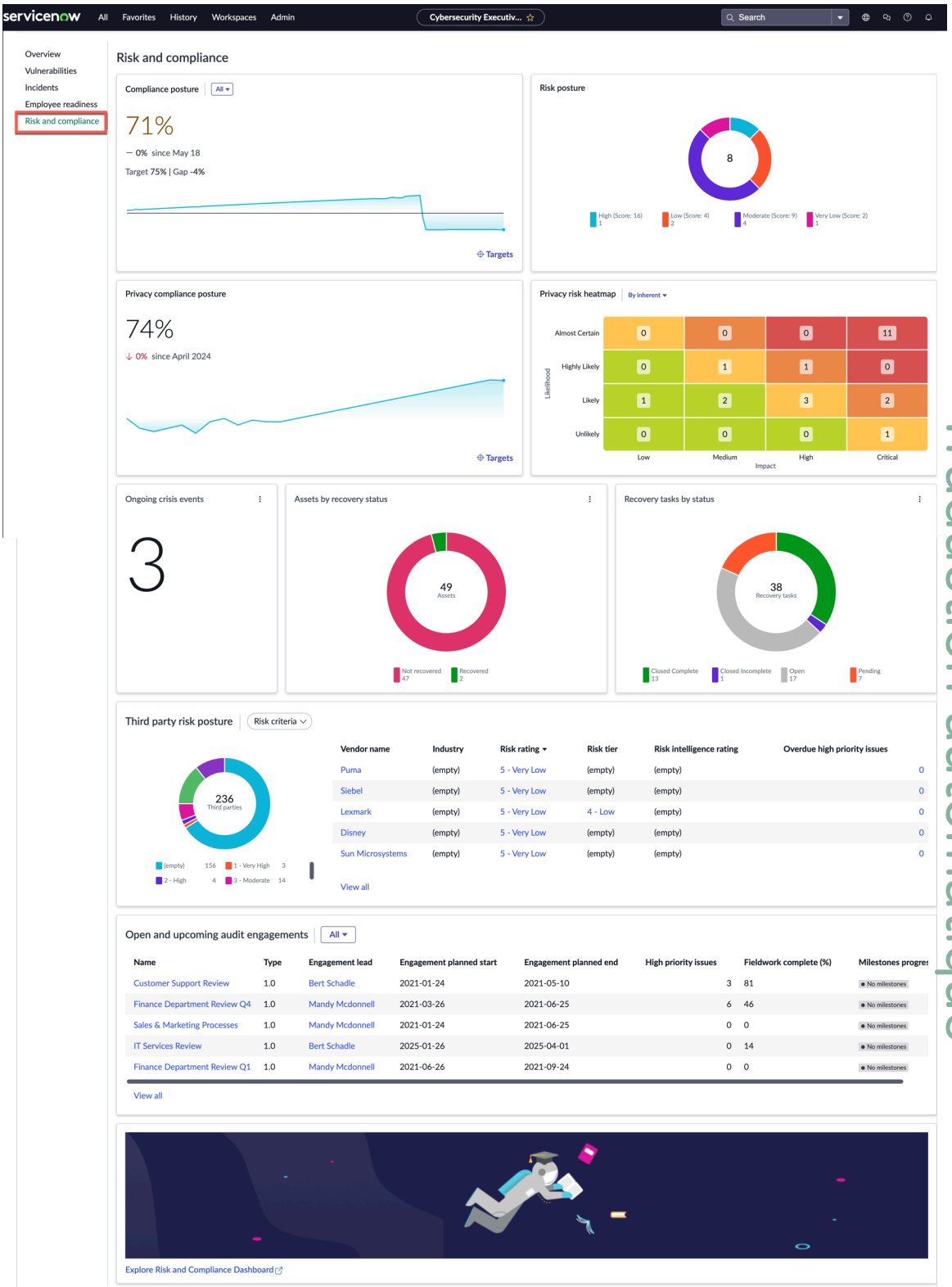
Accéder au tableau de bord de risque et conformité

1. Pour accéder au tableau de bord de risque et conformité, accédez à **Tous** > **Tableau de bord de direction de cybersécurité** > **Tableau de bord de direction de cybersécurité**.
2. Sélectionnez l'étiquette **Risque et conformité** dans la liste située à gauche du tableau de bord.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord de direction de cybersécurité unifié pour les mesures de risque et de conformité



3. Pour visualiser vos données, et pour afficher les rapports et solutions disponibles sur le tableau de bord conçu pour l'utilisateur, sélectionnez l'étiquette Explorer le tableau de bord Risque et conformité.

Traduction automatique

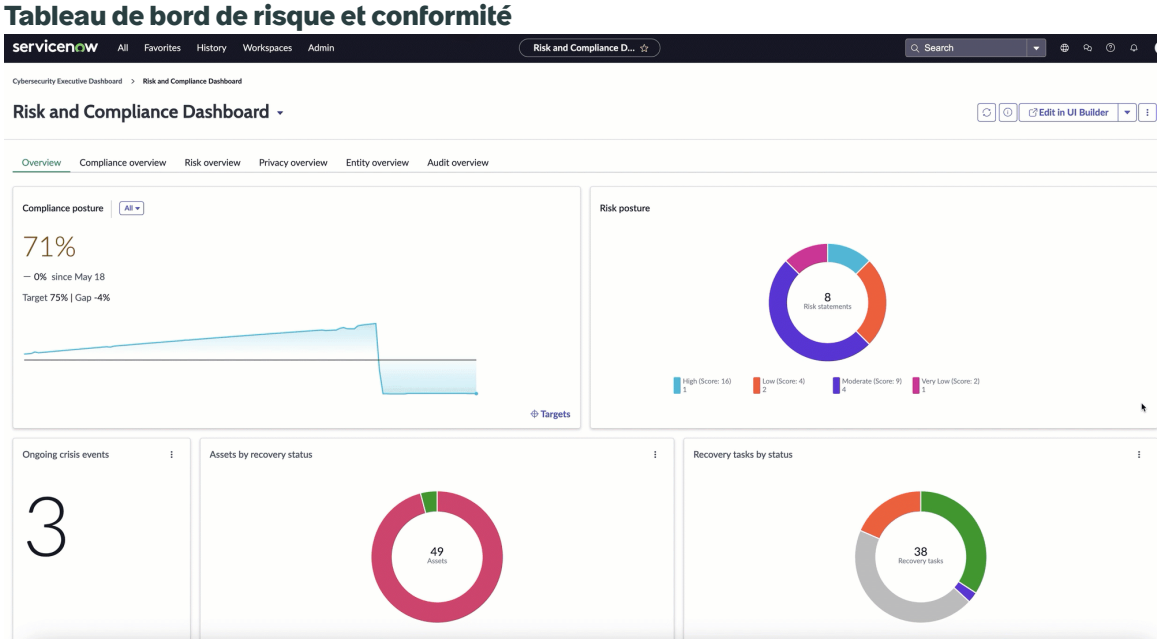
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Risque et conformité Rapports et solutions de tableau de bord

Le tableau de bord Risque et conformité est un tableau de bord unifié qui fournit des données analytiques complètes des rapports disponibles à partir des principales applications GRC pour que le responsable de la sécurité de l'information comprenne la conformité et la posture de risque de l'organisation. Le tableau de bord consolide les données de divers produits au sein de la ServiceNow GRC suite d'applications.

Remarque : Tous les rapports ne sont disponibles que lorsque les espaces de travail correspondants sont installés.

Tableau de bord de risque et conformité



Rôles ServiceNow AI Platform requis

Pour les rapports associés à la conformité

L'utilisateur doit disposer d'un rôle sn_grc_dashboards.grc_ciso_user et d'un rôle sn_bod.ciso.

Pour les rapports liés aux risques

L'utilisateur doit disposer d'un rôle sn_grc_dashboards.grc_ciso_user et d'un rôle sn_bod.ciso.

Pour les rapports associés à Business Continuity Management

L'utilisateur doit avoir un rôle sn_bcm.viewer et un rôle sn_bod.ciso.

Pour les rapports associés aux risques de tiers

L'utilisateur doit disposer du rôle sn_vdr_risk_asmt.vendor_assessment_reviewer et du rôle sn_bod.ciso.

Pour les rapports liés à la confidentialité

L'utilisateur doit avoir un rôle sn_privacy.analyst et un rôle sn_bod.ciso.

Pour les rapports associés à l'audit

L'utilisateur doit disposer du rôle sn_audit_ws.auditor et du rôle sn_bod.ciso.

Accéder au tableau de bord de risque et conformité

Pour ouvrir le tableau de bord, accédez à **Tous** > **Tableau de bord de direction de cybersécurité** > **Tableau de bord de direction de cybersécurité**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateurs

Posture de conformité

- Pourcentage de conformité : indicateur de formule qui décrit la posture de conformité.
- Tous les contrôles : indicateur automatisé qui prend en charge l'indicateur de formule.
- Contrôles conformes : indicateur automatisé qui prend en charge l'indicateur de formule.

Posture de conformité en matière de confidentialité

Indicateur PA : score de conformité de l'activité de traitement (%)

Répartitions

Domaine fonctionnel.

Rapports

Remarque : Tous les rapports ne sont disponibles que lorsque les espaces de travail correspondants sont installés.

Onglet Vue d'ensemble

Titre	Type	Table source	Description
Posture de conformité	Graphique linéaire	Contrôle [sn_compliance_control]	Fournit aux gestionnaires de conformité des systèmes de cybersécurité et de risque, ainsi que de risque informatique et de conformité en fonction de l'analyse des données.
Situation vis-à-vis du risque	Graphique en anneau	Les tables sources sont les suivantes : • Risque [sn_risk_risk] • Risque agrégé détaillé [sn_risk_advanced_risk_assessment_result] (lorsque l'application est installée et que l'évaluation Risque avancé Advanced Risk est activée	Fournit le nombre de risques en fonction des évaluations de risque.
Événements de crise en cours	Score unique	Événement de reprise [sn_recovery_event] où le type d'événement est réel	Affiche le nombre total d'événements de crise en cours qui ne sont ni approuvés ni fermés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble (suite)

Titre	Type	Table source	Description
Ressources par état de reprise	Graphique en anneau 	Actifs [sn_recovery_event_asset]	Fournit le nombre total d'actifs pour les événements de crise en cours regroupés par leur état de reprise, y compris les actifs qui ont été récupérés et ceux qui ne l'ont pas été.
Tâches de reprise par état	Graphique en anneau 	Tâches de reprise [sn_recovery_event_task]	Fournit l'état des tâches de reprise dans différents états pour les événements de crise en cours.

Onglet Vue d'ensemble de la conformité

Titre	Type	Table source	Description
Documents de référence	Graphique en anneau 	Source de référence [sn_compliance_authority_document]	Fournit les données des documents de référence conformes et non conformes dans le graphique. La liste fournit des détails sur les documents de référence, leur score de conformité individuel en pourcentage, le nombre de problèmes de priorité élevée et d'exceptions à risque élevé sur les documents de référence, ainsi que le nombre de tickets de conformité.
Politiques	Graphique en anneau 	Politique [sn_compliance_policy]	Fournit le nombre de politiques conformes et non conformes dans le graphique. La liste fournit des détails sur les politiques, leur score de conformité individuel en pourcentage, le nombre de problèmes de priorité élevée et d'exceptions de risque soulevés sur chaque politique, ainsi que le nombre de tickets de conformité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble des risques

Titre	Type	Table source	Description
Situation vis-à-vis du risque	Graphique en anneau 	Les tables sources sont les suivantes : • Risque [sn_risk_risk] • Risque agrégé détaillé [sn_risk_advanced_risk_assessment_result] (Lorsque l'application est installée et que l'évaluation Risque avancé Advanced Risk est activée)	Fournit le nombre de risques en fonction des évaluations de risque.
Situation vis-à-vis du risque		État du contenu GRC [sn_grc_content_reports]	Fournit la cote de risque pour chaque risque organisationnel afin de comprendre les résultats globaux de l'évaluation des risques. Ces évaluations aident les organisations à comprendre l'impact potentiel et la probabilité de divers risques, ce qui leur permet de hiérarchiser et de gérer ces risques. La carte de situation vis-à-vis du risque met également en évidence les informations suivantes pour chaque risque : • **Appétit au risque** : valeur de l'appétit au risque définie. • **Problèmes de priorité élevée** : le nombre de problèmes de priorité est défini comme élevé. • **Tâches de réponse aux risques en retard** : nombre de tâches de réponse aux risques en retard.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble des risques (suite)

Titre	Type	Table source	Description
			• **% de violation de KRI** : pourcentage d'indicateurs de risque clés (KRI) qui ont dépassé leurs seuils ou limites prédéfinis.
Situation de risque de tiers	Graphique en anneau	Risques tiers [sn_grc_dashboards_third_party_risk]	Fournit la cote de risque pour chaque tiers. L'évaluation des risques est l'évaluation globale qui prend en compte les scores et les évaluations de toutes les évaluations effectuées pour un tiers ou un fournisseur. La carte de posture du risque du tiers met également en évidence les informations suivantes pour chaque tiers ou fournisseur : • **Critères de risque** : groupe de domaines de risque (parfois appelés domaines de risque dans d'autres fonctionnalités de la plateforme) qui s'applique à un type particulier de tiers. • **Hiérarchisation du risque** : valeur déterminée en fonction des réponses recueillies après l'achèvement d'une évaluation inhérente des risques (IRQ). • **Cote des renseignements** sur les risques : agrégat de tous les scores collectés auprès des fournisseurs de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d'ensemble des risques (suite)

Titre	Type	Table source	Description
			renseignements sur les risques. • **Tâches de réponse aux risques en retard** : nombre de tâches de réponse aux risques en retard.

Onglet Vue d'ensemble de la confidentialité

Titre	Type	Table source	Description
Posture de conformité en matière de confidentialité	Ligne	Indicateur PA : score de conformité de l'activité de traitement (%) [pa_indicators]	Fournit la posture de conformité par mois et est tracé en se référant au score de conformité global de toutes les activités de traitement.
Questions de haute priorité en retard	Score unique	Problèmes [sn_grc_issue]	Fournit une vue d'ensemble ciblée de tous les problèmes de confidentialité hautement prioritaires en retard, permettant une identification et une résolution rapides des tâches critiques pour garantir la conformité et la protection des données.
Carte thermique des risques de confidentialité	Carte thermique	Méthodologie d'évaluation des risques [sn_risk_advanced_risk_assessment_methodology]	Fournit les données d'évaluation des risques pour la confidentialité sous la forme d'une carte thermique. Les évaluations des risques de confidentialité sont des évaluations détaillées qui sont effectuées si le score de criticité est élevé. Évaluez chaque risque associé à l'activité de traitement et connaissez le score de risque agrégé de l'activité de traitement. Après avoir évalué les risques pour la confidentialité, vous pouvez afficher la situation en matière de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Vue d’ensemble de la confidentialité (suite)

Titre	Type	Table source	Description
			risque de confidentialité sur la carte thermique des risques.

Onglet Vue d’ensemble de l’entité

Titre	Type	Table source	Description
Entités		Statut de conformité de l’entité [sn_compliance_entities_reporting]	Fournit le résumé des risques directement associés à l’entité qui contribuent à la cote de risque globale de l’entité. La liste affiche également le score de conformité des entités, ainsi que les problèmes de priorité élevée et les exceptions de risque qui sont soulevés en raison des contrôles non conformes associés à l’entité.

Onglet Vue d'ensemble de l'audit

Titre	Type	Table source	Description
Engagements d'audit ouverts et à venir		Engagement [sn_audit_engagement]	Fournit une liste des engagements d’audit ouverts et à venir. La liste fournit également des détails sur le responsable de mission pour chaque document de référence, les dates de début et de fin prévues de chaque mission, les problèmes hautement prioritaires, le pourcentage de travail sur le terrain achevé et les jalons en cours.

Filtres

Nom	Type	Description
Critère de risque	Rapport	En fonction des critères de risque que vous sélectionnez, le graphique en anneau et la liste affichent les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

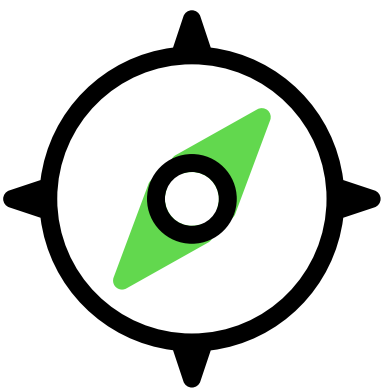
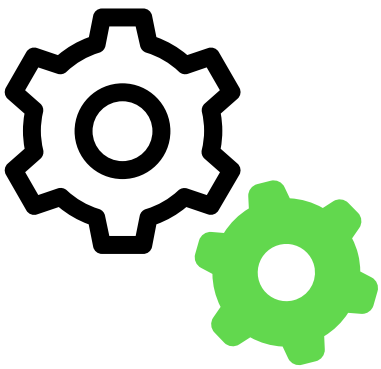
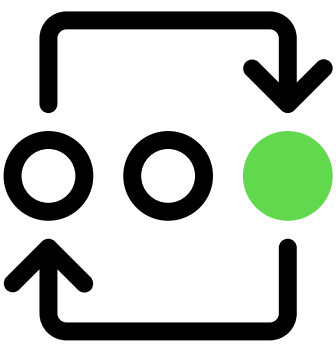
Nom	Type	Description
		tiers ou fournisseurs qui se trouvent dans ces domaines de risque.

Centre de sécurité des renseignements sur les menaces

La Centre de sécurité des renseignements sur les menaces plateforme (TISC) fournit une solution technologique pour l'agrégation, la gestion et l'opérationnalisation des renseignements sur les menaces.

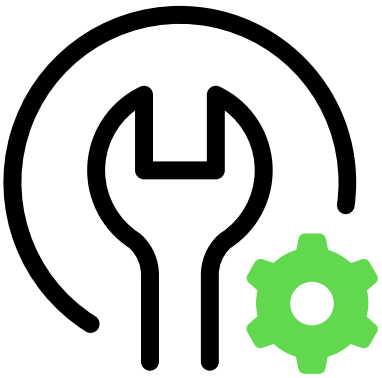
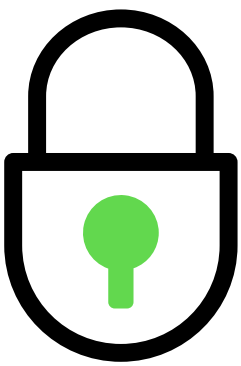
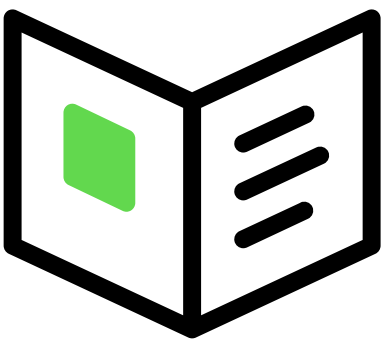
Premiers pas

Cliquez sur une tuile pour commencer.

Explorer	Configurer	Intégrer
		
Découvrez comment Threat Intelligence Security Center peut vous aider grâce à ses principales fonctionnalités et avantages.	Installez et configurez Threat Intelligence Security Center pour répondre à vos besoins spécifiques.	Intégrer à Threat Intelligence Security Center

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Administrer	Utiliser	Modèles de rapports
		
Gérez et personnalisez votre centre de sécurité des renseignements sur les menaces.	Gérez votre bibliothèque et vos objets du centre de sécurité des renseignements sur les menaces.	Gérez et personnalisez vos rapports de gestion des tickets.
Référentiel MITRE ATT&CK	TISC Archivage des données Archivez	Référence
		
Gérez les données du référentiel MITRE ATT&CK.	, gérez les règles d'archivage et de destruction des données.	Obtenez des informations supplémentaires sur le Centre de sécurité des renseignements sur les menaces.

Traduction automatique

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

L'installation Centre de sécurité des renseignements sur les menaces de (sn_sec_tisc) installera automatiquement toutes les applications dépendantes à partir de ServiceNow Store.

Plus de ressources

Visitez le Réponse aux incidents de sécurité forum sur le ServiceNow Community.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage et demande d'aide

- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Explorer Centre de sécurité des renseignements sur les menaces

Centre de sécurité des renseignements sur les menaces (TISC) vous permet de collaborer avec les équipes de renseignements sur les menaces, dispose de plusieurs options pour collecter et traiter divers flux de renseignements sur les menaces, ainsi que d'un espace de travail pour analyser, collaborer, agir et partager les informations nécessaires.

Regardez une vue d'ensemble de l'application Centre de sécurité des renseignements sur les menaces .

https://player.vimeo.com/video/1020328039?h=33e58d6e14&badge=0&autopause=0&player_id=0&app_id=58479

Le Centre de sécurité des renseignements sur les menaces est doté d'options permettant de gérer la collecte et le traitement des données (DEDUPLICATION, normalisation et agrégation), l'analyse des renseignements sur les menaces, la diffusion des renseignements sur les menaces, ainsi que l'espace de travail qui fournit les tâches d'administration.

Fonctionnalités principales

Centre de sécurité des renseignements sur les menaces offre une suite complète et robuste de fonctionnalités conçues pour améliorer les capacités de Threat Intelligence pour les équipes de sécurité :

- **Catalogue organisé de flux de menaces OSINT** : donne accès à une large sélection de flux de renseignements sur les menaces open source populaires, garantissant une large couverture.
- **Intégration de flux premium** : améliore la qualité des renseignements sur les menaces en incorporant des sources premium aux données OSINT.
- **Extraction automatisée d'observables** : identifie et extrait automatiquement tous les observables pertinents des fichiers chargés, rationalisant ainsi l'ingestion de données.
- **Agrégation de données diverses** : prend en charge plusieurs formats de données, notamment STIX, MISP, JSON et autres, permettant une consolidation transparente du flux.
- **Enrichissement et validation** : supprime les faux positifs, attribue des scores de confiance, valide les indicateurs et ajoute des informations contextuelles précieuses pour améliorer la qualité des données.
- **Moteur de règles de corrélation** : établit automatiquement des relations entre les observables, ce qui permet d'obtenir un aperçu plus approfondi des modèles de menace.
- **Score de menace personnalisable** : permet d'affiner les scores de menace pour une évaluation plus nuancée et précise des menaces.
- **Intégration de l'intelligence interne** : combine les flux externes avec les données internes provenant des rapports de vulnérabilité (VR), de Security Incident Response (SIR), des actifs, des services et de la CMDB.
- **Tableaux de bord spécifiques à l'utilisateur** : adapte les visualisations et les vues de données en fonction des profils Threat Intelligence, améliorant ainsi l'expérience utilisateur et la pertinence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Outils de visualisation graphique** : facilite la compréhension des données complexes des renseignements sur les menaces grâce à une représentation graphique intuitive.
- **Espace de travail dédié à l'analyste** : fournit un espace de travail d'analyste dédié et rationalisé Renseignements sur les menaces qui permet aux analystes du renseignement sur les menaces de se concentrer sur l'enquête et l'analyse avec un minimum de distractions.
- **Chasse aux menaces avec Gestion des tickets** : prend en charge les workflows d'enquête avec le suivi des tâches et la gestion des tickets.
- **Intégration MITRE ATT&CK** : permet aux utilisateurs de lier les enregistrements de tickets aux données du cadre de travail MITRE ATT&CK pour une analyse contextuelle améliorée.
- **Intégration SIR transparente** : Assure une migration fluide des données et l'interopérabilité entre Renseignements sur les menaces les Réponse aux incidents de sécurité applications et les Centre de sécurité des renseignements sur les menaces.
- **Règles de notification et d'alerte** : établit des alertes de déclenchement pour informer les équipes en fonction de l'évolution des renseignements sur les menaces.
- **Politiques de nettoyage et de conservation des données** : permet aux organisations de définir des règles de gestion des données pour maintenir les performances et la conformité des applications.
- **Reporting & Collaboration** : Génère des rapports d'état et des résumés d'enquête complets à l'aide d'éditeurs de texte enrichi et de modèles personnalisables.
- **Séparation de domaine pour les MSSP** : prend en charge les environnements mutualisés, ce qui permet aux fournisseurs de services de sécurité gérés (MSSP) de séparer les données des clients en toute sécurité.
- **Intégration étendue de l'API** : Offre une API TISC pour une connectivité transparente avec d'autres outils et plateformes de sécurité.

Terminologie clé TISC

Les termes définis ci-dessous sont utilisés dans l'ensemble du Centre de sécurité des renseignements sur les menaces (TISC).

Définitions terminologiques

Terminologie	Définition
Traitement des données	Une plateforme de renseignements sur les menaces (TIP) est une solution technologique qui collecte, agrège et organise des données de veille sur les menaces provenant de diverses sources et modèles. Les renseignements sur les menaces sont les données qui sont collectées, traitées et analysées pour comprendre les cibles et les comportements d'attaque des acteurs de la menace.
Observables	Les observables représentent des propriétés avec état (telles que le hachage MD5 d'un fichier ou la valeur d'une clé de registre) ou des événements mesurables (tels que la création d'une clé de registre ou la suppression d'un fichier) qui sont pertinents pour le fonctionnement des ordinateurs et des réseaux. Pour plus d'informations, consultez Observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définitions terminologiques (suite)

Terminologie	Définition
Indicateurs	Les indicateurs contiennent un modèle qui peut être utilisé pour détecter les cyberactivités suspectes ou malveillantes. Par exemple, un indicateur peut être utilisé pour représenter un ensemble de domaines malveillants et utiliser le langage de modèle STIX pour spécifier ces domaines. Le SDO d'indicateur contient une description textuelle simple, les phases de kill chain dans lesquelles il détecte le comportement, une fenêtre de temps indiquant quand l'indicateur est valide ou utile, et une propriété de **modèle** requise pour capturer un modèle de détection structuré. Pour plus d'informations, consultez Indicateurs.
Objets	Définit l'ensemble des objets de domaine STIX (SDO), chacun correspondant à un concept unique communément représenté dans Cyber Threat Intelligence (CTI). En utilisant les SDO et les objets de relation STIX (SRO) comme éléments de base, les individus peuvent créer et partager des renseignements sur les cybermenaces vastes et complets. Pour plus d'informations, consultez Référentiel de bibliothèque TISC.
Relations	Une relation est un lien entre deux observables ou deux SDO ou un observable et un SDO qui décrit la façon dont les objets sont liés. Les relations peuvent être représentées à l'aide d'un objet de relation STIX (SRO) externe ou, dans certains cas, par certaines propriétés qui stockent une référence d'identificateur qui comprend une relation intégrée. Pour plus d'informations, consultez Objets de relations.

Afficher la TISC page d'accueil

Utilisez la page d'accueil TISC , qui est la page de destination, pour visualiser les données relatives à Threat Intelligence.

Avant de commencer

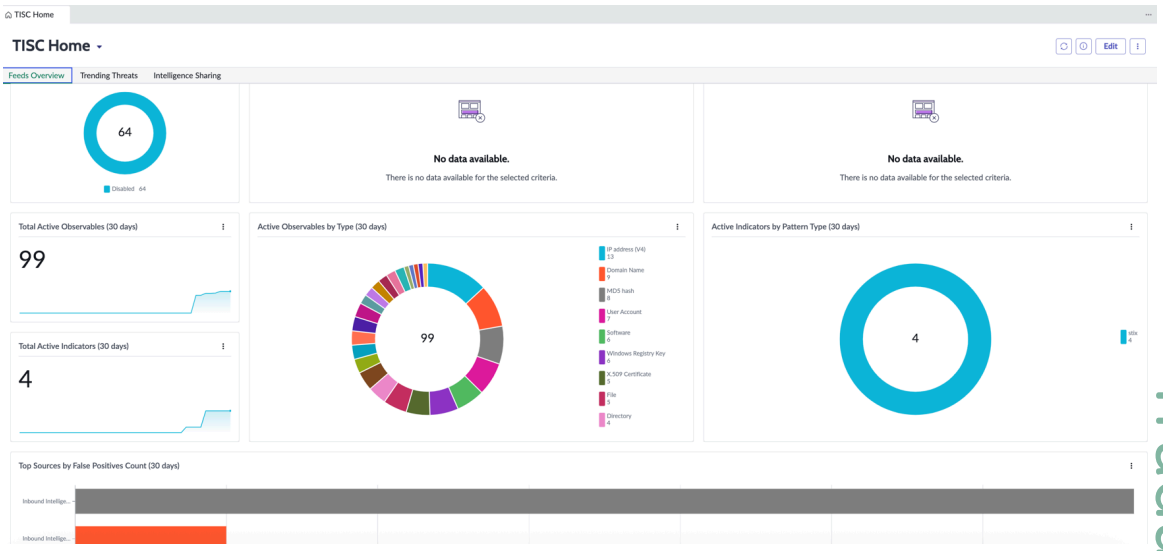
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
   La page d'accueil TISC s'affiche.



2. Afficher la page d'accueil TISC avec différentes données de widgets.
   La page d'accueil se compose de trois onglets différents : **Vue d'ensemble des flux**, **Tendances des menaces et Partage d'intelligence**. Le contenu de la page d'accueil provient de diverses sources telles que des observables, des indicateurs et des flux de données.

   a. **Vue d'ensemble des flux** : cet onglet fournit une vue d'ensemble de haut niveau des différentes sources ingérées par les données et des sources configurées pour l'ingestion de données.

Vue d'ensemble des flux

Nom du widget	Description	Action
Nombre de sources	Affiche le nombre de sources par état, par exemple brouillon, activé ou désactivé dans le système.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Sources actives par type de source	Affiche la distribution des sources actives par type de source.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Sources actives par format de flux	Affiche le nombre de sources activées par type de flux.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Nombre total d'observables actifs (30 jours)	Affiche les 10 premières sources par volume d'enregistrements de renseignements qui ont été créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Observables actifs par type	Affiche le volume total supérieur d'agrégats d'observables créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom du widget	Description	Action
		sélectionné s'ouvre dans un nouvel onglet.
Indicateurs actifs par type de modèle	Affiche le volume total d'agrégats d'indicateurs par type de modèle qui ont été créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Nombre total d'indicateurs actifs (30 jours)	Affiche le volume total d'agrégats d'indicateurs qui ont été créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Principales sources par nombre de faux positifs (30 jours)	Affiche le volume total d'observables de faux positif créés au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.

b. Tendances des menaces : cet onglet fournit une vue d'ensemble de haut niveau des tendances en matière de menaces.

Tendances des menaces

Nom du widget	Description	Action
Rapports les plus récents (les 10 principaux)	Affiche la liste des rapports et des liens : les 10 premiers classés par date de publication.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Derniers flux RSS (les 10 principaux)	Affiche la liste des flux RSS et des liens - Les 10 premiers classés par date de publication.	Lorsque vous cliquez sur ce widget, la page de liste s'ouvre avec les enregistrements filtrés.
Observables actifs par plage de score de menace (30 jours)	Affiche le nombre d'observables créés au cours des 30 derniers jours, répartis par plage de score de menace.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Observables actifs par réputation (30 jours)	Affiche le nombre d'observables créés au cours des 30 derniers jours, répartis par réputation.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Balises principales (30 jours)	Affiche les principales balises sur les enregistrements créés au cours des 30 derniers jours en fonction de la fréquence d'utilisation.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.
Secteurs les plus ciblés (30 jours)	Affiche les 10 premiers secteurs classés en fonction des activités déclarées qui ont été créées au cours des 30 derniers jours.	Lorsque vous cliquez sur ce widget, la page des détails des KPI du widget pour le filtre sélectionné s'ouvre dans un nouvel onglet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer Centre de sécurité des renseignements sur les menaces

Configurez les fonctionnalités, les composants et les intégrations dont vous avez besoin pour fournir un service et une assistance à vos clients.

Télécharger l'application TISC à partir du ServiceNow Store

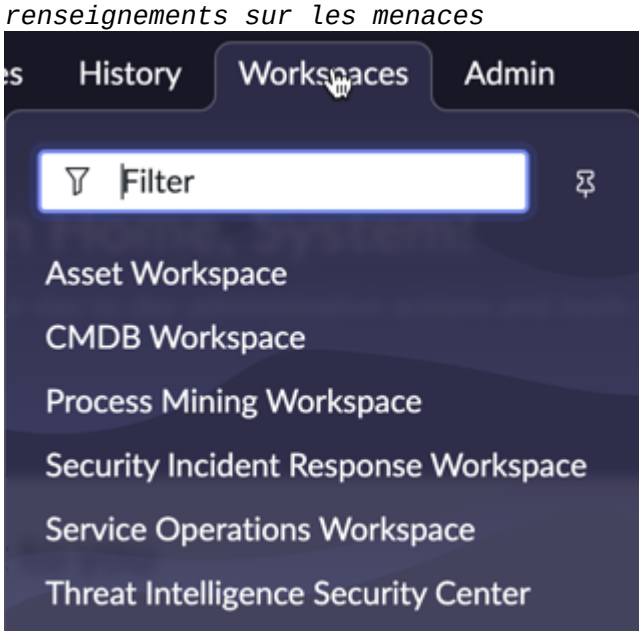
Avant d'exécuter l'application Centre de sécurité des renseignements sur les menaces dans votre instance, vous devez la télécharger à partir de et l'installer ServiceNow® Store .

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Suivez les instructions pour Télécharger une application à partir de ServiceNow Store et installer l'application **Security Operations du Centre de renseignements sur les renseignements sur les menaces** .
2. Une fois l'installation terminée, vous pouvez ouvrir l'espace de Centre de sécurité des renseignements sur les menaces travail en accédant à **Espaces de travail** > *`Centre de sécurité des renseignements sur les menaces`*



Que faire ensuite

Une fois que vous avez téléchargé l'application, vérifiez que vous avez terminé toutes les tâches mentionnées ici dans cette section Configurer Threat Intelligence Security Center pour une intégration fluide.

Configurer Threat Intelligence Security Center

Avant d'utiliser le Centre de sécurité des renseignements sur les menaces, vous devez le télécharger à partir du ServiceNow Store.

Rôles installés

Examinez les informations suivantes et vérifiez que vous avez terminé toutes les tâches pour une intégration fluide. Vous trouverez ci-dessous la liste des différents profils d'utilisateur définis pour accéder à l'application et travailler avec celle-ci :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Analyste Threat Intelligence (sn_sec_tisc.analyst)
- Administrateur Threat Intelligence (sn_sec_tisc.admin)

Droits applicables aux rôles TISC

Configuration	Description
Affectez et vérifiez les rôles requis ServiceNow AI Platform et Centre de sécurité des renseignements sur les menaces.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • En tant qu'administrateur, vous devez installer l'application TISC à partir du ServiceNow magasin et affecter le rôle en tant que sn_sec_tisc.admin. • Ce rôle sn_sec_tisc.admin effectue les tâches suivantes : ◦ Configure les sources de données pour ingérer les données. Pour plus d'informations, consultez Flux Threat Intelligence. ◦ Configuration des intégrations requises pour l'enrichissement des données observables dans TISC. Pour plus d'informations, consultez Intégrations de l'enrichissement TISC. ◦ Configure les rôles d'approbation d'importation de données pour l'importation de données à l'aide de l'assistant d'importation. Pour plus d'informations, consultez Utilisation des importations de données. ◦ Configure le calculateur de score de menace à l'aide des critères requis pour le calcul automatique du score de menace des observables. Pour plus d'informations, consultez Définir le calculateur de score de menace. ◦ Configure les taxonomies et les valeurs de taxonomie requises. Pour plus d'informations, consultez Création de taxonomies. ◦ Configurez le référentiel MITRE ATT&CK correspondant à votre organisation. Pour plus d'informations, consultez MITRE-ATT&CK Dépôt. **Remarque :** En tant que sn_sec_tisc.admin, vous pouvez également affecter le rôle sn_sec_tisc.analyst.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Droits applicables aux rôles TISC (suite)

Configuration	Description
	• Le rôle sn_sec_tisc.analyst effectue les tâches suivantes : ○ Affiche la vue d'ensemble des données dans le système à l'aide de la page d'accueil de l'application. Pour plus d'informations, consultez Afficher la TISC page d'accueil. ○ Importez des données dans le système à l'aide du bouton Importer des renseignements sur la page de la bibliothèque de menaces. Pour plus d'informations, consultez Centre de sécurité des renseignements sur les menaces Bibliothèque. ○ ▪ Recherche dans les données présentes dans l'application à l'aide de la recherche fournie dans la page Bibliothèque de menaces. ▪ Gère les données ingérées à partir de diverses sources dans la bibliothèque de menaces. ▪ Effectue diverses actions d'enrichissement sur les observables. ▪ Crée et gère les tickets. Pour plus d'informations, consultez Création de tickets à l'aide de la Console d'analyste de menaces.

Modules d'extension de dépendance

Module d'extension	Description
Les applications suivantes sont requises pour l'installation de cette application : • Composants communs de l'espace de travail de la gestion des tickets de sécurité [com.snc.escm.ws_commons] • Structure commune de Support pour Threat Intelligence [com.snc.threat] • Chiffrement au niveau des colonnes (com.glide.encryption) • API du générateur de charge utile JSON et XML volumineuse (com.glide.streaming_builder)	Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration sont installées et activées avant de configurer cette intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Module d'extension	Description
• Support de sécurité Core (com.snc.security_support.core) • Carte de nœud Composant d'expérience (sn_node_map) • Composant d'interface utilisateur de génération de rapports pour l'espace de travail (sn_sec_reporting) • Composant de l'éditeur de texte enrichi pour Security Operations (sn_escm_rte) • Cadre de travail d'intégration de sn_sec_int de sécurité • Base(sn_sec_cmn) commune(s) de support de sécurité • Orchestration de support de sécurité (sn_sec_cmn_orch)	

Intégrant Centre de sécurité des renseignements sur les menaces

Utilisez cette section pour comprendre les Centre de sécurité des renseignements sur les menaces intégrations.

La section **Intégrations comprend les** sous-modules suivants.

Intégrations

Nom du module	Description
Catalogue	Tous les flux Threat Intelligence et les intégrations d'enrichissement disponibles sont affichés sous forme de tuiles/cartes ici. Les utilisateurs ne pourront pas créer un nouveau flux ou une nouvelle intégration à partir de cette section.
Flux de menaces	Cette section contient uniquement les détails relatifs aux flux Threat Intelligence et les utilisateurs auront la possibilité de configurer de nouveaux flux Threat Intelligence à partir de cette section.
Intégrations des enrichissements	Cette section contient uniquement les détails relatifs aux intégrations d'enrichissement et les utilisateurs auront la possibilité de configurer les intégrations d'enrichissement disponibles à partir de cette section. **Remarque :** La section Intégrations d'enrichissement n'est visible que si au moins un module d'extension d'intégration d'enrichissement est installé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

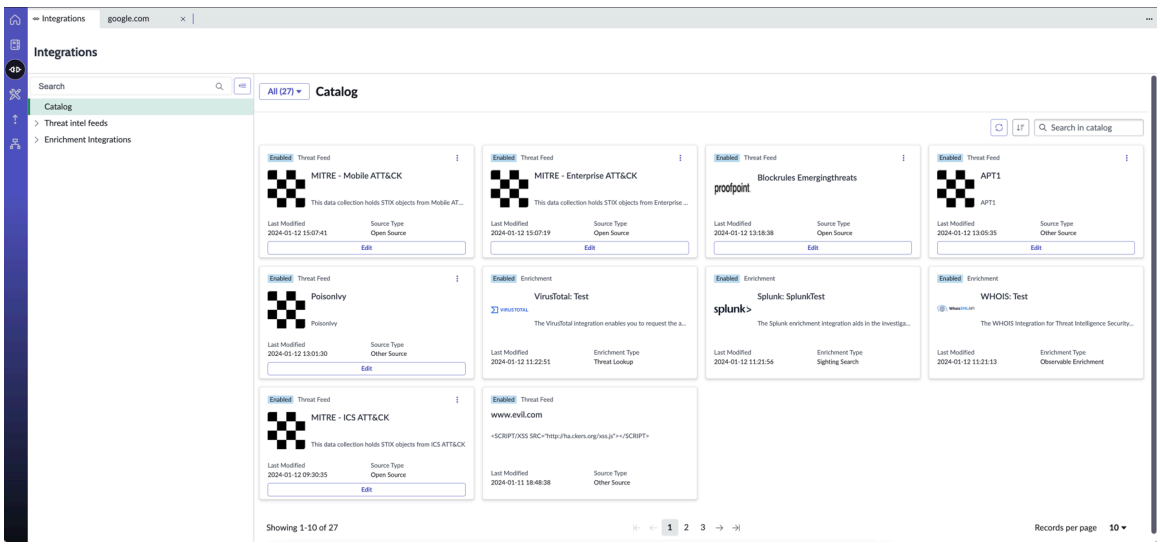
Centre de sécurité des renseignements sur les menaces Catalogue

Le Centre de sécurité des renseignements sur les menaces catalogue est une liste organisée des flux Threat Intelligence et des intégrations d'enrichissement disponibles dans l'application pour que vous puissiez les activer après avoir ajouté les informations requises et planifier le flux pour qu'il ingère automatiquement des données Threat Intelligence à une fréquence définie.

En tant que sn_sec_tisc.admin, vous pouvez également rechercher et modifier les configurations sources existantes, activer ou désactiver et supprimer les configurations du catalogue. Toute nouvelle source de données ajoutée au catalogue apparaît comme une nouvelle carte de configuration sur le catalogue.

Rôle requis :

- sn_sec_tisc.admin (créer/mettre à jour)
- sn_sec_tisc.analyst (lecture)



Remarque : Les cartes du catalogue se différencient par son étiquette qui se trouve en haut de la carte Flux de menaces/Enrichissement.

Actions sur la vue du catalogue

La vue Catalogue vous permet d'effectuer les actions suivantes.

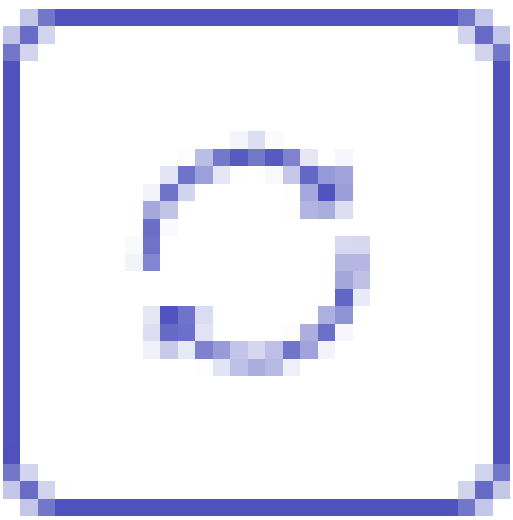
Actions sur la vue du catalogue

Action	Description
Tous	Utilisez ce menu déroulant pour filtrer les flux et les intégrations en fonction de leur état actuel. Vous pouvez filtrer en fonction des états suivants : • **Tout** : affiche tous les flux et intégrations sur la page. Il s'agit de l'option par défaut. • **Activé** : affiche tous les flux et intégrations à l'état Activé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions sur la vue du catalogue (suite)

Action	Description
	• **Désactivé** : affiche tous les flux et intégrations à l'état désactivé. • **Brouillon** : affiche tous les flux et intégrations qui sont à l'état brouillon.
	Utilisez cette action pour actualiser le catalogue.
	Utilisez cette action pour trier tous les flux et intégrations en fonction des éléments suivants : • **Dernière modification (récente)** • **Dernière modification (la plus ancienne)** • **Nom (A-Z)** • **Nom (de Z à A)**
Rechercher dans le catalogue	Utilisez cette action pour rechercher des flux/ intégrations en fonction du nom et de la description dans le catalogue.

Flux Threat Intelligence

Utilisez les flux Threat Intelligence pour ajouter, modifier ou supprimer une source de données de flux Threat Intelligence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

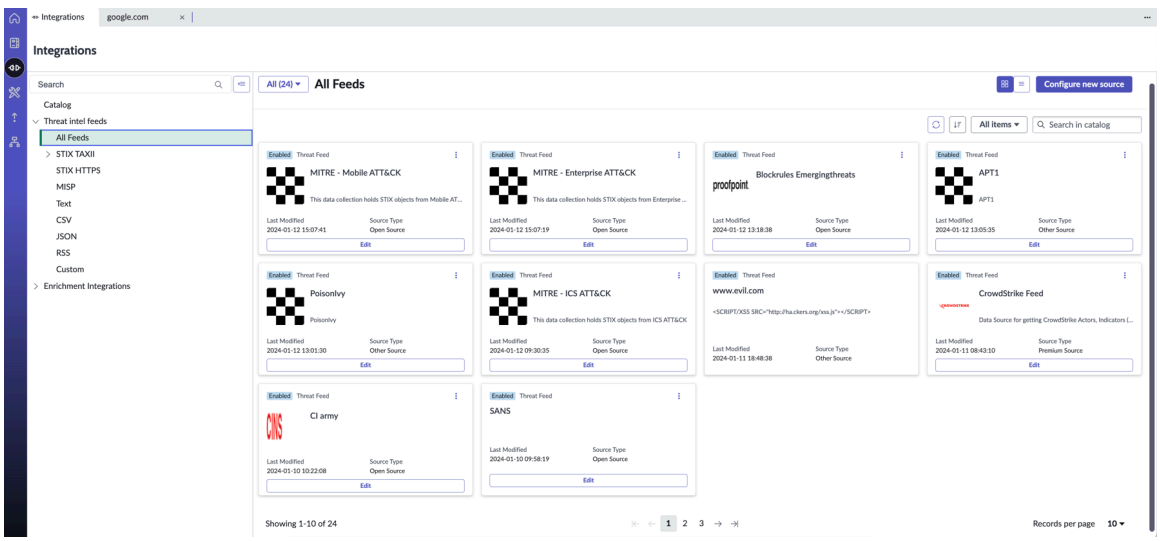
Les flux de sources de données sont disponibles dans le catalogue Threat Intelligence sous la section Intégrations.

Le catalogue des flux Threat Intelligence est conçu pour afficher les sources de données de flux disponibles sous forme de tuiles et peut filtrer, rechercher et accéder aux détails de la configuration source, ainsi qu'effectuer diverses actions.

Tous les flux

Le système de base comprend une série de cartes pour chacun des flux que vous pouvez activer et utiliser.

Vous pouvez consulter les flux en accédant à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Intégrations** > **Flux de Threat Intelligence** > **Tous les flux**.



Actions sur la vue Tous les flux

La section Tous les flux vous permet d'effectuer les actions suivantes.

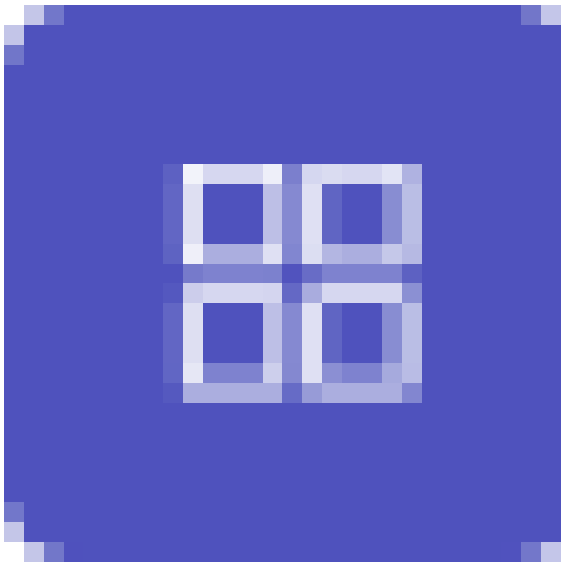
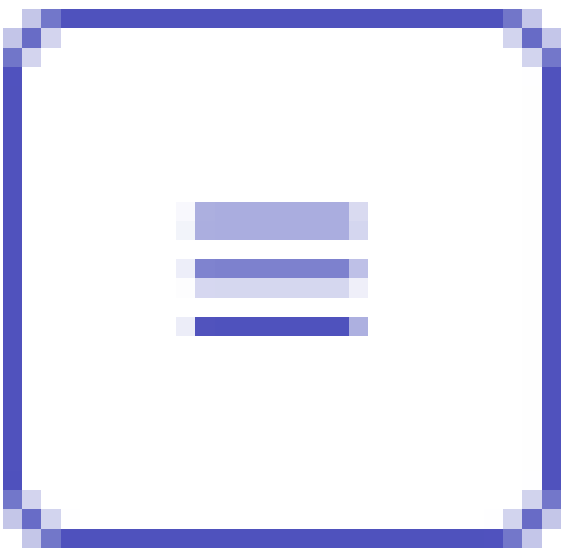
Actions sur la vue Toutes les intégrations

Action	Description
Tous	Ce menu déroulant vous permet de filtrer les flux en fonction de leur état actuel. Vous pouvez filtrer en fonction des états suivants : • **Tout** : affiche tous les flux de la page. Il s'agit de l'option par défaut. • **Activé** : affiche tous les flux qui sont à l'état Activé. • **Désactivé** : affiche tous les flux qui sont à l'état désactivé. • **Brouillon** : affiche tous les flux qui sont à l'état brouillon.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

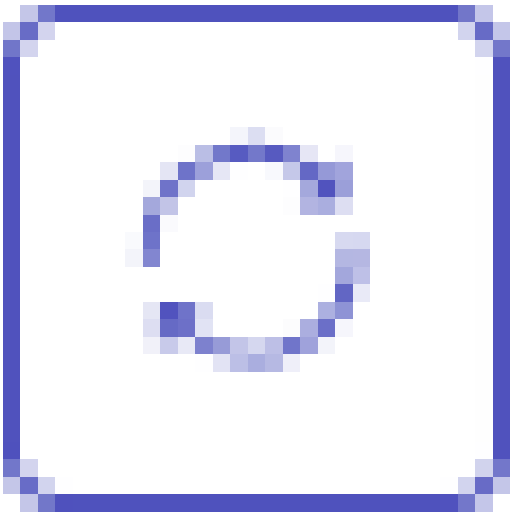
Actions sur la vue Toutes les intégrations (suite)

Action	Description
	Utilisez cette action pour afficher tous les flux sous forme de cartes.
	Utilisez cette action pour afficher tous les flux sous la forme d’une vue de liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions sur la vue Toutes les intégrations (suite)

Action	Description
	Utilisez cette action pour actualiser la page.
	Utilisez cette action pour trier toutes les intégrations en fonction des éléments suivants : • **Dernière modification (récente)** • **Dernière modification (la plus ancienne)** • **Nom (A-Z)** • **Nom (de Z à A)**
Tous les éléments	Utilisez cette action pour filtrer et répertorier les vignettes de flux Threat Intelligence par type de source ou par type de flux. **Type de source** : • Open source • Autre source • Source premium **Type de flux** : • CSV • Flux personnalisé • JSON

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions sur la vue Toutes les intégrations (suite)

Action	Description
	• MISP • RSS • STIX HTTPs • Texte
Rechercher dans le catalogue	Cette action permet de rechercher des flux en fonction du nom et de la description dans le catalogue.

Types de flux de Renseignements sur les menaces

Voici les types de flux Threat Intelligence qui peuvent être configurés et activés :

Flux Threat Intelligence

Type	Description
Flux TAXII	Flux disponibles au format de collections STIX/TAXII.
STIX HTTPS	Flux Threat Intelligence au format STIX accessibles via des API REST sur le protocole HTTPS.
MISP	Flux au format MISP Flux.
Texte	Flux disponibles en tant que fichiers hébergés au format texte. **Remarque :** Le système analyse les fichiers pour l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP est uniquement extrait et aucun autre type d'observable n'est extrait.
CSV	Flux disponibles en tant que fichiers hébergés au format CSV. **Remarque :** Le système analyse les fichiers pour l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP est uniquement extrait et aucun autre type d'observable n'est extrait.
JSON	Flux disponibles en tant que fichiers hébergés au format JSON. **Remarque :** Le système analyse les fichiers pour l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP est uniquement extrait et aucun autre type d'observable n'est extrait.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux Threat Intelligence (suite)

Type	Description
RSS	Flux disponibles en format RSS. L'application stockera les données sous forme d'enregistrements de flux RSS.
Personnalisé	Flux configurés à l'aide d'analyseurs personnalisés. **Remarque :** Le système analyse les fichiers pour l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP est uniquement extrait et aucun autre type d'observable n'est extrait.

Pour connaître les étapes suivantes de la procédure, reportez-vous à la section correspondante relative à la configuration de chaque type de flux spécifique sous Flux Threat Intelligence.

Configurer un nouveau flux Threat Intelligence

Configurez un nouveau flux Threat Intelligence.

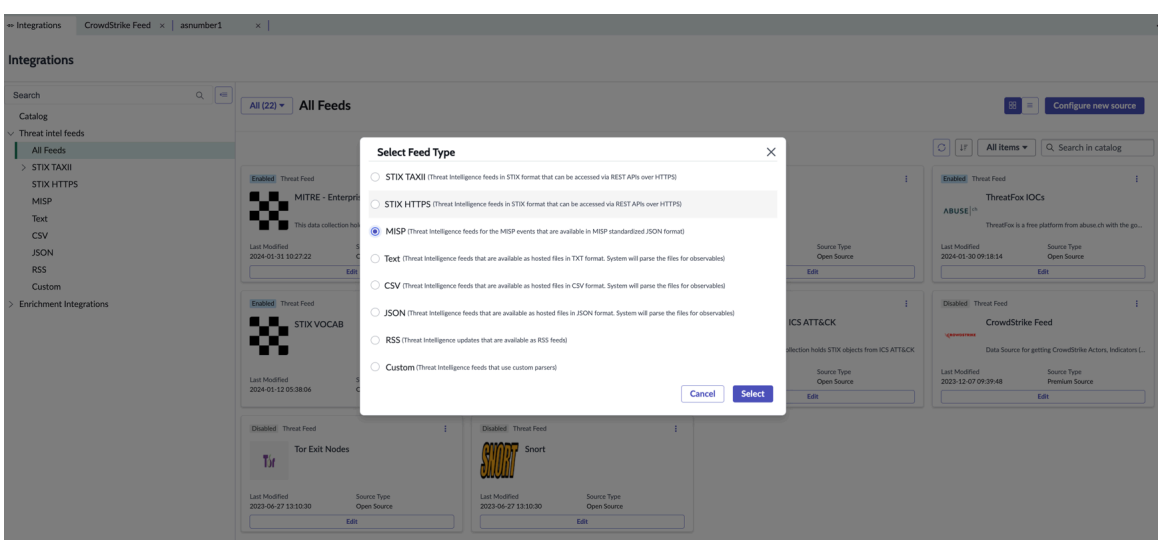
Avant de commencer

Rôle requis : sn_sec_tisc.admin

Pour configurer un nouveau flux de renseignements sur les menaces, procédez comme suit :

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionner **Flux de Threat Intelligence** > **Tous les flux**.
4. Cliquez sur **Configurer une nouvelle source**.
   Les différents types de flux s'affichent.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez le type de flux respectif.
6. Remplissez les champs du formulaire.

Configurer une nouvelle source

Champ	Description
Nom	Saisissez un nom pour le flux.
Description	Description du flux.
Type de flux	Type de flux. Par exemple, MISP. Par défaut, cette valeur est affichée en fonction du type de flux que vous avez sélectionné dans le catalogue.
Logo	Joindre le logo du flux source. **Remarque :** La taille doit être de 72px/72px.
Secteur	Sélectionnez la catégorie d'industrie (aérospatiale, agriculture, etc.) à laquelle l'aliment s'applique.
Type de source	Sélectionnez le type de source dans la liste des types de sources disponibles. La liste des sources disponibles est la suivante : ○ Gouvernement ○ ISACs ○ Open source ○ Source premium ○ Autre source

7. Cliquez sur **Sélectionner**.
8. Renseignez les champs de la section Configuration comme il convient.

Configuration

Champ	Description
Période d'expiration (jours)	Saisissez la période d'expiration du flux en jours. Par exemple, 180 jours. **Remarque :** Quelles que soient les données ingérées à la source, elles expireront 180 jours après l'ingestion.
Utiliser le message REST	Cochez la case **Utiliser le message REST** si vous devez utiliser la fonctionnalité de message REST/de méthode REST fournie par ServiceNow AI Platform. Si cette case n'est pas cochée, l'application utilise le point de terminaison

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	fourni dans **l'URL du point de terminaison REST** pour extraire les données du flux. Pour plus d'informations, consultez Service Web REST sortant dans la ServiceNow AI Platform documentation. **Remarque :** Les champs Message REST et Méthode REST sont obligatoires lorsque vous sélectionnez le message REST.
Message REST	Sélectionnez l'enregistrement du message REST dans la liste des enregistrements du message REST déjà configurés dans l'instance. Pour plus d'informations, consultez Service Web REST sortant dans la ServiceNow AI Platform documentation. **Remarque :** Sélectionnez cette valeur lorsque vous devez afficher des en-têtes spécifiques et définissez les enregistrements connexes REST à l'aide de l'option de message REST.
Méthode REST	Sélectionnez Méthode REST dans la liste des méthodes REST disponibles configurées pour le message REST sélectionné. Pour plus d'informations, consultez Service Web REST sortant dans la ServiceNow AI Platform documentation.
Fiabilité	Définissez la confiance pour tous les enregistrements applicables qui sont ingérés via ce flux spécifique. **Remarque :** Définissez la confiance entre 0 et 100 pour cette source.
Mécanisme d'analyse des données	Sélectionnez l'option de mécanisme d'analyse de données appropriée. Les options disponibles sont les suivantes : ○ **Extraction IoC automatisée** : cette option est sélectionnée par défaut lors de la configuration des flux texte, CSV ou JSON. ○ **Mappage de champs personnalisés** : sélectionnez cette option si vous souhaitez définir la façon dont les champs spécifiques de vos données de flux doivent être mappés aux attributs observables. Une fois cette option sélectionnée, vous pouvez configurer les mappages dans la section **Mappage de champ** . Pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	plus d'informations sur le mappage des champs personnalisés, reportez-vous à la section Configurer le mappage de champs personnalisés. **Remarque :** L'option de mécanisme d'analyse de données n'est disponible que pour les flux de texte, CSV et JSON, où le **processeur de rapports** de flux est défini sur SimpleFeedDatasourceResponseProcessor.
URL du point de terminaison REST	Entrez l'URL du point de terminaison REST où les données sont hébergées par le flux de renseignements sur les menaces. **Remarque :** Pour les types de flux MISP, les URL de point de terminaison REST qui se terminent par /manifest.json sont prises en charge.
Authentification requise	Cochez cette case si l'authentification est requise pour votre nouveau flux de renseignements sur les menaces. **Remarque :** Cela s'applique uniquement lorsque l'URL du point de terminaison REST est utilisée pour récupérer les données.
Type d'authentification	Type d'authentification pour le flux source. Voici les types d'authentification configurés et mis en service dans le système de base pour les utilisateurs : ○ ID API/Clé API ○ ID API/secret API ○ Clé API ○ Clé API/Secret API ○ Nom d'utilisateur API/Mot de passe API/Clé API ○ Authentification de base
En-têtes à transmettre avec la demande	Tous les en-têtes à transmettre avec les demandes peuvent être fournis dans le mappage d'en-tête de demande. ○ L'en-tête doit être fourni dans une paire clé-valeur séparée par deux-points (« : »). ○ Chaque paire clé-valeur d'en-tête doit être fournie dans une nouvelle ligne. ○ Pour fournir des paramètres d'authentification en tant que valeurs d'en-tête, encadrez l'étiquette

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'authentification requise avec « ${ » et « }$ ». Par exemple, x-api-key :${API Key}$.
Avancés	Cochez cette case pour définir un script d'intégration personnalisé et un script de processeur de rapport. **Remarque :** Lorsque vous cochez cette case, les champs **Script d'intégration** et **Processeur de rapport** s'affichent pour vous permettre de sélectionner les scripts personnalisés.
Script d'intégration	Le script d'intégration appelle un appel à l'URL du point de terminaison REST à l'aide des paramètres d'authentification et des en-têtes configurés dans le flux, puis le script récupère les données disponibles à partir du flux spécifique. Dans le système de base, les includes de scripts personnalisés suivants sont disponibles, qui sont mis en service dans l'application pour les scripts d'intégration : ○ MITRESourceIntegration : utilisé pour extraire les données à partir des flux MITRE. ○ RSSFeedDatasourceIntegration : utilisé pour extraire les données à partir des flux RSS. ○ SimpleFeedDatasourceIntegration : utilisé pour extraire les données de flux simples sans authentification ni authentification de base. ○ SimpleMISPFeedDatasourceIntegration : utilisé pour extraire les données à partir des flux MISP hébergés. Le script d'intégration par défaut est basé sur le type de flux que vous sélectionnez. Par exemple, si vous sélectionnez le type de flux MISP, qui est un format standard pour traiter et extraire les données, le script d'intégrations est **SimpleMISPFeedDatasourceIntegration**. **Remarque :** Pour les scripts d'intégration personnalisés, vous pouvez créer un include de script en étendant **FeedDatasourceIntegrationBase** et en remplaçant les méthodes requises.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Script de processeur de rapport	Le script de processeur de rapports traite les données extraites du flux à l'aide du script d'intégration. Le système de base inclut les scripts personnalisés suivants, qui sont mis en service dans l'application pour prendre en charge le script de processeur de rapports : ○ AtomFeedDatasourceResponseProcessor : utilisé pour traiter les flux RSS au format Atom. ○ MITRECollectionDataProcessor : utilisé pour le traitement des flux MITRE. ○ RSSFeedDatasourceResponseProcessor : utilisé pour le traitement des flux RSS. ○ SimpleDataplaneFeedResponseProcessor : utilisé pour le traitement des flux de plans de données. ○ SimpleFeedDatasourceResponseProcessor : utilisé pour le traitement de flux simples utilisant l'extraction d'observables par expression régulière. ○ SimpleFeodotrackerFeedResponseProcessor : Utilisé pour traiter les flux Feodotracker. ○ SimpleMISPFeedDatasourceResponseProcessor : utilisé pour le traitement des flux MISP hébergés. ○ TAXIIV2CollectionDataProcessor : utilisé pour le traitement des données de collecte TAXII. Le processeur de rapport par défaut pour les flux MISP est `SimpleMISPFeedDatasourceResponseProcessor`. Ce processeur est préconfiguré par l'application et ne peut être ni modifié ni remplacé.

9. Renseignez les champs de la section Planification, comme il convient.

Ordonnancement

Champ	Description
Exécuter	Définissez la fréquence à laquelle vous souhaitez ingérer les enregistrements. Le flux s'exécutera et s'exécutera en fonction de l'intervalle de tâche de planification. Les intervalles de tâches disponibles sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Quotidien ○ Hebdomadaire ○ Mensuel ○ Périodiquement ○ Une fois ○ Sur demande ○ Calendrier d'entreprise : début de l'entrée ○ Calendrier d'entreprise : fin de l'entrée **Remarque :** Par défaut, la fréquence est définie sur Sur demande. Pour plus d'informations, consultez Travaux planifiés et comment exécuter automatiquement un script de votre choix .
Extraire les données de	Date de début à partir de laquelle les données doivent être extraites. Ce champ doit être défini avec le délai à partir duquel les données doivent être ingérées à partir de la source correspondante. Une fois ce champ défini, l'exécution d'ingestion suivante extrait les données à partir de l'heure configurée et les exécutions d'ingestion consécutives extraient des données incrémentielles. Par exemple, la source est planifiée pour ingérer les données toutes les heures. L'utilisateur définit **Extraire les données du** 12 janvier à 6h00 le 12 janvier à 9h30. L'ingestion se déclenchant le 12 janvier à 10h00 permet d'extraire les données du 12 janvier à 6h00 au 12 janvier à 10h00. L'ingestion suivante qui se déclenche à 11h00 extrait uniquement les données incrémentielles du 12 janvier à 10h00 au 12 janvier à 11h00. **Remarque :** Cela signifie que les exécutions planifiées extrairont les données de façon incrémentielle à partir de la date spécifiée. **Important :** Cela ne s'applique pas non plus aux flux texte, CSV et JSON.

Balises

Champ	Description
Sélectionner des balises	Utilisez les balises pour annoter ou marquer à l'oreille les enregistrements qui sont ingérés dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	le système à partir de cette source. Commencez à saisir le nom de la balise dans la barre **de recherche** pour choisir les balises disponibles dans l'application ou saisissez un nouveau nom de balise et cliquez sur **Ajouter** pour l'affecter à la source.

10. Cliquez sur l'action **Enregistrer** pour stocker et créer le flux.
    Les détails fournis sont validés et, par défaut, l'état des flux est désactivé.
11. **Facultatif :** Cliquez sur l'action **Enregistrer comme brouillon** pour stocker uniquement les configurations de flux comme brouillon.
    Les utilisateurs ne peuvent pas activer un flux lorsqu'il est enregistré en mode brouillon. Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez renseigner les informations restantes dans la version brouillon et la créer.
12. Cliquez sur **Activer** pour activer l'enregistrement.

    Une fois l'enregistrement du flux Threat Intelligence activé, vous pouvez l'exécuter pour exécuter l'intégration.

    Remarque :
    - L'enregistrement du flux Threat Intelligence est étiqueté et indiqué comme **activé**. De même, vous pouvez désactiver le flux de renseignements sur les menaces en cliquant sur le bouton **Désactiver** .
    - Vous pouvez également activer, désactiver ou supprimer un flux particulier à l'aide du menu **Actions** de la vignette du flux requis sur la page **Catalogue** ou **Flux de Renseignements sur les menaces** .
13. Cliquez sur **Supprimer** pour supprimer l'enregistrement du flux des renseignements sur les menaces.
14. Sélectionnez **la section Exécution des intégrations** pour vérifier les détails de l'exécution.

Remarque : La procédure de configuration du flux Threat Intelligence ci-dessus est la même pour tous les autres types de flux Threat Intelligence, à l'exception de STIX TAXII. Pour plus d'informations sur la configuration de STIX TAXII, reportez-vous à la section Configurer un nouveau flux TAXII.

Configurer le mappage de champs personnalisés

Le mappage de champs vous permet de configurer la façon dont chaque champ d'un flux de données tel que Texte, CSV ou JSON est interprété et affecté à l'observable correspondant.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

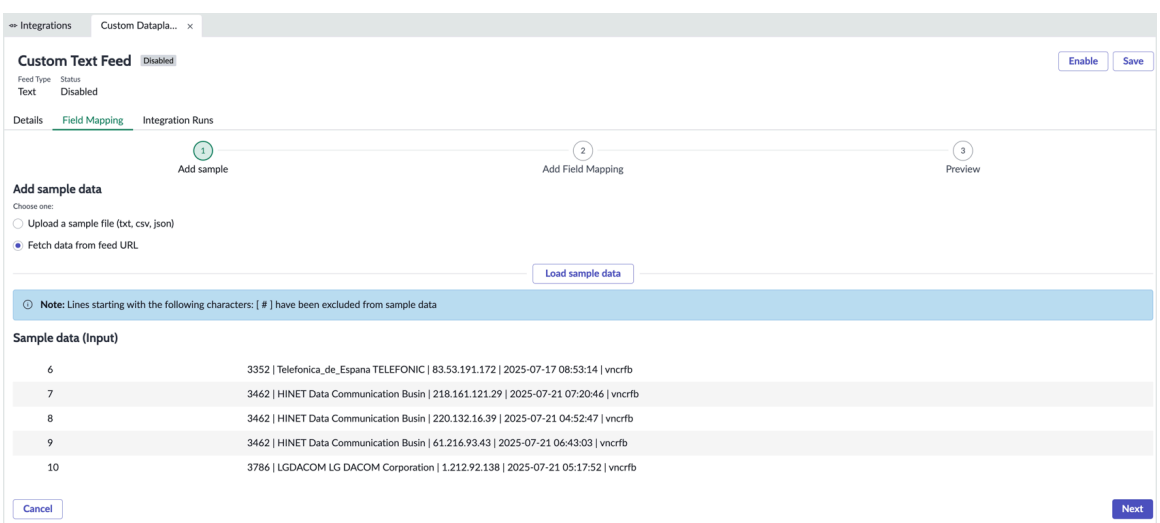
Procédure
1. Accédez à la **Tous** > **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Intégrations**.
2. Sélectionner **Flux de Threat Intelligence** > **Tous les flux** > **Texte**.
3. Sélectionnez **Configurer une nouvelle source**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Remplissez les détails du formulaire de flux de texte selon vos besoins.
   Pour plus d'informations, reportez-vous à la section Configurer un nouveau flux Threat Intelligence.
5. Dans la nouvelle vue de formulaire, accédez au champ **Mécanisme d'analyse des données** dans la section **Configuration** .
   Pour plus d'informations sur le mécanisme d'analyse de données, reportez-vous à la section Configurer un nouveau flux Threat Intelligence.
6. Sélectionnez **l'option Mappage de champ personnalisé** .
7. Accédez à la section **Mappage de champ** .
8. Sélectionnez **Configurer** pour ajouter le mappage de champs pour la nouvelle source de données.
   Cette section comprend trois étapes, telles que l'ajout d'exemples de données, le mappage de champs et l'aperçu des exemples d'enregistrements mappés.
9. Pour ajouter les exemples de données, sélectionnez **Charger les exemples de données**.
   Cela affiche les données d'exemple de l'option sélectionnée. L'application affiche uniquement les lignes de données pertinentes et les lignes qui commencent par # sont exclues des données d'échantillon. Les identificateurs de commentaire peuvent être modifiés avec la propriété système : `sn_sec_tisc.feed_comment_identifiers`.

   L'application extrait un échantillon des données entrantes soit à partir d'un exemple de fichier (tel que .txt, .csv ou .json), soit directement à partir de l'URL de flux configurée (l'URL du flux et les informations d'identification saisies dans la section **Détails**). Cela vous permet de prévisualiser la structure et le contenu des données avant de définir des mappages de champs.
10. Sélectionnez **Charger un exemple de fichier** ou **Flux de données à partir de l'URL du flux**.
    Ces données d'échantillon extrait les dix premiers enregistrements par défaut. Ce nombre total d'enregistrements à récupérer peut être modifié avec la propriété système `sn_sec_tisc.feed_field_mapping_sample_count`.



11. Sélectionnez **Suivant** pour configurer le mappage de champ.
12. Sélectionnez **l'option Définir un délimiteur pour l'analyse des données** dans la liste déroulante.
    Lorsque vous utilisez des flux de texte, le délimiteur est essentiel pour analyser correctement les données en champs individuels.

    Dans ce scénario, le flux de texte utilise l'opérateur de tuyau (|) comme délimiteur qui sépare chaque valeur des données textuelles d'exemple en colonnes distinctes.

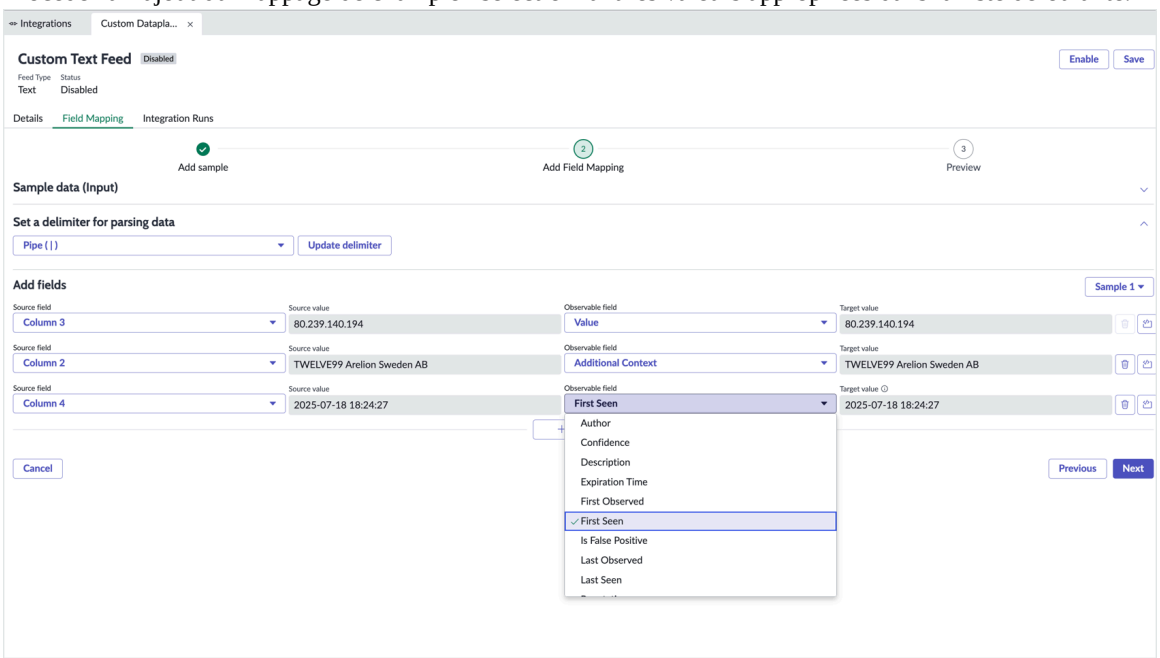
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'identification et l'application correctes de ce délimiteur sont essentielles pour garantir un mappage précis des champs et une ingestion réussie des données.

Remarque : Pour les flux CSV, la virgule (,) est le délimiteur par défaut, et les flux JSON ne nécessitent aucun délimiteur.

13. Sélectionnez **Mettre à jour le délimiteur**.
    Les options permettant d'ajouter des champs pour le mappage de champs s'affichent.
14. Procédez à l'ajout du mappage de champ en sélectionnant les valeurs appropriées dans la liste déroulante.



15. Utilisez le **script de transformation** pour transformer et normaliser les valeurs d'entrée avant de les mapper aux observables.

    a. Sélectionnez **l'icône Activer/désactiver le script de transformation** pour configurer le script.
    La boîte de dialogue Configurer le script pour le champ source s'affiche.

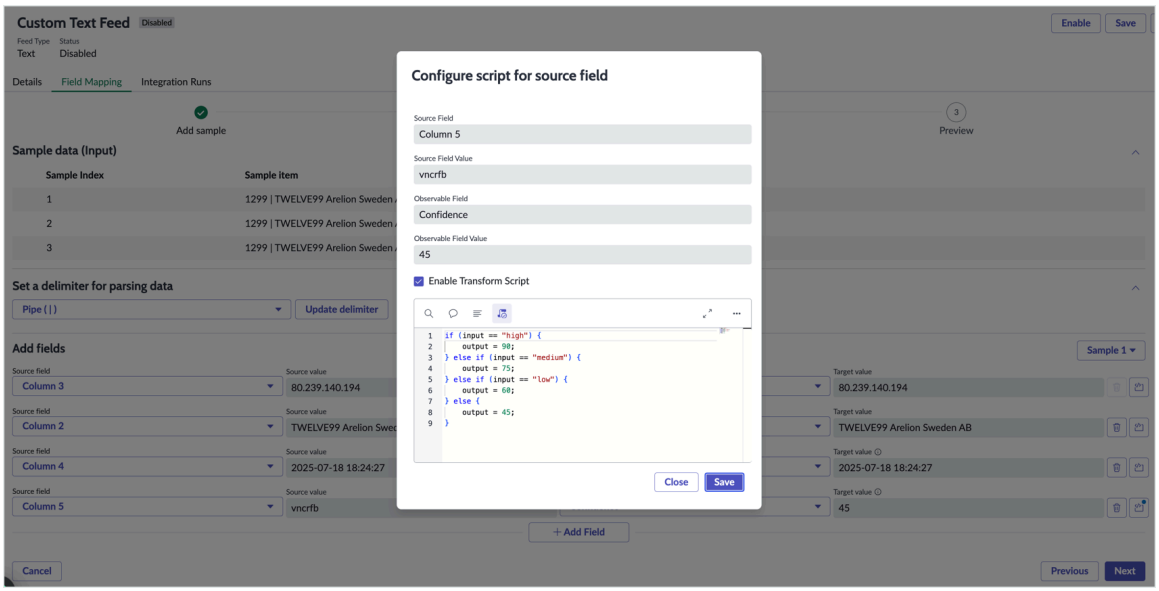
    b. Cochez la case **Activer le script de transformation** dans la boîte de dialogue Configurer le **script pour le champ source** .

    c. Ajoutez ou modifiez le script.

    Par exemple, si votre champ d'entrée contient des valeurs telles que faible, moyenne ou élevée et que vous souhaitez mapper ces valeurs à des niveaux de fiabilité numériques (compris entre 0 et 100), vous pouvez utiliser Transformer le script pour convertir la valeur entrée et la mapper au champ de **confiance** de l'observable.

Traduction automatique

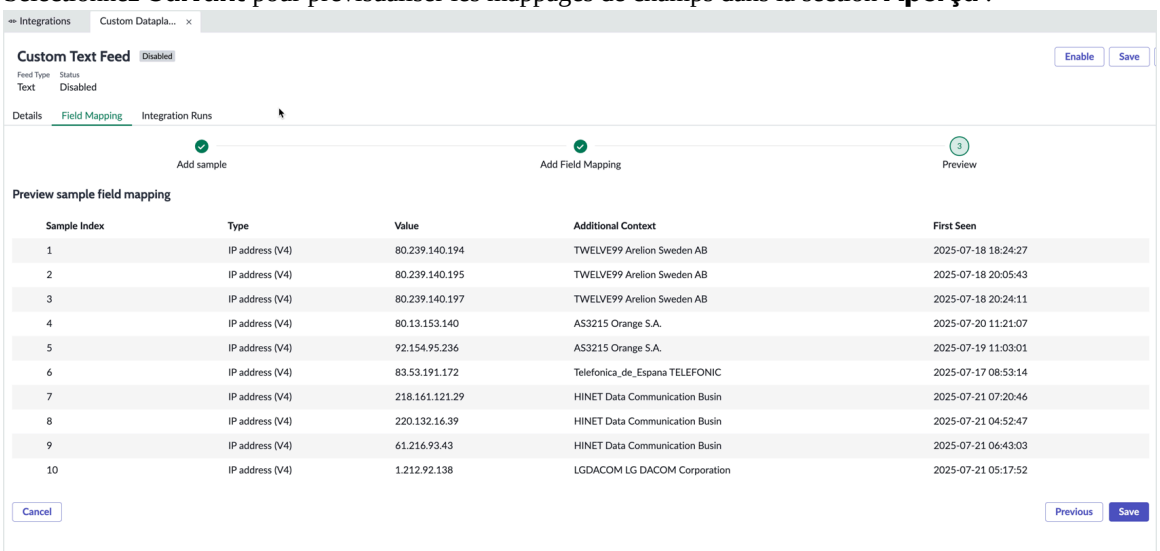
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



d. Sélectionnez **Enregistrer** pour enregistrer le script et obtenir la valeur cible mise à jour.

e. Fermez la boîte de dialogue **Configurer le script pour le champ source** et passez à l'étape suivante.

16. Sélectionnez **Suivant** pour prévisualiser les mappages de champs dans la section **Aperçu** .



17. Prévisualisez l'exemple de mappage de champs et sélectionnez **Enregistrer**.
Un message de confirmation s'affiche et indique que le mappage de champs est enregistré avec succès.

Dans le cadre du mappage d'échantillons de champs, l'application identifie automatiquement le type d'observable (tel que l'adresse IP v4, entre autres) que l'utilisateur a mappé à partir des exemples de données. Ce mécanisme rationalise le processus de mappage et garantit que les types d'observables appropriés sont affectés en fonction de l'entrée.

Important : Exécution de l'intégration du mappage de champs : toute exécution de l'intégration effectuée pour ce type de flux utilisera la configuration de mappage de champs enregistrée. Cela garantit que les données entrantes sont systématiquement analysées et mappées aux attributs observables corrects en fonction de la structure définie lors de la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Sélectionnez **Modifier le mappage de champs** pour modifier et apporter les changements nécessaires au mappage de champs, si nécessaire. Un message d'alerte s'affiche pour confirmer si vous souhaitez poursuivre la modification. Confirmez l'invite et sélectionnez **Oui** pour continuer. Apportez les changements nécessaires aux mappages de champs à l'aide des exemples de données mis à jour et enregistrez les changements.

Toutes les modifications apportées au mappage de champs seront appliquées aux futures exécutions d'intégration pour ce flux.

Vérifiez toujours les exemples de données après les changements pour garantir une analyse correcte avant d'exécuter l'intégration.

Afficher les flux de Threat Intelligence

Cette section vous fournit les flux de Renseignements sur les menaces configurés dans le système de base.

Voir les flux STIX TAXII

Affichez les flux STIX TAXII configurés dans le système de base.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **STIX TAXII**.
   Les flux MISP dans le système de base sont décrits dans le tableau suivant.

Flux de menaces	Description	URL
Cyware TAXII	Cyware Threat Intelligence eXchange (CTIX) est une plateforme conçue pour faciliter le partage de renseignements sur les cybermenaces entre les organisations.	https://threatfeed.cyware.com/ctixapi/ctix21/
Futur enregistré TAXII	Recorded Future est une plateforme cloud indépendante de renseignements sur les menaces qui permet aux organisations d'identifier et d'atténuer les menaces dans les domaines de la cybersécurité, de la chaîne d'approvisionnement, du physique et de la fraude.	https://api.recordedfuture.com/taxii2
TAXII pulsé	Pulsedive est une plateforme de renseignements sur les menaces qui fournit une large gamme de services et d'outils	https://pulsedive.com/taxii2/api/

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
	de renseignements sur les cybermenaces aux organisations.	

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher les flux HTTP STIX

Affichez les flux STIX HTTP configurés dans le système de base.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **STIX HTTP**.
   Le tableau suivant décrit les flux STIX HTTPs dans le système de base.

Flux des menaces	Description	URL
MITRE - Mobile ATT&CK	Cette collection de données contient des objets STIX de Mobile ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE - ICS ATT&CK	Cette collection de données contient des objets STIX d'ICS ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
MITRE : ATT&CK d'entreprise	Cette collection de données contient des objets STIX d'Enterprise ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

4. Cliquez sur **Modifier** pour modifier le flux et effectuer les mises à jour nécessaires.

Afficher les flux MISP

Affichez les flux MISP configurés dans le système de base.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **MISP**.
   Les flux MISP dans le système de base sont décrits dans le tableau suivant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
Flux OSINT de Renseignements sur les menaces côté numérique	Source de données permettant d'extraire des informations Open Source Cyber Threat Intelligence à partir du flux OSINT de DigitalSide Threat-Intel, qui est principalement basé sur l'analyse des programmes malveillants et les URL, adresses IP et domaines compromis.	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json
IOC URLhaus	URLhaus est un projet de abuse.ch dont l'objectif est de partager des URL malveillantes utilisées pour la distribution de logiciels malveillants.	https://urlhaus.abuse.ch/downloads/misp/manifest.json
Bazar de programmes malveillants	MalwareBazaar est un projet de abuse.ch dont l'objectif est de partager des échantillons de logiciels malveillants avec la communauté de la sécurité de l'information, les fournisseurs d'antivirus et les fournisseurs de renseignements sur les menaces.	https://bazaar.abuse.ch/downloads/misp/manifest.json
IOC ThreatFox	ThreatFox est une plateforme gratuite de abuse.ch dont l'objectif est de partager les indicateurs de compromission (IOC) associés aux logiciels malveillants avec la communauté de la sécurité de l'information, les fournisseurs d'antivirus et les fournisseurs de renseignements sur les menaces.	https://threatfox.abuse.ch/downloads/misp/manifest.json

Remarque : Pour les types de flux MISP, les URL de point de terminaison REST qui se terminent par `/manifest.json` sont prises en charge.

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher les flux de texte

Affichez les flux de texte configurés dans le système de base.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez l'option **Texte** .
   La section suivante répertorie les flux de texte configurés dans le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
Adresses IP de Haley's Brute Force	Fournit une liste des adresses IP de l'ordinateur attaquant au cours des 2 dernières années, triées par adresse IP	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt
Bloquer les règles Menaces émergentes	Emerging Threat Intelligence (ET) fournit des flux d'informations exploitables sur les menaces pour identifier les adresses IP impliquées dans des activités suspectes et malveillantes.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Toile à groper Nuug Pop3	Liste des hôtes qui ont essayé et échoué à se connecter au service POP3 à bsdly.net.	https://home.nuug.no/%7Epeter/pop3gropers.txt
Nœuds de sortie Tor	Les nœuds de sortie Tor peuvent être utilisés pour détecter le trafic provenant du réseau TOR.	https://www.dan.me.uk/torlist/?exit
Liste noire d'adresses IP Talos Intelligence	Talos a été formé en combinant l'équipe de recherche sur les vulnérabilités de SourceFire, le groupe Cisco Threat Research and Communications et le groupe Cisco Secure Applications. L'expertise combinée est soutenue par une infrastructure sophistiquée et la télémétrie inégalée de Cisco qui s'étend sur les réseaux, les terminaux, les environnements cloud, les systèmes virtuels et le trafic Web et de messagerie quotidien.	https://www.talosintelligence.com/documents/ip-blacklist
SANS	ISC fournit un service gratuit d'analyse et d'alerte à des milliers d'internautes et d'organisations.	https://isc.sans.edu/feeds/topips.txt
Snort	Snort est le premier système de prévention des intrusions (IPS) Open Source au monde. Snort IPS utilise une série de règles qui aident à définir l'activité réseau malveillante.	https://snort.org/downloads/ip-block-list
Armée de CI	La liste CINS Army est un sous-ensemble de l'ensemble de règles CINS Active Threat Intelligence et se compose d'adresses IP qui répondent à l'un des deux critères de base suivants : 1) le récent facteur de score Rogue Packet de l'adresse IP est très faible, ou 2) l'adresse IP a déclenché un nombre désigné d'alertes « de	https://cinsscore.com/list/ci-badguys.txt

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
	confiance » sur un nombre donné de ses Sentinel déployés dans le monde entier.	
Point de preuve	IP brutes pour les listes de blocs du pare-feu. Ceux-ci proviennent de : les réseaux de spam identifiés par Spamhaus (www.spamhaus.org), les principaux attaquants répertoriés par DShield (www.dshield.org) et Abuse.ch	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
Liste de blocage Greensnow	GreenSnow est une équipe composée des meilleurs spécialistes de la sécurité informatique, GreenSnow récolte un grand nombre d'IP provenant de différents ordinateurs situés dans le monde entier. GreenSnow est comparable à SpamHaus.org pour les attaques de toutes sortes, à l'exception du spam.	https://blocklist.greensnow.co/greensnow.txt
Armée de CI	La liste CINS Army est un sous-ensemble de l'ensemble de règles CINS Active Threat Intelligence et se compose d'adresses IP qui répondent à l'un des deux critères de base suivants : 1) le récent facteur de score Rogue Packet de l'adresse IP est très faible, ou 2) l'adresse IP a déclenché un nombre désigné d'alertes « de confiance » sur un nombre donné de ses Sentinel déployés dans le monde entier.	https://cinsscore.com/list/ci-badguys.txt
Liste de blocage	www.blocklist.de est un service gratuit et volontaire fourni par un spécialiste de la fraude/abus, dont les serveurs sont souvent attaqués via SSH, Mail-Login-, FTP-, Webserver- et autres.	https://lists.blocklist.de/lists/all.txt
Nœuds de sortie Tor	Les nœuds de sortie Tor peuvent être utilisés pour détecter le trafic provenant du réseau TOR.	https://www.dan.me.uk/torlist/?exit
IP des BOT Botscout	BotScout permet d'empêcher les scripts Web automatisés, connus sous le nom de « bots », de s'inscrire sur les forums, de polluer les bases de données, de diffuser du spam et d'abuser des formulaires sur les sites Web.	http://botscout.com/last_caught_cache.txt

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
Plan de données VNC RFB	Adresses IP identifiées comme initiant des sessions de mémoire tampon de trames distantes VNC.	https://dataplane.org/signals/vncrfb.txt
Connexion TELNET du plan de données	Adresses IP identifiées comme tentant de connexion via l'authentification par mot de passe TELNET.	https://dataplane.org/signals/telnetlogin.txt
Authentification par mot de passe SSH du plan de données	Adresses IP identifiées comme tentant de se connecter via l'authentification par mot de passe SSH.	https://dataplane.org/signals/sshpwauth.txt
Connexion client SSH du plan de données	Adresses IP identifiées comme effectuant des négociations de protocole client SSH.	https://dataplane.org/signals/sshclient.txt
Bloquer les règles Menaces émergentes	Emerging Threat Intelligence (ET) fournit des flux d'informations exploitables sur les menaces pour identifier les adresses IP impliquées dans des activités suspectes et malveillantes.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Message d'accueil SMTP du plan de données	Adresses IP identifiées comme étant des clients SMTP émettant des commandes HELO ou EHLO non sollicitées.	https://dataplane.org/signals/smtpgreet.txt
Requête SIP de plan de données	Adresses IP identifiées comme envoyant des requêtes SIP OPTIONS.	https://dataplane.org/signals/sipquery.txt
Protocole IP du plan de données 41	Adresses IP identifiées comme relais ouvert du protocole IPv4 41 (c.-à-d. IPv6 sur IPv4).	https://dataplane.org/signals/proto41.txt
Invitation SIP de plan de données	Adresses IP identifiées comme étant à l'origine des opérations d'invitation SIP.	https://dataplane.org/signals/sipinvitation.txt
Plan de données DNS CH TXT version.bind	Adresses IP identifiées comme étant à l'origine de la version DNS CH TXT. Lier les requêtes.	https://dataplane.org/signals/dnsversion.txt
TCP DNS du plan de données	Adresses IP identifiées comme envoyant des requêtes DNS sur le port TCP 53.	https://dataplane.org/signals/dnstcp.txt
Plan de données Récursivité DNS souhaitée DANS N'IMPORTE QUEL	Adresses IP identifiées comme envoyant du DNS récursif DANS TOUTES LES REQUÊTES.	https://dataplane.org/signals/dnsrdany.txt
Plan de données Récursivité DNS souhaitée	Adresses IP identifiées comme envoyant des requêtes DNS récursives.	https://dataplane.org/signals/dnsrd.txt
Base de données de hameçonnage de GitHub Liens de hameçonnage actifs	Source de données pour l'extraction des liens d'hameçonnage actifs à	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
	partir de la base de données d'hameçonnage disponible sur GitHub.	master/phishing-links-ACTIVE.txt
Base de données d'hameçonnage à partir des domaines actifs GitHub	Source de données pour l'extraction des domaines actifs à partir de la base de données d'hameçonnage disponible sur GitHub.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt
Base de données de hameçonnage à partir de GitHub Adresses IP actives	Source de données pour l'extraction des adresses IP actives à partir de la base de données d'hameçonnage disponible sur GitHub.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
Liste de blocage des bots	Toutes les adresses IP qui ont été signalées au cours des dernières 48 heures comme ayant exécuté des attaques sur les attaques RFI, REG-Bots, IRC-Bots ou BadBots.	https://lists.blocklist.de/lists/bots.txt
Bloquer les attaques Apache	Toutes les adresses IP qui ont été signalées au cours des dernières 48 heures comme ayant exécuté des attaques sur le service Apache, Apache-DDOS, RFI-Attacks.	https://lists.blocklist.de/lists/apache.txt
Liste noire Voip par Scopserv	Récupérer la liste des adresses IP sur liste de blocage à partir de la liste noire VoIP.	http://voipbl.org/update/?dm=bl
Liste de blocage du domaine ThreatView	Domaines malveillants identifiés pour l'hameçonnage/la diffusion de programmes malveillants/le commandement et le contrôle.	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
Liste de blocage de hachage Threatview MD5	Hachages MD5 de fichiers malveillants ou associés à des logiciels malveillants, des rançongiciels, des outils de piratage, des bots, etc.	https://threatview.io/Downloads/MD5-HASH-ALL.txt
URL Threatview Liste de blocage	URL malveillantes servant les logiciels malveillants, le phishing, les botnets et C2.	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
Liste de blocage de hachage de fichier SHA Threatview	Hachages SHA de fichiers connus ou liés à l'exécution de programmes malveillants.	https://threatview.io/Downloads/SHA-HASH-FEED.txt
Liste de blocage d'adresses IP Threatview	Liste de blocage d'adresses IP malveillantes pour les adresses IP incorrectes connues.	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
Flux de chasse Threatview C2	Hébergement de l'infrastructure Serveurs de commande et de contrôle trouvés pendant la chasse proactive par Threatview.io	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
Flux de menaces OSINT Threatview	Indicateurs malveillants de compromission recueillis à partir de la source OSINT - Twitter et Pastebin.	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher les flux CSV

Affichez les flux CSV configurés dans le système de base.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **CSV**.
   Les flux CSV dans le système de base sont expliqués dans le tableau suivant.

Flux des menaces	Description	URL
PhishStats	URL de hameçonnage des 30 derniers jours à partir de PhishStats.	https://phishstats.info/phish_score.csv
Abuse.ch Liste noire des certificats SSL	La liste noire des certificats SSL (CSV) est un CSV qui contient l'empreinte SHA1 de tous les certificats SSL mis sur liste noire sur SSLBL.	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Liste noire d'IP C2 du botnet	Un certificat SSL peut être associé à un ou plusieurs serveurs (combinaison adresse IP :port). SSLBL collecte les adresses IP qui s'exécutent avec un certificat SSL mis sur liste noire sur SSLBL. Il s'agit généralement de serveurs de commande et de contrôle (C&C) de botnet. SSLBL publie donc une liste noire contenant ces adresses IP qui peuvent être utilisées pour détecter le trafic C2 des botnets des machines infectées vers Internet, quittant votre réseau.	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
Phishtank en ligne	N/A	https://data.phishtank.com/data/online-valid.csv

4. Cliquez sur **Modifier** pour modifier le flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les flux JSON

Affichez les flux JSON configurés dans le système de base.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **l'option JSON** .
   La section suivante répertorie les flux JSON configurés dans le système de base.

Flux de menaces	Description	URL
Hôtes C&C Feodotracker	Source de données pour extraire la liste de blocage des adresses IP C2 du botnet à partir de Feodotracker	https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.json
Feodotracker	Source de données pour extraire la liste de blocage des adresses IP C2 du botnet à partir de Feodotracker	https://feodotracker.abuse.ch/downloads/ipblocklist.json

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher les flux RSS

Affichez les flux RSS configurés dans le système de base.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **l'option RSS** .
   La section suivante répertorie les flux RSS configurés dans le système de base.

Flux de menaces	Description	URL
CISO2CISO.COM flux RSS	Données du flux RSS à partir de CISO2CISO.com	https://ciso2ciso.com/feed/
Schneier dans Flux RSS de sécurité	Données du flux RSS de Schneier sur la sécurité	https://www.schneier.com/feed/atom/
Krebs sur le flux RSS de sécurité	Données du flux RSS de KerbsonSecurity	https://krebsonsecurity.com/feed/
Flux RSS de sécurité en direct	Données du flux RSS de welivesecurity	http://feeds.feedburner.com/eset/blog
Flux RSS JISA Softech	Données du flux RSS de JISA	https://www.jisasoftech.com/feed/

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de menaces	Description	URL
Flux RSS de sécurité de Cisco Newsroom	Dernières nouvelles sur la sécurité de cisco.	https://newsroom.cisco.com/c/services/i/servlets/newsroom/rssfeed.json?feed=security
Sécurité HelpNet	Actualités sur la sécurité de l'information avec un accent sur la sécurité des entreprises.	https://www.helpnetsecurity.com/feed/
Affaires de sécurité	Informations sur la criminalistique numérique provenant de médias de premier plan.	https://securityaffairs.com/feed
Flux RSS Volexity	Données du flux RSS des blogs sur la sécurité de l'information de Volexity.	https://www.volexity.com/blog/feed/
Flux RSS de Hackers News	Données du flux RSS de "The Hacker News	https://feeds.feedburner.com/TheHackersNews?format=xml
Graham Cluley Fil RSS	Données du flux RSS de Graham Cluley	https://grahamcluley.com/feed/

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher le flux personnalisé

Affichez les flux personnalisés envoyés dans le système de base.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez **Personnalisé**.
   Le tableau suivant répertorie le flux personnalisé prêt à l'emploi.

Flux des menaces	Description	URL
Flux CrowdStrike	Source pour obtenir les données d'acteurs, d'observables et de rapports de CrowdStrike.	https://api.crowdstrike.com

4. Cliquez sur **Modifier** pour modifier le flux.

Afficher le flux de menaces Premium pour CrowdStrike

Le flux CrowdStrike permet aux utilisateurs d'ingérer des indicateurs, des acteurs, des rapports et leur contexte associé à partir du flux CrowdStrike Falcon Intelligence vers TISC.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

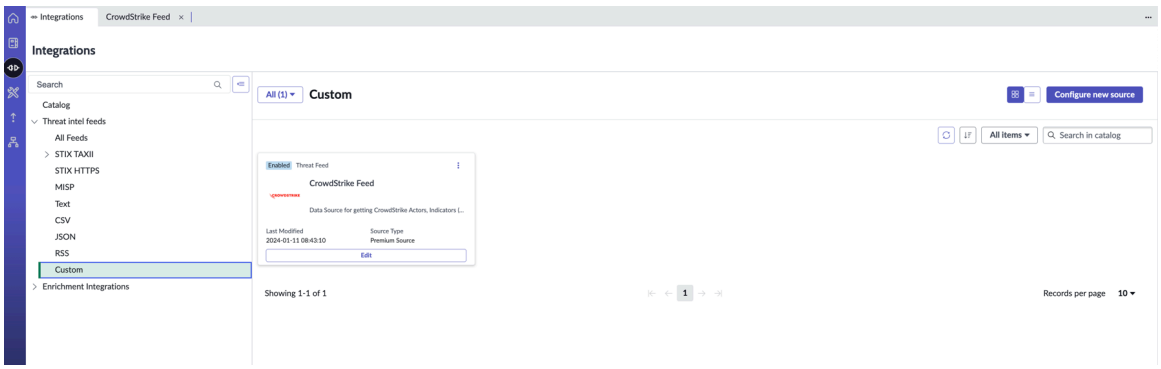
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Intégrations**.
2. Sélectionnez **Personnalisé**.
3. Cliquez sur le bouton **Modifier** dans la page `CrowdStrike` **du formulaire Flux** .

   Remarque : Par défaut, le flux CrowdStrike est désactivé, vous devez modifier les configurations pour activer le flux.



4. Explorez jusqu'à la section **Détails de la configuration** .
5. Saisissez **l'ID et** le **secret client**.

   Remarque :

   a. Vous devez générer votre ID client et votre secret client au cas où vous ne les auriez pas. Pour plus d'informations sur l'ID client et le secret client, consultez la section Définir votre premier client API .

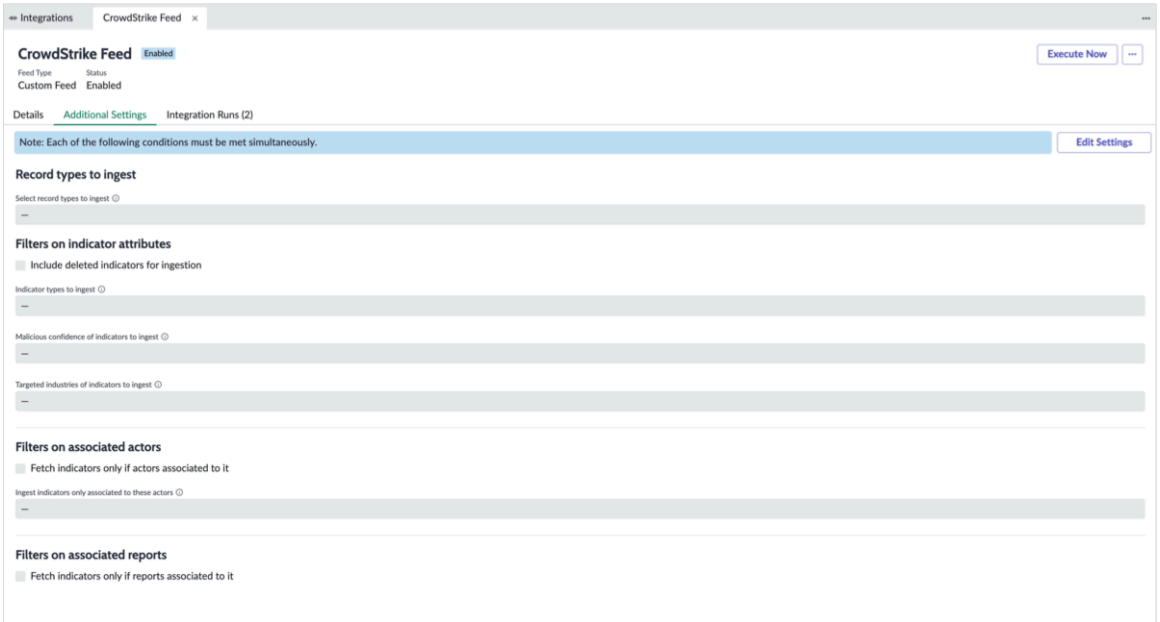
   b. Obtenir l'ID client et le secret client pour `CrowdStrike` les champs d'application requis. Vous trouverez ci-dessous les champs d'application requis pour l'ID client et le secret client de `CrowdStrike`:

   - Indicateurs (Falcon intelligence)
   - Acteurs (Falcon Intelligence)
   - Rapports (Falcon Intelligence)

6. Naviguez vers **Paramètres supplémentaires** pour configurer les filtres qui seront appliqués lors de l'ingestion d'indicateurs à partir de CrowdStrike.

Traduction automatique

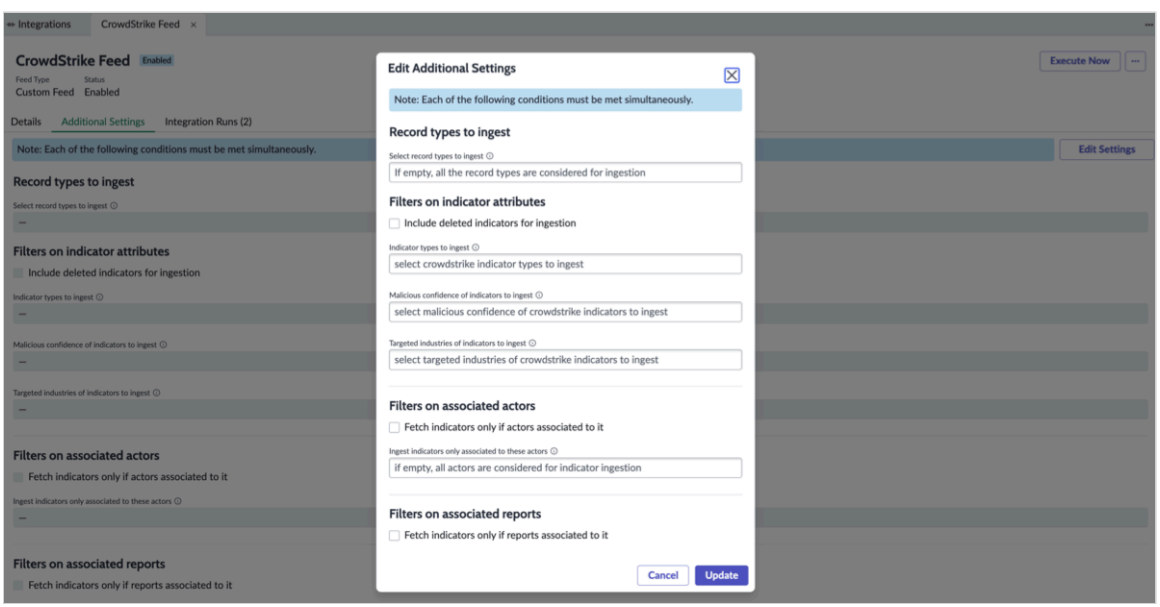
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'onglet **Paramètres supplémentaires** est principalement utilisé pour configurer les filtres qui contrôlent la façon dont les données sont ingérées dans l'application.

Ces filtres vous permettent de personnaliser le processus d'intégration des données pour répondre à vos besoins spécifiques, en veillant à ce que seules les informations les plus pertinentes soient incluses.

7. Cliquez sur **Modifier les paramètres**.



8. Sélectionnez les filtres requis.

Remarque : Tous les filtres configurés seront appliqués conjointement lors de l'ingestion d'indicateurs à partir de CrowdStrike.

La section ci-dessous fournit une explication détaillée de chaque option disponible. Passez en revue chaque option dans le tableau suivant pour comprendre comment les filtres peuvent être appliqués pour optimiser les données ingérées dans l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Sélectionnez les valeurs requises dans les filtres disponibles ci-dessous.

Modifier les paramètres supplémentaires

Champ	Description
Types d'enregistrements à ingérer	
Sélectionner les types d'enregistrement à ingérer	Sélectionnez les types d'enregistrements que vous souhaitez ingérer. Les types d'enregistrement disponibles sont Indicateurs, Rapports et Acteurs. **Remarque :** Si vous sélectionnez uniquement **les indicateurs** comme type d'enregistrement à ingérer, les rapports connexes et les acteurs associés à ces indicateurs ne seront pas ingérés automatiquement. Pour ingérer les rapports et acteurs connexes, vous devez sélectionner les trois types d'enregistrements : Indicateurs, Rapports et Acteurs.
Filtres sur les attributs d'indicateur	
Inclure les indicateurs supprimés pour l'ingestion	Cochez cette case pour autoriser l'ingestion des indicateurs qui ont été supprimés. **Remarque :** Les indicateurs supprimés ne seront créés en tant qu'observables que s'ils ont été précédemment ingérés. Une balise **Supprimé dans CrowdStrike** est ajoutée aux indicateurs qui sont supprimés de CrowdStrike.
Types d'indicateurs à ingérer	Sélectionnez les types d'indicateurs spécifiques CrowdStrike que vous souhaitez ingérer. Si aucun n'est sélectionné, tous les indicateurs disponibles sont récupérés par défaut.
Confiance malveillante des indicateurs à ingérer	Sélectionnez le niveau de confiance malveillante des CrowdStrike indicateurs à ingérer. Si ce champ est laissé vide, tous les indicateurs sont extraits CrowdStrike , quelle que soit leur confiance malveillante.
Secteurs ciblés des indicateurs à ingérer	Sélectionnez les secteurs ciblés associés CrowdStrike aux indicateurs à ingérer. Si aucun n'est sélectionné, tous les indicateurs sont extraits CrowdStrike , quel que soit le secteur ciblé.
Filtres sur les acteurs associés	
Extraire les indicateurs uniquement si des acteurs y sont associés	Cochez cette case pour extraire des indicateurs uniquement s'ils sont associés à des acteurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Indicateurs d'ingestion associés uniquement à ces acteurs	Spécifiez des noms d'acteurs séparés par des virgules liés aux indicateurs pour l'ingestion. S'ils ne sont pas fournis, tous les indicateurs sont récupérés, CrowdStrike quels que soient les acteurs associés.
Filtres sur les rapports associés	
Extraire les indicateurs uniquement si des rapports leur sont associés	Cochez cette case pour extraire des indicateurs uniquement s'ils sont associés à des rapports.
Ingérer les indicateurs uniquement associés à ces rapports	Saisissez les noms des rapports séparés par des virgules associés aux indicateurs pour l'ingestion. Si ce champ est laissé vide, tous les rapports seront inclus dans le processus d'ingestion. Si ce n'est pas fourni, tous les indicateurs sont extraits CrowdStrike , quels que soient les rapports associés.
Filtres sur les familles de programmes malveillants associées	
Extraire les indicateurs uniquement si des familles de programmes malveillants y sont associées	Cochez cette case pour extraire les indicateurs uniquement s'ils sont associés à des familles de programmes malveillants.
Indicateurs d'ingestion uniquement associés à ces familles de programmes malveillants	Entrez des noms de familles de programmes malveillants séparés par des virgules associés aux indicateurs pour l'ingestion. Si ce champ est laissé vide, toutes les familles de programmes malveillants seront incluses dans le processus d'ingestion. S'ils ne sont pas fournis, tous les indicateurs sont récupérés, quelle que soit la famille de CrowdStrike programmes malveillants.
Mappage de la confiance malveillante d'indicateur à la confiance TISC **Remarque :** Les valeurs Élevé, Moyen et Faible correspondent à la valeur source de la confiance malveillante reçue de CrowdStrike.	
Élevé	Entrez une valeur de confiance (0-100) pour les indicateurs avec un score de confiance malveillant élevé. **Remarque :** Si un mappage de fiabilité malveillante correspondant est trouvé dans les **paramètres supplémentaires**, il remplacera la valeur fournie dans la section **Détails** même si une valeur de confiance est saisie manuellement.
Moyen	Entrez une valeur de confiance (0-100) pour les indicateurs avec une confiance malveillante moyenne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Faible	Entrez une valeur de confiance (0 à 100) pour les indicateurs dont le score de confiance malveillant est faible.
Non vérifié	Saisissez une valeur de confiance (0-100) pour les indicateurs dont la fiabilité malveillante n'est pas vérifiée.

Remarque : Avec les mêmes paramètres supplémentaires que ceux définis ci-dessus, vous pouvez dupliquer le flux lors de la création d'un nouveau flux.

10. Cliquez sur **Mettre à jour** dans la boîte de dialogue **Paramètres supplémentaires** pour enregistrer les paramètres supplémentaires modifiés.
11. Cliquez sur **Activer** pour activer CrowdStrike le flux pour l'ingestion.

Remarque : Le flux Premium est identique aux autres flux, à l'exception de la réponse qui est analysée lors de la configuration. Une réponse spécifique est analysée CrowdStrike en ajoutant l'ID client et le secret client.

À partir de quel type de données sont extraites : *CrowdStrike*

a. Les indicateurs qui sont mis à jour après l'heure d'ingestion CrowdStrike configurée et qui correspondent aux filtres configurés dans le cadre des paramètres supplémentaires. Ces indicateurs seront CrowdStrike ensuite mappés aux observables dans TISC. Voici les types d'indicateurs qui sont ingérés dans TISC:
   - Hachage SHA256
   - Hachage MD5
   - Hachage SHA1
   - URL
   - Domaine
   - Adresse IP
   - Nom Mutex
   - Nom du fichier
   - Adresse e-mail
   - Nom d'utilisateur
   - Bloc d'adresses IP

b. Les acteurs de menace qui sont mis à jour après le délai d'ingestion configuré sont mappés aux acteurs de CrowdStrike menace dans TISC.

c. Les rapports mis à jour après le délai d'ingestion configuré sont mappés aux rapports sur CrowdStrike les menaces en TISC fonction des attributs correspondants.

d. En plus des entités mentionnées ci-dessus, les données connexes suivantes sont également extraites :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

i. Acteurs de menace, rapports et indicateurs associés aux indicateurs précédemment ingérés.

ii. Acteurs de menace et indicateurs associés à tous les rapports ingérés au cours du processus d'ingestion actuel.

Remarque : Les filtres configurés dans Paramètres **supplémentaires** seront également appliqués lors de l'ingestion des indicateurs associés aux indicateurs, rapports ou acteurs précédemment ingérés.

12. **Facultatif :** Cliquez sur **Dupliquer pour dupliquer** le flux.
Pour plus d'informations, consultez Dupliquer les flux Threat Intelligence.

Propriétés système pour CrowdStrike

Ce qui suit détaille les propriétés système de CrowdStrike.

1. sn_sec_tisc.crowdstrike_actor_batch_size : indique le nombre d'acteurs à extraire dans un seul appel d'API. Remarque : applicable uniquement lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système.
   - Type : entier
   - Valeur : 250
2. sn_sec_tisc.crowdstrike_api_limit : nombre d'enregistrements à extraire simultanément à partir de CrowdStrike. Plus la valeur est élevée, plus la mémoire consommée pour le traitement de la charge utile est élevée.
   - Type : entier
   - Valeur : 1000
3. sn_sec_tisc.crowdstrike_indicator_batch_size : indique le nombre d'indicateurs à extraire dans un seul appel d'API. Remarque : applicable uniquement lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système.
   - Type : entier
   - Valeur : 150
4. sn_sec_tisc.crowdstrike_offset_limit_total : total autorisé du décalage et de la limite par l'API CrowdStrike.
   - Type : entier
   - Valeur : 50000
5. sn_sec_tisc.crowdstrike_report_batch_size : indique le nombre de rapports à extraire dans un seul appel d'API. Remarque : applicable uniquement lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système.
   - Type : entier
   - Valeur : 50

Comprendre STIX TAXII

STIX (Structured Threat Information Expression) est un langage et un format de sérialisation utilisés pour échanger des renseignements sur les cybermenaces (CTI). Le TAXII (Trusted Automated Exchange of Intelligence Information) est un protocole utilisé pour échanger des renseignements sur les cybermenaces (CTI) via HTTPS.

Avec STIX, tous les aspects de la suspicion, de la compromission et de l'attribution sont représentés sous forme d'objets et de relations descriptives. Les informations STIX

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

peuvent être représentées visuellement pour un analyste ou stockées au format JSON pour être rapidement lisibles par machine.

Cyber Threat Intelligence (CTI) a été créé pour définir un ensemble de représentations et de protocoles d'information afin de répondre au besoin de modéliser, d'analyser et de partager des renseignements sur les cybermenaces. Le CTI se concentre principalement sur le développement et la normalisation de STIX (Structured Threat Information Expression) et de TAXII (Trusted Automated Exchange of Indicator Information).

Configurer un nouveau flux TAXII

Vous pouvez gérer des flux TAXII pour partager des informations au format STIX. Chaque flux TAXII contient une ou plusieurs collections TAXII.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionner **Flux de Threat Intelligence** > **STIX TAXII** > **Flux TAXII**.

   Remarque : Configurez le flux TAXII pour qu'il serve de profil pour toutes les collectes TAXII à l'intérieur.

4. Cliquez sur **Configurer une nouvelle source**.
   La page Configurer un nouveau flux TAXII s'affiche.
5. Remplissez les champs du formulaire.

Créer une source de données

Champ	Description
Nom	Saisissez un nom pour le flux.
Description	Description du flux.
Type de source	Le type de source (source ouverte, source premium...) fourni pour le flux. Les types de sources disponibles sont les suivants : ○ Gouvernement ○ ISACs ○ Open source ○ Source premium ○ Autre source
Logo	Joindre le logo du flux source.
Secteur	Sélectionnez la catégorie d'industrie (aérospatiale, agriculture, etc.) à laquelle la source de données de flux s'applique.

Renseignez les champs de la section Configuration comme il convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration

Champ	Description
Version TAXII	Sélectionnez la version TAXII du serveur TAXII à configurer. Les versions prises en charge sont 2.0 et 2.1.
Type de configuration	Fournissez un type de configuration pour extraire les collections TAXII. Les valeurs disponibles sont les suivantes : ○ **URL du service Découverte** : choisissez l'URL du service Découverte pour extraire les collections de toutes les racines d'API disponibles dans le service Découverte du serveur TAXII. ○ **URL racine de l'API** : choisissez l'URL racine de l'API pour extraire les collections à partir de la racine API spécifique du serveur TAXII.
Authentification	Sélectionnez l'option requise dans la liste déroulante si l'authentification est requise. Les options disponibles sont les suivantes : ○ **Aucun** : sélectionnez cette option si aucune authentification n'est requise. ○ **De base** : sélectionnez cette option pour fournir un nom d'utilisateur et un mot de passe. ○ **Clé API** : sélectionnez cette option pour fournir une clé API. ○ **Choisir un message REST** : sélectionnez cette option pour tout autre type d'authentification. Les options du message REST sont les suivantes : ▪ **Utiliser le message REST** : cochez cette case si vous avez besoin d'un message REST pour créer un message REST prédéfini. Si vous ne sélectionnez pas, la valeur du champ de point de terminaison sera utilisée. Cliquez sur l'icône de recherche, puis sélectionnez le message REST dans la liste. ▪ **Méthode REST** : cochez cette case si vous avez besoin d'une méthode REST. Cliquez sur l'icône de recherche, puis sélectionnez la méthode REST dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Les champs de message REST et de méthode REST deviennent disponibles lorsque l'option de message REST est sélectionnée.
URL	Entrez l'URL du service de découverte du serveur TAXII ou l'URL racine de l'API spécifique en fonction du type de configuration sélectionné.
Section avancée	
Avancés	Cochez la case pour choisir un script d'intégration et un processeur de rapport différents. Assurez-vous que les scripts choisis sont compatibles avec la version TAXII sélectionnée. En fonction de la version et de l'authentification TAXII, ces scripts sont renseignés automatiquement par défaut.
Script d'intégration	Appelle un appel à l'API de l'URL du point de terminaison REST à l'aide des paramètres d'authentification tels que le type d'authentification : nom d'utilisateur/mot de passe/clé API et les en-têtes à transmettre avec la demande, puis le script récupère les observables ou les indicateurs Données STIX disponibles pour le flux spécifique. **Remarque :** Les données récupérées sont uniquement des données brutes (aucun enregistrement n'est créé) qui seront jointes au processus d'intégration et pourront ensuite être affichées dans la section **Exécution de l'intégration** . Dans le système de base, les includes de scripts personnalisés sont fournis dans l'application pour les scripts d'intégration : ○ TAXIIV2_0QueryParamAPIKeyIntegrationScript ○ TAXIIV2_0BasicAuthIntegrationScript ○ TAXIIV2_1QueryParamAPIKeyIntegrationScript ○ TAXIIV2_1BasicAuthIntegrationScript Le script d'intégration par défaut est basé sur le type de flux que vous sélectionnez. Le script includes exécute un appel REST simple, enregistre la réponse sous forme de pièce jointe, puis renvoie la pièce jointe au processeur.
Script de processeur de rapport	Le processeur de rapports appelle l'URL du point de terminaison REST.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Dans le système de base ci-dessous se trouve le Includes de scripts personnalisés, qui est mis en service dans l'application pour les scripts d'intégration, **TAXIIV2CollectionDataProcessor**.

Renseignez les champs de la section Planification, comme il convient.

Ordonnancement

Champ	Description
Fréquence d'exécution des collectes	Intervalle de planification qui sera appliqué aux enregistrements de collecte TAXII. La fréquence d'exécution d'une collecte TAXII peut être modifiée dans la vue du formulaire de collecte TAXII, si nécessaire. **Remarque :** Ce paramètre est appliqué par défaut à toutes les collectes TAXII qui sont récupérées. Il existe une option pour remplacer le paramètre dans les collectes TAXII, si nécessaire. Pour plus d'informations, consultez Travaux planifiés et comment exécuter automatiquement un script de votre choix .
Extraire les données de	Date de début à partir de laquelle les données doivent être extraites. Ce champ doit être défini avec le délai à partir duquel les données doivent être ingérées à partir de la source correspondante. Une fois ce champ défini, l'exécution d'ingestion suivante extrait les données à partir de l'heure configurée et les exécutions d'ingestion consécutives extraient des données incrémentielles. Par exemple, la source est planifiée pour ingérer les données toutes les heures. L'utilisateur définit **Extraire les données du** 12 janvier à 6h00 le 12 janvier à 9h30. L'ingestion se déclenchant le 12 janvier à 10h00 permet d'extraire les données du 12 janvier à 6h00 au 12 janvier à 10h00. L'ingestion suivante qui se déclenche à 11h00 extrait uniquement les données incrémentielles du 12 janvier à 10h00 au 12 janvier à 11h00. **Remarque :** Cela signifie que les exécutions planifiées extrairont les données de façon incrémentielle à partir de la date spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquer sur **Valider la connexion**
   Un message d'information s'affiche indiquant que la connexion du flux TAXII a réussi. Pour extraire les collections, passez à l'étape suivante.
7. Cliquez sur **Obtenir les collections TAXII**.

   Remarque : En cas d'erreurs, un message d'erreur s'affiche indiquant qu'une erreur s'est produite lors de l'extraction des collectes TAXII et vérifiez les journaux pour plus de détails.

   Les collections TAXII sont affichées dans la section Collections TAXII et sont désactivées par défaut.
8. Activez les collections TAXII pour récupérer les objets STIX disponibles dans ces collections TAXII.

Dupliquer les flux Threat Intelligence

La duplication d'un flux de menaces vous permet de créer une copie exacte d'un flux existant, y compris tous les observables, indicateurs, acteurs associés, etc.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur **l'icône Intégrations** .
3. Sélectionnez l'intégration souhaitée dans la vue **Catalogue** .
   Par exemple, sélectionnez CrowdStrike
4. Cliquez sur le bouton **Modifier** pour CrowdStrike la carte de flux afin d'ouvrir le formulaire de configuration.
5. Cliquez sur le menu **Actions supplémentaires** , puis sélectionnez **Dupliquer**.
   Une confirmation s'affiche, indiquant que vous avez dupliqué la configuration actuelle du flux et créé un nouveau flux portant le nom [integrationname, Feed-copy] avec un lien vers le nouveau flux dupliqué. Par exemple, CrowdStrike Feed-copy.

Intégrations de l'enrichissement TISC

Le Centre de sécurité des renseignements sur les menaces système de base n'inclut aucune intégration préconfigurée. Cette section fournit des instructions pour configurer les intégrations ServiceNow tierces.

Important :

Assurez-vous d'avoir installé les intégrations d'applications tierces requises. Vous pouvez voir les détails des observables, de la recherche de perception et de la recherche de menaces uniquement pour les applications tierces qui sont installées.

Toutes les configurations d'intégration

Toutes les intégrations sont des applications distinctes qui doivent être installées. TISC prend en charge les intégrations avec des fournisseurs tiers. Toutes les intégrations installées peuvent être configurées ici.

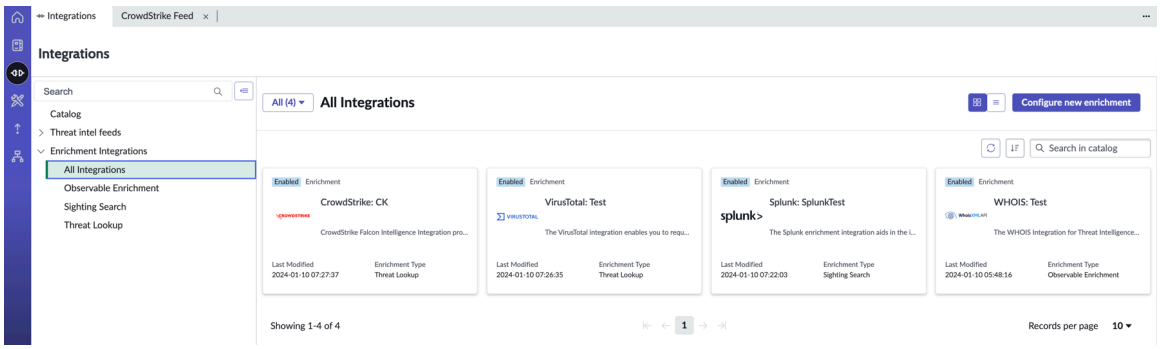
Cette section affiche les cartes pour chacune des implémentations d'intégration configurées que vous pouvez activer et utiliser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La section de chaque type d'enrichissement n'est visible que si au moins une des intégrations correspondantes pour ce type d'enrichissement est installée. Par exemple, la section **Recherche de menaces n'est** visible sous **Intégrations d'enrichissement** que si au moins une intégration de Recherche de menaces est installée.

Les cartes d'intégration configurées peuvent être consultées en accédant à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.



Actions sur la vue Toutes les intégrations

La vue Toutes les intégrations vous permet d'effectuer les actions suivantes.

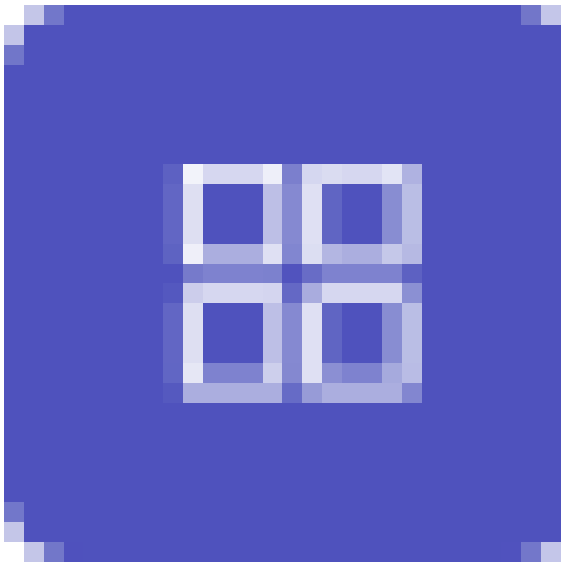
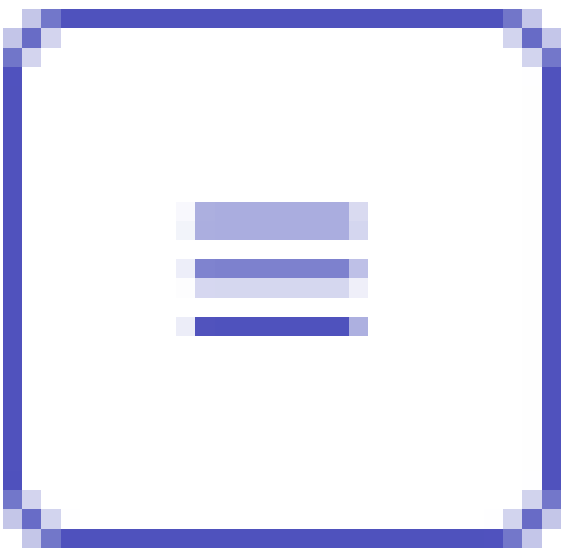
Actions sur la vue Toutes les intégrations

Action	Description
Tous	Utilisez ce menu déroulant pour filtrer les intégrations en fonction de leur état actuel. Vous pouvez filtrer en fonction des états suivants : • **Tout** : affiche toutes les intégrations sur la page. Il s'agit de l'option par défaut. • **Activé** : affiche toutes les intégrations qui sont à l'état Activé. • **Désactivé** : affiche toutes les intégrations qui sont à l'état désactivé. • **Brouillon** : affiche toutes les intégrations qui sont à l'état de brouillon.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

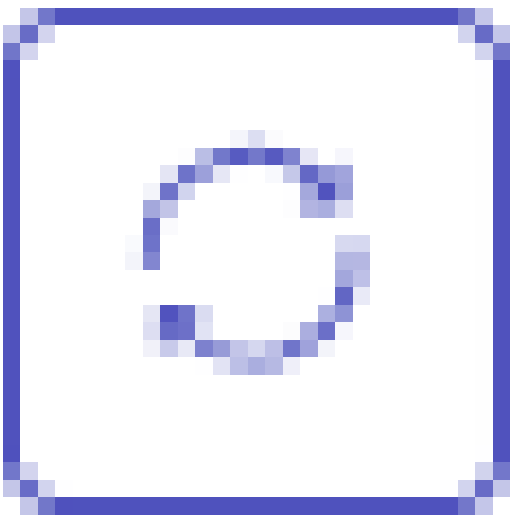
Actions sur la vue Toutes les intégrations (suite)

Action	Description
	Utilisez cette action pour afficher toutes les intégrations sous forme de cartes.
	Utilisez cette action pour afficher toutes les intégrations sous forme de listes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions sur la vue Toutes les intégrations (suite)

Action	Description
	Utilisez cette action pour actualiser la page Toutes les intégrations.
	Utilisez cette action pour trier toutes les intégrations en fonction des éléments suivants : • **Dernière modification (récente)** • **Dernière modification (la plus ancienne)** • **Nom (A-Z)** • **Nom (de Z à A)**
Rechercher dans le catalogue	Utilisez cette action pour rechercher les intégrations configurées en fonction du nom et de la description dans le catalogue.

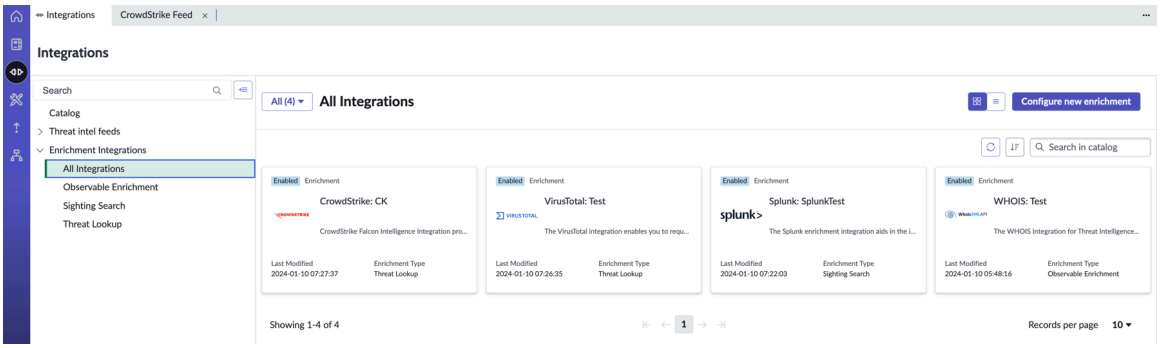
Traduction automatique

Configurer un nouvel enrichissement à partir de la vue Toutes les intégrations

Vous pouvez configurer de nouveaux enrichissements à partir de la vue Toutes les intégrations ou directement à partir des sections Enrichissement des observables, Recherche de perception ou Recherche de menace respectivement. Pour configurer le nouvel enrichissement à partir de la vue Toutes les intégrations, procédez comme suit.

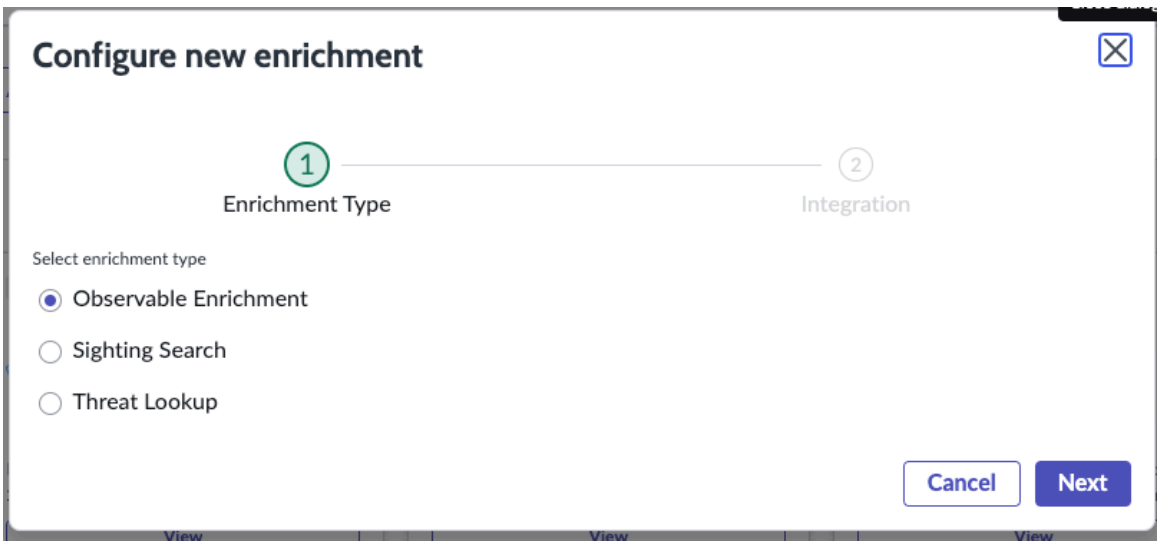
1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Intégrations** , puis sélectionnez la section **Toutes les intégrations** .

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur l'action **Configurer un nouvel enrichissement** .

   La fenêtre contextuelle Configurer un nouvel enrichissement s'affiche avec trois types d'enrichissement : Enrichissement des observables, Recherche de perception ou Recherche de menaces. Vous devez choisir le type d'enrichissement que vous souhaitez configurer.



4. Sélectionnez un type d'enrichissement, puis cliquez sur **Suivant**.

   Vous accédez alors à la fenêtre contextuelle qui affiche les intégrations disponibles. Vous devez choisir l'intégration que vous souhaitez configurer.

5. Sélectionnez une intégration dans la liste des intégrations disponibles, puis cliquez sur **Sélectionner**.

   Vous accédez alors à la page Créer une intégration d'enrichissement de l'intégration sélectionnée. Cette page est préremplie avec les détails de l'intégration sélectionnée par défaut. Par exemple, l'intégration WHOIS.

6. Renseignez les champs du formulaire Créer une intégration.

Configurer le nouveau formulaire d'intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration de l'enrichissement. Par exemple, WHOIS1.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont préremplis par défaut. Par exemple, WHOIS.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Enrichissement des observables. Les détails du type d'intégration sélectionné sont préremplis par défaut. Les types d'intégration suivants sont pris en charge : ○ Enrichissement des éléments observables ○ Recherche de perception ○ Recherche de menace
Description	Saisissez une description unique pour la nouvelle intégration de l'enrichissement.

7. Dans la section Configuration de l'intégration, configurez les détails de l'intégration en fonction de vos besoins.

   La section Configuration de l'intégration comprend des détails de configuration tels que la clé API, l'ID ou le secret client API, le nom d'utilisateur, le mot de passe, etc., que vous devez remplir. Ces détails de configuration varient selon les intégrations.

8. Cliquez sur l'action **Enregistrer** pour stocker et créer la configuration de l'intégration de l'enrichissement.

   Les détails fournis sont validés et, par défaut, l'état de l'intégration d'enrichissement est désactivé.

9. (Facultatif) Cliquez sur l'action **Enregistrer comme brouillon** pour stocker uniquement les configurations d'intégration comme brouillon. Les utilisateurs ne peuvent pas activer une intégration lorsqu'elle est enregistrée dans le brouillon

   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez renseigner les informations restantes dans la version brouillon et la créer.

10. Pour activer l'intégration de l'enrichissement, cliquez sur **Activer**.

    L'intégration de l'enrichissement est activée avec succès.

11. Vous pouvez également activer, désactiver ou supprimer une intégration d'enrichissement particulière à l'aide du menu Actions de la vignette d'intégration requise sur la page Catalogue ou la page Intégrations d'enrichissement.

Configurer l'enrichissement des observables

Vous pouvez effectuer un enrichissement de la connaissance des menaces sur un ou plusieurs observables pour déterminer s'ils sont associés à des menaces de sécurité connues. Les implémentations qui s'exécutent dépendent de celles que vous avez activées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Prend Centre de sécurité des renseignements sur les menaces en charge l'enrichissement des observables uniquement pour l'intégration WHOIS pour l'instant. Pour plus d'informations, consultez Configurer et activer l'intégration Whois.

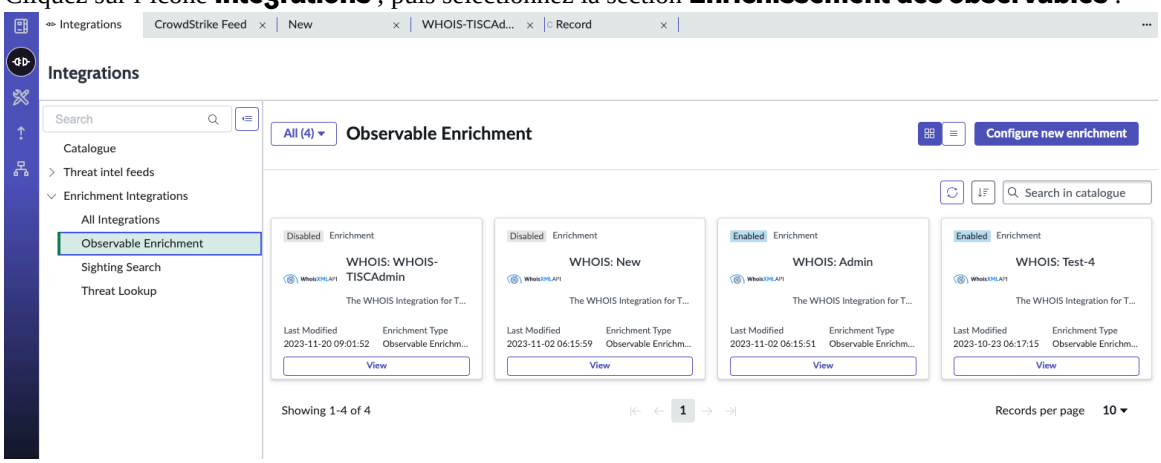
Remarque : Le module Intégrations de l'enrichissement s'affiche uniquement si au moins une des intégrations prenant en charge l'une des options est installée dans l'application.

Pourquoi et quand exécuter cette tâche

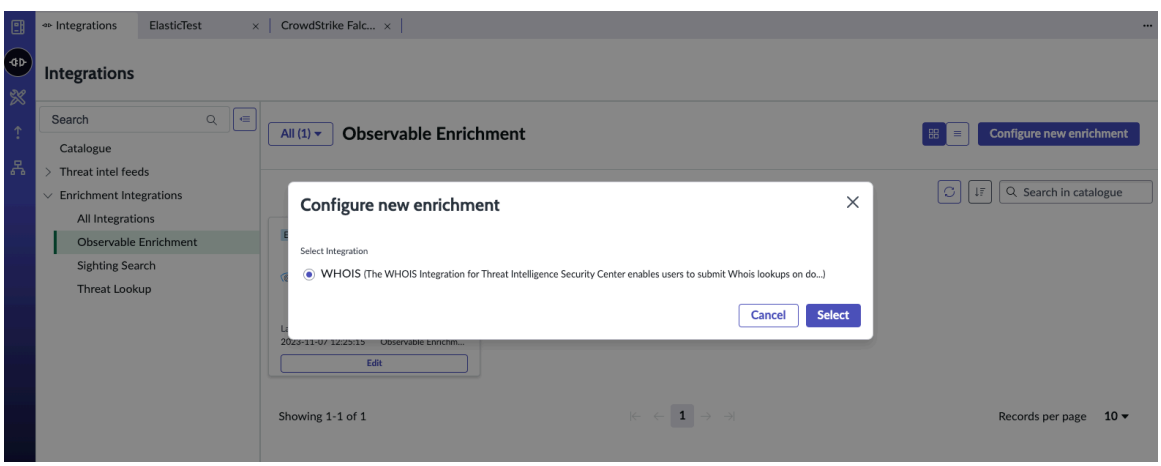
La section Enrichissement des observables contient uniquement les intégrations avec le type d'intégration en tant qu'enrichissement des observables. Cette section affiche les cartes pour chacune des implémentations d'intégration configurées que vous pouvez activer et utiliser.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Intégrations** , puis sélectionnez la section **Enrichissement des observables** .



3. Cliquez sur l'action **Configurer un nouvel enrichissement** .
   Vous accédez alors à la fenêtre contextuelle qui affiche les intégrations disponibles. Vous devez choisir l'intégration que vous devez configurer.
4. Sélectionnez une intégration dans la liste des intégrations disponibles, puis cliquez sur **Sélectionner**.
   Vous accédez alors à la page Créer une intégration d'enrichissement de l'intégration sélectionnée. Cette page est préremplie avec les détails de l'intégration sélectionnée par défaut. Par exemple, l'intégration WHOIS.

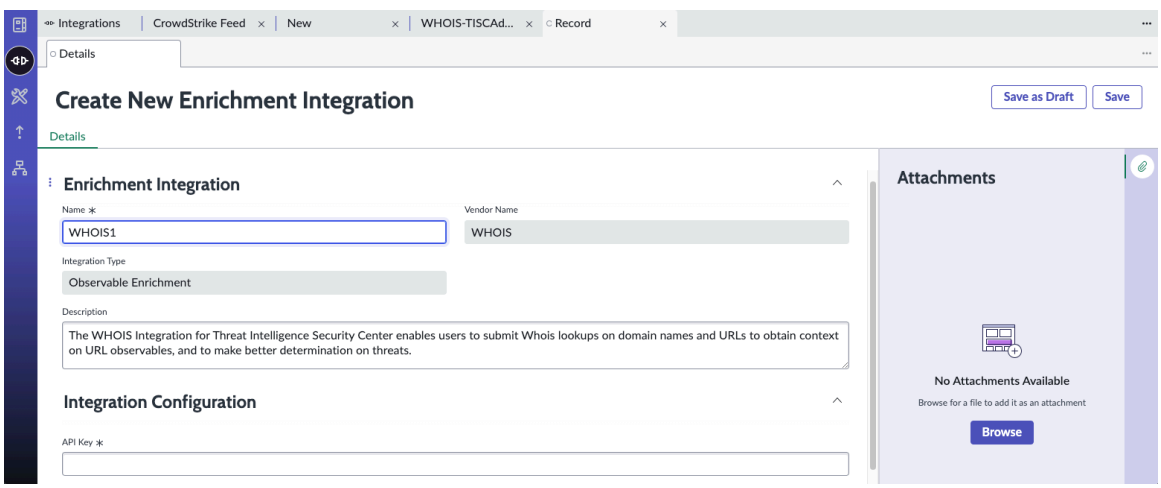


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Renseignez les champs du formulaire Créer une intégration.

Champ	Description
Intégration de l'enrichissement	
Nom	Entrez un nom pour la nouvelle intégration de l'enrichissement. Par exemple, WHOIS1.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont préremplis par défaut. Par exemple, WHOIS.
Type d'intégration	Type d'intégration que vous avez sélectionné, à savoir l'enrichissement des observables. Les détails du type d'intégration sélectionné sont préremplis par défaut.
Description	Saisissez une description unique pour la nouvelle intégration de l'enrichissement.



6. Dans la section Configuration de l'intégration, configurez les détails de l'intégration en fonction de vos besoins.
   La section Configuration de l'intégration comprend des détails de configuration tels que la clé API, l'ID ou le secret client API, le nom d'utilisateur, le mot de passe, etc., que vous devez remplir. Ces détails de configuration varient selon les applications.

7. Cliquez sur l'action **Enregistrer** pour stocker et créer la nouvelle configuration de l'intégration de l'enrichissement.
   Une fois que vous avez cliqué sur l'action **Enregistrer** ou **Activer** , l'intégration est validée à l'aide des configurations d'intégration fournies. Par défaut, l'état de l'intégration d'enrichissement est défini sur désactivé.

8. Cliquez sur l'action **Enregistrer comme brouillon** pour stocker uniquement les mises à jour apportées à la configuration d'enrichissement et ne pas la créer.
   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez renseigner les informations restantes dans la version brouillon et la créer.

9. Pour activer l'intégration de l'enrichissement, cliquez sur **Activer**.
   L'intégration de l'enrichissement est activée avec succès. Vous pouvez également activer, désactiver ou supprimer une intégration d'enrichissement particulière à l'aide du menu Actions de la vignette d'intégration requise sur la page Catalogue ou la page Intégrations d'enrichissement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la recherche de perception

Vous pouvez effectuer une recherche de perceptions sur un ou plusieurs observables pour déterminer le nombre de fois où les observables sont vus dans les journaux de votre organisation. Vous pouvez effectuer une recherche de perception sur les observables dans un nombre de jours ou une plage de dates sélectionné.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Remarque : Le module Intégrations de l'enrichissement s'affiche uniquement si au moins une des intégrations prenant en charge l'une des options est installée dans l'application.

Le prend Centre de sécurité des renseignements sur les menaces en charge la recherche de perception uniquement pour les intégrations suivantes :

- Recherche Splunk
- Elasticsearch

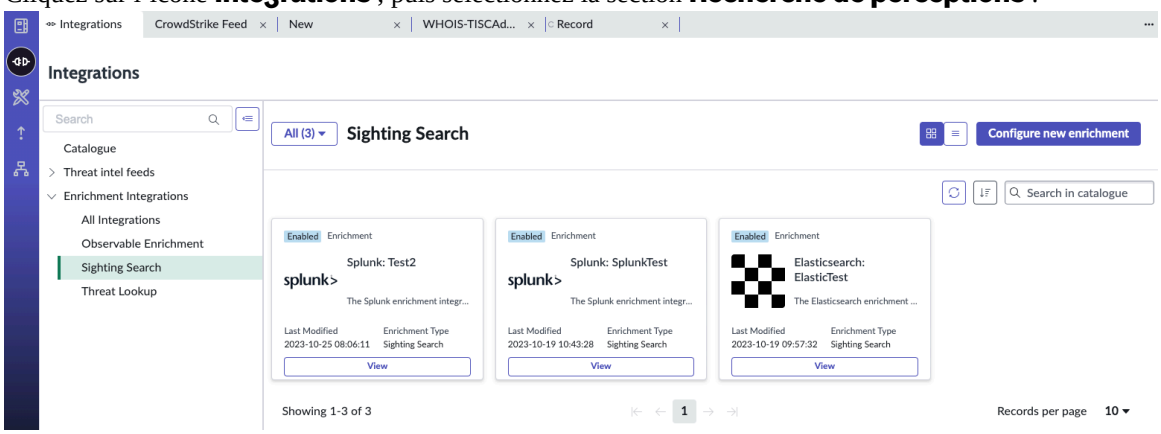
Pourquoi et quand exécuter cette tâche

La section Recherche de perceptions contient uniquement les intégrations avec le type d'intégration Recherche de perceptions.

Cette section affiche les cartes pour chacune des implémentations d'intégration configurées que vous pouvez activer et utiliser.

Procédure

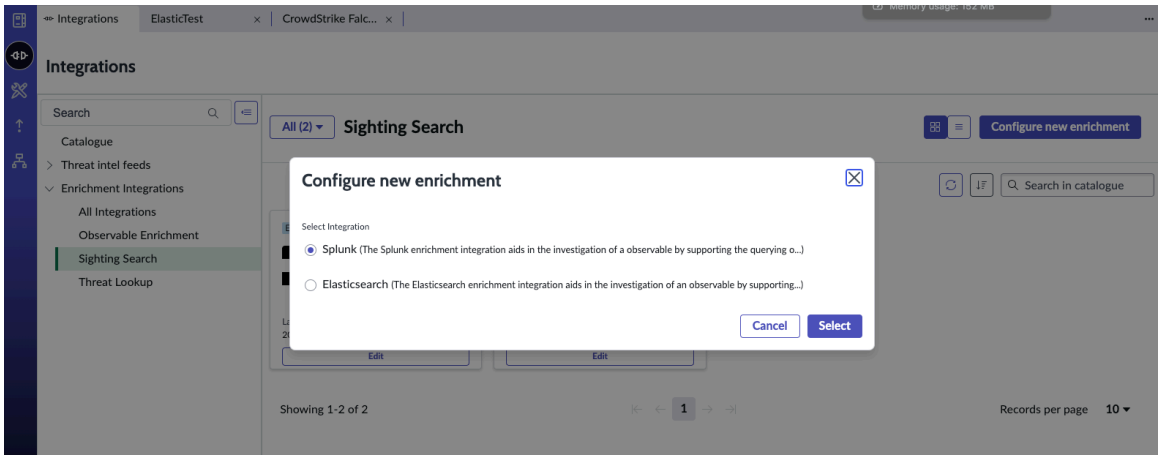
1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Intégrations** , puis sélectionnez la section **Recherche de perceptions** .



3. Cliquez sur l'action **Configurer un nouvel enrichissement** .
   Vous accédez alors à la fenêtre contextuelle qui affiche les intégrations disponibles. Vous devez choisir l'intégration que vous devez configurer.
4. Sélectionnez une intégration dans la liste des intégrations disponibles, puis cliquez sur **Sélectionner**.
   Vous accédez alors à la page Créer une intégration d'enrichissement de l'intégration sélectionnée. Cette page est préremplie avec les détails de l'intégration sélectionnée par défaut. Par exemple, Intégration Splunk.

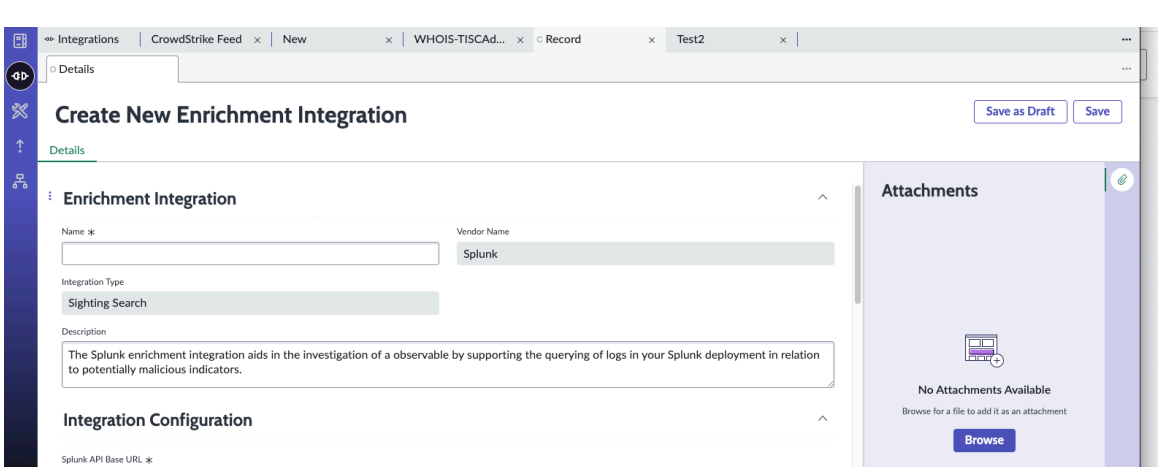
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Renseignez les champs du formulaire Créer une intégration.

Champ	Description
Intégration de l'enrichissement	
Nom	Entrez un nom pour la nouvelle intégration de l'enrichissement. Par exemple, Splunk-1.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont préremplis par défaut. Par exemple, Splunk.
Type d'intégration	Type d'intégration que vous avez sélectionné, à savoir Recherche de perception. Les détails du type d'intégration sélectionné sont préremplis par défaut.
Description	Saisissez une description unique pour la nouvelle intégration de l'enrichissement.



6. Dans la section Configuration de l'intégration, configurez les détails de l'intégration en fonction de vos besoins.
   La section Configuration de l'intégration comprend des détails de configuration tels que la clé API, l'ID ou le secret client API, le nom d'utilisateur, le mot de passe, etc., que vous devez remplir. Ces détails de configuration varient selon les applications.
7. Cliquez sur l'action **Enregistrer** pour stocker et créer la nouvelle configuration de l'intégration de l'enrichissement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les détails fournis sont validés et, par défaut, l'état de l'intégration d'enrichissement est désactivé.

8. Cliquez sur l'action **Enregistrer comme brouillon** pour stocker uniquement les mises à jour apportées à la configuration d'enrichissement et ne pas la créer.
   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez renseigner les informations restantes dans la version brouillon et la créer.
9. Pour activer l'intégration de l'enrichissement, cliquez sur **Activer**.
   L'intégration de l'enrichissement est activée avec succès. Vous pouvez également activer une intégration d'enrichissement particulière à l'aide du menu Actions de la vignette d'intégration requise sur la page Catalogue ou de la page Toute l'intégration.

Définir des requêtes pour la recherche de perception

Vous pouvez utiliser des configurations de recherche de perception pour définir les requêtes utilisées pour trouver la récurrence des observables dans votre environnement dans le cadre des enquêtes sur les observables.

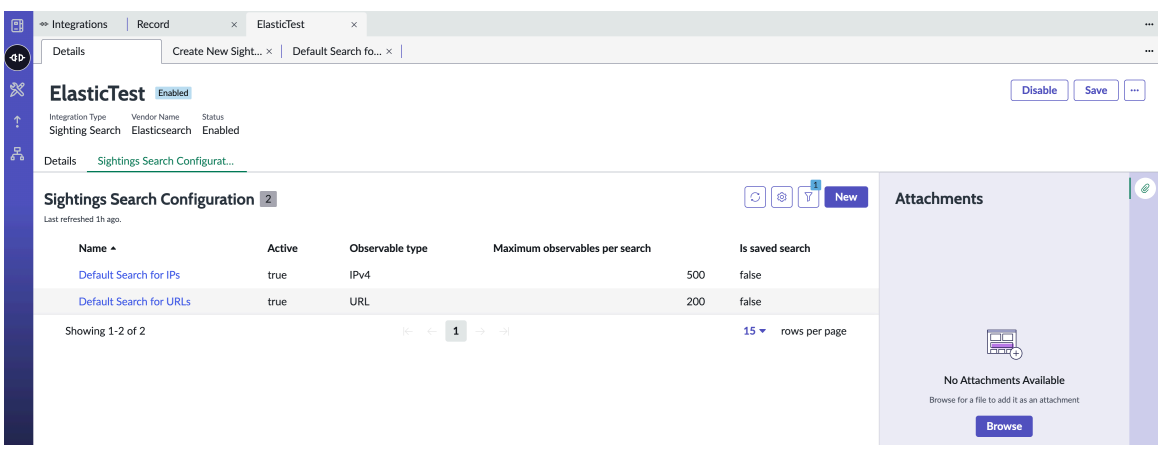
Afficher les requêtes pour la recherche de perception

Rôle requis : sn_sec_tisc.admin

Pour afficher les configurations de recherche de perceptions, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Intégrations**.
2. Sur la page Intégrations, accédez à **Intégrations de l'enrichissement** > **Recherche de perception**.
3. Recherchez l'intégration pour laquelle vous souhaitez afficher la configuration de recherche de perceptions, puis cliquez sur **Modifier**.
4. Sélectionnez l'onglet **Configurations de recherche de perceptions** .

   Vous pouvez afficher la liste des configurations de recherche de perceptions.



5. Cliquez sur la configuration de recherche de perceptions requise pour afficher les détails de la configuration.
6. Pour générer une requête de recherche de perception de test, cliquez sur l'action **Générer une requête de recherche de perception de test** .

   Remarque : L'action **Générer une requête de recherche de perceptions de test** ne fonctionne que si vous avez configuré les paramètres de requête de recherche de perceptions. Pour plus d'informations, consultez Utilisation des paramètres de recherche de perceptions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Dans la fenêtre contextuelle Générer une requête de recherche de perceptions de test, saisissez ou collez plusieurs observables à l'aide de séparateurs de virgules, de nouvelles lignes, d'onglets ou de barres verticales pour générer une requête de test.
8. Cliquez sur **Générer** pour générer la requête de recherche de perceptions de test.
9. Vous pouvez également effectuer les actions suivantes dans l'onglet Configurations de recherche de perceptions :
   a. Pour actualiser la liste des configurations de recherche de perception, cliquez sur l'icône  .
   b. Pour effectuer une action de liste sur les configurations de recherche de perceptions, cliquez sur l'icône  de liste.

      Vous pouvez effectuer les deux actions de liste suivantes :

      - **Modifier les colonnes** : vous pouvez utiliser cette action pour ajouter ou supprimer des colonnes existantes et modifier l'ordre en fonction de vos besoins.
      - **Rétablir la largeur** des colonnes : vous pouvez utiliser cette action pour réinitialiser la largeur des colonnes.

   c. Pour filtrer les configurations de recherche de perceptions en fonction des conditions, cliquez sur l'icône  .

      La valeur 1 indique qu'une condition est utilisée pour le filtrage.

Créer des configurations de recherche de soupirs

Rôle requis : sn_sec_tisc.admin

Maximum observables per search = "maximum number of observables that can be substituted in a single search query"
Search = "Search query that should be executed in sighting search source. Search query can contain substitution variables that would be substituted with observables of specific type as configured in sighting search parameters when sighting search query is formed"

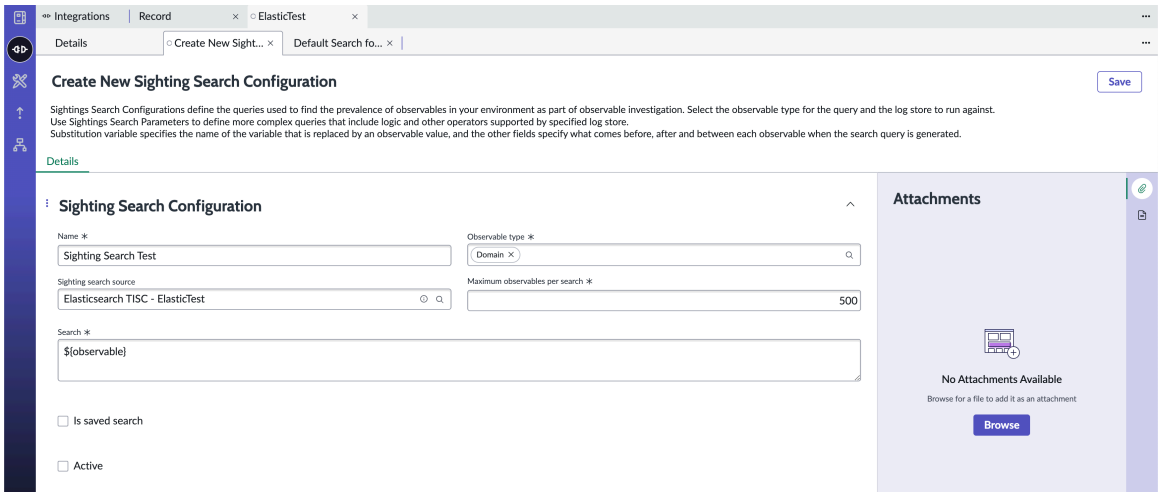
Pour créer une configuration de recherche de perceptions, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Intégrations**.
2. Sur la page Intégrations, accédez à **Intégrations de l'enrichissement** > **Recherche de perception**.
3. Recherchez l'intégration pour laquelle vous souhaitez afficher la configuration de recherche de perceptions, puis cliquez sur **Modifier**.
4. Sélectionnez l'onglet **Configurations de recherche de perceptions** .

   Vous pouvez afficher la liste des configurations de recherche de perceptions.
5. Pour créer une configuration de recherche de perceptions, cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Renseignez les champs du formulaire.

Créer une configuration de recherche de perceptions

Champ	Description
Nom	Nom de la configuration de recherche de perceptions.
Type d'observable	Définit le type de catégorie d'observable.
Source de recherche de perceptions	Définit la source configurée pour l'intégration.
Nombre maximum d'observables par recherche	Le nombre d'observables avant que la requête de recherche ne soit fractionnée en plusieurs requêtes. Définissez cette valeur sur 500 pour cette intégration.
Rechercher	Ajoutez une chaîne de recherche native pour former une requête. Par exemple, ${observable}.
Est une recherche enregistrée	Exécute une recherche enregistrée, c'est-à-dire que le champ Nom doit correspondre au nom de la recherche enregistrée.
Actif	La requête s'exécute uniquement si l'option active est sélectionnée.

7. Cliquez sur **Enregistrer**.

Utilisation des paramètres de recherche de perceptions

Vous pouvez utiliser des paramètres de recherche de perception qui définissent des requêtes plus complexes, notamment la logique et d'autres opérateurs pris en charge par le magasin de journaux spécifié.

Afficher les paramètres de recherche de perceptions

Rôle requis : sn_sec_tisc.admin

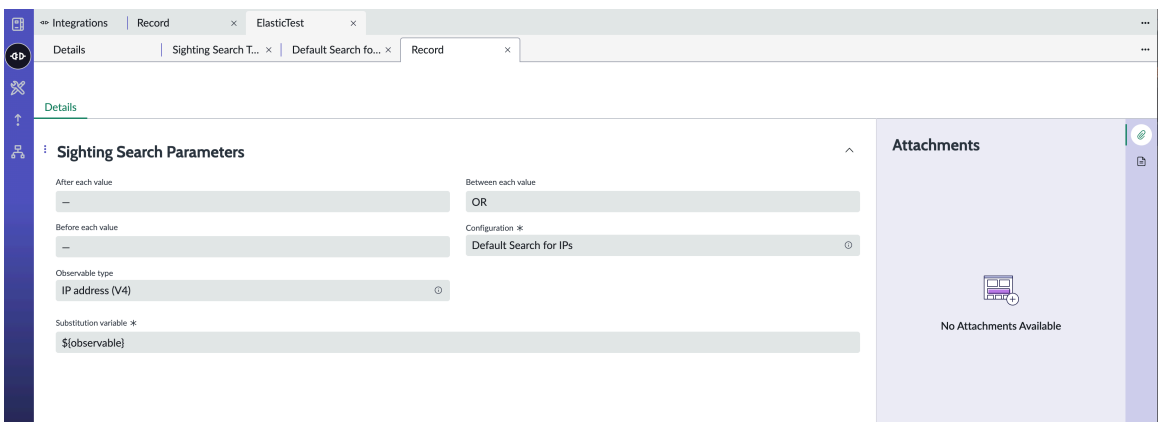
Pour afficher les paramètres de recherche de perception, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Intégrations**.
2. Sur la page Intégrations, accédez à **Intégrations de l'enrichissement** > **Recherche de perception**.
3. Recherchez l'intégration pour laquelle vous souhaitez afficher la configuration de recherche de perceptions, puis cliquez sur **Modifier**.
4. Sélectionnez l'onglet **Configurations de recherche de perceptions** .

   Vous pouvez afficher la liste des configurations de recherche de perceptions.
5. Cliquez sur la configuration de recherche de perceptions requise pour afficher les détails de la configuration.



6. Sélectionnez l'onglet **Paramètres de recherche de perception** .

   Vous pouvez afficher la liste des paramètres de recherche de perception.
7. Cliquez sur le paramètre Recherche de perception requis pour afficher les détails du paramètre.
8. Vous pouvez également effectuer les actions suivantes dans l'onglet Paramètres de recherche de perception :
   a. Pour actualiser la liste des paramètres de recherche de perception, cliquez sur l'icône .
   b. Pour effectuer une action de liste sur les paramètres de recherche de perception, cliquez sur l'icône Actions de la .

      Modifier les colonnes : vous pouvez utiliser cette action pour ajouter ou supprimer des colonnes existantes et modifier l'ordre en fonction de vos besoins.
   c. Pour filtrer les paramètres de recherche de perception en fonction des conditions, cliquez sur l'icône .

      La valeur 1 indique qu'une condition est utilisée pour le filtrage.

Créer un paramètre de recherche de perceptions

Exemple de génération de requête

```
Configured Query: ${Observable}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Observables Substitutes for Sightings search: Obs1 , Obs2

Query: {Before each Value}Obs1{After each Value}{Between each value}{Before each Value}Obs2{After each Value}

Let observables are: 172.32.31.41 & 192.168.10.12

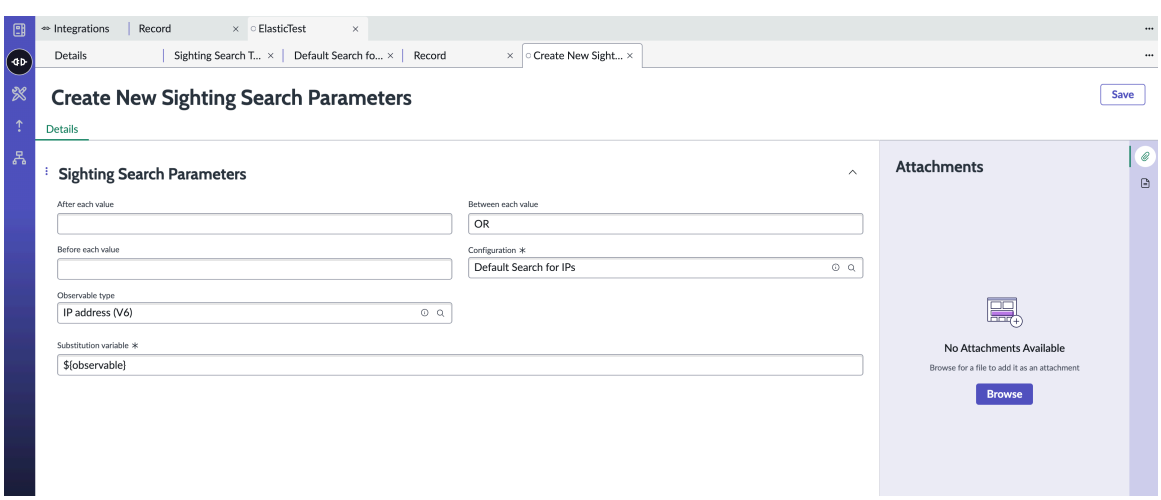
Query Formed with below configuration will be: “ip_address = 172.32.31.41 OR ip_address = 192.168.10.12”

Pour créer un paramètre de recherche de perception, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Intégrations**.
2. Sur la page Intégrations, accédez à **Intégrations de l'enrichissement** > **Recherche de perception**.
3. Recherchez l’intégration pour laquelle vous souhaitez afficher la configuration de recherche de perceptions, puis cliquez sur **Modifier**.
4. Sélectionnez l’onglet **Configurations de recherche de perceptions** .

   Vous pouvez afficher la liste des configurations de recherche de perceptions.
5. Cliquez sur la configuration de recherche de perceptions requise pour afficher les détails de la configuration.
6. Sélectionnez l’onglet **Paramètres de recherche de perception** .

   Vous pouvez afficher la liste des paramètres de recherche de perception.
7. Pour créer un paramètre de recherche de perception, cliquez sur **Nouveau**.



8. Renseignez les champs du formulaire.

Créer un paramètre de recherche de perception

Champ	Description
Après chaque valeur	Le paramètre de recherche de perception après chaque observable lorsque la requête de recherche est générée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Entre chaque valeur	Le paramètre de recherche de perception entre chaque observable lorsque la requête de recherche est générée. Par exemple, OU.
Avant chaque valeur	Le paramètre de recherche de perception avant chaque observable lorsque la requête de recherche est générée.
Configuration	Les détails de configuration du paramètre de recherche.
Type d'observable	Définit le type de catégorie d'observable.
Variable de substitution	Spécifie le nom de la variable qui est remplacée par une valeur observable.

9. Cliquez sur **Enregistrer**.

Configurer la recherche de menaces

Vous pouvez configurer la recherche de menace pour effectuer une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par Threat Intelligence, ils sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés. Vous pouvez effectuer une recherche de menace sur un ou plusieurs observables pour déterminer la malveillance d'un observable.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Remarque : Le module Intégrations de l'enrichissement s'affiche uniquement si au moins une des intégrations prenant en charge l'une des options est installée dans l'application.

Le prend Centre de sécurité des renseignements sur les menaces en charge la recherche de menace uniquement pour les intégrations suivantes :

- VirusTotal
- Renseignements sur CrowdStrike

Pour plus d'informations, consultez Recherche de menace.

Pourquoi et quand exécuter cette tâche

La section Recherche de menaces contient uniquement les intégrations avec le type d'intégration Recherche de menaces.

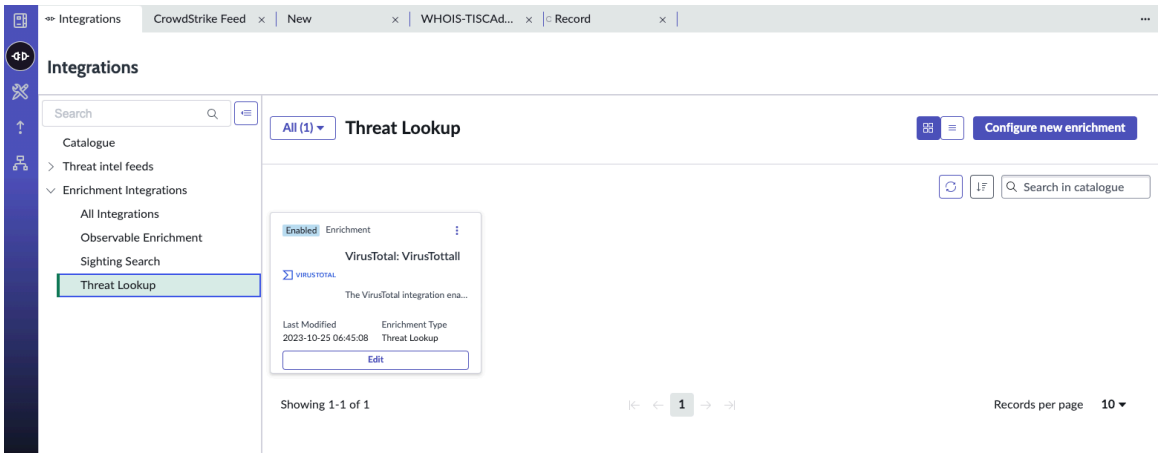
Cette section affiche les cartes pour chacune des implémentations d'intégration configurées que vous pouvez activer et utiliser.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Intégrations** , puis sélectionnez la section **Recherche de menace** .

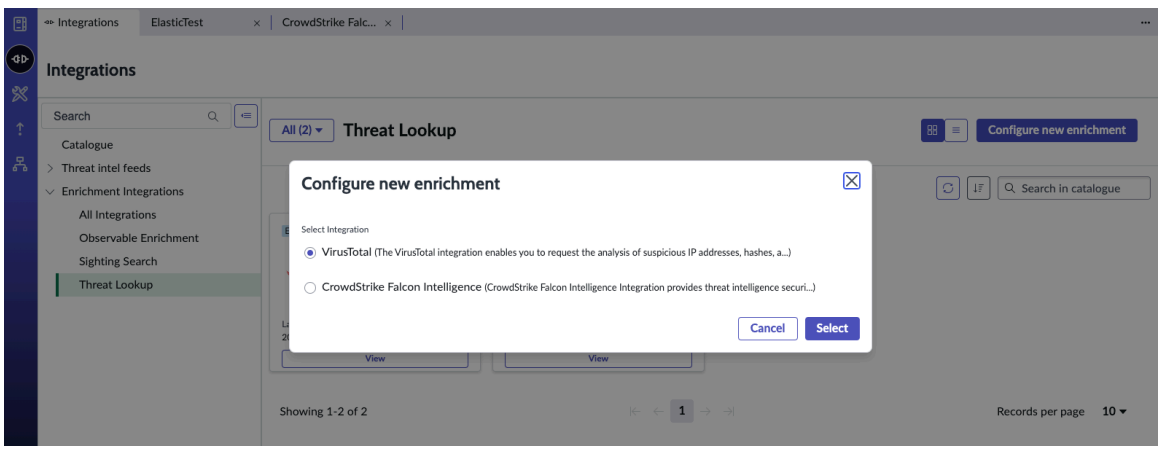
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur l'action **Configurer un nouvel enrichissement** .
   Vous accédez alors à la fenêtre contextuelle qui affiche les intégrations disponibles. Vous devez choisir l'intégration que vous devez configurer.

4. Sélectionnez une intégration dans la liste des intégrations disponibles, puis cliquez sur **Sélectionner**.
   Vous accédez alors à la page Créer une intégration d'enrichissement de l'intégration sélectionnée. Cette page est préremplie avec les détails de l'intégration sélectionnée par défaut. Par exemple, l'intégration de VirusTotal.

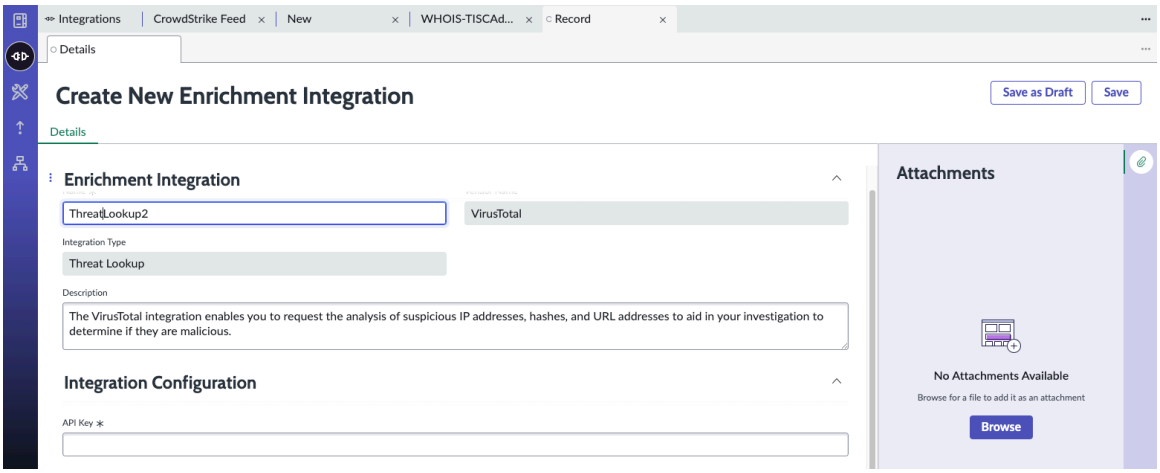


5. Renseignez les champs du formulaire Créer une intégration.

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration de l'enrichissement. Par exemple, `VirusTotal-1`.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont préremplis par défaut. Par exemple, `VirusTotal`.
Type d'intégration	Type d'intégration que vous avez sélectionné, à savoir la recherche de menace. Les détails du type d'intégration sélectionné sont préremplis par défaut.
Description	Saisissez une description unique pour la nouvelle intégration de l'enrichissement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Dans la section Configuration de l'intégration, configurez les détails de l'intégration en fonction de vos besoins.
   La section Configuration de l'intégration comprend des détails de configuration tels que la clé API, l'ID ou le secret client API, le nom d'utilisateur, le mot de passe, etc., que vous devez remplir. Ces détails de configuration varient selon les applications.
7. Cliquez sur l'action **Enregistrer** pour stocker et créer la nouvelle configuration de l'intégration de l'enrichissement.
   Les détails fournis sont validés et, par défaut, l'état de l'intégration d'enrichissement est désactivé.
8. Cliquez sur l'action **Enregistrer comme brouillon** pour stocker uniquement les mises à jour apportées à la configuration d'enrichissement et ne pas la créer.
   Si vous n'êtes pas sûr des détails de la configuration, vous pouvez utiliser l'option **Enregistrer comme brouillon** . Une fois que vous avez obtenu les détails de la configuration, vous pouvez renseigner les informations restantes dans la version brouillon et la créer.
9. Pour activer l'intégration de l'enrichissement, cliquez sur **Activer**.
   L'intégration de l'enrichissement est activée avec succès. Vous pouvez également activer, désactiver ou supprimer une intégration d'enrichissement particulière à l'aide du menu Actions de la vignette d'intégration requise sur la page Catalogue ou la page Intégrations d'enrichissement.

Afficher les calculateurs de réputation de la recherche de menace

Vous pouvez consulter le calculateur de résultat de la recherche de menace pour calculer les résultats observables pour votre intégration.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

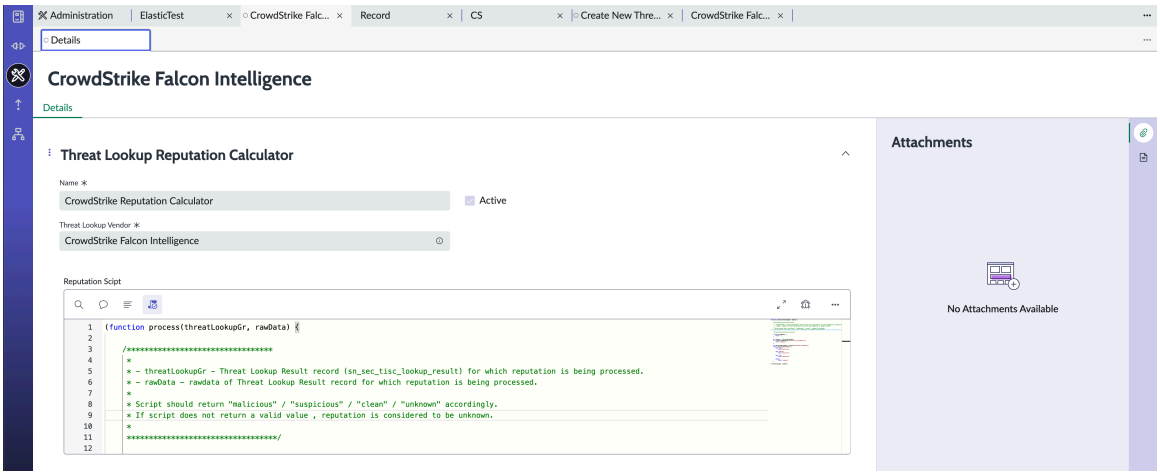
Pour en savoir plus sur les calculateurs de réputation de la recherche de menaces, reportez-vous à la section Gestion du calculateur de réputation de la recherche de menaces.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionnez la section **Calculateur de réputation de la recherche de menaces** .
   Vous pouvez consulter la liste des calculateurs de réputation de la recherche de menaces.
3. Cliquez sur le calculateur de réputation de la recherche de menaces requis pour afficher les détails du calculateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Vous pouvez également effectuer les actions suivantes dans la section Calculateur de réputation de la recherche de menaces :

   a. Pour actualiser la liste des calculateurs de réputation de la recherche de menaces, cliquez sur l'icône de .

   b. Pour effectuer une action de liste sur les calculateurs de réputation de la recherche de menace, cliquez sur l'icône Actions de la .

      Vous pouvez effectuer les deux actions de liste suivantes :

      - **Modifier les colonnes** : vous pouvez utiliser cette action pour ajouter ou supprimer des colonnes existantes et modifier l'ordre en fonction de vos besoins.
      - **Rétablir la largeur** des colonnes : vous pouvez utiliser cette action pour réinitialiser la largeur des colonnes.

   c. Pour filtrer les calculateurs de réputation de la recherche de menaces en fonction des conditions, cliquez sur l'icône .

      La valeur 1 indique qu'une condition est utilisée pour le filtrage.

Références de l'API TISC

La table suivante fournit les références des points de terminaison d'API qui facilitent les enrichissements.

API TISC

API	Description
API TISC : POST /sn_sec_tisc/threat_intel_data/observables	Cette API récupère les données des observables, y compris les relations entre les observables et d'autres données Threat Intelligence associées.
API TISC : POST /sn_sec_tisc/threat_intel_data/add_observables	Cette API ajoute des observables valides à l'application Centre de sécurité des renseignements sur les menaces (TISC) en créant des enregistrements sources d'observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations sur les points de terminaison de l'API TISC, consultez API TISC sous la section de référence de l'API REST sur l'implémentation de l'API et la référence sur les servicenow.com/docs.

Intégrations TISC

Cette section fournit des instructions pour configurer et activer les intégrations de Renseignements sur les menaces.

Enrichissement des éléments observables

Le workflow Enrichir l'observable WhoIs effectue un enrichissement sur les observables sélectionnés. Si les observables sont d'un type reconnu par l'intégration de l'API WhoisXML, les observables sont enrichis.

Remarque : Le Threat Intelligence Security Center prend en charge l'enrichissement des éléments observables uniquement pour l'intégration WHOIS.

Intégration d'identification

L'intégration Whois vous permet de soumettre des recherches Whois sur les noms de domaine et les URL afin d'obtenir un contexte sur les observables d'URL et de mieux déterminer les menaces.

Configurer et activer l'intégration Whois

Avant d'utiliser l'intégration Whois, vous devez la télécharger à partir du ServiceNow Store et disposer d'un compte valide dans Whois.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Les modules d'extension d'intégration des observables Centre de sécurité des renseignements sur les menaces et Whois sont requis.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Télécharger l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Enrichissement des éléments observables**.
6. Dans la carte **WHOIS** , cliquez sur **Configurer le nouvel enrichissement pour configurer l'intégrationWHOIS** .
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration de l'enrichissement. Par exemple, WHOIS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, WHOIS.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Entrez la description de la nouvelle intégration de l'enrichissement. Par exemple, la description de l'intégration WHOIS est la suivante : L'intégration WHOIS pour Centre de sécurité des renseignements sur les menaces permet aux utilisateurs de soumettre des recherches Whois sur les noms de domaine et les URL afin d'obtenir un contexte sur les observables d'URL et de mieux déterminer les menaces.

8. Explorez jusqu'à la section **Configuration de l'intégration** .
9. Entrez (ou collez) la **clé API** que vous avez acquise sur le site WHOIS.
10. Cliquez sur **Enregistrer**.
    Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration WHOIS est désactivé.
11. Cliquez sur **Activer** pour activer l'intégration WHOIS.

Résultats

Une fois configuré, WHOIS peut être sélectionné pour effectuer des enrichissements sur les observables dans Threat Intelligence Security Center.

Intégration Shodan

Shodan est un moteur de recherche qui analyse les informations des bannières de service à partir d'appareils connectés dans le monde entier.

L'intégration Shodan effectue un enrichissement sur les observables suivants :

- Adresses IP
- URL
- Domaines

Configurer et activer l'intégration Shodan

Avant d'utiliser l'intégration Shodan, vous devez la télécharger à partir du ServiceNow Store.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Télécharger l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Enrichissement des éléments observables**.
6. Dans la carte **Shodan** , cliquez sur **Configurer un nouvel enrichissement** pour configurer l'intégration.
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration de l'enrichissement. Par exemple, Shodan.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés automatiquement et, par défaut, ce champ est en lecture seule. Par exemple, Shodan.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Enrichissement des observables.
Description	Entrez la description de la nouvelle intégration de l'enrichissement. Par exemple, la description de l'intégration Shodan est la suivante : Shodan vous aide à analyser les informations de bannière à partir d'appareils connectés dans le monde entier.

8. Explorez jusqu'à la section **Configuration de l'intégration** .
9. Entrez (ou collez) la **clé API** que vous avez acquise à partir du portail Shodan.
10. Cliquez sur **Enregistrer**.
    Les détails de l'intégration sont validés et, par défaut, l'état est désactivé.
11. Cliquez sur **Activer** pour activer l'intégration.

Recherche de perception

Cette section décrit les intégrations Recherche de perception TISC et Recherche élastique.

Introduction à l'intégration Elasticsearch

L'intégration d'enrichissement Elasticsearch recherche vos journaux et ajoute des informations de perception pertinentes à vos observables.

Configurer et activer l'intégration Elasticsearch

Elasticsearch est un moteur de recherche et d'analyse RESTful distribué qui s'intègre facilement à Security Operations.

Avant de commencer

Avant de pouvoir utiliser Elasticsearch, vous devez le télécharger à partir du ServiceNow Store.

Rôle requis : sn_sec_tisc.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le module d'extension Centre de sécurité des renseignements sur les menaces doit être installé et activé avant de pouvoir utiliser l'intégration Elasticsearch.
- Obtenez l'URL de base de l'API Elasticsearch, l'URL de base Kibana, le nom d'utilisateur et le mot de passe sous votre profil Elasticsearch.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Télécharger l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Recherche de perception**

   Remarque : Les intégrations configurées apparaissent sous la forme d'une série de cartes.

6. Dans la carte **Elasticsearch** , cliquez sur **Configurer un nouvel enrichissement pour configurer l'intégrationElasticsearch** .
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la configuration de recherche de perceptions.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, Elasticsearch.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Saisissez la description de l'intégration Elasticsearch. Par exemple, l'intégration d'enrichissement Elasticsearch facilite l'enquête d'un observable en prenant en charge l'interrogation des journaux dans votre déploiement Elasticsearch.
Configuration de l'intégration	
URL de base de l'API Elasticsearch	URL de base que vous avez acquise sur le site Elasticsearch.
URL de base Kibana	L'URL de base Kibana. [Facultatif] Liens vers une instance Kibana, le cas échéant.
Nom d'utilisateur	Votre nom d'utilisateur Intel Elasticsearch.
Mot de passe	Votre mot de passe Intel Elasticsearch.
Index Elasticsearch	Index Elasticsearch. Ceux-ci contiendront à leur tour des documents uniques à chaque index. Les index sont identifiés par des noms en minuscules qui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	font référence aux actions effectuées (telles que la recherche et la suppression).
Champ de plage de dates	Horodatage de la configuration.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend de votre paramètre dans la propriété nombre de lignes de données brutes dans les propriétés de Réponse aux incidents de sécurité .
Serveur MID	Sélectionnez N'importe lequel pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à l'éditeur de workflow.

8. Cliquez sur **Enregistrer**.
   Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration Elasticsearch est désactivé.
9. Cliquez sur **Activer** pour activer l'intégration Elasticsearch.

Résultats
Une fois configuré, Elasticsearch peut être sélectionné pour effectuer une recherche de perception sur les observables dans Centre de sécurité des renseignements sur les menaces.

Introduction à l'intégration de Recherche Splunk

Le logiciel Splunk recherche, surveille et analyse les données volumineuses générées par les machines et s'intègre facilement à Security Operations. Avant de pouvoir utiliser l'intégration de recherche d'observations Splunk, vous devez la télécharger à partir du ServiceNow Store.

Configurer et activer l'intégration Splunk

L'intégration d'enrichissement de Splunk recherche vos journaux et ajoute des informations de perception pertinentes.

Avant de commencer
Avant de pouvoir utiliser la recherche Splunk, vous devez la télécharger à partir du ServiceNow Store.

Rôle requis : sn_sec_tisc.admin

- Le module d'extension Centre de sécurité des renseignements sur les menaces doit être installé et activé avant de pouvoir utiliser l'intégration de recherche Splunk.
- Obtenez Splunk et obtenez la recherche Splunk et obtenez l'URL de base de l'API, l'URL de lien, le nom d'utilisateur et le mot de passe à partir de votre instance Splunk.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Télécharger l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Recherche de perception**
   Les intégrations configurées apparaissent sous la forme d'une série de cartes.
6. Dans la carte **de recherche Splunk** , cliquez sur **Configurer un nouvel enrichissement pour configurer l'intégration dela recherche Splunk** .
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la configuration de recherche de perceptions.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, Splunk.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Saisissez la description de l'intégration Splunk. Par exemple, l'intégration d'enrichissement de Splunk facilite l'enquête d'un observable en prenant en charge l'interrogation des journaux dans votre déploiement Splunk en ce qui concerne les indicateurs potentiellement malveillants.
Configuration de l'intégration	
URL de Base de l'API Splunk	URL de base que vous avez acquise sur le site Splunk.
URL de lien	[Facultatif] L'URL de lien qui renvoie à l'interface Web de Splunk, le cas échéant.
Nom d'utilisateur	Votre nom d'utilisateur Intel Elasticsearch.
Mot de passe	Votre mot de passe Intel Elasticsearch.
Lignes max.	Le nombre maximal de lignes que vous souhaitez rechercher.
Tout premier résultat (jours)	Les résultats les plus récents que vous souhaitez voir, en nombre de jours.
Inclure les exemples de données brutes dans les résultats de recherche	Sélectionnez cette option pour inclure des exemples de données brutes dans vos résultats de recherche d'observations. La quantité de données renvoyées dépend de votre paramètre dans la propriété nombre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	de lignes de données brutes dans les propriétés de Réponse aux incidents de sécurité .
Déploiement sur site	L'environnement déployé sur site.
Serveur MID	Sélectionnez N'importe lequel pour utiliser n'importe quel serveur MID actif ou sélectionnez un nom de serveur MID spécifique.

Remarque : La configuration de cette intégration active les workflows. Pour gérer les workflows, accédez à l'éditeur de workflow.

8. Cliquez sur **Enregistrer**.
   Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration Splunk est désactivé.
9. Cliquez sur **Activer** pour activer l'intégration Splunk.

Résultats
Une fois configuré, Splunk peut être sélectionné pour effectuer une recherche de perception sur les observables dans Centre de sécurité des renseignements sur les menaces.

Recherche de menace

Le workflow Recherche de menace - VirusTotal et CrowdStrike Falcon Intelligence effectue une recherche sur les observables sélectionnés. Si les observables sont d'un type reconnu par VirusTotal et CrowdStrike, ils sont analysés à la recherche de programmes malveillants et les résultats sont renvoyés.

Intégration TISC VirusTotal

L'intégration de TISC VirusTotal vous permet de demander l'analyse des adresses IP, des hachages de fichiers et des adresses URL suspects afin d'aider à déterminer s'ils sont malveillants.

Configurer et activer l'intégration de VirusTotal

Avant de pouvoir utiliser l'intégration de VirusTotal, vous devez la télécharger à partir du ServiceNow Store.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Le module d'extension Centre de sécurité des renseignements sur les menaces est requis pour activer l'intégration de VirusTotal.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Télécharger l'intégration à partir de ServiceNow Store.
3. Une fois l'installation terminée, accédez à VirusTotal et obtenez la clé API sous votre profil VirusTotal.
4. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
5. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
6. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Recherche de menace**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Configurer le nouvel enrichissement pour configurer l'intégrationde VirusTotal** .
8. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration de l'enrichissement. Par exemple, VirusTotal.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, VirusTotal.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Entrez la description de la nouvelle intégration de l'enrichissement.

9. Explorez jusqu'à la section **Configuration de l'intégration** .
10. Saisissez (ou collez) la **clé API** que vous avez acquise sur le site VirusTotal.
11. Cliquez sur **Enregistrer**.
    Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration de VirusTotal est désactivé.
12. Cliquez sur **Activer** pour activer l'intégration de VirusTotal.

Résultats

Une fois configuré, VirusTotal peut être sélectionné pour effectuer des recherches sur les observables dans Centre de sécurité des renseignements sur les menaces.

Intégration TISC CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence fournit des renseignements de cybersécurité qui s'intègrent facilement à Security Operations.

Remarque :

Le module d'extension Centre de sécurité des renseignements sur les menaces est requis pour implémenter l'intégration de CrowdStrike Falcon Intelligence.

Configurer et activer l'intégration de CrowdStrike Falcon Intelligence

Avant de pouvoir utiliser CrowdStrike Falcon Intelligence, vous devez le télécharger à partir du ServiceNow Store et y ajouter l'ID client et le secret client appropriés.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

- L'application Centre de sécurité des renseignements sur les menaces doit être installée et activée.
- Obtenez l'ID et le secret du client API sous votre profil CrowdStrike Falcon Intelligence.
- Dans les champs d'application de l'API du portail CrowdStrike Falcon Intelligence, activez le paramètre Lecture pour les indicateurs (Falcon Intelligence).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Télécharger l'intégration à partir de ServiceNow Store.
3. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
4. Sélectionner **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations**.
5. Vous pouvez également accéder à **Intégrations** > **Intégrations de l'enrichissement** > **Toutes les intégrations** > **Recherche de menace**.
6. Cliquez sur **Configurer le nouvel enrichissement** pour configurer l'intégration **de CrowdStrike Falcon Intelligence** .
7. Renseignez les champs du formulaire Configurer un nouvel enrichissement.

Intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration de l'enrichissement. Par exemple, CrowdStrike Falcon Intelligence.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, CrowdStrike Falcon Intelligence.
Type d'intégration	Type d'intégration que vous avez sélectionné. Par exemple, Recherche de menace.
Description	Entrez la description de la nouvelle intégration de l'enrichissement.
Configuration de l'intégration	
ID client	L'ID client que vous avez obtenu de CrowdStrike.
Secret client	Clé secrète du client que vous avez obtenue auprès de CrowdStrike.

8. Cliquez sur **Enregistrer**.
   Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration de CrowdStrike Falcon Intelligence est désactivé.
9. Cliquez sur **Activer** pour activer l'intégration de CrowdStrike Falcon Intelligence.

Résultats

Une fois configuré, CrowdStrike Falcon Intelligence peut être sélectionné pour effectuer des recherches sur les observables dans Centre de sécurité des renseignements sur les menaces.

Outils de sécurité TISC - EDR

Les intégrations EDR (Endpoint Detection and Response) TISC se concentrent sur l'identification et le traitement des menaces de sécurité au niveau du point de terminaison.

Les solutions réseau EDR prédisent et anticipent les menaces émergentes et contribuent à améliorer la posture de sécurité globale de l'organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En s'intégrant à d'autres outils de sécurité tels que l'EDR, TISC permet une surveillance proactive des menaces sur les points de terminaison et améliore ainsi la posture de sécurité globale et la résilience face à l'évolution des menaces.

Information associée

CrowdStrike Intégration de Falcon EDR

CrowdStrike Intégration de Falcon EDR

L'intégration à CrowdStrike Falcon EDR permet une surveillance continue et des alertes en temps réel basées sur les informations de TISC.

Cette intégration peut aider à rationaliser les opérations de sécurité et à réduire tout risque potentiel pour les activités de l'organisation.

Configurer l'intégration EDR Crowdstrike Falcon

Avant de pouvoir utiliser l'intégration CrowdStrike EDR Falcon, vous devez la télécharger à partir de la ServiceNow Store boutique et y ajouter l'ID client et le secret client appropriés.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

- L'application Centre de sécurité des renseignements sur les menaces doit être installée et activée.
- Obtenez l'ID du client API et le secret du client API à partir de CrowdStrike la console Falcon.
- Dans les champs d'application de l'API CrowdStrike du portail Falcon, activez **l'accès en lecture et en écriture à la gestion IOC**.

Procédure

1. À l'aide de votre instance, accédez au **Centre de sécurité des renseignements sur les menaces**.
2. Télécharger l'intégration à partir de ServiceNow Store.
3. Sélectionner **Intégrations** > **Outils de Security** > **EDR**.
4. Cliquez sur **Configurer le nouvel outil de sécurité** pour configurer CrowdStrike l'intégration EDR Falcon.
5. Sélectionnez l'option **EDR CrowdStrike Falcon** .
6. Renseignez les champs du formulaire Configurer le nouvel outil de Security.

Créer une intégration de l'enrichissement

Champ	Description
Nom	Entrez un nom pour la nouvelle intégration de l'outil de Security. Par exemple, CrowdStrike Falcon EDR.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut. Par exemple, CrowdStrike Falcon EDR.
Description	Saisissez la description de la nouvelle intégration de l'outil de Security.
Type d'intégration	Option qui affiche le type d'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Catégorie d'intégration	Option qui affiche la catégorie d'intégration.
Configuration de l'intégration	
URL de base	L'URL de base est l'URL de base de l'API CrowdStrike. La valeur par défaut est https://api.crowdstrike.com . Pour plus d'informations, voir https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis#k9578c40
ID client	ID client que vous avez obtenu auprès de CrowdStrike. Pour plus d'informations, consultez https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis .
Secret client	Clé secrète du client que vous avez obtenue auprès de CrowdStrike. Pour plus d'informations, consultez https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis .
Période d'expiration en jours pour tout type d'observables	Période d'expiration, en jours, qui est appliquée à tout type d'observable lorsqu'ils sont envoyés à CrowdStrike EDR. **Remarque :** Cette option est une période d'expiration de secours lorsque le délai d'expiration n'est défini pour aucun type d'observable spécifique.
Délai d'expiration de l'observable IP	La période d'expiration en jours qui est appliquée au type d'adresse IP de l'observable lorsqu'il est envoyé à CrowdStrike EDR.
Délai d'expiration de l'observable du domaine	La période d'expiration, en jours, qui est appliquée au type de domaine des observables lorsqu'ils sont envoyés à CrowdStrike EDR.
Délai d'expiration de l'observable de hachage	Période d'expiration, en jours, qui est appliquée au type de hachage de l'observable lorsqu'il est envoyé à CrowdStrike EDR.

7. Cliquez sur **Enregistrer**.
   Les détails de l'intégration sont validés et, par défaut, l'état de l'intégration CrowdStrike EDR est désactivé.
8. Cliquez sur **Activer** pour activer l'intégration CrowdStrike EDR.

Remarque : Plusieurs configurations sont autorisées pour CrowdStrike l'intégration de Falcon EDR.

Envoyer des observables à EDR

Envoyez des observables à l'outil de sécurité EDR.

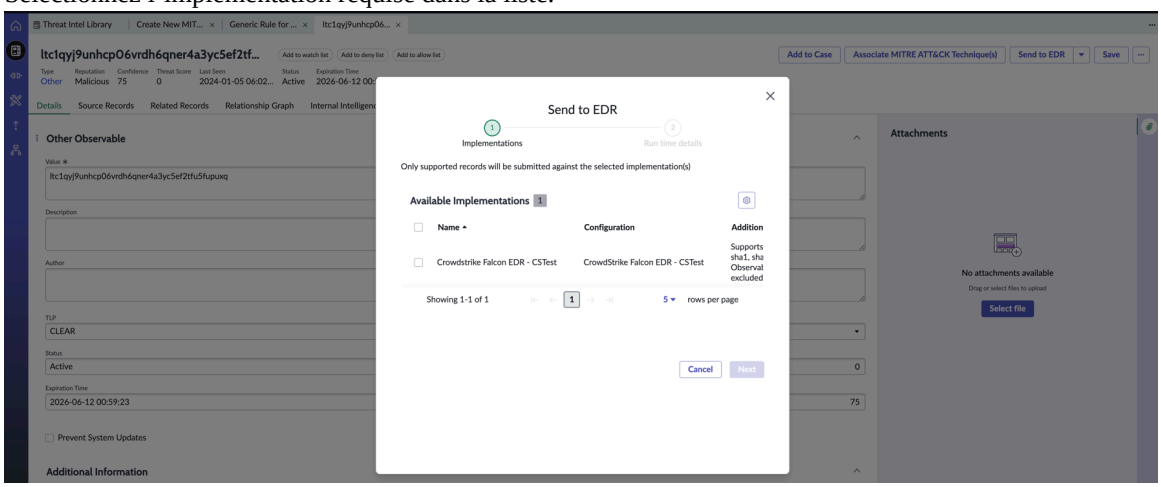
Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

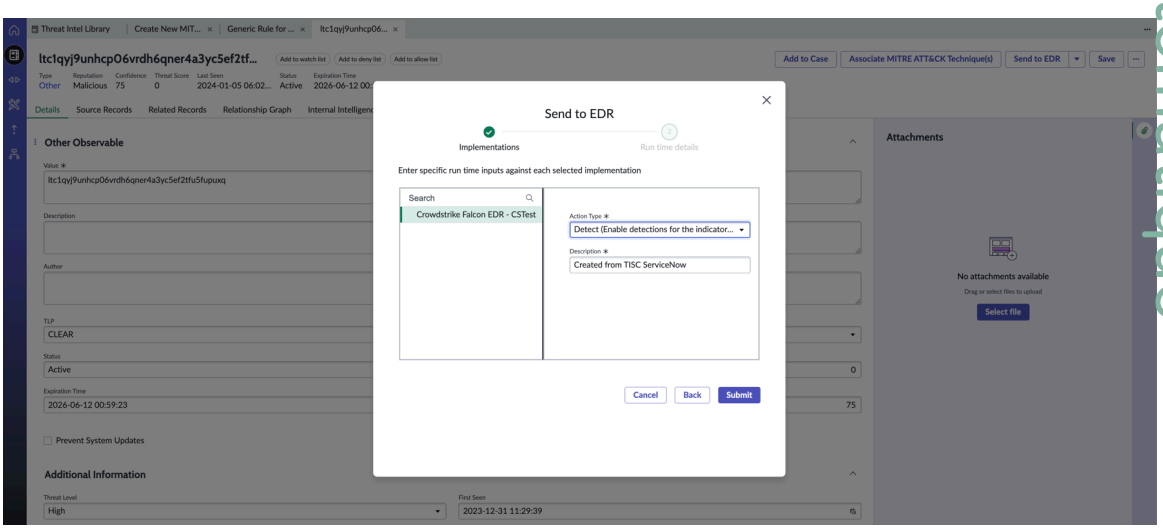
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Sélectionnez **Envoyer à EDR**.
   L'écran modal Envoyer aux **implémentations EDR** s'affiche.
6. Sélectionnez l'implémentation requise dans la liste.



7. Cliquez sur **Suivant**.
8. Sélectionnez les détails de la durée d'exécution, tels que le **type d'action** et la **description** de l'implémentation.



Les options disponibles pour les détails de la durée d'exécution de l'implémentation CrowdStrike sont les suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Aucune action (enregistrez l'indicateur pour une utilisation ultérieure, mais n'effectuez aucune action)** : dans la vue de formulaire Observable, la gravité de menace de l'observable est facultative pour CrowdStrike Falcon EDR.
- **Détecter (activer les détections pour l'indicateur au niveau de gravité de la menace de l'enregistrement)** : dans la vue de formulaire Observable, la gravité de la menace est obligatoire pour CrowdStrike Falcon EDR. La gravité de la menace de l'observable ne doit pas être vide pour cet observable sélectionné.

9. Cliquez sur **Envoyer**.
   L'action sélectionnée est exécutée et un message d'information s'affiche indiquant que l'exécution de l'envoi observable à EDR a commencé.

Remarque :

- Une fois l'exécution lancée ou terminée, une note de travail est publiée sur le flux d'activité de la vue de formulaire.
- **L'action Envoyer à EDR** est également disponible dans la liste des observables sous l'onglet Artefacts pour un enregistrement **de** ticket. Pour plus d'informations, consultez Ajouter des artefacts aux tickets ou aux tâches de ticket.

Intégration de Microsoft Defender pour EDR

L'intégration avec Microsoft Defender pour EDR permet aux analystes de Renseignements sur les cybermenaces (CTI) d'envoyer automatiquement les adresses IP, les domaines, les hachages de fichiers et les URL malveillants ou suspects à Microsoft Defender pour une surveillance continue et des alertes en temps réel.

Inscrire et configurer Microsoft Defender dans le Microsoft Azure portail

Enregistrez Microsoft Defender EDR dans le Microsoft Azure portail et accordez l'accès en lecture et en écriture à l'application.

Avant de commencer

Rôle requis : développeur d'application, administrateur de locataire.

Procédure

1. Connectez-vous au portail Microsoft Azure.
2. Entrez les inscriptions d'applications dans la zone de recherche, puis cliquez **sur Cliquez sur Nouvelle inscription**.
3. Saisissez un nom pour votre application et l'URI de redirection, puis cliquez sur **Enregistrer**.
   Un exemple de nom est Microsoft Defender pour point de terminaison. L'URI de redirection est utilisé lors de la fourniture du consentement de l'administrateur pour l'application.
4. Sur la page **Inscriptions d'applications** , sélectionnez l'application que vous avez enregistrée à l'étape 3.
5. Sous Gérer, sélectionnez **Certificats et secrets**.
6. Pour créer un secret client, sélectionnez **Nouveau secret client**.
7. Copiez le secret client et enregistrez-le.

   Si vous avez oublié le secret client, vous pouvez générer un nouveau secret client.

8. Accédez à la **Gérer** > **Autorisations d'API**.
9. Cliquez sur **Ajouter une autorisation**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Dans la fenêtre Autorisations de l'API de demande, cliquez sur l'onglet **API utilisées par mon organisation** .
11. Recherchez et sélectionnez **WindowsDefenderATP**.
12. Dans les autorisations WindowsDefenderATP, sélectionnez **Autorisations d'application**.
    L'activation de cette autorisation garantit que l'application s'exécute en tant que service d'arrière-plan ou démon sans utilisateur connecté.
13. Ajoutez l'autorisation au niveau de l'application suivante et accordez le consentement administrateur pour l'autorisation d'API nouvellement ajoutée.

Autorisation	Nom d'affichage de l'autorisation
Ti.ReadWrite.All	Indicateurs de lecture et d'écriture

Installer et configurer l'intégration de Microsoft Defender pour EDR

Installez et configurez l'intégration de Microsoft Defender pour EDR à partir du ServiceNow Store.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

- Centre de sécurité des renseignements sur les menaces L'application doit être installée et activée à partir de ServiceNow Store.
- Obtenez l'ID du locataire de l'API, l'ID client et le secret client à partir de la console Microsoft Defender pour EDR.

Procédure

1. Téléchargez l'intégration de Microsoft Defender pour PEPT à partir du ServiceNow Store et installez-la.
2. À l'aide de votre instance, accédez à *`Centre de sécurité des renseignements sur les menaces`*.
3. Télécharger l'intégration à partir de ServiceNow Store.
4. Sélectionner **Intégrations** > **Outils de Security** > **EDR**.
5. Cliquez sur **Configurer l'intégration d'un nouvel outil source**.
6. Sélectionnez **l'option Microsoft Defender pour EDR** .
7. Cliquez sur **Sélectionner**.
8. Renseignez les champs suivants du formulaire.

Configurer l'intégration de Microsoft Defender pour EDR

Champ	Description
Nom	Nom de la nouvelle configuration de l'intégration de l'outil de Security. Par exemple, l'intégration de Microsoft Defender pour EDR.
Catégorie d'intégration	Option qui affiche la catégorie d'intégration.
Nom du fournisseur	Nom du fournisseur. Les détails du fournisseur sélectionné sont renseignés par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type d'intégration	Option qui affiche le type d’intégration.
Description	Saisissez la description de la nouvelle configuration d’intégration de l’outil de Security.
Configuration de l’intégration	
URL de base	L’URL de base est l’URL de base de l’API Microsoft Defender pour EDR. La valeur par défaut est https://api.securitycenter.microsoft.com/ .
ID de locataire	L’ID de locataire que vous avez obtenu de Microsoft Defender.
ID client	L’ID client que vous avez obtenu à partir de Microsoft Defender.
Secret client	Clé secrète du client que vous avez obtenue à partir de Microsoft Defender.
Titre prérempli (utilisé lors de la soumission)	Le titre prérempli définit le titre par défaut utilisé lors de la soumission d’observables à Microsoft Defender. Ces détails sont affichés par défaut, vous n’avez donc pas besoin de les saisir à nouveau chaque fois que vous les soumettez à EDR.
Description préremplie (utilisée lors de la soumission)	La description préremplie définit le titre par défaut utilisé lors de la soumission d’observables à Microsoft Defender. Ces détails sont affichés par défaut, vous n’avez donc pas besoin de les saisir à nouveau chaque fois que vous les soumettez à EDR.
Période d’expiration en jours pour tout type d’observables	La période d’expiration en jours qui est appliquée pour le ou les observables lorsqu’ils sont envoyés à Microsoft Defender EDR. **Remarque :** Cette option est une période d’expiration de secours lorsque le délai d’expiration n’est défini pour aucun type d’observable spécifique.
Période d’expiration en jours pour le type IP des observables	La période d’expiration en jours qui est appliquée au type d’adresse IP de l’observable lorsqu’il est envoyé à Microsoft Defender EDR.
Période d’expiration en jours pour le type de domaine des observables	La période d’expiration, en jours, qui est appliquée au type de domaine des observables lorsqu’ils sont envoyés à Microsoft Defender EDR.
Période d’expiration en jours pour le type de hachage des observables	La période d’expiration en jours qui est appliquée au type de hachage des observables lorsqu’ils sont envoyés à Microsoft Defender EDR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Cliquez sur **Enregistrer** après avoir ajouté les informations de configuration nécessaires.
10. Cliquez sur **Activer** pour activer la configuration, après avoir enregistré la nouvelle intégration EDR de Microsoft Defender.
    Un message de confirmation s'affiche pour indiquer que l'intégration de l'enrichissement est activée.

Résultats

Une fois l'intégration configurée, vous pouvez sélectionner n'importe quel type d'observable qui prend en charge Microsoft Defender EDR à partir de la bibliothèque Renseignements sur les menaces. Vous pouvez ensuite envoyer des observables à EDR. Pour plus d'informations, consultez Envoyer des observables à EDR.

Propriétés système de Microsoft Defender EDR

Ce qui suit détaille les propriétés système de Microsoft Defender EDR.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tous** > **Catalogue de propriétés Glide** > **Propriétés Glide**.
2. Recherchez les propriétés de Microsoft Defender.

Propriété	Description
sn_tisc_defender.rate_limiter.minute	Cela permet aux utilisateurs de limiter le taux d'envoi d'EDR à MS Defender sur une base infime. ○ Type : entier ○ Valeur : 100
sn_tisc_defender.rate_limiter.hour	Cela permet aux utilisateurs de limiter le taux d'envoi d'EDR à MS Defender sur une base horaire. ○ Type : entier ○ Valeur : 1500

Envoyer des observables à EDR

Envoyez des observables à l'outil de sécurité EDR.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Sélectionnez **Envoyer à EDR**.
   L'écran modal Envoyer aux **implémentations EDR** s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez l'implémentation requise dans la liste.
   Par exemple, sélectionnez l'implémentation associée à Microsoft Defender EDR.
7. Cliquez sur **Suivant**.
8. Sélectionnez les détails de la durée d'exécution tels que le **titre** et la **description** de l'implémentation.
9. Cliquez sur **Envoyer**.
   L'action sélectionnée est exécutée et un message d'information s'affiche indiquant que l'exécution de l'envoi observable à EDR a commencé et que les résultats de cette exécution seront disponibles sous le flux d'activité une fois l'exécution terminée.

Remarque : Une fois l'exécution lancée ou terminée, une note de travail est publiée dans le flux d'activité de la vue de formulaire et vous pouvez vérifier la progression de l'exécution en conséquence.

Outils de sécurité TISC : pare-feu

Outils de sécurité TISC - Le pare-feu empêche tout accès non autorisé au réseau. L'intégration de Palo Alto à TISC permet de bloquer les adresses IP, les URL et les domaines malveillants à l'aide des options de liste dynamique externe (EDL) avec ServiceNow les données Threat Intelligence.

Dans TISC, en s'intégrant à d'autres outils de sécurité tels que Palo Alto Networks l'amélioration de la sécurité réseau globale de l'organisation.

Intégration Palo Alto Networks

Une fois configurée, l'intégration de Palo Alto Networks permet à l'analyste de menaces d'ajouter des adresses IP, des URL et des domaines malveillants à la liste dynamique externe (EDL) ou de supprimer ces entrées de l'EDL une fois qu'il a été confirmé qu'elles ne sont pas malveillantes ou qu'elles sont propres.

Une EDL est un fichier texte hébergé sur un serveur Web externe. Pour cette intégration, ce serveur Web est votre ServiceNow AI Platform instance, ce qui permet au pare-feu Palo Alto Networks d'importer des objets inclus dans la liste, les adresses IP, les URL et les domaines.

Créer une nouvelle EDL pour Palo Alto Networks

Créer une nouvelle liste dynamique externe (EDL) pour Palo Alto Networks. Une fois que vous avez créé des EDL, vous pouvez commencer à créer des entrées pour ces EDL.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Après avoir enregistré la configuration Palo Alto NGFW nouvellement configurée, accédez à **la section EDL** .
2. Cliquez sur **Nouveau** pour créer une nouvelle liste dynamique externe (EDL).
3. Remplissez les champs du formulaire.

Formulaire de liste dynamique externe de pare-feu Palo Alto Networks

Champ	Description
Nom	Nom de la liste dynamique de pare-feu Palo Alto Networks.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type d'observable	Sélectionnez un type d’observable que cette EDL accepte dans la liste de choix : adresse IP (y compris CIDR), URL ou domaine.
Période d'expiration (jours)	Période d’expiration de l’EDL. 0 (valeur par défaut) indique que l’entrée EDL n’expire jamais. Si vous modifiez cette valeur, cette entrée est active pendant le nombre de jours que vous saisissez. Vous pouvez entrer une valeur minimale de 1, mais il n’y a pas de valeur maximale. Par exemple, si vous saisissez 30 jours à 14h01 le 1er novembre, l’EDL expirera à 14h01 le 30 novembre. Toutes les entrées de cette EDL héritent alors de cette valeur par défaut, sauf si vous remplacez la valeur sur une base individuelle.
Création d'une demande de changement	Cette case à cocher est sélectionnée par défaut pour créer automatiquement une demande de changement et des tâches de changement dans votre ServiceNow AI Platform instance, qui sont jointes à l’enregistrement EDL. La demande de changement est utilisée pour configurer l’URL de récupération de la liste des EDL dans le serveur de pare-feu de nouvelle génération de Palo Alto Networks. Cette option est recommandée si votre administrateur de pare-feu utilise également le pour modifier la politique ou les règles du ServiceNow AI Platform pare-feu. Si vous créez une demande, une fois qu’elle est fermée, la liste EDL est automatiquement activée.
Description	Description de la liste dynamique du pare-feu Palo Alto Networks. Le nom contient généralement les types de sites et d’observables que vous vous attendez à trouver sur cette EDL, et vous pouvez utiliser ce champ pour plus de détails.
Demande de changement	Lorsque la case Créer une demande de changement est cochée, le numéro de la demande de changement s’affiche sur l’instance ServiceNow AI Platform une fois l’EDL enregistrée. Lorsque la case à cocher **Créer une demande de changement** est désactivée, ce champ n’apparaît pas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Combiner les adresses IP et les adresses de sous-réseau en une seule entrée	Option permettant de combiner les adresses IP et les adresses de sous-réseau en une seule entrée. Lorsque vous cochez cette case et si l'adresse IP de type CIDR est ajoutée, les entrées existantes se trouvant dans la plage CIDR sont automatiquement supprimées. Par exemple : s'il existe une entrée dans EDL avec la valeur 192.168.1.1, et si une valeur CIDR de 192.168.1.0/24 est ajoutée à la même EDL, l'entrée d'adresse IP initiale sera supprimée, car elle se trouve dans la plage CIDR de la nouvelle entrée. **Remarque :** cette option n'est affichée que lorsque vous sélectionnez le **type d'observable** IP.
URL de récupération de l'EDL	Le lien URL que l'administrateur du pare-feu Palo Alto Networks utilise pour la configuration dans le pare-feu Palo Alto Networks est automatiquement généré et affiché.

4. Créez et ajoutez d'autres EDL selon vos besoins.
   Les EDL sont affichées dans la liste des listes dynamiques externes de Palo Alto Networks.

Information associée

Règles d'approbation de l'EDL Palo Alto

Règles d'approbation de l'EDL Palo Alto

Les règles d'approbation permettent aux utilisateurs d'activer le workflow d'approbation requis pour approuver ou rejeter les entrées EDL.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche

L'administrateur TISC définit ces règles d'approbation pour accorder le consentement sur les demandes d'approbation. En tant qu'administrateur TISC, vous pouvez également définir plusieurs niveaux d'approbation à partir d'ici.

Procédure

1. Après avoir enregistré la configuration Palo Alto NGFW nouvellement configurée, accédez à **la section Règles d'approbation de l'EDL** .
2. Cliquez sur **Nouveau** pour créer une règle d'approbation.
   Les règles suivantes sont les règles préconfigurées dans le système de base pour l'intégration Palo Alto NGFW.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles d’approbation de l’EDL préconfigurées

Nom	Description	Action de l'EDL
Règle d’approbation pour l’ajout à l’EDL	Cette règle d’approbation permet aux utilisateurs d’activer le workflow d’approbation pour l’ajout d’entrées à l’EDL.	Ajouter à l'EDL
Règle d’approbation pour la suppression de l’EDL	Cette règle d’approbation permet aux utilisateurs d’activer le workflow d’approbation pour la suppression d’entrées de l’EDL.	Supprimer de l'EDL

3. Renseignez les champs du formulaire comme il convient.

Créer des règles d’approbation de l’EDL

Champ	Description
Nom	Nom de la règle d’approbation.
Action de l'EDL	Option permettant d’ajouter ou de supprimer l’entrée EDL.
EDL	Sélectionnez les EDL qui nécessitent une approbation. Si vous laissez ce champ vide, il inclura toutes les EDL.
Description	Entrez la description de la règle d’approbation.
Sélectionner un utilisateur ou des groupes nécessitant une approbation	
Utilisateur(s)	Sélectionnez le ou les utilisateurs qui nécessitent une approbation.
Groupe(s)	Sélectionnez le ou les groupes qui nécessitent une approbation.
Sélectionner approbateur(s)	
Utilisateur(s)	Sélectionnez le ou les utilisateurs pour approbation.
Groupe(s)	Sélectionnez le(s) groupe(s) pour approbation.
Notifications	
Notifier le demandeur de l'approbation	Cochez cette case pour notifier le demandeur de l’approbation des EDL.
Notifier le demandeur du rejet	Cochez cette case pour notifier le demandeur du rejet d’EDL.

4. Cliquez sur **Enregistrer** pour valider et enregistrer la règle d’approbation.
5. Cliquez sur **Activer** pour activer la règle d’approbation.

Ajouter des observables à l’EDL

Ajoutez des observables tels que des adresses IP, des domaines et des hachages à la liste dynamique externe (EDL).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Cliquez sur **Ajouter à l'EDL.**
   L'écran modal Add to EDL (Ajouter à EDL) s'affiche.

Supprimer les observables de l'EDL

Supprimez les observables de l'EDL.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Cliquez sur **Supprimer de l'EDL.**
   L'écran modal Supprimer de l'EDL s'affiche.

Approuver les entrées EDL pour Palo Alto Networks

L'approbation des entrées de liste dynamique externe (EDL) fait partie de la préconfiguration. Vous devez approuver les entrées EDL avant qu'elles ne soient activées sur les EDL pour que le pare-feu récupère l'entrée et applique la politique de sécurité.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche
Lorsque le processus d'approbation est activé, une entrée EDL n'est pas activée ou désactivée sur l'EDL tant qu'elle n'est pas approuvée.

Procédure

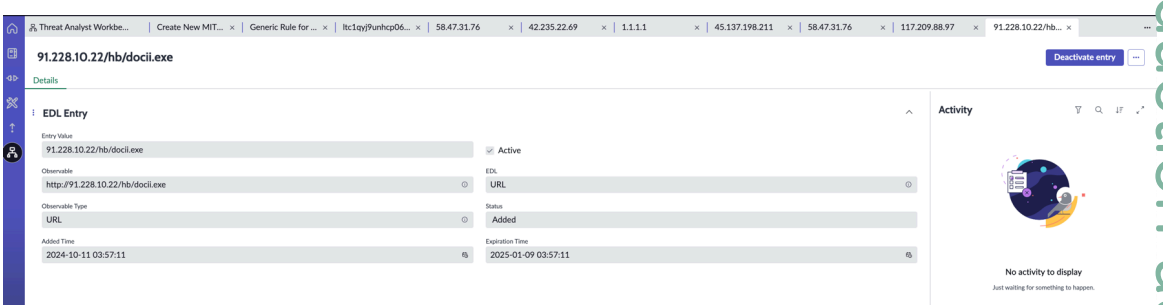
1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Console d'analyste de menaces**.
2. Explorez la section **PAN NGFW** et sélectionnez l'enregistrement EDL pour approbation.
3. Accédez à **Mes approbations**.
4. Sélectionnez le ou les enregistrements EDL pour approbation.
5. Cliquez sur **Approuver**.
6. Sous **Mes demandes d'approbation** , cliquez sur un élément dans la colonne **État** pour l'ouvrir.
7. Choisissez l'option d'approbation de l'entrée EDL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Approuver	Sur l'enregistrement d'entrée, le champ **État** bascule sur Ajouté et la case **Actif** est cochée. Le bouton **Désactiver** est affiché et actif. Les notes de travail montrent que la demande d'entrée EDL a été approuvée.
Refuser	Sur l'enregistrement de l'entrée, le champ État bascule sur **Rejeté** et la case **Actif** est décochée, indiquant que l'entrée n'est pas bloquée sur le pare-feu. Les notes de travail montrent que la demande d'entrée EDL a été rejetée.

Une fois que vous avez approuvé l'entrée EDL et qu'elle est activée, Palo Alto Networks récupère l'entrée EDL après l'intervalle de récupération suivant. Une fois l'entrée récupérée, l'observable est bloqué à partir de ce moment-là. Dans la figure suivante, notez que la case **Actif** est cochée, que l'état est Ajouté et que les notes de travail indiquent que la demande a été approuvée.



Module complémentaire TISC pour la vue d'ensemble de Splunk

Le Centre de sécurité des renseignements sur les menaces (TISC) pour Splunk l'application offre l'intégration entre TISC et Splunk permet aux utilisateurs d'importer de manière transparente les dernières informations sur les menaces de TISC pour les surveiller Splunk et enrichir les alertes. Les utilisateurs peuvent configurer des collectes d'indicateurs, effectuer des recherches et utiliser des tableaux de bord pour analyser efficacement les correspondances de recherche et les collectes d'indicateurs.

Intégration TISC avec Splunk

L'intégration entre le (TISC) et Splunk permet aux utilisateurs de filtrer et d'extraire Centre de sécurité des renseignements sur les menaces des données observables pertinentes de Threat Intelligence vers .Splunk Dans le Splunk, les utilisateurs peuvent utiliser ces données pour générer des alertes de sécurité.

Rôle requis : Splunk admin

À l'aide de l'application TISC complémentaire, vous pouvez configurer l'intervalle auquel vous pouvez extraire des observables de l'instance ServiceNow TISC .

Cet intervalle détermine la fréquence à laquelle l'application peut effectuer des demandes et ServiceNow récupérer les données des observables. En outre, vous pouvez définir et appliquer des filtres pour spécifier les observables que vous souhaitez extraire de l'instance ServiceNow TISC .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois les observables extraits de ServiceNow, les données des observables sont stockées dans Splunk KV Store (Key-Value Store) et vous pouvez écrire les règles de corrélation sur l'ensemble des observables qui ont été extraits.

Création d'utilisateurs dans l'instance ServiceNow TISC

Vous pouvez créer des utilisateurs dans l'instance avec n'importe ServiceNow TISC quel rôle d'utilisateur valide : sn_sec_tisc.api_obs_read_access.

Installer TISC l'application complémentaire sur Splunk

Pour plus d'informations, consultez Affecter un rôle à un utilisateur .

Rôle requis : admin Splunk.

1. Connectez-vous à *Splunk*.
2. Accédez à la **Applications** > **Gérer les applications** ou cliquez sur l'icône **Gérer** l'engrenage.
3. Recherchez l'application *Centre de sécurité des renseignements sur les menaces* **pour** *Splunk* et installez-la.
4. Une fois installée, l'application serait visible sous la liste des applications.

Configurer TISC le module complémentaire dans Splunk

Suivez la procédure ci-dessous pour configurer l'application.

Avant de commencer

Rôle requis : Splunk admin

Pourquoi et quand exécuter cette tâche

La procédure ci-dessous décrit la configuration du module complémentaire TISC dans Splunk.

Procédure

1. **Recherchez Centre de sécurité des renseignements sur les menaces pour l'application Splunk** dans le volet de navigation de gauche.
2. Cliquez sur **Configurer** dans la colonne **Actions** .
   La page **Configuration** s'affiche et vous pouvez configurer votre ServiceNow TISC compte.
3. Sélectionnez **Ajouter**.
4. Remplissez les champs du formulaire.

Champ	Description
Ajouter des comptes	
Nom	Nom unique pour le compte.
Nom d'utilisateur	Indiquez le nom d'utilisateur de votre ServiceNow compte. Vous pouvez utiliser le même nom d'utilisateur que celui utilisé pour les utilisateurs qui est créé lors de la création du rôle sn_sec_tisc.api_obs_read_access dans l'étape ci-dessus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mot de passe	Fournissez le ServiceNow mot de passe du compte.
URL d'instance	Indiquez l’adresse URL de l’instance ServiceNow .

5. Cliquez sur **Ajouter**.
   Le ServiceNow compte d’instance Splunk est ajouté au .
6. Accédez à la page **Entrées** pour créer des collections, gérez vos entrées de données pour votre ServiceNow compte.
7. Cliquez sur **Créer une entrée**.
   La boîte de dialogue **Ajouter une entrée** s’affiche pour vous permettre d’ajouter les entrées à votre ServiceNow compte.

   Une fois le jeu d’entrées défini, l’application envoie les informations à l’instance TISC pour récupérer un nombre spécifique d’observables qui répondent aux critères.
8. Renseignez les détails de l’entrée, le cas échéant.

Champ	Description
Nom	Un nom unique pour votre entrée. Par exemple, la liste d’adresses IP malveillantes.
Compte	Indiquez le nom d’utilisateur de votre ServiceNow compte. Vous pouvez utiliser le même nom d’utilisateur que celui utilisé pour les utilisateurs créés avec le rôle `sn_sec_tisc.api_obs_read_access` dans l’étape ci-dessus.
Intervalle	Définissez l’intervalle de temps en secondes pour récupérer les données à partir de TISC.
Période d’expiration (en jours)	Option permettant de définir la période d’expiration en jours. **Remarque :** La date de péremption de l’échantillon est fixée à 30 jours. Par exemple, lorsque des données sont extraites à une date spécifique, un ensemble de 10 000 enregistrements peut être récupéré. Ces enregistrements seront stockés dans le magasin KV (clé-valeur) au sein de Splunk. À compter de la date d’ingestion, les enregistrements sont conservés pendant 30 jours. Le 31e jour, ils seront automatiquement supprimés de la boutique KV.
N’expire jamais	Choisissez cette option si vous ne souhaitez pas faire expirer les enregistrements ingérés.
Attributs supplémentaires	Vous permet d’ajouter des attributs supplémentaires à partir de la liste des options recommandées à inclure dans le magasin KV. Les attributs doivent être séparés par des virgules.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Une liste des attributs autorisés est fournie dans la table après la table des attributs obligatoires.
Filtres	Définissez les conditions selon lesquelles les données à importer seront filtrées. Pour définir les conditions de filtre, vous pouvez définir les critères en fonction des champs tels que le score de menace, le niveau de fiabilité et le type. Pour les conditions de filtre simples, vous pouvez utiliser cette option de filtrage. Toutefois, si les conditions de filtre sont plus complexes et pour tout filtrage avancé, vous pouvez choisir d'ajouter des filtres JSON. ○ Les opérateurs de nombre entier autorisés sont : "=", "!=", ">", "<", ">=", "<=" ○ Les opérateurs de chaîne autorisés sont les suivants : « = », « != », « IN » **Vous trouverez ci-dessous un exemple de filtre simple** : {Sample filter format: Allowed Tokens: "threat_score", "confidence", "reputation", "type", "value". Allowed Integer Operators: "=", "!=", ">", "<", ">=", "<=". Allowed String Operators: "=", "!=", "IN". Example: reputation IN ("clean","suspicious","malicious") AND threat_score > 90 AND confidence > 90 AND type = "ip_v4_address"}
JSON	Les filtres basés sur JSON vous permettent de définir des conditions plus complexes. L'état de l'objet JSON doit être actif. Cochez la case Filtres **JSON** pour passer à des filtres avancés où un JSON peut être utilisé pour appliquer une condition de filtre.

Exemple de filtre avancé :

```
{"boolean_operator":"AND","filters":[{"field_name":"reputation","operator":"IN","field_value":"
clean,suspicious,malicious"},{"field_name":"threat_score","operator":">","field_value":"90"},{"
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

field_name":"confidence","operator":">","field_value":"90"},{"field_name":"type","operator":"=","field_value":"ip_v4_address"}]}

Remarque : Les comptes sont actifs par défaut, mais les entrées sont inactives par défaut, vous devez les activer pour commencer à importer les données. Pour connaître les filtres possibles, reportez-vous à Observable_filters section dans Ajoute des enregistrements sources observables à l'application Centre de sécurité des renseignements sur les menaces (TISC).

9. Cliquez sur **Ajouter** pour ajouter les entrées.
10. Cliquez sur **Cloner** ou copier pour copier et créer un compte basé sur le compte existant. Assurez-vous que l'entrée est désactivée avant le clonage pour éviter de créer des entrées en double lors de l'importation de données à l'aide des mêmes critères.
11. Une fois les données extraites, les informations suivantes sont récupérées et stockées dans le magasin KV à l'intérieur Splunk , avec les enregistrements extraits de TISC :

Champ	Description
fiabilité	Indique le niveau de fiabilité associé à l'exactitude du score de menace.
kvlookup_created_time	Indique l'heure de création de l'enregistrement dans le magasin de valeurs de clés.
kvlookup_days_till_expiry	Indique le nombre de jours après lesquels l'enregistrement sera supprimé de la boutique KV.
instance_url	Indique l'adresse URL de l'instance ServiceNow .
réputation	Indique la réputation de l'entité impliquée.
source_reported_score	Le score source rapporté à partir de TISC.
sys_id	ID système de l'enregistrement qui arrive.TISC
threat_level	Indique le niveau de gravité de la menace.
threat_score	Score indiquant le niveau de menace associé à un enregistrement.
threat_severity	Indique la gravité de menace de l'observable.
type	Indique le type d'observables.
updated_by	Fournit les informations sur la personne qui a mis à jour l'enregistrement pour la dernière fois.
kvlookup_updated_time	Indique l'horodatage de la dernière mise à jour de l'enregistrement dans le magasin de valeurs clés.
valide	Valeur de l'enregistrement. Par exemple, IP, hachage, etc.

Attributs supplémentaires

Champ	Description
additional_context	Fournissez tout contexte supplémentaire, si nécessaire.
attack_phases	Indique les phases d'attaque d'une chaîne de frappe telles que LM, MITRE ATT&CK.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
auteur	Indiquez le nom de l’auteur.
commentaires	Ajoutez des commentaires supplémentaires si nécessaire.
créé(s)	Indique quand l’observable a été créé.
description	Fournissez la description.
expiration_time	Spécifie le délai d’expiration de l’enregistrement observable.
extensions	Indique les extensions d’un observable.
first_observed	La première fois que les données ont été observées.
first_seen	Première fois que cet enregistrement a été vu en train d’effectuer des activités malveillantes.
historically_significant	Indique si l’observable est considéré comme historiquement significatif. Ce marqueur système TISC est utilisé pour exclure l’observable de l’archivage.
id	Identificateur unique affecté à l’observable par le système TISC.
is_defanged	Marqueur indiquant si la valeur de l’observable a été neutralisée.
is_false_positive	Marqueur booléen qui indique si l’observable est identifié comme faux positif.
language	Indique la langue du contenu textuel dans cet objet.
last_observed	La dernière fois que les données ont été observées.
last_seen	Heure à laquelle cet objet a été vu pour la dernière fois en train d’effectuer des activités malveillantes.
notes	Ajoutez des notes supplémentaires pour un enregistrement d’observable.
Numéro	Numéro généré par le système affecté à l’observable par TISC.
security_type	Spécifie si l’observable appartient à la liste d’autorisation ou à la liste de refus.
no_of_sources	Représente le nombre de sources uniques qui ont contribué à l’observable.
sources	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
état	Saisissez l’état de l’observable s’il est actif ou inactif.
tisc_tags	Sélectionnez les balises TISC associées à un observable.
Taxonomies	Sélectionnez la taxonomie associée à un observable.
Tlp	Valeur unique qui indique le paramètre de sensibilité des données par TLP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
mises à jour	Indique quand l'enregistrement observable a été mis à jour pour la dernière fois
usage_categories	Catégories auxquelles appartient l'observable, telles que botnet ou hameçonnage.
watch_list	Marqueur spécifiant si l'observable est inclus dans la liste de surveillance.

Ces champs, ainsi que tous les autres définis par vos critères, seront disponibles dans Splunk et peuvent être consultés, recherchés et analysés via l'onglet de recherche.

Stockage des données dans Splunk

Cette section explique comment TISC utiliser les recherches lors de l'intégration dans le magasin clé-valeur de Splunk pour le stockage des données. Elle détaille comment ces recherches sont configurées et récupérées dans .Splunk

Recherche	Description de la recherche
`tisc_store_lookup`	Nom de la recherche KV à utiliser pour rechercher les enregistrements entrants.
`tisc_kv_store`	Nom du magasin KV où résident les données.
`inputlookup <lookup_name>" example : | inputlookup tisc_store_lookup`	Requête pour rechercher des enregistrements dans le magasin KV.

TISC - Intégration de Microsoft Sentinel

Centre de sécurité des renseignements sur les menaces pour Microsoft Sentinel offre plusieurs fonctionnalités, notamment l'importation d'observables de TISC vers Sentinel, l'enrichissement des incidents Sentinel avec les détails des observables connexes, ainsi que la possibilité d'exporter des observables de Sentinel vers TISC.

Remarque : Sur Microsoft Sentinel, les observables sont appelés des entités.

Prérequis

Dépendances

La solution **Threat Intelligence** de Microsoft Sentinel Content Hub doit être installée.

Rôles et autorisations

Application	Rôles et autorisations	Description
Rôles spécifiques à Microsoft Sentinel	1. Contributeur de l'application logique 2. Contributeur Microsoft Sentinel	1. Pour installer les playbooks requis au niveau d'un groupe de ressources. 2. Interagissez avec les playbooks Microsoft Sentinel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles et autorisations (suite)

Application	Rôles et autorisations	Description
		Pour plus d'informations, consultez Rôles et autorisations dans Microsoft Sentinel.
Centre de sécurité des renseignements sur les menaces	sn_sec_tisc.api_azure_sentinel_solution	L'utilisateur configuré dans le connecteur personnalisé TISC doit avoir ce rôle pour autoriser l'accès aux API TISC.

Modèles de Playbook TISC

Cette section décrit les modèles de playbook fournis avec la solution TISC Sentinel.

Cas d'utilisation de Playbook

Le tableau suivant décrit les différents cas d'utilisation de Playbook.

Cas d'utilisation	Playbook	Description
Importation d'observables de TISC vers Sentinel	Batch_Indicator_Uploader	Fournit un mécanisme de traitement par lots pour exporter des observables à partir de TISC à l'aide de l'API Charger des indicateurs fournie par Microsoft Sentinel.
	Import_Observables_Batch	Active l'exportation planifiée d'observables à partir de TISC.
Exporter des entités de Sentinel vers TISC	Export_Incident_Entities	Exporter toutes les entités d'un incident Sentinel.
	Export_Hash_Entity	Exporter les entités de hachage de fichier de l'incident Sentinel.
	Export_Domain_Entity entités	Exporter les entités de domaine de l'incident Sentinel.
	Export_IP_Entity	Exporter les entités IP de l'incident Sentinel.
	Export_URL_Entity	Exporter les entités URL de l'incident Sentinel.
Enrichir les incidents Sentinel	Incident_Enrichment	Permet l'enrichissement des incidents Sentinel en extrayant les détails relatifs aux entités qui y sont associées et en publiant des informations sous la forme de commentaires sur l'incident.

Remarque : Tous les playbooks utilisent le connecteur personnalisé TISC en interne pour utiliser les API TISC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer des playbooks à partir de modèles

1. Accédez à la page de contenu de la**solution T ISC** à partir du **concentrateur de contenu dans l'espace de travail Sentinel**.
2. Pour chaque playbook affiché dans la page de contenu, procédez comme suit :
   a. Sélectionnez le modèle de playbook, un volet contextuel s'affiche dans la partie droite de l'écran, cliquez sur **Configuration**.
   b. Lisez la description du modèle de playbook, passez en revue **les étapes Prérequis** et **Post déploiement** mentionnées dans la description.
   c. Cliquez sur **Déployer un connecteur personnalisé** (si vous n'avez pas déjà déployé le connecteur personnalisé).

      Ajoutez **l'URL de l'instance ServiceNow** sur la page **Configuration du déploiement** .
   d. Cliquez sur **Créer un playbook**, vous serez redirigé vers l'écran de configuration du déploiement
   e. Dans l'écran de configuration Créer un playbook :
      - Sélectionnez le groupe de ressources approprié.
      - Modifiez le nom du playbook ou utilisez le nom par défaut.
      - Indiquez le **nom du connecteur personnalisé**e (assurez-vous que cela correspond au nom du connecteur que vous avez déployé à l'étape précédente) dans la section Paramètres.
      - Cliquez sur **Examiner et créer**.

Configurer Import_Observables_Batch playbook

Assurez-vous de créer Batch_Indicator_Uploader playbook avant la création du playbook Import_Observables_Batch.

1. Accédez à la **Concepteur d'application logique** pour modifier le playbook.
2. Mettez à jour la durée de récurrence (en heures) selon vos besoins.
3. À partir du composant Connecteur personnalisé TISC dans le playbook, mettez à jour les paramètres envoyés à l'API TISC.

Nom de paramètre	Description
Type d'observable	Les types pris en charge sont suivants, sélectionnez-en un ou plusieurs : ○ IP ○ Hachage de fichiers ○ Domaine ○ URL
Score de menace	Saisissez le score de menace pour les observables. La valeur du score de menace DOIT être un nombre compris entre 0 et 100.
Fiabilité	Entrez la confiance pour les observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de paramètre	Description
	La valeur de confiance DOIT être un nombre compris entre 0 et 100.
Réputation	Les valeurs prises en charge sont les suivantes, sélectionnez-en une ou plusieurs : ○ Nettoyer ○ Malveillant ○ Suspect ○ Inconnu
Gravité de la menace	Les niveaux de gravité pris en charge sont les suivants, sélectionnez-en un ou plusieurs : ○ Critique ○ Élevé ○ Moyenne ○ Faible
Niveau de menace	Voici les niveaux de menace pris en charge, sélectionnez-en un ou plusieurs : ○ Élevé ○ Moyenne ○ Faible
Dernière mise à jour du différentiel en heures	Heure de la dernière mise à jour (en heures) des observables.

Configurer Export_Incident_Entities playbook

Ce playbook utilise l'API Ajouter des observables TISC. À l'aide du concepteur d'application logique, vous pouvez modifier les paramètres envoyés à l'API à partir du playbook. Pour plus d'informations, consultez API TISC : POST /sn_sec_tisc/threat_intel_data/add_observables .

Vous pouvez suivre la même procédure pour tous les playbooks énumérés ci-dessous qui exportent différents types d'entités :

- Export_Hash_Entity
- Export_Domain_Entity
- Export_IP_Entity
- Export_URL_Entity

Configurer Incident_Enrichment playbook

Ce playbook utilise l'API Observables TISC. À l'aide du concepteur d'application logique, vous pouvez modifier les paramètres envoyés à l'API à partir du playbook. Pour plus d'informations, consultez API TISC : POST /sn_sec_tisc/threat_intel_data/observables .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exécuter les playbooks

La table suivante décrit comment exécuter les playbooks suivants.

Playbook	Action
Import_Observables_Batch	Ce playbook s'exécute automatiquement en fonction de l'heure planifiée mentionnée dans le déclencheur de récurrence.
Export_Incident_Entities	Lors d'un incident Sentinel, sélectionner **Actions d'incidents** > **Exécuter le playbook** pour exécution.
Export_Hash_Entity	Lors d'un incident Sentinel, sélectionner **Entité de hachage de fichier** > **Exécuter le playbook** pour exécution.
Export_Domain_Entity	Lors d'un incident Sentinel, sélectionner **Entité du domaine** > **Exécuter le playbook** pour exécution.
Export_IP_Entity	Lors d'un incident Sentinel, sélectionner **Entité IP** > **Exécuter le playbook** pour exécution.
Export_URL_Entity	Lors d'un incident Sentinel, sélectionner **Entité de l'URL** > **Exécuter le playbook** pour exécution.
Incident_Enrichment	Lors d'un incident Sentinel, sélectionner **Actions d'incidents** > **Exécuter le playbook** pour exécution.

Administrer Centre de sécurité des renseignements sur les menaces

Utilisez le volet de navigation de gauche pour accéder au module Administration et Centre de sécurité des renseignements sur les menaces afficher les modules suivants de l'administration des données, afin de définir plus précisément les règles de filtrage et les règles d'approbation, définir le score de TISC menace et gérer les notifications.

Administration des données

Module	Description
Moteur de règles	Cette section comprend les règles suivantes requises lors de la gestion des données : 1. **Règles d'approbation des importations de données** : définissez les règles d'approbation et intégrez le flux d'approbation dans la section Intelligence d'importation après avoir soumis l'importation des données. 2. **Règles de filtrage entrant** : créez des règles de filtrage afin de filtrer les données des enregistrements sources entrants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Administration des données (suite)

Module	Description
	3. **Règle de notation de menace** : personnalisez le calculateur de score de menace qui affecte le score de menace aux observables.
Listes des contrôles de sécurité	Ce module vous aide avec les contrôles de sécurité : 1. **AllowList** 2. **DenyList** 3. **Liste de surveillance**
Taxonomies	Ce module vous aide à créer des taxonomies pour les enregistrements de source de données.
Notifications	Ce module définit comment gérer les notifications par e-mail.
Modèles	Ce module explique comment créer des modèles de rapport dans l'expérience de conception et d'exécution.

Définition des règles d'approbation des importations de données

Utilisez cette section pour définir les règles d'approbation et intégrer le flux d'approbation dans la section Intelligence d'importation après l'envoi de l'importation de données.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Administration** dans l'espace de travail.
3. Accéder à **Moteur de règles** > **Importations des données pour les règles d'approbation**.
4. Sélectionnez **la règle d'approbation pour les importations de données**.

   Dans le système de base, la **règle d'approbation pour les importations de données** est la règle d'approbation par défaut mise en place pour permettre aux utilisateurs d'activer le workflow d'approbation.

5. Entrez au moins un nom d'utilisateur ou un groupe d'utilisateurs pour chacune des sections **Sélectionner un utilisateur ou des groupes nécessitant une approbation** et **Sélectionner un ou plusieurs approbateurs** .
6. Cliquez sur le bouton **Activer** pour activer le flux d'approbation des importations de données.

   Lorsque cette option est activée, les importations de données sont dans la file d'attente d'approbation pour que l'approbateur approuve ou rejette le traitement des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'approbateur examine les changements apportés par l'analyste, puis approuve ou rejette la demande d'importation de données.

Remarque : Une notification par e-mail est envoyée au(x) utilisateur(s) ou au(x) groupe(s) d'utilisateurs pour leur indiquer que la tâche d'importation est traitée et approuvée ou rejetée.

Définition des règles d'expiration

Définissez des règles d'expiration pour divers observables ou une combinaison de divers objets sources ou sources d'indicateurs créés dans TISC.

Avant de commencer

Chaque source créée dans l'application a une période d'expiration. Les flux de données utilisent des techniques telles que la période d'expiration basée sur le temps pour stimuler l'ingestion de données. Dans TISC, les règles d'expiration définissent le délai d'expiration d'un ensemble particulier de sources de données ou d'un ensemble de types d'objets ou de types d'observables.

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Règles d'expiration**.
   La page Règles d'expiration s'affiche.
3. Cliquez sur **Nouveau**.

Champ	Description
Nom	Entrez un nom pour la règle d'expiration.
Description	Entrez une description pour la règle d'expiration.
Période d'expiration (jours)	Spécifiez la durée après laquelle les données ingérées doivent expirer ou être considérées comme obsolètes. Saisissez la période d'expiration de l'observable en jours. Par exemple, 100 jours. **Remarque :** Quelles que soient les données ingérées à la source, elles expireront 100 jours après l'ingestion.
Sources de données	Indique la règle d'expiration de la source de données actuelle. Sélectionnez la liste des sources de données à partir de la recherche. **Remarque :** Ne sélectionnez pas ce champ et veillez à le laisser vide si vous souhaitez sélectionner toutes les sources de données. Si vous souhaitez sélectionner l'indicateur en tant qu'objet, vous devez sélectionner l'objet, puis sélectionner la valeur **Type d'enregistrements** comme **indicateur**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Par défaut, un exemple de règle d'expiration sn_sec_tisc_m2m_entity_-rules est mis en service pour les utilisateurs dans le système de base. Pour les observables, cet échantillon de règle d'expiration sera dans l'état désactivé. Vous devez activer et activer la règle. Pour appliquer la règle aux enregistrements sources, vous devez activer la règle.
Catégorie	Indique le type de catégorie de règle d'expiration pour la source de données actuelle. Sélectionnez le type de catégorie dans la liste déroulante, par exemple observable ou objet.
Type des enregistrements	Sélectionnez le type d'enregistrements.

4. Cliquez sur **Activer** pour activer la règle d'expiration après avoir créé une règle.
   Si vous n'activez pas la règle d'expiration, elle ne sera pas appliquée à l'enregistrement source.

   Remarque :

   - Chaque fois que vous activez une règle d'expiration, une vérification de duplication se produit en arrière-plan pour vérifier s'il existe une règle en double dans le système avec la même combinaison de sources de données et de type d'enregistrements. Si tel est le cas, l'application affiche un message d'information indiquant que la règle contient déjà la même combinaison de source de données et de catégorie d'objet et que vous devez modifier la combinaison existante pour activer la règle.
   - Une règle d'expiration d'exemple est mise en service pour les utilisateurs dans le système de base et cette **règle d'expiration d'exemple** pour l'observable sera dans l'état désactivé par défaut et vous devez activer et activer la règle.

5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Supprimer** si vous souhaitez supprimer une règle d'expiration.

Règles d'expiration pour les enregistrements sources

Les règles d'expiration sont essentiellement utiles pour définir le délai d'expiration des enregistrements sources. L'enregistrement agrégé hérite du délai d'expiration le plus élevé de ses enregistrements sources correspondants.

Comment les règles sont appliquées

Example: Le type d'enregistrement source entrant est un programme malveillant provenant du type de source de données CrowdStrike

Processus d'évaluation de règle basé sur les règles fournies pour l'application des délais d'expiration aux enregistrements sources :

1. **Extrayez toutes les règles activées :** L'application commence par vérifier toutes les règles qui sont actuellement activées.
2. Rechercher une combinaison de règles spécifique :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherchez une règle qui correspond spécifiquement à la combinaison des éléments suivants :

- **Type de source de données** : CrowdStrike
- **Type des enregistrements** : Programme malveillant

3. **Priorité basée sur les combinaisons de règles de correspondance :**

   S'il existe une règle dans laquelle le type de source de données est **CrowdStrike** et le type d'enregistrement est **Programme malveillant**, cette règle a priorité. Le délai d'expiration spécifié dans cette règle sera appliqué.

4. **Règles de secours :**

   a. Si aucune règle ne correspond à la combinaison **CrowdStrike et Malware** , le système recherche une règle dans laquelle le type de source de données est **CrowdStrike** et le type d'enregistrement est **Tous**.

   b. Si aucune règle n'est trouvée, il recherche alors une règle où le type de source de données est **Tous** et le type d'enregistrement est **Programme malveillant**.

   c. Enfin, si aucune des règles ci-dessus n'existe, la règle est définie par défaut sur une règle dans laquelle le type de source de données et le type d'enregistrement sont **Toutes**.

5. Si aucune de ces règles n'existe dans le système, aucune règle d'expiration n'est alors appliquée aux enregistrements sources. Dans ce cas, accédez à la table ci-dessous (illustrée dans la capture d'écran) pour vérifier la combinaison de règles qui a été appliquée aux objets.



6. **Suppression des sources de données :**

   Supposons qu'une source de données à laquelle les règles d'expiration sont associées soit supprimée, la suppression peut être restreinte ou non autorisée jusqu'à ce que ces règles soient résolues. Cela permet de s'assurer qu'il n'y a pas d'incohérences dans l'application des politiques d'expiration.

Créer des règles d'exclusion des données entrantes

Créez des règles d'exclusion des données entrantes afin de filtrer tout type de données ou tout type de données d'enregistrements sources entrants.

Avant de commencer

L'application prend en charge l'intégration de plusieurs flux de renseignements sur les menaces, y compris les sources de données STIX. Pour s'assurer que seules les données pertinentes sont ingérées, des règles d'exclusion personnalisables doivent être appliquées.

Rôle requis : sn_sec_tisc.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Des règles d'exclusion sont créées et appliquées sur un enregistrement source pour traiter les étapes suivantes. Le système de base fournit la **règle de filtrage d'échantillon** pour les utilisateurs avec une règle prédéfinie pour filtrer les observables, les données d'indicateur ou les entités/objets ingérés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Explorez jusqu'à **Moteur de règles** > **Règles d'exclusion des données entrantes**.
3. Cliquez sur **Nouveau** pour définir des règles d'exclusion.
   La page Créer des règles d'exclusion des données entrantes s'affiche.
4. Remplissez les champs du formulaire.

Définir des règles d'exclusion

Champ	Description
Nom	Nom de la nouvelle règle d'exclusion.
Description	Brève description de la règle d'exclusion.
Ordre	Priorité de la règle d'exclusion. Ce champ indique l'ordre dans lequel les règles d'exclusion sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle d'exclusion dotée du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100 pour la règle d'exclusion du système de base.
Sources de données	Sélectionnez les flux pour lesquels la règle d'exclusion doit être appliquée.
Table	Sélectionnez le type de table auquel vous souhaitez appliquer le filtre. Par exemple, Source observable, Source indicateur et Source objet.
Type de filtre (uniquement lorsque la table sélectionnée est Source d'observables)	L'option Types de filtres contient deux options sur lesquelles vous pouvez appliquer le filtre. ○ Filtre basé sur une condition ○ Filtre basé sur une liste
Type de filtre (filtre basé sur la condition)	Conditions de filtre dans le générateur de conditions. Ces conditions sont basées sur la table source. Par exemple, la source de l'indicateur et la source de l'objet n'ont que le type de filtre : filtre basé sur la condition. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. Si **ET** est sélectionné, toutes les conditions doivent être mises

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	en correspondance. Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouvel ensemble de conditions**.
Type de filtre (filtre basé sur la liste)	Si les observables entrants correspondent aux entrées de la liste sélectionnée, ils sont filtrés. **Remarque :** Ces règles d'exclusion ne s'appliquent pas aux importations de données à l'aide de l'intelligence d'importation et les options disponibles sont Liste d'autorisation, Liste de refus et Liste de surveillance.

Les enregistrements exclus par la règle d'exclusion peuvent être consultés dans les sections suivantes.

a. **Enregistrements d'observables filtrés** : filtre et répertorie les enregistrements d'observables.
b. **Enregistrements d'indicateurs filtrés** : filtre et répertorie les enregistrements d'indicateurs.
c. **Enregistrements d'objets filtrés** : filtre et répertorie les enregistrements d'objets.

Remarque : Pour appliquer les règles d'exclusion basées sur les balises ajoutées aux enregistrements sources *TISC*, **sélectionnez** l'option balises dans le générateur de conditions de filtre.

Calculateur de score de menace personnalisé dans TISC

Le calculateur de score de menace personnalisé vous permet de définir et de calculer le score de gravité de menace d'un observable en fonction des critères définis par l'utilisateur, qui fournit un score d'intelligence transparent des observables. Le score de menace est calculé automatiquement pour les enregistrements d'observables.

Définir le calculateur de score de menace

Définissez le score de menace pour les enregistrements d'observables qui sont générés en fonction des paramètres définis par l'utilisateur. Le système de base est doté d'une règle de notation des menaces, qui peut être personnalisée et activée en conséquence.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Remarque : Par défaut, la règle de notation de la menace est inactive. Vous devez activer la règle pour voir le score des observables.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Accéder à **Règle de notation de menace**.
   La page Calculateur du score de menace s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :

- Dans l'application, dans le système de base, une règle de notation est mise en service pour que les utilisateurs puissent afficher, modifier ou modifier le score de menace, mais l'utilisateur ne peut pas créer une nouvelle règle ou supprimer la règle de notation de menace prédéfinie.
- Les changements s'appliqueront à tous les nouveaux observables ou mises à jour des observables à partir de ce moment-là. Pour reformuler les scores historiques, ils doivent utiliser l'option recalculer.

3. Sur le formulaire, les champs suivants contiennent les valeurs prédéfinies.

Calculateur score de menace

Champ	Description
Nom	Nom de la valeur de notation de la menace. Par exemple, Calculateur de score de menace.
Description	Description de l'enregistrement du score de menace. Par exemple, calcule le score de menace en fonction de la somme pondérée des scores de critères prédéfinis.
Pondération globale (applicable au générateur de critères)	Ce champ n'est pas modifiable et affiche la pondération globale calculée par le système en fonction du poids correspondant aux critères activés.
Critères de notation	Indique les critères de notation pour un observable. Voici les deux options disponibles pour définir les critères de notation de menace : ○ **Générateur de critères** : Utilisez cette option pour ajouter, modifier ou supprimer, activer et désactiver les critères qui contribuent au calcul du score de menace et vous assurer que la pondération agrégée totale est de 100 %. ○ **Utiliser un script (avancé)** : la fonctionnalité de scripting est une fonctionnalité avancée permettant de créer un script personnalisé qui doit renvoyer le score de menace dans une plage comprise entre 0 et 100.

Vous trouverez ci-dessous les options disponibles pour définir les **critères de notation** :

- Générateur de critères
- Utiliser le script (avancé)

Voici la procédure pour le générateur de critères :

Remarque : Vous pouvez modifier les critères existants ou en ajouter un nouveau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sélectionnez le type de critères.
Par exemple, ajoutez un nouveau critère.

b. Sélectionnez la **table** pour laquelle les critères sont configurés.
La liste des valeurs de la liste déroulante est la suivante : Observables, Acteur de menace, Campagne, Emplacement, Identité, Vulnérabilité, Événement de menace, Incident de sécurité et Agrégats. Lorsque vous sélectionnez l'une de ces options dans la liste déroulante, une condition est appliquée. Cette condition garantit que seuls les enregistrements associés à la valeur sélectionnée sont affichés ou calculés.

Remarque :

- Si l'observable est sélectionné, la condition sera appliquée à l'enregistrement observable pour lequel le score de menace sera calculé. Si la table sélectionnée n'est pas un observable, la condition sera appliquée uniquement si les enregistrements sont liés à l'observable pour lequel le score de menace sera calculé.
- Une table d'agrégats supplémentaire est ajoutée pour définir les scores en fonction du nombre de relations associées aux observables. Par exemple, sélectionnez la table : agrégats et la valeur de champ : acteurs de menace, puis pour un observable, s'il y a plus de deux acteurs de menace, définissez le score et appliquez les conditions le cas échéant.
- Par exemple, si vous souhaitez définir un score pour un ou plusieurs acteurs de menace associés à un observable, sélectionnez le champ Nombre d'acteurs de menace et définissez le score souhaité et appliquez les conditions le cas échéant.

c. Sélectionnez le **champ** dans la table sélectionnée ci-dessus.

d. Entrez la **pondération** des critères entre 0 et 100.
La pondération globale de tous les critères doit être de 100 %.

e. Saisissez le nom et la description brève des critères.

f. Cochez la case **Activer les critères de notation** pour activer les critères de notation.

g. Définissez les **conditions** et définissez le score pour les conditions.

h. Vous pouvez également ajouter de nouvelles conditions à l'aide du bouton **Nouvelle condition** et supprimer la condition à l'aide de l'icône **Supprimer les critères** .

i. Cliquez sur **Ajouter** pour ajouter les critères configurés.

Voici un exemple de définition d'une condition pour un score de menace :

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
Condition-3: CVSS2.0 < 4, Score = 10
```

4. Cliquez sur le bouton **Recalculer l'historique** pour recalculer le score de menace.
   Si des changements sont apportés à la règle de notation de menace, vous devez réappliquer la règle de notation aux observables dont le score de menace a déjà été calculé dans le passé. Utilisez le bouton **Recalculer l'historique** pour déclencher la tâche de recalcul.

   Remarque :

   - Un message de confirmation s'affiche pour vous permettre d'effectuer l'action. Il s'agit d'un processus de longue durée qui s'exécute en arrière-plan. Vous ne serez pas en mesure d'apporter des changements tant que le processus n'est pas terminé. Voulez-vous vraiment exécuter cette action ?
   - Pour tous les événements de mise à jour générés pour les observables dans le cadre de **Recalculer l'historique**, le traitement des webhooks est désactivé. Si vous souhaitez l'activer, modifiez cette propriété système `webhook_ignore_threat_score_reapply`.

5. Cliquez sur **OK**.

Important : Cette action déclenchera une tâche de longue durée et le système ne vous permettra pas d'apporter d'autres modifications à la règle de notation de menace tant que la tâche n'est pas terminée. Pour plus d'informations sur la configuration de la tâche en arrière-plan, consultez Configuration du cadre de travail de la tâche en arrière-plan de Vulnerability Response .

Le script Utiliser un **script (avancé)** est le suivant : Utilisez ce script pour créer un script personnalisé qui doit renvoyer le score de menace dans une plage comprise entre 0 et 100.

Le champ de script avancé est renseigné automatiquement avec une fonction qui prend les paramètres **actuels** et **agrégés** et cette fonction doit renvoyer le score de menace dans la plage comprise entre 0 et 100.

Ici, le paramètre actuel est l'objet GlideRecord de l'entité (observable) pour laquelle le score de menace est calculé. Pour les observables, cela correspond au GlideRecord pour la table sn_sec_tisc_observable. Le paramètre des agrégats est un objet GlideRecord de l'enregistrement de la table sn_sec_tisc_aggregates qui est utilisé pour accéder aux nombres d'enregistrements des différents types d'enregistrements associés (tels que les campagnes ou les identités) à l'entité principale (observable).

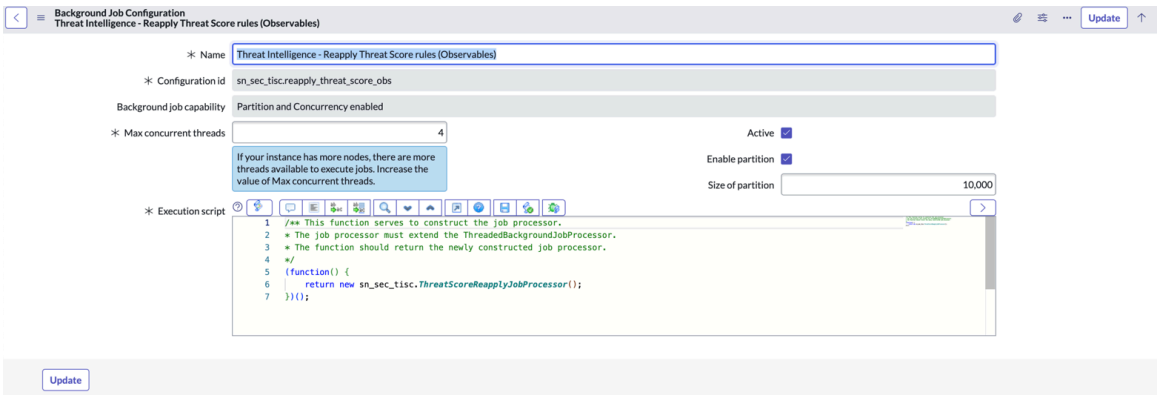
Exemple de script dans l'option avancée :

```
answer = (function threatScoreCalculator(current, aggregates) {

   // return the threat score in the range of 0-100
   var threatSeverity = current.getValue("threat_severity");
   if(threatSeverity == "high")
    return 80;
   else {
      let associatedCampaigns = aggregates.getValue("num_of_campaigns");
      if(associatedCampaigns > 0)
         return 50;
   }
   return 0;

})(current, aggregates);
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À titre de référence, vous trouverez ci-dessous la capture d'écran qui vous montre le processus de configuration de la tâche en arrière-plan du score de menace.



Règles d'extraction technique MITRE ATT&CK

Extrayez automatiquement les techniques MITRE des observables ou des objets ingérés à partir de diverses sources de données, ainsi que les techniques MITRE des résultats de la recherche de menaces sur l'enregistrement d'observable.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Remarque : Assurez-vous de vérifier que les données du référentiel MITRE ATT&CK sont disponibles dans l'instance que vous utilisez. Si les données ne sont pas disponibles, l'application n'effectuera pas l'extraction.

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Accéder à **Moteur de règles** > **Règles d'extraction technique MITRE ATT&CK**.
   La page Règles d'extraction technique MITRE ATT&CK s'affiche.
3. Cliquez sur **Nouveau**.

Champ	Description
Nom	Entrez un nom pour la règle d'extraction technique MITRE ATT&CK.
Description	Saisissez une description pour la règle d'extraction technique MITRE ATT&CK.
Type d'intégration	Indique la règle d'extraction de la technique MITRE ATT&CK pour les sources de données ou les résultats de la recherche de menaces. Sélectionnez la liste des sources de données à partir de la recherche. Les options disponibles pour les sources de données sont les suivantes : ○ **Sources de données - Toutes** : ce qui signifie que la règle s'applique à tous les types de sources de données telles que les flux Renseignements sur les menaces, les enregistrements Import Intel–

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ligence, les sources d'API (par exemple, les observables créés à partir de l'API), les éléments envoyés par SIR (observables envoyés par SIR) et diverses entités créées manuellement par les utilisateurs dans la bibliothèque Renseignements sur les menaces. ○ **Sources de données : flux de Renseignements** sur les menaces : correspond aux règles d'extraction qui ne s'appliquent qu'aux flux de renseignements sur les menaces. ○ **Sources de données : sources API** : correspond aux règles d'extraction qui ne s'appliquent qu'aux sources API. ○ **Intégrations de recherche de menaces** : pour ce type d'option, la règle d'extraction s'applique à toutes les intégrations de recherche de menaces telles que Virustotal. **Remarque :** ▪ Lorsque vous sélectionnez cette option, vous devez saisir le nom du fournisseur pour la recherche de menace. Les noms des fournisseurs ne sont automatiquement renseignés que lorsque les intégrations de recherche de menaces sont installées à partir du ServiceNow magasin. ▪ Pour les sources de données Threat Intelligence, les règles d'extraction ne sont prises en charge que pour les types STIX, MISP et Flux personnalisé. ○ **Intégrations d'enrichissement d'observables** : pour ce type d'option, la règle d'extraction est applicable à toutes les intégrations d'enrichissement d'observables.
Type de flux de menaces	Les options disponibles pour le type de flux de menaces sont les suivantes : ○ **STIX(TAXII/HTTPS) :** option permettant de filtrer les flux de menaces du type de flux STIX TAXII ou HTTPS et de sélectionner les flux associés dans la recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **MISP** : option permettant de filtrer les flux de menaces du type de flux MISP et de sélectionner les flux associés en effectuant une recherche à l'aide de l'icône de recherche. ○ **Flux personnalisé** : option permettant de filtrer les flux de menaces du type de flux personnalisé et de sélectionner les flux associés en effectuant une recherche à l'aide de l'icône de recherche.
Flux	Sélectionnez une ou plusieurs intégrations de flux de menaces pour le type de flux sélectionné. **Remarque :** Si ce champ est laissé vide, toutes les intégrations de flux de menaces pour le type de flux sélectionné sont automatiquement prises en compte pour l'extraction.
Méthode d'extraction des tactiques et techniques MITRE ATT&CK	Option permettant de sélectionner la méthode d'extraction des tactiques et techniques MITRE ATT&CK. Les deux méthodes disponibles sont les suivantes : **a.** Utiliser Regex **b.** Utiliser un script
Méthode d'extraction : utiliser Regex	Cette méthode utilise une expression régulière qui permet aux analystes de menaces de définir un modèle avec une séquence de caractères pour effectuer la méthode d'extraction.
Regex de la tactique	Option permettant de fournir une expression régulière pour l'extraction du ou des ID de tactiques MITRE ATT&CK.
Technique de regex	Option permettant de fournir une expression régulière pour l'extraction du ou des ID de la technique MITRE ATT&CK.
Méthode d'extraction : utiliser un script	Cette méthode utilise un format de script pour effectuer l'extraction sur les résultats de recherche de la source observable, de la source de l'objet, de la source de l'indicateur ou de la menace ou de la source de menace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description

	Remarque :
	○ Cette méthode de script peut être utilisée pour extraire des tactiques et des techniques MITRE de l'enregistrement source de l'entité et lier les tactiques et techniques à l'enregistrement source de l'entité lui-même.
	○ Cette méthode de script peut être utilisée pour extraire des tactiques et techniques MITRE des résultats de recherche de menaces et lier les tactiques et techniques à l'enregistrement d'entité.
	L'exemple de script est affiché ci-dessous à titre de référence :
	`(function process(lookupResultRawData, recordGr, ruleGr, lookupResultGr) { /*********************************`
	`* - threatLookupResult: The raw data of the threat lookup result in stringified JSON format.`
	`* - recordGr: The GlideRecord of the observable record.`
	`* - ruleGr: GlideRecord of matched MITRE extraction rule`
	`*`
	`* Once you extracted MITRE tactic IDs and technique IDs,`
	`* then you can use this method to link the tactics and techniques to the observable record.`
	`*********************************/`
	`var utils = new MITREExtractionUtils();`
	`var parsedRawData =JSON.parse(lookupResultRawData);`
	`var mitreDataField = parsedRawData.mitre_data;`
	`var response = utils.extractMITREDataUsingRegex(mitreDataField,'TA[0-9][0-9][0-9][0-9]','T[0-9][0-9][0-9][0-9].[0-9][0-9][0-9]|T[0-9][0-9][0-9][0-9]');`
	`utils.addTacticTechniquesForLookup(response.tacticIds, response.techniqueIds, recordGr, ruleGr.getUniqueValue(), lookupResultGr);`
	`})(lookupResultRawData, recordGr, ruleGr, lookupResultGr);`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur **Activer** pour activer la règle d'extraction technique MITRE ATT&CK après avoir créé une règle.
   Si vous n'activez pas la règle d'extraction technique MITRE ATT&CK, la règle ne sera pas appliquée à l'enregistrement.

Remarque :

a. Sources de données : chaque fois que vous activez la règle d'extraction, la combinaison de sources de données et le type d'intégration ne doivent correspondre à aucune des règles d'extraction activées existantes. Si tel est le cas, l'application affiche un message d'erreur vous permettant de modifier les combinaisons existantes et de réactiver la règle.

b. Recherche de menaces : chaque fois que vous activez la règle d'extraction, le nom du fournisseur ne doit correspondre à aucune des règles d'extraction activées existantes. Si tel est le cas, l'application affiche un message d'erreur vous permettant de modifier le nom du fournisseur et de réactiver la règle.

c. Un exemple de règles d'extraction technique MITRE ATT&CK est mis en service pour les utilisateurs dans le système de base et ces règles seront désactivées par défaut et vous devez activer et activer la règle.

Champ	Description
Règle générique pour l'ingestion de sources de données	Il s'agit d'une règle générique pour l'ingestion à partir de tous les types de sources de données, y compris l'intelligence d'importation et la création manuelle.
Règle générique pour la recherche de menace	Il s'agit d'une règle générique pour toute intégration de recherche de menace.
Règle générique pour les intégrations d'enrichissement d'observables	Il s'agit d'une règle générique pour toutes les intégrations d'enrichissement d'observables.

5. Cliquez sur **Dupliquer** pour créer une copie de la règle d'extraction.
6. Cliquez sur **Désactiver** pour désactiver la règle d'extraction.

Remarque : Une fois désactivée, la règle ne sera plus prise en compte pour l'extraction de données MITRE.

7. Cliquez sur **Enregistrer**.
8. Cliquez sur **Supprimer** si vous souhaitez supprimer toute règle d'extraction technique MITRE ATT&CK.

Méthode d'extraction technique MITRE ATT&CK

La méthode d'extraction de la technique MITRE ATT&CK décrit comment les méthodes d'extraction sont effectuées et les techniques associées sont vérifiées.

1. Les règles d'extraction pour les sources de données (les recherches de menaces ne sont pas applicables) sont traitées chaque fois qu'un enregistrement source d'entité (par exemple, source d'observable ou source objet) est créé.
2. Les règles s'appliquent à tous les champs de l'enregistrement source de l'entité (à l'exception des champs de date, de nombre, de catégorie d'utilisation et des phases d'attaque).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Les techniques MITRE extraites sont associées à l'enregistrement d'entité correspondant et vous affichez les enregistrements dans la liste connexe des techniques MITRE dans l'onglet **Enregistrements connexes** .

> **Remarque :** Les techniques MITRE sont d'abord extraites et associées à l'enregistrement source de l'entité, puis les associations de techniques sont dédupliquées et regroupées à l'enregistrement d'entité parent.

Afficher les techniques MITRE

1. Accédez à la **Bibliothèque de Renseignements sur les menaces**tout enregistrement d'entité (observable ou objet) utilisant le fichier .
2. Cliquez sur l'onglet **Enregistrements connexes** .
3. Sélectionnez **Techniques MITRE** et affichez les techniques associées qui sont extraites.
4. Cliquez sur l'ID de la technique MITRE pour afficher et accéder à l'enregistrement d'association de la technique MITRE. La colonne **Sources** affiche toutes les sources (également séparées par une virgule s'il existe une ou plusieurs sources) qui sont associées à l'enregistrement source de l'entité sur lequel l'extraction MITRE est effectuée.

> **Remarque :** Si les mêmes ID de tactiques et de techniques sont extraits de plusieurs sources, un seul enregistrement d'association de tactiques et de techniques s'affiche et la colonne **Sources** affiche toutes les sources extraites.

5. Pour le dépannage, vous pouvez afficher la règle d'extraction MITRE responsable de l'extraction des associations de tactiques et de techniques en accédant aux **relations sources** de techniques.

> **Remarque :** Assurez-vous d'ajouter la colonne **Règle d'extraction** à l'aide de l'icône **Actions de liste** au cas où vous ne verriez pas la colonne Règle d'extraction.

Les règles d'extraction pour les recherches de menaces sont traitées chaque fois que l'enregistrement de résultat de la recherche de menace est créé pour tout observable pour lequel **l'action Exécuter la recherche de menaces** est déclenchée et l'extraction est effectuée uniquement sur la charge utile des données brutes (champ raw_data) qui est disponible dans l'enregistrement de résultat de la recherche de menace.

> **Remarque :**
>
> - Si aucun ID de tactique n'est présent dans la source de l'entité extraite (observable ou objet) ou dans le résultat de recherche de menace pour une technique MITRE ATT&CK, les associations de techniques sont créées pour toutes les tactiques associées à la technique correspondante dans le référentiel MITRE.
> - Si un ID de tactique est présent dans la source de l'entité extraite (observable ou objet) ou le résultat de recherche de menace pour une technique MITRE ATT&CK, les associations de techniques sont spécifiquement créées uniquement pour toutes les tactiques extraites associées à la technique correspondante dans le référentiel MITRE.

Définition des listes de contrôle de sécurité

Utilisez cette fonctionnalité pour ajouter ou supprimer des observables en bloc.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Accéder à **Listes des contrôles de sécurité**.
   Par exemple, ajouter des observables à la liste d'autorisation, puis accéder à l'option Liste d'autorisation.
3. Sélectionnez **Liste d'autorisation**.
4. Sélectionnez le type d'observables à ajouter à la liste d'autorisation, par exemple Adresse IP, Fichier, etc.
5. Cliquez sur **Ajouter**.
   La **liste Sélectionner des observables pour l'autorisation** s'affiche.
6. Sélectionnez tous les observables qui doivent être ajoutés à la liste d'autorisation.
7. Cliquez sur **Ajouter à la liste d'autorisation**.
   Les observables sélectionnés sont ajoutés.
8. De même, sélectionnez **Ajouter à la liste de refus** pour ajouter les observables à la liste supprimée.
9. Sélectionnez **Ajouter à la liste de surveillance** pour ajouter les observables à la liste de surveillance.

   Remarque : Vous pouvez ajouter directement les observables à la liste d'autorisation, à la liste de refus ou à la liste de surveillance directement à partir de la page de vue du formulaire Observables, qui sont disponibles au-dessus de la bannière du formulaire.

10. Pour vérifier, accédez à la **bibliothèque de Renseignements sur les menaces**.
11. Sélectionnez le type d'observable qui a été ajouté à la liste d'autorisation.
    L'observable est indiqué comme ajouté à la liste d'autorisation.

    Remarque : La liste d'autorisation et la liste de refus s'excluent mutuellement et le système s'assure automatiquement qu'un observable figurant dans la liste d'autorisation ne figure pas dans la liste de refus et vice-versa.

Création de taxonomies

Créez des taxonomies pour les enregistrements de source de données.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration** > **Taxonomies**.
2. Cliquez sur **Nouveau**.
3. Entrez le **nom**.
4. Activer ou désactiver **l'état** de taxonomie à l'aide des actions de formulaire Activer ou désactiver.

   Remarque : Les taxonomies désactivées ne seront pas disponibles pour la sélection d'enregistrements où des taxonomies sont applicables.

5. Accédez à la section **Valeurs de taxonomie** pour ajouter des valeurs de taxonomie.
6. Cliquez sur **Nouveau** pour ouvrir une nouvelle vue de formulaire de valeur de taxonomie et entrez la **taxonomie** et la **valeur**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Enregistrer**.
8. Par exemple, accédez à **Bibliothèque de Renseignements sur les menaces** > **Observables** pour vérifier les taxonomies de l'enregistrement des observables.
9. Accédez à la section **Balises et taxonomies** sur n'importe quelle page de formulaire d'observable et sélectionnez la taxonomie nouvellement créée.

Remarque : Vous pouvez également ajouter des balises et des taxonomies à partir de la vue de liste de la bibliothèque Renseignements sur les menaces.

Importer taxonomies en bloc

Importez les enregistrements de taxonomie.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez importer les taxonomies à l'aide des données de la feuille de calcul. Cela vous permet d'importer plusieurs enregistrements en bloc.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration** > **Taxonomies**.
2. Sélectionnez **le bouton Importer** .
   Cette action ouvre une action pour importer le fichier de données au format XLSX ou CSV. Vous pouvez également télécharger le fichier d'exemple pour comprendre le format à importer. Le format de fichier contient deux valeurs qui incluent Taxonomie et Valeur de taxonomie.
3. Cliquez sur **Ajouter un lien de fichier** .
4. Sélectionnez le fichier et **chargez-le**.
5. Cliquez sur **Terminé**.
   Un message de confirmation indique que les données du fichier joint ont été importées avec succès. Vous pouvez cliquer sur le lien pour afficher le résumé de l'importation. En cliquant sur le lien, l'enregistrement s'ouvre dans un nouvel onglet. Vous pouvez afficher le nombre de taxonomies et de valeurs de taxonomie créées. Si des erreurs sont enregistrées, elles sont enregistrées dans la section des erreurs d'importation.

   Remarque : Par défaut, toutes ces taxonomies et valeurs de taxonomie sont créées avec l'état Activé. Si vous souhaitez le désactiver, vous pouvez toujours le faire à partir de la vue de liste.

6. Sur la page **Taxonomies** , vous pouvez cliquer sur n'importe quel enregistrement. Cette action affichera les valeurs de taxonomie sous forme d'un onglet distinct et vous pourrez voir les deux valeurs de taxonomie importées avec succès, et ces valeurs de taxonomie seront à l'état activé.
7. En outre, pour afficher l'une des importations de taxonomie, vous pouvez toujours accéder à la section **Importations** . Les taxonomies importées sont affichées dans la section **Importations de taxonomie** .
8. Cliquez sur **Toutes les importations** pour afficher toutes les importations de taxonomie créées par différents utilisateurs dans l'application.
9. Cliquez sur **Mes importations** pour afficher les importations de taxonomie de l'utilisateur connecté actuel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion du calculateur de réputation de la recherche de menaces

Vous pouvez utiliser le calculateur de résultats de recherche de menaces pour calculer les résultats observables en fonction des réponses reçues du fournisseur de recherche de menaces.

Vous pouvez créer un calculateur de résultats de recherche de menaces pour votre intégration et utiliser un script pour déterminer comment vous souhaitez identifier les différents résultats observables. Le calculateur de résultats de recherche de menace comprend un exemple de script fourni avec le système de base, que vous pouvez utiliser pour identifier les résultats observables ou modifier ce script en fonction de vos besoins.

Pour les intégrations tierces qui fournissent les résultats calculés, le calculateur de résultats de la recherche de menace mappe les résultats aux conclusions prises en charge dans le système de base.

Résultats de la recherche de menace de déploiement

Lorsque vous disposez de plusieurs résultats de recherche de menaces pour un observable provenant des différents fournisseurs d'intégration, les résultats de la recherche de menaces récente de tous les fournisseurs sont pris en compte et les résultats globaux de l'observable sont marqués comme suit :

Déployer les conclusions de la recherche de menace

Dernier résultat observable	Résultat global de l'observable
Malveillant	Si l'un des fournisseurs de l'intégration signale l'observable comme malveillant, le résultat global de l'observable est marqué comme malveillant.
Suspect	Si aucun des fournisseurs d'intégration ne signale l'observable comme malveillant, l'un d'eux le signale comme suspect, puis le résultat observable global est marqué comme suspect.
Nettoyer	Si tous les fournisseurs de l'intégration signalent l'observable comme Propre, le résultat global de l'observable est marqué comme Propre.
Inconnu	Si aucun des fournisseurs d'intégration ne signale l'observable comme malveillant ou suspect et que l'un d'eux le signale comme inconnu, le résultat global de l'observable est marqué comme inconnu.

Afficher les calculateurs de réputation de la recherche de menace

Vous pouvez consulter le calculateur de recherche de menaces pour déterminer comment la réputation de l'observable est calculée en fonction de la réponse d'un fournisseur de recherche de menaces spécifique.

Rôle requis : sn_sec_tisc.admin

Pour afficher le calculateur de réputation de la recherche de menaces, procédez comme suit :

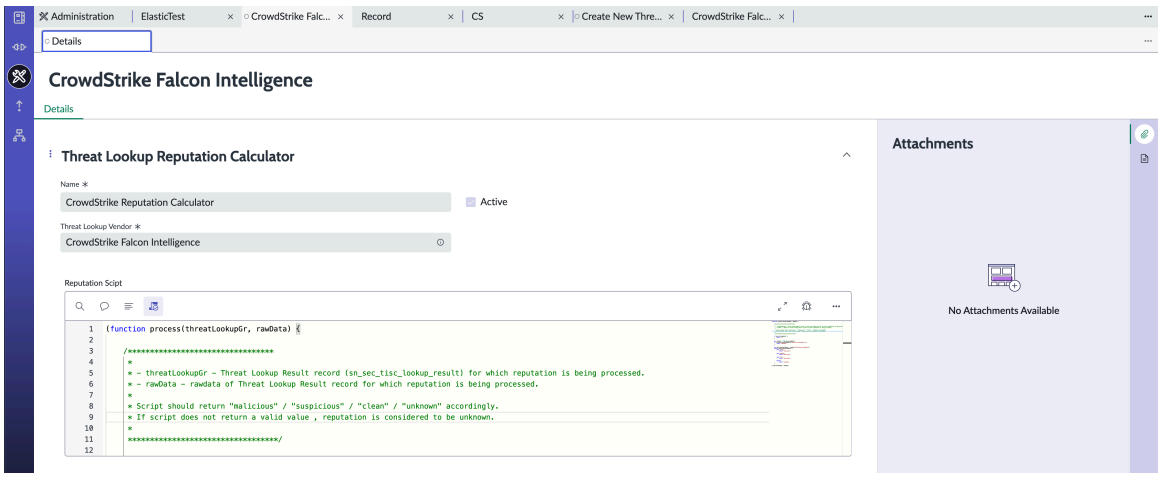
1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionnez la section **Calculateur de réputation de la recherche de menaces** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez consulter la liste des calculateurs de réputation de la recherche de menaces.

3. Cliquez sur le calculateur de réputation de la recherche de menaces requis pour afficher les détails du calculateur.



Créer un calculateur de réputation de la recherche de menaces

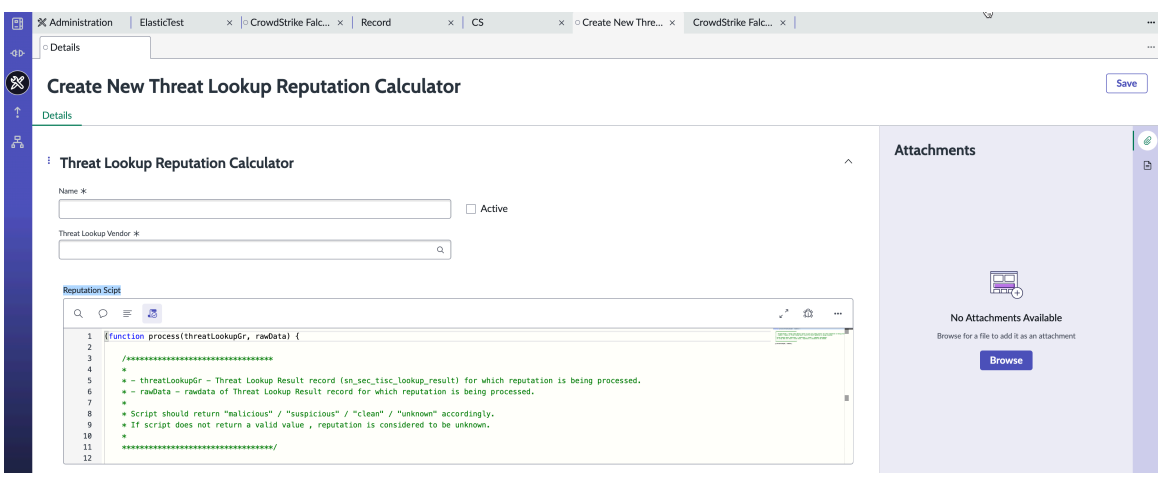
Rôle requis : sn_sec_tisc.admin

Remarque : Un seul calculateur de recherche de menaces peut être actif à tout moment par fournisseur de recherche de menaces.

Pour créer un calculateur de réputation de la recherche de menaces, procédez comme suit :

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionnez la section **Calculateur de réputation de la recherche de menaces** .

   Vous pouvez consulter la liste des calculateurs de réputation de la recherche de menaces.
3. Pour créer un calculateur de réputation de la recherche de menaces, cliquez sur **Nouveau**.



4. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un calculateur de réputation de la recherche de menaces

Champ	Description
Nom	Nom du calculateur de réputation de la recherche de menaces.
Actif	Le calcul de la recherche de menace ne s'exécute que si l'option Actif est sélectionnée.
Fournisseur de la recherche de menace	Nom du fournisseur de recherche de menaces. Par exemple, CrowdStrike Falcon Intelligence.
Script de réputation	Éditeur de script pour déterminer comment vous souhaitez identifier les différents résultats observables. Chaque intégration de recherche de menaces est accompagnée d'un script de base pour calculer la réputation de la recherche de menaces.

5. Cliquez sur **Enregistrer**.

Gérer les notifications par e-mail

Utilisez ServiceNow Notifications pour créer et gérer des notifications par e-mail système, et afficher les journaux d'e-mail.

Notifications par e-mail

Utilisez les notifications par e-mail pour envoyer aux utilisateurs sélectionnés des notifications par e-mail sur des tâches spécifiques au sein de l'application, telles que les mises à jour des observables/indicateurs/divers autres objets.

Rôle requis : admin

Remarque : En tant qu'administrateur système, vous pouvez afficher, créer ou modifier les détails de la règle de notification par e-mail dans la vue classique de l'application.

Centre de sécurité des renseignements sur les menaces Fournit des notifications par e-mail basées sur des règles qui sont envoyées à des adresses e-mail individuelles ou à une liste d'adresses e-mail. Habituellement, la diffusion d'informations de Renseignements sur les menaces aux utilisateurs internes est généralement envoyée sous la forme d'un e-mail. Le processus consiste à fournir les données Threat Intelligence aux utilisateurs selon leur format et leurs chronologies spécifiés.

Les notifications par e-mail permettent aux administrateurs de spécifier :

- La période d'envoi de la notification
- Qui reçoit la notification
- Quel est le contenu de la notification

Remarque : Si vous souhaitez apporter des modifications, vous devez configurer le destinataire de l'envoi de l'e-mail en modifiant les règles du système de base en fonction de vos besoins.

Pour plus d'informations, consultez la section Créer une notification par e-mail dans la Administration de ServiceNow AI Platform documentation.

Traduction automatique

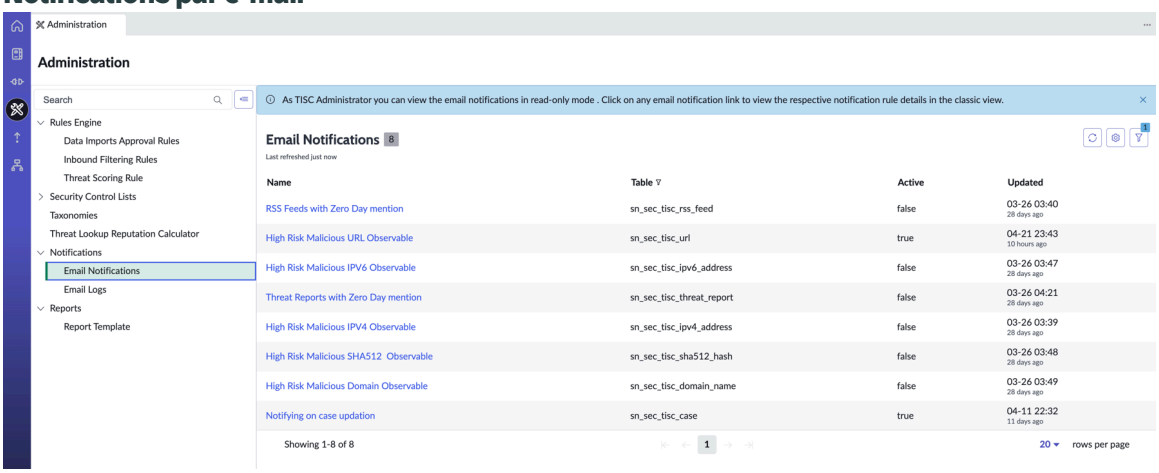
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le tableau suivant détaille les règles de notification par e-mail mises en service dans le système de base.

Notifications par e-mail

Nom	Table
Flux RSS avec mention Zero Day	sn_sec_tisc_rss_feed
Observable d'URL malveillante à risque élevé	sn_sec_tisc_url
Observable IPV6 malveillant à haut risque	sn_sec_tisc_ipv6_address
Rapports de menace avec mention Zero Day	sn_sec_tisc_threat_report
Observable IPV4 malveillant à haut risque	sn_sec_tisc_ipv4_address
Observable SHA512 malveillant à haut risque	sn_sec_tisc_sha512_hash
Observable de domaine malveillant à haut risque	sn_sec_tisc_domain_name
Notification lors de la mise à jour du ticket	sn_sec_tisc_case

Notifications par e-mail



Remarque : Cliquez sur chaque notification par e-mail pour accéder à l'interface utilisateur classique, afin que vous puissiez effectuer les actions nécessaires, telles que l'affichage, la modification ou la création de notifications.

Journaux d'e-mails

Cette section fournit une visibilité claire aux administrateurs TISC sur les e-mails envoyés à l'aide des règles de notification par e-mail configurées.

Notifications par e-mail et vue des journaux

TISC offre différentes latitudes pour accéder, afficher ou modifier les notifications par e-mail et les journaux en fonction de différents profils.

Remarque :

Profil	Niveaux d'accès
Administrateur TISC (sn_sec_tisc.admin)	En tant que sn_sec_tisc.admin, vous ne pouvez afficher que les notifications par e-mail configurées pour TISC.

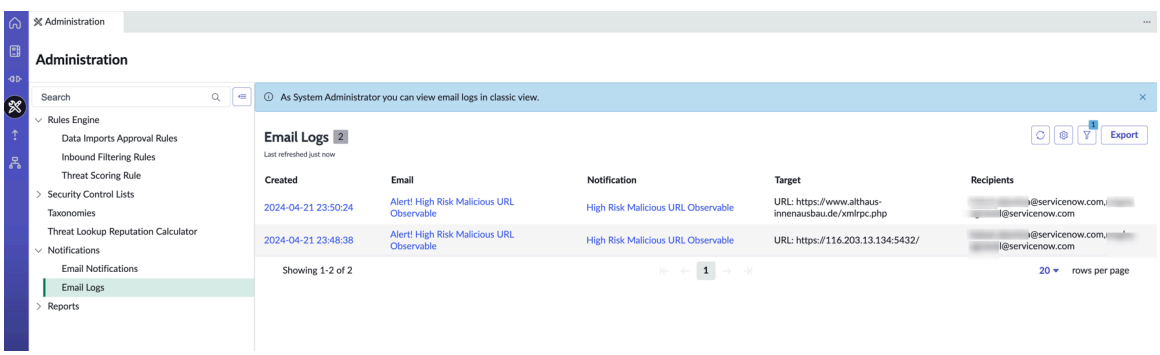
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Profil	Niveaux d'accès
	Remarque : Cliquez sur les liens hypertexte des journaux d'e-mails pour accéder à l'interface utilisateur classique et afficher ces notifications.
Administrateur système (admin)	En tant qu'administrateur, vous pouvez créer, afficher et modifier les notifications dans l'interface utilisateur classique. **Remarque :** Cliquez sur les liens hypertexte des journaux d'e-mails pour accéder à l'interface utilisateur classique afin d'afficher et de créer ces notifications.

Remarque : L'administrateur TISC et l'administrateur système peuvent tous deux utiliser les filtres et rechercher les journaux d'e-mails.

Journaux d'e-mails



Modèles de rapports

Définit la possibilité de réutiliser les modèles de rapport qui peuvent être partagés au sein du groupe d'utilisateurs pour générer des rapports rapidement et de façon cohérente.

Utilisez cette fonctionnalité pour créer différents types de modèles de rapport, qui peuvent être appliqués à un ou plusieurs tickets qui fournissent l'état de l'enquête en cours en fonction de toute menace pour votre organisation et aident à générer des rapports à ce sujet.

Cette section explique comment implémenter la génération de rapports CTI au niveau d'un ticket et fournit également des expériences d'administrateur (conception de modèle) et d'analyste (exécution).

Vous pouvez ajouter au modèle de rapport des champs de formulaire de tâche de ticket personnalisés ou des listes connexes accessibles par points. En outre, vous pouvez formater et configurer le rapport en fonction de vos besoins à l'aide de divers éléments de rapport.

Rôle requis : sn_sec_tisc.admin

Le tableau suivant explique quelques modèles de rapport qui sont mis en service dans le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modèle de rapport

Nom	Description
Rapport de statut de ticket : profil de l'acteur de menace	Le rapport est conçu pour fournir un état d'avancement de l'enquête en cours sur un cas lié à un acteur malveillant qui tente de comprendre le contexte et la pertinence de la menace pour l'organisation, le comportement et les objectifs potentiels de l'adversaire, l'enrichissement de la COI, les logiciels malveillants et outils associés, les TTP observés, la différence par rapport aux TTP existants – nouvelles capacités nettes, légères modifications, etc.
Résumé du cadre	Le rapport est conçu pour informer les principaux décideurs d'un risque particulier. L'accent est mis sur les publics de cadres et sur les problèmes stratégiques expliquant pourquoi et comment, plutôt que quoi et quand. Les détails techniques et les annexes à l'appui de l'écriture narrative de longue durée ne seront pas inclus dans le présent rapport.
Publier la synthèse d'examen : profil de l'acteur de menace	Le rapport est conçu pour fournir le contexte et la pertinence de la menace pour l'organisation ; le comportement de l'adversaire et les objectifs potentiels ; l'enrichissement de la COI ; Logiciels malveillants et outils associés ; TTP observés ; Différence avec les TTP existants : nouvelles capacités nettes, légères modifications, etc.

Remarque : Par défaut, ces rapports sont à l'état Publié et seront en mode lecture seule. Comme les modèles de rapport seront en mode lecture seule, les utilisateurs ne pourront pas apporter de modifications aux modèles et les analystes ne pourront pas générer les rapports car les modèles de rapport seront désactivés.

Créer un nouveau modèle de rapport

Créez un nouveau modèle de rapport de ticket en fonction des besoins professionnels de votre organisation.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Rapports** > **Modèle de rapport**.
   Cette section affiche les modèles disponibles dans le système de base, ainsi que les modèles publiés. Vous pouvez choisir n'importe quel modèle de votre choix pour travailler avec les rapports.

   Remarque : Dans cette section, vous pouvez également supprimer les modèles, si nécessaire.
3. Cliquez sur **Nouveau**.
4. Saisissez le nom et la description du modèle.
5. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La section Contenu du modèle s'affiche.

Remarque : Chaque fois que vous créez un nouveau modèle de rapport, le modèle sera à l'état de brouillon, ce qui signifie que la création du modèle est un travail en cours et que tout autre utilisateur ne sera pas en mesure d'afficher le modèle de rapport tant qu'il n'aura pas été terminé.

6. **Développez le contenu du modèle** pour insérer les champs souhaités dans le corps du modèle.

Remarque :

- Le modèle que vous modifiez vous permet de définir le corps du modèle et de sélectionner les variables requises à ajouter à la section de l'éditeur de modèle. Les modèles sont pris en charge par l'éditeur de texte enrichi (RTE) afin que vous puissiez contrôler diverses fonctions disponibles telles que l'indentation, la taille de police, créer des tableaux, ajouter des images et diverses autres capacités de formatage.
- Vous pouvez également insérer des images dans vos modèles de rapport, pour cela vous devez copier et coller l'image directement dans le modèle. Lorsque vous ajoutez une image, cette image est téléchargée en tant que pièce jointe.
- Vous pouvez télécharger ou joindre une image jusqu'à 698 pixels, si l'image est au-dessus de la taille définie, elle sera automatiquement ajustée à la taille d'origine. Cette restriction de la taille des pixels aidera la génération de rapports PDF à s'afficher dans un format approprié et les images ne seront pas tronquées dans le rapport.

7. Ajoutez les éléments requis du ticket.
8. Cliquez sur **Enregistrer le contenu** pour enregistrer le contenu de votre nouveau modèle de rapport.
9. Cliquez sur **Aperçu** pour prévisualiser le format de votre rapport et pour voir comment un rapport est généré lorsque vous générez un rapport de ticket.

Remarque :

- **Champs de ticket** : chaque fois que vous modifiez votre ou vos modèles de rapport, prévisualisez le contenu ajouté au modèle. Par exemple, lorsque vous générez un rapport de ticket et que vous souhaitez ajouter un champ appelé Description brève, vous pouvez sélectionner ce champ dans les champs Ticket, puis ce champ est ajouté en tant que variable dans le modèle de rapport. Lorsqu'un rapport est généré pour l'analyste, quelle que soit la description, cette description sera affichée dans le rapport.
- **Enregistrements** : dans le modèle de rapport, vous pouvez également ajouter les enregistrements connexes de ce ticket particulier qui s'affichent en tant qu'artefacts du ticket. Par exemple, si vous souhaitez voir des observables malveillants dans le rapport à partir des listes connexes Observables, vous pouvez les ajouter à votre modèle de rapport. Ces enregistrements connexes sont affichés au format de table
- **Scripts** : chaque fois que vous souhaitez voir la date et l'heure du rapport, vous pouvez ajouter les scripts **de date/heure actuelles** à votre modèle de rapport, ce qui ajoutera la date et l'heure de création du rapport.
- **MITRE ATT&CK** : affiche les techniques associées à la carte MITRE dans votre rapport.

Une fois que vous avez ajouté tous les champs requis liés au ticket à votre modèle de rapport, vous devez publier votre modèle de rapport.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Cliquez sur **Publier** pour publier le modèle.
    Un message de confirmation s'affiche si vous souhaitez publier le modèle de rapport.

    Remarque : Lorsque vous publiez un modèle de rapport, ce modèle est activé pour tous les utilisateurs. S'il est obsolète et que vous souhaitez restreindre l'affichage du rapport pour les utilisateurs, vous pouvez désactiver le rapport publié, ce qui signifie que le modèle de rapport sera masqué pour les utilisateurs. Vous devez réactiver le rapport publié pour que les utilisateurs puissent le voir et l'utiliser jusque-là.

11. Cliquez sur **Supprimer** pour supprimer le modèle de rapport au cas où vous ne le voudriez pas.
    Si vous souhaitez renommer votre modèle de rapport, cliquez sur **Modifier** et modifiez les champs souhaités.

Propriétés système pour les rapports

Les propriétés système des rapports sont expliquées ci-dessous.

Propriété	Description	Valeur
sn_sec_reporting.max_colonnes_liste_autorisé	Limite le nombre de colonnes pouvant être ajoutées lors du rendu des listes dans les pdf de rapport. Cela utilisera les colonnes depuis le début, de la vue jusqu'à la limite autorisée.	5
sn_sec_reporting.report_default_style_object	Utilisez cette propriété pour contrôler le css des champs de formulaire libre, du panneau de gauche, des listes de rapports.	(objet JSON)
sn_sec_reporting.load_all_records	Charge tous les enregistrements des listes du rapport créé à partir d'un modèle. true : charge tous les enregistrements et false : charge un nombre spécifique d'enregistrements défini par la propriété sn_sec_reporting.reporting_list_records_count.	Faux
sn_sec_reporting.reporting_list_records_count	Charge un nombre spécifique d'enregistrements dans l'éditeur de rapports.	20
sn_sec_tisc.sn_sec_tisc_case.defang_control_list	Contrôle si les URL des listes sont neutralisées ou non.	Vrai
sn_sec_tisc.show_all_tactics_reporting	Si vrai, affiche toutes les tactiques (y compris celles qui n'ont aucune technique associée au ticket) pour les listes MITRE rendues dans le rapport.	Faux
sn_sec_tisc.reporting_email_template_sys_id	ID système du modèle de client de messagerie pour la table Ticket (sn_sec_tisc_case) qui sera utilisé dans le rapport de partage.	B55E22C54324021060EEE0ea78B8F2DF

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur
sn_sec_tisc.sn_sec_tisc_case.excluded_ta_fields	Champs exclus du ticket dans le menu rapport/modèle options de substitution d'un champ.	(Liste de tous les champs de tickets exclus
sn_sec_tisc.sn_sec_tisc_case.ctx_menu_field_header	Cette propriété est utilisée pour obtenir l'enregistrement du message d'interface utilisateur correspondant pour l'étiquette des champs du ticket dans les options de menu rapport/modèle.	sn_sec_tisc_case_reporting_ctx_menu_field_header

Modifier un modèle de rapport publié

Utilisez cette section pour modifier un modèle de rapport publié.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Rapports** > **Modèle de rapport**.
3. Sélectionnez le modèle de rapport requis.
4. Sélectionnez le bouton **Modifier** qui s'affiche sur le modèle de rapport.

Remarque :

Un message de confirmation s'affiche indiquant que vous modifiez un modèle publié et que vous devez republier le modèle pour le rendre disponible sous Rapports de tickets. Voulez-vous continuer la modification ? Cela signifie que vous devez republier le modèle modifié après avoir apporté les modifications nécessaires.

5. Sélectionnez **Modifier** dans la boîte de dialogue de confirmation.
6. Apportez les changements nécessaires en ajoutant les champs de contenu requis ou la liste connexe.
7. Sélectionnez **Enregistrer le contenu**.
8. Sélectionnez le bouton **Publier** pour publier les changements.
   Une fois le modèle de rapport publié, un message de confirmation s'affiche et indique que le modèle de rapport a été publié avec succès.

Remarque :

- Vous pouvez également prévisualiser le contenu du modèle de rapport avant de publier le modèle de rapport.
- Si vous souhaitez supprimer le modèle de rapport, vous pouvez sélectionner **Supprimer** pour supprimer le modèle de rapport.

Dupliquer un modèle de rapport

Dupliquer un modèle de rapport Si vous souhaitez ajouter des mises à jour incrémentielles, vous pouvez créer une copie du modèle de rapport.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > > **Administration**.
2. Sélectionner **Rapports** > **Modèle de rapport**.
3. Sélectionnez le modèle.
4. Cliquez sur **Dupliquer**.
   Les contenus du modèle sélectionné sont dupliqués et une copie de ce modèle est affichée. Le modèle sera à nouveau à l'état Brouillon, vous pourrez personnaliser le contenu, puis renommer le modèle selon vos besoins.
5. Modifiez ou modifiez le contenu du modèle copié.

Remarque : Vous pouvez également supprimer les modèles de rapport si vous n'en avez plus besoin et créer de nouveaux modèles.

Utilisation des webhooks

Un webhook est une requête HTTP déclenchée par un événement dans le système source (TISC) et envoyée à un système de destination (où se trouve l'URL du point de terminaison), avec une charge utile de données d'événement.

Ces webhooks sont Centre de sécurité des renseignements sur les menaces utiles pour avertir l'application de destination chaque fois que les événements se produisent.

Dans TISC, vous pouvez effectuer les opérations suivantes :

- Configurer les webhooks
- Gérer les déclencheurs
- Mécanisme de nouvelle tentative
- Effectuer la validation
- Gérer les abonnements

Propriétés système pour les webhooks

Les propriétés système des webhooks sont expliquées ci-dessous.

Nom de la propriété	Description	Type	Valeur
sn_sec_tisc.webhook_ignore_threat_score_recalculate	Ignorer les événements de webhook déclenchés par le score de menace Recalculez l'historique.	Vrai/Faux	Vrai
sn_sec_tisc.webhook_max_event_batch_size	Nombre maximal d'événements à envoyer dans le cadre d'une demande de webhook. La taille du lot est limitée à 2 000 même si une valeur plus élevée est définie dans cette propriété.	Entier	1 000

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété	Description	Type	Valeur
sn_sec_tisc.webhook_retry_count	Nombre de fois qu'une demande ayant échoué doit être réessayée avant de la marquer comme erreur et de passer au lot d'événements suivant. Le nombre de nouvelles tentatives est limité à 10 même si un nombre plus élevé est défini dans cette propriété.	Entier	5
sn_sec_tisc.webhook_retry_interval	Nombre de secondes à attendre avant de retenter un lot ayant échoué. Cette valeur augmentera de façon exponentielle en fonction du nombre de nouvelles tentatives. Par exemple, si retry_count est 3 et retry_interval est 30, les nouvelles tentatives sont déclenchées après 30, 60 et 120 s. L'intervalle entre les tentatives initiales est limité à 300 secondes, même si une valeur plus élevée est définie dans cette propriété.	Entier	30

Traduction automatique

Configurer les webhooks

Configurez un webhook pour vous abonner aux événements dans Centre de sécurité des renseignements sur les menaces.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche

Les webhooks TISC offrent la possibilité de s'intégrer à des outils de sécurité tels que SIEM. Les utilisateurs peuvent ensuite s'abonner à divers événements liés à différents artefacts tels que des observables ou des indicateurs, des programmes malveillants ou des acteurs malveillants. TISC notifie les outils de sécurité (tels que SIEM) lorsqu'une nouvelle connaissance des menaces est disponible ou que des données de Threat Intelligence existantes sont mises à jour ou supprimées dans TISC.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, chaque fois qu'un nouvel observable est ajouté à Threat Intelligence, une demande de charge utile est envoyée à la configuration de l'URL Webhook. Cette demande de charge utile collecte généralement les informations observables et les fournit en tant qu'informations supplémentaires aux outils de sécurité (tels que SIEM).

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Webhooks**.
   La page Webhooks s'affiche.
3. Cliquez sur **Nouveau**.

Champ	Description
Nom	Saisissez un nom de webhook.
Description	Ajoutez la description du webhook.
Détails de la configuration	
Utiliser le message REST	Cochez la case **Utiliser le message REST** si vous devez utiliser la fonctionnalité de message REST/de méthode REST fournie par ServiceNow AI Platform. Si cette case n'est pas cochée, l'application utilise le point de terminaison fourni dans l'URL Webhook pour envoyer les informations sur l'événement. Pour plus d'informations, consultez Service Web REST sortant dans la ServiceNow AI Platform documentation.
Message REST	Sélectionnez l'enregistrement du message REST dans la liste des enregistrements du message REST déjà configurés dans l'instance. Pour plus d'informations, consultez Service Web REST sortant dans la ServiceNow AI Platform documentation. **Remarque :** Les champs Message REST et Méthode REST sont obligatoires lorsque vous sélectionnez le message REST.
Méthode REST	Sélectionnez Méthode REST dans la liste des méthodes REST disponibles configurées pour le message REST sélectionné. Pour plus d'informations, consultez Service Web REST sortant dans la ServiceNow AI Platform documentation. **Remarque :** Seules les méthodes POST Rest sont prises en charge pour les webhooks.
URL Webhook	Un point de terminaison Webhook est une URL qui reçoit des notifications d'événements webhook.
Authentification requise	Cochez cette case si l'authentification est requise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Cela ne s'applique que lorsque l'URL Webhook est utilisée pour récupérer les données.
Type d'authentification	Le type d'authentification pour le webhook. **Remarque :** Pour l'instant, seul le type d'authentification de base est pris en charge.
Nom d'utilisateur	Fournissez un nom d'utilisateur à votre type d'authentification.
Mot de passe	Fournissez un mot de passe pour votre type d'authentification.
En-têtes à transmettre avec la demande	Tous les en-têtes à transmettre avec les demandes peuvent être fournis dans le mappage d'en-tête de demande. L'en-tête doit être fourni dans une paire clé-valeur séparée par deux-points (« : »). Chaque paire clé-valeur d'en-tête doit être fournie dans une nouvelle ligne. Pour fournir des paramètres d'authentification en tant que valeurs d'en-tête, encadrez l'étiquette d'authentification requise avec « ${ » et « }$ ». Par exemple, nom d'utilisateur :${Nom d'utilisateur}$.

4. Cliquez sur **Valider et enregistrer**.
   Si les détails de votre configuration sont incorrects, le système validera automatiquement la connexion si les détails de configuration sont modifiés, puis l'application affichera un message d'avertissement indiquant que la validation du webhook a échoué et que vous devez vérifier les détails de la configuration et les modifier en conséquence.

Remarque :

- Pour la validation du webhook, une charge utile de demande vide est envoyée au point de terminaison et l'utilisateur doit s'assurer que le point de terminaison envoie correctement le code de réponse (200) lorsque la demande vide est transmise au point de terminaison webhook configuré.
- Par défaut, tout webhook créé sera à l'état Désactivé. Vous devez activer le webhook et l'activer. Un exemple de webhook est mis en service dans le système de base en tant que référence aux utilisateurs.

S'abonner aux déclencheurs

Affichez la liste de tous les déclencheurs de webhook abonnés pour le webhook actuel.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Webhooks**.
   La page Webhooks s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez le webhook.
   La section Déclencheurs abonnés s'affiche.
4. Cliquez sur le bouton **S'abonner** dans la section Déclencheur abonné.
   La vue de liste affiche tous les déclencheurs de webhook activés dans l'instance.
5. Sélectionnez les déclencheurs de webhook souhaités et cliquez sur **S'abonner** dans la boîte de dialogue Déclencheurs de webhook.
   Un message de confirmation s'affiche indiquant que le webhook est abonné au ou aux déclencheurs sélectionnés. À partir de là, vous pouvez également créer directement un nouveau déclencheur et vous abonner au webhook.

> **Remarque :** Vous pouvez également **vous désabonner** du webhook du ou des déclencheurs sélectionnés.

Afficher les journaux d'erreurs de webhook

Utilisez cette section de journaux d'erreurs pour afficher toutes les entrées d'audit qui sont marquées comme erreur dans l'état d'un webhook particulier.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche
Les journaux d'audit permettent aux utilisateurs d'enquêter plus en détail, de déboguer l'exécution et d'identifier la cause première de l'échec de l'exécution.

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Webhooks**.
   La page Webhooks s'affiche.
3. Sélectionnez le webhook.
4. Accédez aux **journaux d'erreurs**.
5. Affichez les journaux d'erreurs.
   La vue de liste affiche tous les journaux d'erreurs d'un webhook particulier.
6. Accédez à la colonne **Lot** .
7. Cliquez sur n'importe quel **ID de lot**.

> **Remarque :** Chaque journal d'erreurs est associé à un lot et à l'aide de l'ID de lot (à partir de la colonne Lot), vous pouvez afficher l'enregistrement de lot associé. Cliquez sur l'un des ID du lot et cela s'ouvrira dans un onglet séparé. Chaque ID de lot contient le numéro de lot de webhook, le message d'erreur, le code d'état de la réponse, le nombre de nouvelles tentatives, les données de charge utile réelle et la liste des événements qui seront envoyés au webhook.

8. Cliquez sur **Réessayer le lot** pour réessayer les lots ayant échoué.
   Lorsque vous cliquez sur ce bouton, une charge utile de demande (de ce lot particulier d'informations) est envoyée au point de terminaison Webhook configuré.

> **Remarque :** Cette action n'est disponible que pour les enregistrements par lots qui comportent des erreurs d'exécution ou qui sont terminés avec succès et les enregistrements qui sont à l'état de nouvelle tentative seront automatiquement réessayés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les lots de webhooks

Un enregistrement par lots de webhook est créé pour chaque exécution de webhook.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche
Afin de réduire le nombre d'appels d'API envoyés aux points de terminaison de webhook, le traitement par lots des événements est implémenté dans les webhooks. Pour chaque webhook, si plusieurs événements sont déclenchés presque en même temps, tous ces événements sont envoyés dans le cadre de la même requête au point de terminaison webhook.

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Webhooks**.
   La page Webhooks s'affiche.
3. Sélectionnez le webhook.
4. Accédez aux **journaux d'erreurs**.
5. Affichez les journaux d'erreurs.
   La vue de liste affiche tous les journaux d'erreurs d'un webhook particulier.
6. Accédez à la colonne **Lot** .
7. Cliquez sur n'importe quel **ID de lot**.
   La page Lot de webhooks s'affiche.

Remarque : Tous les lots sont stockés dans la table `sn_sec_tisc_webhook_batch`.

Vous trouverez ci-dessous l'exemple de format de charge utile que le point de terminaison de webhook reçoit :


```
{
  "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
  "events": [
    {
      "record": "Observable",
      "record_fields": {
        "is_false_positive": "false",
        "reputation": "malicious",
        "sys_updated_on": "2024-07-22T14:31:26.000Z",
        "type": "url",
        "sys_updated_by": "admin",
        "sys_created_on": "2024-07-04T06:45:20.000Z",
        "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
        "is_defanged": "false",
        "sys_created_by": "SecCommon.System",
        "tags": "Enriched",
        "taxonomies": "T1: V1",
        "domain": "urlhaus.abuse.ch",
        "status": "active",
        "source_count": "1",
        "threat_score": "20",
        "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
        "value": "https://urlhaus.abuse.ch/url/2578255/",
```


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
            "confidence": "89",
            "expiration_time": "2025-10-07T07:13:18.000Z",
            "tlp": "CLEAR"
         },
         "trigger": {
            "name": "Observable Update",
            "type": "UPDATE",
            "trigger_time": "2024-07-22T14:31:26.000Z",
            "trigger_fields": [
               {
                  "field_name": "reputation",
                  "previous_value": null,
                  "current_value": "malicious"
               }
            ]
         }
      },
      {
         "record": "Observable",
         "record_fields": {
            "is_false_positive": "false",
            "reputation": "malicious",
            "sys_updated_on": "2024-07-22T14:31:19.000Z",
            "type": "url",
            "sys_updated_by": "admin",
            "sys_created_on": "2024-07-04T06:45:20.000Z",
            "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
            "is_defanged": "false",
            "sys_created_by": "SecCommon.System",
            "tags": "Enriched",
            "taxonomies": "T1: V1",
            "domain": "urlhaus.abuse.ch",
            "status": "active",
            "source_count": "1",
            "threat_score": "20",
            "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
            "value": "https://urlhaus.abuse.ch/url/2578264/",
            "confidence": "89",
            "expiration_time": "2025-10-07T07:13:18.000Z",
            "tlp": "CLEAR"
         },
         "trigger": {
            "name": "Observable Update",
            "type": "UPDATE",
            "trigger_time": "2024-07-22T14:31:19.000Z",
            "trigger_fields": [
               {
                  "field_name": "reputation",
                  "previous_value": null,
                  "current_value": "malicious"
               }
            ]
         }
      }
   ]
}
```


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La table suivante répertorie la structure de charge utile par lots et ses attributs qui seront envoyés aux utilisateurs en tant que charge utile webhook :

Paramètres dans la charge utile par lots	Type	Description
batch_id	Chaîne	Spécifie l'identificateur unique pour un lot.
Événements	Tableau d'objets	Contient un tableau d'événements qui sont déclenchés dans le cadre de ce webhook. Chaque événement contient l'instantané des valeurs de champ au moment de la génération de l'événement ainsi que les informations de déclenchement. **Remarque :** Pour plus d'informations sur l'affichage des paramètres dans l'objet d'événement, reportez-vous à la section Déclencheurs de webhook.

Remarque :

8. Cliquez sur le bouton **Réessayer le lot** pour réessayer le lot ayant échoué.

Remarque : Vous pouvez également déclencher le lot de nouvelles tentatives pour les lots terminés.

Déclencheurs de webhook

Les déclencheurs de webhook sont utilisés pour filtrer les entités Threat Intelligence qui doivent être suivies pour tout changement d'événement tel que Créer, Mettre à jour et Supprimer.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Webhooks Configurations** > **Déclencheurs**.
   La page Déclencheurs de webhooks s'affiche.
3. Cliquez sur **Nouveau**.

Champ	Description
Nom	Saisissez un nom de déclencheur de webhook.
Description	Ajoutez la description du déclencheur de webhook.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Table	Sélectionnez la table pour le déclencheur de webhook.
Type de déclencheur	Définit si le déclencheur de webhook configuré est un événement créer/mettre à jour/supprimer sur la table spécifiée. **Champs de déclencheur** : Cela s'affiche lorsque vous sélectionnez le **type de déclencheur : Mettre à jour**. Il s'agit de la liste des champs de l'enregistrement pour lesquels l'événement de mise à jour doit faire l'objet d'un suivi. Si ce champ est vide, l'événement est pris en compte pour tout changement de champ dans l'enregistrement. Par exemple, si les champs de déclencheur sont **Confiance** et **Réputation** pour la table **Observables** , ce déclencheur n'est pris en compte que lorsque les champs Confiance ou Réputation sont mis à jour. **Remarque :** Les champs sélectionnés dans les champs d'exclusion ne seront pas disponibles dans la sélection des champs de déclenchement. **Supprimer** : si le **type de déclencheur « Supprimer »**, les champs d'exclusion ne sont pas visibles.
Champs d'exclusion	Il s'agit de l'ensemble des champs qui sont exclus de la charge utile du déclencheur de webhook.
Conditions de filtre	Conditions facultatives qui peuvent être appliquées pour filtrer les enregistrements de correspondance pour n'importe quel déclencheur d'événement. Par exemple, si la gravité de la menace est élevée et que le type de déclencheur est défini sur Mettre à jour dans la table Observable, seuls les observables qui sont modifiés et où la gravité de la menace est élevée sont envoyés à l'URL Webhook.

4. Cliquez sur **Enregistrer**.
   Par défaut, le déclencheur est créé à l'état désactivé.
5. Cliquez sur **Activer** pour activer le déclencheur et ce déclencheur sera disponible pour que les webhooks s'abonnent.

   Remarque : Cliquez sur **Désactiver** pour désactiver le déclencheur activé et la désactivation désabonnera tous les webhooks associés de ce déclencheur.

6. Cliquez sur **Afficher l'exemple de charge utile** pour sélectionner l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichez l’exemple de charge utile de ce déclencheur de webhook particulier. En fonction de la table sélectionnée, les enregistrements de cette table spécifiée seront renseignés dans la liste déroulante **Sélectionner un enregistrement** . Sélectionnez l’enregistrement pour afficher l’exemple de charge utile. L’exemple de charge utile est affiché au format JSON. Les champs de la charge utile sont répertoriés ci-dessous.

7. Sélectionnez le type d’enregistrement dans la liste déroulante.
La charge utile sera automatiquement modifiée en fonction de l’enregistrement sélectionné.


```
{
   "record": "Observable",
   "record_fields": {
      "additional_context": "This could be a potential malicious IP. ",
      "attack_phases": "Lockheed Martin: Command and Control",
      "author": "Anomali",
      "confidence": "50",
      "description": "This could be a potential malicious IP. ",
      "expiration_time": "2024-12-01T00:00:00.000Z",
      "first_observed": "2024-01-01T00:00:00.000Z",
      "first_seen": "2024-01-01T00:00:00.000Z",
      "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
      "is_defanged": "false",
      "is_false_positive": "false",
      "last_observed": "2024-01-01T00:00:00.000Z",
      "last_seen": "2024-01-01T00:00:00.000Z",
      "reputation": "suspicious",
      "source_count": "1",
      "status": "active",
      "sys_created_by": "SecCommon.System",
      "sys_created_on": "2024-06-04T00:00:00.000Z",
      "sys_id": "30526b0a436a02102164e0ea78b8f210",
      "sys_updated_by": "system",
      "sys_updated_on": "2024-06-15T00:00:00.000Z",
      "tags": "critical",
      "taxonomies": "MITRE: T121",
      "threat_level": "medium",
      "threat_score": "24",
      "threat_severity": "medium",
      "tlp": "CLEAR",
      "type": "ip_v4_address",
      "usage_categories": "APT",
      "value": "116.98.170.70"
   },
   "trigger": {
      "name": "Observable Update",
      "type": "UPDATE",
      "trigger_time": "2024-07-26T07:27:29.000Z",
      "trigger_fields": [
         {
            "field_name": "confidence",
            "previous_value": "30",
            "current_value": "50"
         }
      ]
   }
}
```


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste des paramètres de la charge utile du déclencheur

Paramètre dans la charge utile du déclencheur	Type	Description
record	Chaîne	Spécifie le type d'enregistrement tel qu'Observable ou Indicateur.
record_fields	Objet	Spécifie l'instantané des champs d'enregistrement lorsque l'événement est généré. Pour obtenir la liste des champs pris en charge, consultez la table dans la section ci-dessous.
déclencher	Objet	Spécifie les informations sur le déclencheur correspondant.
trigger.name	Chaîne	Spécifie le nom du déclencheur
trigger.type	Chaîne	Spécifie le type de déclencheur. Les valeurs valides sont CRÉER, METTRE À JOUR, SUPPRIMER.
trigger.trigger_time	Date (au format ISO avec le fuseau horaire UTC)	Spécifie l'heure à laquelle l'événement s'est produit dans l'enregistrement.
trigger_fields	Tableau d'objets	Ceci n'est disponible que pour le type de déclencheur METTRE À JOUR. Elle spécifie la liste des champs de déclencheur qui ont été modifiés lors de l'événement qui s'est produit. Les paramètres à l'intérieur **trigger_fields** sont les suivants : ○ **field_name** : fournit le nom du champ qui a été modifié ○ **previous_value** : fournit la valeur précédente du champ. ○ **current_value** : fournit la valeur actuelle du champ.

Liste des champs pris en charge pour les déclencheurs de création et de mise à jour

Table	Nom de colonne	Étiquette de colonne
Campagne	Alias	Alias
Campagne	description	Description
Campagne	first_seen	Premier observé
Campagne	last_seen	Dernier observé
Campagne	nom	Nom

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Nom de colonne	Étiquette de colonne
Campagne	objectif	Objectif
Indicateur	additional_context	Contexte supplémentaire
Indicateur	attack_phases	Phases d'attaque
Indicateur	auteur	Auteur
Indicateur	fiabilité	Fiabilité
Indicateur	description	Description
Indicateur	expiration_time	Délai d'expiration
Indicateur	first_detected	Premier détecté
Indicateur	first_observed	Premier observé
Indicateur	first_seen	Premier observé
Indicateur	id	ID
Indicateur	indicator_types	Types des indicateurs
Indicateur	ioc_classification	Classification IOC
Indicateur	last_observed	Derniers observés
Indicateur	last_seen	Dernier observé
Indicateur	nom	Nom
Indicateur	modèle	Schéma
Indicateur	pattern_type	Type de schéma
Indicateur	pattern_version	Version du modèle
Indicateur	Plates-formes	Plateformes
Indicateur	Révoqué	Révoqué
Indicateur	source_count	Nombre de sources
Indicateur	spec_version	Version de spéc.
Indicateur	état	Statut
Indicateur	balises	Balises TISC
Indicateur	Taxonomies	Taxonomies
Indicateur	threat_level	Niveau de menace
Indicateur	threat_severity	Gravité de la menace
Indicateur	Tlp	TLP
Indicateur	usage_categories	Catégories d'utilisation
Indicateur	valid_from	Date de début de validité
Indicateur	valid_until	Fin de validité
Programme malveillant	Alias	Alias
Programme malveillant	attack_phases	Phases d'attaque
Programme malveillant	description	Description

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Nom de colonne	Étiquette de colonne
Programme malveillant	executable_process_architectures	Architectures de processus
Programme malveillant	first_seen	Premier observé
Programme malveillant	implementation_languages	Langues d'implémentation
Programme malveillant	is_family	Est la famille
Programme malveillant	last_seen	Dernier observé
Programme malveillant	malware_capabilities	Options de logiciel malveillant
Programme malveillant	malware_types	Types de programmes malveillants
Programme malveillant	nom	Nom
Objet (champs d'objet commun)	additional_context	Contexte supplémentaire
Objet (champs d'objet commun)	fiabilité	Fiabilité
Objet (champs d'objet commun)	expiration_time	Délai d'expiration
Objet (champs d'objet commun)	id	ID
Objet (champs d'objet commun)	Révoqué	Révoqué
Objet (champs d'objet commun)	source_count	Nombre de sources
Objet (champs d'objet commun)	spec_version	Version de spéc.
Objet (champs d'objet commun)	état	Statut
Objet (champs d'objet commun)	balises	Balises TISC
Objet (champs d'objet commun)	Taxonomies	Taxonomies
Objet (champs d'objet commun)	threat_level	Niveau de menace
Objet (champs d'objet commun)	threat_severity	Gravité de la menace
Objet (champs d'objet commun)	Tlp	TLP
Observable	additional_context	Contexte supplémentaire
Observable	attack_phases	Phases d'attaque
Observable	auteur	Auteur
Observable	fiabilité	Fiabilité
Observable	description	Description
Observable	expiration_time	Délai d'expiration
Observable	first_observed	Premier observé
Observable	first_seen	Premier observé
Observable	id	ID
Observable	is_defanged	Est neutralisé
Observable	is_false_positive	Est un faux positif
Observable	last_observed	Derniers observés
Observable	last_seen	Dernier observé
Observable	réputation	Réputation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Nom de colonne	Étiquette de colonne
Observable	source_count	Nombre de sources
Observable	état	Statut
Observable	balises	Balises TISC
Observable	Taxonomies	Taxonomies
Observable	threat_level	Niveau de menace
Observable	threat_score	Score de menace
Observable	threat_severity	Gravité de la menace
Observable	Tlp	TLP
Observable	type	Type
Observable	usage_categories	Catégories d'utilisation
Observable	valide	Valeur
Acteur de menace	Alias	Alias
Acteur de menace	description	Description
Acteur de menace	first_seen	Premier observé
Acteur de menace	objectifs	Objectifs
Acteur de menace	last_seen	Dernier observé
Acteur de menace	nom	Nom
Acteur de menace	personal_motivations	Motivations personnelles
Acteur de menace	primary_motivation	Motivation principale
Acteur de menace	resource_level	Niveau de ressource
Acteur de menace	secondary_motivations	Motivations secondaires
Acteur de menace	sophistication	Sophistication
Acteur de menace	threat_actor_roles	Rôles d'acteur de menace
Acteur de menace	threat_actor_types	Types d'acteurs de menace
Rapport de menace	description	Description
Rapport de menace	nom	Nom
Rapport de menace	publié	Publié
Rapport de menace	report_types	Types de rapports
Vulnérabilité	affected_software	Logiciel affecté
Vulnérabilité	description	Description
Vulnérabilité	exploitation_status	État d'exploitation
Vulnérabilité	exploit_exists	Un exploit existe
Vulnérabilité	nom	Nom
Vulnérabilité	publié	Publié
Vulnérabilité	record_last_modified	Dernière modification de l'enregistrement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Nom de colonne	Étiquette de colonne
Vulnérabilité	severity	Gravité

Vous trouverez ci-dessous la liste des champs système applicables qui sont communs à toutes les entités, et ceux-ci sont pris en charge dans la charge utile du déclencheur de webhook pour les déclencheurs de création et de mise à jour.

- sys_id (ID système)
- sys_created_on (créé)
- sys_created_by (créé par)
- sys_updated_on (mis à jour)
- sys_updated_by (Mis à jour par)

Remarque : Pour la suppression, seul sys_id (ID système) est envoyé à l'URL du point de terminaison Webhook dans le cadre de la charge utile et les autres champs système ne sont pas pris en charge.

Liste des champs pris en charge pour supprimer le déclencheur

Table	Nom de colonne	Étiquette de colonne
Observable	type	Type
Observable	valide	Valeur
Indicateur	nom	Nom
Indicateur	modèle	Schéma
Indicateur	pattern_type	Type de schéma
Indicateur	valid_from	Début de validité
Campagne	nom	Nom
Programme malveillant	is_family	Est la famille
Programme malveillant	nom	Nom
Acteur de menace	nom	Nom
Rapport de menace	nom	Nom
Rapport de menace	publié	Publié
Vulnérabilité	nom	Nom
Vulnérabilité	severity	Gravité

Traduction automatique

Configurer les info-bulles pour les cartes de nœud

Utilisez cette section pour configurer les info-bulles des relations de carte de nœud sur le canevas d'examen.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Administration** > **Contrôles de mappage de nœud** > **Configuration de l'info-bulle**.
2. Sélectionnez l'objet souhaité dans la liste.
   Par défaut, les trois enregistrements suivants sont mis en service dans le système de base.
   a. Observables
   b. Indicateurs
   c. Objets
3. Sélectionnez **Observable** comme exemple d'enregistrement.
4. Ajoutez une ou plusieurs valeurs à l'enregistrement de l'observable, si nécessaire.
   De même, ajoutez des valeurs aux indicateurs et aux autres objets.

   Remarque : Chaque objet prend en charge un maximum de six valeurs.

5. Sélectionnez **Enregistrer** pour appliquer les modifications.
6. Accédez à la section **Canevas d'examen** et sélectionnez l'icône **Actualiser** .
   Les mêmes valeurs configurées sur la page **Configuration de l'info-bulle** s'afficheront sur chaque carte de nœud.

Utiliser des flux automatisés

Suivez ces étapes définies pour apprendre à utiliser les flux automatisés dans TISC et ses options.

Créez des flux qui s'exécutent avec des rôles TISC. Dans TISC, les flux sont créés pour les éléments suivants :

- Enrichissement automatisé IOC
- Analyser, évaluer et diffuser les IoC liés aux menaces
- Analysez, évaluez les IoC liés à la menace et créez un incident.
- Prise en charge de la gestion de la vulnérabilité.
- Suivi des vulnérabilités zero-day.

Remarque : Tous les flux sont des modèles qui sont expédiés à l'état de brouillon pour que les utilisateurs puissent les personnaliser ou les copier en fonction de leurs propres besoins.

Actions réutilisables

Action de flux	Description
Ajouter une balise à l'entité	Ajout d'une balise à une entité qui le prend en charge (observable/indicateur/objet).
Supprimer la balise de l'entité	Suppression de la balise d'une entité qui la prend en charge (observable/indicateur/objet).
Vérifier si l'adresse IP se trouve dans la plage CIDR	Vérification si une adresse IP se trouve dans une plage CIDR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action de flux	Description
Vérifier si l'adresse IP se trouve dans la plage	Vérification si une adresse IP se trouve entre la plage de départ et la plage de destination.

Enrichissement automatisé IOC

Découvrez comment automatiser l'enrichissement des IOC à l'aide de flux lorsqu'ils correspondent à un certain critère.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (vue)

Pourquoi et quand exécuter cette tâche

Automatisez l'enrichissement des déclencheurs d'IOC uniquement lorsque :

- Le type de l'observable est un nom de domaine, une adresse IPv4 ou une adresse IPv6.
- L'observable est dans un état Traité.
- l'observable n'a pas les balises enrichies ou ignorer l'enrichissement.

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez le lien de l'action **d'enrichissement IOC automatisé** pour afficher les détails des règles respectives dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

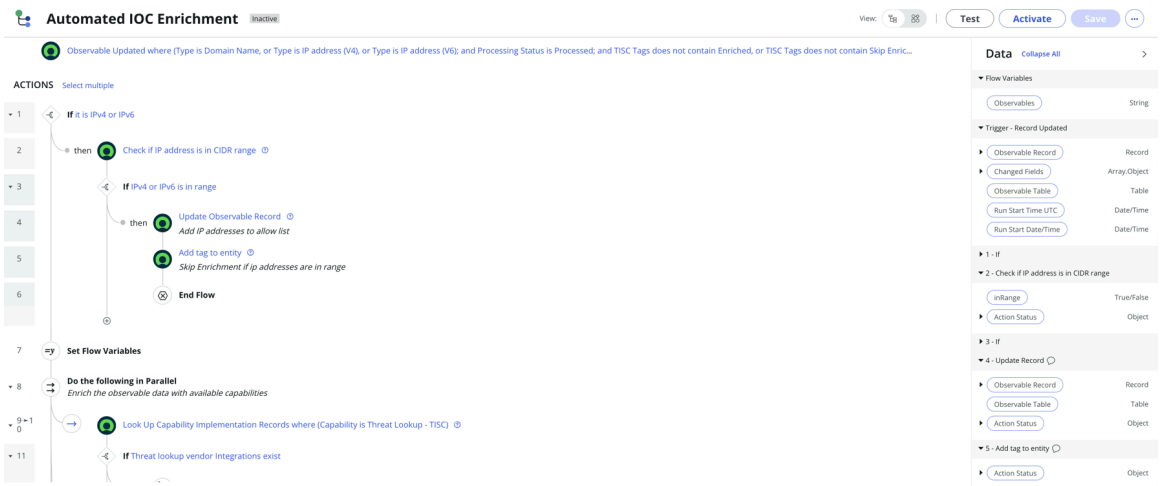
   Observable Updated where (Type is Domain Name, or Type is IP address (V4), or Type is IP address (V6); and Processing Status is Processed; and TISC Tags does not contain Enriched, or TISC Tags does not contain Skip Enrichment, or TISC Tags does not contain Potential New Threat)

5. **Si l'observable est une adresse IPv4 ou IPv6 et qu'il se trouve dans une plage CIDR autorisée :**
   a. Ajouter l'observable à la liste d'autorisation.
   b. Mettre à jour les balises des observables sur Ignorer l'enrichissement.
   c. Arrêtez le flux pour cet observable.
6. **Sinon, enrichissez les données observables avec les options disponibles :**
   a. Effectuez une recherche de menace et une recherche de perception pour recueillir des informations supplémentaires sur l'observable.
   b. Mettez à jour l'observable avec des données enrichies.
   c. Ajouter une balise **Enrichi** pour indiquer que l'IOC a été traité.
7. **En outre, si la réputation des observables est propre, alors :**
   a. Marquez l'observable comme faux positif et inactivez.
8. **Sinon, si la réputation de l'observable est inconnue**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Ajouter une balise **Pas une menace potentielle et Enrichi** pour indiquer qu'il ne s'agit pas d'une menace.



Analyser, évaluer et diffuser les observables

Apprenez à analyser et à diffuser des observables liés à une menace.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (vue)

Pourquoi et quand exécuter cette tâche

Chaque fois qu'un enrichissement de recherche d'observation est demandé, il revient sans aucune observation.

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez **Analyser, évaluer et diffuser sur le lien IoC liés à l'action de menace** pour afficher les détails des règles respectives dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

   ```
   Sighting Created where (Sighting count is 0)
   ```

5. **L'observable a un score de menace supérieur à 80, un score de confiance supérieur à 80 et une réputation malveillante :**

   a. Ajoutez l'observable à la liste de refus.

   b. Arrêtez le flux pour cet observable.

6. **Sinon, la réputation de l'observable est suspecte et le score de menace est compris entre 60 et 80 :**

   a. Ajoutez une balise appelée Nouvelle menace potentielle.

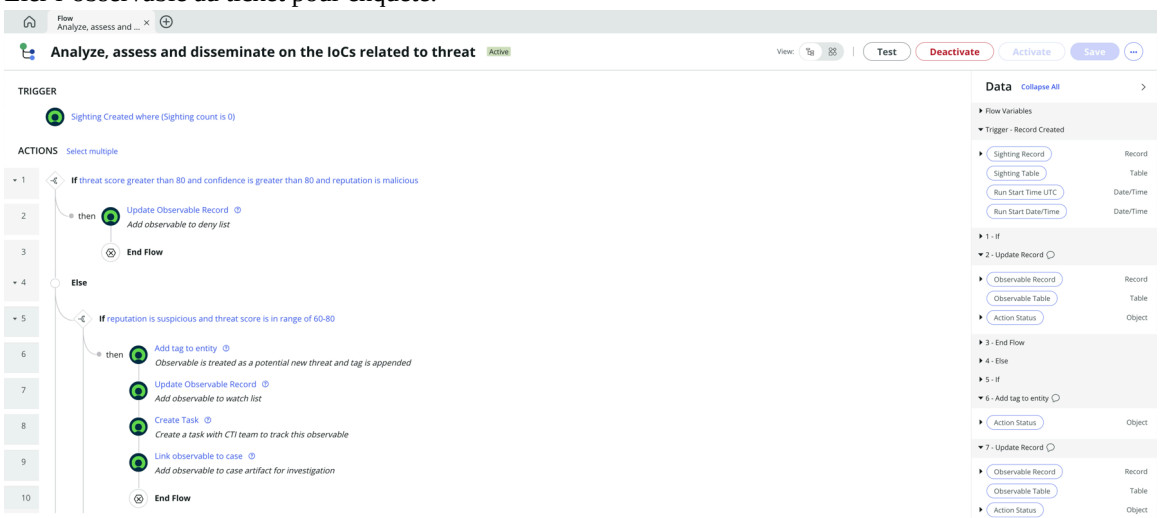
   b. Ajoutez l'observable à la liste de surveillance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Créez une tâche de ticket avec l'équipe CTI pour suivre cet observable et effectuer une analyse plus approfondie.

d. Lier l'observable au ticket pour enquête.



Analyser et évaluer les menaces IoC

Apprenez à analyser les menaces d'un CIO et à notifier l'équipe des incidents de sécurité.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (vue)

Pourquoi et quand exécuter cette tâche

Chaque fois qu'un enrichissement de recherche d'observation est demandé :

- si l'observable est vu (nombre > 0) et
- La réputation de l'observable est malveillante et
- Le score de menace de l'observable est > 80 et
- Fiabilité observable > 80

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez **le lien d'action Analyser, évaluer les IoC liés à la menace et créer un incident** pour afficher les détails des règles respectives dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

Sighting Created where (Sighting count greater than 0, and Observable. Reputation is Malicious, and Observable. Threat Score greater than 80, and Observable. Confidence greater than 80)

Traduction automatique

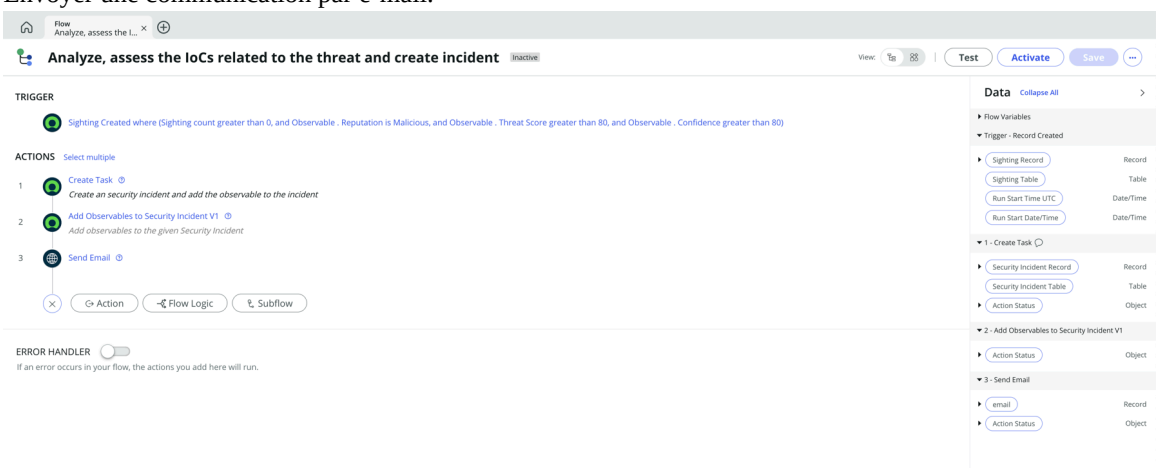
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Si la perception a été créée où (nombre de perception supérieur à 0 et observable. La réputation est malveillante et observable. Score de menace supérieur à 80 et observable. Confiance supérieure à 80), alors :**

   a. Créez un incident de sécurité et ajoutez l'observable à l'incident.

   b. Ajouter des observables à l'incident de sécurité V1.

   c. Envoyer une communication par e-mail.



Soutien à la gestion des vulnérabilités

Découvrez comment une nouvelle vulnérabilité est créée dans TISC avec une vulnérabilité connexe dans VR.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (vue)

Pourquoi et quand exécuter cette tâche

Lorsqu'une nouvelle vulnérabilité est créée dans TISC et qu'il existe une vulnérabilité connexe dans VR.

- Si le score de vulnérabilité VR (v2) est > 8 OU si le score de vulnérabilité VR (v3) est > 8.
- Le total des VI qui lui sont associés est supérieur à 0.

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez le lien de l'action **de prise en charge de la gestion des vulnérabilités** pour afficher les détails des règles respectives dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

   When new vulnerability is created in TISC and there is a related vulnerability in VR.

5. **Si le pourcentage du total des VI rattrapés qui sont associés à cette vulnérabilité est de 100 %, alors :**

Traduction automatique

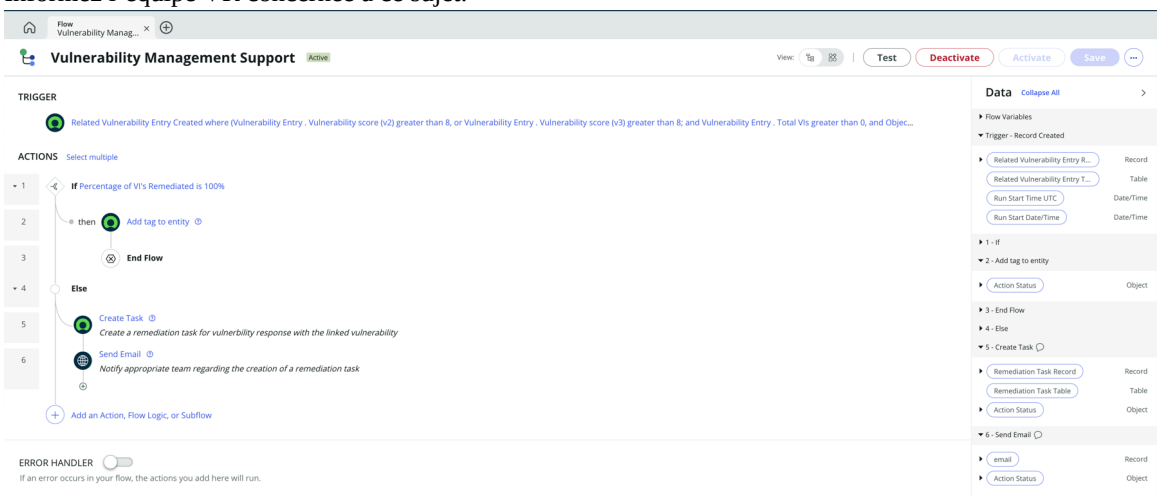
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Ajoutez une balise appelée Remediated à l'observable.

6. **Sinon, enrichissez les données observables avec les options disponibles :**

a. Créez une tâche de rattrapage pour la VR.

b. Informez l'équipe VR concernée à ce sujet.



Suivi des vulnérabilités zero-day

Apprenez à analyser les flux RSS entrant dans le système.

Avant de commencer

Rôle requis :

- Administrateur système (afficher, créer ou modifier)
- sn_sec_tisc.admin (vue)

Pourquoi et quand exécuter cette tâche

Chaque fois qu'un nouveau flux RSS est créé dans le système, et qu'il y a une mention de 'Zero Day' dans le titre ou la description.

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Administration**.
2. Sélectionner **Flux automatisés**.
3. Sélectionnez le lien **de suivi des vulnérabilités zero-day** pour afficher les détails des règles respectives dans le concepteur de flux.
4. Affichez l'action du Concepteur de flux pour le déclencheur suivant :

```
RSS Feed Created where (Title contains zero day, or Description contains zero day, or
Title contains zero_day, or Description contains zero_day, or Title contains zero-day, or
Description contains zero-day)
```

5. **Si l'observable est une adresse IPv4 ou IPv6 et qu'il se trouve dans une plage CIDR autorisée :**

a. Créez un ticket pour l'équipe TISC ainsi qu'une tâche de rattrapage pour l'équipe VR.

b. Informez les équipes TISC et VR concernées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables de flux automatisés

Les tables suivantes vous aident à comprendre les tables de relations entre les entités et les tables d'enrichissement utilisées dans les flux automatisés.

Tables de relations entre les entités

Table	Entité
Observable d'indicateur connexe	sn_sec_tisc_m2m_indicator_observable
Indicateur connexe	sn_sec_tisc_m2m_indicator
Observable connexe	sn_sec_tisc_m2m_observable
Relation objet-objet	sn_sec_tisc_m2m_object
Objet d'indicateur connexe	sn_sec_tisc_m2m_object_indicator
Relation objet-observable	sn_sec_tisc_m2m_object_observable

Table d'enrichissement

Table	Entité
Résultats de la recherche de menace	sn_sec_tisc_lookup_result
Perceptions	sn_sec_tisc_sighting
Résultat de l'enrichissement de l'observable	sn_sec_tisc_observable_enrichment_result

Référence Centre de sécurité des renseignements sur les menaces

Les rubriques de référence fournissent des informations supplémentaires sur le Centre de sécurité des renseignements sur les menaces.

Informations de référence	Liens vers des rubriques
Séparation en domaines et Centre de sécurité des renseignements sur les menaces	Séparation de domaine et Threat Intelligence Security Center
Composants installés avec Centre de sécurité des renseignements sur les menaces l'application	Composants installés avec Threat Intelligence Security Center

Séparation de domaine et Threat Intelligence Security Center

Centre de sécurité des renseignements sur les menaces prend en charge Séparation de domaine. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Standard

- Inclut tous les aspects du support de niveau **basique** .
- Les propriétés d'application sont sensibles au domaine selon les besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

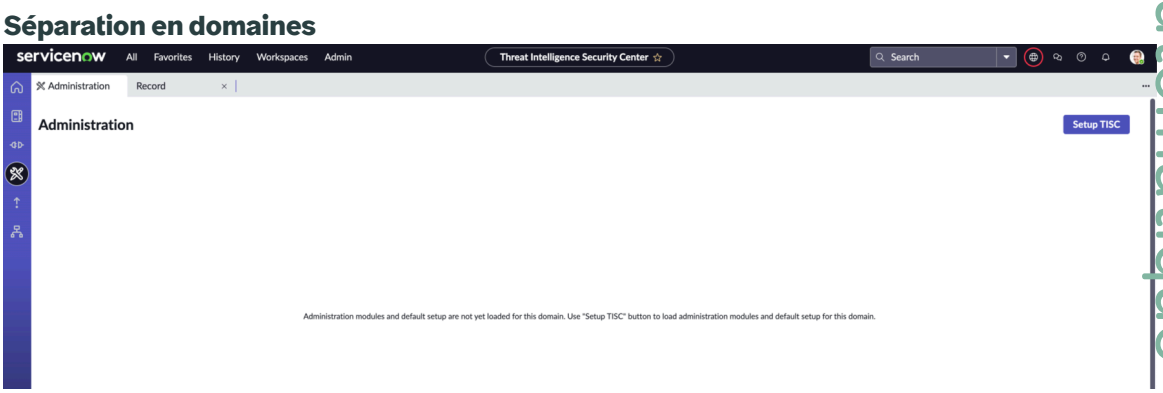
Vue d'ensemble

Séparation de domaine est activé pour toutes les fonctionnalités de Centre de sécurité des renseignements sur les menaces.

Comment fonctionne Séparation de domaine dans Centre de sécurité des renseignements sur les menaces

- Tous les enregistrements liés à la configuration qui sont mis en service dans le système de base sont expédiés dans le domaine global. Si l'instance est séparée par domaine, l'utilisateur voit un bouton explicite **Configurer TISC** sous le module **Administration** de l'espace de travail TISC. Cliquez sur ce bouton pour cloner les configurations de domaine global mises en service par le système de base dans les domaines respectifs.

Séparation en domaines



Remarque : Les utilisateurs ne doivent activer ou modifier que les enregistrements de configuration spécifiques à un domaine et ne doivent pas activer ou modifier les enregistrements de configuration dans le domaine global.

- Deux règles de notification de plateforme (sysevent_email_action) sont mises en service dans le système de base. Ces règles de notification doivent être clonées dans les domaines requis et seules les règles de notification spécifiques à un domaine doivent être activées.

Remarque : Pour plus d'informations sur les notifications de règles, accédez à **Notification système** > **Notifications** et filtrer toutes les règles de notification de domaine globales définies sur les tables en commençant par le nom `sn_sec_tisc` pour comprendre comment les utilisateurs peuvent identifier les règles de notification de base qui sont mises en service dans le système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Toutes les configurations et données ingérées seront spécifiques à chaque domaine, ce qui signifie que les utilisateurs d'un domaine ne pourront pas accéder aux données d'un autre domaine.
- Configurez un environnement séparé par domaine avec cette application en installant le module d'extension Domain Support - Domain Extensions Installer .
- Des colonnes de domaine sont ajoutées pour toutes les tables d'application du système de base.
- À l'aide de la fonctionnalité fournie par la plateforme, les domaines locataires gèrent leurs propres données d'application.
- La logique métier et les processus qui peuvent être séparés par domaine par le propriétaire de l'instance sont identiques à ceux pris en charge par la plateforme.
- La logique métier et les processus pouvant être administrés par le domaine du locataire sont les mêmes que ceux pris en charge par la plateforme.
- Vous pouvez accéder à la page Configuration à partir de la section Administration. Cliquez sur le lien fourni sous la section Administration pour afficher la vue de séparation de domaine.
- Pour prendre en charge la séparation de domaine pour les widgets à l'aide des indicateurs Analyse des performances (PA) dans le tableau de bord d'accueil TISC, reportez-vous à l'article de la base de connaissances KB1647990 pour connaître la procédure détaillée.

Tables séparées de domaine

Toutes les tables sont séparées par domaine.

Cas d'utilisation

Toutes les fonctionnalités de cette application sont séparées par domaine.

Information associée

Séparation de domaine pour les fournisseurs de services

Composants installés avec Threat Intelligence Security Center

Plusieurs types de composants sont installés lorsque vous téléchargez et activez l'application, notamment les rôles d'utilisateur et les Centre de sécurité des renseignements sur les menaces propriétés.

Propriétés installées

Rôle requis : sn_sec_tisc.admin

Les utilisateurs disposant du rôle d'administrateur de sécurité [sn_sec_tisc.admin] peuvent les modifier.

Propriété	Utilisation
Propriétés du Centre de sécurité des renseignements sur les menaces	
Toutes les règles de corrélation seront alors désactivées. Si nous avons juste besoin de désactiver les règles de corrélation sélectionnées, utilisez plutôt le champ « actif » de la règle de corrélation.	• **Type** : vrai | faux • **Valeur par défaut** : faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
sn_sec_tisc.disable_correlation_rules	
Cette propriété permet d'activer/de désactiver le traitement des agrégats dans la fonctionnalité du calculateur de score de menace. sn_sec_tisc.agrégats_pour_calculatrice	• **Type** : vrai | faux • **Valeur par défaut** : true
Nombre de lignes de données brutes qui sont enregistrées lors de l'exécution d'une recherche d'observations. Plage 0 – 100 sn_sec_tisc.sighting_search_raw_data_rows	• **Type** : nombre entier • **Valeur par défaut** : 50
Associez les résultats de la recherche de perception aux CI dans la CMDB. sn_sec_tisc.associate_ci_with_sighting_search	• **Type** : vrai | faux • **Valeur par défaut** : true
Cela permet de contrôler si les URL des listes sont neutralisées ou non sn_sec_tisc.sn_sec_tisc_case.defang_record_list_urls	• **Type** : vrai | faux • **Valeur par défaut** : faux
Cette propriété permet de déployer automatiquement la ou les techniques MITRE dans les tickets à partir des objets associés ou des incidents de sécurité. sn_sec_tisc.auto_rollup_mitre_data	• **Type** : vrai | faux • **Valeur par défaut** : true
Si vrai, affiche toutes les tactiques (y compris celles qui n'ont aucune technique associée au ticket) pour les listes MITRE rendues dans le rapport. sn_sec_tisc.show_all_tactics_reporting	• **Type** : vrai | faux • **Valeur par défaut** : true
ID système du modèle de client de messagerie pour la table Ticket (sn_sec_tisc_case) qui sera utilisé dans le rapport de partage. sn_sec_tisc.reporting_email_template_sn_sec_tisc_case	• **Type** : chaîne • **Valeur par défaut** : b55e22c54324021060eee0ea78b8f2df
Le niveau TLP par défaut est appliqué lors de la création d'un nouvel enregistrement. Si elle n'est pas définie manuellement sur le formulaire, cette valeur sera utilisée. sn_sec_tisc.tlp_default_value	• **Type** : liste de choix • **Valeur par défaut** : 955c9e5543d35110baf06e434ab8f2fb
Niveau de connexion : débogage, information, avertissement, erreur sn_sec_tisc.logging.verbosité	• **Type** : liste de choix • **Valeur par défaut** : info
Propriétés des flux de Renseignements sur les menaces	
Délai maximal, en secondes, pendant lequel une connexion HTTP sortante attend pour récupérer les données de collecte TAXII sn_sec_tisc.taxii.http.max_timeout	• **Type** : nombre entier • **Valeur par défaut** : 300

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
Nombre maximal d'objets récupérés dans un seul appel REST à partir d'un serveur TAXII (applicable uniquement pour les versions 2.0 et 2.1 de TAXII) sn_sec_tisc.taxii.max_taille_page_	• **Type** : nombre entier • **Valeur par défaut** : 5 000
Nombre maximal de nouvelles tentatives pour un échec de TAXII2. X appel REST sn_sec_tisc.taxii2.retry_count	• **Type** : nombre entier • **Valeur par défaut** : 3
Nombre maximal d'objets récupérés dans un seul appel REST à partir du serveur Cyware TAXII sn_sec_tisc.cyware_taxii.max_taille_page_	• **Type** : nombre entier • **Valeur par défaut** : 1 000 **Remarque :** Spécifie la taille de page utilisée lors de l'extraction des données à partir des collections TAXII liées au flux Cyware TAXII. Pour toutes les autres collections TAXII, la taille de page récupérée à partir de la collection TAXII est par défaut la valeur définie dans la propriété correspondante : sn_sec_tisc.taxii.max_page_size.
Nombre d'enregistrements à extraire simultanément à partir de CrowdStrike. Plus la valeur est élevée, plus la mémoire consommée pour le traitement de la charge utile est élevée. sn_sec_tisc.crowdstrike_api_limit	• **Type** : nombre entier • **Valeur par défaut** : 1 000
Indique le nombre d'indicateurs à extraire dans un seul appel d'API. **Remarque :** Cela ne s'applique que lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système. sn_sec_tisc.crowdstrike_indicator_batch_size	• **Type** : nombre entier • **Valeur par défaut** : 1 000
Indique le nombre d'acteurs à extraire dans un seul appel d'API. **Remarque :** Cela ne s'applique que lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système. sn_sec_tisc.crowdstrike_actor_batch_size	• **Type** : nombre entier • **Valeur par défaut** : 1 000
Indique le nombre de rapports à extraire dans un seul appel d'API. **Remarque :** Cela ne s'applique que lorsque l'intégration ne détecte pas la présence des éléments nécessaires dans le système.	• **Type** : nombre entier • **Valeur par défaut** : 50

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
sn_sec_tisc.crowdstrike_report_batch_size	
Total autorisé de décalage et de la limite par l'API CrowdStrike. sn_sec_tisc.crowdstrike_offset_limit_total	• **Type** : nombre entier • **Valeur par défaut** : 50000
Propriétés des API REST	
Définit la taille maximale de la page (nombre maximal d'observables retournés dans le cadre de la réponse) pour l'API d'extraction des observables. Il n'est pas recommandé d'augmenter la valeur à une valeur élevée, car elle peut affecter le délai de réponse de l'API. sn_sec_tisc.api_maximum_page_size_limit	• **Type** : nombre entier • **Valeur par défaut** : 1 000
Définit le nombre maximal d'observables qui peuvent être envoyés dans le corps de la demande pour l'API d'ajout d'observables. Il n'est pas recommandé d'augmenter la valeur à une valeur élevée, car elle peut affecter le délai de réponse de l'API. sn_sec_tisc.add_obs_api_max_records	• **Type** : nombre entier • **Valeur par défaut** : 100
Propriétés des webhooks	
Nombre maximal d'événements à envoyer dans le cadre d'une demande de webhook. La taille du lot est limitée à 2 000 même si une valeur plus élevée est définie dans cette propriété. sn_sec_tisc.webhook_max_event_batch_size	• **Type** : nombre entier • **Valeur par défaut** : 100
Nombre de fois qu'une demande ayant échoué doit être réessayée avant de la marquer comme erreur et de passer au lot d'événements suivant. Le nombre de nouvelles tentatives est limité à 10 même si un nombre plus élevé est défini dans cette propriété. sn_sec_tisc.webhook_retry_count	• **Type** : nombre entier • **Valeur par défaut** : 100
Nombre de secondes à attendre avant de retenter un lot ayant échoué. Cette valeur augmentera de façon exponentielle en fonction du nombre de nouvelles tentatives. Par exemple, si retry_count est 3 et retry_interval est 30, les nouvelles tentatives sont déclenchées après 30, 60 et 120 secondes. L'intervalle entre les tentatives initiales est limité à 300 secondes, même si une valeur plus élevée est définie dans cette propriété. sn_sec_tisc.webhook_retry_interval	• **Type** : nombre entier • **Valeur par défaut** : 30
Ignorer les événements de webhook déclenchés par la réapplication du score de menace sn_sec_tisc.webhook_ignore_threat_score_reapply	• **Type** : vrai | faux • **Valeur par défaut** : true
Propriétés du canevas d'enquête	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Utilisation
Si vous définissez la valeur sur vrai, de nouveaux nœuds sont ajoutés dans le coin supérieur gauche alors qu'une définition sur faux les ajoute au centre du canevas. sn_sec_tisc.canvas_suspend_reLayout	• **Type** : vrai | faux • **Valeur par défaut** : true
Propriétés pour l'exportation au format CTI	
Nombre maximal de lignes pouvant être exportées vers un fichier STIX 2.1 sn_sec_tisc.stix_export_limit	• **Type** : nombre entier • **Valeur par défaut** : 10 000
Inclure les champs de type journal dans le fichier d'exportation. sn_sec_tisc.export_journal_fields	• **Type** : vrai | faux • **Valeur par défaut** : true

Travaux planifiés

La table suivante décrit les travaux planifiés :

Tâche	Description
Regrouper les enregistrements source de l'indicateur	Regroupe les enregistrements sources des indicateurs.
Regrouper les enregistrements sources de l'objet	Regroupe les enregistrements sources de l'objet.
Regrouper les enregistrements source observable	Regroupe les enregistrements sources des observables.
Nettoyage des importations périmées	Nettoie les enregistrements de tâches d'importation périmés.
Nettoyage des nouveaux nœuds de canevas inutilisés	Nettoie les nouveaux nœuds de canevas inutilisés.
Nettoyer les enregistrements de téléchargement de fichiers sécurisés	Nettoie les enregistrements de téléchargement de fichiers sécurisés.
Dédupliquer les enregistrements sources des indicateurs	Déduplique les enregistrements sources des indicateurs.
Dédupliquer les enregistrements sources de l'objet	Déduplique les enregistrements sources de l'objet.
Dédupliquer les enregistrements sources d'observables	Déduplique les enregistrements sources des observables.
Désactiver les indicateurs expirés	Désactive les enregistrements d'indicateurs expirés.
Désactiver les objets expirés	Désactive les enregistrements d'objets expirés.
Désactiver les observables expirés	Désactive les enregistrements d'observables expirés
Migrer les données de TI vers TISC	Enregistrements d'exécution de tâches de migration en attente de processus
Remplir les enregistrements agrégés pour les enregistrements sources des indicateurs	Identifie l'enregistrement agrégé parent pour les enregistrements sources d'indicateurs nouvellement créés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
Remplir les enregistrements agrégés pour les enregistrements sources de l'objet	Identifie l'enregistrement agrégé parent pour les enregistrements sources d'objets nouvellement créés.
Remplir les enregistrements agrégés pour les enregistrements sources observables	Identifie l'enregistrement agrégé parent pour les enregistrements sources d'observables nouvellement créés.
Renseigner la référence TISC dans TI	Remplit la référence de l'observable agrégé TISC dans l'enregistrement d'observable TI.
Traiter les importations approuvées	Traite les tâches d'importation approuvées.
Traiter les enregistrements de file d'attente Dsm MISP importés	Enregistrements de file d'attente d'ingestion de flux MISP intermédiaires traités.
Traiter les enregistrements de file d'attente d'importation d'indicateurs MISP importés	Traite les données MISP intermédiaires ingérées à partir d'Import Intelligence
Traiter les enregistrements de file d'attente d'importation STIX importés	Données STIX intermédiaires ingérées à partir de l'intelligence d'importation
Traiter les enregistrements de file d'attente d'importation STIX importés : ingestion	Traite les données STIX intermédiaires ingérées à partir des flux de menaces.
Traiter la migration des artefacts de ticket en attente	Migre les artefacts de ticket de l'application Threat Intelligence vers le centre de sécurité Threat Intelligence.
Traiter l'ingestion de source de menace en attente Enregistrements de file d'attente	Traite les enregistrements de file d'attente d'ingestion source en attente.
Traiter les entités en file d'attente pour le calculateur de score de menace	Traite les entrées de file d'attente en attente du calculateur de menace
Traiter les enregistrements de file d'attente MISP Dsm mis en file d'attente	Processus mis en file d'attente Données MISP ingérées à partir du flux de menaces
Traiter les enregistrements de file d'attente d'importation d'indicateurs MISP en file d'attente	Processus mis en file d'attente Données MISP ingérées à partir de l'intelligence d'importation
Traiter les enregistrements de file d'attente d'importation STIX en file d'attente : ingestion	Traite les données STIX mises en file d'attente ingérées à partir des flux de menaces.
Traiter les enregistrements de file d'attente d'importation d'indicateurs STIX en file d'attente	Processus mis en file d'attente Données STIX ingérées à partir de l'intelligence d'importation
Traiter la file d'attente de webhooks	Traite les enregistrements de file d'attente de webhook en attente.
Réagrégater les enregistrements sources	Réagrège les enregistrements sources pour lesquels les enregistrements agrégés sont supprimés.
Supprimer l'enregistrement source filtré	Nettoie les enregistrements sources filtrés
Reprendre l'intégration CrowdStrike Traiter le vérificateur / retraiter les enregistrements sources CrowdStrike	Reprend les exécutions d'intégration de flux CrowdStrike en attente de limite de taux/Reporcess enregistrements sources pour l'agrégation de relations
Nombre d'observables de faux positif de synchronisation	Synchronise les nombres de faux positifs observables avec les nombres de faux positifs par source
TISC : créer des lots de webhooks	Lots créés pour le webhook en file d'attente Entrées de file d'attente pour le traitement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
TISC Fire Webhooks	Exécute les lots de webhooks en attente
Mise à jour de la relation Colonne archivée	Met à jour l'état d'archivage des enregistrements sources et cibles des relations

Utiliser Centre de sécurité des renseignements sur les menaces

Utilisez cette fonction Centre de sécurité des renseignements sur les menaces pour gérer les enregistrements de bibliothèque Threat Intelligence, importer des données sur les menaces externes et rationaliser la gestion des tickets. Elle aide les équipes de sécurité à centraliser les données de renseignement, à améliorer l'analyse et à répondre plus efficacement aux menaces en intégrant les informations pertinentes dans les enquêtes en cours.

Intégration TISC à l'espace de travail SIR

L'intégration TISC à SIR joint automatiquement le contexte des observables dans l'espace de travail des incidents de sécurité pour les analystes de sécurité. Tout nouvel observable de SIR peut être envoyé à TISC pour une analyse plus approfondie par l'équipe CTI à l'aide des actions d'interface utilisateur fournies à l'écran.

En outre, tous les résultats d'enrichissement produits à partir d'intégrations disponibles uniquement dans SIR peuvent également être transmis par push à l'aide des actions d'interface utilisateur fournies dans l'espace de travail.

Utilisation des importations de données

Les importations de données vous permettent d'afficher tous les enregistrements en cours de traitement pour la tâche d'importation et répertorient également les tâches d'importation en attente d'approbation.

Afficher toutes les importations

Utilisez cette section pour afficher tous les enregistrements importés qui sont affichés dans la vue de liste pour tous les utilisateurs.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Importations**.
2. Sélectionner **Importations de données** > **Toutes les importations**
   Cette page affiche tous les enregistrements en cours de traitement pour la tâche d'importation.
3. Ouvrez n'importe quel enregistrement pour afficher l'état du processus d'importation.

> **Remarque :** Vous pouvez également cliquer sur **Nouvelle importation** pour créer un enregistrement d'importation. Après avoir cliqué sur ce bouton, l'application vous dirigera vers la page **Import Intelligence** . Pour plus d'informations sur la création de nouveaux enregistrements, reportez-vous à Importer des renseignements dans TISC la section et poursuivez avec le type d'importation respectif.

Affichage de mes importations

Utilisez cette section pour afficher les enregistrements d'importation créés par l'utilisateur connecté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Importations**.
2. Sélectionner **Importations de données** > **Mes importations**
   Cette page affiche tous les enregistrements, les enregistrements d'importation qui sont catégorisés pour un processus ultérieur pour la tâche d'importation.
3. Ouvrez n'importe quel enregistrement pour afficher l'état du processus d'importation.

   Remarque : Vous pouvez également cliquer sur **Nouvelle importation** pour créer un enregistrement d'importation. Après avoir cliqué sur ce bouton, l'application vous dirigera vers la page **Import Intelligence** . Pour plus d'informations sur la création de nouveaux enregistrements, reportez-vous à Importer des renseignements dans TISC la section et poursuivez avec le type d'importation respectif.

4. Affichez le résumé des enregistrements d'importation.

   Remarque : Si l'une des tâches d'importation n'est pas soumise, vous pouvez **soumettre** les enregistrements pour un traitement ultérieur et les envoyer pour approbation. Si l'approbation n'est pas requise pour cette tâche d'importation particulière, ces enregistrements sont traités automatiquement.

Affichage de mes approbations

Utilisez cette section pour examiner et approuver les enregistrements de tâches d'importation.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Importations**.
2. Sélectionner **Importations de données** > **Mes approbations**
   Cette page affiche tous les enregistrements d'importation en attente d'approbation par l'utilisateur connecté.
3. Ouvrez n'importe quel enregistrement pour approuver ou rejeter l'enregistrement d'importation.
4. Cliquez sur **Approuver** pour approuver l'enregistrement de la tâche d'importation.
   La boîte de dialogue **Approuver l'importation** s'affiche et un message de confirmation s'affiche quant à l'approbation des importations sélectionnées.

   Remarque : Une notification par e-mail est envoyée à l'utilisateur ou aux utilisateurs respectifs pour les informer que la tâche d'importation en cours de traitement est maintenant approuvée. Pour plus d'informations sur l'approbation des règles, reportez-vous à Définition des règles d'approbation des importations de données.

5. Sélectionnez **Approuver** dans la boîte de dialogue.
   Une notification par e-mail est envoyée à l'utilisateur qui a créé la tâche d'importation et la tâche d'importation en cours de traitement est maintenant approuvée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Rejeter** pour rejeter un enregistrement.

Remarque :

- Vous pouvez examiner et soumettre à nouveau la tâche d'importation rejetée. Assurez-vous d'ajouter des commentaires pour le rejet.
- Une notification par e-mail est envoyée à l'utilisateur qui a créé la tâche d'importation Tâche d'importation lorsque la tâche d'importation en cours de traitement est rejetée.
- Une notification par e-mail est envoyée aux approbateurs pour demander l'approbation.

Importer des renseignements dans TISC

Utilisez cette fonctionnalité pour importer manuellement des données de renseignements sur les menaces dans le référentiel, ce qui permet aux analystes d'ingérer les informations pertinentes provenant de sources externes selon les besoins.

Les formats suivants sont pris en charge pour l'importation de données Threat Intelligence :

Format d'importation	Description	Enregistrements pris en charge
Importer à partir du fichier structuré	Téléchargez le fichier d'exemple à l'aide du lien Aperçu et chargez vos données structurées dans un format compatible tel que CSV, XLS ou XLSX.	• Observables • Indicateurs
Importer à partir du format standard	Les types de fichiers pris en charge incluent les formats JSON STIX 2.x et MISP JSON.	• **STIX 2.1** : Observables, indicateurs • **MISP** : observables
Importer à partir de texte brut	Analysez l'entrée en tant que texte brut pour importer les observables. La limite maximale de caractères pour l'entrée est de 10 000 caractères.	Observables
Importer à partir du fichier (non structuré)	L'application analyse automatiquement le fichier chargé pour en extraire les observables. Types de fichiers pris en charge : TXT, CSV, JSON, XLS et XLSX.	Observables

Pour mieux comprendre chaque format d'importation et les types d'enregistrements pris en charge, reportez-vous à la section Informations connexes.

Information associée

Importer des données à l'aide d'un fichier structuré

Importer des données à l'aide d'un format standard

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer des données à l’aide de texte brut

Importer des données à l’aide d’un format de fichier non structuré

Importer des données à l’aide d’un fichier structuré

Chargez les données structurées dans les formats de fichier pris en charge tels que CSV, XLSX ou XLS.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**. La page Bibliothèque de Renseignements sur les menaces s’affiche.
2. Cliquez sur **Renseignements sur l’importation**.
3. Cliquez sur **Importer à partir de la carte de fichier structuré** .

> **Important :** Lors de l’importation des données Threat Intelligence dans les formats de fichier pris en charge tels que TXT, CSV, STIX 2.x JSON, MISP JSON ou Fichier structuré, la taille du fichier est limitée à 5 Mo. La limite de caractères au texte brut est limitée à 10 000.

4. Remplissez les champs du formulaire.

Champ	Description
Choisir une option	Sélectionnez l’option requise dans la liste déroulante, comme Observables ou Indicateurs. ○ **Observables** : sélectionnez les données observables à importer. **Remarque :** Sélectionnez cette option si vous importez des données observables. Ne modifiez pas non plus les en-têtes de colonne dans le fichier. Les champs obligatoires sont Valeur et Type, les autres étant facultatifs. Saisissez également la date/heure au format AAAA-MM-JJThh :mm :ssZ. ○ **Indicateurs** : sélectionnez les données d’indicateur à importer. **Remarque :** Sélectionnez cette option si vous importez des données d’indicateurs. Ne modifiez pas non plus les en-têtes de colonne dans le fichier. Les champs obligatoires pour les indicateurs sont Modèle, Type de modèle et Début de validité, les autres sont facultatifs. Saisissez également la date/heure au format AAAA-MM-JJThh :mm :ssZ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Prévisualiser et télécharger le fichier d'exemple pour les indicateurs	Utilisez ce lien pour télécharger le fichier d’exemple à l’aide du lien Aperçu et charger les données structurées dans un format de fichier compatible tel que CSV, XLS ou XLSX. **Remarque :** Les en-têtes de colonne doivent correspondre exactement aux en-têtes. Les champs Valeur et Type sont requis pour chaque observable du fichier. Les champs restants sont facultatifs où Premier vu, Dernier observé doit être exprimé en nombres et correspond à l’heure epoch en millisecondes.
Charger un fichier	Cliquez sur ce lien pour charger les données du fichier dans le format de fichier de structure recommandé. **Remarque :** Vous ne pouvez charger qu’un seul fichier à la fois. Pour ajouter un nouveau fichier, vous devez supprimer le fichier existant et ajouter un nouveau fichier.
Définir des définitions	
TLP	Sélectionnez l’indicateur Traffic Light Protocol (TLP) dans la liste déroulante à appliquer aux enregistrements importés. TLP est dans TISC et est étiqueté avec différentes couleurs pour garantir que les données sensibles sont partagées avec les utilisateurs prévus. ○ CLAIR : L’information peut être partagée sans restriction. ○ ROUGE ○ AMBRE+STRICT ○ AMBRE ○ VERT
Fiabilité (0-100)	Définissez la valeur de confiance entre 0 et 100 pour les enregistrements importés.
Période d'expiration (jours)	Entrez la période d’expiration des enregistrements importés. **Remarque :** Il s'agit d'un champ obligatoire.
Ajouter un ou des observables à la liste de contrôle de sécurité	Sélectionnez cette option pour ajouter des observables à la liste des contrôles de sécurité appropriée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Cette option vous permet d'ajouter directement les observables à une liste de contrôles de sécurité lors de l'importation. Les options disponibles dans la liste déroulante sont les suivantes : ○ Liste d'autorisation ○ Liste de refus ○ Aucun L'option par défaut est **Aucun**.
Balises	
Ajouter des balises	Utilisez les balises pour annoter ou marquer à l'oreille les enregistrements ingérés dans le système à partir de cette source. Commencez à saisir le nom de la balise dans la barre **de recherche** pour choisir les balises disponibles dans le système ou saisissez un nouveau nom de balise et cliquez sur **Ajouter** pour l'affecter à la source.
Taxonomie	
Sélectionner une taxonomie	Sélectionnez la taxonomie des données importées. À l'aide des taxonomies, définissez des dictionnaires qui peuvent être utilisés comme taxonomies affectées aux enregistrements de Renseignements sur les menaces. Par exemple, nomenclature CAPEC. Pour plus d'informations, consultez Création de taxonomies. **Remarque :** Les options de valeurs de taxonomie changent en fonction de la taxonomie sélectionnée.
Remplacer valeur source	Cochez cette case si vous souhaitez remplacer les valeurs source pour TLP, Fiabilité, Expiration, Balises et Taxonomies par les valeurs configurées. Si vous ne sélectionnez pas cette case à cocher, les valeurs configurées sont appliquées, si elles ne sont pas vides.

5. Cliquez sur **Suivant**.
6. Examinez les données avant de les soumettre pour traitement.

Remarque : L'examen des enregistrements importés n'est pas pris en charge pour l'option STIX.

Après avoir cliqué sur **Suivant**, vous pouvez voir le résumé de toutes les informations fournies par l'utilisateur dans la section ci-dessus, et la section ci-dessous vous fournit tous les enregistrements qui doivent être importés.

L'utilisateur peut effectuer n'importe quel type d'activités et les multiples utilisateurs peuvent collaborer à l'aide de la section des commentaires disponible dans le menu contextuel de droite. La liste des enregistrements importés est restituée une fois que

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'intégralité du fichier ou du texte brut est traitée. Le traitement de l'importation de fichiers volumineux prendra plus de temps et, pendant son traitement, vous pouvez également vérifier l'état, l'examiner et l'envoyer à partir de la page d'enregistrement d'importation.

Remarque : Tous les enregistrements qui échouent aux validations sont ignorés du processus d'importation et ne sont pas affichés sur la page Révision et soumission pour un traitement ultérieur.

7. Cliquez sur **Mettre à jour le type** et sélectionnez le type pour mettre à jour n'importe quel type d'enregistrements importés.
8. Cliquez sur **Supprimer** pour supprimer tout type d'enregistrements importés.
9. Cliquez sur **Envoyer**.

Remarque : Une fois l'enregistrement d'importation envoyé, l'utilisateur est dirigé vers l'approbateur pour approuver l'enregistrement d'importation correspondant en fonction des règles d'approbation configurées. Si l'utilisateur actuel qui crée l'enregistrement n'a pas besoin du processus d'approbation, l'enregistrement passe par le processus d'approbation automatique, la tâche d'importation est approuvée automatiquement lors de la soumission de la demande.

10. Cliquez sur **Afficher l'état** pour afficher l'état de l'enregistrement d'importation ou cliquez sur **Terminé**. L'enregistrement affiche l'état traité une fois les données importées pour traitement.
11. Cliquez sur **Annuler** pour abandonner le processus d'importation.
12. Cliquez sur **Revenir** pour revenir à la page précédente et examiner l'enregistrement, si nécessaire.

Importer des données à l'aide d'un format standard

Chargez les données standard dans les formats de fichier pris en charge tels que STIX 2.x JSON, MISP JSON.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**. La page Bibliothèque de Renseignements sur les menaces s'affiche.
2. Cliquez sur **Renseignements sur l'importation**.
3. Cliquez sur **Importer à partir d'une carte de fichier standard** .

Important : Lors de l'importation des données Threat Intelligence dans les formats de fichier pris en charge tels que TXT, CSV, STIX 2.x JSON, MISP JSON ou Fichier structuré, la taille du fichier est limitée à 5 Mo. La limite de caractères au texte brut est limitée à 10 000.

4. Remplissez les champs du formulaire.

Champ	Description
Format de fichier	Sélectionnez l'option requise dans la liste déroulante, par exemple STIX 2.x JSON ou MISP JSON.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **JSON STIX 2.x** : sélectionnez le format dans JSON STIX 2.x à importer. **Remarque :** Seuls les observables et les indicateurs seront importés à partir du fichier STIX chargé. Tous les autres types d'objets seront ignorés lors du processus d'importation. ○ **JSON MISP** : sélectionnez le format au format JSON MISP à importer.
Charger un fichier	Cliquez sur ce lien pour charger les données au format de fichier standard.
Définir des définitions	
TLP	Sélectionnez l'indicateur TLP dans la liste déroulante à appliquer aux enregistrements importés.
Fiabilité (0-100)	Définissez la valeur de confiance.
Période d'expiration (jours)	Entrez la période d'expiration des enregistrements importés. **Remarque :** Il s'agit d'un champ obligatoire.
Ajouter des balises	Utilisez les balises pour annoter ou marquer à l'oreille les enregistrements ingérés dans le système à partir de cette source. Commencez à saisir le nom de la balise dans la barre de recherche pour choisir les balises disponibles dans le système ou saisissez un nouveau nom de balise et cliquez sur Ajouter pour l'affecter à la source.
Ajouter un ou des observables à la liste de contrôle de sécurité	Sélectionnez cette option pour ajouter des observables à la liste des contrôles de sécurité appropriée. Cette option vous permet d'ajouter directement les observables à une liste de contrôles de sécurité lors de l'importation. Les options disponibles dans la liste déroulante sont les suivantes : ○ Liste d'autorisation ○ Liste de refus ○ Aucun L'option par défaut est **Aucun**.
Taxonomie	
Sélectionner une taxonomie	Sélectionnez la taxonomie des données importées. À l'aide des taxonomies, définissez des dictionnaires qui peuvent être utilisés comme taxonomies affectées aux enregistrements de Renseignements sur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	les menaces. Par exemple, nomenclature CAPEC. Pour plus d'informations, consultez Création de taxonomies.
Sélectionner valeurs de taxonomie	Indique les valeurs de taxonomie associées à la taxonomie.
Remplacer valeur source	Cochez cette case si vous souhaitez remplacer les valeurs source pour TLP, Fiabilité, Expiration, Balises et Taxonomies à partir des valeurs configurées. Si vous ne sélectionnez pas cette case, les valeurs par défaut sont appliquées.

5. Cliquez sur **Suivant**.
6. Examinez les données avant de les soumettre pour traitement.

   Remarque : L'examen des enregistrements importés n'est pas pris en charge pour l'option STIX.

   Après avoir cliqué sur **Suivant**, vous pouvez voir le résumé de toutes les informations fournies par l'utilisateur dans la section ci-dessus, et la section ci-dessous vous fournit tous les enregistrements qui doivent être importés.

   L'utilisateur peut effectuer n'importe quel type d'activités et les multiples utilisateurs peuvent collaborer à l'aide de la section des commentaires disponible dans le menu contextuel de droite.

   Remarque : Tous les enregistrements qui échouent aux validations sont ignorés du processus d'importation et ne sont pas affichés sur la page Révision et soumission pour un traitement ultérieur.

7. Cliquez sur **Mettre à jour le type** et sélectionnez le type pour mettre à jour n'importe quel type d'enregistrements importés.
8. Cliquez sur **Supprimer** pour supprimer tout type d'enregistrements importés.
9. Cliquez sur **Envoyer**.

   Remarque :

   Une fois l'enregistrement d'importation envoyé, l'utilisateur est dirigé vers l'approbateur pour approuver l'enregistrement d'importation correspondant en fonction des règles d'approbation configurées. Si l'utilisateur actuel qui crée l'enregistrement n'a pas besoin du processus d'approbation, l'enregistrement passe par le processus d'approbation automatique, la tâche d'importation est approuvée automatiquement lors de la soumission de la demande.

10. Cliquez sur **Afficher l'état** pour afficher l'état de l'enregistrement ou cliquez sur **Terminé**. L'enregistrement affiche l'état traité une fois qu'il est traité.
11. Cliquez sur **Annuler** pour abandonner le processus d'importation.
12. Cliquez sur **Revenir** pour revenir à la page précédente et examiner l'enregistrement, si nécessaire.

Importer des données à l'aide de texte brut

Importez les données des observables en copiant et collant du texte brut ou en saisissant du texte libre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
   La page Bibliothèque de Renseignements sur les menaces s'affiche.
2. Cliquez sur **Renseignements sur l'importation**.

> **Important :**
> - Tous les caractères de neutralisation seront nettoyés dans le cadre de l'analyse et de l'extraction des observables.
> - Pour cette option de texte collé, seuls l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP sont extraits et aucun autre type d'observable n'est extrait pour l'importation de données. Dans le cas de ce type d'observables tels que les types de registre, de répertoire, ceux-ci sont ignorés de l'importation.

3. Cliquez sur **Importer à partir d'une carte texte brute** .

> **Important :** Lors de l'importation des données Threat Intelligence au format texte brut, les caractères sont limités à 10 000. L'option de texte brut peut être utilisée comme solution de contournement pour extraire les observables du PDF.

4. Remplissez les champs du formulaire.

Champ	Description
Zone de texte des données brutes	Entrez ou copiez et collez le texte brut ici dans cette zone de texte. **Remarque :** Vous ne pouvez saisir ou coller que du texte brut de 10 000 caractères.
Définir des définitions	
TLP	Sélectionnez l'indicateur TLP dans la liste déroulante à appliquer aux enregistrements importés.
Fiabilité (0-100)	Définissez la valeur de confiance.
Période d'expiration (jours)	Entrez la période d'expiration des enregistrements importés. **Remarque :** Il s'agit d'un champ obligatoire.
Ajouter un ou des observables à la liste de contrôle de sécurité	Sélectionnez cette option pour ajouter des observables à la liste des contrôles de sécurité appropriée. Cette option vous permet d'ajouter directement les observables à une liste de contrôles de sécurité lors de l'importation. Les options disponibles dans la liste déroulante sont les suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Liste d'autorisation ○ Liste de refus ○ Aucun L'option par défaut est **Aucun**.
Ajouter des balises	Utilisez les balises pour annoter ou marquer à l'oreille les enregistrements ingérés dans le système à partir de cette source. Tapez le nom de la balise dans la barre de recherche pour choisir les balises disponibles dans le système ou saisissez un nouveau nom de balise et cliquez sur Ajouter pour l'affecter à la source.
Taxonomie	
Sélectionner une taxonomie	Sélectionnez la taxonomie des données importées. À l'aide des taxonomies, définissez des dictionnaires qui peuvent être utilisés comme taxonomies affectées aux enregistrements de Renseignements sur les menaces. Par exemple, nomenclature CAPEC. Pour plus d'informations, consultez Création de taxonomies.

5. Cliquez sur **Suivant**.
6. Examinez les données avant de les soumettre pour traitement.

   Après avoir cliqué sur **Suivant**, vous pouvez voir le résumé de toutes les informations fournies par l'utilisateur dans la section ci-dessus, et la section ci-dessous vous fournit tous les enregistrements qui doivent être importés.

   L'utilisateur peut effectuer n'importe quel type d'activités et les multiples utilisateurs peuvent collaborer à l'aide de la section des commentaires disponible dans le menu contextuel de droite.

   Remarque : Tous les enregistrements qui échouent aux validations sont ignorés du processus d'importation et ne sont pas affichés sur la page Révision et soumission pour un traitement ultérieur.

7. Cliquez sur **Mettre à jour le type** et sélectionnez le type pour mettre à jour n'importe quel type d'enregistrements importés.
8. Cliquez sur **Supprimer** pour supprimer tout type d'enregistrements importés.
9. Cliquez sur **Envoyer**.

   Remarque : Une fois l'enregistrement d'importation envoyé, l'utilisateur est dirigé vers l'approbateur pour approuver l'enregistrement d'importation correspondant en fonction des règles d'approbation configurées. Si l'utilisateur actuel qui crée l'enregistrement n'a pas besoin du processus d'approbation, l'enregistrement passe par le processus d'approbation automatique, la tâche d'importation est approuvée automatiquement lors de la soumission de la demande.

10. Cliquez sur **Afficher l'état** pour afficher l'état de l'enregistrement ou cliquez sur **Terminé**. L'enregistrement affiche l'état traité une fois qu'il est traité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

11. Cliquez sur **Annuler** pour abandonner le processus d'importation.
12. Cliquez sur **Revenir** pour revenir à la page précédente et examiner l'enregistrement, si nécessaire.

Importer des données à l'aide d'un format de fichier non structuré

Chargez les données dans un format non structuré pris en charge à l'aide des formats de fichier tels que TXT, CSV, JSON, XLS, XLSX.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**. La page Bibliothèque de Renseignements sur les menaces s'affiche.
2. Cliquez sur **Renseignements sur l'importation**.

Important :
- Tous les caractères de neutralisation seront nettoyés dans le cadre de l'analyse et de l'extraction des observables.
- Pour cette option de format de fichier non structuré, seuls l'URL, le domaine, le nom de fichier, les hachages et l'adresse IP sont extraits et aucun autre type d'observable n'est extrait pour l'importation de données. Dans le cas d'un tel type d'observables tels que les types de registre, de répertoire, ceux-ci sont ignorés de l'importation.

3. Cliquez sur **Importer à partir d'une carte de fichier (non structurée).**

Remarque : Lors de l'importation des données Threat Intelligence dans les formats de fichier pris en charge tels que TXT, CSV, STIX 2.x JSON, MISP JSON ou Fichier structuré, la taille du fichier est limitée à 5 Mo.

4. Remplissez les champs du formulaire.

Champ	Description
Charger un fichier	Cliquez sur ce lien pour charger les données au format de fichier standard.
Définir des définitions	
TLP	Sélectionnez l'indicateur TLP dans la liste déroulante à appliquer aux enregistrements importés.
Fiabilité (0-100)	Définissez la valeur de confiance.
Période d'expiration (jours)	Saisissez la période d'expiration des observables associés. **Remarque :** Il s'agit d'un champ obligatoire.
Ajouter un ou des observables à la liste de contrôle de sécurité	Sélectionnez cette option pour ajouter des observables à la liste des contrôles de sécurité appropriée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Cette option vous permet d'ajouter directement les observables à une liste de contrôles de sécurité lors de l'importation. Les options disponibles dans la liste déroulante sont les suivantes : ○ Liste d'autorisation ○ Liste de refus ○ Aucun L'option par défaut est **Aucun**.
Ajouter des balises	Utilisez les balises pour annoter ou marquer à l'oreille les enregistrements ingérés dans le système à partir de cette source. Commencez à saisir le nom de la balise dans la barre de recherche pour choisir les balises disponibles dans le système ou saisissez un nouveau nom de balise et cliquez sur **Ajouter** pour l'affecter à la source.
Taxonomie	
Sélectionner une taxonomie	Sélectionnez la taxonomie des données importées. À l'aide des taxonomies, définissez des dictionnaires qui peuvent être utilisés comme taxonomies affectées aux enregistrements de Renseignements sur les menaces. Par exemple, nomenclature CAPEC. Pour plus d'informations, consultez Création de taxonomies.

5. Examinez les données avant de les soumettre pour traitement.

   Après avoir cliqué sur **Suivant**, vous pouvez voir le résumé de toutes les informations fournies par l'utilisateur dans la section ci-dessus, et la section ci-dessous vous fournit tous les enregistrements qui doivent être importés.

   L'utilisateur peut effectuer n'importe quel type d'activités et les multiples utilisateurs peuvent collaborer à l'aide de la section des commentaires disponible dans le menu contextuel de droite.

   Remarque : Les formats pris en charge pour importer les données sont TXT, CSV, JSON, XLS et tous les enregistrements qui échouent aux validations sont ignorés du processus d'importation et ne sont pas affichés sur la page Révision et soumission pour traitement.

6. Cliquez sur **Mettre à jour le type** et sélectionnez le type pour mettre à jour n'importe quel type d'enregistrements importés.
7. Cliquez sur **Supprimer** pour supprimer tout type d'enregistrements importés.
8. Cliquez sur **Envoyer**.

   Remarque : Une fois l'enregistrement d'importation envoyé, l'utilisateur est dirigé vers l'approbateur pour approuver l'enregistrement d'importation correspondant en fonction des règles d'approbation configurées. Si l'utilisateur actuel qui crée l'enregistrement n'a pas besoin du processus d'approbation, l'enregistrement passe par le processus d'approbation automatique, la tâche d'importation est approuvée automatiquement lors de la soumission de la demande.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Cliquez sur **Afficher l'état** pour afficher l'état de l'enregistrement ou cliquez sur **Terminé**. L'enregistrement affiche l'état traité une fois la soumission réussie.
10. Cliquez sur **Annuler** pour abandonner le processus d'importation.
11. Cliquez sur **Revenir** pour revenir à la page précédente et examiner l'enregistrement, si nécessaire.

Console d'analyste de menaces

La page Console d'analyste de menaces répertorie les tickets et les tâches de ticket qui relèvent des analystes de menaces et de leur équipe.

Utilisez la fonctionnalité **Gestion des tickets** pour créer et suivre les enquêtes sur les menaces et les activités d'analyse.

Au cours des enquêtes sur les menaces, les analystes collectent les données des enregistrements de renseignement interne tels que les observables, les acteurs de menace, les campagnes, etc.

Vue d'ensemble de la console

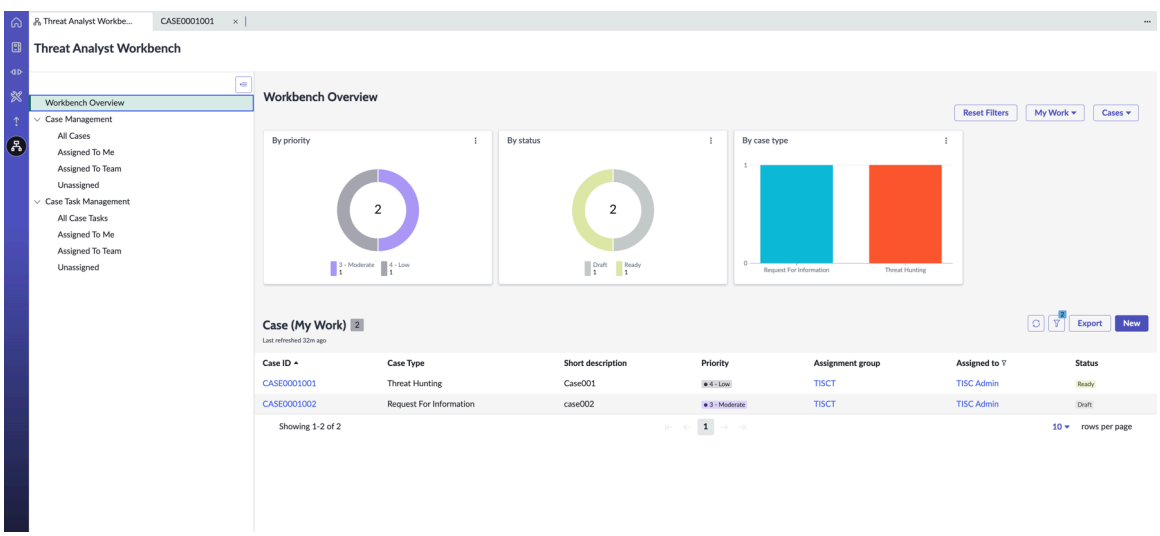
La page Vue d'ensemble de la console comprend les tâches de ticket et les tickets qui relèvent des analystes de menaces et de leur équipe.

La vue d'ensemble répertorie tous les tickets ouverts et leur statut, ce qui aide les analystes à gérer leur charge de travail et à hiérarchiser leurs enquêtes.

Rôle requis : sn_sec_tisc.analyst, sn_sec_tisc.admin

Une fois le ticket créé, les analystes affecteront les tâches du ticket à d'autres analystes ou équipes pour une enquête plus approfondie, et collaboreront également avec eux pour partager des informations et des idées.

Différents widgets sont présents sous chaque filtre, regroupés par priorité, statut et type de ticket qui se trouvent dans les files d'attente des analystes de menaces et de l'équipe d'analystes de menaces.



Lorsque des filtres sont appliqués aux widgets, la moitié inférieure de la page de vue d'ensemble est remplie avec les tickets ou tâches de ticket correspondants présentés sous forme d'éléments de liste. Pour supprimer les filtres appliqués, cliquez sur Réinitialiser les **filtres** pour rétablir la vue d'origine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À l'aide de cette page, les analystes de menaces et les administrateurs peuvent afficher leur travail, le travail des équipes et tout travail non affecté. Vous pouvez accéder à la liste déroulante. Les options disponibles sont les suivantes :

- Mes tâches : sélectionnez cette option pour afficher les tâches qui vous sont affectées.
- Travail de mon équipe : sélectionnez cette option pour afficher le travail de votre équipe affecté à tous les groupes dont vous faites partie.
- Travail non affecté : sélectionnez cette option pour afficher le ticket ou la tâche de ticket non affecté. Pour affecter le ticket ou la tâche de ticket, vous devez accéder à la vue de formulaire et affecter le ou les utilisateurs ou le ou les groupes d'utilisateurs au ticket et à la ou aux tâches de ticket.

Vous pouvez également afficher les tickets et les tâches de ticket directement à partir de la vue d'ensemble de la console qui vous sont affectées. Par défaut, la vue de ticket s'affiche. Vous pouvez utiliser la liste déroulante et sélectionner les tâches de ticket si vous souhaitez afficher les tâches de ticket par priorité et état.

Création de tickets à l'aide de la Console d'analyste de menaces

Les tickets sont utilisés pour suivre les informations sur une campagne ou un acteur malveillant menaçant votre organisation. Une fois qu'un ticket est créé, vous pouvez ajouter des artefacts qui vous permettent d'examiner et d'analyser toutes les informations connexes à partir d'un seul ticket ou d'une seule tâche de ticket.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst, sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs comme il convient.

Créer un ticket

Champ	Description
ID du ticket	Un identificateur unique pour le ticket. Il s'agit d'un ID généré par le système.
Description brève	Résumé de la demande ou du problème en cours d'examen ou brève description.
Description	Une description détaillée comprenant toute information pertinente sur le ticket telle que le contexte, l'analyse requise et les résultats attendus.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête. Les options possibles pour l'enquête sont les suivantes : ○ Recherche des menaces ○ Demande d'informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Ticket de gestion de la vulnérabilité ○ Ticket de conformité ○ Ticket de réponse aux incidents ○ Ticket de collaboration ○ Autres
Priorité	Une évaluation de la gravité de la demande ou du problème.
Groupe d'affectation	Le groupe affecté responsable du travail sur le ticket.
Statut	État actuel du ticket.
Affecté à	L'analyste responsable du travail sur un ticket.
Date d'échéance	Date et heure auxquelles la tâche doit être terminée ou fermée.
Contributeurs	Liste des délégataires déployée à partir des tâches et il doit être possible de l'ajouter par-dessus.
TLP	Valeur unique qui indique le paramètre de sensibilité des données par TLP.
Liste de surveillance	Lorsqu'un utilisateur est ajouté à la liste de surveillance, il reçoit des notifications par e-mail sur les changements de statut et de priorité.
Appliquer la restriction	Cochez cette case pour modifier les membres du groupe autorisé et les membres autorisés. Pour plus d'informations, consultez Restrictions appliquées pour le(s) ticket(s).

6. Renseignez les champs de la section Aperçus, le cas échéant.

Aperçus

Champ	Description
Notes	Toute remarque supplémentaire relative à l'enquête sur les menaces.
Recommandations ou actions	Toute recommandation ou action liée à l'enquête sur les menaces.
Analyses et résultats	Saisissez l'analyse et les conclusions relatives à l'enquête sur les menaces.
Synthèse de fermeture	Ajoutez le résumé de clôture des résultats.

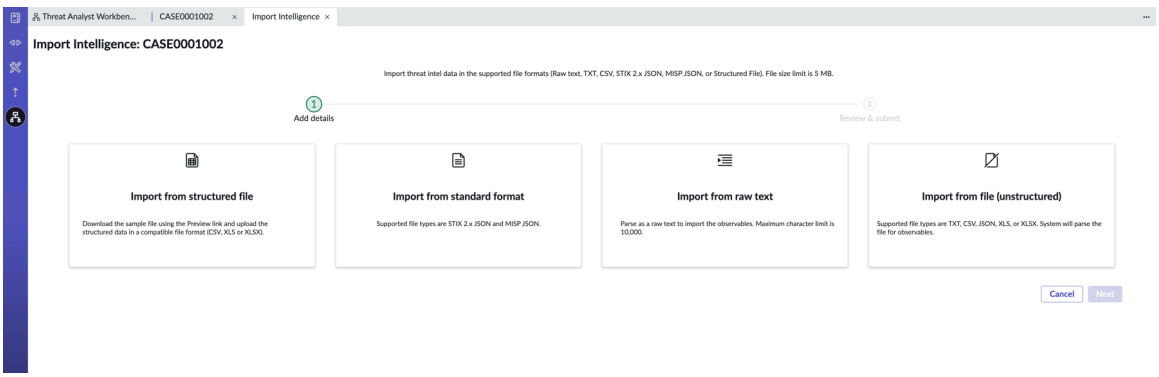
7. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois l'enregistrement sauvegardé, vous pouvez cliquer sur l'onglet **Import Intelligence** pour importer les données Threat Intelligence à l'aide de la fonctionnalité **Import Intelligence** .

Remarque : Si vous importez et traitez des données à partir de la gestion des tickets, un élément unique est associé à l'enregistrement d'importation.



Restrictions appliquées pour le(s) ticket(s)

Utilisez cette fonctionnalité pour restreindre un ticket et fournir une liste des groupes et des utilisateurs qui peuvent y accéder.

Rôle requis :

- sn_sec_tisc.analyste
- sn_sec_tisc_admin
- sn_sec_tisc.restriction_access_manager

Considérations clés

1. Restreignez un ticket et fournissez une liste de groupes/utilisateurs qui peuvent y accéder.
2. Activez le champ Appliquer la restriction sur la page du formulaire de ticket.
3. Modifier les membres du groupe autorisé et les membres autorisés.
4. Une fois qu'un ticket est marqué comme restreint, seuls les membres des groupes autorisés, les membres de la liste des utilisateurs autorisés et l'utilisateur disposant du rôle sn_sec_tisc.admin peuvent accéder à ce ticket.
5. Accordez l'accès à l'analyste (sn_sec_tisc.restriction_access_manager avec ce rôle) qui doit accéder au champ Appliquer la restriction.
6. L'analyste assigned_to existant et l'analyste qui l'a marqué comme restreint perdront également l'accès s'ils ne sont pas ajoutés aux groupes ou membres autorisés.
7. La restriction de ticket au sein de l'équipe CTI est mise en œuvre au cas par cas. Les membres autorisés peuvent accéder aux tickets restreints s'ils figurent sur la liste des autorisations. Les mettre dans l'une des cases autorisées ne signifie pas qu'ils peuvent accéder à toutes les autres cases restreintes.
8. Si le ticket est marqué comme restreint et membres autorisés ou si le groupe autorisé est laissé vide, seul sn_sec_tisc.admin peut accéder à ces tickets restreints.
9. Seuls les groupes auxquels le rôle d'analyste (sn_sec_tisc.analyst) est affecté sont autorisés dans la liste Membres autorisés et Groupes autorisés.

Remarque : Une note de travail est publiée si un ticket est marqué comme restreint.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôles d’accès pour un ticket

Autorisez les contrôles d’accès spécifiques à un ticket.

La table suivante décrit les rôles et les contrôles d’accès.

Rôle	Accès	Description
sn_sec_tisc.restriction_access_manager	Accès en lecture	Les utilisateurs externes ajoutés ici auront accès à l’affichage du formulaire de ticket, mais ne pourront modifier aucun champ du ticket ni effectuer aucune action.
	Accès privilégié	Les utilisateurs externes ajoutés ici auront accès à la modification de n’importe quel champ du formulaire de ticket, mais ne seront pas autorisés à exécuter des orchestrations.
sn_sec_tisc.special_access_read_manager	Accès en lecture	Les utilisateurs externes ajoutés ici auront accès à l’affichage du formulaire de ticket, mais ne pourront modifier aucun champ du ticket ni effectuer aucune action.
sn_sec_tisc.special_access_write_manager	Accès privilégié	Les utilisateurs externes ajoutés ici auront accès à la modification de n’importe quel champ du formulaire de ticket, mais ne seront pas autorisés à exécuter des orchestrations.

Accès de l’utilisateur externe aux tâches de tickets

Cette section décrit l’accès de l’utilisateur externe pour les tâches de ticket.

Affectation de tâches de ticket à des utilisateurs externes

Les tâches de ticket sont affectées aux utilisateurs ayant le rôle externe même s’ils n’ont pas accès au rôle sn_sec_tisc.analyst.

1. Tout utilisateur externe affecté à une tâche de ticket peut uniquement afficher le module de tâche de ticket et aura le privilège de modifier la tâche de ticket.
2. L’utilisateur externe peut uniquement afficher les tâches de ticket affectées à cet utilisateur spécifique ou au(x) groupe(s) auquel l’utilisateur appartient.
3. L’utilisateur externe doit être en mesure de réaffecter la tâche au sein du groupe auquel il appartient.

Associer des techniques MITRE à un ticket

Associez une ou plusieurs techniques MITRE à un ticket.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez n'importe quel ticket.
5. Cliquez sur le bouton **Associer la technique MITRE** .
6. Cliquez sur **Ajouter une matrice** pour associer la technique MITRE.
   La boîte **de dialogue Associer la technique MITRE au ticket s'affiche** .
7. Sélectionnez la **matrice**.
   Toutes les matrices activées s'affichent pour que vous puissiez sélectionner la matrice.
8. Sélectionnez la tactique dans les listes déroulantes.
   Toutes les tactiques associées à une matrice seront affichées.

   Remarque : Si vous souhaitez ajouter d'autres tactiques, cliquez sur **Ajouter une tactique**. Les tactiques précédemment sélectionnées ne seront plus affichées dans la liste déroulante si vous ajoutez une nouvelle tactique.

9. Sélectionnez la **technique**.
   Toutes les techniques associées à la tactique que vous avez sélectionnée s'affichent. Si vous ajoutez d'autres tactiques, vous pouvez sélectionner les techniques associées pour ces tactiques sélectionnées.
10. Cliquez sur **Enregistrer**.
    Si vous souhaitez supprimer l'intégralité des données associées à la **matrice**, cliquez sur Supprimer la matrice, cette action supprimera uniquement les données de matrice associées, mais la matrice restera dans le référentiel MITRE ATT&CK.

    L'enregistrement de données matricielles associé s'affiche sous la section Carte MITRE ATT&CK. Dans la vue de carte :

    Remarque : Vous pouvez basculer entre plusieurs matrices à partir de la liste déroulante Matrix.

    a. La première ligne de la vue de la carte affiche toutes les tactiques associées à la matrice sélectionnée actuelle.
    b. Chaque carte de tactique affiche le nom de la tactique et le nombre de techniques de cette tactique mappées à l'enregistrement du ticket actuel.
    c. Toutes les techniques associées à ce cas sont affichées verticalement sous chaque tactique. Vous pouvez cliquer sur n'importe quelle technique pour afficher la vue de formulaire technique.
11. Cliquez sur **Afficher l'ID** pour afficher les ID de toutes les techniques associées.

    Remarque : Chaque carte de technique affiche le nom et l'ID de la technique uniquement lorsque **l'option Afficher l'ID** est activée.

12. Cliquez sur **Actualiser** pour actualiser la vue de la carte.
    Vous pouvez afficher l'horodatage de la dernière actualisation de la matrice sélectionnée.

    Remarque : Cliquez sur l'icône contextuelle pour afficher la carte matricielle associée dans un nouvel onglet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déploiement des associations de techniques MITRE

Déploiement des associations de techniques MITRE à partir d'observables, d'indicateurs, d'objets et d'incidents de sécurité liés ou non d'un enregistrement de ticket.

Avant de commencer

Remarque :

- Le déploiement des associations de techniques MITRE pour les incidents de sécurité permet de déployer les données associées à la technique MITRE à partir des incidents de sécurité vers la gestion des tickets dans TISC.
- Par défaut, cette propriété sn_sec_tisc.auto_rollup_mitre_data est activée pour que la ou les techniques MITRE soient déployées automatiquement dans des tickets à partir des objets associés ou des incidents de sécurité.
- Si vous souhaitez effectuer un déploiement à la demande d'associations de techniques MITRE, accédez à Actions supplémentaires dans la **vue du formulaire Ticket** et sélectionnez **l'option Déployer les techniques MITRE** . Cette opération se produit de manière asynchrone et vous pouvez vérifier la section **Flux d'activité** pour les mises à jour de l'activité de déploiement.

Rôle requis : sn_sec_tisc.analyst

Pourquoi et quand exécuter cette tâche

- Chaque fois qu'une entité telle qu'un observable ou un indicateur est liée à un cas, toutes les associations de techniques MITRE présentes pour cette entité sont automatiquement déployées sur le ticket.
- Chaque fois qu'une entité, telle qu'un observable ou un indicateur, est dissociée et supprimée du ticket, toutes les associations de techniques MITRE qui sont déployées à partir du ticket et qui sont présentes pour cette entité sont automatiquement supprimées et déployées dans le ticket.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Ouvrez n'importe quel ticket.
5. Accédez à l'onglet **Artefacts** .
6. Sélectionnez **Observables** dans la liste connexe Artefacts.
7. Sélectionnez le bouton **Lien** .
8. Sélectionnez les observables que vous souhaitez peut-être lier au ticket.
9. Cliquez sur **un lien** pour lier les observables.
   Une fois que vous avez lié les observables à un ticket, les techniques MITRE associées à cet observable particulier sont automatiquement déployées et le nombre de listes de techniques MITRE sous la section Artefacts est automatiquement mis à jour.
10. Cliquez sur **Dissocier** pour dissocier les observables du ticket.
    Une fois que vous avez dissocié les observables d'un ticket, les techniques MITRE associées à cet observable particulier sont automatiquement supprimées et le nombre de listes de techniques MITRE sous la section Artefacts est automatiquement mis à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Création d'une tâche de ticket à l'aide de la Console d'analyste de menaces

Créez des tâches de ticket à associer à un ou plusieurs tickets.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst, sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tâches de ticket** > **Toutes les tâches de tickets**.
   Toutes les tâches de ticket s'affichent.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs comme il convient.

Créer une nouvelle tâche de ticket

Champ	Description
ID de tâche	Un identificateur unique pour la tâche de ticket. Il s'agit d'un ID généré par le système.
Description brève	Résumé de la demande ou du problème en cours d'examen ou brève description.
Description	Description détaillée comprenant toute information pertinente sur la tâche de ticket comme le contexte, l'analyse requise et les résultats attendus.
ID de ticket parent	Sélectionnez l'ID du ticket parent à partir de la recherche.
Priorité	Une évaluation de la gravité de la demande ou du problème.
Groupe d'affectation	Le groupe affecté responsable du travail sur la tâche de ticket.
Statut	État actuel de la tâche de ticket.
Affecté à	L'analyste responsable du travail sur une tâche de ticket.
Date d'échéance	Date et heure auxquelles la tâche de ticket doit être terminée ou fermée.
TLP	Valeur unique qui indique le paramètre de sensibilité des données par TLP.
Appliquer la restriction	En sn_sec_tisc_admin, cochez cette case pour modifier les membres du groupe autorisé et les membres autorisés. Pour plus d'informations, consultez Restrictions appliquées pour le(s) ticket(s).

6. Renseignez les champs de la section Aperçus, le cas échéant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus

Champ	Description
Notes	Toute remarque supplémentaire relative à l'enquête sur les menaces.
Fermeture	Ajoutez le résumé de clôture des résultats.

7. Cliquez sur **Enregistrer**.
   Votre tâche de ticket sera associée à votre ticket.

> **Remarque :** Après avoir enregistré la tâche de ticket, vous pouvez ajouter des balises et des taxonomies à la tâche. Pour plus d'informations, consultez Création de taxonomies.

Utilisation du canevas d'enquête

Le canevas d'examen est une fonctionnalité importante qui fournit des informations plus précieuses aux analystes de Threat Intelligence (TI). Il fournit un cadre de travail structuré en mappant les relations un à un ou un à plusieurs et en visualisant des informations relatives aux observables, aux indicateurs de compromis (IOC) ou aux entités.

En utilisant le canevas d'enquête, les analystes de menaces peuvent efficacement :

- **Relations de cartes** : visualisez les connexions de nœuds entre diverses entités, telles que les observables, les indicateurs de compromission, les auteurs de menace, les schémas d'attaque, les actifs affectés, entre autres. Chaque objet sur le canevas d'enquête est représenté par une couleur spécifique, ainsi que son type d'objet, son type de nœud et son état. L'état reflète la réputation de l'objet (**suspect,faible** ou **critique**) pour les observables et les autres types d'objets. Les indicateurs sont affichés avec leur gravité de menace associée pour aider à hiérarchiser l'analyse.
- **Lier les tickets ou les canevas** : liez un ticket ou un canevas pour améliorer l'analyse et fournir une vue plus complète du paysage des menaces au sein de la gestion des tickets.
  - La fonctionnalité de liaison permet aux analystes d'ajouter ou de supprimer des nœuds dynamiquement. Les relations existantes entre les nœuds et le canevas sont également renseignées.
  - Graphiques de relations temporaires en enregistrant les relations séparément dans le contexte du canevas d'enquête.
- **Associations de techniques MITRE** : associez ou supprimez des techniques MITRE à des nœuds directement sur le canevas et fournissez une analyse sur la carte de chaîne de frappe MITRE.

Points d'entrée pour le canevas d'examen

1. **Premier point d'entrée : Nouveau canevas vierge** : Ce point d'entrée doit permettre aux analystes d'ouvrir un nouveau canevas vierge sans aucun nœud ni lien.
2. **Deuxième point d'entrée : canevas ouvert dans l'enquête sur le ticket** :
   a. Ce point d'entrée ouvre un ticket d'enquête existant et permet d'éditer, de modifier et de renommer le canevas.
   b. Un nouveau canevas avec des artefacts existants en tant que nœuds.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

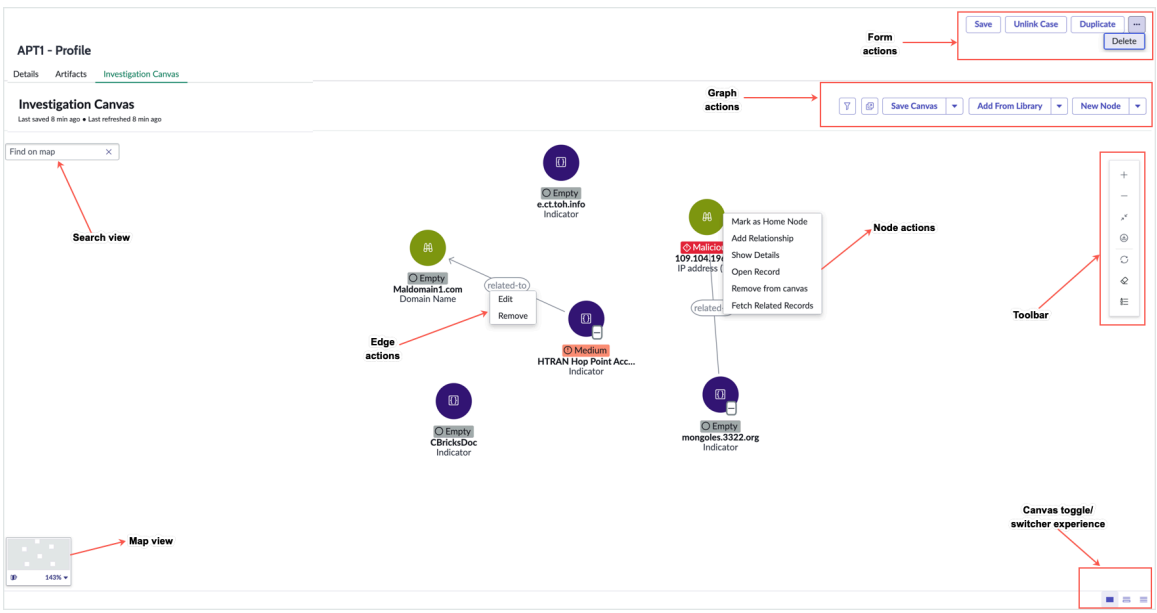
Utiliser des actions sur le canevas d’examen

Cette section décrit les différentes actions que vous pouvez effectuer sur le canevas d’enquête.

Le canevas d’examen comprend :

1. Actions des formulaires
2. Actions du graphique
3. Actions de nœud
4. Actions de bordure
5. Actions de la barre d’outils

Canevas d'examen



Canevas d’examen Actions de formulaire

Action	Opération
Lien vers le ticket	Vous permet de lier le ticket sur le canevas d’enquête.
Annuler lien du ticket	Vous permet de dissocier le ticket sur le canevas d’enquête.
Enregistrer	Option permettant de sauvegarder l’enregistrement du ticket.
Dupliquer	Option permettant de dupliquer les nœuds sur le canevas d’examen.
Supprimer	Option pour supprimer le canevas.

Canevas d’examen Actions du graphique

Action	Opération
Rechercher sur la carte	Vous permet d’effectuer des recherches dans différents nœuds et bordures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Canevas d'examen Actions du graphique (suite)

Action	Opération
Filtre de canevas	La fonctionnalité **Filtre** vous aide à affiner votre vue sur le canevas d'examen. Par exemple, si vous filtrez un type d'enregistrement tel que Campagne, il est temporairement supprimé de l'affichage du canevas. En appliquant des filtres, vous pouvez contrôler les types d'entités ou d'enregistrements affichés sur la carte, ce qui permet une expérience d'enquête plus propre et plus ciblée. **Remarque :** Utilisez des filtres pour mettre en évidence uniquement les nœuds les plus pertinents, tels que les observables ou les auteurs de menace, tout en masquant temporairement les informations moins critiques sur le canevas.
Enregistrer le canevas	Vous permet d'enregistrer le canevas d'enquête.
Ajouter des données à la bibliothèque	Cette option vous permet d'établir une nouvelle relation entre deux nœuds différents sur le canevas d'examen. Toutes les modifications apportées sur le canevas, y compris les nouveaux nœuds, les nouveaux liens entre les nœuds et les étiquettes de bordure modifiées ou modifiées, seront enregistrées dans la bibliothèque. Tous les nœuds actuellement présents sur le canevas seront ajoutés en tant qu'artefacts au ticket lié. Un message de confirmation s'affichera une fois les données enregistrées avec succès dans la bibliothèque.
Ajouter à partir de la bibliothèque	Cette action ajoute les données de la bibliothèque Threat Intelligence et établit également la relation entre le nouveau nœud importé de la bibliothèque Threat Intelligence et les nœuds existants sur le canevas d'examen.
Ajouter à partir des artefacts de ticket	Vous permet d'ajouter des données à partir d'artefacts de ticket correspondants liés au canevas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Canevas d'examen Actions de nœud

Action	Opération
Marquer comme nœud d'accueil	Cette option vous permet de marquer un noeud spécifique comme noeud d'accueil sur le canevas d'examen. Lors du pivotement pendant l'analyse, l'application met automatiquement en surbrillance et centre le nœud d'accueil, en le plaçant au centre du canevas. Le nœud ciblé est visuellement mis en évidence par : • Une frontière distincte • Soulignant • Une animation de mouvement circulaire subtile Il est ainsi plus facile d'identifier et d'explorer les données du canevas liées à l'objectif principal de votre enquête.
Ajouter une relation	Cette option vous permet d'ajouter des relations personnalisées entre les nœuds sur le canevas d'examen. Vous pouvez définir des types de relations tels que : • Un-à-plusieurs • Plusieurs-à-un • Plusieurs-à-plusieurs Cela permet de représenter des associations complexes entre les entités.
Afficher les détails	Cette option vous permet d'afficher des informations détaillées sur le nœud sélectionné sur le canevas d'examen, y compris ses attributs et tous les observables ou relations associés.
Ouvrir l'enregistrement	Cette option vous permet d'ouvrir l'enregistrement sélectionné dans un nouvel onglet de navigateur pour faciliter la consultation et le multitâche.
Supprimer de la zone de travail	Cette option vous permet de supprimer le nœud sélectionné du canevas d'examen, le supprimant ainsi de la vue actuelle.
Extraire les enregistrements connexes	Cette option vous permet d'extraire les enregistrements connexes pour un nœud spécifique et de les ajouter directement au canevas d'examen à l'aide de la boîte de dialogue **Sélectionner les types d'entité** . Sélectionnez **l'option Ajouter tout** pour inclure automatiquement tous les types

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Canevas d'examen Actions de nœud (suite)

Action	Opération
	d'enregistrements associés à l'objet dans la zone de sélection indiquée. Par exemple, s'il existe 5 à 10 types différents d'enregistrements connexes, vous devrez sélectionner manuellement chaque type d'objet. La fonctionnalité **Ajouter tout** rationalise ce processus en remplissant tous les enregistrements pertinents à la fois, améliorant ainsi l'expérience utilisateur. Après avoir ajouté des enregistrements, vous pouvez les supprimer ou sélectionner l'option **Développer** pour afficher les nœuds connexes. Cependant, pour améliorer la convivialité, vous pouvez maintenant sélectionner **Développer tout** pour développer instantanément tous les enregistrements connexes liés à un nœud, au lieu d'ajouter ou de développer manuellement les enregistrements.

Canevas d'examen Actions de bordure

Action	Opération
Modifier	Cette option vous permet d'éditer et de modifier l'étiquette d'une arête sur le canevas d'examen, ce qui permet une représentation plus claire des relations entre les nœuds.
Supprimer	Cette option vous permet de supprimer une arête du canevas d'enquête, supprimant ainsi la connexion visuelle entre deux nœuds.

Icônes de la barre d'outils du canevas d'examen

Action	Opération
Zoom avant	Option permettant de zoomer dans le canevas d'examen pour se concentrer facilement sur des zones spécifiques du canevas.
Zoom arrière	Option permettant de faire un zoom arrière sur le canevas d'enquête pour se concentrer facilement sur des zones spécifiques du canevas.
Adapter à l'écran	Option permettant d'adapter le canevas d'examen à la taille de l'écran.
Exporter la carte	Option permettant d'exporter le canevas d'enquête au format PDF pour une meilleure visualisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

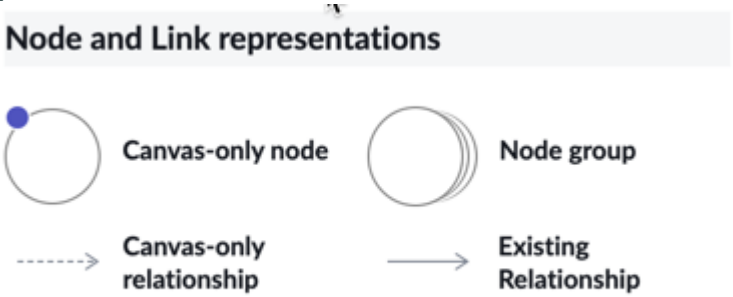
Icônes de la barre d'outils du canevas d'examen (suite)

Action	Opération
Actualiser	L'option **Actualiser** vous permet d'actualiser et de recharger les données de la bibliothèque sur le canevas d'enquête. **Remarque :** Toutes les modifications non enregistrées sur le canevas seront perdues si vous actualisez sans enregistrer. Il est recommandé d'enregistrer votre canevas avant de rafraîchir pour éviter la perte de données.
Effacer le canevas	Vous permet d'effacer le canevas. Cette sélection supprimera temporairement les nœuds du canevas d'examen. Un message de confirmation s'affiche, vous invitant à confirmer si vous souhaitez effacer le canevas. Accusez réception du message pour continuer. **Remarque :** Après avoir apporté des modifications sur le canevas d'examen, vous devez **enregistrer** le canevas. Si les modifications ne sont pas enregistrées et si vous actualisez le canevas, il reviendra à son état précédent et tous les nœuds ou modifications non enregistrés seront perdus.
Légende	Cette option vous fournit une représentation visuelle des nœuds et des entités actuellement affichés sur le canevas d'examen. La légende comprend deux vues principales : • **Représentation de nœuds et de liens** : affiche la façon dont les différents types de nœuds apparaissent sur le canevas et comment ils sont connectés via des bordures. Cela vous aide à comprendre rapidement la structure et la relation entre les différents éléments de l'enquête. • **Représentation des entités** : affiche les types d'entités actuellement présentes sur le canevas (observables, indicateurs et objets). L'élément suivant illustre les légendes des représentations de nœud, de lien et d'entité :

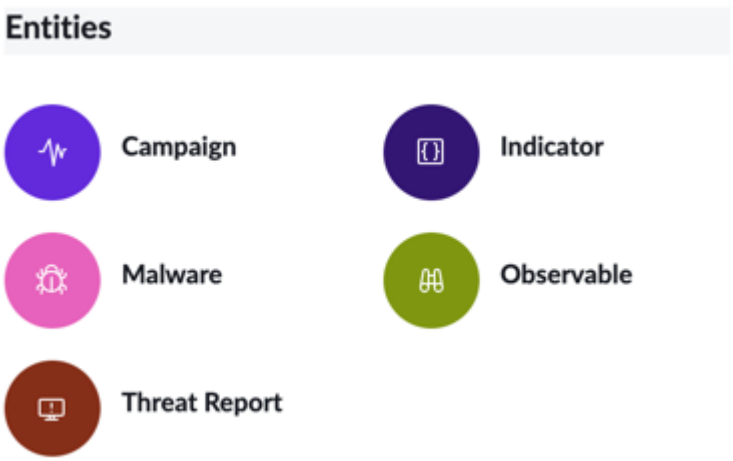
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Représentation de nœuds et de liens



Représentation des entités



Regroupement ou dissociation d'enregistrements du canevas d'examen

La fonctionnalité de groupe vous permet de regrouper des nœuds pour faciliter l'analyse. Un bouton de regroupement a été ajouté à côté des nœuds qui peuvent être regroupés. Par défaut, ce bouton affiche une icône moins (–) sur le canevas, indiquant que le nœud connecté peut être réduit ou regroupé.

N'importe quel nœud de degré externe serait pris en compte pour un groupe.

Remarque : L'icône de groupe est introduite pour réduire l'encombrement sur le canevas et simplifier la navigation pendant les enquêtes critiques. Pour les nœuds sans bordures supplémentaires (connexions), le bouton de regroupement ne s'affiche pas car il n'existe aucun nœud connexe disponible pour le regroupement.

Le tableau suivant explique les instructions lors du regroupement ou de l'annulation du groupement des nœuds :

Action	Résultat
Regroupement d'un nœud	• Tous les nœuds enfants avec un seul parent (même sur plusieurs niveaux) seront masqués au sein du groupe. • Les nœuds avec plusieurs parents restent visibles, mais les connexions du groupe à eux seront masquées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action	Résultat
Dissociation d’un nœud	• Révèle tous les nœuds précédemment masqués avec un parent et leurs connexions. • Si des nœuds avec plusieurs parents étaient déjà visibles, leurs connexions masquées seront également restaurées.
Importation du nœud/extraction des enregistrements connexes	Développe automatiquement un groupe réduit si le nouveau nœud se connecte à un nœud masqué à l’intérieur de celui-ci.
Actions autorisées	Les nœuds groupés prennent uniquement en charge l’action **Afficher les détails** , qui affiche les détails du nœud parent. Les autres actions sont désactivées.
Filtre	Le filtrage **des nœuds non groupés suit le** comportement de filtrage standard, tout en respectant les règles de regroupement. Le filtrage **d’un nœud groupé** masque l’ensemble du groupe et son nœud enfant.
Autres actions	Les actions telles que la suppression d’un nœud ou la modification des bordures suivent toutes les règles et tous les comportements de regroupement.

Lier un ticket existant à partir du canevas d’enquête

Utilisez cette section pour lier un ticket existant à partir du canevas d’enquête.

Avant de commencer

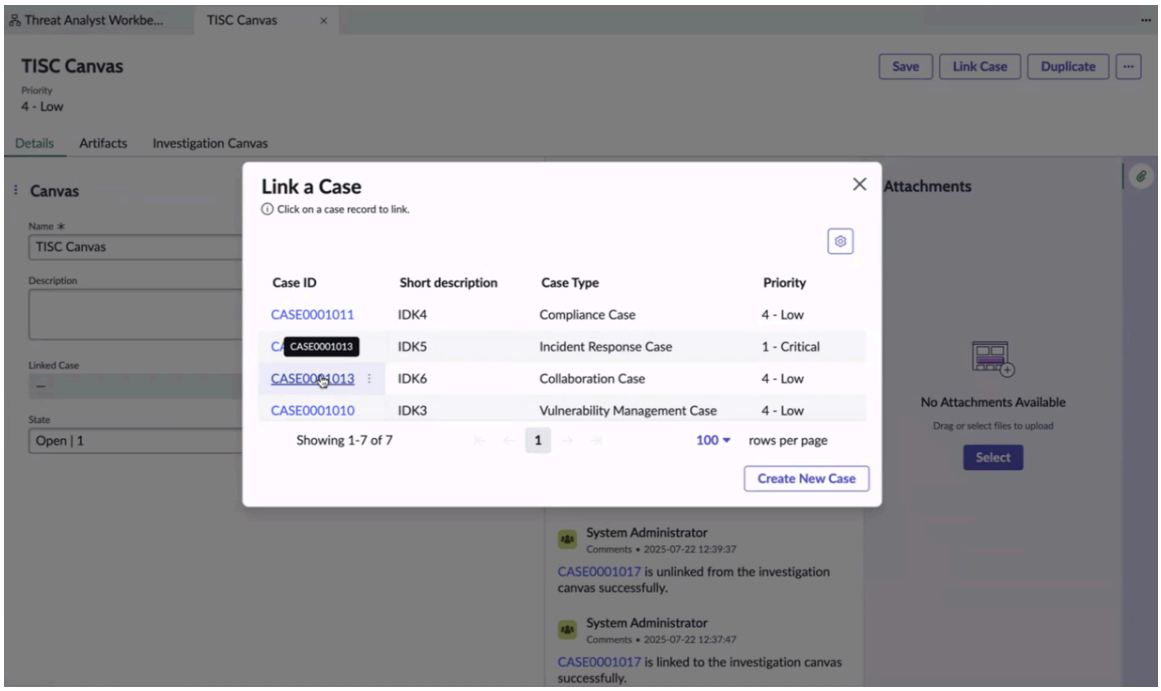
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Sélectionnez l’icône **Console d’analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionner **Gestion des tickets** > **Tous les tickets**
5. Ouvrez n’importe quel enregistrement de ticket à partir de la vue de liste.
6. Sélectionnez **Lier le ticket** dans la section **Détails** .
   La boîte de dialogue Lier un ticket s’affiche.
7. Sélectionnez un ID de ticket dans la liste pour associer le ticket à un canevas d’enquête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un message de confirmation s’affiche confirmant que le ticket est lié avec succès.

Remarque : Si aucun ticket n’est disponible pour être lié au canevas d’enquête, vous pouvez créer un nouveau ticket pour lancer et organiser votre contexte d’enquête. Pour en savoir plus sur la création d’un ticket, consultez Création d’un ticket et liaison à partir du canevas d’enquête

.

8. Pour supprimer un ticket lié, sélectionnez le bouton **Dissocier** .

Information associée

Création d’un canevas d’examen

Création d’un ticket et liaison à partir du canevas d’enquête

Utilisez cette section pour créer et lier un ou plusieurs tickets à partir d’un canevas d’enquête.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Sélectionnez l’icône **Console d’analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Ouvrez n’importe quel enregistrement de ticket de la liste.
5. Sélectionnez **Lier le ticket** dans la section **Détails** .
   La boîte de dialogue Créer et lier un ticket s’affiche.
6. Sélectionnez un ticket dans la liste pour l’associer à un canevas d’enquête.
7. Sélectionnez **Créer un canevas**.
   La boîte de dialogue Créer un nouveau ticket s’affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Renseignez les champs de formulaire comme il convient.

Champ	Description
ID du ticket	Un identificateur unique pour le ticket. Il s'agit d'un ID généré par le système.
Description brève	Résumé de la demande ou du problème en cours d'examen ou brève description.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête. Les options possibles pour l'enquête sont les suivantes : ○ Recherche des menaces ○ Demande d'informations ○ Ticket de gestion de la vulnérabilité ○ Ticket de conformité ○ Ticket de réponse aux incidents ○ Ticket de collaboration ○ Autres
Priorité	Indique la priorité d'un ticket.
Groupe d'affectation	Le groupe affecté responsable du travail sur le ticket.
Statut	État actuel du ticket.
Affecté à	L'analyste responsable du travail sur un ticket.

9. Sélectionnez **Créer et lier** pour créer un nouveau ticket et le lier directement au canevas d'enquête.

   Une confirmation s'affiche et confirme que le ticket est créé et lié au canevas d'enquête avec succès.

   Remarque : Cette option est utile lorsqu'aucun ticket existant n'est associé au canevas d'enquête.

10. Pour supprimer un ticket lié, sélectionnez le bouton **Dissocier** .
    Pour en savoir plus sur la façon de lier directement un ticket existant au canevas d'enquête, reportez-vous à la section Lier un ticket existant à partir du canevas d'enquête.

Information associée

Création d'un canevas d'examen

Liaison du canevas à partir d'un ticket

Utilisez cette section pour lier un canevas à partir d'un ticket.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

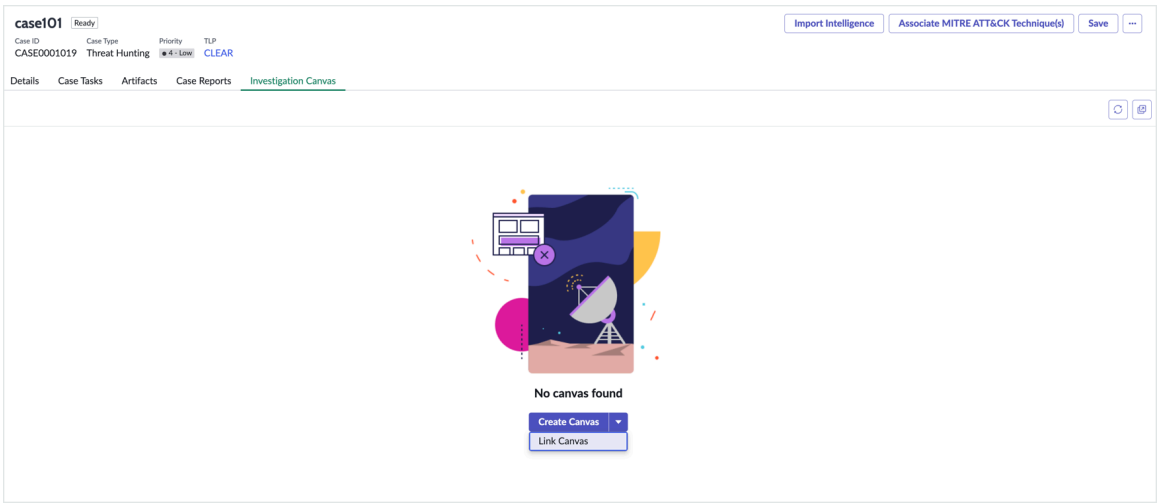
Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Accéder à **Canevas d'examen** > **Tous les canevas**.
4. Dans la vue de liste **Tous les tickets** , sélectionnez un ticket qui n'est pas lié au canevas.
5. Accédez à la section **Canevas d'enquête** .
6. Sélectionnez **Lier la casse** dans la liste déroulante sur la page de canevas vide (l'option est affichée dans la capture d'écran suivante).



7. Sélectionnez le canevas.
8. Sélectionnez le bouton **Lien** pour lier le canevas à un ticket.

   Un message d'information s'affiche indiquant que les données du canevas ont été actualisées avec succès.

Création d'un canevas d'examen

Créez un canevas pour ajouter des observables à partir de la bibliothèque Threat Intelligence.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Canevas d'examen** > **Tous les canevas**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs comme il convient.

Créer un canevas

Champ	Description
Nom	Entrez le nom du canevas.
Description	Ajoutez la description du canevas.
Ticket lié	Cette option affiche une liste de tickets auxquels aucun canevas n'est associé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Le champ est renseigné dynamiquement en fonction de l'absence d'un canevas lié pour chaque ticket, ce qui permet aux utilisateurs d'identifier facilement les tickets qui peuvent nécessiter la création ou la liaison de contextes d'enquête.
Priorité	Sélectionnez la priorité du canevas.
État	Sélectionnez l'état du canevas.

6. Cliquez sur **Enregistrer**
   Les deux nouvelles sections s'affichent **: Artefacts** et **Canevas d'enquête**. Lorsque vous créez un canevas, le canevas n'inclut aucun nœud. Vous devez ajouter des nœuds à partir de la bibliothèque Threat Intelligence ou des artefacts via l'option d'ajout à partir de la bibliothèque.
7. Accédez au **canevas d'enquête**.
8. Cliquez sur **Ajouter à partir de la bibliothèque**.

   Remarque : Deux options sont disponibles pour ajouter les nœuds. Vous pouvez sélectionner **Importer** pour importer tous les observables ou sélectionner **l'option Ajouter à partir de la bibliothèque** pour ajouter les observables à partir de la bibliothèque des renseignements sur les menaces.

   La boîte **de dialogue Importer le nœud à partir de la bibliothèque** s'affiche.
9. Sélectionnez le **type de nœud** dans la liste déroulante.
   Par exemple, sélectionnez le type Observables si vous ajoutez des observables au canevas d'enquête.
10. Sélectionnez le nombre requis d'observables.
11. Cliquez sur **Importer**.
    Une fois les observables importés, les nœuds sont ajoutés au canevas d'enquête. Quoi qu'il en soit, les nœuds ajoutés au canevas sont actuellement ajoutés temporairement au canevas et ne seront pas conservés sur le canevas.
12. Sélectionnez **Enregistrer le canevas**.
    Si vous souhaitez traiter les données des nœuds sur le canevas, vous devez enregistrer les données pour les conserver de manière permanente.

    Remarque : Si vous n'exécutez pas l'option **Enregistrer le canevas** , vous risquez de perdre les données chaque fois que vous actualisez le canevas.

13. Sélectionnez **Ajouter des données à la bibliothèque** pour créer une nouvelle relation entre deux nœuds différents.
    La relation entre les deux nœuds est indiquée par la ligne pointillée, ce qui signifie que les nœuds sont temporaires. Si vous souhaitez déplacer les données des nœuds vers les relations, sélectionnez **Enregistrer les données dans la bibliothèque** et ajoutez des données à la bibliothèque. Une fois cette opération effectuée, la ligne pointillée se transforme en une ligne de bordure continue indiquant que le nœud fait maintenant partie de la bibliothèque.
14. Utilisez l'icône **Filtre** pour afficher le type d'observables et d'objets présents dans le canevas et vous pouvez choisir de manière sélective le type de données à afficher sous le canevas d'examen.
15. Sélectionnez également l'icône contextuelle pour afficher ou effectuer une opération sur les nœuds du canevas d'examen sur un espace plus grand.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

16. Sélectionnez **Lier le ticket** pour lier le ticket au canevas d'enquête.
    a. Sélectionnez **l'ID du ticket**.
    b. Cliquez sur le bouton **Lien** .
17. Cliquez sur **Dupliquer pour dupliquer** les données et les nœuds du canevas dans le canevas.

Information associée

Utiliser des actions sur le canevas d'examen

Liaison du canevas à partir d'un ticket

Création d'un ticket et liaison à partir du canevas d'enquête

Ajout d'un nouveau nœud au canevas

Utilisez cette section pour créer et ajouter de nouvelles entités, y compris des observables ou des objets, directement à partir du canevas d'enquête.

Avant de commencer

Cette fonction permet un enrichissement rapide du canevas sans avoir à naviguer hors de la vue actuelle.

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Sélectionnez l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
4. Ouvrez n'importe quel enregistrement de ticket.

   Remarque : Lors de la création d'un ticket, vous devez créer un canevas ou lier un canevas existant. Après la liaison, les actions du canevas, y compris l'option d'ajout de nouveaux nœuds, seront automatiquement disponibles dans l'interface utilisateur.

5. Sélectionner **Canevas d'examen** > **Nouveau nœud**.
   - Vous pouvez également afficher la fonctionnalité **Nouveau nœud** à partir de la liste déroulante de la section**Canevas d'examen** vide du ticket.
   - Une autre option pour afficher la fonctionnalité **Nouveau nœud** consiste à l'afficher directement à partir de la page de canevas d'examen.
6. Pour créer un nœud, sélectionnez la **catégorie d'entité** et le **type d'entité** appropriés.

Champ	Description
Catégorie d'entité	Sélectionnez la catégorie d'entité telle que Observable ou Objet.
Type d'entité	Sélectionnez le type d'entité parmi les options disponibles en fonction de la catégorie sélectionnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : ○ Lorsqu'un type d'entité est sélectionné, le formulaire d'objet correspondant s'affiche automatiquement, affichant les champs clés tels que Nom et Description ainsi que tous les champs requis pour identifier l'entité parente. ○ Si vous tentez de créer une entité en double, ce qui signifie que si vous sélectionnez une entité qui existe dans l'application et que vous essayez d'en créer une avec la même valeur, un message d'erreur apparaîtra indiquant que l'entité existe déjà dans la bibliothèque Threat Intelligence avec la même valeur et le même type.

7. Renseignez les détails nécessaires de l'objet tels que le nom, la description.
8. Sélectionnez **Ajouter** pour ajouter le nouveau nœud.
   Ce processus ajoute automatiquement le nœud au canevas d'examen.

   Les nœuds nouvellement ajoutés sont différenciés visuellement par un point



   sur le nœud des nœuds importés via la bibliothèque ou les artefacts de ticket.

Important : Les nœuds nouvellement ajoutés sont temporaires et ne sont pas enregistrés dans la bibliothèque ou le canevas des renseignements sur les menaces. Si vous actualisez le canevas avant d'enregistrer, ces nœuds seront perdus. Assurez-vous d'enregistrer le canevas après avoir ajouté de nouveaux nœuds pour conserver vos modifications.

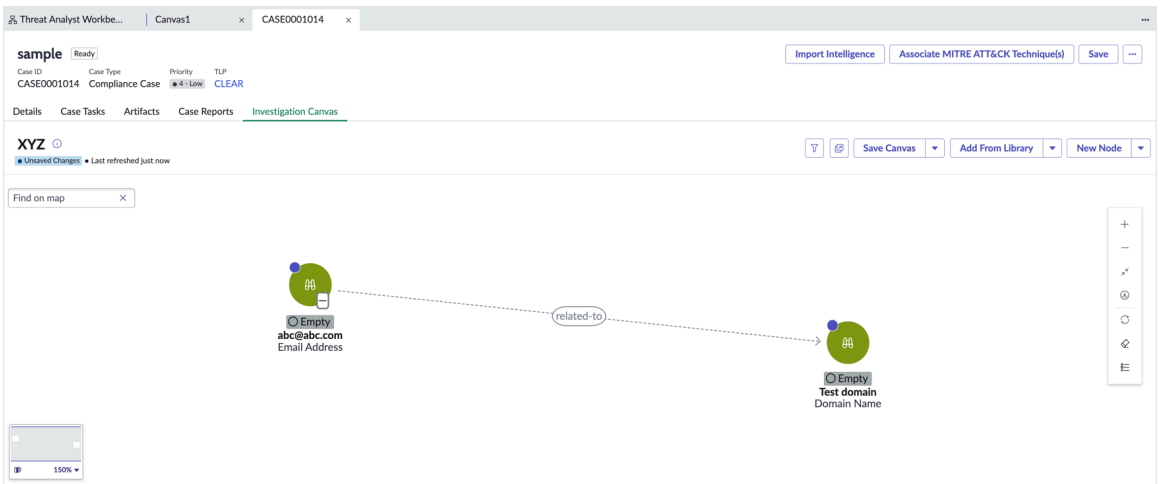
9. Cliquez avec le bouton droit sur le nouveau nœud et sélectionnez l'option **Ajouter une relation** pour créer des relations entre les nœuds.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Lors de la création de nouvelles relations, les bordures apparaissent sous forme de lignes pointillées, indiquant qu'il s'agit de nœuds temporaires qui ne sont pas enregistrés dans la bibliothèque Renseignements sur les menaces.
- Les bordures nouvellement ajoutées sont temporaires et ne sont pas enregistrées dans la bibliothèque ou le canevas des renseignements sur les menaces. Si vous actualisez le canevas avant d'enregistrer, ces bords seront perdus. Assurez-vous d'enregistrer le canevas après avoir ajouté de nouvelles arêtes pour conserver vos modifications.



10. Cliquez avec le bouton droit et sélectionnez **Afficher les détails** pour afficher les détails relatifs à l'entité sélectionnée.

Remarque : Pour ajouter des données, vous pouvez cliquer sur le lien hypertexte dans le volet de détails ou sélectionner l'option **Ouvrir l'enregistrement** et ajouter les données liées au nœud requise.

11. Sélectionnez **l'option Ajouter des données à la bibliothèque** pour enregistrer tous les nœuds et bordures qui ont été temporairement ajoutés au cours de votre enquête.
En effectuant cette action, les enregistrements temporaires sont convertis en enregistrements agrégés permanents au sein de la bibliothèque Threat Intelligence.

Canevas d'examen et MITRE ATT&CK

Dans le canevas d'examen, vous pouvez afficher les techniques et sous-techniques MITRE ATT&CK associées à tous les nœuds actuellement présents sur le canevas.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

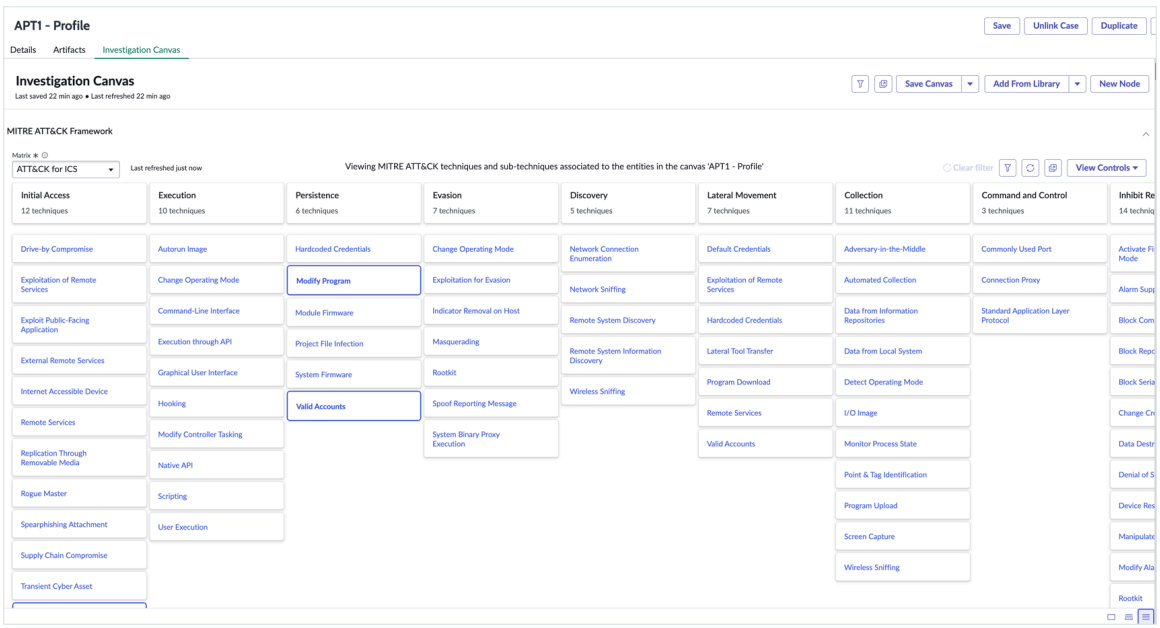
Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Sélectionnez l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
4. Ouvrez n'importe quel ticket.
5. Accédez à l'onglet **Canevas d'enquête** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sur le canevas d’examen, utilisez la **poignée de division des panneaux redimensionnables** pour faire glisser le pointage afin d’afficher le cadre de travail MITRE ATT&CK.
7. Sélectionnez la matrice MITRE ATT&CK requise dans la liste déroulante **Matrice** .



Le cadre MITRE ATT&CK montre différents niveaux d’association de tactiques et de techniques.

a. La ligne supérieure affiche toutes les tactiques présentes dans la matrice MITRE ATT&CK sélectionnée.

b. Par défaut, chaque tactique affiche le nombre total de techniques et de sous-techniques qui lui sont associées.

c. Utilisez l’icône **Actualiser** pour recharger le cadre de travail MITRE ATT&CK et afficher les dernières associations technique-tactique.

d. Affichez les techniques et sous-techniques MITRE ATT&CK associées à tous les nœuds (entités) du canevas.

e. Cliquez sur un ou plusieurs nœuds pour afficher les techniques et sous-techniques MITRE ATT&CK associées associées au(x) nœud(s) sélectionné(s) dans le canevas.

> **Important :** Dans le cadre, les techniques et sous-techniques associées aux nœuds du canevas sont mises en surbrillance.

8. Sélectionnez **Filtres** pour vous permettre de créer et d’enregistrer des filtres pour les TTP associés à des adversaires spécifiques et à d’autres attributs de technique MITRE.
Pour plus d’informations sur les options de filtrage MITRE, reportez-vous à la section Canevas d’examen Filtres MITRE.
9. Utilisez **les contrôles d’affichage** pour des options de filtrage avancées.
Une fois que vous avez sélectionné le filtre approprié, il n’affiche que les techniques et sous-techniques MITRE ATT&CK associées au(x) nœud(s) sélectionné(s). Les options de la liste **Afficher les contrôles** sont les suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Afficher l'ID** : affiche l'ID unique de la technique (par exemple `T1059`) sur chaque carte pour une référence facile.
- **Afficher les sous-techniques** : affiche les sous-techniques. Cette option développe automatiquement les cartes de technique parentes pour afficher leurs sous-techniques, sans nécessiter d'expansion manuelle.
- Sélectionner **Afficher uniquement les techniques associées** : affiche uniquement les techniques qui sont actuellement liées aux nœuds sur le canevas d'examen, masquant toutes les techniques non pertinentes même si elles répondent aux critères de filtre. Lorsque cette option est sélectionnée, chaque tactique affiche le nombre total de techniques et sous-techniques associées actuellement liées au canevas.

10. Cliquez sur l'icône contextuelle pour afficher le cadre MITRE ATT&CK dans un espace plus grand.

Important :

- Chaque fois que vous ajoutez ou supprimez un nœud, le framework MITRE ATT&CK s'actualise automatiquement. Vous pouvez également utiliser l'icône d'actualisation pour effectuer une actualisation manuelle à tout moment.
- Chaque fois que vous filtrez des types de nœuds spécifiques, le cadre de travail MITRE ATT&CK s'actualise automatiquement pour refléter les modifications.

Canevas d'examen Filtres MITRE

Les filtres MITRE vous permettent de créer et d'enregistrer des filtres pour les tactiques, les techniques et les procédures (TTP) associées à des adversaires spécifiques et à d'autres attributs de technique MITRE.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Pourquoi et quand exécuter cette tâche

Les analystes peuvent utiliser les filtres disponibles sur la carte MITRE pour filtrer des TTP d'acteurs spécifiques pertinents pour les adversaires impliqués dans l'enquête.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Sélectionnez l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
4. Ouvrez n'importe quel ticket.
5. Accédez à l'onglet **Canevas d'enquête** .
6. Sélectionnez **Filtres** pour créer des filtres pour les tactiques, les techniques et les procédures (TTP) associées à des adversaires spécifiques et à d'autres attributs de technique MITRE.
7. Renseignez les valeurs nécessaires dans le panneau de filtre pour appliquer les filtres souhaités.
   Le panneau de filtre MITRE vous permet de filtrer et de visualiser les techniques MITRE ATT&CK en fonction de critères sélectionnés tels que les groupes, les programmes malveillants, les outils, les balises et la priorité.

Champ	Description
Filtres enregistrés	Les analystes peuvent enregistrer des critères spécifiques sous forme **de filtres enregistrés**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	pour les réutiliser. Les filtres enregistrés par un analyste sont spécifiques à l'utilisateur. **Remarque :** Par exemple, si l'analyste X enregistre une configuration de filtre, elle ne sera visible que par l'analyste X. Lorsqu'un autre analyste se connecte et affiche la liste déroulante des filtres, il ne voit pas les filtres enregistrés par d'autres. Cela garantit que chaque utilisateur peut créer et gérer des vues personnalisées sans affecter ou être affecté par les préférences de filtre des autres utilisateurs.
Nom du filtre	Nom du filtre.
Groupe MITRE	Indique le groupe MITRE. Sélectionnez un ou plusieurs groupes pour filtrer les techniques qui leur sont associées.
Programme malveillant MITRE	Indique le programme malveillant MITRE. Sélectionnez un ou plusieurs éléments de programme malveillant pour filtrer les techniques qui leur sont associées.
Outils MITRE	Indique les outils MITRE. Sélectionnez un ou plusieurs outils pour filtrer les techniques qui leur sont associées.
Balises TISC	Indique les TISC balises. Sélectionnez une ou plusieurs balises pour filtrer les techniques en fonction de leur classification.
Priorité des techniques	Indique le niveau de priorité des techniques. Vous pouvez sélectionner une ou plusieurs options pour filtrer les techniques en fonction de leur priorité affectée.
Tout effacer	Permet d'effacer les entrées saisies dans le panneau de filtre.
Enregistrer comme nouveau filtre	Enregistre les critères saisis dans le panneau de filtre en tant que nouveau filtre enregistré. **Remarque :** Le nom du filtre enregistré doit être unique.
Enregistrer le filtre actuel	Enregistre les changements apportés aux critères dans le filtre enregistré actuellement sélectionné. Vous pouvez également renommer un filtre à l'aide de cette option. **Remarque :** Le nom du filtre enregistré doit être unique.

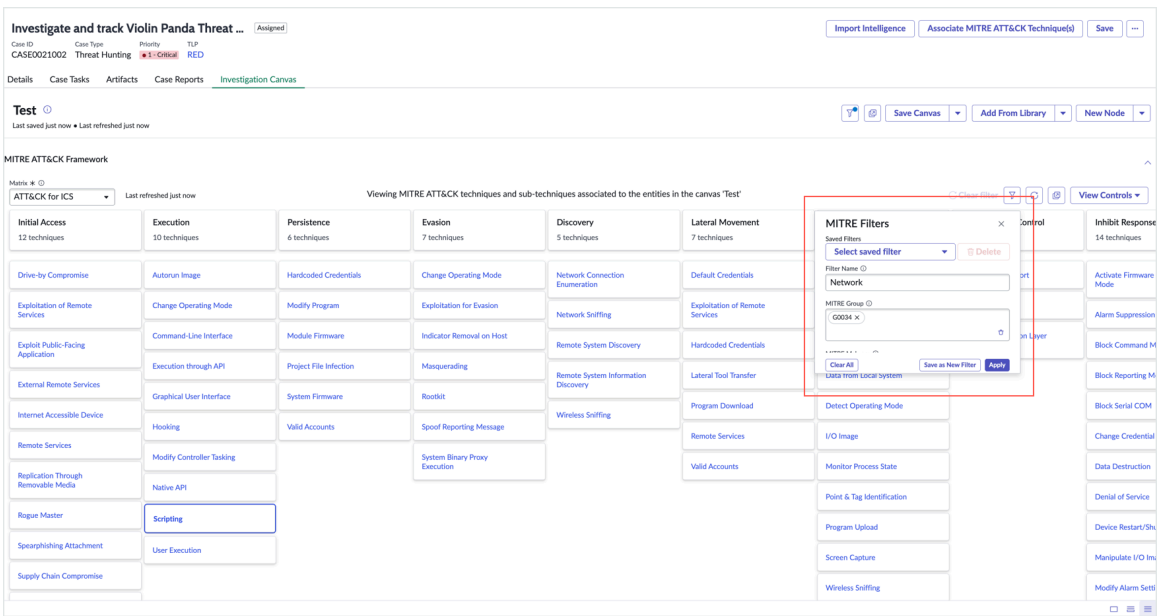
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Appliquer	Cette option vous permet d'appliquer les modifications à vos filtres dans la carte MITRE.
Supprimer	Sélectionnez cette option pour supprimer un filtre enregistré sélectionné. Lorsque vous cliquez sur le bouton **Supprimer** en regard d'un filtre enregistré, un message de confirmation s'affiche si vous êtes sûr de vouloir supprimer ce filtre. La confirmation de cette action supprimera définitivement le filtre enregistré. Pour supprimer une valeur de champ individuelle dans le panneau de filtre, cliquez sur l'icône **Supprimer (corbeille)** en regard de ce champ spécifique.

En appliquant des filtres à l'aide de ces valeurs, la matrice MITRE est mise à jour dynamiquement pour afficher uniquement les techniques associées aux attributs sélectionnés. Cette vue ciblée permet aux analystes de se concentrer davantage sur les tactiques, techniques et procédures (TTP) les plus pertinentes au cours des enquêtes.

En outre, les analystes peuvent affiner davantage les TTP en utilisant des filtres pour les logiciels malveillants, les outils, les balises et les niveaux de priorité.



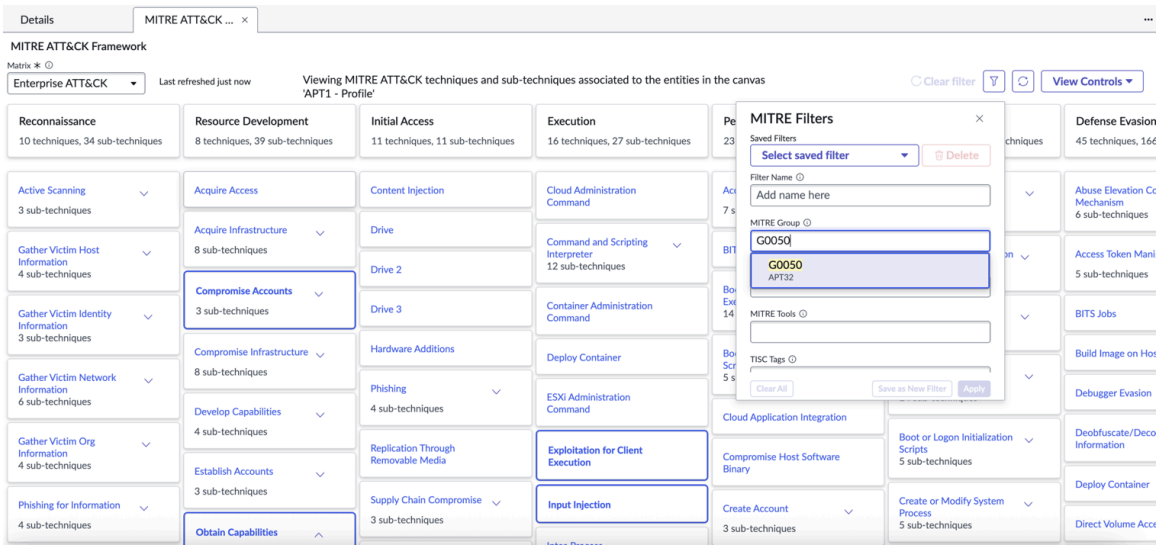
8. **Facultatif :** Sélectionnez **Enregistrer en tant que nouveau filtre** pour enregistrer vos critères de filtrage.
9. Sélectionnez **Appliquer** pour appliquer les changements.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

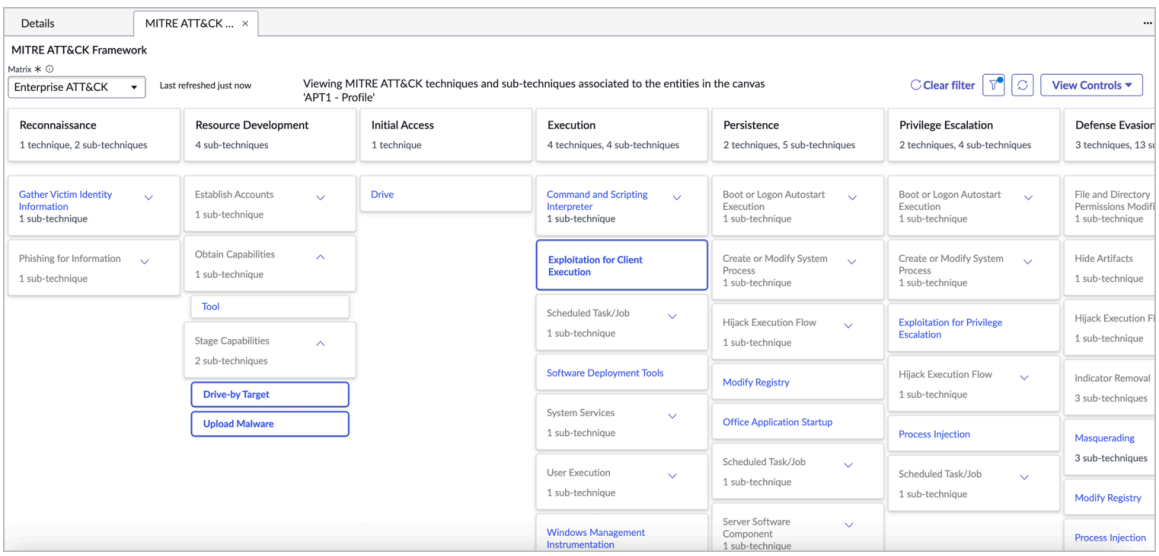
Example: Filtrage par groupe MITRE

Sélectionnez un groupe MITRE comme APT32 (G1001, voir la capture d'écran suivante). Lorsque vous appliquez ce filtre, la matrice MITRE se met à jour pour afficher uniquement les techniques directement liées au groupe sélectionné.



Cette vue ciblée aide les analystes à se concentrer spécifiquement sur les tactiques, les techniques et les procédures (TTP) associées au groupe de menaces sélectionné.

Lorsque vous appliquez le filtre, certaines techniques de la matrice s'affichent en bleu, tandis que d'autres s'affichent en gris.



La représentation visuelle sur le cadre MITRE indique comment les techniques et les sous-techniques sont liées aux filtres appliqués et au contexte d'enquête.

- **Texte bleu :** Les techniques ou sous-techniques affichées en bleu indiquent celles qui correspondent aux critères de filtre.
- **Texte bleu en gras avec bordure bleue :** Les techniques ou sous-techniques affichées en gras bleu avec une bordure bleue indiquent celles qui correspondent aux critères de filtre et qui sont associées à un ou plusieurs nœuds sur le canevas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Carte grise :** Les techniques parentes sont affichées en gris lorsqu'elles ne correspondent pas directement aux critères de filtre (ce qui signifie qu'elles ne sont pas liées au groupe sélectionné) mais qu'elles représentent la relation parente avec les sous-techniques liées qui correspondent aux critères de filtre.

Ajouter des artefacts aux tickets ou aux tâches de ticket

Une fois le ticket créé, vous pouvez y afficher ou ajouter des artefacts, tels que des incidents de sécurité, des CI et des indicateurs de compromission. Ces artefacts servent d'indices pour résoudre l'affaire.

Avant de commencer

Rôle requis : admin

Remarque : Les artefacts ne sont disponibles que pour les tickets existants. Pour les observables et les indicateurs, les artefacts peuvent également être ajoutés ou associés à un ticket à partir de la tâche d'importation à l'aide du bouton Import Intelligence. Pour plus d'informations sur l'importation, consultez Importer des renseignements dans TISC

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez un ticket ou une tâche de ticket.
5. Accédez à l'onglet **Artefacts** .
   Les artefacts associés sont affichés sous forme de listes connexes pour ce ticket ou cette tâche de ticket spécifique.
6. Liez ou dissociez les enregistrements du ticket ou de la tâche de ticket.

Remarque : Pour plus d'informations, voir Lier les enregistrements connexes à Threat Intelligence

La table suivante répertorie les artefacts connexes Listes associées au(x) ticket(s) ou au(x) document/s de ticket :

Enregistrements connexes

Liste connexe	Description
Techniques MITRE	Répertoriez les techniques MITRE associées au(x) ticket(s). Les techniques MITRE affichent également toutes les techniques associées dans un ticket.
Observable	Liste des observables associés à ces tickets ou tâches de ticket.
Indicateurs	Liste des indicateurs associés à ces tickets ou tâches de tickets.
Schémas d'attaque	Liste des schémas d'attaque associés à ces tickets ou tâches de tickets.
Campagnes	Répertorier les campagnes associées à ces tickets ou tâches de ticket.
Déroulement des actions	Répertoriez le plan d'actions associés à ces tickets ou tâches de ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Description
Composants de données	Liste des composants de données associés à ces tickets ou tâches de ticket.
Regroupements des menaces	Répertoriez les regroupements de menaces associés à ces tickets ou tâches de ticket.
Identités	Répertoriez les identités associées à ces tickets ou tâches de ticket.
Infrastructure	Énumérez l'infrastructure telle que les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont liées à ces tickets ou tâches de tickets.
Ensembles d'intrusion	Répertoriez les ensembles d'intrusion, tels qu'un ensemble de comportements et de ressources contradictoires ayant des propriétés communes qui sont liées à ce ticket ou à ces tâches de ticket.
Emplacements	Répertorier les enregistrements d'emplacements associés à ces tickets ou tâches de tickets.
Programme malveillant	Répertoriez les enregistrements sources de programmes malveillants associés à ces tickets ou tâches de tickets.
Définitions de marquage	Répertoriez les enregistrements de définitions de marquage associés à ces tickets ou tâches de ticket.
Notes de menace	Répertoriez les enregistrements de définitions de marquage associés à ces tickets ou tâches de ticket.
Données observées	Répertoriez les données observées qui sont liées à ces tickets ou tâches de ticket.
Opinions sur la menace	Répertoriez les opinions sur une menace liées à ces tickets ou tâches de ticket.
Rapports de menace	Répertoriez les rapports de menace associés à ces tickets ou tâches de ticket.
Perceptions	Liste des perceptions associées à ces tickets ou tâches de tickets.
Acteurs de menace	Dressez la liste des acteurs de menace associés à ces tickets ou tâches de tickets.
Outils	Répertoriez les outils associés à ces tickets ou tâches de ticket.
Vulnérabilités	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante et qui sont liées à ce ticket ou à ces tâches de ticket.
Tickets connexes	Répertorie les tickets connexes.
Tâches du ticket connexe	Répertorie les tâches de ticket connexes.
Incidents de sécurité	Répertoriez les incidents de sécurité associés à ces tickets ou tâches de ticket.
Éléments de configuration affectés	Répertoriez les éléments de configuration affectés qui sont associés à ces tickets ou tâches de ticket.
Services affectés	Répertoriez les services affectés qui sont associés à ces tickets ou tâches de ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste connexe	Description
Actifs affectés	Répertoriez les actifs affectés qui sont associés à ces tickets ou tâches de ticket.
Entrées de vulnérabilité	Répertoriez les entrées de vulnérabilité associées à ces tickets ou tâches de ticket.

Déploiement des techniques MITRE des artefacts au ticket

Lorsque des enregistrements d'intelligence sont ajoutés à un ticket, toutes les techniques MITRE associées sont automatiquement déployées au niveau du ticket.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez n'importe quel ticket.
5. Accédez à l'onglet **Artefacts** .
   Les artefacts associés s'affichent sous forme de listes connexes pour ce ticket spécifique.

Afficher le cadre de travail MITRE ATT&CK pour un ou plusieurs tickets

Affiche toutes les techniques associées d'un ticket dans le cadre de travail MITRE ATT&CK.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Pourquoi et quand exécuter cette tâche
Sélectionnez la matrice MITRE ATT&CK requise dans la liste déroulante **Matrice** . Le cadre MITRE ATT&CK montre différents niveaux d'association de tactiques et de techniques.

1. La ligne supérieure affiche toutes les tactiques présentes dans la **matrice** sélectionnée. Par défaut, toutes les tactiques affichent le nombre total de techniques et de sous-techniques présentes pour les tactiques correspondantes. Vous pouvez utiliser l'icône **Actualiser** pour recharger le cadre de travail MITRE ATT&CK et afficher les dernières associations.
2. Sous chaque tactique, le cadre affiche toutes les techniques présentes en relation avec cette tactique correspondante.
3. Le cadre de travail affiche les sous-techniques présentes sous chaque technique. Développez chaque technique pour afficher les sous-techniques.

Important : Dans le cadre, les techniques et sous-techniques associées à un cas sont mises en évidence.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez n’importe quel ticket.
5. Accédez à l’onglet **Artefacts** .
   Les artefacts associés s’affichent sous forme de listes connexes pour ce ticket spécifique.
6. Sélectionnez **le bouton Afficher le cadre de travail MITRE ATT&CK**
   Lorsque vous sélectionnez ce bouton, l’infrastructure affiche toutes les techniques associées d’un cas et les artefacts sur le MITRE ATT&CK.
7. Affichez les techniques et sous-techniques MITRE ATT&CK associées au ticket à partir des techniques MITRE que vous avez choisies d’afficher.
8. Sélectionnez n’importe quel enregistrement pour afficher les techniques et sous-techniques MITRE ATT&CK associées au ticket.
9. Utilisez les **contrôles d’affichage** pour afficher les techniques et sous-techniques MITRE ATT&CK comme vous le souhaitez.
   Dans les listes de contrôles :
   - Sélectionnez **Afficher l’ID** pour afficher les ID MITRE des techniques et des sous-techniques.
   - Sélectionnez **Afficher les sous-techniques** pour afficher toutes les sous-techniques. Lorsque vous sélectionnez cette option, toutes les techniques sont affichées dans la vue développée. La vue élargie de la technique montre toutes les sous-techniques présentes pour cette technique correspondante.
   - Sélectionnez **Afficher uniquement les techniques associées** pour afficher uniquement les techniques MITRE associées à un ticket. Lorsque vous sélectionnez cette option, chaque tactique affiche le nombre total de techniques et de sous-techniques associées.

Exécuter des actions d’enrichissement dans un ticket

Utilisez cette section pour comprendre comment les actions d’enrichissement sont effectuées sur le ou les tickets.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

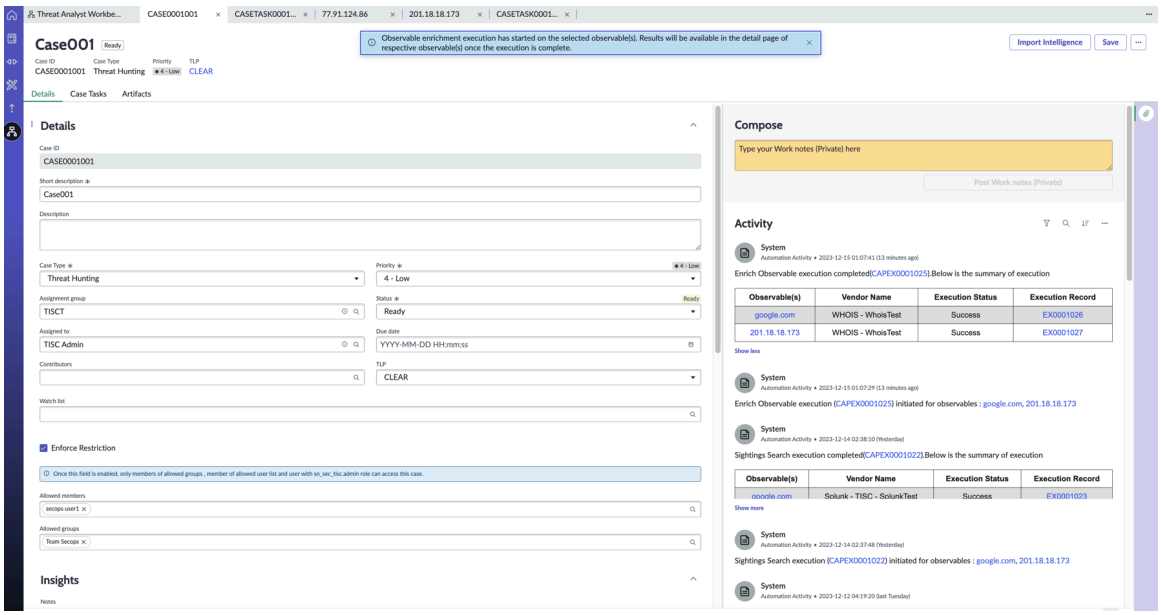
1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l’icône **Console d’analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez un ticket ou une tâche de ticket.
5. Accédez à l’onglet **Artefacts** .
6. Sélectionnez la liste connexe Observables.
7. Sélectionnez un ou plusieurs observables.
8. Cliquez sur une action d’enrichissement dans la liste déroulante.
9. Sélectionnez la ou les implémentations disponibles.
10. Cliquez sur **Envoyer**.
    Par exemple, Exécuter une recherche de menace. L’action d’enrichissement sélectionnée sera exécutée et un message d’information s’affichera indiquant que l’exécution de l’enrichissement de l’observable a

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

commencé sur le ou les observables sélectionnés. Les résultats seront disponibles dans la page détaillée du ou des observables respectifs une fois l'exécution terminée.

Remarque : Une fois l'exécution initiée ou terminée, une note de travail est publiée sur le flux d'activité de la vue de formulaire.



Afficher les rapports de tickets

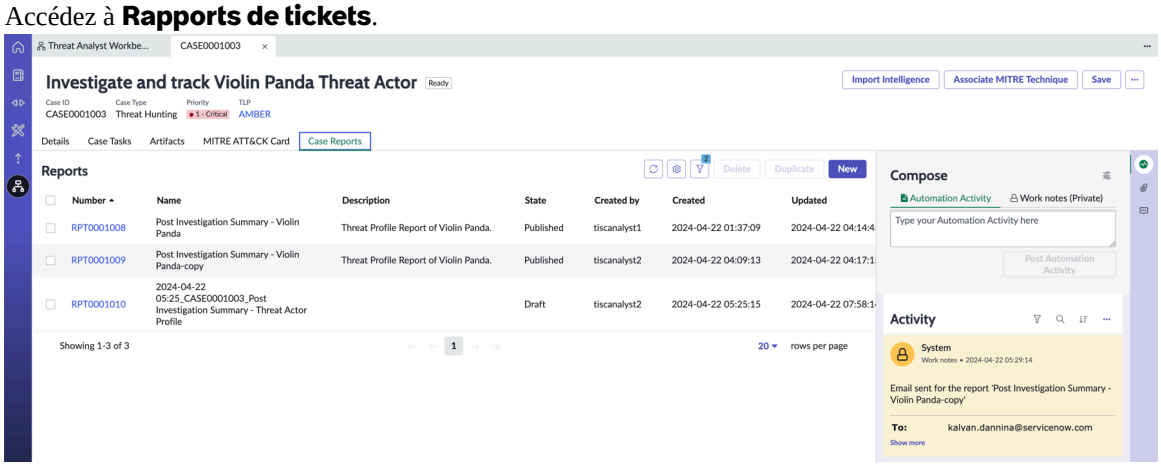
Utilisez la fonctionnalité de rapports de tickets pour générer des rapports liés aux tickets. Ces rapports comprennent un rapport post-enquête ou un rapport sommaire.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez n'importe quel ticket.
5. Accédez à **Rapports de tickets**.

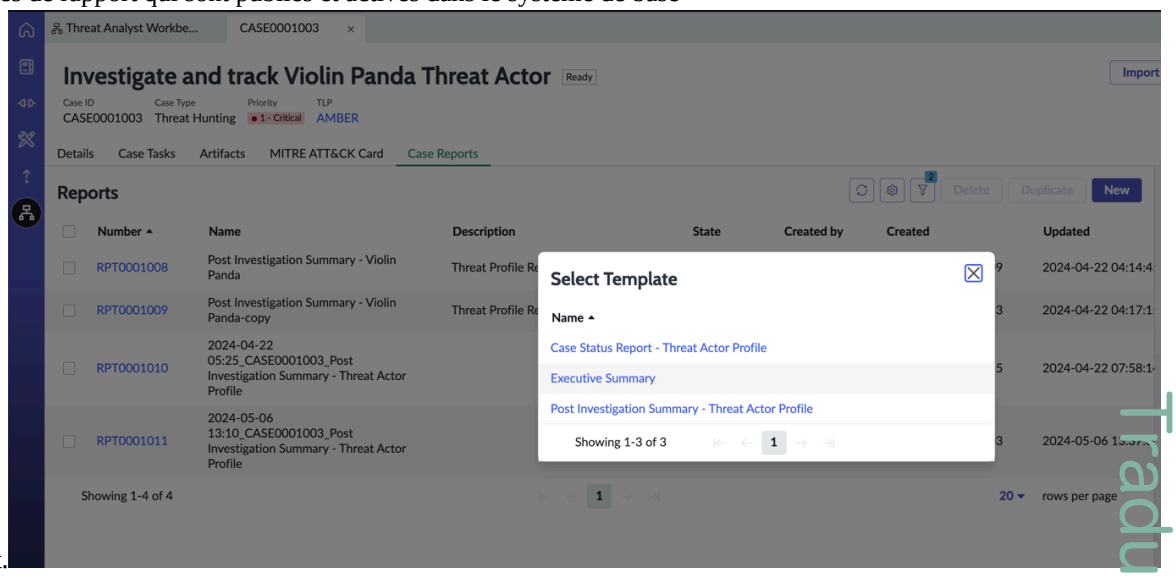


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous pouvez supprimer les rapports de la liste, créer une copie en double des rapports existants et personnaliser votre propre rapport.

6. Cliquez sur **Nouveau**.
   Les modèles de rapport qui sont publiés et activés dans le système de base s'affichent.



7. Sélectionnez le modèle de rapport souhaité.
   Le modèle de rapport sélectionné pour le type de rapport est généré. De plus, ici, une fois que le rapport est publié, cela signifie qu'un plus grand groupe d'utilisateurs peut le consulter, mais si le rapport est à l'état de brouillon, ce rapport est caché aux utilisateurs. En tant qu'analyste, vous pouvez uniquement afficher les rapports publiés, mais pas les rapports à l'état de brouillon.

   Remarque :
   - Si vous souhaitez ajouter d'autres champs, sélectionnez les champs et ajoutez-les directement dans votre rapport de ticket.
   - Si vous souhaitez ajouter une liste connexe, par exemple une liste d'observables, sélectionnez Observables. Tous les observables associés à ce cas particulier seront répertoriés, sélectionnez un ou plusieurs observables puis cliquez sur **Ajouter**. Vous pouvez également filtrer l'observable requis et l'ajouter à votre ticket.

8. Cliquez sur **Enregistrer le contenu** pour enregistrer le contenu de votre rapport.
9. Cliquez sur **Aperçu** pour prévisualiser le rapport.

   Remarque : Vous pouvez faire ce qui suit :
   - **Agrandir** la fenêtre du rapport.
   - **Téléchargez** le rapport à l'aide de l'icône **Télécharger** .
   - Affichez le rapport dans un nouvel onglet au cas où la hauteur ou la taille du rapport aurait une meilleure expérience de visualisation.
   - **Modifiez** le nom et la description du rapport.
   - **Publiez** le rapport.

10. Cliquez sur le bouton **Modifier le contenu** pour republier le rapport.

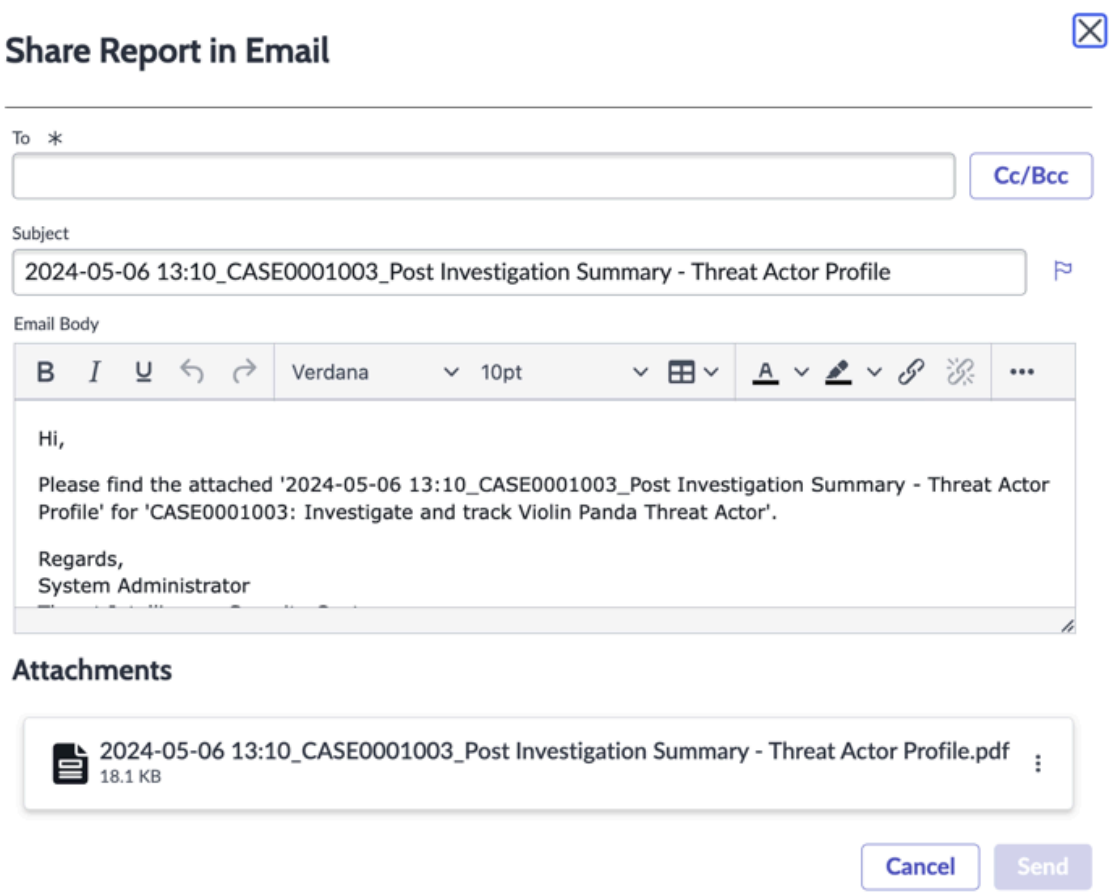
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Un message d'avertissement s'affiche pour vous permettre de partager le rapport :

Vous devez republier le rapport après avoir effectué des modifications pour pouvoir télécharger ou partager le rapport. Voulez-vous quand même continuer la modification ?

11. Cliquez sur **Modifier**.
    Si vous souhaitez modifier le rapport, vous pouvez continuer à le modifier comme expliqué ou vous pouvez publier le rapport. Une fois publié, le rapport sera en lecture seule.
12. Cliquez sur **Partager le rapport par e-mail** pour partager le rapport.
    Lors du partage du rapport, le rapport PDF généré est joint en tant que pièce jointe à l'e-



mail.

13. Ajoutez les champs d'e-mail requis tels que À (à (à qui vous souhaitez partager le rapport), CC et CCI
14. Marquez l'e-mail comme important, si nécessaire.
15. Cliquez sur **Envoyer**.
    Le rapport sera partagé avec un groupe plus large d'utilisateurs.

Créer un incident de sécurité à partir d'un TISC ticket

Créer des incidents de sécurité et associer des observables aux incidents de sécurité à partir d'un TISC ticket.

Avant de commencer
Rôle requis : sn_si_basic

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Ouvrez n'importe quel ticket.
5. Cliquez sur **le bouton Créer un incident de sécurité** .

   Remarque : Sur la **console de gestion des tickets** , le bouton **Créer un incident de sécurité** n'est activé que pour les enregistrements de tickets ouverts et désactivé pour les enregistrements de tickets fermés.

   La boîte de dialogue Créer un incident de sécurité s'affiche.
6. Remplissez le formulaire avec les détails d'incident appropriés :

Ajouter des détails

Champ	Description
Description brève	Saisissez une brève description de l'incident de sécurité.
Description	Saisissez une description de l'incident de sécurité.
Catégorie	Définit la classification de l'incident de sécurité.
Priorité	Définit la priorité de l'incident de sécurité.
Sous-catégorie	Définit la sous-classification de l'incident de sécurité en fonction de sa catégorie.
Groupe d'affectation	Spécifie le groupe d'affectation auquel l'incident de sécurité doit être affecté.
Parent	Indique l'incident de sécurité parent, qui est un TISC ticket à partir duquel cette action est déclenchée.

7. Cliquez sur **Suivant** pour continuer.

   Remarque : Vous devez renseigner tous les champs obligatoires. Le bouton **suivant** reste désactivé jusqu'à ce que vous saisissiez tous les champs obligatoires.

8. Sélectionnez les observables associés au TISC ticket pour les lier à un incident de sécurité, puis cliquez sur **Suivant** pour continuer
9. Examinez les détails de l'incident de sécurité et les observables qui seront associés à l'incident de sécurité nouvellement créé, puis cliquez sur **Créer** pour continuer et créer l'incident de sécurité.

   Remarque : Un message de confirmation s'affiche indiquant que l'incident de sécurité est créé. Un lien vers l'incident de sécurité s'affiche. Cliquez sur le lien pour accéder à l'incident de sécurité dans le Espace de travail de la Réponse aux incidents de sécurité fichier .

   Une fois l'incident de sécurité créé, vous serez redirigé vers l'onglet TISC **Artefacts** du ticket.
10. Accédez à la section **Incidents de sécurité** sous l'onglet TISC **Artefacts** pour afficher les incidents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Une note de travail est également publiée sur le flux d'activité du TISC ticket indiquant que l'incident de sécurité (numéro d'incident de sécurité) est créé avec les observables associés TISC . Ces notes de travail incluent des détails tels que le type et la valeur de l'observable.

Sur le formulaire d'incident Espace de travail de la Réponse aux incidents de sécurité de sécurité :

- Une note de travail est publiée sur le flux d'activité et indique que l'incident de sécurité a été créé avec succès à partir du TISC ticket. Ces notes de travail incluent également un lien vers le TISC ticket confirmant que les observables sélectionnés ont été associés à l'incident de sécurité.
- En outre, vous pouvez également vérifier cela en accédant à l'onglet **Enregistrements connexes** de et Espace de travail de la Réponse aux incidents de sécurité en examinant les entrées observables sous **Connaissance de la menace** > **Observables associés**. À partir de là, vous pouvez également afficher les observables associés dans la section **Contexte TISC** . Vous remarquerez peut-être que ces observables ont été directement associés à partir de TISC.

Télécharger les pièces jointes du fichier sécurisé

Utilisez cette section pour comprendre comment télécharger les pièces jointes sécurisées dans le(s) ticket(s).

Avant de commencer

Rôle requis : sn_sec_tisc_secure_file_access, sn_sec_tiscadmin

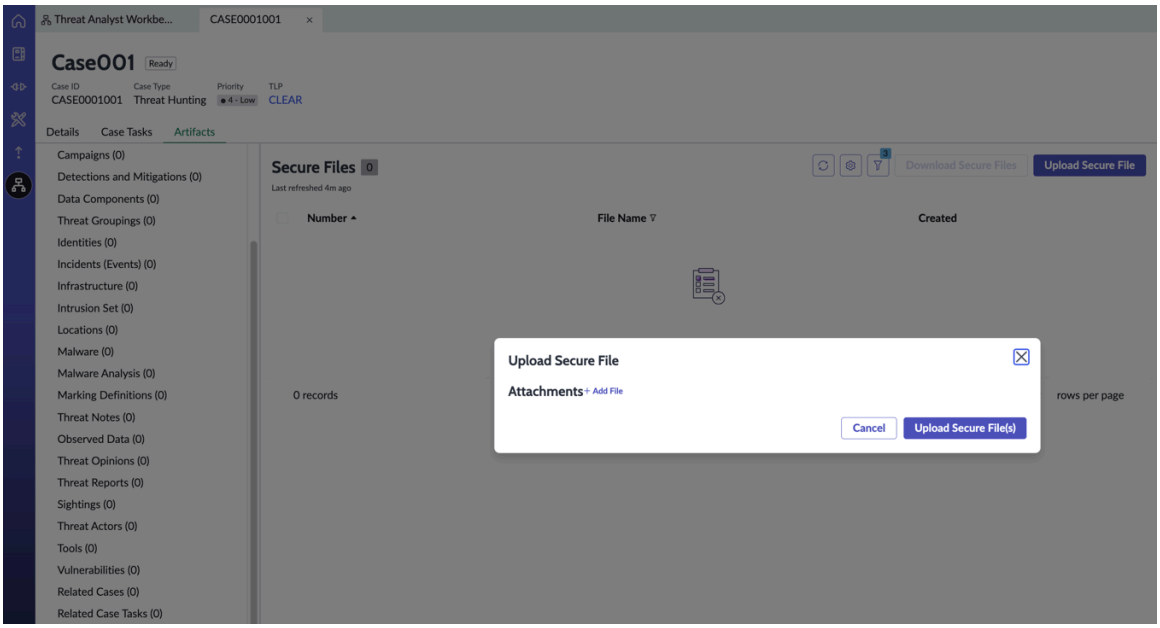
Remarque : Les listes connexes Fichiers sécurisés ne s'affichent que si vous disposez du rôle d'utilisateur sn_sec_tisc.secure_file_access.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Gestion des tickets** > **Tous les tickets**.
   Tous les tickets sont affichés.
4. Sélectionnez n'importe quel ticket.
5. Accéder à **Artifacts** > **Fichiers sécurisés** listes connexes.
6. Cliquez sur le bouton **Télécharger le fichier sécurisé** .
7. Cliquez sur **Ajouter un fichier** pour ajouter les pièces jointes.
8. Sélectionnez les fichiers et cliquez sur le bouton **Charger le(s) fichier(s) sécurisé(s).**
   Les pièces jointes sont téléchargées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Cliquez sur **Télécharger des fichiers sécurisés** pour télécharger les pièces jointes.
   Les pièces jointes sont disponibles au format zip.
10. Vous pouvez également télécharger le fichier en accédant à la page des détails de l'enregistrement de fichier sécurisé.

Remarque :

- Toutes les pièces jointes sécurisées sont chiffrées et stockées dans le système à l'aide du Cadre de travail de gestion des clés (KMF). Pour plus d'informations, consultez Chiffrement des pièces jointes .
- Si les utilisateurs ont un abonnement à *ServiceNow Centre d'intégration* **Professional Pack Installer**, les fichiers sécurisés sont compressés au format zip, ainsi que cryptés et stockés

Centre de sécurité des renseignements sur les menaces Bibliothèque

Une bibliothèque de menaces est définie comme un groupe d'objets et d'entités organisés qui servent aux organisations des informations structurées et non structurées sur les menaces de sécurité.

Les informations sur les menaces sont disponibles sous forme de flux. Les flux vous fournissent des données précieuses sur les menaces provenant de sources telles que STIX, MISP, etc., qui répertorient les entités de veille sur les menaces.

La bibliothèque du Centre de sécurité des renseignements sur les menaces explique comment parcourir les données, en effectuant des recherches de base et avancées et des règles de filtrage, en invoquant l'assistant d'importation, en ajoutant manuellement des enregistrements de renseignements sur les menaces, en effectuant les actions nécessaires telles que l'ajout à la liste d'autorisation, à la liste de refus et à la liste de surveillance.

La vue détaillée fournit des informations sur les enregistrements d'intelligence et, à partir de vues de listes, vous pouvez effectuer des actions rapides sur un ou plusieurs enregistrements.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comprendre le modèle de données

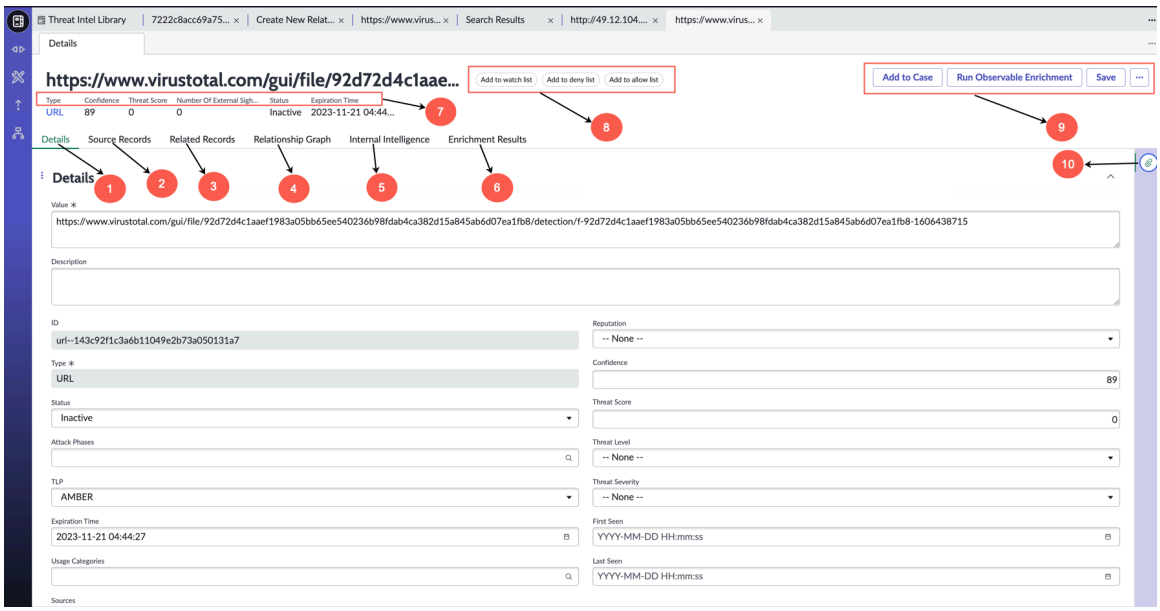
Le modèle de données et l'architecture du module Threat Intelligence Security Center sont conçus pour prendre en charge les fonctionnalités de la plateforme Threat Intelligence et différentes vues de sécurité qui fournissent des données détaillées aux analystes de menaces.

Le modèle de données comporte les structures de données qui sont représentées comme des objets dans le référentiel Threat Intelligence.

TISC Vue du formulaire des objets de bibliothèque

La Centre de sécurité des renseignements sur les menaces page d'accueil des objets comprend les fonctionnalités suivantes.

Utilisez ou accédez à ces sections suivantes pour en savoir plus sur chaque SDO.



TISC Vue du formulaire des objets de bibliothèque

Ordre	Menu/Onglet	Description
1	Onglet **Détails**	Utilisez cette section pour afficher ou modifier les SDO dans la vue de formulaire.
2	**Onglet Enregistrements sources**	Les enregistrements sources contribuent à un enregistrement agrégé tel qu'affiché dans la vue de formulaire. Ces enregistrements sources sont créés automatiquement à partir de flux ou créés manuellement par l'utilisateur.
3	Onglet **Enregistrements connexes**	Répertorie tous les enregistrements connexes associés au SDO.
4	**Onglet Graphe des relations**	Représentation visuelle des objets connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

TISC Vue du formulaire des objets de bibliothèque (suite)

Ordre	Menu/Onglet	Description
5	**Onglet Intelligence interne**	Répertorie les enregistrements d'intelligence interne des objets associés.
6	**Onglet Résultats de l'enrichissement**	Répertorie les intégrations d'enrichissement associées aux objets.
7	**Bannière de formulaire**	Il s'agit d'une section en lecture seule, qui contient les champs clés tels que le type, la fiabilité, le score de menace, le nombre de perceptions, l'état et le délai d'expiration.
8	**Actions d'interface utilisateur de la bannière de formulaire**	Il s'agit des listes de contrôles de sécurité sur lesquelles vous pouvez cliquer si vous devez les ajouter à la liste d'autorisation, les supprimer de la liste d'autorisation (liste de refus ou les ajouter à la liste de surveillance en fonction des observables). Cliquez pour : • Ajouter à la liste de surveillance • Ajouter à la liste de refus • Ajouter à la liste d'autorisation **Remarque :** Les actions du formulaire ne sont applicables qu'aux observables.
9	**Actions d'interface utilisateur du formulaire**	Les actions d'interface utilisateur de formulaire disponibles sont : 1. **Ajouter au ticket** : ajoutez les objets au ticket. 2. **Exécuter l'enrichissement de l'observable** : exécutez les enrichissements dans les objets sélectionnés. 3. **Enregistrer : enregistrez** l'enregistrement. 4. **Supprimer** : supprimer l'enregistrement.
10	**Menu contextuel de droite**	Permet d'accéder facilement aux contrôles rapides tels que les pièces

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

TISC Vue du formulaire des objets de bibliothèque (suite)

Ordre	Menu/Onglet	Description
		jointes, les notes, etc., en fonction des tâches associées à cet objet. Cette option est disponible dans les deux onglets restants pour que l'analyste de menaces puisse y accéder à tout moment. Le menu contextuel permet de naviguer facilement vers : 1. **Pièces jointes** : joignez tout fichier associé aux objets. **Remarque :** Chaque fois que vous créez un nouvel observable, des indicateurs ou des objets ou que vous affichez les objets existants, le volet **Pièces jointes** s'affiche par défaut sur la vue de formulaire respective. Vous pouvez cliquer sur l'icône **Pièces jointes** dans le menu contextuel de droite ou accéder à **Préférences** > **Espaces de travail** et désactivez **l'option Afficher la barre latérale**. Pour plus d'informations, consultez Configurer les préférences de l'espace de travail Next Experience . 2. **Aperçus** : ajoutez toute information supplémentaire relative aux observables ou indicateurs associés à cet objet.
N/A	**Rechercher dans le navigateur**	Utilisez cette fonction de recherche pour rechercher divers objets dans la bibliothèque Threat Intelligence (TI). Par exemple, vous pouvez rechercher tous les enregistrements d'observables dans le module de bibliothèque TI.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

TISC Vue du formulaire des objets de bibliothèque (suite)

Ordre	Menu/Onglet	Description
N/A	**Rechercher dans la bibliothèque Threat Intelligence**	Utilisez cette fonction de recherche pour rechercher les enregistrements sources dans plusieurs sources en fonction de vos critères de recherche. Les résultats seront affichés dans un onglet Résultats **de recherche** distinct. Par exemple, pour une adresse IP 104.227.137.35, si vous devez rechercher les enregistrements, en saisissant 104.*, la recherche réduira les enregistrements et affichera les enregistrements contenant l'adresse IP commençant par 104 dans l'onglet Résultats **de recherche** distinct. • Vous pouvez également modifier les mots clés de recherche existants dans les critères de recherche sur la même page de résultats de recherche sans revenir à la page Bibliothèque de menaces. • De même, vous pouvez également effectuer une recherche basée sur le nom et la description d'un enregistrement particulier. • Une fois les enregistrements filtrés et répertoriés, vous pouvez cliquer sur la vue de liste qui vous amènera à l'enregistrement respectif dans un nouvel onglet.

Traduction automatique

Référentiel de bibliothèque TISC

Le référentiel IoC contient des objets STIX, chacun de ces objets contient une information spécifique.

Observables

Les observables représentent des propriétés avec état (telles que le hachage MD5 d'un fichier ou la valeur d'une clé de registre) ou des événements mesurables (tels que la création d'une clé de registre ou la suppression d'un fichier) qui sont pertinents pour le fonctionnement des ordinateurs et des réseaux.

Le type d'observables disponibles dans l'application est le suivant :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Artefact
- Numéro AS
- Répertoire
- Nom du domaine
- Adresse e-mail
- E-mail
- Objet de l'e-mail
- Fichier
- Adresse IPv4
- CIDR IPv4
- Adresse IPv6
- CIDR IPv6
- Adresse MAC
- Hachage MD5
- Nom Mutex
- Réseau
- Autre observable
- Processus
- Hachage SHA1
- Hachage SHA256
- Hachage SHA512
- Logiciel
- URL
- Compte d'utilisateur
- Clé de registre Windows
- Certificat X.509

Traduction automatique

Définir un observable

Les observables peuvent être récupérés à partir de l’ingestion de flux planifiée ou de l’assistant d’importation. Toutefois, vous pouvez créer des observables selon vos besoins.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **Observables** > **Tous les observables**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez le **type d’observable**.
   Le formulaire d’enregistrement Créer un observable s’affiche.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

4. Remplissez les champs du formulaire.

Remarque : Chaque fois que vous créez un nouvel observable ou que vous affichez les observables existants, le volet **Pièces jointes** s'affiche par défaut sur la vue de formulaire. Vous pouvez cliquer sur l'icône Pièces jointes dans le menu contextuel de droite ou accéder à **Préférences** > **Espaces de travail** et désactivez **l'option Afficher la barre latérale**. Pour plus d'informations, consultez Configurer les préférences de l'espace de travail Next Experience .

Section des détails

Champ	Description
Valeur	Valeur (par exemple, adresse IP ou hachage) associée à l'observable.
Description	Description de l'enregistrement de l'observable.
Auteur	Saisissez le nom.
Type	Type de classification de l'observable, tel qu'une adresse IP, un nom de domaine, un artefact, un répertoire, un fichier ou un hachage. Par défaut, il s'affiche lorsque vous sélectionnez le nouvel enregistrement.
Statut	État actif ou inactif de l'observable.
Phases d'attaque	Représente la phase d'attaque dans une chaîne de frappe telle que LM, MITRE ATT&CK.
TLP	Valeur unique qui indique le paramètre de sensibilité des données par TLP.
Réputation	Spécifie la réputation malveillante de l'observable.
Statut	Saisissez l'état de l'observable s'il est actif ou inactif.
Score de menace	Indique le score de menace pour cet observable.
Délai d'expiration	Spécifie le délai d'expiration de l'enregistrement observable.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Fiabilité	Saisissez le score de confiance pour cet enregistrement observable. La propriété de confiance identifie la confiance que le créateur a dans l'exactitude de ses données. La valeur de confiance DOIT être un nombre compris entre 0 et 100.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Empêcher les mises à jour système	Si vous définissez ce marqueur sur vrai, le système ne remplace pas les valeurs des champs de l'enregistrement.
Est un faux positif	Marqueur booléen qui indique si l'observable est identifié comme faux positif.

Attributs

Champ	Description
Résolution à	Spécifie une liste de références à une ou plusieurs adresses IP ou noms de domaine auxquels le nom de domaine se résout.
Est FQDN	Un nom de domaine complet (FQDN) est l'adresse complète d'un hôte Internet ou d'un ordinateur. Il fournit son emplacement exact dans le système de noms de domaine (DNS) en spécifiant le nom d'hôte, le nom de domaine et le domaine de premier niveau (TLD).

Information supplémentaire

Champ	Description
Niveau de menace	Indique le niveau de menace de l'enregistrement de l'observable.
Premier observé	Heure à laquelle cet enregistrement observable a été vu pour la première fois en train d'effectuer des activités malveillantes.
Gravité de la menace	Indique la gravité de la menace de l'enregistrement de l'observable.
Dernier observé	Heure à laquelle cet enregistrement observable a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Catégories d'utilisation	Catégories auxquelles appartient l'observable, telles que botnet ou hameçonnage.
Phases d'attaque	Représente la phase d'attaque dans une chaîne de frappe telle que LM, MITRE ATT&CK.
Contexte supplémentaire	Ajoutez un contexte supplémentaire.
Sources	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.

Important : Score rapporté de la source : ce champ contient la valeur agrégée des scores de menace signalés par les sources à partir desquelles l'observable est ingéré. Pour afficher ce champ sur le formulaire d'enregistrement d'observable, vous devez l'ajouter manuellement, car il n'est pas disponible par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attributs

Champ	Description
Résolution à	Spécifie une liste de références à une ou plusieurs adresses IP ou noms de domaine auxquels le nom de domaine se résout.
Est FQDN	Un nom de domaine complet (FQDN) est l'adresse complète d'un hôte Internet ou d'un ordinateur. Il fournit son emplacement exact dans le système de noms de domaine (DNS) en spécifiant le nom d'hôte, le nom de domaine et le domaine de premier niveau (TLD).

Remarque : Résout les attributs **FQDN** de et Est ne s'appliquent qu'au type **de nom de domaine** des observables.

Attributs de type observable

Nom d'attribut	Types d'attributs
Artefact	○ Clé de déchiffrement ○ Algorithme de chiffrement ○ Hachage MD5 ○ Type MIME ○ Hachage SHA1 ○ Hachage SHA256 ○ Hachage SHA512 ○ URL
Numéro AS	○ Nom ○ RIR
Répertoire	○ Heure de création du répertoire ○ Heure du dernier accès au répertoire ○ Heure de la dernière modification du répertoire ○ Chemin d'accès codé
Nom du domaine	○ Est FQDN ○ Résolution à
Adresse e-mail	○ Nom complet ○ Corps de l'e-mail ○ Destinataires d'e-mail Bcc ○ Destinataires d'e-mail Cc

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'attribut	Types d'attributs
	○ Destinataires d'e-mail à ○ Expéditeur d'e-mail ○ Objet de l'e-mail ○ Date d'envoi
Fichier	○ Information supplémentaire ○ Nom de fichier codé ○ Heure de création du fichier ○ Heure du dernier accès au fichier ○ Heure de la dernière modification du fichier ○ Nom du fichier Nombre magique ○ Hachage MD5 ○ Type MIME ○ Hachage SHA1 ○ Hachage SHA256 ○ Hachage SHA512
Adresse IPv4	○ Numéro AS ○ Adresse MAC
CIDR IPv4	○ Numéro AS ○ Adresse MAC
Adresse IPv6	○ Numéro AS ○ Adresse MAC
CIDR IPv6	○ Numéro AS ○ Adresse MAC
Réseau	○ Octets de destination ○ Nombre Nombre de paquets de destination ○ Port de destination ○ Heure de fin ○ Longueur de corps de message HTTP ○ En-tête de demande HTTP ○ Méthode de demande HTTP ○ Valeur de demande HTTP ○ Version de demande HTTP ○ Octet de code ICMP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'attribut	Types d'attributs
	○ Octet de type ICMP ○ Le réseau est-il actif ? ○ L'embase bloque-t-elle ? ○ L'embase est-elle à l'écoute ? ○ Protocoles réseau ○ Famille d'adresses d'embases ○ Descripteur d'embase ○ Traitement d'embase ○ Options d'embase ○ Nombre d’octets source de type d’embase ○ Nombre de paquets source ○ Port source ○ Heure de début ○ Marqueurs de destination TCP ○ Marqueurs source TCP
Processus	○ ASLR activée ○ Ligne de commande ○ Répertoire de travail actuel (CWD) ○ DEP activée ○ Variables environnementales ○ Est masqué ○ SID du propriétaire ○ ID de processus ○ Priorité ○ Heure de création de processus ○ Descriptions des services ○ Nom d'affichage du service ○ Nom du groupe de services ○ Nom de service ○ Type de démarrage de service ○ État de service Type de service ○ Information sur le démarrage ○ Niveau d'intégrité Windows ○ Titre de la fenêtre

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'attribut	Types d'attributs
Logiciel	○ Common Platform Enumeration (CPE) ○ Langues prises en charge ○ Identification logicielle (SWID) ○ Version du fournisseur
Compte d'utilisateur	○ Heure de création du compte ○ Délai d'expiration du compte ○ Connexion au compte ○ Type de compte ○ Information supplémentaire ○ Peut escalader les privilèges ○ Heure de la dernière modification des informations d'identification ○ Nom d'affichage ○ Heure de la première connexion ○ Le compte est-il désactivé ? ○ Est doté de privilèges ○ Est un compte de service ○ Heure de la dernière connexion ○ ID d'utilisateur
Clé de registre Windows	○ Clé modifiée ○ Valeur de registre temporel ○ Nombre de sous-clés
Certificat X.509	○ Information supplémentaire ○ Identificateur de clé d'autorité ○ Contraintes de base ○ Politiques de certificat ○ Points de distribution CRL ○ Utilisation de clé étendue ○ Empêcher toute politique ○ Émetteur ○ Nom alternatif de l'émetteur ○ Est signé automatiquement ○ Utilisation de la clé ○ Contraintes de nom ○ Contraintes de politique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom d'attribut	Types d'attributs
	○ Mappages de politiques ○ Date de début de validité de l'utilisation de clé privée ○ Date de fin de validité de l'utilisation de clé privée ○ Algorithme de signature ○ Objet ○ Nom alternatif du sujet ○ Attributs du répertoire d'objet ○ Identificateur de clé d'objet ○ Algorithme de clé publique d'objet ○ Exposant de clé publique d'objet ○ Module de clé publique d'objet ○ Date de début de validité ○ Fin de validité ○ Version

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour un enregistrement d’observable.

5. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d’invite s’affiche indiquant qu’un nouvel enregistrement d’observable est créé. Cliquez sur **Continuer** pour modifier l’enregistrement et créer de nouvelles relations.
6. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d’observable, la case **à cocher Empêcher les mises à jour système** s’affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l’observable, de l’indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à un observable.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez la taxonomie associée à un observable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à un observable.

Enregistrements sources

Champ	Description
Les détails des enregistrements sources d’un observable sont affichés, le cas échéant.	

Que faire ensuite

La table suivante répertorie les enregistrements connexes associés aux observables :

Enregistrements connexes

Liste connexe	Description
Observable	Liste des observables associés à cet observable. **Remarque :** Cette section contient également les relations potentielles entre deux observables. Pour plus d’informations, consultez Confirmer la relation observable-observable potentiel et consultez Définir les relations observable-observable les relations confirmées entre les deux observables.
Indicateurs	Liste des indicateurs associés à cet observable.
Schémas d'attaque	Liste des schémas d’attaque associés à cet observable.
Campagnes	Répertorie les campagnes associées à cet observable.
Infrastructure	Énumérez l’infrastructure telle que les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont liées à cet observable.
Ensembles d'intrusion	Répertoriez les ensembles d’intrusion, tels qu’un ensemble de comportements et de ressources antagonistes ayant des propriétés communes à cet observable.
Programme malveillant	Répertoriez les enregistrements sources de programmes malveillants associés à cet observable.
Acteurs de menace	Répertoriez les acteurs de menace associés à cet observable.
Événements de menace	Répertoriez les événements de menace associés à cet observable.
Vulnérabilités	Si l’observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante et qui sont liées à cet observable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. En outre, à partir de la section **Enregistrements connexes** , vous pouvez confirmer les relations entre deux observables à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire **Observables** . Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
3. Vous pouvez ajouter des observables aux tickets. Pour plus d'informations, consultez Ajouter au ticket.
4. Vous pouvez également exécuter des actions d'enrichissement des observables. Pour plus d'informations, consultez Exécuter des actions d'enrichissement dans un ticket.

Enregistrements sources des observables

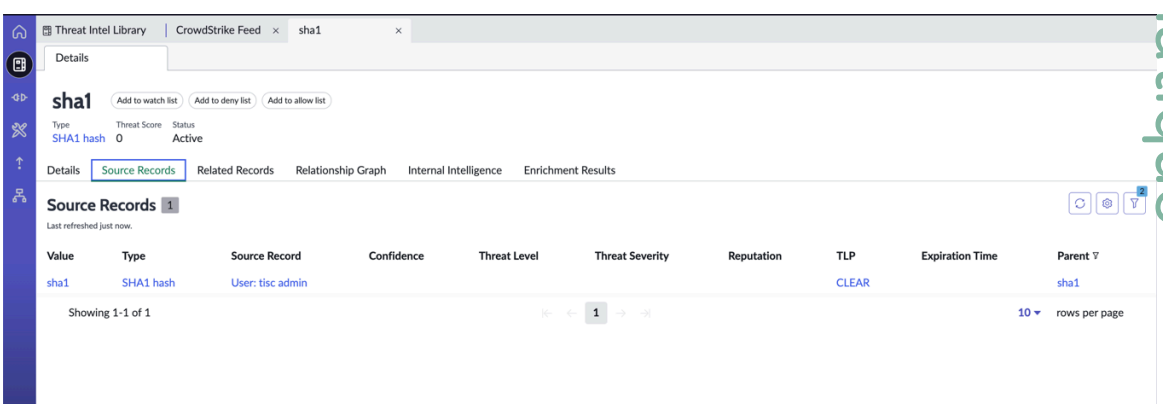
Les enregistrements sources contribuent à un enregistrement agrégé, comme indiqué dans la vue de formulaire. Ces enregistrements sources sont créés automatiquement à partir de flux ou créés manuellement par l'utilisateur.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Sélectionnez un ou plusieurs observables.
5. Accédez aux **enregistrements sources**.
   Les enregistrements sources d'un enregistrement agrégé s'affichent.



6. Affichez les enregistrements.

Lier les enregistrements connexes à Threat Intelligence

Lier les enregistrements associés aux objets Threat Intelligence correspondants.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez n'importe quel enregistrement d'observable à titre d'exemple.
3. Accédez à la section **Enregistrements connexes** .
4. Sélectionnez n'importe quel enregistrement associé.
5. Cliquez sur **un lien**.
   La boîte de dialogue Objets de lien s'affiche.
6. Sélectionnez les objets dans la liste et cliquez sur le bouton **Lien** .
   Les objets associés à un enregistrement d'observable seront liés et affichés dans la vue de liste Enregistrements connexes.
7. Cliquez sur **Enregistrer**.
   Cliquez sur le bouton **Dissocier** pour supprimer le lien des objets

Extraire les données des observables

Extraire les données des enregistrements connexes des observables.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **Observables**.
   Les observables associés à l'objet sélectionné s'affichent.
4. Sélectionnez n'importe quel enregistrement observable.
   Si des CVE sont associées aux observables donnés, vous pouvez extraire automatiquement les données associées à la vulnérabilité à l'aide du bouton fourni, et ces enregistrements associés s'affichent dans la section Contexte métier des vulnérabilités.
5. Accéder à **Intelligence interne** > **Entrées vulnérables**.
   Les enregistrements CVE associés pour les observables s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

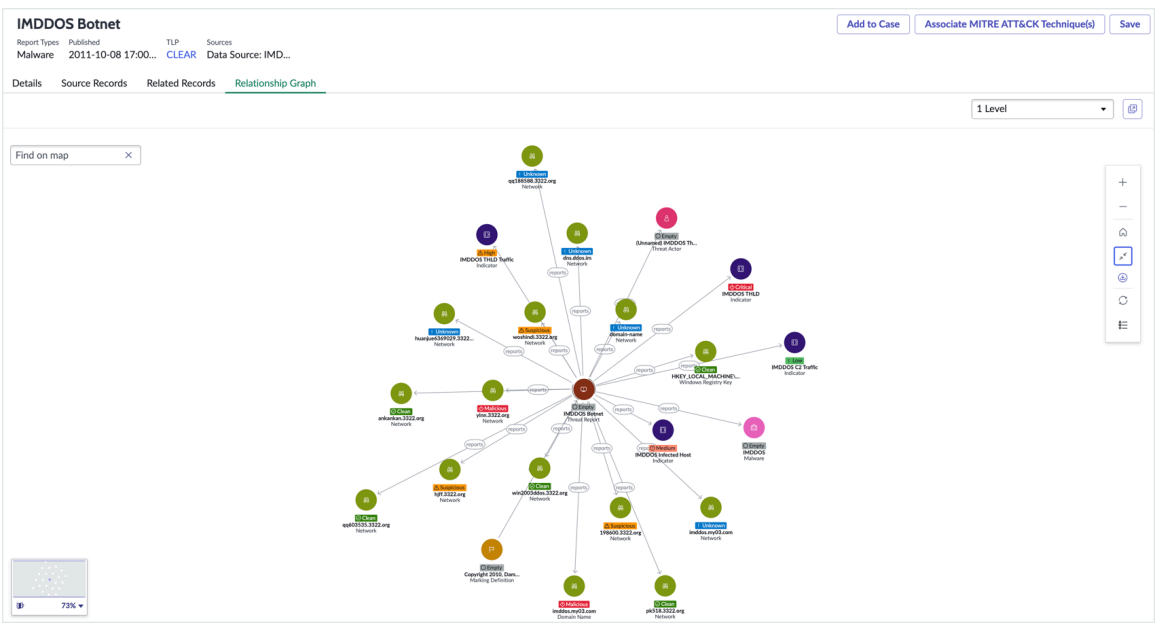
6. Sélectionnez n'importe quel CVE et cliquez sur **le bouton Extraire les données associées à la vulnérabilité** .

Remarque :

- Un message d'information indique que cet objet de vulnérabilité spécifique n'a aucune entrée vulnérable qui lui est associée. Vous devez associer le ou les objets aux entrées vulnérables pour extraire les données. Pour plus d'informations, Extraire les données de vulnérabilité consultez comment lier les enregistrements et effectuer la tâche planifiée pour extraire les données. et pour plus d'informations sur les travaux planifiés, voir Travaux planifiés .
- Ce bouton déclenche une tâche planifiée en arrière-plan, et les détails de lancement et d'exécution de la tâche sont affichés dans la section Flux d'activité. Par exemple, lorsque la tâche est déclenchée, le flux d'activité affiche une activité dont la récupération des données associées avec les entrées vulnérables a commencé. La tâche planifiée en arrière-plan vérifie en permanence tous les observables qui ont une entrée vulnérable associée à l'observable et s'exécute automatiquement. Cette tâche planifiée s'exécute toutes les heures. Si les enregistrements ne sont pas récupérés, vous pouvez lier manuellement les enregistrements et extraire les données.

Afficher les détails dans le visualiseur

À l'aide du visualiseur, vous pouvez visualiser les relations entre les objets, les observables et les indicateurs, ce qui vous fournit un contexte pour une étude plus approfondie. Le visualiseur utilise des couleurs et des icônes pour illustrer diverses informations sur les objets.



Vous pouvez faire ce qui suit :

- Zoomez sur n'importe quel objet, adaptez-le à l'écran, faites glisser les nœuds ou épinglez-les pour vous concentrer sur une relation particulière.
- Cliquez sur n'importe quel objet pour ouvrir le volet de détails. Dans le volet de détails, vous pouvez obtenir plus d'informations associées à l'objet. Vous pouvez afficher les propriétés du nœud telles que l'objet, le nom de l'objet, la description et les sources. Par défaut, la section des détails de chaque nœud de graphe n'est pas affichée et vous devez cliquer sur chaque nœud du graphe pour afficher les détails du nœud sélectionné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Le visualiseur est disponible pour tous les objets de domaine STIX (SDO), à l'exception des objets de données observées. Cliquez sur le bouton **Actualiser** pour actualiser le visualiseur.

- Vous pouvez également cliquer sur l'icône contextuelle pour afficher le graphique dans une fenêtre beaucoup plus grande.

Lier les actions de nœud dans le graphe des relations

Ajoutez de nouveaux enregistrements connexes pour lier les nœuds.

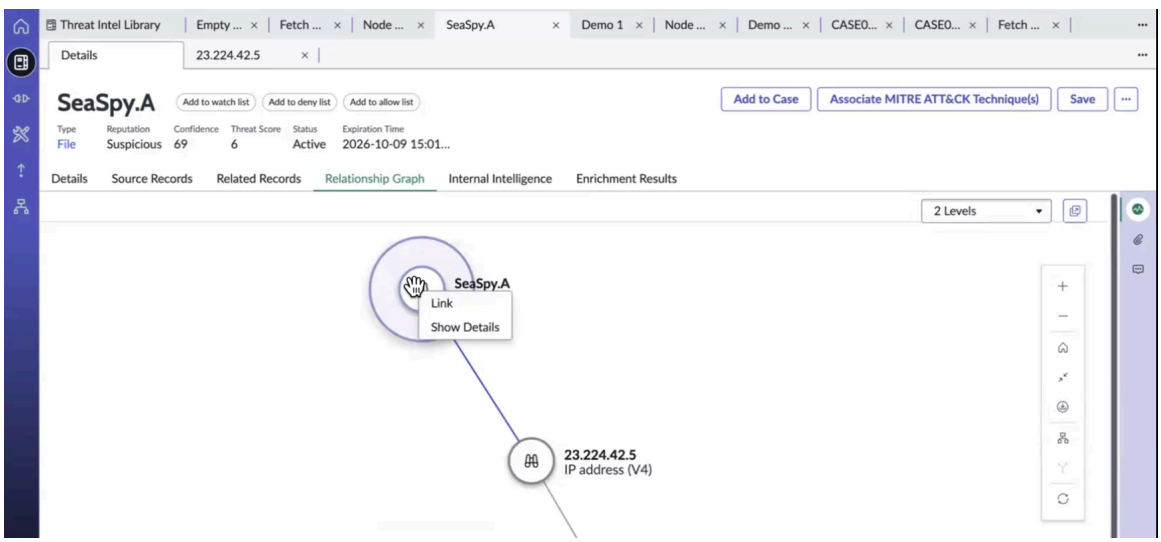
Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez n'importe quel enregistrement d'observable à titre d'exemple.
3. Accédez à la section **Graphiques des relations** .
4. Cliquez sur le nœud.
5. Cliquez sur **un lien**.

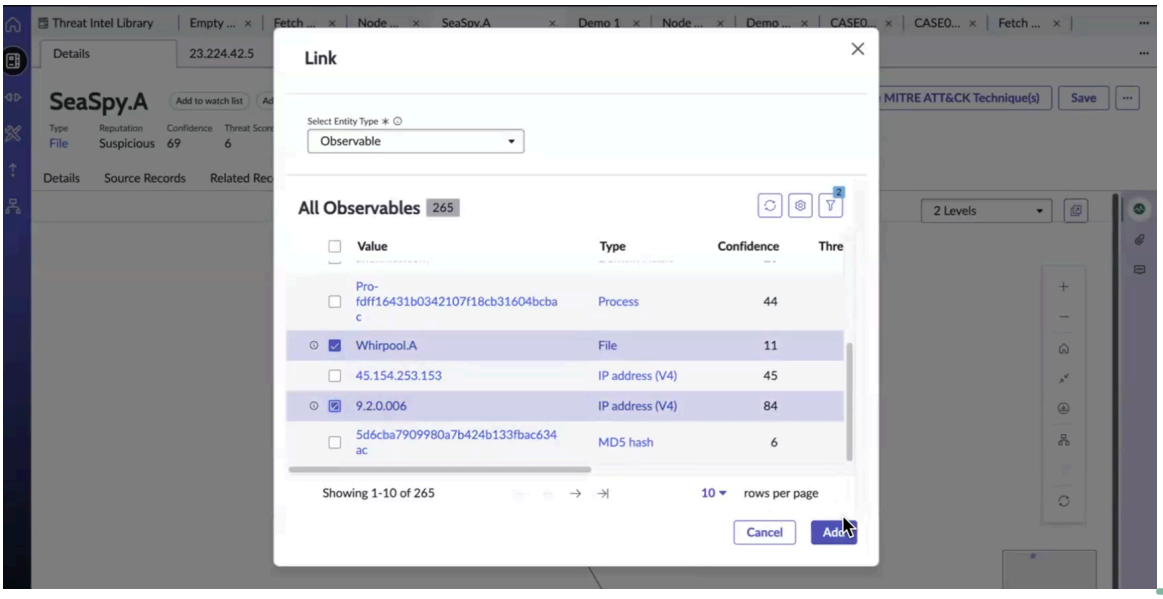
Remarque : Cette action n'est disponible qu'au niveau d'un nœud d'accueil.



6. Sélectionnez le type d'entité tel qu'observable.
7. Sélectionnez un ou plusieurs observables sur le nœud parent.
8. Cliquez sur **Ajouter**.
   Les observables sont ajoutés au nœud parent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Sélectionnez **Dissocier** pour dissocier les enregistrements connexes des nœuds.

> **Remarque :** Les données des enregistrements connexes ne sont pas liées, mais les relations entre le nœud d'accueil et l'observable seront toujours présentes dans la bibliothèque Threat Intelligence.

10. Sélectionnez **Afficher les détails** pour afficher les données observables associées.

Utilisation des enregistrements de renseignements internes

Utilisez cette fonctionnalité pour utiliser les données d'intelligence internes collectées depuis le système de gestion de la base de données de configuration (CMDB) dans Centre de sécurité des renseignements sur les menaces.

Afficher les enregistrements d'intelligence interne

Affichez les enregistrements d'intelligence interne collectés à partir de CMDB, Security Incident Response (SIR) et Vulnerability Response (VR) ces enregistrements.

Avant de commencer

La section Intelligence interne fournit le contexte d'autres applications sur la plateforme telles que SIR, VR et CMDB afin de fournir une perspective plus large de la menace aux analystes.

Rôle requis : sn_sec_tisc.analyst

> **Remarque :** L'onglet Intelligence interne n'est visible que pour les observables et les objets de vulnérabilité.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez n'importe quel enregistrement d'observable.
3. Accédez à l'onglet **Intelligence interne** .
   La section Intelligence interne comprend trois sous-sections telles que Réponse aux incidents de sécurité, Contexte commercial, Réponse aux vulnérabilités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Vous devez avoir installé les applications respectives sur votre instance pour que ces sections soient répertoriées dans l'onglet **Intelligence interne** .

a. **Réponse aux incidents de sécurité** : affiche tous les incidents qui sont liés aux observables et aux éléments de vulnérabilité associés.

Remarque : La valeur du ou des observables doit correspondre entre l'incident SIR et également dans le TISC, puis les observables ou indicateurs associés sont répertoriés dans la section Réponse aux incidents de sécurité. Vous pouvez également lier et dissocier les enregistrements en recherchant les enregistrements dans les systèmes sources. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.

- Sélectionnez n'importe quel enregistrement pour naviguer et afficher les détails dans le système source. Par exemple, Observables associés dans Réponse aux incidents de sécurité pour extraire les enregistrements observables associés.
- Dans le cadre de la version actuelle, les données d'intelligence que vous pouvez extraire des enregistrements sources (SIR) sont les suivantes :
  - Observables associés
  - Éléments de vulnérabilité

b. **Contexte professionnel** : affiche les utilisateurs affectés et tout autre élément de configuration. Dans le cadre de la version actuelle, les données d'intelligence que vous pouvez extraire des enregistrements sources (contexte métier) sont les suivantes :
  - Éléments de configuration
  - Services affectés
  - Actifs affectés

c. **Réponse aux vulnérabilités** : affiche les données d'intelligence sur les vulnérabilités.

Entrées de vulnérabilité : cette option permet de faire correspondre les vulnérabilités et d'extraire les enregistrements connexes.

Exécuter des actions d'enrichissement à partir d'observables

Utilisez cette section pour comprendre comment les actions d'enrichissement sont effectuées sur les observables et autres objets.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Cliquez sur toutes les actions d'enrichissement à partir du bouton fractionner.
5. Sélectionnez la ou les implémentations disponibles.
6. Cliquez sur **Envoyer**.
   Par exemple, Exécuter une recherche de menace. L'action d'enrichissement sélectionnée sera exécutée et un message d'information s'affichera indiquant que l'exécution de l'enrichissement de l'observable a

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

commencé sur le ou les observables sélectionnés. Les résultats seront disponibles dans la page détaillée du ou des observables respectifs une fois l'exécution terminée.

Remarque : Une fois l'exécution initiée ou terminée, une note de travail est publiée sur le flux d'activité de la vue de formulaire.

Ajouter au ticket

Ajouter des observables, des indicateurs ou d'autres objets au ticket.

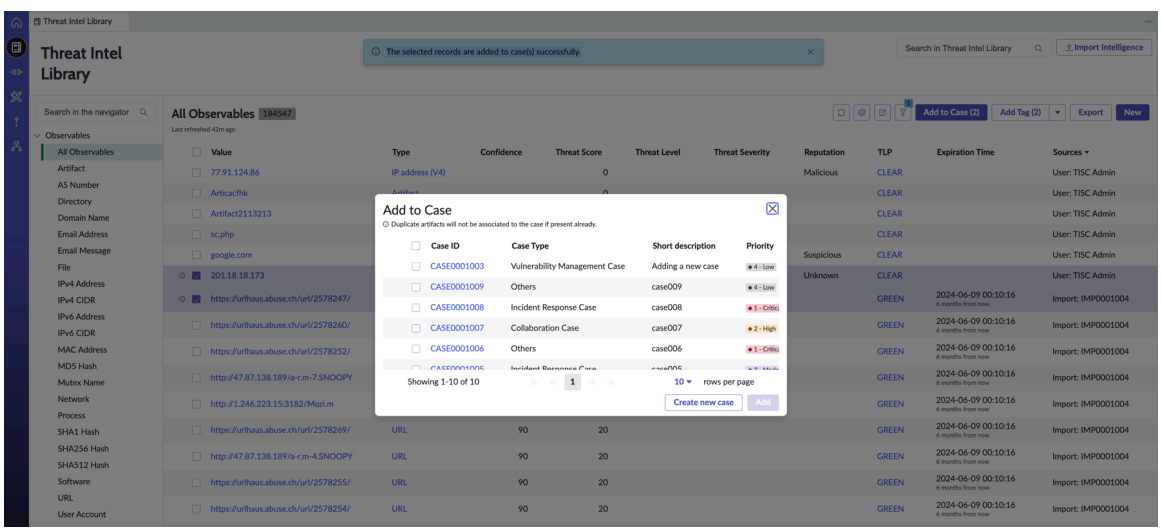
Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Voici la procédure qui montre comment ajouter un ticket à un enregistrement observable.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez le ou les observables.
3. Cliquez sur **le bouton Ajouter au ticket** .
   Cela affiche uniquement les tickets pour lesquels l'enregistrement n'est pas déjà associé.



4. Vérifiez si vous souhaitez ajouter l'enregistrement aux tickets existants, puis sélectionnez le ticket existant.
   Sinon, cliquez sur **Créer un nouveau ticket**.
   Créez un nouveau ticket en saisissant les informations suivantes.

Créer un ticket

Champ	Description
ID du ticket	Un identificateur unique pour le ticket. Il s'agit d'un ID généré par le système.
Description brève	Résumé de la demande ou du problème en cours d'examen ou brève description.
Type de ticket	Sélectionnez le type de ticket faisant l'objet de l'enquête. Les options possibles pour l'enquête sont les suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Recherche des menaces ○ Demande d'informations ○ Ticket de gestion de la vulnérabilité ○ Ticket de conformité ○ Ticket de réponse aux incidents ○ Ticket de collaboration ○ Autres
Priorité	Une évaluation de la gravité de la demande ou du problème.
Groupe d'affectation	Le groupe affecté responsable du travail sur le ticket.
Affecté à	L'analyste responsable du travail sur un ticket.

5. Cliquez sur **Créer** si vous créez un nouveau ticket.

   Remarque : Le nouveau ticket est ajouté à la liste de tickets existante.

6. Sélectionnez le ou les tickets nouvellement ajoutés.
7. Cliquez sur **Ajouter**.
   Un message d'information s'affiche indiquant que les enregistrements sélectionnés sont ajoutés au ou aux tickets.

Exécuter des opérations d'enrichissement dans TISC

Le tableau ci-dessous décrit les interactions impliquées dans l'exécution de différentes opérations d'enrichissement à partir de TISC.

Écrans modaux TISC

Option	Interactions avec les cadres de travail UX	Intégrations prises en charge
Exécuter une recherche de menace	À l'écran 1 – Sélectionnez la ou les implémentations et soumettez-les. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour l'exécution de la recherche de menace.	• Virus Total • Crowd Strike Falcon Intelligence
Exécuter la recherche de perception	Écran 1 – Sélectionner Implémentations et Écran 2 – Entrées communes sont applicables. La recherche de perception utilise la date et la	• Recherche élastique • Perception Splunk

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Interactions avec les cadres de travail UX	Intégrations prises en charge
	fréquence comme entrées communes dans plusieurs implémentations de Splunk et d'autres intégrations.	
Exécuter l'enrichissement de l'élément observable	Écran uniquement 1 – Sélectionnez Implémentations. Il n'existe pas d'entrées communes ou d'entrées spécifiques à l'implémentation applicables pour Exécuter l'enrichissement de l'élément observable.	• WHOIS (en anglais seulement) • Shodan

Exécuter une recherche de menace

Sélectionnez une ou plusieurs implémentations applicables pour exécuter une recherche de menace sur les observables.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

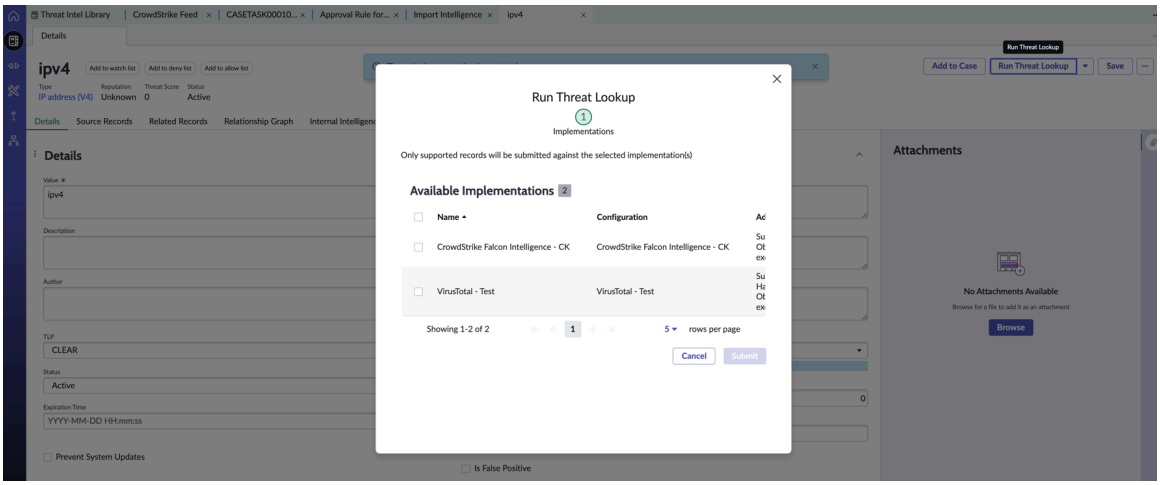
1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Cliquez sur **Exécuter une recherche de menace**.
   L'écran modal Exécuter **les implémentations de sélection de** la recherche de menace s'affiche.

   Remarque : L'option Exécuter une recherche de menace effectue des recherches de renseignements sur les menaces afin de déterminer si les observables sont associés à des menaces connues.

6. Sélectionnez la ou les implémentations requises dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Cliquez sur **Envoyer**.
   L'action d'enrichissement sélectionnée est exécutée et un message d'information s'affiche indiquant que l'exécution de la recherche de menaces a commencé.

Remarque :

- Une fois l'exécution initiée ou terminée, une note de travail est publiée sur le flux d'activité de la vue de formulaire.
- Les résultats de l'enrichissement transmis depuis l'espace de travail SIR se trouvent dans l'onglet **Résultats de l'enrichissement** de la page détaillée des observables correspondante dans l'espace de travail TISC.
- Les résultats d'enrichissement transmis depuis l'espace de travail SIR peuvent être identifiés à l'aide du champ **Source** de la table des résultats d'enrichissement.

Exécuter la recherche de perception

Exécuter l'intégration liée à la recherche de perception.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Pour effectuer cette action, sélectionnez l'implémentation et ajoutez des entrées d'exécution communes qui s'appliquent à toutes les implémentations sélectionnées, le cas échéant.

Procédure

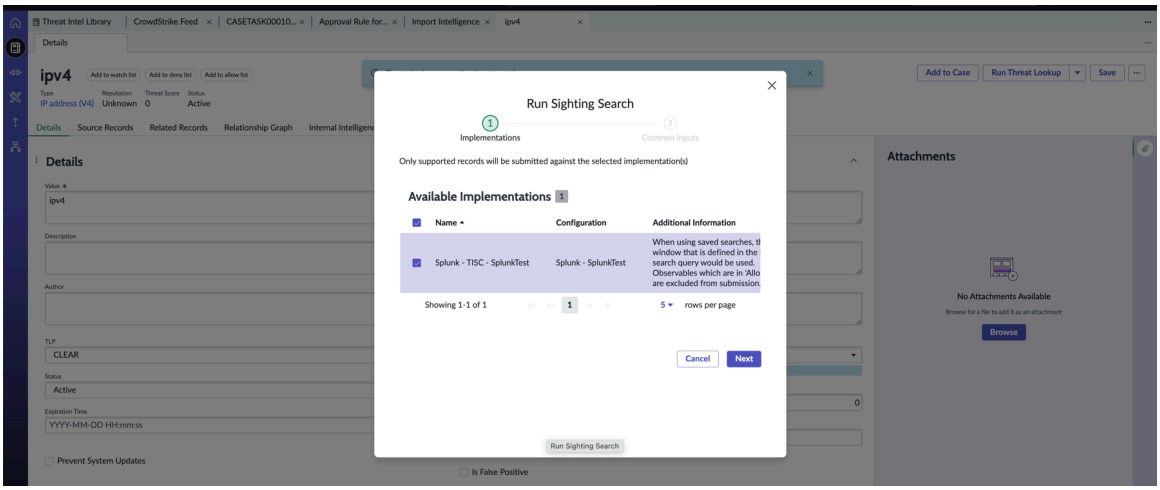
1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Console d'analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n'importe quel enregistrement d'observable.
5. Cliquez sur **Exécuter la recherche de perception**.
   L'écran modal Exécuter la recherche de perception **Sélectionner des implémentations** s'affiche.

Remarque : L'exécution de la recherche de perception effectue des recherches de renseignements sur les menaces pour déterminer si les observables sont associés à des menaces connues.

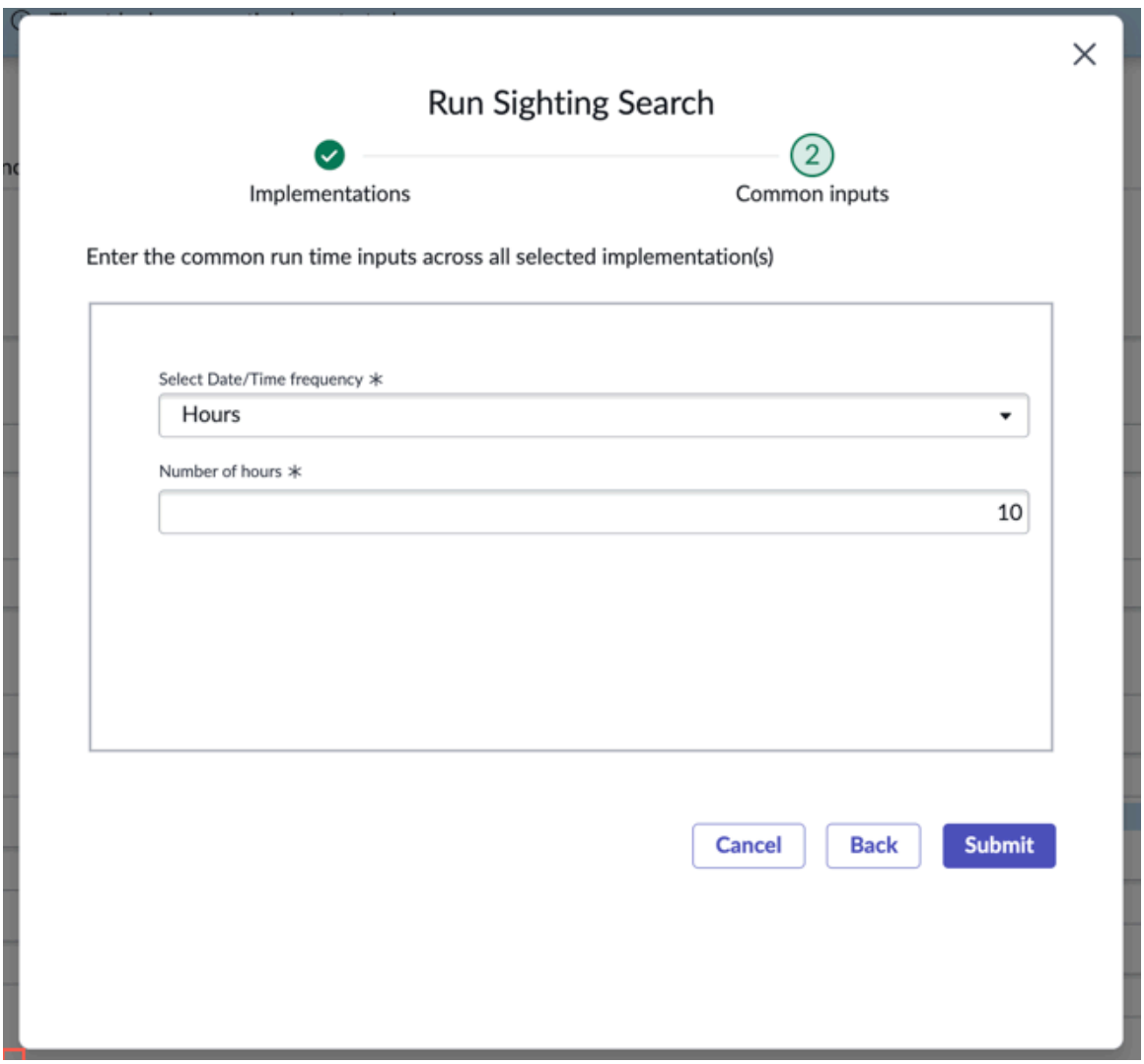
6. Sélectionnez la ou les implémentations requises dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Cliquez sur **Suivant**.
8. Sélectionnez la valeur d'entrée de temps d'exécution commune, telle que Sélectionner la fréquence de l'heure et la date/l'heure.



9. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’action d’enrichissement sélectionnée est exécutée et un message d’information s’affiche indiquant que l’exécution de la recherche de perception a commencé.

Remarque :

- Une fois l’exécution initiée ou terminée, une note de travail est publiée sur le flux d’activité de la vue de formulaire.
- Les résultats de l’enrichissement transmis depuis l’espace de travail SIR se trouvent dans l’onglet **Résultats de l’enrichissement** de la page détaillée des observables correspondante dans l’espace de travail TISC.
- Les résultats d’enrichissement transmis depuis l’espace de travail SIR peuvent être identifiés à l’aide du champ **Source** de la table des résultats d’enrichissement.

Exécuter l'enrichissement de l'élément observable

Sélectionnez une ou plusieurs implémentations applicables pour exécuter une recherche de menace sur les observables.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Procédure

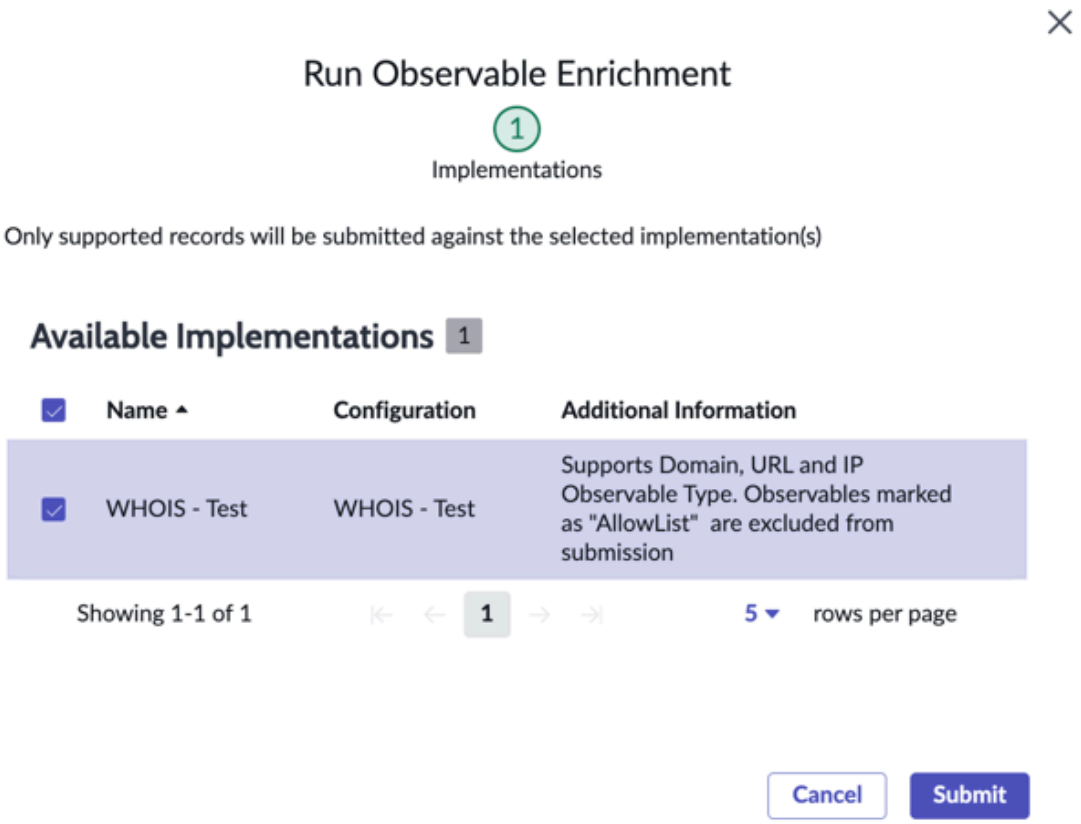
1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l’icône **Console d’analyste de menaces** .
3. Accéder à **Observables** > **Tous les observables**.
4. Ouvrez n’importe quel enregistrement d’observable.
5. Cliquez sur **Exécuter l’enrichissement de l’observable**.
   L’écran modal Exécuter **les implémentations de sélection d’enrichissement de l’observable** s’affiche.

   Remarque : Seuls les enregistrements pris en charge seront soumis sur la ou les implémentations sélectionnées

6. Sélectionnez la ou les implémentations requises (par exemple, WHOIS) dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Cliquez sur **Envoyer**.
L'action d'enrichissement sélectionnée est exécutée et un message d'information s'affiche indiquant que l'exécution de la recherche de menaces a commencé.

Remarque :

- Une fois l'exécution initiée ou terminée, une note de travail est publiée sur le flux d'activité de la vue de formulaire.
- Les résultats de l'enrichissement transmis depuis l'espace de travail SIR se trouvent dans l'onglet **Résultats de l'enrichissement** de la page détaillée des observables correspondante dans l'espace de travail TISC.
- Les résultats d'enrichissement transmis depuis l'espace de travail SIR peuvent être identifiés à l'aide du champ **Source** de la table des résultats d'enrichissement.

Afficher les résultats de l'enrichissement

Affichez les résultats de l'enrichissement des observables, des indicateurs et divers objets.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **Observables** > **Tous les observables**.
2. Sélectionnez n'importe quel enregistrement d'observable.
3. Accédez à **l'onglet Résultats de l'enrichissement** .
   Résultats de l'enrichissement affiche les résultats d'enrichissement des intégrations TISC.

Nom de l'enrichissement	Description
Résultats de la recherche de menace	Répertorie tous les résultats de la recherche de menaces associées pour un observable.
Perceptions	Répertorie toutes les perceptions associées pour un observable.
Résultats de l'enrichissement de l'observable	Répertorie tous les résultats d'enrichissement d'observables associés pour un observable.

Indicateurs

Les indicateurs sont des artefacts observés sur un réseau ou un système d'exploitation qui sont susceptibles d'indiquer une intrusion. Les IoC typiques sont les signatures de virus et les adresses IP, les hachages MD5 de fichiers ou d'URL de logiciels malveillants ou les noms de domaine.

Définir un indicateur

Définissez un indicateur.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **Indicateurs**.
2. **Sélectionnez Indicateur**.
3. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

4. Remplissez les champs du formulaire.

Section des détails

Champ	Description
ID	ID unique de l'indicateur.
Description	Description de l'indicateur.
Nom	Nom de l'indicateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Schéma	Le modèle de détection de cet indicateur peut être exprimé sous la forme d'un modèle STIX.
Type de modèle	Langue du modèle utilisée dans cet indicateur.
Version du modèle	Version du langage de modèle utilisée pour les données dans la propriété de modèle qui doit correspondre au type de données de modèle incluses dans la propriété de modèle.
Date de début de validité	Heure à partir de laquelle cet indicateur est considéré comme un indicateur valide des comportements auxquels il est associé ou qu'il représente.
Fin de validité	Heure après laquelle cet indicateur ne doit plus être considéré comme un indicateur valide des comportements auxquels il est lié ou qu'il représente.
Classification IOC	Classification IOC des indicateurs.
Types des indicateurs	Indique les différentes catégories de l'indicateur.
Statut	Indique l'état des indicateurs.
Plateformes	Définit les plateformes pour lesquelles cet indicateur s'applique.
TLP	Valeur unique qui indique le paramètre de sensibilité des données par TLP.
Phases d'attaque	Représente la phase d'attaque dans une chaîne de frappe telle que LM, MITRE ATT&CK.
Fiabilité	Entrez le score de confiance pour cet enregistrement d'indicateur. La propriété de confiance identifie la confiance que le créateur a dans l'exactitude de ses données. La valeur de confiance DOIT être un nombre compris entre 0 et 100.
Niveau de menace	Indique le niveau de menace de l'enregistrement de l'indicateur.
Délai d'expiration	Spécifie le délai d'expiration de l'enregistrement de l'indicateur.
Gravité de la menace	Indique la gravité de la menace de l'enregistrement de l'indicateur.
Catégories d'utilisation	Catégories auxquelles appartient l'observable, telles que botnet ou hameçonnage.
Premier observé	Heure à laquelle cet enregistrement d'indicateur a été vu pour la première fois en train d'effectuer des activités malveillantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Dernier observé	Heure à laquelle cet enregistrement d'indicateur a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour un indicateur.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet indicateur.
Version de spéc.	Version de la spécification STIX utilisée pour représenter l'indicateur. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Créées	Spécifie l'heure à laquelle l'indicateur est créé dans le système.
Mis à jour	Spécifie l'heure à laquelle l'indicateur est mis à jour dans le système.
Extensions	Indique les extensions de l'indicateur.
État du traitement	Représente l'état de traitement de cet indicateur.

5. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
6. Cliquez sur **Continuer**.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à un indicateur.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez la taxonomie associée à un indicateur.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à un indicateur.

Enregistrements sources

Champ	Description
Les détails des enregistrements sources d'un indicateur sont affichés, le cas échéant.	

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux indicateurs.

Enregistrements connexes

Liste connexe	Description
Techniques MITRE	Répertorie les techniques MITRE associées à cet indicateur.
Schémas d'attaque	Répertorie la source Schémas d'attaque qui décrit les méthodes par lesquelles les adversaires tentent de compromettre les cibles liées à cet indicateur.
Campagnes	Répertorie la source de campagnes qui décrit un ensemble d'activités malveillantes ou d'attaques qui se produisent au fil du temps contre un ensemble spécifique de cibles liées à cet indicateur.
Mesures à prendre	Répertorie les plans d'action associés à cet indicateur.
Sources de données	Répertorie les sources de données associées à cet indicateur.
Composants de données	Répertorie les composants de données associés à cet indicateur.
Identités	Répertorie les identités associées à cet indicateur.
Indicateurs	Répertorie les indicateurs associés à cet indicateur. **Remarque :** Cette section contient également les relations potentielles entre deux indicateurs. Pour plus d'informations, consultez Confirmer les relations potentielles indicateur-indicateur et consultez Définir les relations indicateur-indicateur les relations confirmées entre les deux observables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Liste connexe	Description
Infrastructure	Répertorie la source d'infrastructure qui décrit tous les systèmes, services logiciels et toutes les ressources physiques ou virtuelles associées destinées à soutenir un objectif d'une attaque et qui sont liées à cet indicateur.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes qui sont liées à cet indicateur.
Emplacements	Répertorie les emplacements géographiques associés à l'objet.
Programme malveillant	Répertorie les enregistrements sources de programmes malveillants associés à cet indicateur.
Définitions de marquage	Répertorie les définitions de marquage associées à cet objet.
Analyse de programme malveillant	Répertorie les métadonnées et les résultats d'une analyse statique ou dynamique particulière effectuée sur une instance de programme malveillant associée à cet indicateur.
Observables	Répertorie les enregistrements observables associés à cet indicateur.
Données observées	Répertorie les données observées qui sont des entités liées à la cybersécurité telles que des fichiers, des systèmes et des réseaux et associées à cet indicateur.
Perceptions	Répertorie les enregistrements sources de perception associés à cet objet.
Acteurs de menace	Répertorie les changements associés à l'observable.
Événements de menace	Répertorie l'événement ou la situation susceptible d'entraîner des conséquences ou un impact indésirables associés à l'indicateur.
Regroupements des menaces	Répertorie les regroupements de menaces en tant qu'objets ayant un contexte commun.
Notes de menace	Répertorie les notes sur les menaces qui transmettent des informations pour fournir un contexte ou une analyse supplémentaire associés à l'indicateur.
Opinions sur la menace	Répertorie les opinions sur une menace comme une évaluation de l'exactitude des informations associées à l'indicateur.
Rapports de menace	Répertorie les rapports de menace associés à cet indicateur.
Outils	Répertorie l'outil associé à cet objet.
Vulnérabilités	Si l'observable est une adresse IP, cette liste affiche toutes les ressources (éléments de configuration) qui ont une adresse IP correspondante.
Tickets connexes	Répertorie les tickets connexes associés à cet indicateur.
Tâches du ticket connexe	Répertorie les tâches de ticket connexes associées à cet indicateur.
Canevas liés	Répertorie les canevas associés à cet indicateur.
Références d'indicateurs	Liste des références externes qui décrivent cet indicateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. En outre, dans la section **Enregistrements connexes** , vous pouvez confirmer les relations entre deux observables à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire **Indicateurs** . Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
3. Vous pouvez ajouter des indicateurs aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Schémas d'attaque

Les schémas d'attaque sont un type de tactiques, de techniques et de procédures (TTP) qui décrivent les méthodes par lesquelles les adversaires tentent de compromettre les cibles.

Les schémas d'attaque sont utilisés pour faciliter la catégorisation des attaques. Ils généralisent des attaques spécifiques aux modèles qu'ils suivent et fournissent des informations détaillées sur la façon dont les attaques sont effectuées.

Par exemple, le spear phishing est un type d'attaque courant où un attaquant envoie un e-mail soigneusement conçu à une partie dans le but de l'amener à cliquer sur un lien ou à ouvrir une pièce jointe pour diffuser un logiciel malveillant. Les schémas d'attaque sont plus spécifiques, tels que le spear phishing par un acteur de menace particulier (par exemple, le fait que la cible ait gagné un concours) peuvent également être un modèle d'attaque.

Définir un modèle d'attaque

Définissez un modèle d'attaque pour aider les analystes de menaces à classer les attaques.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Allez dans Modèle **d'attaque**.
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails du modèle d'attaque

Champ	Description
ID	ID unique d'un modèle d'attaque.
Nom	Entrez un nom pour ce modèle d'attaque.
Description	Saisissez une description pour un modèle d'attaque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Alias	Noms alternatifs pour identifier ce modèle d'attaque. **Remarque :** Pour ajouter un nouvel alias qui n'existe pas dans l'application, cliquez sur l'icône **Ajouter de nouveaux alias** disponible dans le champ Alias lui-même.
Phase d'attaque	Représente la phase d'attaque dans une chaîne de frappe telle que LM, MITRE ATT&CK.
Autorisations requises	Sélectionnez les autorisations requises pour ce modèle d'attaque.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour ce mode de modèle d'attaque. La propriété de confiance identifie la confiance que le créateur a dans l'exactitude de ses données. La valeur de confiance DOIT être un nombre compris entre 0 et 100.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Empêcher les mises à jour système	Si vous définissez ce marqueur sur vrai, le système ne remplace pas les valeurs des champs de l'enregistrement.

Important : Après avoir créé un nouvel enregistrement d'objet, la case **Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour un modèle d'attaque.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet, modèle d'attaque. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Créées	Spécifie l'heure à laquelle l'enregistrement est créé dans le système.
Mis à jour	Spécifie l'heure à laquelle l'enregistrement est modifié dans le système.
Extensions	Indique les extensions du modèle d'attaque.
État du traitement	Représente l'état de traitement de cet objet, modèle d'attaque.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à un observable.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à un modèle d'attaque.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à un modèle d'attaque.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au modèle d'attaque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Campagne

La campagne est définie comme un regroupement de comportements antagonistes qui décrit un ensemble d'activités malveillantes ou d'attaques, parfois appelées vagues, qui se produisent sur une période de temps contre un ensemble spécifique de cibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir la campagne

Définissez une campagne pour regrouper les comportements antagonistes.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **l'objet de la campagne** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue de campagne

Champ	Description
ID	ID unique d'un comportement contradictoire.
Nom	Saisissez un nom pour un comportement contradictoire.
Description	Saisissez une description pour cette campagne.
Objectif	Le but principal, l'objectif, le résultat souhaité ou l'effet recherché de la campagne. Ce que l'acteur de la menace ou l'ensemble de l'intrusion espère accomplir avec cette campagne.
Alias	Noms alternatifs à identifier pour cette campagne. **Remarque :** Pour ajouter un nouvel alias qui n'existe pas dans l'application, cliquez sur l'icône **Ajouter de nouveaux alias** disponible dans le champ Alias lui-même.
TLP	Le protocole TLP (Traffic Light Protocol) indique les informations sensibles partagées avec la bonne audience. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité pour ce modèle d'attaque.
Fiabilité	Entrez la confiance pour cette campagne.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour une campagne.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cette campagne.
Premier observé	Heure à laquelle cet objet a été vu pour la première fois en train d'exécuter un comportement contradictoire.
Dernier observé	Heure à laquelle cet objet a été vu pour la dernière fois en train d'effectuer un comportement contradictoire.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Créées	Spécifie la date et l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
État du traitement	Représente l'état de traitement de cet objet, de cette campagne.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner des balises	Sélectionnez les tags associés à une campagne.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à une campagne.
Ajouter valeurs de taxonomie	Ajouter des valeurs de taxonomie associées à la campagne.

Que faire ensuite

Vous pouvez maintenant cliquer sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la campagne.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensemble d'intrusions	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Mesures à prendre

Les plans d'action sont une action prise soit pour empêcher une attaque, soit pour répondre à une attaque en cours.

Les plans d'action décrivent des réponses techniques ou automatisées telles que l'application de correctifs, la reconfiguration des pare-feu. Il peut également décrire des actions de niveau supérieur telles que la formation des employés ou des changements de politique.

Par exemple, les plans d'action pour atténuer une vulnérabilité peuvent décrire l'application du correctif qui la corrige.

Définir des plans d'action

Définissez des plans d'action pour prévenir une attaque ou pour répondre à une attaque en cours.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Allez à **l'objet Plans d'action** .
4. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails des plans d'action

Champ	Description
ID	ID unique de plans d'action pour prévenir une attaque.
Nom	Entrez un nom descriptif pour ces lignes de conduite.
Description	Une description qui fournit plus de détails et de contexte sur les plans d'action, y compris potentiellement son objectif et ses principales caractéristiques.
Action	Pour capturer des plans d'action structurés ou automatisés.
TLP	Le protocole TLP (Traffic Light Protocol) indique les informations sensibles partagées avec la bonne audience. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité pour ce modèle d'attaque.
Fiabilité	Entrez la confiance pour ces lignes de conduite.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour des plans d'action.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, les plans d'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à un observable.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à un modèle d'attaque.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à un modèle d'attaque.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux plans d'action.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Identité

Les identités représentent des individus, des organisations ou des groupes réels, ainsi que des classes d'individus, de systèmes ou de groupes. Les identités s'appliquent pour STIX 2.x.

Un SDO d'identité peut capturer des informations d'identification de base, des informations de contact et les secteurs auxquels l'identité appartient. L'identité représente les cibles des attaques, les sources d'information, les créateurs d'objets et les identités des acteurs de la menace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir les identités

Définissez des identités qui représentent des individus, des organisations ou des groupes réels.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **l'objet d'identité** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails de l'identité

Champ	Description
ID	ID unique d'une identité.
Nom	Entrez un nom descriptif pour cette identité. Lorsqu'il s'agit d'une entité spécifique (un individu ou une organisation), cette propriété doit contenir le nom canonique de l'entité spécifique.
Description	Une description qui fournit plus de détails et de contexte sur le plan d'action, y compris potentiellement son objectif et ses principales caractéristiques.
Rôles	La liste des rôles que cette identité remplit.
Classe d'identité	Type d'entité que cette identité décrit. Par exemple, une personne ou une organisation.
Secteurs	La liste des secteurs industriels auxquels appartient cette identité.
Informations de contact	Les informations de contact telles que l'adresse e-mail et le numéro de téléphone pour cette identité.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez le score de confiance pour cette identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour l'identité.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire associé à cette identité.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'identité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à l'identité.
Ajouter valeurs de taxonomie	Ajouter des valeurs de taxonomie associées à l'identité.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'identité.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, les groupes ou les organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Infrastructure

Le SDO Infrastructure représente un type de tactiques, de techniques et de procédures (TTP). Ils décrivent tous les systèmes, services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'attaque. L'infrastructure s'applique à STIX 2.x.

Les éléments d'une attaque sont représentés par d'autres SDO ou SCO. Toutefois, le SDO d'infrastructure représente un groupe nommé de données qui constitue l'infrastructure.

Parmi les exemples d'infrastructure, citons les serveurs C2 utilisés dans une attaque, un appareil ou un serveur faisant partie d'une défense, ou les serveurs de base de données ciblés par une attaque.

Définir l'infrastructure

Définissez une infrastructure, c'est-à-dire tous les systèmes, services logiciels et toutes les ressources physiques ou virtuelles associées destinés à soutenir un objectif d'attaque.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **Infrastructure** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue des détails de l'infrastructure

Champ	Description
ID	ID unique d'un plan d'action visant à prévenir une attaque.
Nom	Entrez un nom descriptif pour cette ligne de conduite. Lorsqu'il s'agit d'une entité spécifique (un individu ou une organisation), cette propriété doit contenir le nom canonique de l'entité spécifique.
Description	Description qui fournit plus de détails et de contexte sur l'infrastructure, y compris potentiellement son objectif, la façon dont elle est utilisée, son lien avec d'autres activités de renseignement saisies dans des objets connexes et ses principales caractéristiques.
Types d'infrastructure	Décrit la catégorisation de l'infrastructure.
Alias	Noms alternatifs pour identifier cette infrastructure. **Remarque :** Pour ajouter un nouvel alias qui n'existe pas dans l'application, cliquez sur l'icône **Ajouter de nouveaux alias** disponible dans le champ Alias lui-même.
Phases d'attaque	Représente la phase d'attaque dans une chaîne de frappe telle que LM, MITRE ATT&CK.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Premier observé	Moment auquel cette infrastructure a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette infrastructure a été vue pour la dernière fois en train d'effectuer des activités malveillantes.
Fiabilité	Entrez la confiance pour ce plan d'action.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour cette infrastructure.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cette infrastructure.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Mis à jour	Spécifie l'heure à laquelle l'enregistrement est modifié dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner des balises	Sélectionnez les balises associées à l'infrastructure.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette infrastructure.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette infrastructure.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'identité.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Ensemble d'intrusions

Un ensemble d'intrusions est un ensemble groupé de comportements et de ressources antagonistes ayant des propriétés communes. Un ensemble d'intrusions implique généralement une seule organisation. L'ensemble d'intrusions s'applique à STIX 2.x.

Un ensemble d'intrusions peut capturer plusieurs campagnes ou d'autres activités. Ces activités ont en commun des attributs indiquant un auteur de menace connu ou inconnu.

Une nouvelle activité peut être attribuée à un ensemble d'intrusions, même si les acteurs de la menace à l'origine de l'attaque ne sont pas connus. Les acteurs de la menace peuvent passer d'un ensemble d'intrusion à un autre, ou ils peuvent prendre en charge plusieurs ensembles d'intrusion.

Un ensemble d'intrusion est l'ensemble de l'attaque et peut être utilisé sur une longue période dans plusieurs campagnes pour atteindre des objectifs potentiellement multiples.

Définir un ensemble d'intrusions

Définissez un ensemble d'intrusions, c'est-à-dire un ensemble groupé de comportements et de ressources adverses ayant des propriétés communes.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **l'ensemble d'intrusions**.
4. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails de l'ensemble d'intrusions

Champ	Description
ID	ID unique d'un ensemble d'intrusions.
Nom	Saisissez un nom descriptif pour cet ensemble d'intrusions. Lorsqu'il s'agit d'une entité spécifique (un individu ou une organisation), cette propriété doit contenir le nom canonique de l'entité spécifique.
Description	Une description qui fournit plus de détails et de contexte sur l'ensemble d'intrusion, y compris potentiellement son objectif et ses principales caractéristiques.
Alias	Noms alternatifs pour identifier cet ensemble d'intrusion. **Remarque :** Pour ajouter un nouvel alias qui n'existe pas dans l'application, cliquez sur l'icône **Ajouter de nouveaux alias** disponible dans le champ Alias lui-même.
Objectifs	Les objectifs de haut niveau de cet ensemble d'intrusion, à savoir, ce qu'ils essaient de faire. Par exemple, ils peuvent être motivés par un gain personnel, mais leur objectif est de voler des numéros de carte de crédit. Pour ce faire, ils peuvent exécuter des campagnes spécifiques qui ont des objectifs détaillés, comme compromettre les systèmes de point de vente d'un grand détaillant.
Premier observé	Heure à laquelle cet ensemble d'intrusion a été vu pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cet ensemble d'intrusion a été vu pour la dernière fois en train d'effectuer des activités malveillantes.
Motivation principale	Raison principale, motivation ou but derrière cet ensemble d'intrusion. La motivation est la raison

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	pour laquelle l'ensemble d'intrusion souhaite atteindre l'objectif (ce qu'il essaie d'atteindre).
Motivations secondaires	Les raisons, motivations ou objectifs secondaires derrière cet ensemble d'intrusion. Ces motivations peuvent exister en tant que cause égale ou presque égale à la motivation principale. Cependant, cela ne remplace pas ou n'amplifie pas nécessairement la motivation principale, mais cela peut indiquer un contexte supplémentaire. La position dans la liste n'a aucune signification.
Niveau de ressource	Cette propriété spécifie le niveau organisationnel auquel cet ensemble d'intrusions fonctionne généralement, qui à son tour détermine les ressources disponibles pour une utilisation dans une attaque.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez le score de confiance pour cet ensemble d'intrusion.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet ensemble d'intrusions.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet ensemble d'intrusions.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Mis à jour	Spécifie l'heure à laquelle l'enregistrement est modifié dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'ensemble d'intrusion.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cet ensemble d'intrusions.
Ajouter valeurs de taxonomie	Ajouter les valeurs de taxonomie associées à cet ensemble d'intrusion.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'ensemble d'intrusions.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
	est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Emplacement

Un emplacement représente un emplacement géographique. Les emplacements sont principalement utilisés pour donner un contexte à d'autres organismes de statistique. Les emplacements s'appliquent à STIX 2.x.

L'emplacement peut contenir tout ou partie des éléments suivants : région (Amérique du Nord), adresse municipale (New York, États-Unis), latitude et longitude.

Le SDO d'emplacement peut se rapporter à un ensemble d'identité ou d'intrusion pour indiquer que l'identité ou l'ensemble d'intrusion se trouve à cet emplacement. Il peut également se rapporter à un logiciel malveillant ou à un modèle d'attaque pour indiquer que la victime cible se trouve à un endroit particulier.

Par exemple, un emplacement pourrait être utilisé dans une relation pour décrire que l'ensemble d'intrusion de l'hirondelle bourgeoise provient d'Europe de l'Est.

Au moins une des propriétés ou jeux de propriétés suivants doit être fourni :

- region
- pays
- Latitude et longitude

Définir l'emplacement

Définissez un emplacement géographique pour fournir plus de contexte aux autres SDO.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **Emplacement** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Renseignez les champs du formulaire

Vue des détails de l'identité

Champ	Description
ID	ID unique pour l'emplacement.
Nom	Entrez un nom descriptif pour identifier l'emplacement.
Description	Une description qui fournit plus de détails et de contexte sur l'ensemble d'intrusion, y compris potentiellement son objectif et ses principales caractéristiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Latitude	Latitude de l'emplacement en degrés décimaux. Les nombres positifs décrivent les latitudes au nord de l'équateur et les nombres négatifs décrivent les latitudes au sud de l'équateur. La valeur de cette propriété doit être comprise entre -90,0 et 90,0 respectivement.
Longitude	Longitude de l'emplacement en degrés décimaux. Les nombres positifs décrivent les longitudes à l'est du méridien d'origine et les nombres négatifs décrivent les longitudes à l'ouest du méridien d'origine. La valeur de cette propriété doit être comprise entre -180,0 et 180,0 inclus.
Précision	Définit la précision des coordonnées spécifiées par les propriétés de latitude et de longitude. Ceci est mesuré en mètres. L'emplacement réel peut être n'importe où jusqu'à des mètres de précision du point défini. Si cette propriété n'est pas présente, la précision n'est pas spécifiée. Si cette propriété est présente, les propriétés de latitude et de longitude doivent être présentes.
Région	Région dans laquelle se trouve cet emplacement.
Pays	Pays dans lequel se trouve cet emplacement.
Zone administrative	État, province ou autre zone administrative infranationale dans lequel se trouve cet emplacement.
Ville	Ville dans laquelle se trouve cet emplacement.
Adresse (rue)	Adresse postale décrite par cet emplacement. Cette propriété comprend tous les aspects ou parties de l'adresse postale.
Code postal	Code postal dans lequel se trouve cet emplacement.
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour cet emplacement.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet emplacement.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions pour cet emplacement.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Mis à jour	Spécifie l'heure à laquelle l'enregistrement est modifié dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'emplacement.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cet emplacement.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cet emplacement.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'emplacement.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Programme malveillant

Un logiciel malveillant est un type de TTP qui représente un code malveillant. Il s'agit d'un programme qui est secrètement inséré dans un système. Les programmes malveillants s'appliquent à STIX 2.x.

L'intention d'un logiciel malveillant est de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation (OS) de la victime.

L'ODD de programme malveillant caractérise, identifie et catégorise les instances et les familles de programmes malveillants à partir des données dérivées de l'analyse. Cette SDO capture des informations détaillées sur le fonctionnement du logiciel malveillant et ce qu'il fait.

Définir un programme malveillant

Définissez un programme malveillant qui représente un code malveillant.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **l'objet Renseignements** sur les menaces de programme malveillant.
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue des détails de Malware

Champ	Description
ID	ID unique permettant d'identifier l'instance de programme malveillant.
Nom	Saisissez un nom pour identifier l'instance ou la famille de programme malveillant, tel que spécifié par le créateur du SDO. Pour une famille de logiciels malveillants, le nom doit être défini.
Description	Description qui fournit plus de détails et de contexte sur l'instance ou la famille de programme malveillant, y compris potentiellement son objectif et ses principales caractéristiques.
Types de programmes malveillants	Indique les différentes catégories de programmes malveillants.
Est la famille	Cochez cette case pour spécifier si l'objet représente une famille de programmes malveillants ou une instance de programme malveillant.
Alias	Noms alternatifs utilisés pour identifier ce programme malveillant ou cette famille de programmes malveillants. **Remarque :** Pour ajouter un nouvel alias qui n'existe pas dans l'application, cliquez sur l'icône **Ajouter de nouveaux alias** disponible dans le champ Alias lui-même.
Phases d'attaque	Représente la phase d'attaque dans une chaîne de frappe telle que LM, MITRE ATT&CK.
Premier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour la première fois en train d'effectuer des activités malveillantes.
Dernier observé	Heure à laquelle cette instance ou famille de programme malveillant a été vue pour la dernière fois en train d'effectuer des activités malveillantes
Architectures de processus	Indique les architectures de processus pour ce programme malveillant.
Langues d'implémentation	Indique les langues d'implémentation de ce programme malveillant.
Options de logiciel malveillant	Les options qui peuvent être présentées par une instance ou une famille de programmes malveillants.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez le score de confiance pour ce programme malveillant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour l'enregistrement de programme malveillant.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet enregistrement de programme malveillant.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, programme malveillant.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au programme malveillant.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée au programme malveillant.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées au programme malveillant.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au programme malveillant.

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Détections et atténuations	Répertorie les détections et les mesures d'atténuation associées à ce programme malveillant.
Identités	Liste des identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis connexes (IoC) qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Analyse de programme malveillant	Répertorie les enregistrements d'analyse de programme malveillant associés à cet objet.
Programme malveillant	Répertorie les enregistrements de programmes malveillants associés à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Analyse de programme malveillant

L'analyse des programmes malveillants capture les métadonnées et les résultats d'un programme malveillant. L'analyse des programmes malveillants s'applique à STIX 2.x.

L'analyse de programme malveillant comprend une analyse statique ou dynamique effectuée sur une instance ou une famille de programme malveillant.

Définir l'analyse de programme malveillant

Définissez une analyse de programme malveillant qui capture les métadonnées et les résultats d'une analyse statique ou dynamique particulière effectuée sur une instance ou une famille de programme malveillant.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **Analyse de programme malveillant** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails de l'analyse de programme malveillant

Champ	Description
ID	ID unique permettant d'identifier l'analyse de programme malveillant.
Produit	Nom du moteur d'analyse ou du produit utilisé. Les noms de produits DEVRAIENT être tous en minuscules avec des mots séparés par un tiret « -« . Dans les cas où le nom d'un produit ne peut pas être spécifié, une valeur d'anonymisé doit être utilisée.
Version	Version du produit d'analyse utilisée pour effectuer l'analyse.
Ordinateur virtuel hôte	Description de l'environnement de machine virtuelle utilisé pour héberger le système d'exploitation invité, le cas échéant, qui a été utilisé pour l'analyse dynamique de l'instance ou de la famille de programme malveillant. Si cette valeur n'est pas incluse en conjonction avec la propriété operating_system_ref, cela signifie que l'analyse dynamique peut avoir été effectuée sur du matériel nu (c'est-à-dire sans virtualisation) ou que les informations ont été rédigées. La valeur de cette propriété DOIT être l'identificateur d'un objet logiciel SCO.
Système d'exploitation	Système d'exploitation utilisé pour l'analyse dynamique de l'instance ou de la famille de programmes malveillants. Cela s'applique aussi bien aux systèmes d'exploitation virtualisés qu'à ceux fonctionnant sur du matériel nu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété DOIT être l'identificateur d'un objet logiciel SCO.
Version de configuration	Noms alternatifs utilisés pour identifier ce programme malveillant ou cette famille de programmes malveillants.
Modules	Modules d'analyse spécifiques qui ont été utilisés et configurés dans le produit au cours de cette exécution d'analyse.
Version du moteur d'analyse	Version du moteur d'analyse ou du produit (y compris les moteurs VA) utilisé pour effectuer l'analyse.
Version de la définition de l'analyse	Version des définitions d'analyse utilisée par l'outil d'analyse, y compris les outils VA.
Analyse démarrée	Date et heure de lancement de l'analyse de programme malveillant.
Analyse terminée	Date et heure auxquelles l'analyse de programme malveillant a été terminée.
Résultat	Résultat de classification tel que déterminé par le processus d'analyse du scanner ou de l'outil.
Nom des résultats	Résultat de classification ou nom attribué à l'instance de programme malveillant par l'outil de scanner.
Soumis	Date et heure auxquelles le programme malveillant a été soumis pour la première fois pour analyse ou analyse. Cette valeur restera constante alors que la date d'analyse peut changer. Par exemple, lorsqu'un programme malveillant a été soumis à un outil d'analyse de virus.
Observable analysé	Sélectionnez l'observable qui a été analysé.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez le score de confiance pour cette analyse de programme malveillant.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour l'enregistrement de famille de programmes malveillants.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet enregistrement de programme malveillant.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet, programme malveillant.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au programme malveillant.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée au programme malveillant.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées au programme malveillant.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au programme malveillant.

Enregistrements associés

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Programme malveillant	Répertorie les enregistrements de programmes malveillants associés à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Perception d'objets

Les observations indiquent qu'un objet a été vu. Les objets peuvent être un logiciel malveillant, un outil, un acteur de menace, etc.

Les observations permettent de suivre qui et quelle est la cible, comment les attaques sont menées et de suivre les tendances du comportement d'attaque.

L'objet de relation Perception contient des propriétés supplémentaires qui ne sont pas présentes dans les objets de relation génériques. Ces propriétés supplémentaires représentent des données spécifiques aux relations de perception.

Définir la perception d'objets

Définissez la perception d'objets qui indique qu'un objet (programme malveillant, outil, acteur malveillant, entre autres) a été vu.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **Objet de perception d'objets** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Choisir l'entité et la valeur

Champ	Description
Entité	Sélectionnez l'enregistrement de perception d'objets d'entité. **Remarque :** Lors de la création de tout nouvel enregistrement de perception d'objets, un enregistrement de relation associé est requis pour l'agrégation.
Perception de	Indique qu'une entité ou un indicateur particulier a été observé dans un environnement ce qui peut indiquer une menace potentielle. **Remarque :** Sélectionnez l'enregistrement connexe de perception associé à l'objet sélectionné dans le champ Entité afin que les enregistrements connexes puissent maintenant être créés et regrouper les enregistrements de perception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue des détails de la perception d'objets

Champ	Description
ID	ID unique d'un plan d'action visant à prévenir une attaque.
Description	Une description qui fournit plus de détails et de contexte sur l'observation.
Premier observé	Début de la fenêtre de temps au cours de laquelle l'ODS a fait référence à la propriété a été observée.
Dernier observé	Fin de la fenêtre de temps pendant laquelle le SDO référencé par laquelle la propriété a été observée.
Nombre	S'il est présent, il doit s'agir d'un nombre entier compris entre 0 et 999 999 999 inclus et représente le nombre de fois où le SDO référencé par lequel la propriété a été observée.
Est une synthèse	Indique si l'observation doit être considérée comme des données récapitulatives. Les données récapitulatives sont une agrégation des rapports d'observations précédents et ne doivent pas être considérées comme des données de source primaire.
Est interne	Indique si l'observation est interne.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour ce plan d'action.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet ensemble d'intrusions.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'identité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette infrastructure.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette infrastructure.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'observation d'objets.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Objets	Répertorie les objets associés aux observations.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Données observées

Les données observées transmettent des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX. Les données observées s'appliquent à STIX 2.x.

Les données observées capturent à la fois une observation unique d'une seule entité (fichier, connexion réseau) et l'agrégation de plusieurs observations d'une entité.

Vous pouvez utiliser des données observées seules (sans relations) pour transmettre des données brutes collectées à partir de n'importe quelle source. Les sources comprennent des rapports d'analystes, des bacs à sable et des outils de détection basés sur le réseau et l'hôte.

Par exemple, les données observées peuvent capturer des informations sur une adresse IP, une connexion réseau, un fichier ou une clé de registre. Les données observées ne sont pas une affirmation de renseignement, ce sont simplement des informations brutes sans aucun contexte pour ce qu'elles signifient.

Définir les données observées

Transmet des informations sur les entités liées à la cybersécurité telles que les fichiers, les systèmes et les réseaux à l'aide des objets cyber-observables (SCO) STIX.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Allez à l'objet **de données observées** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails des données observées

Champ	Description
ID	ID unique permettant d'identifier les données observées.
Premier observé	Première fois où les données ont été vues.
Derniers observés	La dernière fois que les données ont été vues.
Nombre observé	Nombre de fois où chaque objet cyber-observable a été vu. La valeur doit être un nombre entier compris entre 1 et 999 999 999.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrer la confiance pour les données observées
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour ces données observées.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ces données observées.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées aux données observées.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ces données observées.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à ces données observées.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux données observées.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
	est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Acteur de menace

Les auteurs de menace sont des personnes, des groupes ou des organisations qui agissent avec des intentions malveillantes. Les acteurs de la menace s'appliquent à STIX 2.x.

Un acteur de menace n'est pas un ensemble d'intrusion, mais peut soutenir ou être affilié à divers ensembles d'intrusion, groupes ou organisations au fil du temps.

Les acteurs de la menace utilisent leurs ressources, et les ressources d'un ensemble d'intrusions, pour mener des attaques et mener des campagnes contre des cibles.

Vous pouvez identifier les acteurs de menace par leurs motivations, leurs capacités, leurs objectifs, leur niveau de sophistication, leurs activités passées, les ressources auxquelles ils ont accès et leur rôle dans l'organisation.

Définir l'acteur de menace

Définissez les acteurs de menace qui sont des individus, des groupes ou des organisations qui agissent avec des intentions malveillantes.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **Acteur de menace** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails de l'acteur de menace

Champ	Description
ID	ID unique d'un plan d'action visant à prévenir une attaque.
Nom	Entrez un nom descriptif pour identifier l'emplacement.
Description	Une description qui fournit plus de détails et de contexte sur l'ensemble d'intrusion, y compris potentiellement son objectif et ses principales caractéristiques.
Alias	Une liste d'autres noms pour identifier cet acteur de menace. **Remarque :** Pour ajouter un nouvel alias qui n'existe pas dans l'application, cliquez sur l'icône **Ajouter de nouveaux alias** disponible dans le champ Alias lui-même.
Objectifs	Les objectifs de haut niveau de cet acteur de la menace, à savoir ce qu'il essaie de faire. Par exemple, ils peuvent être motivés par un gain personnel, mais leur objectif est de voler des numéros de carte de crédit.
Types d'acteurs de menace	Type(s) de cet acteur de menace.
Rôles d'acteur de menace	Les différents rôles d'acteur de menace pour cet objet.
Premier observé	L'heure à laquelle cet acteur de menace a été vu pour la première fois. Cette propriété est une propriété récapitulative des données provenant de perceptions et d'autres données qui peuvent ou non être disponibles dans STIX. Si de nouvelles observations sont reçues avant le premier horodatage vu,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	l'objet peut être mis à jour pour prendre en compte les nouvelles données.
Dernier observé	Heure à laquelle cet acteur de menace a été vu pour la dernière fois.
Motivation principale	La raison, la motivation ou le but principal derrière cet acteur de menace. La motivation est la raison pour laquelle l'acteur de la menace souhaite atteindre l'objectif (ce qu'il essaie d'atteindre). Par exemple, un acteur de la menace ayant pour objectif de perturber le secteur financier d'un pays peut être motivé par une haine idéologique du capitalisme.
Sophistication	Compétence, connaissances spécifiques, formation spéciale ou expertise qu'un acteur malveillant doit posséder pour exécuter l'attaque.
Motivations secondaires	Cette propriété spécifie les raisons, les motivations ou les objectifs secondaires de cet acteur de menace. Ces motivations peuvent exister en tant que cause égale ou presque égale à la motivation principale. Cependant, cela ne remplace pas ou n'amplifie pas nécessairement la motivation principale, mais cela peut indiquer un contexte supplémentaire. La position dans la liste n'a aucune signification.
Niveau de ressource	Niveau organisationnel auquel cet acteur de menace travaille généralement, qui à son tour détermine les ressources dont il dispose pour une utilisation dans une attaque. Cet attribut est lié à la propriété de sophistication : un niveau de ressource spécifique implique que l'acteur malveillant a accès à au moins un niveau de sophistication spécifique.
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet acteur de menace.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner des balises	Sélectionnez les balises associées à l'auteur de la menace.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cet acteur de menace.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cet acteur de menace.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'auteur de la menace.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque qui permettent de catégoriser les attaques associées à cet objet.
Campagnes	Répertorie les campagnes associées à cet objet.
Identités	Liste des identités associées à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Liste des emplacements associés à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Événement de menace

Événement ou situation susceptible d'avoir des conséquences ou un impact indésirables.

Un pirate attaquant un site Web est un événement menaçant. Si les pirates parviennent à endommager un site Web ou à voler des informations, cela serait défini comme un événement de menace.

Définir l'événement de menace

Définissez un événement de menace lorsqu'il s'agit d'un événement qui entraîne l'accès non autorisé à des informations non publiques et leur acquisition, ou la perturbation ou l'utilisation abusive d'un système d'information.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **l'objet de l'événement de menace** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails de l'acteur de menace

Champ	Description
ID	ID unique d'un plan d'action visant à prévenir un événement de menace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Entrez un nom descriptif pour identifier l'événement de menace.
Description	Description qui fournit plus de détails et de contexte sur l'événement de menace, y compris potentiellement son objectif et ses principales caractéristiques.
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet acteur de menace.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'événement de menace.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cet événement de menace.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cet événement de menace.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'événement de menace.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Regroupement des menaces

Un objet Regroupement des menaces affirme explicitement que les objets STIX référencés ont un contexte commun. Le regroupement des menaces s'applique à STIX 2.x.

Un objet Regroupement des menaces représente un ensemble de données qui, avec une analyse suffisante, arrive à maturité pour transmettre un rapport d'incident ou de menace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

en tant qu'objet de rapport STIX. Par exemple, un regroupement peut être utilisé pour caractériser une enquête en cours sur un événement ou un incident de sécurité.

Un objet Regroupement des menaces peut également être utilisé pour déclarer que les objets STIX référencés sont liés à un processus d'analyse en cours. Par exemple, un analyste des menaces peut collaborer avec d'autres membres de sa communauté de confiance pour examiner une série de campagnes et d'indicateurs.

Le SDO Regroupement des menaces contient une liste de références aux SDO, aux SCO et aux OAR, ainsi qu'une déclaration explicite du contexte partagé par le contenu, une description textuelle et le nom du regroupement.

Définir le regroupement des menaces

Définissez les regroupements de menaces comme des objets qui ont un contexte commun.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **Regroupement de menaces** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails de regroupement de menaces

Champ	Description
ID	ID unique d'un plan d'action visant à empêcher la production d'une attaque de type Groupe de menaces.
Nom	Saisissez un nom descriptif pour identifier le groupe de menaces.
Description	Description qui fournit plus de détails et de contexte sur l'événement de menace, y compris potentiellement son objectif et ses principales caractéristiques.
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour ce regroupement de menaces.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au regroupement de menaces.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ce regroupement de menaces.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à ce regroupement de menaces.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au regroupement de menaces.

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Note de menace

Une note sur les menaces transmet un texte informatif pour fournir une analyse supplémentaire qui n'est pas contenue dans les objets STIX, les objets de définition de marquage ou les objets de contenu linguistique auxquels la note se rapporte. Les notes de menace s'appliquent à STIX 2.x.

Par exemple, un analyste peut ajouter une note à un objet Campagne créé par une autre organisation. La note peut indiquer qu'ils ont vu des messages liés à cette campagne sur un forum de pirates.

Les notes sont généralement créées par des analystes humains et sont composées de texte orienté vers l'homme, elles contiennent une propriété supplémentaire pour capturer l'auteur qui a créé la note.

Définir la note de menace

Définissez des notes sur les menaces qui transmettent des informations pour fournir un contexte ou une analyse supplémentaire qui n'est pas disponible dans les objets existants.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **la note de menace**.
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue Détails de la note de menace

Champ	Description
ID	ID unique d'une note de menace.
Abstrait	Spécifiez un bref résumé du contenu de la note.
Contenu	Spécifie le contenu de la note.
Auteurs	Spécifie le nom de l'auteur (par exemple, un analyste).
Fiabilité	Entrez la confiance pour ce plan d'action.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette note de menace.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au regroupement de menaces.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ce regroupement de menaces.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à ce regroupement de menaces.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la note de menace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Opinion sur la menace

Un avis est une évaluation de l'exactitude des informations contenues dans un objet STIX produit par une entité différente. Les opinions sur la menace s'appliquent à STIX 2.x.

La propriété opinion capture le niveau d'accord ou de désaccord à l'aide d'une échelle fixe. L'échelle fixe prend également en charge une cartographie numérique pour permettre des opérations statistiques cohérentes entre les opinions.

Par exemple, un analyste d'une organisation consommatrice peut dire qu'il est « fortement en désaccord » avec un objet de campagne et expliquer pourquoi.

Les opinions sont subjectives et le cahier des charges n'aborde pas la meilleure façon de les interpréter.

Les analystes humains créent des opinions et sont composés de texte orienté vers l'homme, ils contiennent une propriété supplémentaire pour capturer l'auteur qui a créé l'opinion.

Définir l'opinion sur la menace

Définissez les opinions sur une menace comme une évaluation de l'exactitude des informations contenues dans un objet STIX.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **d'opinion sur les menaces** .
4. Cliquez sur **Nouveau**.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Remplissez les champs du formulaire.

Vue détaillée de l'opinion sur la menace

Champ	Description
ID	ID unique d'une opinion sur une menace.
Avis	L'avis du producteur sur l'objet STIX.
Explication	Précise le contenu de l'avis.
Auteurs	Spécifie le nom de l'auteur (par exemple, un analyste).
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour ce plan d'action.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette opinion sur la menace.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cette opinion sur la menace.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Créées	Spécifie l'heure à laquelle l'enregistrement est créé dans la source.
Mis à jour	Spécifie l'heure à laquelle l'enregistrement est modifié dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à l'opinion sur une menace.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette opinion sur la menace.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à cette opinion sur la menace.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à l'opinion sur les menaces.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rapport de menace

Les rapports de menace sont des collections de renseignements sur les menaces axés sur une ou plusieurs rubriques. Les rapports de menace s'appliquent à STIX 2.x.

Les rapports de menace comprennent une description d'un auteur de menace, d'un programme malveillant, d'une technique d'attaque, y compris le contexte et des détails connexes. Ils sont utilisés pour regrouper les renseignements sur les menaces liés afin qu'ils puissent être publiés sous forme d'article complet sur les cybermenaces.

Le SDO Rapport de menace contient une liste de références aux objets STIX ainsi qu'une description textuelle et le nom du rapport.

Définir le rapport de menace

Définissez les rapports de menace décrivant un auteur de menace, un programme malveillant ou une technique d'attaque, y compris le contexte et les détails connexes.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **Rapport de menace** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails du rapport de menace

Champ	Description
ID	Spécifiez un nom pour identifier le rapport de menace.
Nom	Spécifiez un bref résumé du contenu de la note.
Description	Une description qui fournit des informations et un contexte supplémentaires sur le rapport.
Types de rapports	Spécifie le nom de l'auteur (par exemple, un analyste).
Publié	Date à laquelle ce rapport a été officiellement publié par l'auteur du rapport.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette note de menace.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce modèle d'attaque.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au regroupement de menaces.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ce regroupement de menaces.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à ce regroupement de menaces.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux rapports de menaces.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Regroupements des menaces	Répertorie les regroupements de menaces associés à cet objet.
Rapports de menace	Répertorie les rapports de menace associés à cet objet.
Outils	Répertorie les logiciels légitimes utilisés par les auteurs de menace pour effectuer des attaques associées à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Outil

Les outils sont des logiciels légitimes utilisés par les acteurs de la menace pour effectuer des attaques. Les outils s'appliquent à STIX 2.x.

Les outils vous permettent de savoir comment et quand les acteurs de la menace les utilisent pour exécuter des campagnes. Contrairement aux logiciels malveillants, ces outils ou progiciels se trouvent souvent sur un système et ont des objectifs légitimes pour les utilisateurs avancés, les administrateurs, les administrateurs réseau ou même les utilisateurs normaux.

Par exemple, les outils d'accès à distance (RDP) et les outils d'analyse réseau (Nmap) sont des outils qu'un acteur malveillant utilise lors d'une attaque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir les outils

Définissez les outils comme des logiciels légitimes utilisés pour effectuer des attaques.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **outil** .
4. Cliquez sur **Nouveau**.

> **Remarque :** Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails des outils

Champ	Description
ID	ID unique permettant d'identifier un outil.
Nom	Entrez un nom descriptif pour identifier l'outil.
Description	Une description qui fournit plus de détails et de contexte sur l'outil, y compris potentiellement son objectif et ses principales caractéristiques.
Types d'outil	Le ou les types d'outils décrits.
Alias	Un autre nom utilisé pour identifier cet outil. **Remarque :** Pour ajouter un nouvel alias qui n'existe pas dans l'application, cliquez sur l'icône **Ajouter de nouveaux alias** disponible dans le champ Alias lui-même.
Version de l'outil	L'identificateur de version associé à l'outil.
Phases d'attaque	Représente la phase d'attaque dans une chaîne de frappe telle que LM, MITRE ATT&CK.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cet outil.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cet outil.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées au regroupement de menaces.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à ce regroupement de menaces.
Ajouter valeurs de taxonomie	Ajoutez les valeurs de taxonomie associées à ce regroupement de menaces.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés aux outils.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Détections et atténuations	Répertorie les détections et les atténuations associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Vulnérabilité

Une vulnérabilité est une faiblesse ou un défaut d'un composant logiciel ou matériel exploité par des attaquants. Les vulnérabilités s'appliquent à STIX 2.x.

La faiblesse ou le défaut réside dans les exigences, les conceptions ou les implémentations du code trouvé dans un composant logiciel ou matériel. Cette faiblesse est directement exploitée pour avoir un impact négatif sur la confidentialité, l'intégrité ou la disponibilité de ce système.

CVE est une liste des vulnérabilités et des expositions en matière de sécurité de l'information qui fournit des noms communs pour les problèmes connus du public [CVE].

Par exemple, si un logiciel malveillant exploite CVE-2015-12345, un objet malveillant peut être lié à un objet de vulnérabilité faisant référence à CVE-2015-12345.

Définir la vulnérabilité

Définissez une vulnérabilité comme une faiblesse ou un défaut d'un composant logiciel ou matériel exploité par des attaquants.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **l'objet de vulnérabilité** .
4. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails des vulnérabilités

Champ	Description
ID	ID unique permettant d'identifier une vulnérabilité.
Nom	Nom utilisé pour identifier la vulnérabilité.
Description	Une description qui fournit plus de détails et de contexte sur la vulnérabilité, y compris potentiellement son objectif et ses principales caractéristiques.
Gravité	Indique le degré normalisé de gravité de cette vulnérabilité
CVSS3.0	Indique le CVSS v3 pour cette vulnérabilité.
CVSS2.0	Indique le CVSS v2 pour cette vulnérabilité.
État d'exploitation	Indique le statut de l'exploit associé à cette vulnérabilité
Publié	Indique quand la vulnérabilité est publiée.
Dernière modification de l'enregistrement	Indique quand l'enregistrement a été modifié pour la dernière fois.
Logiciel affecté	Répertorie les logiciels affectés associés à la vulnérabilité.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des notes supplémentaires pour cette vulnérabilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cette vulnérabilité.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à la vulnérabilité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette vulnérabilité.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à cette vulnérabilité.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la vulnérabilité.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Campagnes	Répertorie les campagnes associées à cet objet.
Détections et atténuations	Répertorie les détections et les atténuations associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Définitions marketing	Répertorie les définitions marketing associées à cet objet.
Perceptions	Répertorie les perceptions associées à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Vulnérabilités	Répertorie une faiblesse ou un défaut dans un logiciel ou un matériel exploité par des attaquants qui est associé à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Extraire les données de vulnérabilité

Récupérez les données relatives à la vulnérabilité telles que les éléments de configuration, les entrées vulnérables et le contexte métier.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **l'objet de vulnérabilité** .
   Les vulnérabilités connexes associées à cet objet s'affichent.
4. Sélectionnez l'enregistrement de vulnérabilité correspondant.
   Si des CVE lui sont associées, vous pouvez extraire automatiquement ses données associées vulnérables à l'aide du bouton fourni, et ces enregistrements associés sont affichés dans la section Contexte métier des vulnérabilités.
5. Accéder à **Intelligence interne** > **Entrées vulnérables**.
   Les enregistrements CVE associés s'affichent.
6. Sélectionnez n'importe quel CVE et cliquez sur **le bouton Extraire les données associées à la vulnérabilité** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Ce lien associera automatiquement les enregistrements et récupérera ce contexte professionnel particulier des enregistrements.
- Si aucun enregistrement n'est associé, un message d'information s'affiche indiquant que cet objet de vulnérabilité spécifique n'a aucune entrée vulnérable qui lui est associée. Vous devez associer manuellement le ou les objets aux entrées vulnérables pour extraire les données.
- Ce bouton déclenche une tâche planifiée en arrière-plan, et les détails de lancement et d'exécution de la tâche sont affichés dans la section **Flux d'activité** . Par exemple, lorsque la tâche est déclenchée, le flux d'activité affiche une activité dont la récupération des données associées avec les entrées vulnérables a commencé. Pour plus d'informations sur la façon dont les travaux planifiés sont exécutés pour extraire les données, voir Travaux planifiés .

7. Cliquez sur **Lien** pour lier manuellement les objets.
8. Sélectionnez les enregistrements à lier et extrayez les données associées à la vulnérabilité à l'aide du bouton **Extraire les données associées** à la vulnérabilité.
   Lorsque vous cliquez sur ce bouton, la tâche d'arrière-plan est déclenchée et les données sont automatiquement extraites dans leur section respective. Un message affiche que la tâche d'extraction des données associées aux entrées vulnérables a commencé. Vous pouvez suivre l'état dans le flux d'activité et actualiser la liste une fois la tâche terminée pour vérifier les résultats. Par exemple, si les données sont liées aux éléments de configuration, vous pouvez vérifier les résultats dans la section Éléments de configuration. Pour plus d'informations sur l'ajout de CVE, consultez Ajouter des CVE à des entrées tierces .

Remarque : De même, vous pouvez extraire les données des enregistrements des observables. Pour plus d'informations, consultez Extraire les données de vulnérabilité.

Définition de marquage

L'objet marking-definition représente un marquage spécifique. Les marquages de données représentent généralement les besoins de traitement ou de partage des données.

Définir la définition de marquage

Définissez des définitions de marquage pour gérer et partager les exigences relatives aux données.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à **l'objet de définition de marquage** .
4. Cliquez sur **Nouveau**.

Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue des détails de la source de la définition de marquage

Champ	Description
ID	ID unique permettant d'identifier une définition de marquage.
Nom	Nom utilisé pour identifier la définition de marquage.
Type de définition	La propriété type identifie le type d'objet. La propriété definition_type identifie le type de définition de marquage.
Définition	La propriété de définition contient l'objet de marquage lui-même, par exemple TLP.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Fiabilité	Entrez la confiance pour cet objet. La propriété de confiance identifie la confiance que le créateur a dans l'exactitude de ses données. La valeur de confiance DOIT être un nombre compris entre 0 et 100.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour cette définition de marquage.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cette définition de marquage.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à la vulnérabilité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette vulnérabilité.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à cette vulnérabilité.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la vulnérabilité.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.
Schémas d'attaque	Répertorie les schémas d'attaque associés à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrements connexes (suite)

Champ	Description
Campagnes	Répertorie les campagnes associées à cet objet.
Détections et atténuations	Répertorie les détections et les atténuations associées à cet objet.
Identités	Répertorie les identités associées à cet objet.
Indicateurs	Répertorie les indicateurs de compromis (IoC) connexes qui ont été identifiés par la source de menace associée à cet objet.
Infrastructure	Répertorie les systèmes, les services logiciels et toutes les ressources physiques ou virtuelles associées qui sont associées à cet objet.
Ensembles d'intrusion	Répertorie un ensemble de comportements et de ressources antagonistes ayant des propriétés communes associées à cet objet.
Emplacements	Répertorie les emplacements qui fournissent un contexte géographique à cet objet.
Programme malveillant	Répertorie le code malveillant associé à cet objet.
Analyse de programme malveillant	Répertorie l’analyse malveillante associée à cet objet.
Observables	Répertorie les observables associés à cet objet.
Données observées	Répertorie les données observées associées à cet objet.
Acteurs de menace	Répertorie les personnes, groupes ou organisations qui agissent avec une intention malveillante associée à cet objet.
Événements de menace	Répertorie les événements de menace associés à cet objet.
Regroupements des menaces	Répertorie les regroupements de menaces associés à cet objet.
Notes de menace	Répertorie les notes de menace associées à cet objet.
Opinions sur la menace	Répertorie les opinions sur la menace associées à cet objet.
Outils	Répertorie les outils associés à cet objet.
Vulnérabilités	Répertorie les vulnérabilités associées à cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Composant de données

Les composants de données sont utilisés pour identifier des propriétés ou des valeurs spécifiques d'une source de données.

Définir le composant de données

Définir un composant de données pour identifier les propriétés ou les valeurs d'une source de données

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **composant de données** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue Détails du composant de données

Champ	Description
ID	ID unique permettant d'identifier un composant de données.
Nom	Nom utilisé pour identifier le composant de données.
Description	Une description qui fournit plus de détails et de contexte sur la vulnérabilité, y compris potentiellement son objectif et ses principales caractéristiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source de données	Indique le degré normalisé de gravité de cette vulnérabilité
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Fiabilité	Indique la fiabilité pour cet objet. La confiance doit être comprise entre 0 et 100.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour ce composant de données.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce composant de données.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du composant de données.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

> **Important :** Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.
>
> Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à la vulnérabilité.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette vulnérabilité.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à cette vulnérabilité.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés au composant de données.

Enregistrements connexes

Champ	Description
Schémas d'attaque	Répertorie les schémas d'attaque associés à cet objet.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sources de données

Les sources de données représentent les différents sujets/sujets d'information qui peuvent être collectés par les capteurs/journaux. Les sources de données comprennent également des composants de données, qui identifient des propriétés/valeurs spécifiques d'une source de données.

Définir les sources de données

Définissez une source de données pour représenter les différents sujets ou rubriques d'informations.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **Sources de données** .
4. Cliquez sur **Nouveau**.

   Remarque : Chaque fois que vous créez de nouveaux enregistrements d'objets pour des observables, des indicateurs, des entités ou des objets, un enregistrement source est créé et un message d'invite s'affiche indiquant que le nouvel enregistrement d'objet est créé, puis l'utilisateur est redirigé vers l'enregistrement agrégé.

5. Remplissez les champs du formulaire.

Vue des détails des vulnérabilités

Champ	Description
ID	ID unique permettant d'identifier la source de données.
Nom	Nom utilisé pour identifier la source de données.
Description	Description qui fournit plus de détails et de contexte sur la source de données, y compris éventuellement son objectif et ses principales caractéristiques.
Couches de collecte	Indique la description de l'endroit où la source de données peut être physiquement collectée, comme l'hôte, le réseau, le plan de contrôle du cloud, et ainsi de suite.
Plateformes	Indique que le système dans lequel un adversaire opère peut être un système d'exploitation ou une application.
Contributeurs	Indique les contributeurs de cette source de données.
TLP	Le TLP est utilisé pour s'assurer que les informations sensibles sont partagées avec le public approprié. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour cette source de données.

Information supplémentaire

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour cette source de données.
Version de spéc.	Version de la spécification STIX utilisée pour représenter cet objet. La valeur de cette propriété doit être de 2,1 pour les objets STIX définis conformément à cette spécification.
Langue	Cette propriété identifie la langue du contenu textuel dans cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Extensions	Indique les extensions du modèle d'attaque.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
État du traitement	Représente l'état de traitement de cet objet et le déroulement de l'action.
Créées	Spécifie la date et l'heure auxquelles l'objet est créé dans la source.
Mis à jour	Spécifie la date et l'heure auxquelles l'objet a été mis à jour dans la source.
Créé par réf.	Cette propriété spécifie que l'objet d'identité qui décrit l'entité a créé cet objet.

6. Cliquez sur **Enregistrer**.
   Une fois que vous avez enregistré, un message d'invite s'affiche indiquant qu'un nouvel enregistrement d'observable est créé. Cliquez sur **Continuer** pour modifier l'enregistrement et créer de nouvelles relations.
7. Cliquez sur **Continuer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important : Après avoir créé un nouvel enregistrement d'observable, la case **à cocher Empêcher les mises à jour système** s'affiche.

Cochez cette case pour empêcher toute mise à jour du système après la création des enregistrements de l'observable, de l'indicateur ou des objets STIX.

Mots clés&Taxonomies

Champ	Description
Balises	
Sélectionner des balises	Sélectionnez les balises associées à la source de données.
Ajouter des balises	Ajouter de nouvelles balises.
Taxonomies	
Sélectionner taxonomie	Sélectionnez une taxonomie associée à cette source de données.
Ajouter valeurs de taxonomie	Ajoutez des valeurs de taxonomie associées à cette source de données.

Que faire ensuite

Cliquez sur l'une des listes connexes suivantes pour afficher des informations supplémentaires sur les objets associés à la source de données.

Enregistrements connexes

Champ	Description
Références externes	Répertorie les références externes qui font référence à des informations autres que STIX. Cette propriété est utilisée pour fournir un ou plusieurs identificateurs d'objets externes.

Remarque :

1. Vous pouvez lier et dissocier les enregistrements connexes associés à cet objet. Pour plus d'informations, consultez Lier les enregistrements connexes à Threat Intelligence.
2. Les différents SDO de la bibliothèque TI contiennent également les relations potentielles. Pour établir des relations entre deux objets, utilisez le lien **Relations éventuelles** de la **bibliothèque Renseignements** sur les menaces pour confirmer les relations entre les objets. Pour plus d'informations, consultez Confirmer les relations éventuelles objet-objet.
3. Utilisez également la section **Enregistrements connexes** de la vue de formulaire d'objets pour confirmer les relations entre deux objets à l'aide de la section **Relations éventuelles** disponible dans la vue de formulaire. Pour plus d'informations sur les rubriques . Confirmer les relations éventuelles à partir d'enregistrements connexes
4. Vous pouvez ajouter des objets aux tickets. Pour plus d'informations, consultez Ajouter au ticket.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir des flux RSS

Un flux de renseignements sur les menaces est un flux de données continu en temps réel qui rassemble des informations relatives aux cyberrisques ou aux cybermenaces. Les flux RSS offrent un moyen facile de rester à jour avec vos sites Web préférés, tels que les blogs ou les dernières nouvelles en matière de cybersécurité.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à l'objet **Flux RSS** .

   Remarque : Vous pouvez parcourir les flux ingérés à l'aide de cette section, mais vous ne pouvez pas créer de nouveaux enregistrements.

4. Sur le formulaire, les champs suivants sont renseignés automatiquement.

Vue des détails des flux RSS

Champ	Description
Titre	Titre du flux RSS.
Description	Une description qui fournit plus de détails et de contexte sur les flux RSS, y compris potentiellement son objectif et ses principales caractéristiques.
Lien	Indique le lien ajouté aux flux RSS.
Source	Spécifie la source du flux RSS à partir de laquelle cet enregistrement d'objet est créé.
Date de publication	Indique quand le flux RSS est publié.
Auteur	Indique l'auteur du flux RSS.

5. Cliquez sur **Enregistrer**.

Aperçus

Champ	Description
Notes	Ajoutez des remarques supplémentaires pour ce flux.

Information supplémentaire

Champ	Description
URL du média	Indique l'URL du média.
Commentaires de commentaires	Tout commentaire supplémentaire sur le commentaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Objets de relations

Utilisez les objets de relations pour lier deux observables ou un observable et SDO pour expliquer comment ils sont liés l'un à l'autre.

Les objets de relation STIX (SRO) représentent des types de relations entre divers objets STIX. Les objets de relation suivants sont disponibles :

- **Relation observable-observable** : cet objet définit les relations entre les observables.
- **Relation objet-objet** : cet objet définit les relations entre les SDO, à l'exception de l'objet indicateur. Un exemple de relation définie objet-objet est qu'un modèle d'attaque livre un logiciel malveillant.
- **Relation objet-observable** : cet objet définit les relations entre les SDO et l'objet observable (SCO). Un exemple de relation définie objet-observable est qu'une infrastructure se compose d'objets cyber-observables qui fournissent des informations sur une attaque potentielle.
- **Relation objet-indicateur** : cet objet définit les relations entre les SDO et l'objet indicateur.
- **Relations indicateur-indicateur** : cet objet définit les relations entre les objets d'indicateur.
- **Relation indicateur-observable** : cet objet définit les relations entre l'objet indicateur et d'autres SDO. Un exemple de relation définie objet-indicateur est qu'un indicateur détecte la preuve d'une campagne.

Relations d'objet

Objet de relation	Exemple de source	Exemple de cible	Exemple de description
Relations observable-observable	Adresse IP, nom de domaine		Cette relation décrit les observables.
Relations objet-objet	Modèle d'attaque	Programme malveillant	Cette relation décrit que ce modèle d'attaque est utilisé pour livrer cette instance (ou famille) de programme malveillant.
Relations objet-observable			Cette relation décrit les objets et les observables.
Relations objet-indicateur	Indicateur	Modèle d'attaque, Campagne, Infrastructure, Ensemble d'intrusion, Programme malveillant, Acteur de menace, Outil	Cette relation décrit que l'indicateur peut détecter des preuves du modèle d'attaque, de la campagne, de l'infrastructure, de l'ensemble d'intrusion, du programme malveillant, de l'acteur de menace ou de l'outil associés. Les preuves peuvent ne pas être directes. Par exemple, l'indicateur peut détecter des preuves secondaires de la campagne, telles que des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Relations d'objet (suite)

Objet de relation	Exemple de source	Exemple de cible	Exemple de description
			logiciels malveillants couramment utilisés par cette campagne particulière.
Indicateur : relations indicateur	Infrastructure	Données observées	Cette relation indique que l'indicateur est créé en fonction des informations provenant d'un objet de données observé. Un exemple de relation définie objet-observable est qu'une infrastructure se compose d'objets cyber-observables qui fournissent des informations sur une attaque potentielle.
Indicateur : observable			Cette relation décrit les entre les indicateurs et les observables.

Définir les relations observable-observable

Définissez les relations entre les observables.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Observable-Observable**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Observable source	Sélectionnez et définissez l'objet source.
Observable cible	Sélectionnez et définissez l'objet cible.
Type de relation	Description qui fournit plus de détails et de contexte sur le type de relation. Les options disponibles sont les suivantes : Définissez le sens de la relation, qu'il soit direct ou inverse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Inverse : il s'agit du type de relation entre l'observable et l'objet. ○ Direct : type de relation entre l'objet et l'observable.
Base de corrélation	Nom de la règle de corrélation sur la base de laquelle le système a identifié les enregistrements connexes de cet observable. Cette règle est renseignée automatiquement.

6. Cliquez sur **Envoyer**.

Définir les relations objet-objet

Définissez les relations entre les SDO, à l'exception de l'objet d'indicateur.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Objet-Objet**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Objet source	Sélectionnez et définissez l'objet source.
Type de l'objet source	Définit le type d'objet source.
Objet cible	Sélectionnez et définissez l'objet cible.
Type de l'objet cible	Définit le type d'objet cible.
Type de relation	Description qui fournit plus de détails et de contexte sur le type de relation. Définissez le sens de la relation, qu'il soit direct ou inverse. ○ Inverse : il s'agit du type de relation entre l'observable et l'objet. ○ Direct : type de relation entre l'objet et l'observable.
Heure de début	Spécifie l'heure à laquelle la relation est créée.
Heure de fin	Spécifie le moment où la relation est interrompue ou supprimée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Brève description des relations d'objet.

6. Cliquez sur **Envoyer**.

Définir les relations objet-observable

Définissez les relations entre les SDO et l'objet observable (SCO).

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Objet-Observable**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Observable	Sélectionnez et définissez l'observable.
Objet	Sélectionnez et définissez l'objet.
Type de relation	Description qui fournit plus de détails et de contexte sur le type de relation. Définissez le sens de la relation, qu'il soit direct ou inverse. ○ Inverse : il s'agit du type de relation entre l'observable et l'objet. ○ Direct : type de relation entre l'objet et l'observable.
Heure de début	Spécifie l'heure à laquelle la relation est créée.
Heure de fin	Spécifie le moment où la relation est interrompue ou supprimée.
Description	Brève description des relations d'objet.

6. Cliquez sur **Envoyer**.

Définir les relations objet-indicateur

Définissez les relations entre l'objet d'indicateur et d'autres SDO.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Objet-Indicateur**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Indicateur	Sélectionnez et définissez l'indicateur.
Objet	Sélectionnez et définissez l'objet.
Type de relation	Description qui fournit plus de détails et de contexte sur le type de relation. Définissez le sens de la relation, qu'il soit direct ou inverse. ○ Inverse : il s'agit du type de relation entre l'observable et l'objet. ○ Direct : type de relation entre l'objet et l'observable.
Heure de début	Spécifie l'heure à laquelle la relation est créée.
Heure de fin	Spécifie le moment où la relation est interrompue ou supprimée.
Description	Brève description des relations d'objet.

6. Cliquez sur **Envoyer**.

Définir les relations indicateur-indicateur

Définir les relations entre l'objet indicateur et d'autres Utilisez les objets de relations pour lier deux observables ou un observable et SDO pour expliquer comment ils sont liés l'un à l'autre.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Indicateur-Indicateur**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire comme il vous convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Domaine	Définit le champ d'application de l'enregistrement d'objet. La valeur de ce champ est renseignée automatiquement.
Indicateur cible	Sélectionnez et définissez l'objet indicateur cible.
Type de relation	Description qui fournit plus de détails et de contexte sur le type de relation. Définissez le sens de la relation, qu'il soit direct ou inverse. ○ Inverse : il s'agit du type de relation entre l'observable et l'objet. ○ Direct : type de relation entre l'objet et l'observable.
Indicateur source	Sélectionnez et définissez l'indicateur d'objet source.

6. Cliquez sur **Envoyer**.

Définir les relations indicateur-observable

Définissez les relations entre l'objet d'indicateur et d'autres SDO.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations** > **Indicateur : observable**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire comme il vous convient.

Champ	Description
Observable	Sélectionnez et définissez l'observable.
Indicateur	Sélectionnez et définissez l'objet d'indicateur.

6. Cliquez sur **Envoyer**.

Relations éventuelles

L'application utilise une corrélation automatisée pour établir des relations possibles entre deux SDO, deux observables ou un observable et SDO.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Sélectionnez un ou plusieurs enregistrements potentiellement connexes et appliquez cette action sur l'interface utilisateur, ce qui modifiera davantage les enregistrements en relations confirmées et visibles dans la section Enregistrements connexes.
2. Toutes les corrélations confirmées ingérées ou créées manuellement par un analyste remplaceront les relations potentielles créées par la corrélation automatique.

Confirmer la relation observable-observable potentiel

Utilisez cette section pour confirmer les relations entre les observables.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations éventuelles** > **Observable-Observable**.
4. Sélectionnez l'enregistrement du ou des observables.
5. Cliquez sur **Confirmer la relation**.
   Idéalement, un enregistrement de relation potentielle est créé et identifié en fonction de ses règles de corrélation. Une fois que vous avez confirmé la relation, l'enregistrement des observables est déplacé vers la section Relations, ce qui signifie que la relation entre les observables et les observables est confirmée. L'enregistrement affiche une relation confirmée uniquement lorsque les règles de corrélation correspondent. Par exemple, une relation potentielle peut être créée lorsque deux observables de type URL ont le même nom de domaine.

   Vous pouvez également créer un nouvel enregistrement d'observables en liant les observables à partir de la liste des observables et confirmer les relations à partir de l'onglet Enregistrements connexes de chaque observable.

   a. Ouvrez n'importe quel enregistrement d'observable.

   b. Accédez à l'onglet **Enregistrements connexes** .

   c. Cliquez sur le bouton **Lien** .

   d. Sélectionnez un ou plusieurs observables.

   e. Cliquez sur **un lien**.
      Cela crée une nouvelle relation entre l'enregistrement observable sélectionné et les observables nouvellement liés.

6. Cliquez sur **Supprimer** pour supprimer les relations.

Confirmer les relations éventuelles objet-objet

Définissez les relations éventuelles entre les objets.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations éventuelles** > **Objet-Objet**.
4. Sélectionnez l'enregistrement observable.
5. Cliquez sur **Confirmer la relation**.
   Idéalement, un enregistrement de relation potentielle est créé et identifié en fonction de ses règles de corrélation. Une fois que vous avez confirmé la relation à partir de cette section, l'enregistrement des observables est déplacé vers la section Relations, ce qui signifie que la relation entre les observables et les observables est confirmée. L'enregistrement affiche une relation confirmée uniquement lorsque les règles de corrélation correspondent. Par exemple, une relation potentielle peut être créée lorsque deux observables de type URL ont le même nom de domaine.

   Vous pouvez également créer un nouvel enregistrement d'observables en liant les observables à partir de la liste des observables et confirmer les relations à partir de l'onglet Enregistrements connexes de chaque observable.

   a. Ouvrez n'importe quel enregistrement d'observable.

   b. Accédez à l'onglet **Enregistrements connexes** .

   c. Cliquez sur le bouton **Lien** .

   d. Sélectionnez un ou plusieurs observables.

   e. Cliquez sur **un lien**.
      Cela crée une nouvelle relation entre l'enregistrement observable sélectionné et les observables nouvellement liés.

6. Cliquez sur **Supprimer** pour supprimer les relations.

Confirmer les relations potentielles indicateur-indicateur

Définissez les relations éventuelles entre les objets.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accéder à **Relations éventuelles** > **indicateur-indicateur**.
4. Sélectionnez l'enregistrement observable.
5. Cliquez sur **Confirmer la relation**.
   Un enregistrement de relation potentielle est idéalement confirmé en fonction des règles de corrélation automatisées. Une fois que vous avez confirmé la relation, l'enregistrement des observables est déplacé vers la section Relations, ce qui signifie que la relation entre les observables et les observables est confirmée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'enregistrement affiche une relation confirmée uniquement lorsque les règles de corrélation correspondent. Par exemple, une relation potentielle est confirmée lorsque deux observables de type URL ont le même nom de domaine.

Vous pouvez également créer un nouvel enregistrement d'observables en liant les observables à partir de la liste des observables et confirmer les relations à partir de l'onglet Enregistrements connexes de chaque observable.

a. Ouvrez n'importe quel enregistrement d'observable.

b. Accédez à l'onglet **Enregistrements connexes** .

c. Cliquez sur le bouton **Lien** .

d. Sélectionnez un ou plusieurs observables.

e. Cliquez sur **un lien**.
Cela crée une nouvelle relation entre l'enregistrement observable sélectionné et les observables nouvellement liés.

6. Cliquez sur **Supprimer** pour supprimer les relations.

Exporter des données d'intelligence

Utilisez la fonction d'exportation pour exporter manuellement les données d'intelligence dans différents formats.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Pourquoi et quand exécuter cette tâche
Actuellement, la fonctionnalité d'exportation est limitée aux observables, aux indicateurs et à la gestion des tickets. La procédure suivante décrit comment exporter les données des observables et suivre la même procédure pour exporter les données des indicateurs.

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **Observables** > **Tous les observables**.

2. Sélectionnez un ou des observables.

3. Cliquez sur **le bouton Exporter** .

> **Remarque :** Le bouton **Exporter** n'est activé que lorsque des observables sont sélectionnés pour l'exportation. Si aucun observable n'est sélectionné, le bouton reste désactivé.

4. Sélectionnez le type de fichier souhaité pour l'exportation.
Actuellement, les formats d'exportation pris en charge sont Excel, CSV et STIX 2.1 JSON. Supposons que si votre type d'exportation est Excel, le nombre d'enregistrements pouvant être exportés à la fois est limité à 10 000, quel que soit le type de format sélectionné.

Si la sélection dépasse 10 000 enregistrements, un message d'erreur s'affiche indiquant que la limite maximale du type de format sélectionné a été dépassée et que seuls les 10 000 premiers enregistrements seront exportés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si le format d'exportation est CSV et que la limite d'enregistrement est dépassée, un message d'alerte s'affiche indiquant que l'exportation est à l'état **en cours** , ainsi qu'un lien permettant d'afficher l'état de l'exportation. Vous pouvez cliquer sur le lien pour afficher l'état, actualiser l'enregistrement et, une fois qu'il est passé à l'état **Traitement** après l'actualisation, télécharger la pièce jointe.

5. Cliquez sur **Exporter**.

Remarque : Vous pouvez également afficher les données d'exportation à partir du module **Imports/Exports** .

Un message de confirmation s'affiche indiquant que l'exportation est réussie et que votre téléchargement est terminé.

Confirmer les relations éventuelles à partir d'enregistrements connexes

Confirmez les relations entre les deux SDO.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements sur les menaces** dans l'espace de travail.
3. Accédez à la section **Enregistrements connexes** .
4. **Développer les relations potentielles**.
5. Ouvrez tout enregistrement tel que des observables, des indicateurs ou tout autre objet dans lequel vous souhaitez confirmer les relations entre deux SDO.
6. Par exemple, sélectionnez **Observables** dans le volet de navigation de gauche.
7. Sélectionnez le ou les enregistrements **d'observables dans** la liste.

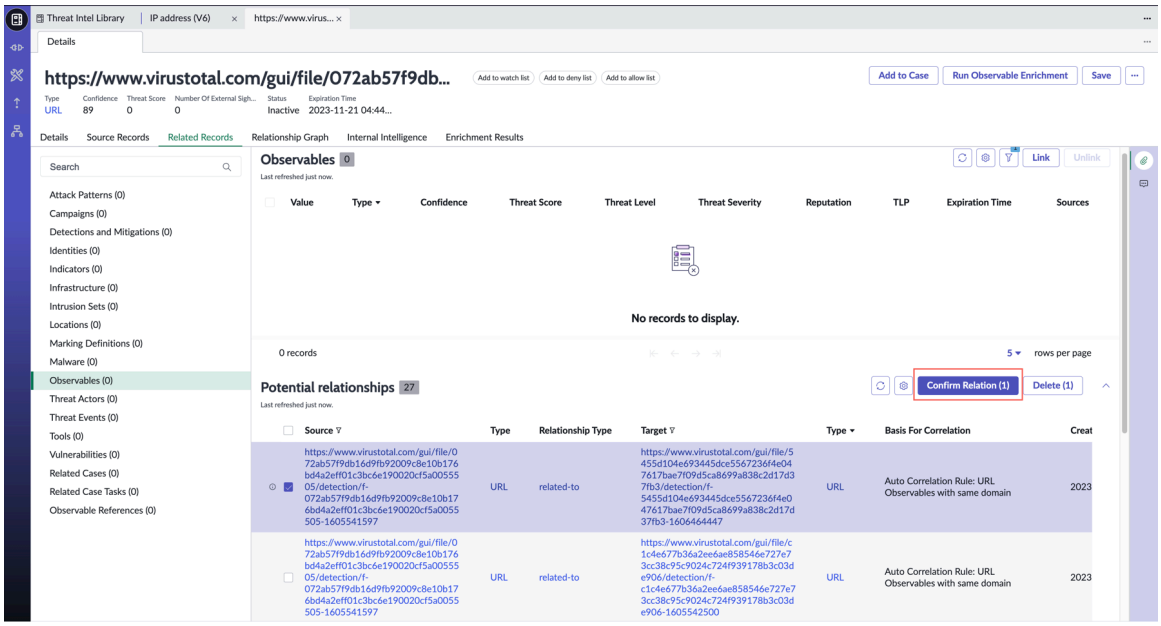
Remarque : La section Liste affiche tous les enregistrements observables liés de l'observable associé.

8. Cliquez sur le bouton **Confirmer les relations** pour confirmer les relations entre les objets.

Remarque : Pour plus d'informations, reportez-vous à etObjets de relationsRelations éventuelles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Cliquez sur **Supprimer** pour supprimer les observables associés.
   Pour plus d'informations sur la façon dont les relations et les relations potentielles sont établies entre les ODD, voir Relations éventuelles et Objets de relations.

Corrélation automatisée

La corrélation automatisée vous aide à identifier les relations entre les observables, les indicateurs et les objets.

Avec le processus de corrélation, l'application établit automatiquement la corrélation entre les enregistrements de renseignements sur les menaces en fonction des règles prédéfinies. Selon le type de règle appliquée, la relation peut être une relation confirmée ou une relation potentielle. Si les relations entre les objets sont confirmées, ces objets s'affichent automatiquement dans la vue de détails de cet objet dans la section **Enregistrements connexes** .

Les relations et les relations éventuelles sont décrites comme suit :

- **Relations** : utilisez les objets de relations pour lier deux observables ou un observable et SDO pour expliquer comment ils sont liés l'un à l'autre.
- **Relations éventuelles** : utilisez les relations potentielles pour établir des relations potentiellement possibles entre deux SDO, deux observables ou un observable et SDO à l'aide de la corrélation automatisée.

Voici les règles de corrélation prédéfinies mises en service dans le système de base :

Règles de corrélation

Nom de la règle	Description de la règle	Définition de règle	Action de règle
Observables avec le même hachage de fichier	La règle compare les valeurs de hachage des observables (du même type) et identifie s'ils partagent le même hachage.	La règle compare les valeurs de hachage (du même type) des indicateurs et identifie s'ils partagent le même hachage.	Crée une relation

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles de corrélation (suite)

Nom de la règle	Description de la règle	Définition de règle	Action de règle
Observables d'URL avec le même domaine	La règle examine les points communs dans la structure des URL pour déterminer si elles partagent le même domaine de base.	La règle examine les points communs dans la structure des URL - Identifie s'ils partagent le même domaine de base et ont une structure de sous-répertoire similaire.	Crée une relation potentielle
Observable trouvé en tant que sources dans l'objet réseau	La règle fait correspondre la valeur de l'attribut Source du réseau avec les observables IPV4, IPV6 ou de nom de domaine dans le système et les liens en tant que source du trafic.	La règle associe la valeur de l'attribut Source aux observables IPV4, IPV6 ou de nom de domaine dans le système et les liens en tant que source du trafic.	Crée une relation
Observable trouvé comme destination dans l'objet réseau	La règle fait correspondre la valeur de l'attribut de destination réseau avec les observables IPV4, IPV6 ou de nom de domaine dans le système et les liens comme destination du trafic.	La règle fait correspondre la valeur de l'attribut Source avec les observables IPV4, IPV6 ou de nom de domaine dans le système et les liens comme destination du trafic.	Crée une relation
Relier les observables basés sur la communication	Sur la base d'objets réseau, la règle identifie tous les observables (IPV4, IPV6 et nom de domaine) qui ont communiqué avec la même destination (IPV4, IPV6 ou nom de domaine) et établit une relation entre ces observables. Il s'agit également des observables associés (IPV4, IPV6 et nom de domaine) s'ils sont associés au même objet réseau que la source communiquant avec la destination.	Sur le bassis des objets réseau, la règle identifie tous les indicateurs qui ont communiqué avec la même destination (IPV4, IPV6, mac-addr ou nom-de-domaine) et établit une relation entre ces indicateurs comme connectés à la même infrastructure C2.	Crée une relation
Observables du domaine racine connexe aux sous-domaines	La règle lie un domaine racine à des sous-domaines et vice versa pour le type de domaine des observables.	La règle lie un domaine racine à des sous-domaines.	Crée une relation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles de corrélation (suite)

Nom de la règle	Description de la règle	Définition de règle	Action de règle
Domaines associés aux adresses IP en fonction des résolutions DNS	À l'aide des attributs domaine-ipv4 ou domaine-ipv6 des observables de domaine, la règle établit des relations entre les domaines et les adresses IP.	Utilisez les attributs domaine-ipv4 ou domaine-ipv6, La règle identifie tous les domaines ou sous-domaines qui se résolvent vers la même adresse IP et établit des relations entre les indicateurs, indiquant leur connexion à la même infrastructure C2.	Crée une relation
Domaines correspondants avec des certificats SSL	La règle analyse les informations de certificat SSL associées aux observables de domaine et établit une relation entre eux.	La règle analyse les informations de certificat SSL associées aux indicateurs et identifie que les deux certificats sont émis par la même autorité de certification et partagent la même date d'expiration. Elle établit des relations entre les indicateurs, indiquant leur connexion à la même infrastructure C2 ou à la même campagne de menaces.	Crée une relation
Relier des entités basées sur des observables communs	La règle compare si le même observable est associé à deux entités différentes et les relie l'une à l'autre.	La règle compare si le même observable est associé à deux entités différentes et les identifie comme étant associés l'un à l'autre.	Crée une relation potentielle
Relier les indicateurs basés sur des observables communs	La règle compare si le même observable est lié à deux indicateurs différents et les relie l'un à l'autre.	La règle compare si le même observable est lié à deux indicateurs différents et les identifie comme étant liés l'un à l'autre.	Crée une relation potentielle
Associer les indicateurs à des objets basés sur des observables communs	La règle compare si le même observable est lié à des indicateurs et des objets et les relie les uns aux autres.	La règle compare si le même observable est lié à deux indicateurs et objets différents et les identifie comme étant liés l'un à l'autre.	Crée une relation potentielle

Utilisation des exportations de données

Centre de sécurité des renseignements sur les menaces Prend en charge l'exportation manuelle d'observables, d'indicateurs et de tickets dans les formats recommandés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette fonctionnalité vous permet d'extraire facilement les données pour une analyse plus approfondie. Les principales fonctionnalités sont les suivantes :

- Exportez des observables, des indicateurs et des tickets individuellement ou en bloc.
- Sortie dans les formats recommandés tels que CSV, STIX 2.1 pour une intégration transparente.

Remarque : La fonctionnalité d'exportation de données n'est actuellement prise en charge que pour les observables, les indicateurs et la gestion des tickets. Dans la gestion des tickets, les exportations sont limitées aux listes d'observables et d'indicateurs sous les artefacts de ticket.

Afficher toutes les exportations

Utilisez cette section pour afficher tous les enregistrements exportés manuellement.

Avant de commencer
Rôle requis : sn_sec_tisc.export

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Importations/Exportations**.
2. Sélectionner **Données exportées** > **Toutes les exportations**
   Cette page affiche les enregistrements d'exportation.
3. Ouvrir n'importe quel enregistrement pour afficher l'état du processus d'exportation.

Afficher mes exportations

Affichez et téléchargez les exportations auxquelles vous êtes autorisé à accéder.

Avant de commencer
Rôle requis : sn_sec_tisc.export

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Importations/Exportations**.
2. Sélectionner **Données exportées** > **Mes exportations**
   Cette page affiche les enregistrements d'exportation.
3. Ouvrir n'importe quel enregistrement pour afficher l'état du processus d'exportation.

Propriétés système de l'intelligence d'exportation

Cette section décrit les limites d'enregistrement et ses propriétés lors de l'exportation de données.

Remarque : TISC Fournit la limite suivante pour les exportations de données. Pour définir les propriétés suivantes, accédez à **Propriétés système** > **Importer/exporter**.

Rôle requis : sn_sec_tisc.export

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Format	Propriété	Description
STIX 2.1 JSON	sn_sec_tisc.stix_export_limit	Nombre maximal de lignes pouvant être exportées vers un fichier STIX 2.1. Le e par défaut est 10000.
STIX 2.1 JSON	sn_sec_tisc.stix_export_payload_streaming_attachment_objects_size	Si le nombre d'objets dans le tableau « Objets » de la charge utile d'exportation STIX est supérieur au nombre spécifié dans cette propriété, JSONStreamingAPI est utilisé pour créer la pièce jointe. La limite d'exportation par défaut est 4 000.
STIX 2.1 JSON	sn_sec_tisc.stix_json_from_json_streaming_api_action_timeout	Délai (en secondes) qui sera utilisé lors du déclenchement de l'action du Concepteur de flux pour générer une pièce jointe JSON STIX à l'aide de l'API de diffusion en continu JSON. La limite d'exportation par défaut est 900.

Remarque : Pour mieux comprendre la limite d'exportation sur les autres types de format, voir Limites d'exportation .

MITRE-ATT&CK™ Dépôt

Le MITRE-ATT&CK référentiel est disponible sous la bibliothèque d'intelligence où les données des sources MITRE sont ingérées.

Les données MITRE qui arrivent dans le référentiel sont stockées dans un référentiel MITRE distinct des données de la bibliothèque Intel sur les menaces, où les données MITRE ne sont pas déployées pour le flux d'agrégation ou de déduplication et sont indépendantes.

Les sources de données disponibles dans l'application sont les suivantes :

1. MITRE : ATT&CK d'entreprise
2. MITRE - Mobile ATT&CK
3. MITRE - ICS ATT&CK

Les données de ces sources sont stockées dans un référentiel MITRE séparé sous la bibliothèque TI dans le système de base. Si vous souhaitez créer une nouvelle source MITRE, configurez une source personnalisée. Pour plus d'informations, consultez Afficher le flux personnalisé et dans la vue de formulaire, cliquez sur **la case à cocher Avancé** et sélectionnez le processeur de **rapports** en tant que : **MITRECollectionDataProcessor**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer les matrices

Gérez les matrices importées à partir des collections MITRE TAXII. Les matrices sont un ensemble de tactiques et de techniques. Vous pouvez consulter les matrices pour vérifier si vos collections sont disponibles dans le référentiel MITRE-ATT&CK.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Une fois que vous avez activé les sources de données de flux associées à MITRE ATT&CK qui sont disponibles dans le système de base, cliquez sur **Exécuter maintenant** pour exécuter les intégrations et extraire les informations connexes MITRE.
   Pour plus d'informations sur l'activation des intégrations
2. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **MITRE ATT&CK**.
   Les enregistrements connexes MITRE ATT&CK s'affichent. Par défaut, tous les enregistrements sont à l'état Activé.

   Remarque : Vous pouvez activer uniquement les matrices pertinentes pour votre organisation.
3. Sélectionnez n'importe quel enregistrement de matrice et cliquez sur **Désactiver** si vous souhaitez désactiver un enregistrement spécifique.
4. Vous pouvez également créer un enregistrement de matrices en cliquant sur **Nouveau** pour créer manuellement les matrices MITRE ATT&CK.
5. Renseignez les champs de manière appropriée.

Créer une nouvelle atténuation MITRE : détails

Champ	Description
Nom	Entrez le nom de la matrice.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Actif	Cochez cette case pour activer l'enregistrement de matrice.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Une description qui fournit plus de détails et de contexte sur l'ensemble d'intrusion, y compris potentiellement son objectif et ses principales caractéristiques.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce type d'objet.
Commentaires	Ajoutez tous les commentaires que vous pourriez avoir en plus.

Gérer les techniques

Gérez les techniques importées des collections MITRE TAXII. Les techniques contiennent différentes façons dont les attaquants se sont développés pour utiliser une tactique donnée. Vous pouvez examiner et désactiver les techniques qui ne sont pas pertinentes pour votre organisation. Dans STIX, les techniques sont connues sous le nom de schémas d'attaque.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Les techniques représentent la façon dont un adversaire atteint un objectif tactique en effectuant une action.

Procédure

1. Une fois que vous avez activé les sources de données de flux associées à MITRE ATT&CK qui sont disponibles dans le système de base, cliquez sur **Exécuter maintenant** pour exécuter les intégrations et extraire les informations connexes MITRE.
   Pour plus d'informations sur l'activation des intégrations
2. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **MITRE ATT&CK** > **Techniques**.
   Les enregistrements des techniques MITRE ATT&CK s'affichent. Par défaut, tous les enregistrements sont à l'état Activé.
3. Sélectionnez un enregistrement de technique et cliquez sur **Désactiver** si vous souhaitez désactiver un enregistrement spécifique.
4. Vous pouvez également créer de nouveaux enregistrements de techniques en cliquant sur **Nouveau** pour créer manuellement les techniques MITRE ATT&CK.
5. Renseignez les champs de manière appropriée.

Créer une nouvelle atténuation MITRE : détails

Champ	Description
ID	ID unique d'une technique.
Nom	Entrez le nom de la technique.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement est créé.
Plateformes	Ajoutez les plates-formes requises.
Autorisations requises	Ajoutez les autorisations requises.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Priorité	Indique le niveau de priorité affecté à la technique MITRE (faible, modéré, élevé ou critique). **Remarque :** Des priorités peuvent être attribuées à des techniques pour ajouter de la pertinence à votre organisation.
Description	Une description qui fournit plus de détails et de contexte sur l'ensemble d'intrusion, y compris potentiellement son objectif et ses principales caractéristiques.
Détection	La technique de détection est utilisée pour identifier l'accès ou l'activité non autorisée de l'adversaire aux réseaux informatiques.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez tout contexte supplémentaire pour ce type d'objet.
Commentaires	Ajoutez tous les commentaires que vous pourriez avoir en plus.
Balises TISC	
Sélectionner des balises TISC	Sélectionnez les balises à annoter ou affectez les enregistrements ingérés dans le système à partir de cette source. **Remarque :** Des balises peuvent être attribuées à des techniques pour ajouter de la pertinence à votre organisation.

Gérer les atténuations

Gérez les atténuations importées à partir des collections MITRE TAXII. Les atténuations vous permettent d'empêcher un adversaire d'exécuter avec succès des techniques ou des sous-techniques contre votre organisation. Dans STIX, les mesures d'atténuation sont connues sous le nom de plan d'action.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Une fois que vous avez activé les sources de données de flux associées à MITRE ATT&CK qui sont disponibles dans le système de base, cliquez sur **Exécuter maintenant** pour exécuter les intégrations et extraire les informations connexes MITRE.
   Pour plus d'informations sur l'activation des intégrations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **MITRE ATT&CK** > **Atténuations**.
   Cliquez sur une atténuation pour afficher toutes les informations associées.
3. Cliquez sur **Nouveau** pour créer manuellement les atténuations MITRE ATT&CK.
4. Renseignez les champs de manière appropriée.

Créer de nouveaux outils MITRE : détails

Champ	Description
ID	ID unique d'un plan d'action visant à prévenir une attaque.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Nom	Entrez un nom descriptif pour identifier l'objet.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Alias	Une liste d'autres noms permettant d'identifier cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'objet, y compris potentiellement son objectif et ses principales caractéristiques.
Contributeurs	Spécifie les contributeurs.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet objet.
Commentaires	Ajoutez des commentaires pour cet objet.

5. Cliquez sur **Enregistrer**.

Gérer les groupes

Gérez les groupes importés à partir des collections MITRE TAXII. Les groupes sont des ensembles d'activités d'intrusion connexes qui sont suivies par un nom commun dans la communauté de sécurité. Les analystes suivent les grappes d'activités à l'aide de divers termes tels que groupes de menaces, groupes d'activités, acteurs de menace, ensembles d'intrusion et campagnes. Dans STIX, les groupes sont appelés ensembles d'intrusion.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **MITRE ATT&CK** > **Groupes**.
   Vous pouvez afficher les groupes répertoriés.
2. Cliquez sur **Nouveau** pour créer manuellement les groupes MITRE ATT&CK.
3. Renseignez les champs de manière appropriée.

Créer de nouveaux groupes MITRE : détails

Champ	Description
ID	ID unique d'un plan d'action visant à prévenir une attaque.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Nom	Entrez un nom descriptif pour identifier l'objet.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Alias	Une liste d'autres noms permettant d'identifier cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'objet, y compris potentiellement son objectif et ses principales caractéristiques.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet objet.
Commentaires	Ajoutez des commentaires pour cet objet.

4. Cliquez sur **Enregistrer**.
5. Pour voir comment ces objets sont liés, cliquez sur **Relations**.

Gérer les programmes malveillants

Gérez les informations sur les programmes malveillants que vous avez importées à partir des collections MITRE TAXII. Il s'agit d'un type de TTP qui représente un code malveillant.

Avant de commencer

Il s'agit d'un programme qui est secrètement inséré dans un système. L'intention d'un logiciel malveillant est de compromettre la confidentialité, l'intégrité ou la disponibilité des données, des applications ou du système d'exploitation (OS) de la victime.

Rôle requis : sn_sec_tisc.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **MITRE ATT&CK** > **Groupes**.
   Vous pouvez afficher les programmes malveillants répertoriés.
2. Cliquez sur un programme malveillant pour afficher toutes les informations associées.
3. Cliquez sur **Nouveau** pour créer manuellement le programme malveillant MITRE ATT&CK.
4. Renseignez les champs de manière appropriée.

Créer un programme malveillant MITRE : détails

Champ	Description
ID	ID unique d'un plan d'action visant à prévenir une attaque.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Nom	Entrez un nom descriptif pour identifier l'objet.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Alias	Une liste d'autres noms permettant d'identifier cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'objet, y compris potentiellement son objectif et ses principales caractéristiques.
Contributeurs	Spécifie les contributeurs.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet objet.
Commentaires	Ajoutez des commentaires pour cet objet.

5. Cliquez sur **Enregistrer**.
6. Pour voir comment ces objets sont liés, cliquez sur **Relations**.

Gérer les outils

Gérez les informations sur les outils que vous avez importées à partir des collections MITRE TAXII. Les outils sont des logiciels légitimes utilisés par les acteurs de la menace pour effectuer des attaques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_tisc.analyst

Pourquoi et quand exécuter cette tâche
Les outils vous permettent de savoir comment et quand les acteurs de la menace les utilisent pour exécuter des campagnes. Contrairement aux logiciels malveillants, ces outils ou progiciels se trouvent souvent sur un système et ont des objectifs légitimes pour les utilisateurs avancés, les administrateurs, les administrateurs réseau ou même les utilisateurs normaux.

Procédure

1. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **MITRE ATT&CK** > **Outils**.
   Vous pouvez afficher les outils répertoriés.
2. Cliquez sur un outil pour afficher toutes les informations associées.
3. Cliquez sur **Nouveau** pour créer manuellement les outils MITRE ATT&CK.
4. Renseignez les champs de manière appropriée.

Créer de nouveaux outils MITRE : détails

Champ	Description
ID	ID unique d'un plan d'action visant à prévenir une attaque.
Révoqué	Indique que les objets révoqués ne sont plus considérés comme valides par le créateur de l'objet.
Nom	Entrez un nom descriptif pour identifier l'objet.
Source	Spécifie la source de menace à partir de laquelle cet enregistrement d'objet est créé.
Alias	Une liste d'autres noms permettant d'identifier cet objet.
Heure de création dans la source	Spécifie l'heure de création de l'objet dans la source.
Heure de modification dans la source	Spécifie l'heure à laquelle l'objet est modifié dans la source.
Description	Description qui fournit plus de détails et de contexte sur l'objet, y compris potentiellement son objectif et ses principales caractéristiques.
Contributeurs	Spécifie les contributeurs.
Aperçus	
Notes	Toute information supplémentaire relative à l'atténuation.
Informations supplémentaires	
Contexte supplémentaire	Ajoutez un contexte supplémentaire pour cet objet.
Commentaires	Ajoutez des commentaires pour cet objet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Enregistrer**.
6. Pour voir comment ces objets sont liés, cliquez sur **Relations**.

Gérer les relations MITRE

Gérez les informations de relations MITRE que vous avez importées à partir des collections MITRE TAXII.

Avant de commencer

Rôle requis : sn_sec_tisc.analyst

Procédure

1. Pour afficher les données du référentiel MITRE ATT&CK, accédez à **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces** > **Bibliothèque de Renseignements sur les menaces** > **MITRE ATT&CK** > **Relations**.
   Vous pouvez afficher les relations répertoriées.
2. Cliquez sur un objet source pour afficher toutes les informations associées.
3. Cliquez sur **Nouveau** pour créer manuellement les relations MITRE ATT&CK.
4. Renseignez les champs de manière appropriée.

Créer de nouveaux outils MITRE : détails

Champ	Description
Objet MITRE source	Ajoutez l'objet MITRE source.
Objet MITRE cible	Ajoutez l'objet MITRE cible.
Type MITRE source	Entrez le type MITRE source.
Type MITRE cible	Entrez le type MITRE cible.
Type de relation	Définissez les relations entre les objets. Description qui fournit plus de détails et de contexte sur le type de relation. Les options disponibles sont les suivantes : Définissez le sens de la relation, qu'il soit direct ou inverse. ○ Inverse : il s'agit du type de relation entre l'observable et l'objet. ○ Direct : type de relation entre l'objet et l'observable.
Source	Sélectionnez et définissez l'objet source.
ID de la relation	Définissez l'ID de la relation.

5. Cliquez sur **Enregistrer**.
6. Pour voir comment ces objets sont liés, cliquez sur **Relations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Migration de données dans TISC

La migration de données est un processus qui consiste à déplacer toutes vos données d'une interface utilisateur classique vers TISC.

L'objectif de cette migration est de permettre aux utilisateurs de migrer les données des données Threat Intelligence existantes vers .TISC Pour exécuter ce processus, un nouveau cadre est introduit et est TISC expliqué dans la section suivante.

Migration de données de SIR TI vers TISC

Configuration de la tâche de migration de données dans TISC vous permet de déplacer les données du module d'extension Threat Intelligence existantes vers les TISC données du module d'extension directement.

Avant de commencer
Rôle requis : sn_sec_tisc.admin

Pourquoi et quand exécuter cette tâche

- **Migration sélective des enregistrements** : seuls les enregistrements de la table sélectionnée qui remplissent les conditions spécifiées sont migrés.
- **Inclure les relations** : les enregistrements connexes sont migrés uniquement si la case **Inclure les relations** est cochée.
- **État de migration d'entité** : une fois qu'une entité (observable ou objet) est migrée, elle n'est pas incluse dans d'autres migrations, sauf si elle est migrée en tant qu'enregistrement connexe.

  Remarque : Critères d'exclusion d'enregistrements pour l'utilitaire de migration

  L'utilitaire de migration exclut certains enregistrements en fonction des critères suivants :

  - **Observables** : les observables de type **fichier** qui contiennent des pièces jointes sécurisées ne seront pas migrés.
  - **Indicateurs** : les indicateurs ayant des valeurs vides dans les champs Modèle ou Type de modèle ne seront pas migrés.
  - **Objets** : les objets ingérés à partir du profil MITRE TAXII dans les données de Renseignements sur les menaces ne sont pas migrés vers Centre de sécurité des renseignements sur les menaces.

- **Enregistrements de tickets** : seuls les enregistrements actifs sont migrés par défaut, sauf si la case **Inclure les tickets fermés** est cochée.

Procédure

1. Accédez à la **Tous** > **Centre de sécurité des renseignements sur les menaces** > **Configuration de la tâche de migration de données**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient sur le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de la tâche de migration de données

Champ	Description
Nom	Nom de la migration de données.
Table	Sélectionnez la table à partir de laquelle les enregistrements doivent être migrés TISC. Les TISC options de table pour la migration sont les suivantes : ○ Observable(sn_ti_observable) ○ Indicateur de compromission (sn_ti_indicator) ○ ticket(sn_ti_case) de sécurité ○ Objets STIX V2 (sn_ti_stix2_object) (options telles que les schémas d'attaque, les campagnes, le plan d'action) **Remarque :** ○ Lorsque vous sélectionnez l'option STIX V2, tous les objets STIX sont migrés à l'exception de MITRE ATT&CK, car TISC dispose d'un cadre de travail différent pour migrer le MITRE ATT&CK. ○ Lorsque vous choisissez de migrer le ticket de sécurité, les tickets fermés ne sont pas migrés, mais seuls les tickets actifs sont migrés. Par exemple, sélectionnez **Table de migration des observables** .
Actif	Cochez cette case si le processus de migration de données est actif.
Inclure des relations	Cochez la case pour migrer les relations des enregistrements Threat Intelligence vers les TISC enregistrements. **Remarque :** Lorsque vous cochez cette case, toutes les entités connexes sont migrées ainsi que l'observable. Si la case n'est pas cochée, seul l'observable unique est migré, sans aucune entité connexe.
Inclure les tickets fermés	Cochez cette case si vous souhaitez inclure les tickets fermés dans le cadre de la migration des enregistrements de tickets.
Migrer uniquement les observables associés à l'incident de sécurité	Cochez la case pour migrer les observables associés aux incidents de sécurité et, si la case

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	n’est pas cochée, tous les observables sont migrés, indépendamment de leur association avec des incidents de sécurité.
Conditions	Option permettant de sélectionner les conditions qui peuvent être utilisées pour filtrer les données en cours de migration.
Configurations supplémentaires	
Fiabilité	Saisissez la fiabilité pour les entités TISC migrées (observables, objets ou indicateurs). La confiance doit être comprise entre 0 et 100.
Période d'expiration (jours)	La période d’expiration pour les entités migrées TISC .

Remarque : Le système ignore ou ignore les enregistrements qui sont déjà migrés TISC lors de la nouvelle extraction.

4. Cliquez sur **Envoyer**.
5. Cliquez sur **Exécuter maintenant** pour exécuter la migration des données.
   Lorsque vous exécutez la migration de données, une tâche en arrière-plan est exécutée et la tâche de migration est créée. Cette tâche crée un processus de migration et la taille de lot de ces enregistrements de migration est de 5 000.
6. Vérifiez l’état de la tâche de migration dans la section Exécution de tâches de **migration** .
   L’état de la tâche est mis en file d’attente et la limite maximale de la taille du lot ne doit pas dépasser 5 000 enregistrements. Cliquez sur l’enregistrement pour afficher les objets qui sont tous migrés pour cette entité spécifique.
7. Vérifiez l’état de la tâche de migration dans la liste connexe **Exécutions de tâches de migration** .
8. Cliquez sur l’enregistrement pour afficher l’état du traitement.
9. Vérifiez l’état de la migration par lots dans la section de liste connexe Enregistrements **de file d’attente de traitement** de la migration dans l’enregistrement d’exécution de la tâche de migration.
   La taille du lot pour la migration des enregistrements est de 5 000.
10. Vérifiez les entités TISC créées dans le cadre de la migration par lots sous les listes connexes respectives dans l’enregistrement de **la file d’attente du traitement de la migration** .

Flux fonctionnel de traitement des données TISC

Threat Intelligence Security Center (TISC) fournit une solution qui automatise la collecte et le traitement des données, ce qui permet de réduire la charge de travail des analystes Threat Intelligence en évitant les étapes manuelles.

Threat Intelligence Security Center (TISC) collecte des renseignements à l’aide de l’une des méthodes suivantes :

1. Ingestion à partir de sources de données préconfigurées et exécutées selon un calendrier.
2. Analystes de Renseignements sur les menaces important des données à l’aide de la fonctionnalité Renseignements sur l’importation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Création manuelle d'enregistrements individuels au sein de l'application.

> **Remarque :** Les données collectées dans l'application sont traitées pour normaliser, dédupliquer et regrouper les informations avant de les charger dans la bibliothèque Threat Intel.

Terminologie de base utilisée dans le traitement des données

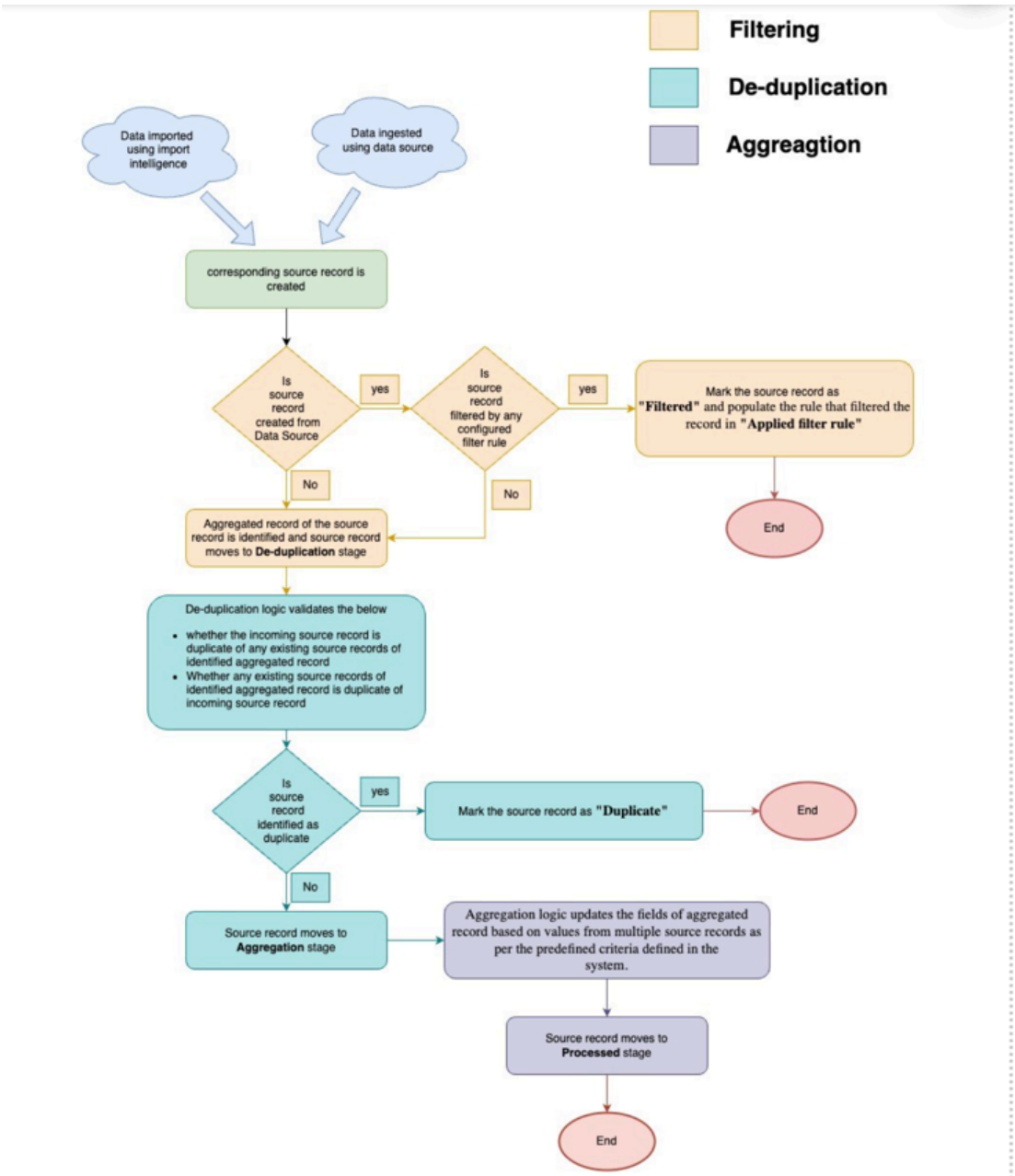
1. Tables sources : les tables sources contiennent les données relatives aux entités qui sont extraites de plusieurs sources, puis les enregistrements seront créés par chaque source.
2. Enregistrements agrégés : les tables d'enregistrements agrégés contiennent les données relatives à une entité spécifique en agrégeant les données de tous les enregistrements sources d'une entité spécifique.

Flux de données TISC

1. Lors de l'exécution réussie de l'intelligence d'importation/de la source de données, les enregistrements sont créés dans les tables sources correspondantes.
2. Une fois que les données entrent dans la table source, elles passent par une logique de filtrage pour valider si l'enregistrement doit être filtré en fonction des **règles de filtrage entrant** configurées. (Considérons SourceRecord1 comme un enregistrement source pour notre explication).
3. Si l'enregistrement est filtré par l'une des règles de filtrage entrant configurées, l'enregistrement source correspondant (SourceRecord1) est marqué comme **filtré** et la règle qui a filtré l'enregistrement se trouve dans la règle de filtrage appliquée.
4. Supposons que l'enregistrement source (SourceRecord1) s'agrège à AggregateRecord1.
5. Si l'enregistrement n'est pas filtré, il est marqué pour déduplication en définissant l'état du traitement sur Prêt pour la déduplication.
6. La logique de déduplication valide les points ci-dessous :
   a. Indique si l'enregistrement source entrant (SourceRecord1) est un doublon de tout enregistrement source existant pour AggregateRecord1.
   b. L'un des enregistrements sources existants pour AggregateRecord1 est un doublon de l'enregistrement source entrant (SourceRecord1).
7. Chaque entité possède des champs et des relations spécifiques sur la base desquels l'enregistrement source est validé pour la duplication.
8. Si l'enregistrement source entrant (SourceRecord1) est un doublon d'un enregistrement source existant d'AggregateRecord1, l'enregistrement source entrant (SourceRecord1) est marqué comme Doublon.
9. Si l'un des enregistrements sources existants (Enregistrement source existant1) d'AggregateRecord1 est identifié comme Doublon de l'enregistrement source entrant (SourceRecord1), l'enregistrement source existant (Enregistrement source existant1) est marqué comme Doublon et l'enregistrement source entrant (SourceRecord1) est marqué pour agrégation en définissant l'état du traitement sur Prêt pour l'agrégation.
10. Dans le cadre de l'agrégation, les champs de l'enregistrement agrégé AggregateRecord1 seront mis à jour en fonction des valeurs provenant de plusieurs enregistrements sources qui seront agrégés selon les critères prédéfinis définis dans le système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

TISC Archivage des données

Les données augmentent rapidement dans les tables avec une adoption accrue de la plateforme. Certaines tables sont intégrées dans le système de base avec diverses stratégies de gestion des données, mais d'autres utilisateurs doivent être implémentés par eux-mêmes.

Gestion des données dans TISC

Les données sont stockées et gérées dans l'instance en fonction de la TISC structure des objets de la TISC bibliothèque pour que les administrateurs puissent les afficher et les configurer selon les besoins de leur organisation.

L'archivage et la restauration des données sont l'une des fonctionnalités clés pour protéger les enregistrements en vue de leur utilisation future. La section suivante décrit le processus d'archivage et la TISC conservation des documents, car ils Renseignements sur les menaces contiennent d'énormes volumes de données et de documents.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il existe plusieurs méthodes différentes permettant aux utilisateurs de gérer leurs données dans des tables :

- Archiver les données
- Supprimer les données

Remarque : Si les utilisateurs n'adoptent aucune des méthodes pour gérer efficacement leurs données, l'utilisation augmente avec le temps et les données ont tendance à devenir beaucoup plus volumineuses, ce qui aura un impact important sur les performances de l'instance d'application ainsi que sur le stockage.

Archivage des données TISC

Le Centre de sécurité des renseignements sur les menaces est approvisionné avec les règles d'archivage dans le système de base pour la TISC table. Les enregistrements connexes sont également ajoutés dans le système de base à la règle d'archivage TISC .

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Archivage système** > **Règles d'archivage**.
   La liste des règles d'archivage applicables pour TISC s'affiche. Ces règles d'archivage sont différentes pour chaque type d'objet et s'appliquent indépendamment.
2. Le filtre des noms de tables commence par sn_sec_tisc.
3. Affichez les TISC enregistrements connexes.

Enregistrement Threat Intelligence	Table de référence
Archiver le modèle d'attaque	sn_sec_tisc_attack_pattern
Archiver la campagne	sn_sec_tisc_campaign
Archiver le plan d'action	sn_sec_tisc_course_of_action
Archiver le composant de données	sn_sec_tisc_aggregated_data_component
Archiver la source de données	sn_sec_tisc_aggregated_data_source
Archiver l'identité	sn_sec_tisc_identity
Infrastructure d'archivage	sn_sec_tisc_infrastructure
Archiver l'ensemble d'intrusions	sn_sec_tisc_intrusion_set
Archiver les programmes malveillants	sn_sec_tisc_malware
Archiver l'analyse de programme malveillant	sn_sec_tisc_malware_analysis
Archiver la définition de marquage	sn_sec_tisc_marking_definition
Archiver la perception d'objets	sn_sec_tisc_object_sighting
Archiver les données observées	sn_sec_tisc_observed_data
Archiver l'acteur de menace	sn_sec_tisc_threat_actor
Archiver l'événement de menace	sn_sec_tisc_threat_event
Archiver le regroupement des menaces	sn_sec_tisc_threat_grouping

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrement Threat Intelligence	Table de référence
Archiver la note de menace	sn_sec_tisc_threat_note
Archiver l’opinion sur la menace	sn_sec_tisc_threat_opinion
Archiver le rapport de menace	sn_sec_tisc_threat_report
Outil d’archivage	sn_sec_tisc_tool
Vulnérabilité d’archivage	sn_sec_tisc_vulnerability
Artefact	sn_sec_tisc_artifact
Numéro AS	sn_sec_tisc_as_number
Répertoire	sn_sec_tisc_directory
Adresse e-mail	sn_sec_tisc_email_address
E-mail	sn_sec_tisc_email_message
Objet de l'e-mail	sn_sec_tisc_email_subject
Fichier	sn_sec_tisc_file
Règle d’archivage de l’indicateur	sn_sec_tisc_indicator
Adresse IPv4	sn_sec_tisc_ipv4_address
CIDR IPv4	sn_sec_tisc_ipv4_cidr
Adresse IPv6	sn_sec_tisc_ipv6_address
Emplacement	sn_sec_tisc_location
Adresse MAC	sn_sec_tisc_mac_address
Hachage MD5	sn_sec_tisc_md5_hash
Nom Mutex	sn_sec_tisc_mutex_name
Autre observable	sn_sec_tisc_other_observable
Processus	sn_sec_tisc_process
Hachage SHA1	sn_sec_tisc_sha1_hash
Hachage SHA256	sn_sec_tisc_sha256_hash
Hachage SHA512	sn_sec_tisc_sha512_hash
URL	sn_sec_tisc_url
Compte d'utilisateur	sn_sec_tisc_user_account
Clé de registre Windows	sn_sec_tisc_windows_registry_key
Certificat X.509	sn_sec_tisc_x_509_certificate
Règle d’archivage des relations objet-objet	sn_sec_tisc_m2m_object
Règle d’archivage de la relation objet-observable	sn_sec_tisc_m2m_object_observable
Règle d’archivage d’indicateur connexe	sn_sec_tisc_m2m_indicator
Règle d’archivage du flux RSS	sn_sec_tisc_m2m_object_indicator
Règles d’archivage des importations	sn_sec_tisc_m2m_indicator_observable

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

Pour en savoir plus sur la création des règles d'archivage, reportez-vous à la section Créer une règle d'archivage .

4. Sélectionnez une règle d'archivage.
   Par exemple, sélectionnez Enregistrement observable du répertoire pour afficher la règle d'archivage du système de base.
5. Mettez à jour la règle si nécessaire.

Archiver TISC les enregistrements connexes

Utilisez la liste connexe Enregistrements connexes à l'archivage pour TISC ajouter les enregistrements connexes à la règle d'archivage.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Archivage système** > **Règles d'archivage**.
2. Le filtre des noms de tables commence par sn_sec_tisc.
3. Accédez à la section de liste connexe **Archiver les enregistrements connexes** pour afficher les TISC enregistrements connexes.

Règles de destruction dans TISC

Affichez les règles de destruction mises en service dans le système de base.

Avant de commencer
Rôle requis : admin

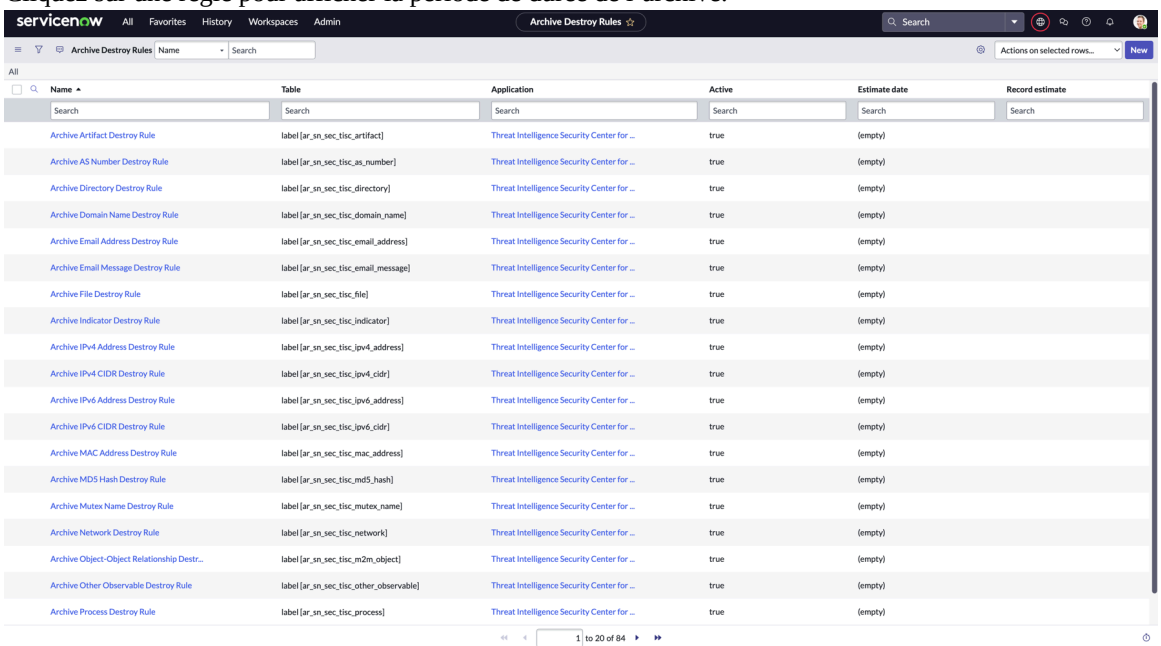
Procédure

1. Accédez à la **Tous** > **Archivage système** > **Archivage Règles de destruction**.
   La liste des règles de destruction applicables à TISC s'affiche. Ces règles de destruction sont différentes pour chaque type d'objet et s'appliquent indépendamment.
2. Affichez les règles de destruction applicables pour TISC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur une règle pour afficher la période de durée de l'archive.



Supprimer les enregistrements d'intelligence

Supprimer les enregistrements de Renseignements sur les menaces la bibliothèque.

Avant de commencer

Rôle requis : sn_sec_tisc.admin

Procédure

1. Accédez à la **Espaces de travail** > **Centre de sécurité des renseignements sur les menaces**.
2. Cliquez sur l'icône **Bibliothèque de Renseignements** sur les menaces dans l'espace de travail.
3. Ouvrez n'importe quel enregistrement.
4. Accédez à la section **Enregistrements sources** .
5. Sélectionnez **Supprimer** pour supprimer les enregistrements sources.
6. Supprimer l'enregistrement de bibliothèque.

Remarque :

a. Si un enregistrement de bibliothèque avec des enregistrements sources associés est supprimé, les enregistrements sources sont retraités et un nouvel enregistrement de bibliothèque est créé en agrégeant les valeurs de champ à partir des enregistrements sources.

b. Pour supprimer définitivement les données de la bibliothèque Threat Intelligence, utilisez des règles d'archivage au lieu de supprimer les enregistrements de la bibliothèque. Pour en savoir plus, consultez TISC Archivage des données.

Data Loss Prevention Incident Response

L'application Data Loss Prevention Incident Response (DLP IR) vous permet d'examiner et de gérer le workflow de rattrapage des incidents DLP à partir de plusieurs sources, telles que le point de terminaison, le réseau, la messagerie électronique et le cloud.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Data Loss Prevention Incident Response

Explorer



Découvrez comment les analystes et les administrateurs utilisent DLP Incident Response

Installation et configuration



Installation et configuration de l’application DLP Incident Response

Administrer



Tâches d’administration sur la façon de gérer les incidents DLP sur le ServiceNow AI Platform

Utiliser



Mettez à jour et gérez les incidents en tirant parti du portail de l’utilisateur final DLP, du portail des opérations DLP et du tableau de bord DLP.

Intégrer



Étendre les options DLP en les intégrant à des applications tierces

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage et demande d'aide

- Bibliothèque de ressources Security Operations
- Communauté Security Operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service client et assistance

Explorer Data Loss Prevention Incident Response

Explorez Data Loss Prevention Incident Response l'application pour apprendre à gérer les informations sensibles de vos clients, telles que les données financières et propriétaires, les dossiers médicaux ou les numéros de sécurité sociale.

La perte de données se produit lorsque des informations confidentielles ou sensibles quittent le réseau de l'entreprise à la suite d'une communication non autorisée. Avec l'application DLP, vous pouvez identifier, répondre et protéger vos canaux de perte de données.

En utilisant l'application Data Loss Prevention Incident Response , votre organisation bénéficie des avantages clés suivants :

- Intégrez plusieurs solutions DLP tierces pour obtenir une vue unifiée des incidents dans le ServiceNow AI Platform.
- Surveillez et affectez des incidents aux utilisateurs finaux afin de rationaliser la gestion des incidents DLP.
- Coachez vos employés grâce aux modèles d'e-mails personnalisés et aux notifications envoyées pour chaque incident, ainsi que sous la forme d'un résumé.
- Escaladez les incidents DLP en retard, des utilisateurs finaux vers les responsables.
- Affichez les rapports récapitulatifs des incidents ouverts par politique, gravité, principaux contrevenants, et ainsi de suite.
- Suivez les tendances des incidents DLP, les tendances des faux positifs et les tendances de rattrapage.

Utilisez cette section pour en savoir plus sur les fonctionnalités clés, les différents rôles impliqués dans le travail avec les incidents DLP.

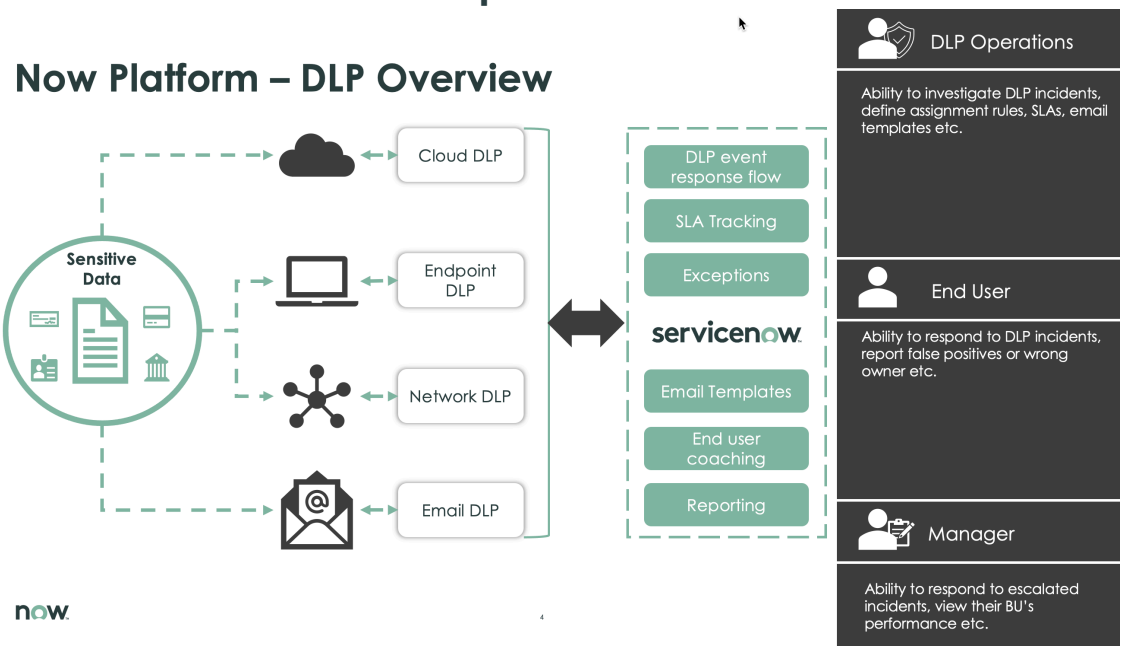
Vue d'ensemble de DLP Incident Response

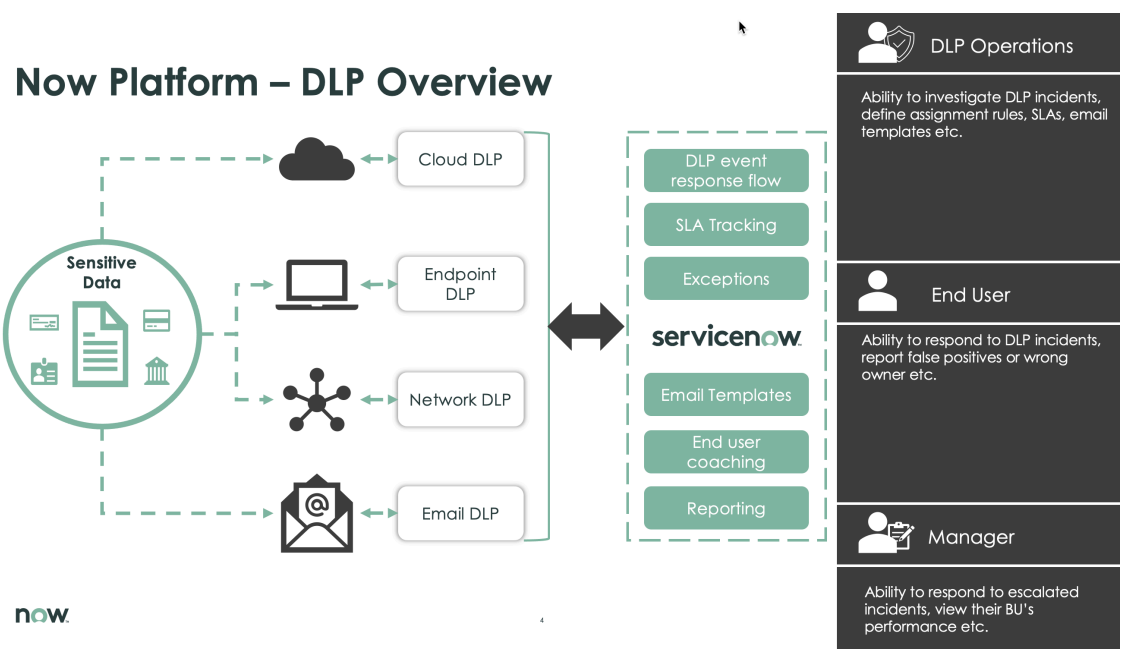
Découvrez comment utiliser l'application ServiceNow AI Platform et l'application Data Loss Prevention Incident Response (DLP IR). Gérez les informations sensibles de vos clients, telles que les données financières et propriétaires, les dossiers médicaux ou les numéros de sécurité sociale. Automatisez les workflows de rattrapage avec l'application DLP Incident Response.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Data Loss Prevention Incident Response et le ServiceNow AI Platform





Traduction automatique

1. Il s’agit d’une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP
2. Tâches d’administrateur DLP : il s’agit d’une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP
3. Utilisation du portail d’utilisateur final DLP : il s’agit d’une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP
4. Utilisation du portail DLP Ops : il s’agit d’une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP
5. Utilisation du tableau de bord DLP - Il s’agit d’une image cliquable, vous pouvez donc essayer de cliquer sur les différentes sections pour en savoir plus sur DLP

L’application Data Loss Prevention Incident Response comprend les fonctionnalités suivantes :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Espace de travail d'utilisateur final où vos utilisateurs finaux ou employés peuvent examiner et répondre aux incidents DLP affectés.
- Un espace de travail de gestionnaire où un gestionnaire peut examiner les incidents DLP remontés et agir en conséquence.
- Espace de travail unifié où votre équipe des opérations DLP peut suivre les tendances des incidents ouverts, les principaux contrevenants et les incidents par source d'analyse, et peut afficher, modifier, affecter et fermer les incidents DLP sur plusieurs sources (points de terminaison, réseaux et e-mail).
- Contrôles administratifs qui définissent les modèles d'e-mail pour le coaching et la communication de l'utilisateur final, les règles d'affectation pour l'affectation automatique des incidents, les règles d'escalade automatique et la délégation pour les réponses aux incidents.

Introduction à DLP Incident Response

Vérifiez les informations suivantes avant de commencer à configurer votre Data Loss Prevention Incident Response application (DLP IR).

Liste de vérification

Tâche de configuration	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform et DLP.	DLP Incident Response prend en charge les rôles suivants : • L'administrateur (admin) installe les applications à partir de et ServiceNow Store affecte l'administrateur DLP (sn_dlir.admin). • sn_dlir.admin • sn_dlir.analyste
Vérifiez que les applications principales nécessaires à la prise en charge de l'application ServiceNowData Loss Prevention Incident Response sont installées et activées.	Le Data Loss Prevention Incident Response module d'extension (com.snc.data_loss_incident) est requis pour prendre en charge le Data Loss Prevention Incident Response produit. Vérifiez que les applications suivantes Opérations de sécurité sont installées et activées à partir du ServiceNow Store. Si ce n'est pas le cas, installez et activez une application à la fois dans l'ordre suivant pour assurer une installation fluide : • Data Loss Prevention Incident Response (com.snc.data_loss_incident) • Security Support Common Pour plus d'informations sur la configuration de votre ServiceNow AI Platform instance pour l'intégration, consultez Obtenir une autorisation pour un produit ou une application

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	Security Operations ou Activer une application ServiceNow Store.
Séparation de domaine	Vérifiez la rubrique si vous avez l'intention de séparer les données, les processus et les Séparation de domaine et DLP Incident Response tâches administratives.

Installation et configuration DLP IR de Réponse aux incidents

Téléchargez l'application Data Loss Prevention Incident Response (DLP IR) à partir de et ServiceNow Store installez-la sur votre instance.

Avant d'appeler les workflows pour l'intégration, installez et configurez l'application Data Loss Prevention Incident Response sur ServiceNow Store votre ServiceNow AI Platform instance.

Installer et configurer l'application DLP Incident Response

Gérez les informations sensibles et automatisez les workflows de rattrapage à l'aide de l'application Data Loss Prevention Incident Response (DLP IR) de votre ServiceNow AI Platform instance.

Avant de commencer

Avant de pouvoir effectuer les étapes de configuration, vous devez télécharger l'application à partir de et ServiceNow Store l'installer sur votre instance.

Rôles requis : admin et sn_dlir.admin

Procédure

1. Suivez les instructions de téléchargement d'une application à partir de ServiceNow Store.
2. Une fois que vous avez téléchargé l'application **DLP Incident Response** et toutes ses applications dépendantes, accédez à **Tous** > **Administration DLP** > **Configuration par défaut** pour terminer le reste de la configuration de l'application.

Séparation de domaine et DLP Incident Response

Vous pouvez utiliser Séparation de domaine avec DLP Incident Response pour séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Standard

- Inclut tous les aspects du support de niveau **basique** .
- Les propriétés d'application sont sensibles au domaine selon les besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications .

Fonctionnement de Séparation de domaine avec DLP Incident Response

- Créez un utilisateur avec les rôles sn_dlir.admin et sn_dlir.analyst requis dans le domaine respectif.
- Effectuez les configurations de Réponse aux incidents DLP dans le domaine approprié.

Administration de Réponse aux incidents DLP

Vous pouvez configurer et affecter des règles, configurer des règles de date d'échéance, utiliser des modèles d'e-mail, configurer des actions de réponse de l'utilisateur final et bien plus encore pour gérer les Data Loss Prevention Incident Response incidents (DLP IR) sur le ServiceNow AI Platform.

L'application Data Loss Prevention Incident Response vous permet d'effectuer les configurations suivantes.

Paramètres de configuration par défaut de DLP

Définissez les paramètres de configuration par défaut des Data Loss Prevention Incident Response incidents (DLP IR) afin d'identifier et de configurer les préférences de notification d'incident et d'affectation d'incident pour vos utilisateurs finaux.

Avant de commencer
Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche
Vous pouvez utiliser ce module pour définir les paramètres de configuration par défaut lorsque les règles d'affectation de base et les règles d'identificateur sont épuisées et ne peuvent pas correspondre à une condition ou à un utilisateur. Vous pouvez également définir et réappliquer des règles de recherche d'utilisateur final et des règles d'affectation aux incidents DLP actifs existants.

La notification d'incident de l'utilisateur final vous permet de spécifier la fréquence à laquelle les notifications par e-mail sont envoyées à vos utilisateurs finaux. Par exemple, vous pouvez configurer des préférences de notification pour accumuler des incidents et envoyer une synthèse d'e-mail une fois par semaine. En affectant un incident, vous pouvez spécifier à quel groupe vous affectez initialement les incidents DLP. Vous pouvez également spécifier comment les utilisateurs finaux sont identifiés par l'équipe des opérations DLP.

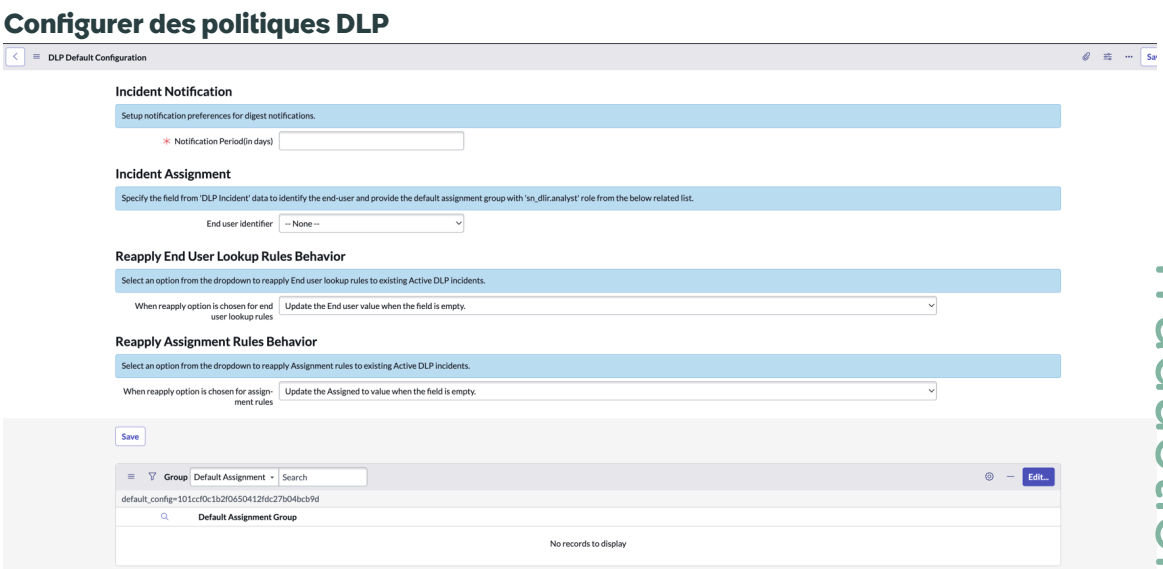
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, supposons qu'un utilisateur a stocké des informations de carte de crédit dans un fichier sur un réseau. Lorsque le produit d'intégration DLP tiers crée un incident pour une violation de la politique en matière de données sensibles, les données d'incident que le ServiceNow AI Platform DLP ingère contiennent des informations sur l'utilisateur final. Vous pourrez alors affecter l'incident à l'utilisateur final approprié.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Configuration par défaut**.



2. Remplissez les champs du formulaire.

Formulaire Configuration DLP par défaut

Nom de la configuration	Champ	Description
Notification d'incident de l'utilisateur final	Période de préavis (jours)	Définissez le nombre de jours après lesquels une notification par e-mail doit être envoyée à l'utilisateur final. Le nombre de jours doit être compris entre 1 et 60 jours.
	Mettre à jour automatiquement l'état parent en fonction des incidents clonés/enfants	Option permettant de mettre à jour automatiquement l'incident de l'état parent en fonction des incidents clonés ou enfants.
Affectation d'incident	Identificateur de l'utilisateur final	Spécifiez le champ à utiliser à partir des données d'incident pour identifier l'utilisateur final. Les valeurs possibles sont les suivantes : ○ **E-mail du propriétaire des données** ○ **Destination** ○ **Fichier créé par** ○ **Fichier modifié par** ○ **Propriétaire du fichier** ○ **Nom d'utilisateur FTP** ○ **Expéditeur**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la configuration	Champ	Description
Réappliquer le comportement des règles de recherche de l'utilisateur final	Quand l'option Nouv. demande choisie pour règles de rech. de l'utilisateur final	Option permettant de réappliquer des règles de recherche d'utilisateur final aux incidents DLP actifs existants. Vous pouvez sélectionner l'une des options suivantes pour postuler à nouveau : ○ **Mettre à jour la valeur Utilisateur final quand le champ est vide** : met à jour la valeur Utilisateur final des incidents DLP actifs existants si ce champ est vide. ○ **Mettre à jour la valeur Utilisateur final** : met à jour la valeur Utilisateur final des incidents DLP actifs existants. ○ **Mettez à jour les valeurs Utilisateur final et Affecté à lorsque les deux champs sont vides** : met à jour les valeurs Utilisateur final et Affecté à des incidents DLP actifs existants si les deux champs sont vides. **Remarque :** Si cette option est sélectionnée, l'option **Mettre à jour la valeur Affecté à lorsque le champ est vide** est automatiquement désactivée dans la section Réappliquer le comportement des règles d'affectation, car elle s'applique aux deux. ○ **Mettez à jour les valeurs Utilisateur final et Affecté à pour tous les incidents DLP actifs** : met à jour les valeurs Utilisateur final et Affecté à pour tous les incidents DLP actifs. **Remarque :** Si cette option est sélectionnée, l'option **Mettre à jour la valeur Affecté à pour tous les incidents DLP actifs** est automatiquement désactivée dans la section Réappliquer le comportement des règles d'affectation, car elle s'applique aux deux.
Réappliquer le comportement des règles d'affectation	Lorsque l'option de Nouvelle demande est choisie pour les règles d'affectation	Option permettant de réappliquer des règles d'affectation aux incidents DLP actifs existants. Vous pouvez sélectionner l'une des options suivantes pour postuler à nouveau :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la configuration	Champ	Description
		○ **Mettez à jour la valeur Affecté à quand le champ est vide.** ○ **Mettez à jour la valeur Affecté à pour tous les incidents DLP actifs.**

3. Sélectionnez le **groupe d'affectation par défaut** dans la section de liste connexe à laquelle tous les incidents DLP sont affectés.
   Cliquez sur **Modifier** pour ajouter le groupe d'utilisateurs. Lorsque vous cliquez sur **Modifier** dans la section de la liste connexe et sélectionnez un élément dans les colonnes **Collections** , puis ajoutez ce délégataire sélectionné aux colonnes Groupe de la page **Modifier les membres** , puis enregistrez la liste.

   Remarque : Vous ne pouvez afficher et sélectionner que les groupes qui ont été affectés au rôle sn_dlir.analyst dans la liste connexe. Vous ne pouvez sélectionner qu'un seul groupe.

4. Cliquez sur **Enregistrer**.

Créer des règles de recherche d'utilisateur final

Vous pouvez créer et configurer des règles de recherche d'utilisateur final et affecter les incidents DLP aux utilisateurs finaux respectifs en fonction de ces règles.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

L'administrateur DLP définit ces règles de recherche d'utilisateur final pour affecter automatiquement les utilisateurs finaux aux incidents DLP en utilisant uniquement le champ d'utilisateur final. La règle de recherche d'utilisateur final DLP vous permet d'affecter l'utilisateur final sur des incidents DLP en fonction de l'identificateur de l'utilisateur final, des attributs personnalisés ou du script.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Règles de recherche d'utilisateur final DLP**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Règle de recherche d'utilisateur final DLP

Champ	Description
Nom	Nom de la règle de recherche de l'utilisateur final.
Actif	Option permettant d'indiquer si la règle de recherche de l'utilisateur final est active.
Ordre d'exécution	La priorité de la règle de recherche de l'utilisateur final. Ce champ indique l'ordre dans lequel les règles de recherche de l'utilisateur final sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle de recherche de l'utilisateur final dotée du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Description	Description unique de la règle de recherche de l'utilisateur final.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle de recherche de l'utilisateur final, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, vous pouvez définir les conditions de cette règle de recherche d'utilisateur final en sélectionnant la condition en tant que **Source d'intégration**, **contient**, **Symantec**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Rechercher un utilisateur final à l'aide de	Option de recherche d'utilisateur final à l'aide du **champ Incident** ou d'un **script**.
Identificateur de l'utilisateur final	Identificateur d'utilisateur final de l'incident DLP. Ce champ s'affiche lorsque le **champ Incident** est sélectionné dans le champ **Rechercher un utilisateur final à l'aide** . Vous pouvez sélectionner un identificateur d'utilisateur final parmi les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **E-mail du propriétaire des données** ○ **Destination** ○ **Fichier créé par** ○ **Fichier modifié par** ○ **Propriétaire du fichier** ○ **Nom d'utilisateur FTP** ○ **Expéditeur** **Remarque :** Les identificateurs d'utilisateur final répertoriés ci-dessus sont configurables à l'aide de la propriété système `sn_dlir.assignment.fields`. Pour plus d'informations, consultez Configurer les paramètres avancés. ○ **Utilisateur personnalisé à partir de l'incident**
Attribut personnalisé	Option permettant de spécifier un attribut personnalisé à partir de l'incident qui fait référence à un utilisateur. Ce champ **s'affiche** uniquement lorsque The est sélectionné dans le champ **Identificateur de l'utilisateur final** .
Script	Vous pouvez utiliser l'éditeur de script pour personnaliser et formater les valeurs de champ lors de la création de la règle de recherche de l'utilisateur final. Par exemple, vous pouvez utiliser le champ d'adresse e-mail pour identifier l'utilisateur final.

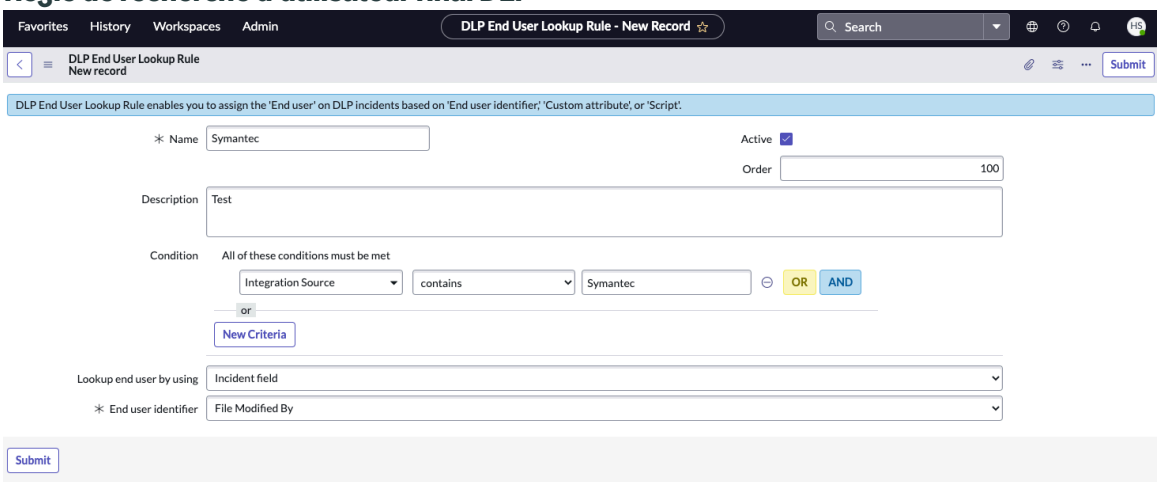
Example

L'exemple suivant montre une règle de recherche d'utilisateur final portant le nom « Symantec ». Le créateur de conditions nécessite « Source d'intégration » comme « Symantec ». **L'option Rechercher un utilisateur final à l'aide** de l'option est définie sur « Champ d'incident » et l'option **d'identificateur de l'utilisateur final** est définie sur « Fichier modifié par ».

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règle de recherche d'utilisateur final DLP



4. Cliquez sur **Envoyer**.
   Vous pouvez également sélectionner une ou plusieurs règles de recherche d'utilisateur final et les réappliquer à tous les incidents DLP existants.
5. Pour réappliquer une règle de recherche d'utilisateur final à tous les incidents DLP existants, cliquez sur **Réappliquer**.

Créer des règles d'affectation

Utilisez cette section pour créer des règles d'affectation. Ensuite, affectez les Data Loss Prevention Incident Response incidents (DLP IR) à des groupes d'utilisateurs, aux utilisateurs finaux, aux gestionnaires ou à un utilisateur à partir d'un incident.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser des règles d'affectation pour affecter des incidents DLP IR à des groupes d'utilisateurs, des utilisateurs finaux ou à des gestionnaires. L'affectation des incidents DLP se produit lorsque les conditions de la règle d'affectation sont remplies.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Règles d'affectation**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de règle d'affectation DLP

Champ	Description
Nom	Nom de la règle d'affectation.
Actif	Option permettant d'indiquer si la règle d'affectation est active.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ordre d'exécution	Priorité de la règle d’affectation. Ce champ indique l’ordre dans lequel les règles d’affectation sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle d’affectation dotée du numéro le plus bas a la priorité la plus élevée. Pour définir l’ordre d’opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Description	Description unique pour cette règle d’affectation.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d’incidents DLP. Pour créer une condition pour la règle d’affectation, sélectionnez l’un des champs d’incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d’autres conditions, cliquez sur **ET** ou **OU**. ○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l’une ou l’autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, supposons que vous créez une règle d’affectation DLP pour un point de terminaison. Vous pouvez spécifier que la source d’analyse de condition est un système de fichiers de point de terminaison qui doit être rempli avant d’affecter un incident. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Affecter à	Affectation à l’un des éléments suivants : ○ Groupe d'utilisateurs ○ Utilisateur final ○ Responsable ○ Utilisateur à partir de l’incident L’affectation se produit lorsque les conditions du générateur de conditions sont remplies.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Groupe d'utilisateurs	Option permettant de rechercher et de sélectionner un groupe d'utilisateurs auquel affecter les incidents DLP. Ce champ s'affiche lorsque Groupe **d'utilisateurs** est sélectionné dans le champ **Affecter à** . **Remarque :** Vous ne pouvez afficher et sélectionner que les groupes auxquels le rôle sn_dlir.analyst a été affecté.
Utilisateur final	Option permettant d'affecter l'incident DLP à l'utilisateur final. L'affectation se produit lorsque les conditions du générateur de conditions sont remplies.
Affecter à l'aide des champs de Gestionnaire	Gestionnaire de l'utilisateur final. Ce champ s'affiche lorsque **le gestionnaire** est sélectionné dans le champ **Affecter à** . Vous pouvez affecter les incidents DLP à un gestionnaire particulier en sélectionnant l'un des champs Gestionnaire, tel que Nom, E-mail, Ville, Numéro d'employé.
Identificateur de l'utilisateur	L'identificateur d'utilisateur de l'incident. Ce champ **s'affiche lorsque l'utilisateur de l'incident** est sélectionné dans le champ **Affecter à** . Vous pouvez sélectionner un identificateur d'utilisateur parmi les suivants : ○ **E-mail du propriétaire des données** ○ **Destination** ○ **Fichier créé par** ○ **Fichier modifié par** ○ **Propriétaire du fichier** ○ **Nom d'utilisateur FTP** ○ **Expéditeur** ○ **Utilisateur personnalisé à partir de l'incident**
Attribut personnalisé	Option permettant de spécifier un attribut personnalisé à partir de l'incident qui fait référence à un utilisateur. Ce champ apparaît uniquement lorsque **l'utilisateur personnalisé de l'incident** est sélectionné dans le champ **Identificateur d'utilisateur** .
Joindre l'évaluation	Option permettant d'indiquer si vous souhaitez joindre une évaluation à l'incident.
État de la réponse pré-évaluation	Option permettant de sélectionner l'état dans lequel l'incident doit se trouver avant que l'utilisateur

Traduction automatique

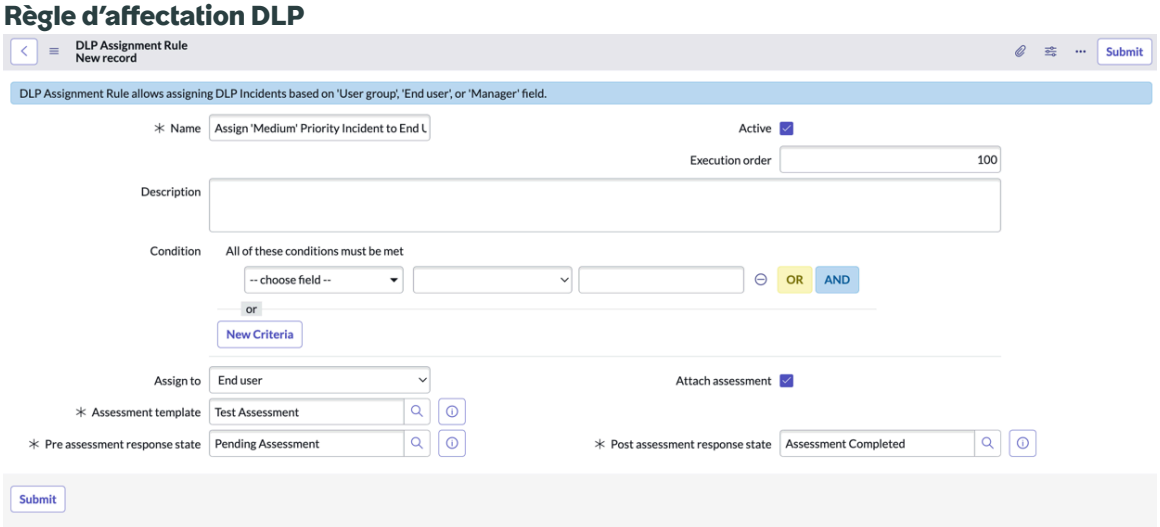
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	final ne réponde. Il peut également s'agir d'un état personnalisé. La valeur par défaut est Évaluation en attente.
État de la réponse post-évaluation	Option permettant de sélectionner l'état dans lequel l'incident DLP doit se trouver après la réponse de l'utilisateur. La valeur par défaut est Évaluation terminée.
Avancés	Option avancée permettant d'identifier l'utilisateur final Ce champ apparaît uniquement lorsque **l'utilisateur personnalisé de l'incident** est sélectionné dans le champ **Identificateur d'utilisateur** . Vous pouvez utiliser l'éditeur de script pour personnaliser et formater les valeurs de champ lors de la création de règles d'affectation afin d'identifier l'utilisateur final. Ensuite, vous choisissez la personne à qui vous souhaitez affecter l'incident DLP, qui peut être un utilisateur final ou le responsable de l'utilisateur final. Par exemple, vous pouvez utiliser le champ d'adresse e-mail pour identifier l'utilisateur final.

Example

L'exemple suivant montre une règle d'affectation intitulée Affecter un incident de priorité « moyenne » à l'utilisateur final. Le générateur de conditions exige que la source d'analyse soit affectée un incident de priorité « moyenne » à l'utilisateur final et que le champ Affecter à soit défini sur l'utilisateur final. Ensuite, vous pouvez rechercher l'adresse e-mail de l'utilisateur final.

Règle d'affectation DLP



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez le champ **Affecter à** dans la section de liste connexe à laquelle tous les incidents DLP sont affectés.
   Cliquez sur **Modifier** pour ajouter le groupe d'utilisateurs. Lorsque vous cliquez sur **Modifier** dans la section de la liste connexe et sélectionnez un élément dans les colonnes **Collections** , puis ajoutez ce délégataire sélectionné aux colonnes Groupe de la page **Modifier les membres** , puis enregistrez la liste.

   Remarque : Vous ne pouvez afficher et sélectionner que les groupes qui ont été affectés au rôle sn_dlir.analyst dans la liste connexe. Vous ne pouvez sélectionner qu'un seul groupe.

5. Cliquez sur **Envoyer**.
   Vous pouvez également sélectionner une ou plusieurs règles d'affectation et les réappliquer à tous les incidents DLP existants.
6. Pour réappliquer une règle d'affectation à tous les incidents DLP existants, cliquez sur **Réappliquer**.

Créer des règles de consolidation des incidents

Créez une règle de consolidation des incidents pour regrouper plusieurs incidents de nature similaire sous un seul incident parent.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer
- sn_dlir.analyst et sn_dlir.analyst_read : afficher (lecture seule)

Pourquoi et quand exécuter cette tâche

L'administrateur DLP définit ces règles de consolidation des incidents pour consolider automatiquement les incidents DLP de même nature sous un incident parent. La règle de consolidation des incidents DLP vous permet de consolider les incidents DLP en fonction de la configuration fournie pour la durée de la consolidation et l'identification de consolidation.

Remarque :

Lorsqu'un incident consolidé est créé, il devient un enfant de l'incident DLP parent. Si la gravité de l'incident consolidé est supérieure à celle du parent, la gravité de l'incident parent est mise à jour pour correspondre à l'incident enfant.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Règles de consolidation des incidents DLP**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de règle d'affectation DLP

Champ	Description
Nom	Nom de la règle de consolidation des incidents.
Actif	Option permettant d'indiquer si la règle de consolidation des incidents est active.
Ordre d'exécution	Priorité de la règle de consolidation des incidents. Ce champ indique l'ordre dans lequel les règles de consolidation des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	incidents sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle de consolidation des incidents dotée du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Description	Description unique de la règle de consolidation des incidents.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle de consolidation des incidents, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, vous pouvez définir les conditions de cette règle de consolidation des incidents en sélectionnant la condition en tant que **Source d'intégration**, **contient**, **Symantec**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Durée de la consolidation	Option permettant de définir la durée de la consolidation de l'incident. Les incidents de cette période ayant les mêmes valeurs pour les champs sélectionnés seront regroupés sous le premier incident. Le premier incident correspondant à cette règle sera l'incident

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	parent et le reste des incidents seront des incidents enfants.
Consolider les incidents par	Sélectionnez le champ d'incident DLP pour consolider les incidents ayant la même valeur dans le champ sélectionné pour différents incidents. Sélectionnez au moins un champ. Sélectionnez au moins un champ.

L'exemple suivant montre une règle de consolidation des incidents intitulée Consolider les incidents pour Symantec Integration. Le créateur de conditions a besoin que la source d'intégration soit Symantec. L'option **Durée de la condition** est définie sur 1 heure et l'option Nom de la politique est sélectionnée pour **Consolider l'incident par**.

Au moment de l'ingestion d'incident Symantec DLP, cette règle est exécutée et, lorsque plusieurs incidents ont le même nom de politique, l'incident est consolidé sous le premier incident ingéré correspondant à cette règle.

4. Cliquez sur **Envoyer**.
   Les incidents consolidés en fonction de la règle de consolidation seront disponibles sous la liste des incidents enfants dans DLP Analyst Workspace.

Créer des règles relatives à la date d'échéance de la réponse

Configurez les règles relatives à la date d'échéance de la réponse pour déterminer le temps que vous souhaitez donner à vos utilisateurs finaux pour répondre aux incidents affectés Data Loss Prevention Incident Response (DLP IR).

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser ce module pour définir les règles de date d'échéance de réponse pour les différents types d'incidents DLP et les règles pour commencer à compter la date d'échéance. Une fois la date d'échéance expirée, les utilisateurs sont informés de l'incident en retard. Vous avez également la possibilité d'escalader l'incident en retard à l'un des éléments suivants :

- Responsable
- Utilisateur personnalisé à partir de l'incident
- Groupe d'utilisateurs

Par exemple, lorsque vous escaladez l'incident en retard à un gestionnaire et que vous avez spécifié un maximum de trois niveaux d'escalade. Le gestionnaire de premier niveau est notifié en premier. Si l'incident est à nouveau en retard, le gestionnaire de deuxième niveau en est informé, suivi du troisième niveau si l'incident est toujours en retard. Si le gestionnaire dispose d'un délégué, le gestionnaire a la possibilité d'affecter l'escalade ou l'incident en retard au délégué.

Vous avez également la possibilité de créer plusieurs règles relatives à la date d'échéance de la réponse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Règles relatives à la date d'échéance de la réponse**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Règle relative à la date d'échéance de la réponse

Champ	Description
Nom	Nom de la règle relative à la date d'échéance de la réponse.
Actif	Option permettant d'indiquer si la règle relative à la date d'échéance de la réponse est active.
Échéance dans (jours)	Nombre de jours d'échéance.
Date d'échéance comptée à partir de	Date de début utilisée pour calculer la date d'échéance. La date d'échéance peut être calculée soit à partir de la première fois où l'utilisateur a été informé de l'incident, soit à partir de la date d'affectation de l'incident.
Notifier avant la date d'échéance	Option permettant d'informer l'utilisateur final de l'incident DLP avant la date d'échéance.
Notifier le (jour avant la date d'échéance)	Nombre de jours avant la date d'échéance lorsque la règle déclenche une notification à l'utilisateur final.
Description	Description unique pour cette règle relative à la date d'échéance de la réponse.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle relative à la date d'échéance de la réponse, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Escalader	Option permettant d'escalader l'incident DLP à quelqu'un si la date d'échéance de la réponse n'a pas été respectée. Pour plus d'informations, voir Ajouter plusieurs utilisateurs pour accéder aux incidents DLP
Escalader un incident en retard à	Option permettant de spécifier si l'incident doit être escaladé à un gestionnaire, à un utilisateur personnalisé ou à un groupe d'utilisateurs. Ce champ s'affiche uniquement lorsque l'option **Escalader** est activée.
Affecter à l'aide de	Spécifiez comment un gestionnaire doit être identifié. Ce champ s'affiche uniquement lorsque le **gestionnaire** est sélectionné dans le champ **Escalader l'incident en retard à** .
Niveaux d'escalades maximums	Option permettant de définir le nombre maximal de niveaux d'escalade pour un gestionnaire et un utilisateur personnalisé. En tant qu'utilisateur Gestionnaire ou Personnalisé, vous pouvez définir n'importe quel nombre de niveaux d'escalade. Par défaut, trois niveaux d'escalade sont fournis. ○ En tant que gestionnaire, vous pouvez définir n'importe quel nombre de niveaux d'escalade en mettant à jour la valeur de ce champ. ○ En tant qu'utilisateur personnalisé, vous pouvez utiliser l'icône + pour définir le nombre souhaité de niveaux d'escalade.
Attribut personnalisé	Option permettant de spécifier un attribut personnalisé à partir de l'incident qui fait référence à un utilisateur. Ce champ **s'affiche uniquement lorsque l'utilisateur personnalisé de l'incident** est sélectionné dans le champ **Escalader l'incident en retard à** .
Groupe d'utilisateurs	Option permettant de rechercher et de sélectionner un groupe d'utilisateurs auquel escalader les incidents DLP. Ce champ s'affiche uniquement lorsque le **groupe d'utilisateurs** est sélectionné dans le champ **Escalader l'incident en retard à** .

Traduction automatique

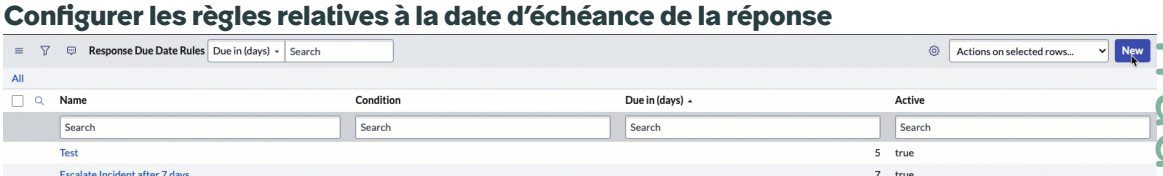
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Vous ne pouvez afficher et sélectionner que les groupes auxquels le rôle sn_dlir.analyst a été affecté.

Example

L'exemple suivant montre la règle relative à la date d'échéance de la réponse pour déterminer le délai que vous souhaitez accorder à vos utilisateurs finaux pour répondre aux incidents affectés Data Loss Prevention Incident Response (DLP). Après la première notification de l'utilisateur final, la date d'échéance de la réponse est dans deux jours. Le générateur de conditions montre que la source d'analyse doit correspondre au système de fichiers du point de terminaison pour procéder à la création de la date d'échéance de la réponse. L'option d'escalade est sélectionnée. L'incident est escaladé au gestionnaire si la date d'échéance de la réponse est dépassée.

Configurer les règles relatives à la date d'échéance de la réponse



4. Cliquez sur **Envoyer**.

Ajouter plusieurs utilisateurs pour accéder aux incidents DLP

Utilisez la fonctionnalité de chaîne d'escalade pour permettre à tous les utilisateurs respectifs impliqués dans l'incident d'accéder aux incidents DLP à partir de la vue de liste, bien que l'incident soit affecté à un autre utilisateur.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.read, sn_dlir.analyst et sn_dlir.analyst_read - Afficher (lecture seule).

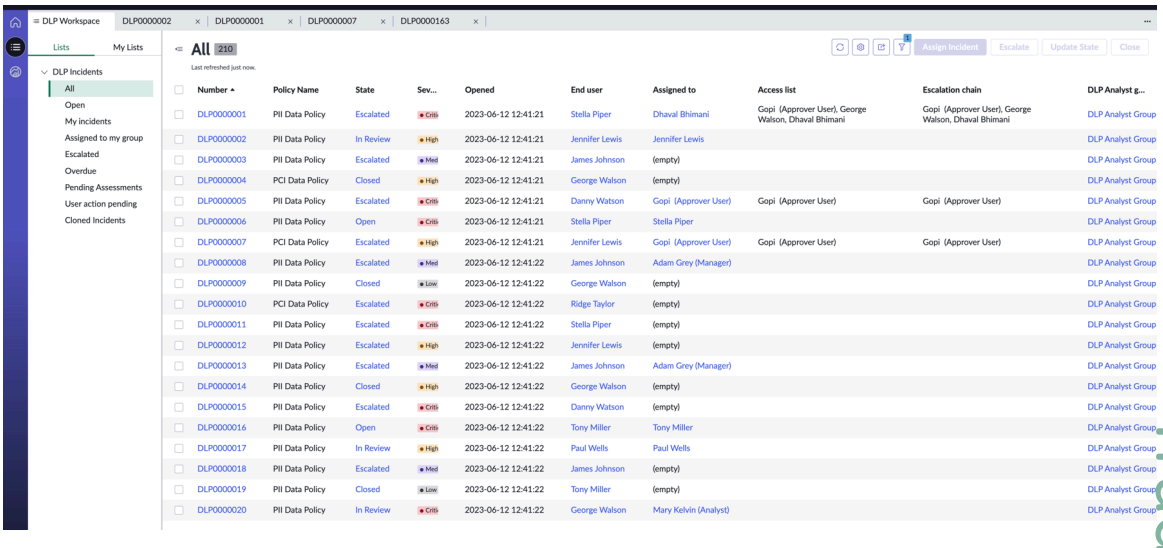
Procédure

1. Accédez à la **DLP** > **Espace de travail de l'analyste DLP**.
   Dans la vue de liste, les utilisateurs et leurs délégués doivent être en mesure d'afficher l'incident DLP sous **l'onglet Incidents escaladés** sur le portail de l'utilisateur final.
2. Ouvrez un incident.
3. Cliquez sur le bouton **Escalader pour escalader** un incident.
4. Sélectionnez l'utilisateur ou le groupe d'utilisateurs dans la liste déroulante.

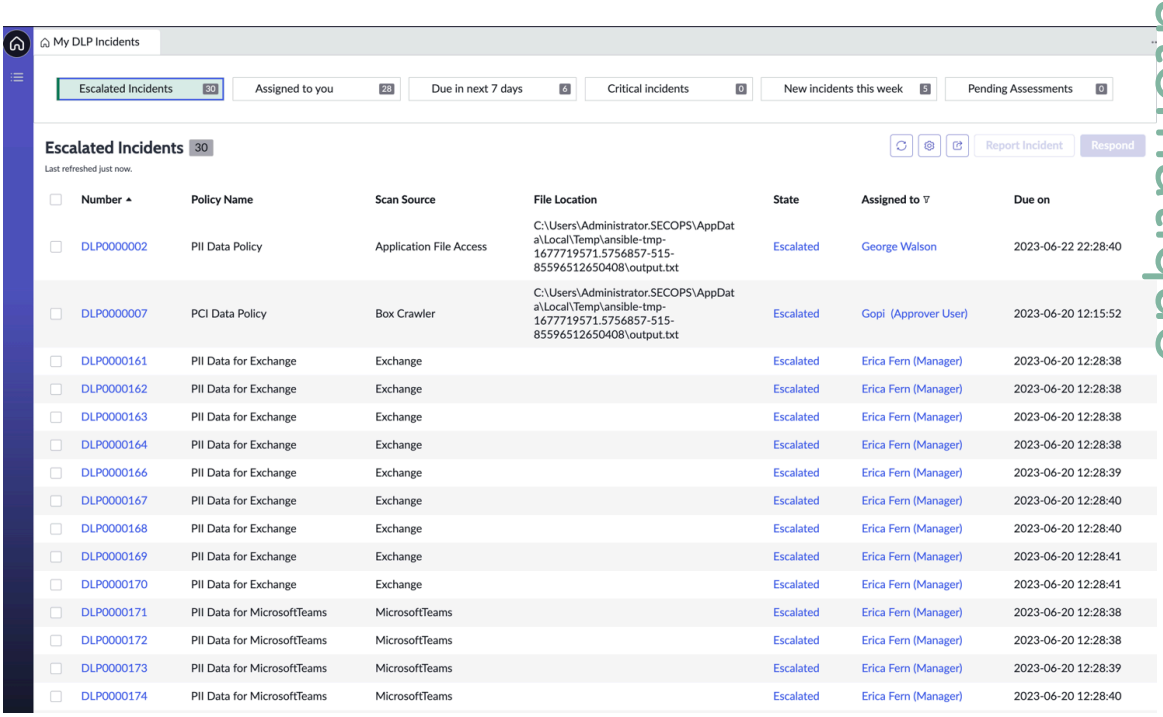
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez ajouter plusieurs utilisateurs à la chaîne d’escalade. Tous les utilisateurs ayant accès sont répertoriés dans la section Détails de la vue de formulaire, ainsi que sous l’onglet **Tous les** incidents. La chaîne d’escalade s’affiche en fonction des paramètres de configuration. Pour plus d'informations, voir Configurer les paramètres avancés



5. Cliquez sur **Envoyer**.
   Une fois l’incident envoyé, l’incident est affecté à un gestionnaire, mais l’utilisateur final peut toujours consulter l’incident.
6. Pour vérifier cela, accédez à **l’espace de travail de l’utilisateur DLP** en tant qu’utilisateur final.
   Tous les incidents qui sont affectés à l’utilisateur final s’affichent.
7. Affichez la liste des incidents escaladés dans la section **Incidents escaladés** .



Vous pouvez également afficher la liste d’accès des utilisateurs sous la colonne **Chaîne d’escalade**de la vue de liste.

8. Ouvrez un incident.
9. Cliquez sur le bouton **Répondre** pour soumettre une réponse à l’incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Sélectionnez la réponse dans la liste déroulante.
11. Cliquez sur **Envoyer**.

Créer des règles d'approbation

Créez des règles d'approbation pour prendre l'approbation de différents niveaux d'utilisateurs approbateurs chaque fois qu'un type avancé d'option de réponse est sélectionné.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

L'administrateur DLP définit ces règles d'approbation pour accorder le consentement sur les demandes émises par les utilisateurs finaux pour l'approbation de type avancé d'option de réponse. L'administrateur DLP peut également définir plusieurs niveaux d'approbation à partir d'ici.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Règles d'approbation DLP**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire de règle d'affectation DLP

Champ	Description
Nom	Nom de la règle d'approbation.
Actif	Option permettant d'indiquer si la règle d'approbation est active.
Ordre d'exécution	La priorité de la règle d'approbation. Ce champ indique l'ordre dans lequel les règles d'approbation sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle d'approbation dotée du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Description	Description unique de la règle d'approbation.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour la règle d'approbation, sélectionnez l'un des champs d'incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, vous pouvez définir les conditions de cette règle de consolidation des incidents en sélectionnant la condition en tant que **Source d'intégration**, **contient**, **Microsoft**.
Applicable aux options de réponses	Option permettant de sélectionner l'option de réponse de type avancé. Vous pouvez sélectionner les multiples options de réponse.
Approbateur	Sélectionnez le type d'utilisateur approbateur que vous souhaitez définir. ○ **Table des utilisateurs** : sélectionnez cette option si vous souhaitez sélectionner l'utilisateur approbateur dans la table Utilisateurs (sys_user). ○ **Liste d'approbation personnalisée** : sélectionnez cette option si vous souhaitez configurer plusieurs niveaux d'approbateur personnalisé pour une seule demande
Identificateur d'approbateur	Ce champ s'affiche lorsque **Table utilisateur** est sélectionnée pour l'option **Approbateur** . Sélectionnez le champ pour identifier l'approbateur dans la table Utilisateur(sys_user).
Nombre de niveaux	Ce champ s'affiche lorsque **Table utilisateur** est sélectionnée pour l'option **Approbateur** . Numéro de fin dans ce champ pour définir les niveaux d'approbation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par exemple, si 3 est ajouté dans le champ Nombre de niveaux et que le responsable est sélectionné dans le champ Identificateur d'approbateur, la demande d'approbation passe à trois niveaux d'approbation.

L'exemple suivant montre la règle d'approbation créée pour l'une des options de réponse avancée. La condition nécessite que le nom de la source d'intégration contienne le mot clé Microsoft qui déclenche ensuite cette configuration.

4. Pour l'option **Approbateur** , sélectionnez **Liste d'approbation personnalisée**.
5. Cliquez sur **Envoyer**.
6. La liste connexe **Niveaux d'approbation** est renseignée dans la vue de formulaire.
7. Dans la section **Niveaux d'approbation** , cliquez sur **Nouveau**.
8. Remplissez les champs du formulaire.

Formulaire de niveau d'approbation

Champ	Description
Nom	Nom du niveau d'approbation.
Actif	Option permettant d'indiquer si le niveau d'approbation est actif.
niveau	Niveau de la règle d'approbation. Ce champ indique l'ordre dans lequel les niveaux d'approbation sont exécutés lorsque deux niveaux ou plus sont configurés. Le niveau d'approbation avec le numéro le plus bas a la priorité la plus élevée. Pour définir le niveau de fonctionnement, saisissez une valeur. Par exemple, 100, 200, 300, etc. La valeur par défaut est 100.
Règle d'approbation	Règle d'approbation pour laquelle vous souhaitez définir cette configuration. Ce champ sera en lecture seule.
Description	Description unique de la règle d'approbation.
Approbations requises	Sélectionnez l'option permettant de définir si l'approbation de tous les utilisateurs/groupes configurés est requise ou uniquement d'un utilisateur.
Approbateurs	Option permettant de sélectionner les approbateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	a. Utilisateurs et groupes : **i. Utilisateurs** : cliquez sur Ajouter ma personne pour ajouter un utilisateur particulier à partir de la liste. Vous pouvez également ajouter un utilisateur à l'aide de son adresse e-mail ou de l'option de recherche. Pour vous ajouter en tant qu'utilisateur auquel les conditions DLP sont applicables, cliquez sur . **ii. Groupes** : cliquez sur l'icône <add_icon> pour ajouter un groupe particulier à partir de la liste. Vous pouvez également ajouter un groupe à l'aide de l'option de recherche. **b. Rechercher à l'aide d'un script** : vous pouvez utiliser l'éditeur de script pour personnaliser et formater les valeurs de champ lors de la création du niveau d'approbation. Par exemple, vous pouvez utiliser le champ d'adresse e-mail pour identifier l'utilisateur approbateur.

9. Cliquez sur **Envoyer**.

Créer des modèles d'instructions de l'utilisateur

Créez et gérez un modèle d'instructions de l'utilisateur pour les incidents DLP afin d'aider les utilisateurs à comprendre les instructions impliquées dans la résolution des incidents et les étapes suivantes impliquées dans le processus de résolution.

Avant de commencer

Le modèle de carte d'instructions de l'utilisateur affiche deux en-têtes différents qui vous fournissent plus d'informations sur un incident spécifique dans la vue de formulaire.

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Lorsqu'un incident est affecté à l'utilisateur final, il peut être demandé à l'utilisateur de connaître les instructions supplémentaires sur la façon de répondre aux incidents, de présenter la terminologie aux utilisateurs et de fournir toute information supplémentaire sur l'incident. Ces modèles peuvent guider les utilisateurs pour fournir une réponse précise aux incidents DLP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Modèles d'instructions de l'utilisateur**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Évaluation de l’incident DLP

Champ	Description
Nom	Nom du modèle d’instruction de l’utilisateur.
Description brève	Description unique de ce modèle d’instruction utilisateur.
Actif	Option permettant d’indiquer si le modèle d’instruction de l’utilisateur est actif.
Ordre d'exécution	Priorité du modèle d’instruction de l’utilisateur de l’incident. Ce champ indique l’ordre dans lequel la commande est exécutée pour évaluer le modèle d’instruction de l’utilisateur lorsqu’un incident est créé. L’option dotée du numéro le plus bas a la priorité la plus élevée. Pour définir l’ordre d’opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Incidents correspondant à la condition	Les incidents qui correspondent aux conditions définies dans le générateur de conditions s’affichent. Ces conditions sont basées sur les données d’incident DLP. Pour créer une condition pour une instruction utilisateur, sélectionnez l’un des champs d’incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d’autres conditions, cliquez sur ET ou OU : Si ET est sélectionné, toutes les conditions doivent être mises en correspondance. Si OU est sélectionné, l’une ou l’autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Concerne	Sélectionnez l'utilisateur ou les groupes d'utilisateurs auxquels le modèle s'applique. Les autres options disponibles sont les suivantes : ○ **Tous les utilisateurs finaux** : cochez cette case si le modèle d'instructions s'applique à tous les utilisateurs. ○ **Tous les réviseurs des incidents escaladés** : cochez cette case si le modèle s'applique à tous les réviseurs des incidents escaladés. ○ **Utilisateurs spécifiques** : cliquez sur l'icône pour ajouter un utilisateur particulier à partir de la liste auquel les conditions d'incident DLP s'appliquent. Vous pouvez également ajouter un utilisateur à l'aide de son adresse e-mail ou de l'option de recherche. Par exemple, Gestionnaire juridique. Pour vous ajouter en tant qu'utilisateur auquel les conditions DLP s'appliquent, cliquez sur l'icône **Ajouter ma personne** . ○ **Groupes d'utilisateurs spécifiques** : cliquez sur l'icône pour ajouter un groupe particulier à partir de la liste auquel les conditions d'incident DLP s'appliquent. Vous pouvez également ajouter un groupe à l'aide de l'option de recherche. Par exemple, les créateurs d'enquêtes.
Modèle d'instructions : Instructions	Ajoutez des instructions dans l'éditeur de texte enrichi avec des variables disponibles au niveau de l'incident.

4. Explorez la section **Modèle d'instructions** , saisissez l'instruction du modèle et ajoutez des informations au niveau de l'incident dans cette section, si nécessaire.
5. Glissez-déplacez les variables requises pour afficher certains champs de manière dynamique.
6. Cliquez sur **Envoyer**.
   Les modèles d'instructions de l'utilisateur sont maintenant créés et vous pouvez cliquer sur n'importe quel en-tête d'instruction utilisateur pour connaître les détails supplémentaires d'un incident DLP.

   Pour plus d'informations, consultez Data Loss Prevention Incident Response Espace de travail de l'utilisateur.

Configurer les instructions de l'utilisateur de l'interface utilisateur DLP

Configurez les messages de l'interface utilisateur du système pour ajouter des en-têtes d'instructions utilisateur détaillés selon vos besoins.

Avant de commencer
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Interface utilisateur du système** > **Messages**.
2. Recherchez **user_instruction_card_heading**.

   Par défaut, user_instruction_card_heading et user_instruction_modal_window_heading sont les deux configurations de message d'interface utilisateur mises en service aux utilisateurs.

3. Cliquez sur l'une des instructions de l'utilisateur pour mettre à jour ou modifier.

Créer des modèles d'e-mail

Créez et gérez les modèles d'e-mail préconfigurés pour l'envoi de notifications à vos utilisateurs finaux, groupes d'utilisateurs ou responsables. Grâce à ces modèles, vous pouvez coacher et communiquer avec vos utilisateurs finaux au sujet des Data Loss Prevention Incident Response incidents (DLP IR).

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

> **Important :** Pour que les analystes puissent afficher les communications par e-mail d'un incident DLP sur le flux d'activité, vous devez ajouter ou ajouter le rôle « sn_dlir.analyst » dans le glide.ui.activity.email_roles de propriété système global.

Pourquoi et quand exécuter cette tâche

Les notifications par e-mail sont classées en fonction des notifications d'incident envoyées aux utilisateurs finaux, des notifications d'escalade envoyées aux gestionnaires ou des notifications de date d'échéance. Vous pouvez envoyer des notifications par e-mail sur les dates d'échéance des incidents DLP, ou même former les utilisateurs finaux sur ce qu'il faut faire lorsque certaines conditions sont remplies dans le filtre des conditions d'e-mail.

Les modèles d'e-mail DLP vous permettent d'envoyer la notification par e-mail pour les utilisateurs finaux, les responsables et les analystes. Vous pouvez configurer les modèles à envoyer par incident ou sous forme de synthèse. L'objet et le corps de votre e-mail peuvent contenir des variables afin que vous puissiez réutiliser votre contenu existant.

DLP fournit les modèles d'e-mail préconfigurés suivants en fonction des catégories :

- **Modèle d'e-mail DLP : notification d'approbation par incident :** Notifiez les utilisateurs de l'approbation de leurs demandes.
- **Modèle d'e-mail DLP : notification d'escalade :** Envoyez des notifications d'escalade aux gestionnaires sous forme de synthèses.
- **Modèle d'e-mail DLP : notification d'approbation en attente :** Notifiez les approbateurs des éléments en attente.
- **Modèle d'e-mail DLP : notification d'annulation de demande d'approbation par incident :**Notifiez les utilisateurs d'une demande d'approbation qui a été annulée par l'équipe d'analystes DLP.
- **Modèle d'e-mail DLP : notification d'achèvement de la réponse de l'utilisateur :** Notifiez l'équipe d'analystes DLP de la réponse soumise par les utilisateurs.
- **Modèle d'e-mail DLP : notification d'incident de l'utilisateur :**Il s'agit d'un modèle par défaut pour la notification de synthèse de l'utilisateur. Envoyez des notifications d'incident aux utilisateurs finaux sous forme de synthèses tous les quelques jours, même s'il n'y a pas

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de nouveaux incidents, afin d'informer les utilisateurs du nombre total d'incidents sur le nom d'un utilisateur particulier. Vous pouvez également envoyer des notifications de synthèse pour informer les utilisateurs des dates d'échéance à venir les plus proches des incidents DLP de gravité critique, élevée, moyenne ou faible.

- **Modèle d'e-mail DLP : notification d'approbation en attente par incident** : notifier les approbations en attente aux approbateurs.
- **Modèle d'e-mail DLP : notification de rejet :** Envoyer une notification de rejet au demandeur.
- **Modèle d'e-mail DLP : notification de la date d'échéance :** Envoyer une notification de date d'échéance de l'incident. Si un incident DLP est affecté à l'utilisateur final et si l'utilisateur final n'a effectué aucune action avant la date d'échéance, une notification par e-mail est envoyée à l'utilisateur final. Vous avez également la possibilité d'escalader l'incident DLP à un gestionnaire, un utilisateur personnalisé ou un groupe d'utilisateurs si la date d'échéance de la réponse n'a pas été respectée.

Remarque : Les notifications de dates d'échéance doivent être sous forme de synthèses.

- **Modèle d'e-mail DLP : notification de réponse utilisateur par incident :** Notifiez les analystes de la réponse soumise aux utilisateurs par incident.
- **Modèle d'e-mail DLP : notification d'escalade par incident :** Notifiez les gestionnaires des escalades par incident.
- **Modèle d'e-mail DLP : notification par incident de l'utilisateur :** Notifiez les utilisateurs de l'affectation par incident.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Modèles d'e-mail**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Modèle d'e-mail DLP

Champ	Description
Nom	Donnez un nom au modèle d'e-mail.
Actif	Option permettant d'indiquer si le modèle d'e-mail DLP est actif. Si cette option n'est pas activée, les notifications ne sont pas envoyées pour ce modèle d'e-mail.
Catégorie	Catégorie de notification par e-mail. DLP prend en charge les options suivantes : ○ **Notification d'incident aux utilisateurs finaux** : envoyée lorsque les incidents sont affectés aux utilisateurs finaux. ○ **Notification d'escalade aux responsables** : envoyée lorsque la date d'échéance de la réponse est dépassée ou affectée manuellement au gestionnaire via le portail DLP Ops. ○ **Notification de date d'échéance** : envoyée lorsque la date d'échéance de la réponse est dépassée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **Notification de réponse de l'utilisateur aux analystes** : envoyée lorsque l'utilisateur final prend des mesures sur l'incident DLP. ○ **Notification d'approbations en attente** : informez les approbateurs des éléments en attente. ○ **Notification d'approbation au demandeur** : informe les utilisateurs de l'approbation de leurs demandes. ○ **Rejeter la notification au demandeur : informez** les utilisateurs du rejet de leurs demandes. ○ **Notification d'annulation au demandeur** : notifiez les utilisateurs de l'annulation de leurs demandes.
Type	Option permettant d'indiquer si l'e-mail est envoyé par incident ou sous forme de synthèse. **Remarque :** Si vous avez sélectionné **Notification de date d'échéance** dans le champ **Catégorie** , vous ne pouvez utiliser que des synthèses. Sélectionnez cette option.
Description	Description unique pour ce modèle d'e-mail.
Ordre d'exécution	Priorité du modèle d'e-mail. Ce champ indique l'ordre dans lequel les modèles d'e-mail sont exécutés lorsque deux modèles d'e-mail ou plus partagent les conditions de déclenchement. Le modèle d'e-mail doté du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Condition du modèle	Options dans les conditions du modèle qui sont basées sur la table d'incidents DLP. Vous pouvez sélectionner l'un des champs d'incident pour créer la condition de déclenchement du modèle d'e-mail. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**. ○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utilisateurs cibles	Ciblez les utilisateurs pour le modèle lorsque les conditions sont remplies. Les utilisateurs cibles peuvent être l'un des suivants : ○ **Tous les récipiendaires** : Envoyez l'e-mail aux utilisateurs cibles. ○ **Destinataires dans le groupe :** Envoyez l'e-mail uniquement aux destinataires d'un groupe particulier à l'aide de l'option de filtre. ○ **Destinataires correspondant aux critères** : Envoyez l'e-mail aux utilisateurs cibles qui correspondent aux critères. Vous pouvez utiliser le filtre pour explorer les utilisateurs cibles en fonction des conditions. Par exemple, la ville.

Modèle d'e-mail	Modèle d'e-mail que vous pouvez sélectionner. Vous pouvez définir les variables à réutiliser contenu existant à ajouter à la notification par e-mail.
	Les champs **Catégorie** et **Type** déterminent les variables disponibles pour la sélection. Par exemple, supposons que la catégorie d'e-mail est définie sur notification d'incident et que le type d'e-mail est une synthèse, alors les variables de sélection sont des champs de synthèse pour prendre en charge l'accumulation de plusieurs incidents DLP.
	Voici un exemple HTML du corps de l'e-mail de chaque modèle d'e-mail :
	○ **Modèle par défaut pour la notification d'approbation par incident** :
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	`- Date protection team`
	○ **Notification d'annulation de demande d'approbation par incident**
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	`No action is required from you at this point. Data protection team will contact you for any further information required.`
	`- Data protection team`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description

	○ **Modèle par défaut pour la notification de date d'échéance** :
	`Dear ${target_user.name},`
	
	`Following incidents require your response.`
	
	`${due_days_table}`
	
	`- Data protection team`
	
	○ **Modèle par défaut pour la notification par incident de l'utilisateur** :
	`Dear ${assigned_to.name},`
	
	`DLP Incident ${number} is assigned to you.`
	
	`Please review and submit your response.`
	
	`- Data protection team`
	
	○ **Modèle par défaut pour la notification d'incident par l'utilisateur** :
	`Hello ${target_user.name},`
	
	`You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication.`
	
	`Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}.`
	
	`Please log in to the ${link_to_dlp_portal} and submit your response.`
	
	`- Data protection team`
	
	○ **Modèle par défaut pour l'escalade : synthèse** :
	`Hi ${target_user.name},`
	
	`The following data security incidents have been escalated to you due to lack of response from the assignees.`
	
	`Please login to the incident response workspace to review the incidents and submit your response.`
	
	`${overdue_table}`
	
	`- Data protection team`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description

	○ **Modèle par défaut pour l'escalade - Par incident** :
	`Dear ${assigned_to.name},`
	
	`Data security incident ${number} has been escalated to you.`
	
	`Please review and submit your response or assign the incident back to the user.`
	
	`- Data protection team`
	
	○ **Modèle par défaut pour la notification d'approbation en attente** :
	`Dear ${approver.first_name},`
	
	`Your approval is required for a few requests on data security incidents.`
	
	`Please login to the workspace here and review the requests.`
	
	`- Data protection team`
	
	○ **Modèle par défaut pour la notification d'approbation en attente par incident** :
	`Dear ${Approver},`
	
	`Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}.`
	
	`Please visit this here to approve or reject the request.`
	
	`- Data Protection Team`
	
	○ **Modèle par défaut pour la notification de rejet par incident** :
	`Dear ${respondent.first_name} ${respondent.last_name},`
	
	`This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected.`
	
	`Please review the incident here.`
	
	`- Data protection team`
	
	○ **Modèle par défaut pour la notification de réponse par utilisateur d'incident** :

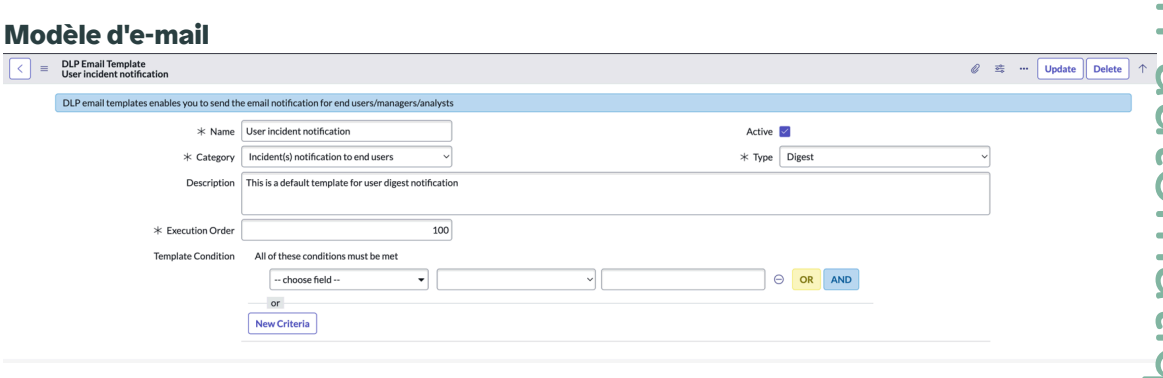
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Hi ${assigned_to.name}, This is to inform you that a response has been submitted for the DLP Incident ${number}. ○ **Modèle par défaut pour la notification d'achèvement de la réponse de l'utilisateur** : Hello ${target_user.name}, This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication. Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.

Example

L'exemple suivant montre le modèle d'e-mail DLP avec les utilisateurs cibles définis comme tous les destinataires.

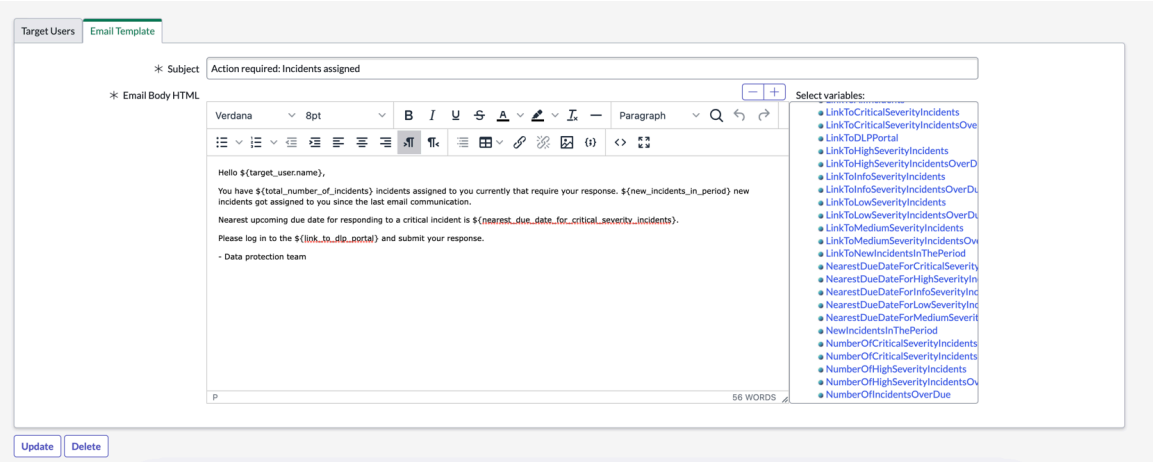


L'exemple suivant montre un modèle d'e-mail avec l'objet « Notification d'incident de l'utilisateur » et une variable *`new_incidents_in_period`*. Le corps de l'e-mail contient plusieurs variables ajoutées à partir de la colonne Sélectionner des variables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de modèle d'e-mail



4. Cliquez sur **Envoyer**.

Résultats

L'utilisateur final reçoit un e-mail de notification de synthèse avec tous les champs de variables sélectionnés dans le modèle.

Créer un déclencheur SLA Data Loss Prevention Incident Response

Créez une condition de Data Loss Prevention Incident Response déclenchement de SLA permettant une réponse rapide et efficace à un incident lorsqu'il est déclenché.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, mettre à jour et supprimer des déclencheurs SLA DLP
- sn_dlir.analyst.read : lire la table de déclencheurs.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Déclencheurs de SLA**.
2. Sélectionnez **Nouveau** pour créer le déclencheur de SLA.

Champ	Description
Nom	Nom du déclencheur
Ordre	Ordre dans lequel le déclencheur est pris en compte.
Actif	Option permettant d'évaluer le déclencheur de SLA.
Déclencher lorsqu'un incident DLP est mis à jour	Option permettant d'évaluer la condition de déclenchement à chaque mise à jour de l'incident DLP.

3. Configurez une condition en sélectionnant l'enregistrement de règle et en définissant les conditions dans le champ **Condition de déclenchement** .
   Par exemple, la condition de déclenchement pour définir des SLA sur des incidents DLP à partir d'une source d'analyse d'e-mail serait **[Source de l'analyse][est][SMTP d'e-mail].**
4. Sélectionnez **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Une fois qu'un enregistrement SLA de tâche est créé pour un Data Loss Prevention Incident Response incident, l'onglet Enregistrements SLA devient visible pour cet incident particulier dans l'espace de travail. Cet onglet vous permet d'utiliser un système SLA pour la tâche de votre organisation.

Créer une définition de Data Loss Prevention Incident Response SLA

Créez une Data Loss Prevention Incident Response définition de SLA décrivant les conditions et la durée de réponse aux violations de données. L'établissement d'attentes et de protocoles clairs permet de garantir une réponse rapide aux incidents, de minimiser les dommages potentiels et d'améliorer les stratégies globales de protection des données.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, mettre à jour et supprimer des définitions de SLA DLP.
- sn_dlir.analyst.read : lire les définitions de SLA DLP.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Définitions de SLA**.
2. Créer une définition de SLA.
   Pour obtenir une description des valeurs de champ, consultez la rubrique Formulaire de définition de SLA DLP.
3. Sélectionnez **Soumettre**.

> **Remarque :** Les règles de date d'échéance, les escalades et les définitions de SLA s'excluent mutuellement. Une définition de SLA détermine principalement quand un SLA particulier commencera à entrer en vigueur, à s'arrêter, à se mettre en pause ou à être déclenché.

Créer des évaluations

Créez et gérez des évaluations pour permettre aux utilisateurs finaux de répondre aux incidents DLP. Vous pouvez utiliser les évaluations pour recueillir des informations sur les données sensibles exposées ou divulguées à la suite des incidents DLP.

Créer et gérer des évaluations pour les incidents

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Les évaluations des incidents DLP vous aident à identifier les menaces et vulnérabilités potentielles pour vos données en fonction de la réponse de l'utilisateur final. Vous pouvez utiliser ces informations pour déterminer les lacunes, les préoccupations et les attentes existantes de vos utilisateurs finaux.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Évaluations**.
2. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Remplissez les champs du formulaire.

Évaluation de l'incident DLP

Champ	Description
Nom	Nom de l'évaluation de l'incident DLP.
Actif	Option permettant d'indiquer si l'évaluation de l'incident DLP est active.
Description	Description unique pour cette évaluation d'incident DLP.
Introduction d'évaluation	Fournissez une introduction ou un contexte pour votre évaluation. Vous pouvez également utiliser des variables de la section Sélectionner des variables pour afficher dynamiquement certains champs.

4. Cliquez sur **Envoyer**.
5. Après avoir créé une évaluation, ouvrez-la, puis cliquez sur **Concepteur d'évaluation**.
6. Dans la section Nouvelle évaluation, sélectionnez un type de question d'évaluation sous la section Contrôles.
7. Glissez-déplacez le type de question d'évaluation requis sous la section Nouvelle évaluation.
   Par exemple, vous pouvez glisser-déposer le contrôle **Choix** sous la section Nouvelle évaluation ou Nouvelle catégorie.
8. Pour ajouter d'autres catégories pour l'évaluation, cliquez sur l'icône  .
9. Pour modifier une catégorie existante, cliquez sur l'icône  .
10. Après avoir créé les différentes questions d'évaluation pour la première fois, cliquez sur **Enregistrer**, puis sur **Publier**.

Créer des règles pour les options de réponse aux incidents

Créez les règles d'option de réponse aux incidents que l'utilisateur final ou l'analyste peut utiliser lors de la réponse à un incident.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le type de réponse qu'un utilisateur final doit effectuer en fonction du type d'incident DLP. L'application DLP Incident Response du système de base offre les options de réponse suivantes aux utilisateurs :

- Évaluation terminée
- Contenu supprimé
- Supprimer le fichier
- Fichier chiffré
- Contenu masqué

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Signaler un faux positif
- Signaler un propriétaire incorrect
- Requis pour le processus business
- Droits révisés

Par exemple, supposons qu'un utilisateur final signale un incident DLP comme faux positif. L'état de cet incident est alors automatiquement marqué comme fermé, car l'état cible que vous avez configuré est fermé.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Règles de l'option de réponse aux incidents**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Règles de l'option de réponse aux incidents

Champ	Description
Nom	Nom de l'option de réponse aux incidents.
Actif	Option permettant d'indiquer si l'option de réponse aux incidents est active.
Ordre d'exécution	Priorité de l'option de réponse aux incidents. Ce champ indique l'ordre dans lequel les options de réponse aux incidents sont exécutées lorsque deux options de réponse aux incidents ou plus partagent les conditions de déclenchement. L'option de réponse aux incidents dotée du numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Description	Description unique de cette option de réponse aux incidents.
État cible par défaut	État cible par défaut que vous avez configuré.
Condition	Conditions dans le générateur de conditions. Ces conditions sont basées sur la table d'incidents DLP. Pour créer une condition pour les options de réponse aux incidents, sélectionnez l'un des champs d'incident. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** :

Traduction automatique

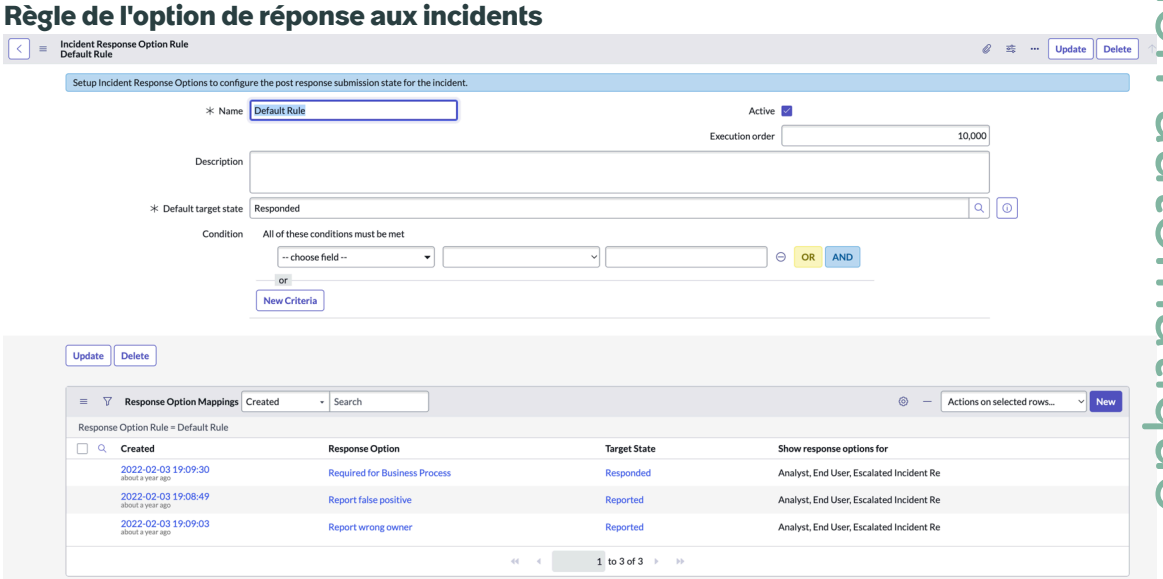
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.

Example

L'exemple suivant montre la configuration d'action de l'utilisateur final pour un point de terminaison. La condition exige que la source d'analyse soit un système de fichiers de point de terminaison qui déclenche ensuite cette configuration d'action de l'utilisateur final. Le mappage montre que le rapport de propriétaire erroné, le rapport de faux positif et le fichier supprimé sont les options de réponse disponibles pour l'utilisateur final.

Règle de l'option de réponse aux incidents



4. Dans la section **Mappages des options de réponse** , cliquez sur **Nouveau**.
5. Remplissez les champs du formulaire.

Formulaire Mappage d'options de réponse

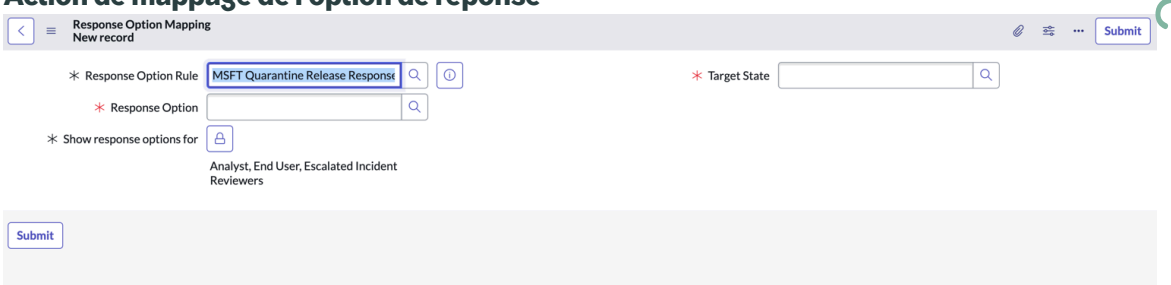
Règle de l'Option de réponse	Nom de la règle d'option de réponse aux incidents. Par exemple, SharePoint implique que la source d'analyse est SharePoint. Vous pouvez saisir le nom de la réponse à un incident ou effectuer une recherche à l'aide de la fonction de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option en matière de réponse	Option permettant de sélectionner l'option de réponse. Vous pouvez soit entrer l'option de réponse, soit effectuer une recherche à l'aide de la fonction de recherche.
État cible	État cible de l'incident DLP une fois que l'utilisateur final a sélectionné l'action appropriée. **Remarque :** **a.** Le champ **État cible s'affiche** uniquement lorsque vous sélectionnez **l'option de réponse** de **type : Basique**. Pour plus d'informations sur la configuration des types d'état cible, reportez-vous à la section Configurer l'option de réponse pour vos incidents DLP. **b.** Lorsqu'une option de réponse de **type avancé** est sélectionnée, vous ne pouvez pas définir l'état cible et elle est masquée. L'état cible est affecté en fonction de l'état personnalisé configuré à partir du flux secondaire du concepteur de flux.
Afficher les options de réponse pour	Option permettant de déterminer les rôles d'utilisateur pour lesquels afficher les options de réponse. Vous pouvez choisir entre **Analyste**, **Utilisateur final** et **Analystes réviseurs escaladés à l'aide** de l'option de déverrouillage. Vous êtes autorisé à choisir un ou tous les rôles.

Action de mappage de l'option de réponse



6. Cliquez sur **Envoyer**.

Configurer l'option de réponse pour vos incidents DLP

Utilisez cette fonctionnalité pour configurer le type de réponse qu'un utilisateur final ou analyste doit effectuer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

L'application DLP Incident Response du système de base fournit les options de réponse suivantes :

1. Évaluation terminée
2. Contenu supprimé
3. Supprimer le fichier
4. Fichier chiffré
5. Contenu masqué
6. Signaler un faux positif
7. Signaler un propriétaire incorrect
8. Demander la sortie de quarantaine de l'e-mail

   Remarque : Cette option est disponible pour les enregistrements DLP Microsoft Exchange.

9. Requis pour le processus business
10. Droits révisés

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Options de réponse**.

   Par défaut, le système de base offre deux types d'options de réponse :

   a. **De base** : option de réponse manuelle soumise par l'utilisateur.

   b. **Avancé** : une option de réponse automatisée déclenche un sous-flux de Flow Designer lorsque l'utilisateur soumet l'option de réponse.

2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire d'option de réponse de type : basique

Champ	Description
Nom	Entrez le nom de l'option de réponse aux incidents.
Type	Option permettant de sélectionner le type d'option de réponse.

Formulaire d'option de réponse de type : Avancé

Champ	Description
Nom	Entrez le nom de l'option de réponse aux incidents.
Type	Option permettant de sélectionner l'option de réponse. Par défaut, ce champ affiche les deux types d'options suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **De base** : lorsque vous sélectionnez cette option lors de la création d'une nouvelle option de réponse, vous devrez peut-être ajouter un nom d'option de réponse et le type. ○ **Avancé** : lorsque vous sélectionnez cette option, vous pouvez sélectionner les champs suivants : ▪ **Flux** : sélectionnez le flux secondaire du concepteur de flux. ▪ **Nécessite Serveur MID** : cochez cette case si le flux sélectionné utilise le Serveur MID.
Flux	Sélectionnez le flux de Concepteur de flux requis pour activer l'application MID et l'aptitude MID. Lorsque vous créez un flux secondaire pour l'option de réponse, ajoutez les entrées de flux secondaires suivantes : **a. Nom** : ▪ dlp_incident ▪ mid_server_capability ▪ mid_server_application **b. Type** : ▪ Référence (vers la table d'incidents DLP) ▪ ID système pour l'application Serveur MID et l'aptitude de Serveur MID
Nécessite un serveur MID	Option permettant de déterminer cette configuration de Serveur MID. En cochant les cases **Exige un serveur MID** , **Application de Serveur MID** et **Option de Serveur MID** , vous pouvez configurer l'application MID et l'option MID. **Remarque :** En fonction de la configuration de l'application et de l'aptitude de Serveur MID Server, et si un MID est en cours d'exécution, seule l'option Réponse sera visible dans l'espace de travail.
Application de serveur MID	Sélectionnez l'application de Serveur MID requise dans la liste déroulante.
Capacité du serveur MID	Sélectionnez l'option Serveur MID requise dans la liste déroulante.

Traduction automatique

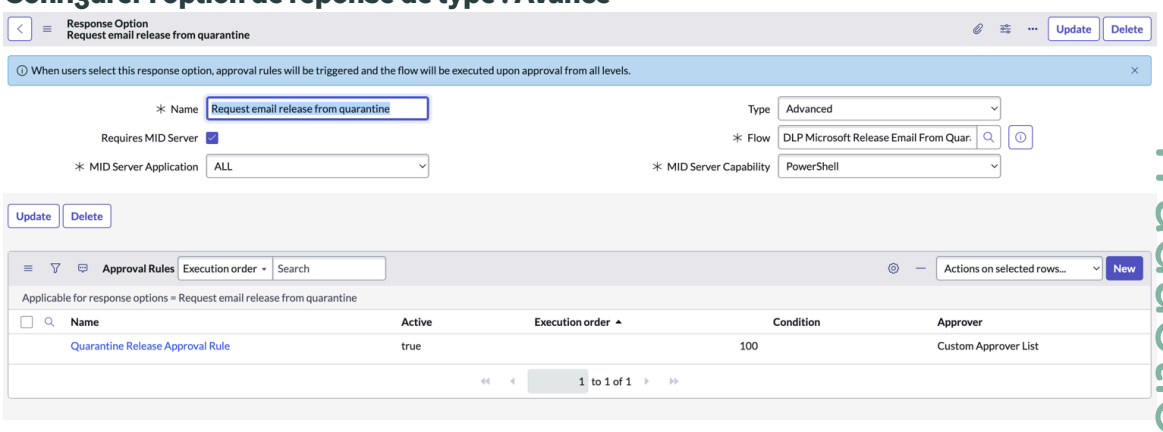
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : S’il n’y a pas de Serveur MID disponible pour l’aptitude de Serveur MID sélectionnée, l’option de réponse ne sera pas visible. Si vous voulez un serveur MID spécifique dans la liste, vous devez configurer l’application MID et l’afficher dans la liste. Au moins un serveur MID configuré doit être opérationnel à partir des applications MID sélectionnées et doit disposer de l’aptitude de serveur MID sélectionnée.

4. Cliquez sur **Envoyer**.

Remarque : Si vous **créez un type** avancé d’option de réponse, la liste connexe **Règles d’approbation** est remplie pour que vous puissiez configurer la règle d’approbation de cette nouvelle option de réponse. Pour plus d'informations, consultez Créer des règles d’approbation.

Configurer l’option de réponse de type : Avancé



Créer des configurations de graphique des âges

Configurez le tableau des âges qui s’affiche dans le Data Loss Prevention Incident Response portail (DLP IR) Ops. Ce graphique montre le nombre d’incidents ouverts par nombre de jours.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Configuration du graphique des âges**.
2. Examinez les entrées du tableau des âges dans la table suivante et personnalisez les entrées en fonction de votre environnement.

Formulaire de configurations du graphique des âges DLP

Nom	Condition
0 à 30 jours	Âge de l’incident ouvert compris entre 0 et 30 jours.
31 à 60 jours	Âge de l’incident ouvert, entre 31 et 60 jours.
61 à 90 jours	Âge de l’incident ouvert, entre 61 et 90 jours.
90 jours et plus	Âge de l’incident ouvert qui est de plus de 90 jours.

3. Ajoutez une nouvelle configuration de graphique des âges en cliquant sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans le champ Nom, entrez un **nom** pour la configuration du graphique des âges DLP.
5. Définissez les conditions de configuration du graphique des âges DLP.

   a. Pour ajouter des conditions, cliquez sur **ET** ou **OU**.
      - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
      - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

      Remarque : Les conditions du générateur de conditions sont sensibles à la casse.

   b. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**.

6. Cliquez sur **Envoyer**.

Créer des configurations de délégués d'utilisateurs

Empêchez certains cadres de l'organisation de recevoir des notifications sur les incidents qui leur sont affectés ou qui leur sont remontés.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Imaginez un scénario dans lequel le cadre est un utilisateur qui appartient à un groupe de direction ou de direction. Le cadre ne doit pas recevoir d'e-mails concernant l'affectation ou l'escalade d'un incident. Un utilisateur délégué peut alors prendre les mesures nécessaires au nom de la direction.

Une fois qu'un utilisateur a affecté une personne particulière, Henry, en tant que délégué, un autre utilisateur ne peut plus affecter Henry en tant que délégué. De même, un délégué ne peut pas affecter un autre utilisateur en tant que délégué.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Configuration du délégué**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Configuration du délégué

Champ	Description
Utilisateur	Nom de l'utilisateur qui a besoin d'un délégué pour les incidents DLP.
Délégué	Nom de l'utilisateur qui peut répondre à l'incident DLP au nom de l'utilisateur final d'origine.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer des règles d'identification des récidivistes

Créez des règles d'identification des récidivistes pour identifier les utilisateurs qui répètent le même problème plusieurs fois.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Vous pouvez identifier les récidivistes à l'aide de certaines règles ou critères. Data Loss Prevention Incident Response fournit des champs que vous pouvez utiliser pour identifier les récidivistes.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Règles d'identification des récidivistes**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Règles d'identification des récidivistes

Champ	Description
Nom	Nom de la règle d'identification des récidivistes.
Ordre d'exécution	Priorité des règles d'identification des récidivistes. Ce champ indique l'ordre dans lequel les règles d'identification des récidivistes sont exécutées lorsque deux règles ou plus partagent les conditions de déclenchement. La règle d'identification des récidivistes avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Description brève	Description unique de cette règle d'identification des récidivistes.
Condition	Conditions du générateur de conditions basées sur la table d'incidents DLP. Vous pouvez sélectionner l'un des champs d'incident pour créer la condition de déclenchement de la règle d'identification des récidivistes. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** :

Traduction automatique

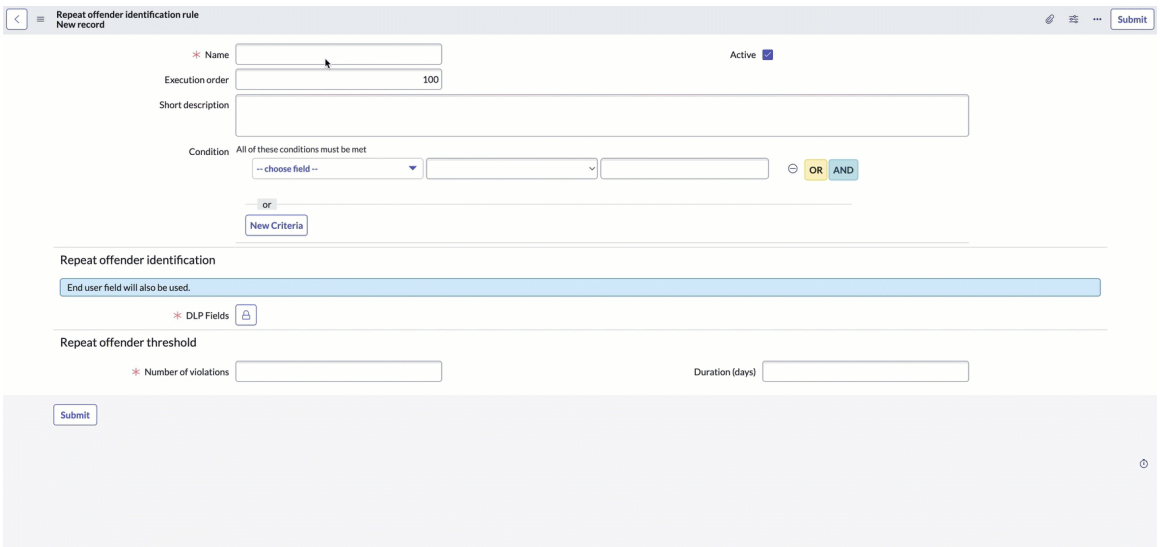
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Champs DLP	Identifiez les récidivistes en fonction des champs DLP requis. Cliquez sur  côté des champs DLP pour afficher la liste des champs DLP disponibles. Sélectionnez les champs DLP que vous souhaitez utiliser dans la colonne Disponible et déplacez-les vers la colonne Sélectionné. Par exemple, vous pouvez sélectionner les champs**Nom du fichier** et **Propriétaire du fichier** dans la colonne Disponible et les déplacer vers la colonne Sélectionné. Ensuite, vous pouvez identifier les récidivistes en fonction des champs **Nom du fichier** et **Propriétaire du fichier** . Ainsi, si un utilisateur dépasse le seuil de récidive (nombre d'infractions et durée), et si le même utilisateur correspond aux champs DLP, cet utilisateur particulier est identifié comme récidiviste.
Nombre d'infractions	Définissez la valeur limite du seuil de récidive. Une fois que l'utilisateur a répété les mêmes actions et dépassé le nombre spécifié d'infractions, il est identifié comme récidiviste.
Durée (en jours)	Définissez la limite du seuil de récidive sous forme de jours. Une fois que l'utilisateur a répété les mêmes actions et dépassé la durée seuil, il est identifié comme récidiviste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identifier les récidivistes



4. Cliquez sur **Envoyer**.

Créer des champs de données d'incident supplémentaires

Créez vos champs de données d'incident supplémentaires pour les incidents DLP. Vous pouvez créer différents types de champs de données d'incident supplémentaires tels que chaîne, numéro, case à cocher, choix, date et heure, et les utiliser dans les formulaires d'incident DLP.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Important : Les champs de données d'incident supplémentaires pour les incidents DLP ne sont pris en charge que sur la version San Diego ou ultérieure.

Pourquoi et quand exécuter cette tâche

Les champs de données d'incident supplémentaires sont associés à des restrictions de niveau de champ. Par conséquent, s'il existe des restrictions de niveau de champ, elles s'appliquent aux champs de données d'incident supplémentaires sur le portail des opérations DLP et le portail de l'utilisateur final.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Champs de données d'incident supplémentaires**.
2. Créez des champs de données d'incident supplémentaires en cliquant sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire Champs de données d'incident supplémentaires DLP

Champ	Description
Nom	Nom des champs de données d'incident supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

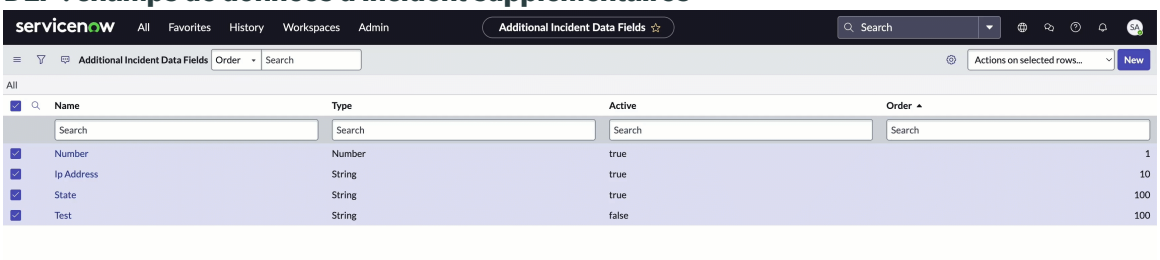
Champ	Description
Type	Option permettant de sélectionner le type de champs de données d'incident supplémentaires. Vous pouvez choisir l'un des types suivants : ○ **Chaîne** ○ **Numéro** ○ **Case à cocher** ○ **Choix** Si vous sélectionnez le type Champs de données d'incident supplémentaires comme **choix**, après avoir créé les champs de données d'incident supplémentaires, vous pouvez définir les options de choix des champs de données d'incident supplémentaires. Pour créer une option de choix de champs de données d'incident supplémentaires : **a.** Ouvrez les champs de données d'incident supplémentaires requis. **b.** Dans la section Options du champ de choix personnalisé, cliquez sur **Nouveau**. **c.** Dans le champ Nom de l'option, définissez le nom de l'option requis. **d.** Cliquez sur **Envoyer**. ○ **Date** ○ **Date/Heure** **Remarque :** Une fois que vous avez sélectionné un type pour vos nouveaux champs de données d'incident supplémentaires, vous n'êtes pas autorisé à le modifier. Si vous souhaitez modifier le type, vous devez créer à nouveau des champs de données d'incident supplémentaires avec le type requis.
Ordre	Option permettant de choisir l'ordre dans lequel les champs de données d'incident supplémentaires doivent être affichés. Vous pouvez définir la valeur d'ordre pour chaque champ de données d'incident supplémentaire. Les champs de données d'incident supplémentaires sont triés en fonction des valeurs d'ordre que vous définissez. Par défaut, les champs de données d'incident supplémentaires sont triés par ordre croissant. Vous pouvez trier les champs de données d'incident supplémentaires par ordre décroissant en cliquant sur la colonne **Ordre** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Option permettant d’indiquer si les champs de données d’incident supplémentaires sont actifs.
Description	Description des champs de données d’incident supplémentaires que vous avez créés.

DLP : champs de données d'incident supplémentaires



4. Cliquez sur **Envoyer**.

Formulaire de définition de SLA DLP

Descriptions des champs du formulaire de définition de SLA DLP utilisé pour créer un enregistrement SLA.

Champ	Description
Nom	Nom de la définition.
Type	Type d’accord, qui dans ce cas est un SLA.
Cible	Cible utilisée pour le filtrage, la recherche et la génération de rapports sur l’accord en cours de définition. Les options disponibles sont les suivantes : • Aucun • Réponse • Résolution
Table	Table qui détermine les enregistrements suivis par le SLA, qui doivent être Tâche SLA DLP [sn_dlir_incident_sla_task].
Flux	Flux à exécuter lorsque la définition de SLA se lie à un enregistrement de tâche, qui doit être le flux SLA par défaut.
Type de durée	Méthode de calcul de la durée du SLA. Les options disponibles sont les suivantes : • Durée spécifiée par l'utilisateur • 2 jours ouvrables avant 16h • 3 jours ouvrables avant 16h • Violation à la date d’échéance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	• Fin du jour ouvrable suivant • Jour ouvrable suivant à 16h
Durée	Durée pendant laquelle le SLA s'exécute avant d'être marqué comme rompu. Ce champ n'est disponible que lorsque la durée spécifiée par l'utilisateur est sélectionnée dans **Type de durée**.
Source du calendrier	Calendrier à utiliser lors de la création des SLA de tâche.
Planifier	Heures pendant lesquelles le compteur du SLA tourne. Cet ensemble de calendriers est défini dans la configuration de base.
Source du fuseau horaire	Source du fuseau horaireà utiliser lors de la création des SLA de tâche. Les options disponibles sont les suivantes : • Le fuseau horaire de l'appelant • Fuseau horaire de la définition de SLA • Le fuseau horaire de l'emplacement CI • Le fuseau horaire d'emplacement de la tâche • Le fuseau horaire de l'emplacement de l'appelant
Actif	Option permettant d'appliquer le déclenchement lorsque la condition de démarrage est remplie.
Onglets	
Condition de démarrage	Condition qui lance le minuteur SLA et active le SLA.
Condition de pause	Conditions sous lesquelles le SLA est suspendu, augmentant le temps total écoulé.
Condition d'annulation	Conditions en vertu desquelles le SLA est annulé.
Condition de réinitialisation	Conditions dans lesquelles le SLA actif est terminé et un nouveau SLA est établi lorsque la valeur d'un champ sur l'enregistrement de tâche change, atteint une certaine valeur ou diffère d'une certaine valeur de l'enregistrement. Par exemple, supposons que la valeur du champ **Emplacement** dans l'enregistrement de tâche est 101 Broadway East, Seattle, WA. Si vous définissez la condition de réinitialisation du SLA sur **[Emplacement] [changes from][101 Broadway East, Seattle, WA],** tout changement de la valeur du

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	champ **Emplacement** réinitialise le SLA de l'enregistrement de tâche.

Information associée

Créer une définition de Data Loss Prevention Incident Response SLA

Configurer les paramètres avancés

Configurez les paramètres avancés afin de pouvoir déterminer les champs de l'incident pour identifier les utilisateurs finaux, entre autres options.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

La configuration des Data Loss Prevention Incident Response paramètres avancés est facultative. Certains paramètres avancés incluent les éléments suivants :

- Définissez le nombre maximal d'incidents qui peuvent être envoyés dans un e-mail de synthèse.
- Activez le mode rapide pour envoyer des e-mails plus rapidement.
- Déterminez la verbosité du journal de l'application.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Paramètres avancés**.
2. Remplissez les champs du formulaire.

Formulaire Paramètres avancés

Champ	Description
Les données sensibles à l'origine de l'infraction doivent-elles être affichées sur l'incident ?	Option permettant de choisir d'afficher ou non les données sensibles à l'origine de l'infraction sur l'incident DLP. Par défaut, cette option est activée.
Les données sensibles à l'origine de l'infraction doivent-elles également être affichées sur les incidents enfants ?	Option permettant de choisir si vous souhaitez afficher également les données sensibles à l'origine de l'incident enfant DLP. Cette option est désactivée par défaut.
Liste des champs de l'incident qui sont utilisés pour identifier l'utilisateur final	Liste des champs de l'incident du module Règle d'affectation qui sont utilisés pour identifier l'utilisateur final. Vous pouvez également spécifier vos propres attributs personnalisés pour identifier l'utilisateur final.
Nombre maximal d'incidents dans un e-mail de synthèse	Nombre maximal d'incidents qui peuvent être envoyés dans un e-mail de synthèse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par défaut, la valeur est 100.
Durée maximale de la récidive (en jours)	La durée maximale pour identifier un récidiviste. Par défaut, la valeur est de 90 jours.
Mode rapide pour envoyer des e-mails	Option permettant de valider les e-mails et d'identifier les problèmes. Vous pouvez effectuer la validation en activant l'option **Oui** . Par défaut, cette option est activée.
Cette propriété est utilisée pour définir la verbosité du journal de l'application	Niveau de verbosité du journal de l'application, c'est-à-dire le nom du type d'information. Vous pouvez également mettre à jour la valeur dans les options suivantes : ○ **erreur** ○ **avertir** ○ **info** ○ **debug** Par défaut, la valeur est **info**.
Exclure les incidents clonés et enfants des rapports	Option permettant d'exclure les incidents clonés et enfants des rapports. Par défaut, cette option est **Oui**.
Jour(s) d'attente pourla suppression du contenu des correspondances sur le stockage cloud après la fermeture de l'incident	Option permettant de choisir le nombre de jours d'attente pour nettoyer le contenu des correspondances des incidents qui sont inactifs pendant une durée spécifique. Par défaut, la valeur est 90. Après 90 jours, si l'incident DLP est inactif, le contenu de la correspondance est nettoyé du stockage dans le cloud.
Affecter un incident au groupe d'analystes DLP après le dernier niveau d'escalade	Cochez cette case pour affecter l'incident à l'analyste après le dernier niveau d'escalade.
Autoriser les utilisateurs à accéder aux incidents après escalade	Cochez cette case pour permettre aux utilisateurs affectés d'accéder à l'incident ou aux incidents après l'escalade. Lorsque vous sélectionnez cette option, tous les utilisateurs qui ont été ajoutés à la liste de chaînes d'escalade peuvent alors accéder à l'incident ou aux incidents.
Autoriser l'analyste à modifier l'évaluation terminée	Cochez cette case pour permettre à l'analyste de modifier l'évaluation terminée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Lorsque vous sélectionnez cette option, les analystes peuvent modifier les évaluations. Si elle n'est pas sélectionnée, vous pouvez afficher les évaluations en mode lecture seule.
Propriétés de l'aperçu des fichiers de preuves	
L'activation de cette propriété système active la fonctionnalité d'aperçu du fichier de preuves dans l'espace de travail de l'analyste DLP. sn_dlir.enable_evidence_file_preview	Option permettant de choisir si vous souhaitez prévisualiser les fichiers de preuves directement dans l'espace de travail. Par défaut, cette option est **Oui**.
Cela permettra aux utilisateurs de DLP de télécharger les fichiers de preuves prévisualisés. Une fois cette propriété activée, les utilisateurs verront un bouton de téléchargement dans la visionneuse de documents pour télécharger le fichier de preuves. in_preview sn_dlir.enable_download	Option permettant de choisir d'afficher le bouton de téléchargement dans la visionneuse de documents, ce qui vous permettra de télécharger les fichiers de preuves prévisualisés. Par défaut, cette option est **Oui**.
Cette propriété détermine la durée pendant laquelle les fichiers seront temporairement conservés à des fins d'aperçu des fichiers de preuve. (en minutes) sn_dlir.preview_temp_files_cleanup_interval	La durée maximale pendant laquelle les fichiers sont temporairement stockés pour l'aperçu du fichier de preuve. Par défaut, la valeur est 10. Au bout de 10 minutes, si l'incident DLP est inactif, le fichier de preuves est nettoyé de l'espace de travail de l'analyste.
L'activation de cette propriété prolonge l'intervalle de nettoyage si des fichiers de preuves sont utilisés. Cela permettra au système de prolonger le délai d'expiration des fichiers de preuves en fonction de la valeur définie dans la propriété système « sn_dlir.preview_temp_files_cleanup_interval ». sn_dlir.extend_cleanup_interval_on_usage	Option permettant de prolonger le délai avant la suppression des fichiers de preuves s'ils sont utilisés. Par défaut, cette option est **Oui**.
La durée maximale pour prolonger l'intervalle de nettoyage des fichiers de preuves (en minutes). sn_dlir.max_extension_duration_for_cleanup	Option permettant de sélectionner la durée, en minutes, pendant laquelle le système conservera vos fichiers de preuves avant de les nettoyer. Par défaut, la valeur est 60.

3. Cliquez sur **Enregistrer**.

Surveiller le processus d'exécution de l'intégration DLP

Suivez et surveillez l'ingestion en cours ou le processus d'exécution de l'intégration. Les processus d'exécution de l'intégration contiennent les statistiques sur la quantité de données traitées et l'état de l'intégration.

Rôle requis : sn_dlir.admin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le processus d'exécution de l'intégration répertorie les détails sur le nombre d'enregistrements ingérés. Par exemple :

1. Dans Symantec Integration, le processus contient des exécutions d'intégration enfant et parent. L'enregistrement parent indique les données d'ingestion et l'enregistrement enfant indique les appels d'enrichissement et les enregistrements d'attributs personnalisés.
2. Dans Microsoft Integration, il n'existe qu'un seul processus d'ingestion d'enregistrement parent à exécuter.

Processus d'exécution de l'intégration DLP : affiche les entrées de file d'attente, l'état des entrées de file d'attente et les enregistrements extraits.

L'exécution de l'intégration contient la source pour laquelle le profil d'intégration et l'enregistrement de l'exécution de l'intégration sont créés, les intervalles d'interrogation du profil, les états et sous-états d'ingestion, le nombre d'incidents qui indique le nombre d'enregistrements ingérés.

1. Accédez à la **Administration DLP** > **Exécutions des intégrations**.
2. Sélectionnez l'exécution d'intégration dans la liste.
3. Accédez au **processus d'exécution de l'intégration DLP**.
4. Affichez l'état d'entrée dans la file d'attente de l'enregistrement.

Restrictions d'accès aux incidents DLP

Gérez la visibilité d'un incident DLP particulier qui contient des informations sensibles. Vous pouvez utiliser les restrictions d'accès aux incidents pour définir qui peut accéder à un incident DLP particulier et empêcher des utilisateurs ou des groupes spécifiques d'accéder à cet incident.

Créer des restrictions au niveau du champ

Définissez des restrictions de niveau de champ dans les incidents DLP afin de protéger les informations sensibles contre l'exposition. Vous pouvez utiliser des restrictions au niveau des champs pour contrôler les utilisateurs ou les groupes qui peuvent accéder à des champs spécifiques dans les incidents DLP.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Les restrictions de niveau de champ vous permettent d'afficher uniquement certains champs pour des utilisateurs ou des groupes spécifiques, offrant ainsi un moyen plus granulaire de contrôler les données auxquelles un utilisateur peut accéder. Vous pouvez créer une restriction au niveau du champ en définissant les conditions de correspondance de l'incident DLP, en sélectionnant les utilisateurs ou les groupes auxquels ces conditions s'appliquent, puis en choisissant les champs DLP que ces utilisateurs ou groupes peuvent afficher.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Restrictions d'accès aux incidents** > **Restrictions de niveaux de champs**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de restriction au niveau du champ DLP

Champ	Description
Nom	Nom de la restriction au niveau du champ.
Actif	Option permettant d'indiquer si la restriction au niveau du champ est active.
Ordre d'exécution	Priorité des restrictions au niveau du champ. Ce champ indique l'ordre dans lequel les restrictions au niveau du champ sont exécutées lorsque deux restrictions au niveau du champ ou plus partagent les conditions de déclenchement. La restriction au niveau du champ avec le numéro le plus bas a la priorité la plus élevée. Pour définir l'ordre d'opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Description brève	Description unique pour cette restriction au niveau du champ.
Condition de correspondance d'incident	Options dans l'incident qui correspondent aux conditions définies. Vous pouvez sélectionner l'un des champs d'incident pour définir la condition de déclenchement des restrictions de niveau de champ. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** : ○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. Par exemple, vous pouvez sélectionner le champ en tant que Nom de politiqueet définir la condition comme dans, et Nom de la politique. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse.
Concerne	Option permettant d'appliquer les conditions de correspondance d'incident à des utilisateurs ou groupes spécifiques. Vous pouvez appliquer les conditions aux éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

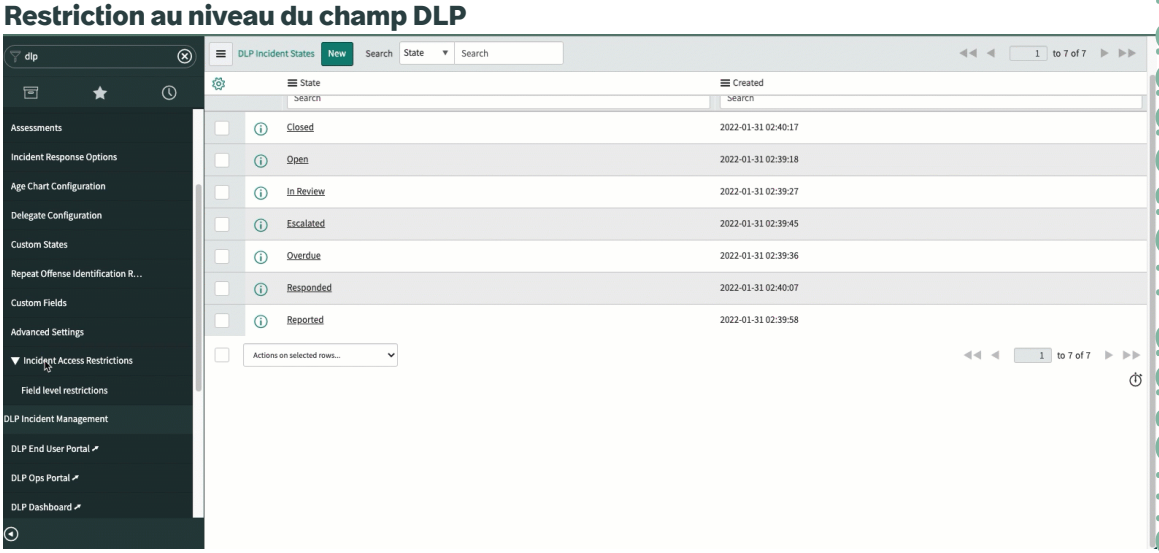
Champ	Description
	○ **Tous les utilisateurs finaux** : option permettant de sélectionner tous les utilisateurs finaux auxquels les conditions d'incident DLP sont applicables. ○ **Tous les réviseurs des incidents escaladés** : option permettant de sélectionner tous les réviseurs des incidents escaladés auxquels les conditions d'incident DLP s'appliquent. Il s'agit de tous les incidents DLP remontés au gestionnaire. ○ **Utilisateurs** : cliquez sur pour ajouter un utilisateur particulier à partir de la liste auquel les conditions d'incident DLP s'appliquent. Vous pouvez également ajouter un utilisateur à l'aide de son adresse e-mail ou de l'option de recherche. Par exemple, Gestionnaire juridique. Pour vous ajouter en tant qu'utilisateur auquel les conditions DLP sont applicables, cliquez sur ○ **Groupes** : cliquez sur l'icône ajouter un groupe particulier à partir de la liste auquel les conditions d'incident DLP s'appliquent. Vous pouvez également ajouter un groupe à l'aide de l'option de recherche. Par exemple, les créateurs d'enquêtes.
Autoriser l'accès aux champs suivants uniquement	○ **Champs DLP** : option permettant de définir les champs DLP pour lesquels vous souhaitez autoriser l'accès aux utilisateurs ou groupes sélectionnés. Sélectionnez les champs DLP auxquels vous souhaitez autoriser l'accès dans la colonne Disponible et déplacez-les vers la colonne Sélectionné. **Remarque :** Les utilisateurs ou groupes sélectionnés pourront accéder uniquement aux champs DLP sélectionnés. Par exemple, vous pouvez sélectionner les champs**Affecté à** et **Ouvert** dans la colonne Disponible et les déplacer vers la colonne Sélectionné. Ensuite, les utilisateurs ou groupes sélectionnés n'ont accès qu'aux champs Affecté à et Ouvert. ○ **Télécharger les pièces jointes** : option permettant d'indiquer si vous souhaitez autoriser les utilisateurs ou les groupes sélectionnés à télécharger des pièces jointes. ○ **Champs personnalisés** : option permettant de définir les champs personnalisés pour lesquels vous souhaitez autoriser l'accès aux utilisateurs ou groupes sélectionnés. Vous pouvez afficher les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	champs personnalisés que vous avez créés dans la colonne Disponible. Sélectionnez les champs personnalisés auxquels vous souhaitez autoriser l'accès dans la colonne Disponible et déplacez-les vers la colonne Sélectionné. **Important :** ▪ Les champs personnalisés pour les incidents DLP ne sont pris en charge que sur la version San Diego ou ultérieure. ▪ Les utilisateurs ou groupes sélectionnés ne pourront accéder qu'aux champs personnalisés sélectionnés.

Restriction au niveau du champ DLP



4. Cliquez sur **Envoyer**.

Créer des restrictions au niveau de l'enregistrement

Définissez des restrictions de niveau d'enregistrement dans les incidents DLP pour protéger les enregistrements sensibles contre l'exposition. Vous pouvez utiliser des restrictions au niveau des enregistrements pour contrôler les utilisateurs ou les groupes qui peuvent accéder à des enregistrements spécifiques dans les incidents DLP.

Avant de commencer

Rôle requis :

- sn_dlir.admin : créer, modifier et supprimer.
- sn_dlir.analyst et sn_dlir.analyst_read : vue (lecture seule).

Pourquoi et quand exécuter cette tâche

Les restrictions de niveau d'enregistrement vous permettent de fournir l'accès aux enregistrements uniquement à des utilisateurs ou groupes spécifiques, offrant un moyen plus granulaire de contrôler les enregistrements auxquels un utilisateur peut accéder. Vous pouvez créer une restriction au niveau de l'enregistrement en définissant les conditions de correspondance de l'incident DLP, en sélectionnant les utilisateurs ou les groupes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

auxquels ces conditions s’appliquent, puis en choisissant les enregistrements DLP que ces utilisateurs ou groupes peuvent afficher.

Procédure

1. Accédez à la **Tous** > **Administration DLP** > **Restrictions d'accès aux incidents** > **Restrictions de niveaux d'enregistrements**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Formulaire de restriction du niveau d’enregistrement DLP

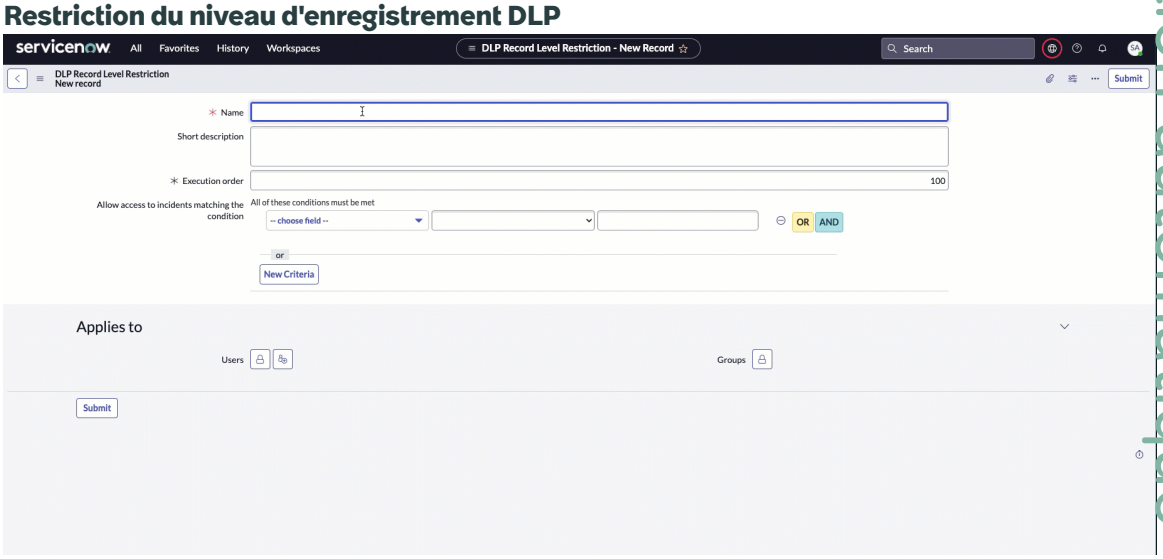
Champ	Description
Nom	Nom de la restriction au niveau de l’enregistrement.
Description brève	Description unique pour cette restriction de niveau d’enregistrement.
Ordre d'exécution	Priorité des restrictions au niveau de l’enregistrement. Ce champ indique l’ordre dans lequel les restrictions au niveau de l’enregistrement sont exécutées lorsque deux restrictions au niveau de l’enregistrement ou plus partagent les conditions de déclenchement. La restriction au niveau de l’enregistrement avec le numéro le plus bas a la priorité la plus élevée. Pour définir l’ordre d’opération, saisissez une valeur. Par exemple, 100, 200 ou tout autre nombre. La valeur par défaut est 100.
Autoriser l’accès aux incidents correspondant à la condition	Les options permettent d’accéder aux incidents qui correspondent aux conditions définies. Vous pouvez sélectionner l’un des champs d’incident pour définir la condition de déclenchement des restrictions au niveau de l’enregistrement. Utilisez les listes et les champs du générateur de conditions pour définir les filtres de la première ligne. Pour ajouter d’autres conditions, cliquez sur **ET** ou **OU** : ○ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ○ Si **OU** est sélectionné, l’une ou l’autre des conditions peut être mise en correspondance. Pour définir une deuxième condition de filtre, cliquez sur **Nouveau critère**. **Remarque :** Les conditions du générateur de conditions sont sensibles à la casse. Par exemple, vous pouvez sélectionner le champ comme Actifet définir la condition telle quelle, et vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Concerne	Option permettant d'appliquer des restrictions au niveau de l'enregistrement à des utilisateurs ou groupes spécifiques. Vous pouvez appliquer les conditions comme suit : ○ **Utilisateurs** : cliquez sur pour ajouter un utilisateur particulier dans la liste auquel l'enregistrement sélectionné s'applique. Vous pouvez également ajouter un utilisateur à l'aide de son adresse e-mail ou de l'option de recherche. Par exemple, Gestionnaire juridique. Pour vous ajouter en tant qu'utilisateur auquel l'enregistrement s'applique, cliquez sur . Par exemple, Administrateur système. ○ **Groupes** : cliquez sur pour ajouter un groupe particulier à partir de la liste auquel l'enregistrement sélectionné s'applique. Vous pouvez également ajouter un groupe à l'aide de l'option de recherche. Par exemple, les créateurs d'enquêtes.

Restriction du niveau d'enregistrement DLP



4. Cliquez sur **Envoyer**.

Archivage des incidents DLP

Le est Data Loss Prevention Incident Response doté d'une règle d'archivage dans le système de base pour la table d'incidents DLP. Les enregistrements connexes sont également ajoutés dans le système de base à la règle d'archivage des incidents DLP.

Avant de commencer
Rôle requis : admin

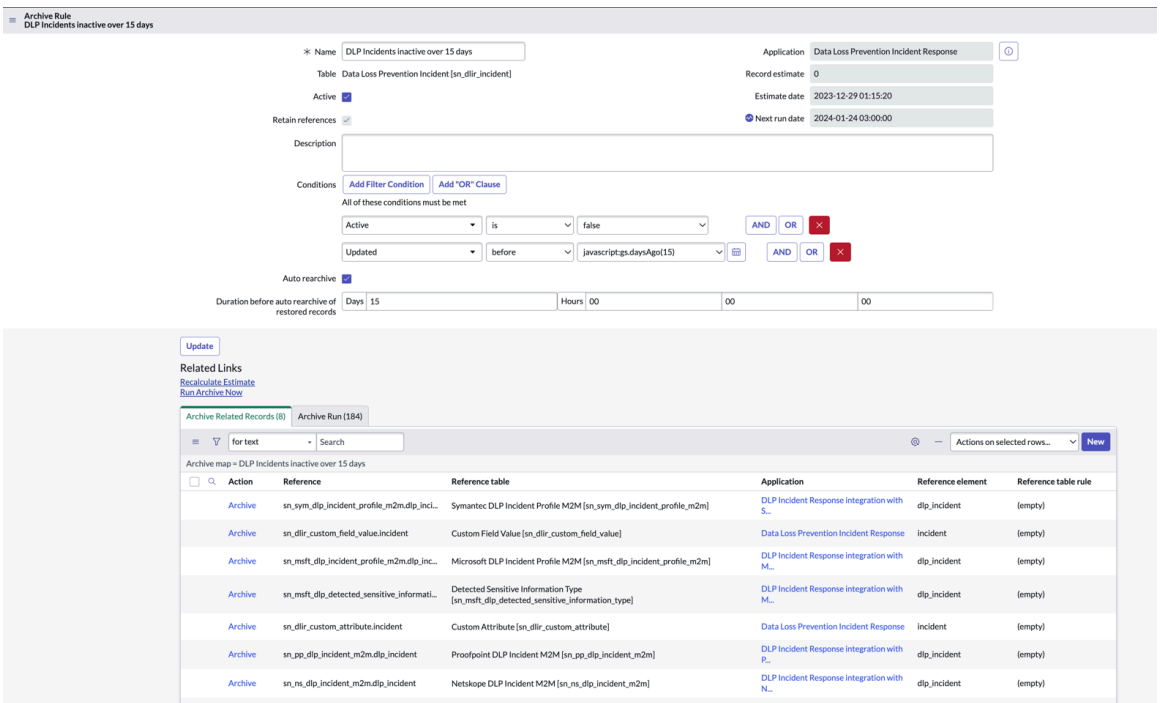
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Archivage système** > **Règles d'archivage**.
   Les règles d'archivage système qui se trouvent dans le système de base s'affichent.
2. Affichez la règle d'archivage DLP.

> **Remarque : Les incidents DLP inactifs pendant plus de 15 jours** est la règle d'archivage du système de base par défaut pour les incidents DLP. Vous pouvez modifier la règle d'archivage si nécessaire. Cette règle signifie que les incidents inactifs de plus de 15 jours seront automatiquement archivés.



> **Remarque :** Pour plus d'informations sur la façon dont les règles d'archivage sont créées, voir Créer une règle d'archivage .

3. **Mettez à jour** la règle, si nécessaire.

Archiver les enregistrements connexes DLP

Utilisez la liste connexe Enregistrements connexes d'archivage pour les incidents DLP afin d'ajouter les enregistrements connexes à la règle d'archivage.

Avant de commencer
Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Archivage système** > **Règles d'archivage**.
2. Sélectionner la règle d'archivage **des incidents DLP inactifs pendant 15 jours** .
3. Accédez à la liste connexe **des enregistrements connexes d'archivage** .
4. Affichez les enregistrements connexes DLP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application	Table de référence
Intégration de Symantec à Réponse aux incidents DLP	Profil d'incident Symantec DLP M2M [sn_sym_dlp_incident_profile_m2m]
Data Loss Prevention Incident Response	Valeur du champ personnalisé [sn_dlir_custom_field_value]
Intégration de Microsoft à Réponse aux incidents DLP	N-N de profil d'incident DLP Microsoft [sn_msft_dlp_incident_profile_m2m]
Intégration de Microsoft à Réponse aux incidents DLP	Type d'information sensible détectée [sn_msft_dlp_detected_sensitive_information_type]
Data Loss Prevention Incident Response	Attribut personnalisé [sn_dlir_custom_attribute]
Intégration de Proofpoint à Réponse aux incidents DLP	M2M d'incident DLP ProofPoint [sn_pp_dlp_incident_m2m]
Intégration de DLP Incident Response à Netskope	M2M d'incident DLP Netskope [sn_ns_dlp_incident_m2m]
Intégration de Symantec à Réponse aux incidents DLP	Type d'information sensible détectée [sn_sym_dlp_detected_sensitive_information_type]

Remarque : Toutes les tables système telles que les e-mails, les évaluations et les pièces jointes dirigeront automatiquement vers l'enregistrement DLP archivé.

5. Sélectionnez la règle d'enregistrement connexe d'archivage que vous souhaitez archiver.

Remarque : Pour plus d'informations sur l'ajout d'enregistrements connexes, consultez Archiver les enregistrements connexes DLP sur ServiceNow AI Platform.

Data Loss Prevention Incident Response Gestion des incidents

Utilisez Gestion Data Loss Prevention Incident Response des incidents pour mettre à jour et gérer les incidents en tirant parti de l'espace de travail de l'utilisateur DLP, de l'espace de travail de l'analyste DLP et du tableau de bord DLP.

Data Loss Prevention Incident Response Espace de travail de l'utilisateur

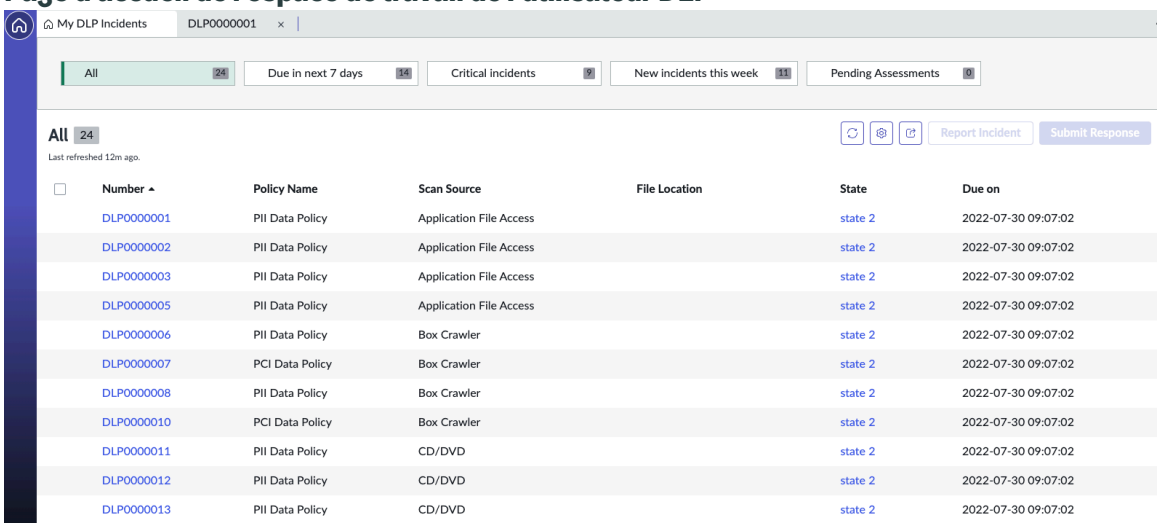
L'espace Data Loss Prevention Incident Response de travail de l'utilisateur (DLP IR) est un espace de travail dans lequel les utilisateurs finaux, les gestionnaires et les approbateurs peuvent répondre aux incidents DLP affectés. Les utilisateurs finaux, les gestionnaires et les approbateurs peuvent ensuite répondre aux incidents en spécifiant les actions correctes.

Vous pouvez également créer et gérer des évaluations pour permettre aux utilisateurs finaux de répondre aux incidents DLP. L'espace de travail se compose d'une page de destination et de vues de listes qui vous permettent de voir les incidents DLP affectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page d'accueil de l'espace de travail de l'utilisateur DLP



Signaler ou répondre aux incidents DLP

Accédez à l'espace de Data Loss Prevention Incident Response travail utilisateur (DLP), examinez les incidents DLP affectés et signalez ou répondez aux incidents.

Avant de commencer

Rôle requis :

- Tout utilisateur/employé valide

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'utilisateur DLP**.
   La page Mes incidents DLP s'ouvre dans un nouvel onglet.
2. Cliquez sur une vue de liste pour passer en revue les incidents qui vous sont affectés.

Vue liste	Description
Tous	Affichez tous les incidents affectés.
Échéance dans les 7 prochains jours	Affichez tous les incidents attendus dans les 7 prochains jours.
Incidents critiques	Affichez tous les incidents avec l'étiquette de gravité critique.
Nouveaux incidents cette semaine	Affichez tous les incidents affectés cette semaine.
Évaluations en attente	Affichez toutes les évaluations encore en attente.

3. Vous pouvez examiner les incidents DLP de deux manières :

   a. La première consiste à localiser et à sélectionner un ou plusieurs incidents DLP que vous souhaitez examiner, puis à cocher la case à côté des incidents.

   b. Choisissez l'option qui vous convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

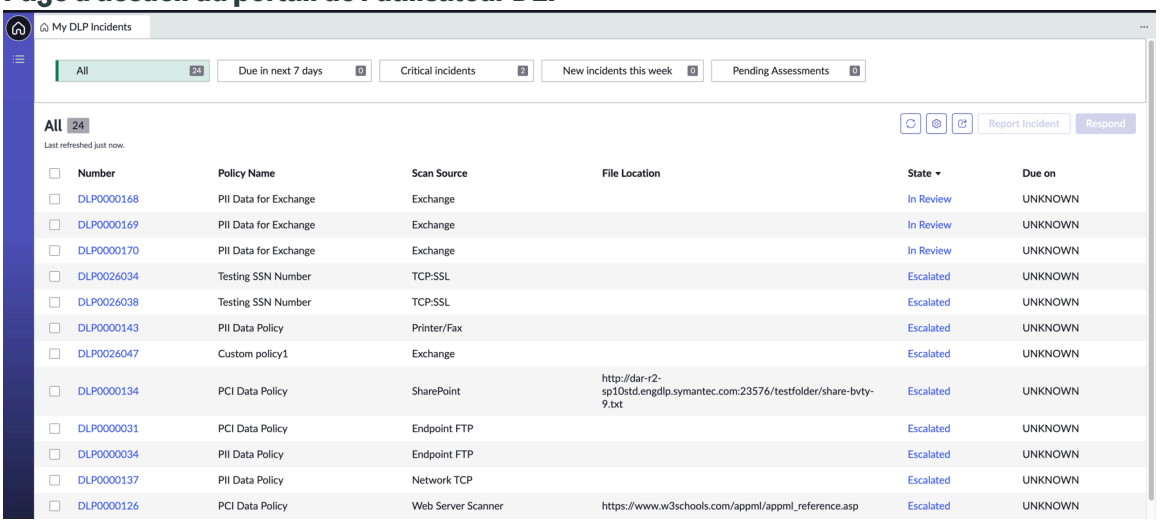
Page d'accueil du portail d'utilisateur final DLP

Option	Description
Actualiser la liste	Option permettant d'actualiser la liste des incidents DLP si vous avez effectué une mise à jour.
Actions des listes	Liste des actions que vous pouvez effectuer. Les choix sont les suivants : ▪ **Enregistrer sous** ▪ **Modifier les colonnes** ▪ **Rétablir la largeur des colonnes** **Remarque :** Lorsque vous avez configuré votre propre liste personnalisée créée sous la section **Mes listes** pour votre espace de travail, vous pouvez également effectuer les actions de liste supplémentaires ci-dessous : ▪ **Renommer** ▪ **Enregistrer** ▪ **Supprimer**
Copier l'URL pour tout	Option permettant de copier les URL de tous les incidents DLP.
Signaler un incident	Action pour signaler l'incident comme faux positif ou propriétaire incorrect. Par exemple, vous pouvez signaler un propriétaire incorrect et suggérer un autre propriétaire ou signaler l'incident comme un faux positif.
Répondre	Répondre à un incident en sélectionnant une option de réponse aux incidents. Par exemple, si un utilisateur supprime un fichier en violation d'une stratégie DLP, il peut choisir l'option **Fichier supprimé** pour soumettre une confirmation manuelle que le fichier a été supprimé et fournir des commentaires. Dans cet emplacement, vous pouvez également sélectionner des options de réponse avancées. Par exemple, **Demander la sortie de quarantaine de l'e-mail**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page d'accueil du portail de l'utilisateur DLP



c. La deuxième consiste à cliquer sur un incident DLP particulier pour l'ouvrir.
L'onglet **Détails** comprend les sections suivantes :

- Détails : vous pouvez afficher les détails de l'incident DLP, tels que le numéro d'incident, la gravité et le nom du fichier.
- Composer : pour ajouter des commentaires sur l'incident DLP visibles par tout le monde, saisissez les commentaires dans l'onglet Commentaires. Pour ajouter des commentaires visibles par certaines personnes, saisissez les commentaires dans l'onglet Notes de travail (privées).
- Activité : vous pouvez afficher les détails des différentes activités sur l'incident DLP.
- Pièces jointes : si vous avez des pièces jointes liées à l'incident DLP, cliquez sur **Parcourir** et sélectionnez la pièce jointe sur votre disque local.

  L'onglet **Détails supplémentaires** affiche toutes les informations supplémentaires sur l'incident DLP, y compris les champs personnalisés.

  Important :
  - Les champs personnalisés pour les incidents DLP ne sont pris en charge que sur la version San Diego ou ultérieure.
  - S'il existe des données de champs personnalisés disponibles pour un incident DLP particulier, vous pouvez les afficher sous l'onglet **Détails supplémentaires** . S'il n'existe aucun champ personnalisé pour l'incident DLP, vous verrez une page blanche.

- **Type d'information sensible détectée** : affiche les informations sensibles détectées par l'incident.

  Remarque : Cette liste connexe n'est visible que pour les incidents DLP créés pour les intégrations Microsoft ou Symantec. Dans l'enregistrement d'incident Microsoft ou Symantec, chaque fois que l'utilisateur accède à l'enregistrement de type d'information sensible détecté, le contenu de correspondance en surbrillance relatif à cette intégration s'affiche.

d. Choisissez l'option qui vous convient.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

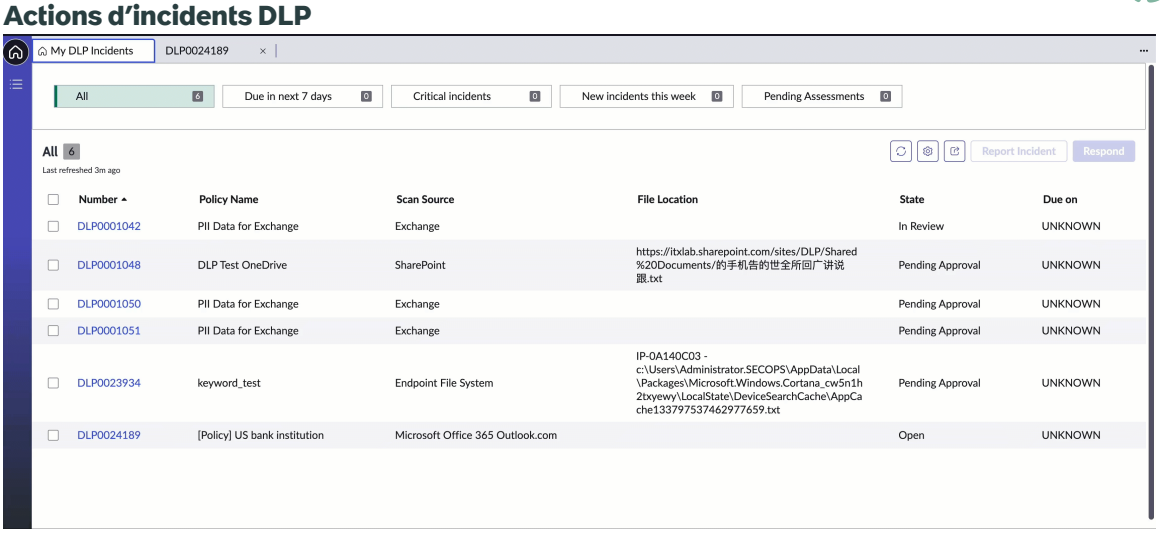
Option	Description
Signaler un faux positif	Action pour signaler que l'incident DLP a été déclenché ou créé de manière incorrecte. Vous pouvez mentionner les détails de la raison pour laquelle vous avez marqué l'incident comme faux positif dans le champ Commentaires.
Signaler un propriétaire incorrect	Action pour signaler que l'incident DLP a été affecté à un utilisateur incorrect. Si vous connaissez le propriétaire correct de l'incident, vous pouvez sélectionner le nom du propriétaire dans le champ Suggérer un propriétaire. Pour ajouter des détails supplémentaires, utilisez le champ Commentaires.
Répondre	Répondre à un incident en sélectionnant une option de réponse aux incidents. Par exemple, si un utilisateur supprime un fichier en violation d'une stratégie DLP, il peut choisir l'option **Fichier supprimé** pour soumettre une confirmation manuelle que le fichier a été supprimé et fournir des commentaires. Dans cet emplacement, vous pouvez également sélectionner des options de réponse avancées. Par exemple, **Demander la sortie de quarantaine de l'e-mail**.

e. Sélectionnez le bouton **Répondre après avoir** répondu à la requête de l'analyste.
Une fenêtre contextuelle pour soumettre une réponse à un incident s'affiche. Sélectionnez la réponse dans le menu déroulant et ajoutez des commentaires.

f. Sélectionnez **Soumettre**.
Une bannière s'affiche pour confirmer que votre réponse a été envoyée avec succès.

Remarque : L'incident est affecté à l'approbateur ou à l'analyste correspondant et l'utilisateur final perd l'accès à l'incident.

Actions d'incidents DLP



Traduction automatique

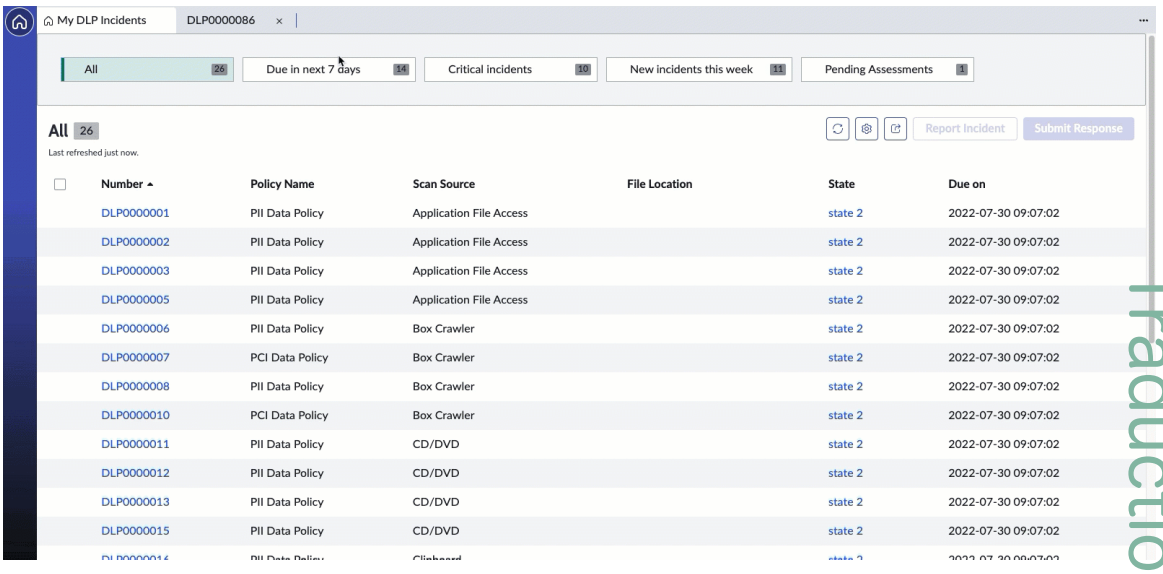
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Pour effectuer des évaluations, sélectionnez la vue de liste **Évaluations en attente** .

   a. Cliquez sur un numéro d'évaluation spécifique pour l'ouvrir.

   b. Répondez aux questions d'évaluation, puis cliquez sur **Enregistrer** ou **Soumettre** en fonction de vos besoins.

Évaluations DLP



5. Cliquez sur la section **Carte d'instructions** qui s'affiche au-dessus de tous les champs de la vue de formulaire d'incident DLP, pour afficher les informations supplémentaires sur un incident particulier.

   Remarque : Cette section de l'espace de travail guide les utilisateurs sur les informations sur les incidents, ce qui les aide à comprendre les prochaines étapes de la résolution des incidents.

   La carte d'instructions de l'utilisateur affiche deux en-têtes différents qui vous fournissent plus d'informations sur un incident spécifique dans la vue de formulaire. Cliquez sur un en-tête d'instruction utilisateur pour connaître les détails supplémentaires.

Pour plus d'informations, consultez Créer des modèles d'instructions de l'utilisateur et Configurer les instructions de l'utilisateur de l'interface utilisateur DLP.

Utilisation du module Mes approbations

Le module Mes approbations est disponible dans l'espace de travail des utilisateurs DLP pour les utilisateurs connectés. Les utilisateurs peuvent approuver ou rejeter les demandes d'approbation d'affectation à partir d'ici.

Avant de commencer

Rôle requis :

- Utilisateur final
- Responsable
- Approbateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'utilisateur DLP**.
   La page **Mes incidents DLP** s'affiche dans un nouvel onglet.
2. Cliquez sur le module **Mes approbations** présent dans le module **Mes incidents DLP** .
   La vue de liste Mes approbations s'affiche.

   L'approbateur peut approuver ou rejeter les demandes à partir de la vue de liste de **la page Mes approbations** . Vous pouvez approuver ou rejeter les demandes multiples à partir de la vue de liste.

   L'approbateur peut afficher les détails de la demande affectée dans la vue de formulaire. En cliquant sur l'action **Approuver** ou **Rejeter** à partir de la vue de formulaire, on peut approuver ou rejeter la demande individuelle.

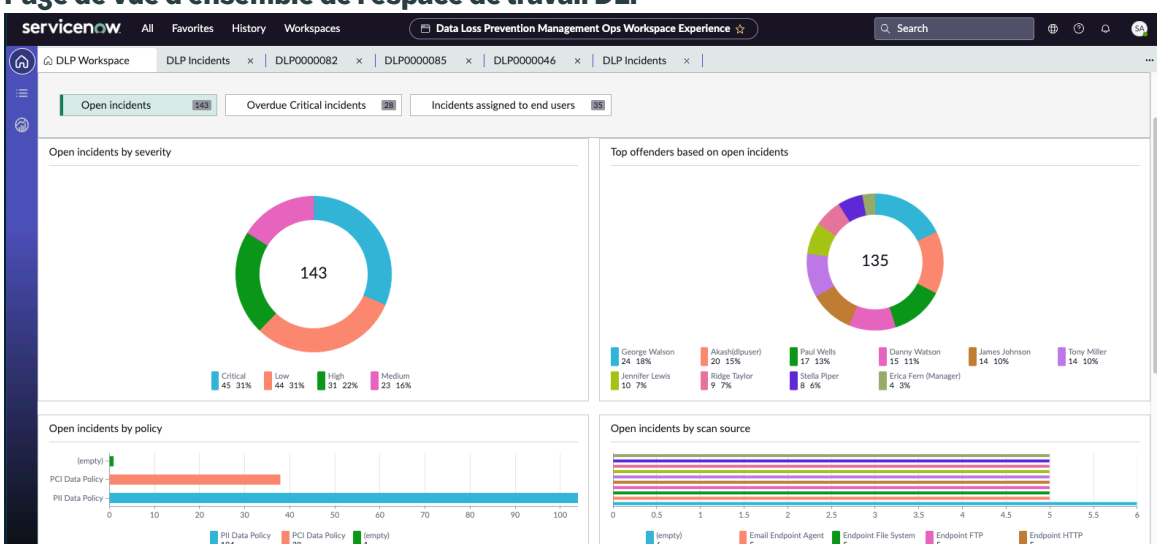
   Remarque : Pour afficher les détails de l'incident DLP, cliquez sur disponible dans le champ **Approuver** .

Data Loss Prevention Incident Response Espace de travail de l'analyste

Utilisez l'espace de travail de l'analyste Data Loss Prevention Incident Response (DLP IR) pour afficher les incidents DLP. Affectez les incidents aux utilisateurs finaux pour la résolution et plus encore.

L'espace de travail DLP se compose d'une page d'accueil avec des tableaux de bord, des vues de listes et des vues de formulaire qui vous permettent de surveiller les incidents DLP.

Page de vue d'ensemble de l'espace de travail DLP



Examiner et affecter vos incidents DLP

Accédez à l'espace de travail de l'analyste Data Loss Prevention Incident Response (DLP IR) pour examiner les incidents DLP et les affecter ou les résoudre. Vous pouvez suivre les tendances des incidents par gravité, les principaux contrevenants, les incidents par source d'analyse et les incidents par politique.

Page d'accueil de l'espace de

Vue d'ensemble de l'espace de travail

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis :

- sn_dlir.analyst : modifiez et affichez des incidents DLP.
- sn_dlir.analyst_read et sn_dlir.read : afficher les incidents DLP.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
   La page de liste Mes opérations d'incidents de l'espace de travail DLP s'ouvre dans un nouvel onglet.
2. Cliquez sur l'icône d'accueil de **l'espace de travail DLP** pour afficher la vue de la page d'accueil de l'espace de travail.
3. Passez en revue les widgets du tableau de bord pour identifier les tendances par incidents par gravité, principaux contrevenants, incidents par source d'analyse et incidents par politique.
4. Cliquez sur les filtres appropriés sur la page d'accueil pour afficher les widgets par leurs différentes catégories.

Filtres	Description
Incidents ouverts	Afficher tous les incidents ouverts.
Incidents critiques en retard	Affichez les incidents qui présentent l'étiquette de gravité critique et qui sont en retard.
Incidents affectés à des utilisateurs finaux	Affichez les incidents qui sont affectés aux utilisateurs finaux.

5. Vous pouvez examiner et affecter les incidents DLP de deux manières :

   a. La première consiste à localiser et à sélectionner un ou plusieurs incidents DLP que vous souhaitez examiner, puis à cocher la case à côté des incidents.

   b. Choisissez l'option qui vous convient.

Option	Description
Actualiser la liste	Option permettant d'actualiser la liste des incidents DLP lorsque vous effectuez une mise à jour.
Actions des listes	Liste des actions que vous pouvez effectuer. Les choix sont les suivants : ▪ **Enregistrer sous** ▪ **Modifier les colonnes** ▪ **Rétablir la largeur des colonnes**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Lorsque vous avez configuré votre propre liste personnalisée créée sous la section **Mes listes** pour votre espace de travail, vous pouvez également effectuer les actions de liste supplémentaires ci-dessous : ▪ **Renommer** ▪ **Enregistrer** ▪ **Supprimer**
Copier l'URL pour tout	Option permettant de copier les URL de tous les incidents DLP.
Afficher le panneau Filtre	Option permettant d'analyser les incidents requis à l'aide de l'option de filtre. **i.** Cliquez sur le filtre en haut à gauche de la page, puis sélectionnez **Vue avancée**. **ii.** Utilisez un filtre existant ou créez le vôtre en ajoutant des conditions qui contiennent un champ, un opérateur et des valeurs. **iii.** Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU** : ▪ Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance. ▪ Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance. **iv.** Cliquez sur **Mettre à jour**.
Affecter l'incident	Action pour déterminer à qui affecter l'incident DLP. Les choix sont les suivants : ▪ **Affecter l'incident à** : option permettant d'affecter l'incident à un analyste, à un utilisateur final ou à quelqu'un d'autre. ▪ **Utilisateur** : option permettant de déterminer à quel utilisateur l'incident doit être affecté. ▪ **État de l'incident Réponse pré-utilisateur** : option permettant de déterminer l'état dans lequel l'incident doit se trouver avant que l'utilisateur ne réponde. Il peut également s'agir d'un état personnalisé. ▪ **Joindre l'évaluation** : option permettant d'indiquer si vous souhaitez joindre une évaluation à l'incident. Si cette option

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	est activée, les options ci-dessous seront disponibles : ▪ **Modèle d'évaluation** : option permettant de sélectionner un modèle d'évaluation pour l'incident DLP. ▪ **État de l'incident Réponse post-utilisateur** Option permettant de sélectionner l'état dans lequel l'incident DLP doit se trouver après la réponse de l'utilisateur.
Répondre	Répondre à un incident en sélectionnant une option de réponse aux incidents. Par exemple, si un utilisateur supprime un fichier en violation d'une stratégie DLP, il peut choisir l'option **Fichier supprimé** pour soumettre une confirmation manuelle que le fichier a été supprimé et fournir des commentaires. Dans cet emplacement, vous pouvez également sélectionner des options de réponse avancées. Par exemple, **Demander la sortie de quarantaine de l'e-mail**.
Escalader	Action pour escalader l'incident. Vous pouvez escalader l'incident en sélectionnant l'utilisateur auquel vous souhaitez l'escalader. Vous pouvez également fournir des informations supplémentaires dans le champ Commentaires.
Mettre à jour l'état	Action pour mettre à jour l'état de l'incident. Vous pouvez mettre à jour l'état de l'incident en sélectionnant l'un des états dans les options déroulantes. Il peut également s'agir d'un état personnalisé.
Fermer	Action pour fermer les incidents. Sélectionnez le **code de fermeture** correspondant dans la liste déroulante et ajoutez des commentaires de fermeture. La fonctionnalité **Fermer** est Data Loss Prevention Incident Response effectuée de manière asynchrone et synchrone à partir de la vue de liste. i. Fermeture synchrone : lors de la fermeture d'incidents de manière synchrone, cela signifie que l'action de fermeture est effectuée immédiatement. Lorsque vous sélectionnez plusieurs incidents à fermer, et si le nombre d'incidents est inférieur ou égal à 100, les incidents sont fermés au premier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	plan de la vue de liste Incidents DLP. Ici, 100 est la valeur par défaut. **ii.** Fermeture asynchrone : cela implique que la demande de fermeture est soumise et que l'application exécute la demande en arrière-plan si le nombre d'incidents sélectionnés est supérieur à 100. Vous devez actualiser la vue de liste des incidents DLP pour afficher l'état des incidents mis à jour. **Remarque :** ▪ Le nombre d'incidents sélectionnés pour la fermeture asynchrone ou synchrone est configuré à l'aide de la propriété système *sn_dlir.closure_sync_count_limit*. ▪ Par défaut, le nombre d'incidents est fixé à 100.

c. La deuxième consiste à cliquer sur un incident DLP particulier pour l'ouvrir.

- **Onglet Détails** : affiche les sections suivantes :
  - **Détails** : vous pouvez afficher les détails de l'incident DLP, tels que le numéro d'incident, la gravité, le nom du fichier, etc. Vous avez également la possibilité de modifier respectivement les champs Gravité, État, Utilisateur final et Groupe d'analystes DLP et de les enregistrer.
  - **Composer** : pour ajouter des commentaires sur l'incident DLP visibles par tout le monde, saisissez les commentaires dans l'onglet Commentaires. Pour ajouter des commentaires visibles par certaines personnes, saisissez les commentaires dans l'onglet Notes de travail (privées).
  - **Activité** : vous pouvez afficher les détails des différentes activités sur l'incident DLP.
  - **Pièces jointes** : si vous avez des pièces jointes liées à l'incident DLP, cliquez sur **Parcourir** et sélectionnez la pièce jointe sur votre disque local.
- **Onglet Détails supplémentaires** : affiche toutes les informations supplémentaires sur l'incident DLP, y compris les champs personnalisés.

Important :

- Les champs personnalisés pour les incidents DLP ne sont pris en charge que sur la version San Diego ou ultérieure.
- Vous pouvez utiliser l'onglet **Détails supplémentaires** pour voir si des champs personnalisés ont été créés pour un incident DLP particulier ou non.

- **Onglet Attributs personnalisés** : affiche la liste des attributs personnalisés associés à l'incident DLP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Autres incidents de l'utilisateur final** : affiche l'incident du même utilisateur final. Vous pouvez consolider les incidents en exécutant l'action **Ajouter en tant qu'incident enfant** à partir de cette liste connexe.
- **Type d'information sensible détectée** : affiche les informations sensibles détectées par l'incident.

> **Remarque :** Cette liste connexe n'est visible que pour les incidents DLP créés pour les intégrations Microsoft ou Symantec. Dans l'enregistrement d'incident Microsoft ou Symantec, chaque fois que l'utilisateur accède à l'enregistrement de type d'information sensible détecté, le contenu de correspondance en surbrillance relatif à cette intégration s'affiche.

- **Incidents enfants** : affiche les incidents enfants créés manuellement (en effectuant l'action « Ajouter comme incident enfant ») ou à partir des règles de consolidation DLP. Pour supprimer le lien de l'incident enfant, exécutez l'option « Dissocier l'incident enfant » à partir de cette liste connexe.
- **Incidents clonés** : affiche les incidents clonés à partir de l'incident parent. En cliquant sur l'action **Cloner l'incident** de la vue de formulaire, vous pouvez créer un nouvel incident cloné.
- **Onglet Évaluations** : affiche la liste des évaluations affectées à l'incident DLP.

d. Choisissez l'option qui vous convient.

Option	Description

Affecter l'incident	Action pour déterminer à qui affecter l'incident DLP. Les choix sont les suivants :
	▪ **Affecter l'incident à** : option permettant d'affecter l'incident à un analyste, à un utilisateur final ou à quelqu'un d'autre.
	▪ **Utilisateur** : option permettant de sélectionner l'utilisateur auquel l'incident doit être affecté.
	▪ **État de l'incident Réponse pré-utilisateur** : option permettant de sélectionner l'état dans lequel l'incident doit se trouver avant que l'utilisateur ne réponde. Il peut également s'agir d'un état personnalisé.
	▪ **Joindre l'évaluation** : option permettant d'indiquer si vous souhaitez joindre une évaluation à l'incident. Si cette option est activée, les options ci-dessous seront disponibles :
	  ▪ **Modèle d'évaluation** : option permettant de sélectionner un modèle d'évaluation pour l'incident DLP.
	  ▪ **État de l'incident Réponse post-utilisateur** : option permettant

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	de sélectionner l'état dans lequel l'incident DLP doit se trouver après la réponse de l'utilisateur.
Annuler l'approbation	Action pour annuler la demande d'approbation. Cette action n'est visible par les analystes sur la vue de formulaire que lorsque l'incident DLP est à l'état **En attente d'approbation** . Les options disponibles sont les suivantes : ▪ **Affecter l'incident à** : option permettant de n'affecter l'incident à personne, à un analyste ou à quelqu'un d'autre. ▪ **Utilisateur** : option permettant de sélectionner l'utilisateur auquel l'incident doit être affecté. ▪ **État de l'incident post-annulation** : option permettant de sélectionner l'état dans lequel l'incident doit se trouver après l'annulation de la demande. ▪ **Commentaires** : pour fournir des détails supplémentaires sur l'annulation.
Affecter une évaluation	Action pour joindre une évaluation lors de l'affectation de l'incident. Les choix possibles sont les suivants : ▪ **Modèle d'évaluation** : option permettant de sélectionner un modèle d'évaluation pour l'incident DLP. ▪ **État de l'incident Réponse post-utilisateur** : option permettant de sélectionner l'état dans lequel l'incident DLP doit se trouver après la réponse de l'utilisateur.
Télécharger le fichier	Action pour télécharger le fichier ou l'e-mail contenant le contenu en infraction. Cette action peut être effectuée pour les incidents créés pour Microsoft OneDrive, SharePoint Online ou Exchange Online.
Enregistrer	Action pour enregistrer toutes les modifications que vous avez apportées. Vous pouvez modifier les champs Gravité, État et Utilisateur final de l'incident DLP et les enregistrer.
Répondre	Répondre à un incident en sélectionnant une option de réponse aux incidents. Par exemple, si un utilisateur supprime un fichier en violation d'une stratégie DLP, il peut choisir l'option **Fichier supprimé** pour soumettre une confirmation manuelle que le fichier a été supprimé et fournir des commentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

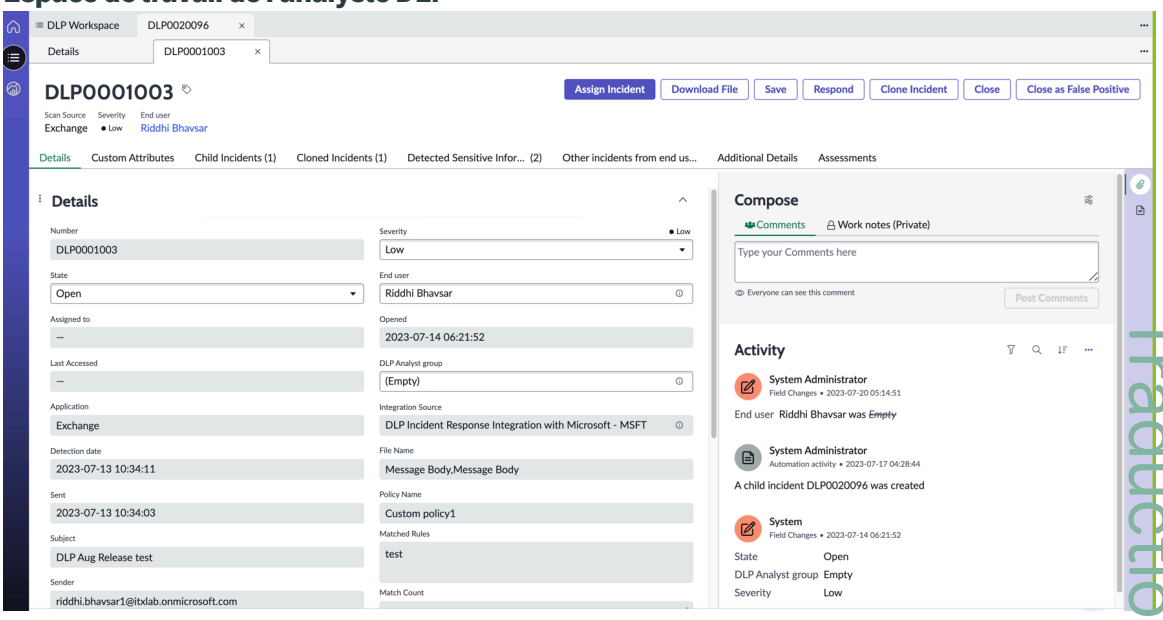
Option	Description
	Dans cet emplacement, vous pouvez également sélectionner les options de réponse avancées. **Par exemple : demandez la sortie de quarantaine de l'e-mail**.
Escalader	Action pour escalader l'incident. Vous pouvez escalader l'incident en sélectionnant l'utilisateur auquel vous souhaitez l'escalader. Vous pouvez également fournir des informations supplémentaires dans le champ Commentaires.
Cloner l'incident	Action pour créer un incident de clone si l'enregistrement d'incident a un impact sur plusieurs utilisateurs. Vous pouvez affecter les incidents clonés à plusieurs personnes concernées, telles que juridique/informatique. Une fois l'enregistrement d'incident cloné créé, un nouvel onglet **Incidents clonés** est créé sous l'incident DLP parent et tous les incidents clonés sont répertoriés dans cette vue. **Remarque :** ▪ Si l'enregistrement d'incident DLP parent est fermé, tous les enregistrements d'incidents clonés se ferment automatiquement. ▪ Si un enregistrement d'incident DLP contient un incident cloné, il ne peut pas être affecté aux utilisateurs finaux. Les enregistrements d'incidents DLP parents ne peuvent être gérés que par les utilisateurs disposant du rôle d'analyste. ▪ Vous avez également la possibilité de mettre à jour automatiquement l'état parent en fonction de l'état des incidents clonés dans le module Configuration par défaut. Par exemple, si tous les incidents clonés sont passés à l'état Escaladé, l'incident parent passera également à l'état Escaladé.
Fermer	Action pour fermer l'incident. Vous devez sélectionner le **code de fermeture** correspondant dans la liste déroulante et ajouter des commentaires sur la fermeture, si nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Fermer en tant que faux positif	Action pour fermer l’incident en tant que faux positif. Vous pouvez également ajouter des commentaires supplémentaires avant de fermer l’incident.

Espace de travail de l’analyste DLP



6. Vous pouvez voir la vue de liste à partir de la page d’accueil en allant en haut à gauche de la page et en cliquant sur l’onglet **Listes** .
   La catégorie Listes se compose des pages de liste par défaut et personnalisées pour les incidents DLP.
   - **Onglet Listes** : listes par défaut pour les incidents DLP. Les listes par défaut sont les suivantes :
     - Tous
     - Ouvert
     - Mes incidents
     - Affecté à mon groupe
     - Remonté
     - En retard
     - Évaluations en attente
     - Action de l'utilisateur en attente
     - Incidents clonés
     - Incidents archivés
   - **Onglet Mes listes** : affiche toutes les listes que vous avez renommées et toutes les listes que vous avez créées.

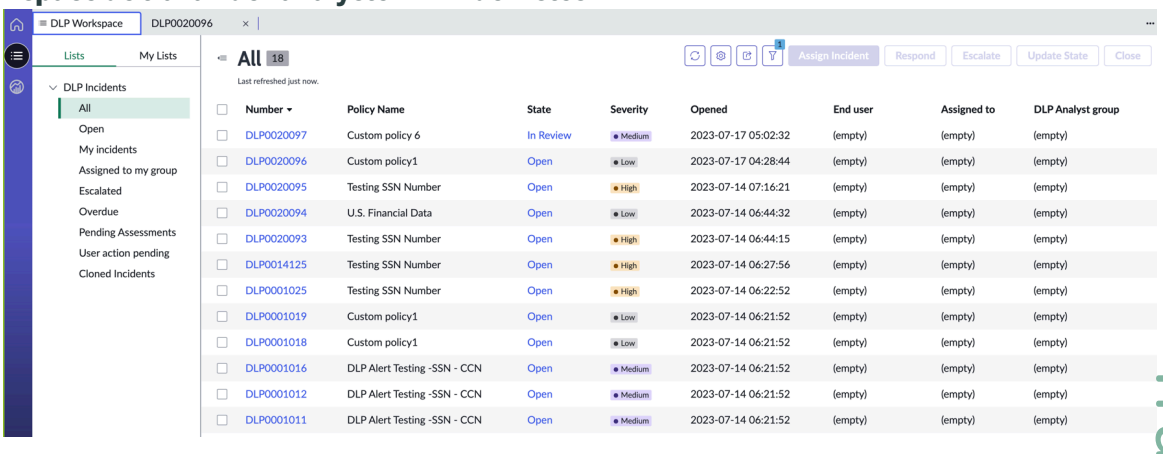
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example

L'exemple suivant montre l'espace de travail DLP avec les catégories de vue de liste. L'option **Tout** la vue de liste est sélectionnée.

Espace de travail de l'analyste DLP Vue Listes



Prévisualiser les fichiers de preuves

Prévisualisez Data Loss Prevention Incident Response les fichiers de preuves dans l'espace de travail de l'analyste DLP IR.

Avant de commencer

Important : Lors de l'utilisation de l'action Fichiers de preuves dans l'espace de travail de l'analyste DLP, les fichiers de preuves sont temporairement stockés dans la base de données ServiceNow dans un format non chiffré. Si vous ne souhaitez pas stocker les fichiers de preuves, désactivez la fonctionnalité d'aperçu des fichiers de preuves. Pour plus d'informations, consultez Configurer les paramètres avancés.

Rôle requis : sn_dlir.analyst

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez un enregistrement d'incident DLP.
3. Dans la barre latérale contextuelle, sélectionnez l'icône Fichiers de preuves ( ).
4. Dans l'onglet **Fichiers de preuves** , sélectionnez la carte **Fichier de preuves** pour afficher un aperçu des fichiers de preuves dans la visionneuse de documents.

   La fonctionnalité d'aperçu est différente pour chaque type de fichier, comme indiqué dans le tableau suivant.

Format de fichier	Extension de fichier
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg et .webp. Les fichiers image s'ouvrent en mode visionneuse de documents.
Microsoft Fichiers Office	.doc, .docx, .ppt, .pptx, .xls et .xlsx

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Format de fichier	Extension de fichier
	Les fichiers Office s'ouvrent en mode visionneuse de documents.
Fichiers texte	.txt Les fichiers texte s'ouvrent en mode éditeur de texte.
Fichiers courrier	.Eml **Remarque :** La taille du fichier doit être inférieure à 5 Mo. Vous devez d'abord télécharger le fichier pour prévisualiser son contenu.
Fichiers PDF	.PDF ○ Saisissez un mot clé pour rechercher le document. ○ Fonctions de zoom avant et arrière pour ajuster la vue et améliorer la lisibilité. ○ Faites pivoter la page dans le sens des aiguilles d'une montre ou dans le sens inverse des aiguilles d'une montre pour afficher le contenu plus clairement.

Remarque :

Les fichiers binaires ne seront pas rendus et devront être téléchargés pour prévisualiser leur contenu. La fonctionnalité d'aperçu du fichier de preuve fonctionne également pour les incidents archivés.

Playbook pour Data Loss Prevention Incident Response

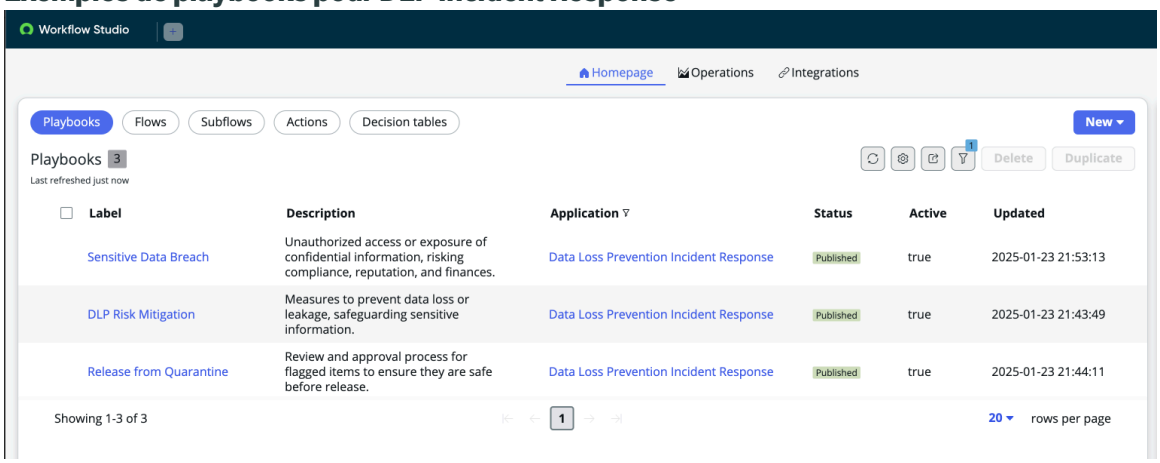
Un Data Loss Prevention Incident Response Playbook est un guide étape par étape pour traiter et atténuer les incidents de perte de données, qui peuvent inclure des expositions non autorisées, des fuites ou des violations d'informations sensibles susceptibles de compromettre la sécurité de votre organisation.

L'image suivante montre les exemples de Playbooks disponibles pour DLP IR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemples de playbooks pour DLP Incident Response



Le tableau suivant répertorie les activités et les étapes disponibles pour créer un Playbook DLP. Pour plus d'informations, consultez Ajouter un Playbook DLP:

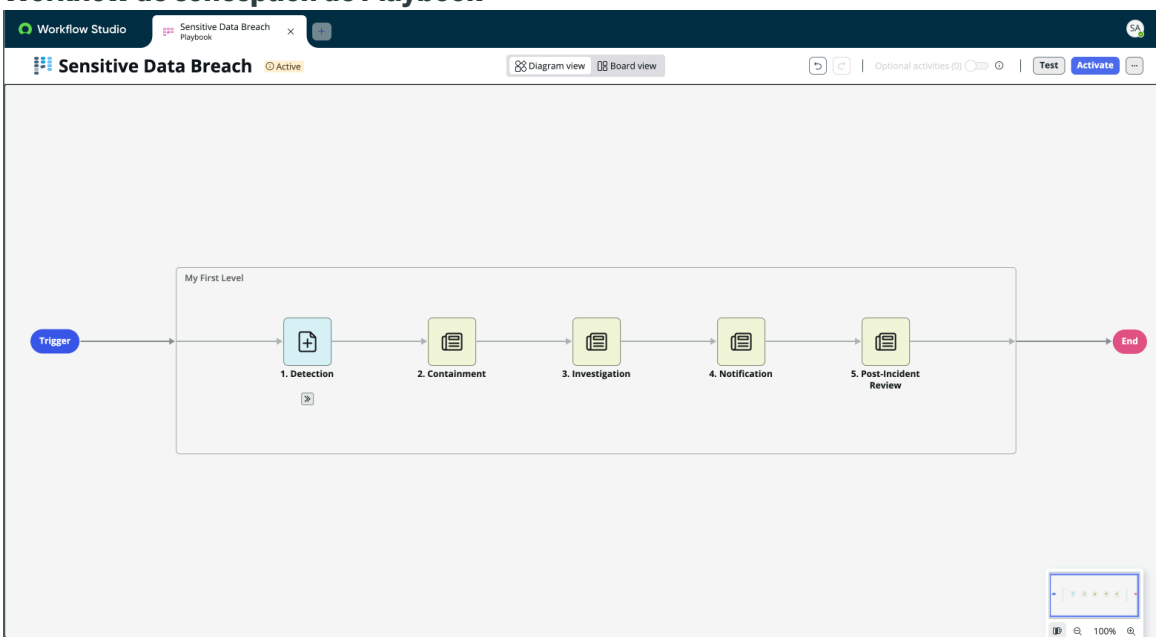
Activité	Description
Détection	Identifiez et confirmez l'accès non autorisé aux données sensibles ou leur exposition.
Confinement	Isolez les systèmes ou les utilisateurs affectés pour éviter toute fuite de données ou accès non autorisé.
Examen	Enquêtez sur la violation pour comprendre comment elle s'est produite, quelles données ont été affectées et l'impact potentiel.
Notification	Notifiez les équipes internes, les personnes concernées externes et les organismes de réglementation comme l'exige la loi ou la politique.
Rattrapage	Appliquez des mesures correctives pour remédier aux vulnérabilités, mettre à jour les politiques et prévenir de futures violations.
Reprise	Restaurez les systèmes à partir de sauvegardes sécurisées et validez l'intégrité des données après l'incident.
Examen post-incident	Analysez l'incident pour identifier les causes premières, améliorer les contrôles de sécurité et renforcer les politiques.

La figure suivante montre le workflow des activités et des étapes impliquées dans la création du Playbook de violation de données sensibles. Les étapes du Playbook varient en fonction du workflow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Workflow de conception de Playbook



Information associée

Ajouter un Playbook DLP

Annuler un Playbook DLP

Ajouter un Playbook DLP

Ajoutez un Playbook dans l'espace de travail de l'analyste Data Loss Prevention Incident Response qui peut servir de guide pour traiter et atténuer les incidents de perte de données susceptibles de compromettre la sécurité de votre organisation.

Avant de commencer

Rôle requis : sn_dlir.analyst : ajoutez ou affichez des playbooks dans l'espace de travail DLP.

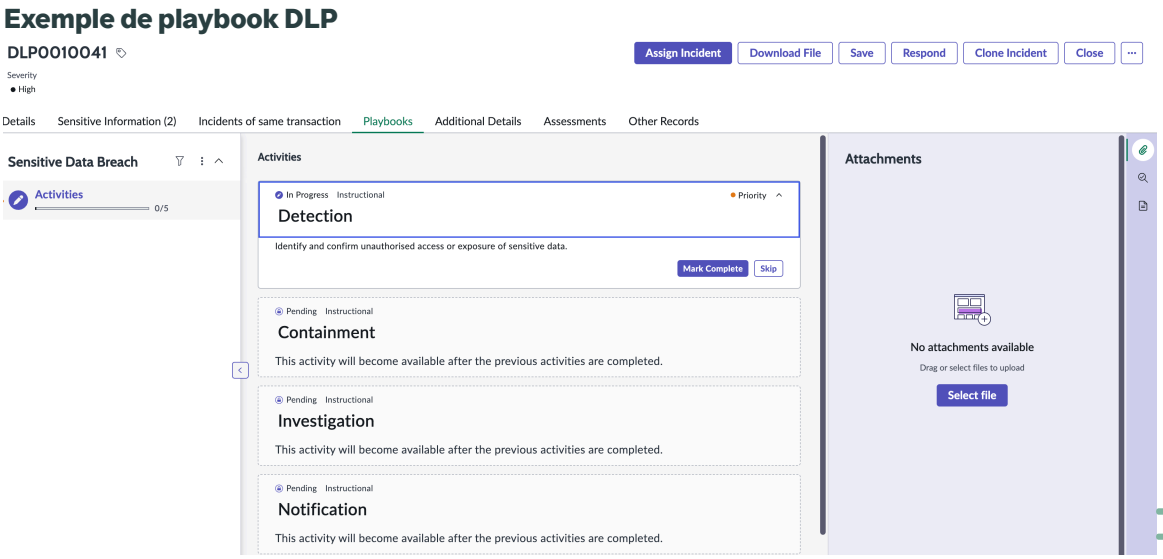
Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Sur la page Espace de travail de l'analyste DLP - Mes incidents, ouvrez n'importe quel incident DLP.
3. Ajoutez le Playbook.
   a. Accédez à l'onglet **Playbooks** .
   b. Dans le menu Actions d'interface utilisateur, sélectionnez l'icône Actions supplémentaires (icône puis sélectionnez **Ajouter des playbooks**.
   c. Dans la boîte de dialogue, sélectionnez un Playbook dans le menu déroulant.
   d. Sélectionnez **Ajouter des playbooks**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez chaque voie pour explorer les tâches effectuées par ce Playbook.



Annuler un Playbook DLP

Annulez un Data Loss Prevention Incident Response Playbook pour arrêter un flux d'entreprise lorsqu'il n'est plus valide.

Avant de commencer

Remarque : Les Playbooks sont automatiquement annulés lorsque l'incident DLP associé est fermé.

Rôle requis : sn_dlir.admin.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez n'importe quel incident DLP.
3. Accédez à l'onglet **Playbooks** .
4. Dans l'en-tête du Playbook que vous souhaitez annuler, sélectionnez l'icône Actions du Playbook (icône), puis sélectionnez **Annuler le Playbook**.
5. Fournir un motif d'annulation du Playbook.
6. Sélectionnez **Annuler le Playbook**.

Résultats

Une bannière apparaît sous l'en-tête du Playbook pour confirmer que le Playbook a été annulé.

Afficher les incidents DLP archivés

Utiliser DLP Analyst Workspace pour afficher les incidents DLP archivés

Avant de commencer

Rôle requis :

- sn_dlir.analyst : modifiez et affichez des incidents DLP.
- sn_dlir.analyst_read et sn_dlir.read : afficher les incidents DLP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
   Par défaut, la section Mes incidents s'affiche.
2. Cliquez sur **Incidents archivés**.
   La liste des incidents DLP archivés s'affiche.
3. Cliquez sur le bouton **Afficher le nombre d'incidents** pour afficher le nombre d'incidents archivés.

   Remarque :

   - Par défaut, le nombre d'incidents archivés est masqué pour améliorer le temps de chargement de la liste. Vous devez cliquer sur le bouton **Afficher le nombre d'incidents** pour afficher le nombre d'incidents. Un message d'information indiquant le nombre d'incidents s'affiche également.
   - La propriété système glide.ui.list.seismic.omit.count est activée dans le système de base pour les incidents archivés afin de masquer le nombre de listes d'incidents.

4. Sélectionnez un ou plusieurs incidents DLP que vous souhaitez afficher.
   L'incident DLP affiche la section des détails de l'incident.

   Remarque :

   - L'onglet **Autres incidents des utilisateurs finaux** inclut également les incidents archivés.
   - **Le contenu de correspondance** est pris en charge pour tous les incidents archivés (qui seront également pris en charge dans toutes les intégrations), mais **le téléchargement du fichier** n'est pris en charge que pour les intégrations Microsoft.

Tableau de bord de Data Loss Prevention Incident Response

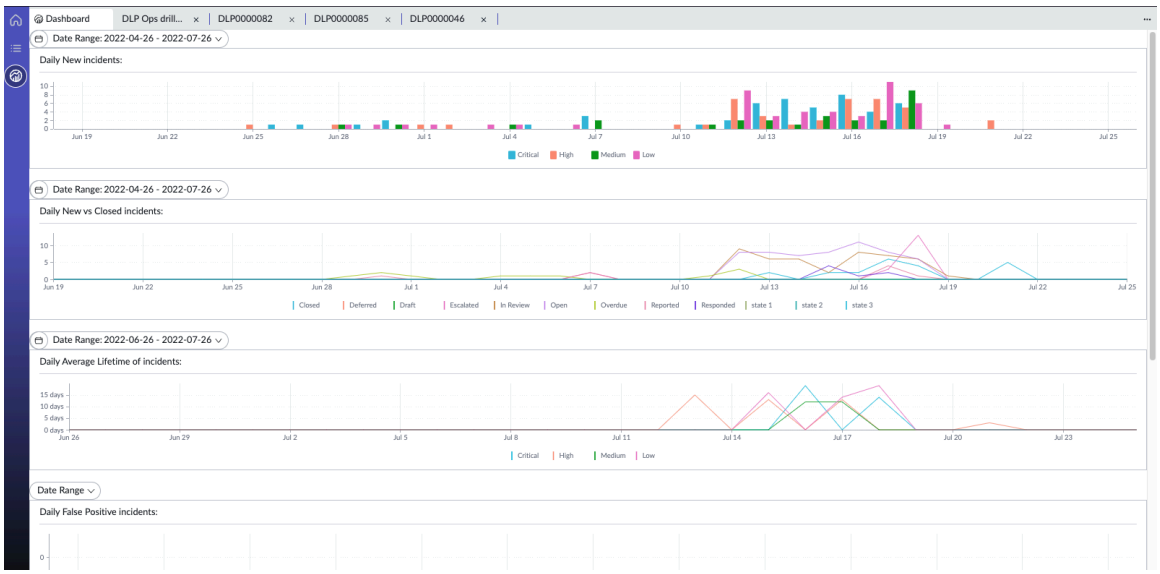
Le Data Loss Prevention Incident Response tableau de bord (DLP IR) fournit une vue d'ensemble de haut niveau de vos incidents DLP et des tendances quotidiennes des incidents dans votre instance sous la forme de graphiques graphiques. Ces graphiques vous aident à afficher, gérer et corriger efficacement les incidents DLP.

Le Data Loss Prevention Incident Response tableau de bord fournit des informations clés sur vos incidents DLP au quotidien. Vous pouvez configurer des indicateurs et collecter régulièrement des instantanés de données des incidents correspondant aux conditions des propriétés de l'indicateur. Les données collectées sont ensuite visualisées à l'aide de widgets dans le tableau de bord. Pour analyser les incidents DLP à différents intervalles de temps, vous pouvez appliquer différentes plages de dates.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord DLP



Analysez les tendances quotidiennes des incidents dans vos incidents DLP

Accédez au Data Loss Prevention Incident Response tableau de bord (DLP IR) pour analyser les tendances quotidiennes de vos incidents DLP et y remédier efficacement.

Avant de commencer

Rôle requis :

- sn_dlir.analyst : modifiez et affichez des incidents DLP.
- sn_dlir.analyst_read et sn_dlir.read : afficher les incidents DLP.

Pourquoi et quand exécuter cette tâche

Vous pouvez visualiser les tendances quotidiennes à l'aide de widgets dans le tableau de bord DLP. Les données ou les statistiques des tendances quotidiennes de vos incidents DLP sont collectées à partir des propriétés de l'indicateur Incidents quotidiens qui sont définies par votre organisation. Vous pouvez obtenir des aperçus clés en appliquant différentes plages de données pour analyser les incidents DLP dans différents intervalles de temps pour les graphiques suivants :

- **Nouveaux incidents quotidiens** : données de l'ensemble des incidents DLP créés quotidiennement, quel que soit l'état des incidents. Les incidents DLP sont classés en fonction de leur gravité, notamment moyenne, critique, élevée et faible. Chaque gravité d'incident DLP est représentée par une couleur particulière sur le graphique.
- **Incidents quotidiens nouveaux par rapport aux incidents fermés** : les différents états des incidents DLP et une comparaison entre les nouveaux incidents quotidiens et les incidents fermés quotidiens. La catégorie Nouveau quotidien inclut tous les incidents DLP ayant les états Ouvert, Brouillon, Escaladé, En cours de révision, En retard, Signalé, A répondu ou Personnalisé (le cas échéant). La catégorie Incident fermé inclut les incidents DLP fermés. L'état de chaque incident DLP est représenté par une couleur particulière sur le graphique.
- **Durée de vie moyenne quotidienne des incidents** : la durée de vie d'un incident est la période entre l'ouverture et la fermeture d'un incident DLP spécifique. La durée de vie moyenne quotidienne est calculée uniquement pour les incidents DLP fermés.
- **Incidents de faux positif quotidiens** : données de tous les incidents DLP signalés comme faux positifs quotidiens. Les incidents de faux positif quotidiens sont classés en fonction de leur gravité, notamment : moyenne, critique, élevée et faible. Chaque gravité d'incident faux positif quotidien est représentée par une couleur particulière sur le graphique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Âge par rapport à la gravité des incidents** : comparaison des données de tous les incidents DLP, classés par âge et configurés avec la gravité des incidents DLP. La catégorie Âge inclut tous les incidents DLP dont l'âge est inférieur à celui défini par votre organisation. Pour plus d'informations sur les graphiques d'âge, reportez-vous à la section Créer des configurations de graphique des âges. La gravité des incidents inclut tous les incidents DLP de la catégorie élevée ou faible. Chaque gravité est représentée par une couleur particulière sur le graphique.
- **Incidents escaladés quotidiennement** : données de tous les incidents DLP escaladés quotidiennement. Les incidents escaladés quotidiennement sont classés en fonction de leur gravité, notamment moyenne, critique, élevée et faible. Chaque gravité d'incident remontée quotidiennement est représentée par une couleur particulière sur le graphique.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Tableau de bord DLP**.
   La page Mon tableau de bord DLP s'affiche dans un nouvel onglet de navigateur.
2. Sélectionnez un widget de tableau de bord pour lequel vous souhaitez effectuer une analyse de tendance quotidienne.
   Par exemple, le graphique Nouveaux incidents quotidiens.
3. Examinez les widgets du tableau de bord pour identifier des tendances.
4. Cliquez sur **Plage de dates**.

Vue d'ensemble du tableau de bord DLP



5. Sélectionnez une plage de dates dans le calendrier, puis cliquez sur **Appliquer**.

   Example
   Par exemple, le graphique Nouveaux incidents quotidiens est mis à jour pour la plage de données sélectionnée.
6. Utilisez les filtres sous le graphique pour l'explorer et effectuer une analyse plus approfondie.

Intégration entrante pour Data Loss Prevention Incident Response

Créez un ou plusieurs incidents DLP à l'aide de l'API REST entrante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer un seul incident DLP

Rôle requis : sn_dlir.api_integration_user.

Pour créer un seul incident DLP, définissez les paramètres suivants si nécessaire :

Champ	Description
Méthode HTTP	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import
En-tête de demande	**Accepter:** `application/json` **Type de contenu :** `application/json`
Exemple de charge utile	{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>", "data_owner_email": "<value>", "destination": "<value>", "dest_ip": "<value>", "dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "", "file_created": "", "file_created_by": "", "file_location": "", "file_modified_by": "", "file_name": "", "file_owner": "", "file_permissions": "", "ftp_user_name": "", "last_modified": "", "machine_ip": "", "machine_name": "", "match_count": "", "policy_id": "", "policy_name": "", "printer_name": "", "printer_type": "", "print_job_name": "", "recipients": "", "scanned_machine": "", "scan_source": "", "seen_before": "", "sender":"", "source":"", "source_file":"", "source_ip":"", "source_ip_port":"", "subject":"", "url":"",

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	"user_justification":"" }

Exemple de réponse	{
	"import_set": "ISET0010003",
	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id": "7cda322297c2411056a43d1e6253af1f"
	}
	]
	}

Créer plusieurs incidents DLP

Rôle requis : sn_dlir.api_integration_user.

Pour créer plusieurs incidents DLP à partir de la même demande, définissez les paramètres suivants si nécessaire :

Champ	Description
Méthode HTTP	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple
En-tête de demande	**Accepter:** `application/json` **Type de contenu :** `application/json`
Exemple de charge utile	{ "records": [{ "file_name": "<value>", "file_modified_by": "<value>", "work_notes": "<value>", "url": "<value>", "scan_source": "<value>", "data_owner_email": "<value>", "file_created_by": "<value>", "file_owner": "<value>", "policy_name": "<value>" },

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description

	{
	"dest_ip": "<value>",
	"dest_ip_port": "<value>",
	"detection_date": "<value>",
	"endpoint_on_corporate_net": "<value>",
	"files": "<value>",
	"file_created": "<value>",
	"file_created_by": "<value>",
	"file_location": "<value>",
	"file_modified_by": "<value>",
	"file_name": "<value>",
	"file_owner": "<value>",
	}
	]
	}

Exemple de réponse	{
	"import_set_id": "a38f69229734dd1056a43d1e6253af75",
	"multi_import_set_id":
	"e78f69229734dd1056a43d1e6253af75"
	}

Remarque : Par défaut, la transformation est asynchrone. Pour définir la transformation synchrone, créez un nouvel enregistrement dans la table Insertion multiple REST [sys_rest_insert_multiple], sélectionnez la table source comme **sn_dlir_incident_import**, puis définissez la transformation sur **synchrone**.

Intégrations DLP

Le Data Loss Prevention Incident Response système de base comprend des intégrations à des progiciels tiers de prévention des pertes de données.

Cette section fournit des instructions pour activer les modules d'extension et configurer les intégrations ServiceNow tierces. Vous y trouverez également des instructions de base pour développer vos propres intégrations, ainsi que des détails sur des intégrations spécifiques incluses dans le système de base.

Configurations d'intégration

Le système de base comprend une série de cartes pour chacune des implémentations d'intégration que vous pouvez activer et utiliser. En outre, des cartes sont affichées pour toutes les intégrations publiées sur le ServiceNow Store qui ont des dépendances à Opérations de sécurité des modules d'extension. Les cartes d'intégration peuvent être affichées en sélectionnant **Security Operations** > **Configurations d'intégration**.

Data Loss Prevention Incident Response prend en charge les progiciels de prévention de la perte de données tiers suivants :

Symantec Intégration pour Data Loss Prevention Incident Response

L'intégration Symantec DLP prend en charge l'ingestion des incidents créés lors Symantec Data Loss Prevention Incident Response du Data Loss Prevention Incident Response déploiement. Après l'ingestion, vous pouvez utiliser les fonctionnalités de gestion des incidents pour corriger les incidents DLP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Vue d'ensemble et fonctionnalités principales

L'intégration Symantec DLP aide les entreprises à suivre l'utilisation et le mouvement des données sensibles sur différentes plateformes.

Cette intégration comprend les fonctionnalités clés suivantes :

- Possibilité de créer plusieurs profils d'intégration pour différents Symantec points de terminaison d'API.
- Ingestion planifiée d'incidents Symantec DLP depuis votre ServiceNow instance.
- Possibilité d'appliquer des filtres d'API pour récupérer les incidents qui correspondent aux critères de filtre et de spécifier le filtre pour Symantec les incidents DLP qui doivent être importés.
- Mappage des états des incidents DLP dans votre ServiceNow instance aux états des incidents DLP dans Symantec.
- Mettez automatiquement à jour l'état de l'incident Symantec lorsque l'état change dans votre ServiceNow instance.
- Possibilité de personnaliser et de définir le mappage de gravité entre les incidents Symantec DLP et les incidents ServiceNow.

Pour en savoir plus sur l'intégration, consultez la documentation produit Symantec .

Mise en route de l'intégration Symantec DLP pour la protection contre la perte de données

Avant de pouvoir utiliser l'intégration, vous devez la télécharger à partir du ServiceNow® Store.

Liste de vérification

Passez en revue les informations suivantes avant de commencer à configurer votre Symantec intégration DLP pour la protection contre la perte de données.

Liste de vérification

Champ	Description
Vérifiez que vous avez affecté les rôles requis de ServiceNow AI Platform l'application Prévention des pertes de données et de l'application MID.	Les rôles suivants sont utilisés dans l'intégration Symantec DLP sur :ServiceNow AI Platform • L'administrateur (admin) installe les applications à partir de et ServiceNow® Store affecte l'administrateur de la prévention des pertes de données (sn_dlir.admin).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Champ	Description
	• L'utilisateur disposant du rôle sn_dlir.admin peut configurer l'intégration et configurer les profils d'incident. • Les utilisateurs ayant le rôle sn_dlir.analyst auront des rôles de lecture dans l'intégration.
Affectez les rôles d'utilisateur DLP requis Symantec .	Passez en revue les rôles et autorisations d'intégration Symantec DLP.
Vérifiez que vous utilisez Symantec DLP 15.8	L'intégration Symantec DLP pour Data Loss Prevention est testée avec la version 15.8 de Symantec Data Loss Prevention. **Remarque :** Assurez-vous d'utiliser Symantec DLP 15.8
Vérifiez que ServiceNow® l'application principale requise pour prendre en charge l'intégration Symantec DLP est installée et activée.	Vérifiez que les applications DLP et les applications courantes de support de sécurité suivantes sont installées et activées à partir de ServiceNow Store. Si ce n'est pas le cas, installez-le et activez-le sur l'application. • Security Support Common • Data Loss Prevention Incident Response

Installer et configurer l'intégration DLP pour la protection contre la Symantec perte de données

Installez et configurez l'intégration Symantec DLP sur ServiceNow® Store votre ServiceNow AI Platform instance. Commencez à enquêter sur les incidents DLP à l'aide des données d'incident Symantec DLP.

Avant de commencer

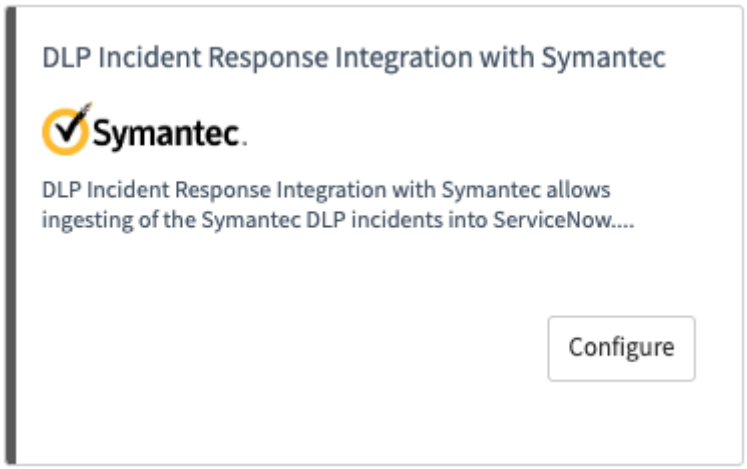
Rôle requis : sn_dlir.admin

Procédure

1. Téléchargez l'intégration Symantec DLP à partir de et ServiceNow® Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez l'intégration de réponse aux incidents DLP avec Symantec tuile et cliquez sur **Configurer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



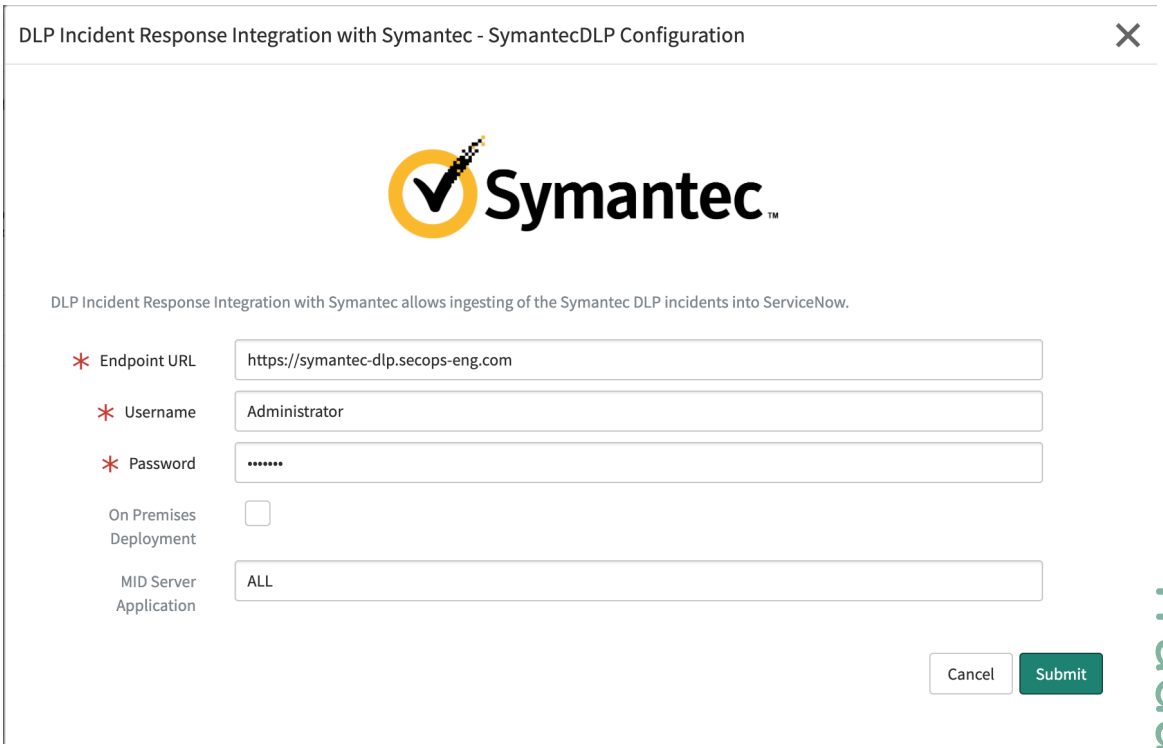
4. Remplissez les champs du formulaire.

Formulaire Configuration de l'intégration DLP Symantec

Champ	Description
Nom	Nom de la configuration de l'intégration Symantec DLP.
URL du point de terminaison	Symantec Point de terminaison REST API.
Nom d'utilisateur	Symantec Nom du compte. Pour plus d'informations sur les rôles et autorisations requis, voir Rôles et autorisations .
Mot de passe	Symantec Mot de passe du compte.
Déploiement sur site	Option que vous pouvez sélectionner si votre Symantec est déployé dans une instance locale. Lorsque vous sélectionnez cette option, vous devez utiliser le serveur MID pour vous connecter à Symantec.
Application de serveur MID	Nom de l'application MID utilisée pour communiquer avec Symantec. Ce champ est nécessaire lorsque vous sélectionnez l'option **Déploiement sur site** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.

Résultats

Remarque : Veuillez connecter la sous-production Symantec à la sous-production ServiceNow. Gardez tous les noms d'utilisateur et mots de passe synchronisés entre les instances pour éviter que les comptes ne soient déconnectés.

Une fois que vous avez validé et soumis la configuration, l'intégration Symantec DLP est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

Créer un profil pour Symantec l'intégration DLP

Créez un profil d'incident dans votre ServiceNow AI Platform instance. Déterminez les Symantec incidents DLP qui se prêtent à la création d'incidents DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Configurez pour ServiceNow AI Platform® extraire les incidents DLP à partir du point de Symantec terminaison. Stockez ces incidents dans votre ServiceNow® instance en tant qu'incidents DLP.

Procédure

1. Accédez à la **Intégration DLP Symantec** > **Profil d'incident**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs de la section Nom du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

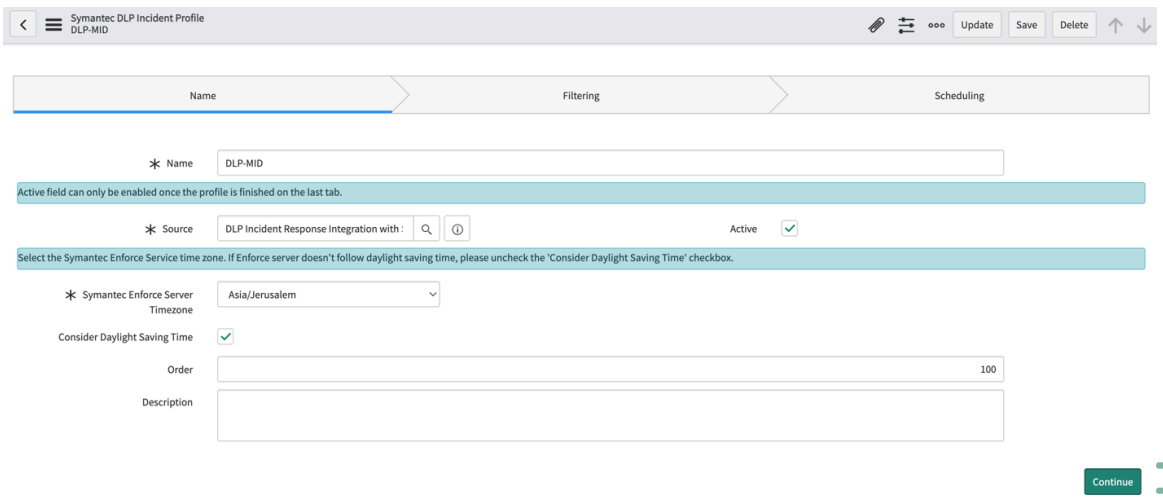
Créer un profil

Champ	Description
Nom	Nom du profil. Ce champ vous permet d'identifier le profil. **Remarque :** Le nom doit être unique pour chaque profil.
Source	Symantec Instance DLP que vous avez configurée pour ingérer des incidents. Si vous avez configuré plusieurs instances, sélectionnez l'instance appropriée pour les types d'incidents que vous prévoyez d'ingérer pour le profil.
Actif	Option permettant d'indiquer si le profil est actif. Ce champ ne peut être activé qu'une fois que vous avez cliqué sur **Terminer** dans la section Planification. Lorsque le profil est actif, cela implique que l'interroge ServiceNow AI Platform activement les Symantec incidents DLP. Les incidents DLP correspondants sont créés dans DLP lorsque les conditions de filtrage sont mises en correspondance en fonction des paramètres de planification que vous avez fournis.
Fuseau horaire du serveur Symantec Enforce	Sélectionnez le fuseau horaire pour le serveur Symantec Enforce dans le profil afin que les incidents ne soient pas manqués en raison de problèmes de fuseau horaire.
Prendre en compte l'heure d'été	Cochez cette case si le serveur d'application suit l'heure d'été.
Ordre	Ordre d'exécution du profil. Le profil avec l'ordre le plus bas considéré comme la priorité la plus élevée. Par défaut, la valeur est 100.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Description	Description unique pour ce profil.



Que faire ensuite

Pour passer à la section Filtrage, cliquez sur **Continuer**.

Définir les filtres à appliquer pour la création d'incident

Définissez et définissez des conditions de filtre pour analyser les incidents DLP entrants Symantec . Déterminez les incidents qui doivent être créés en tant qu'incidents DLP dans ServiceNow®.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Le filtrage vous aide à isoler les incidents DLP et à limiter le nombre d'incidents DLP que vous créez. Si des critères de filtrage supplémentaires sont définis, seuls les incidents qui correspondent aux conditions sont créés.

Procédure

1. Cochez la case **Filtre basé sur une API pour l'ingestion d'incidents** afin d'appliquer les filtres d'API et de récupérer les incidents qui correspondent aux critères de filtre.
2. Ajoutez les filtres d'API.
   L'exemple suivant montre les filtres d'API.

```
{
        "operandOne": {
          "name": "incidentStatusName"
        },
        "filterType": "string",
        "operator": "EQ",
        "operandTwoValues": [
          "incident.status.New"
        ]
      }
```

Remarque : Pour plus d'informations sur les filtres d'API sur l'intégration Symantec, consultez Listes d'incidents : Paramètres - Détails de l'objet de la demande .

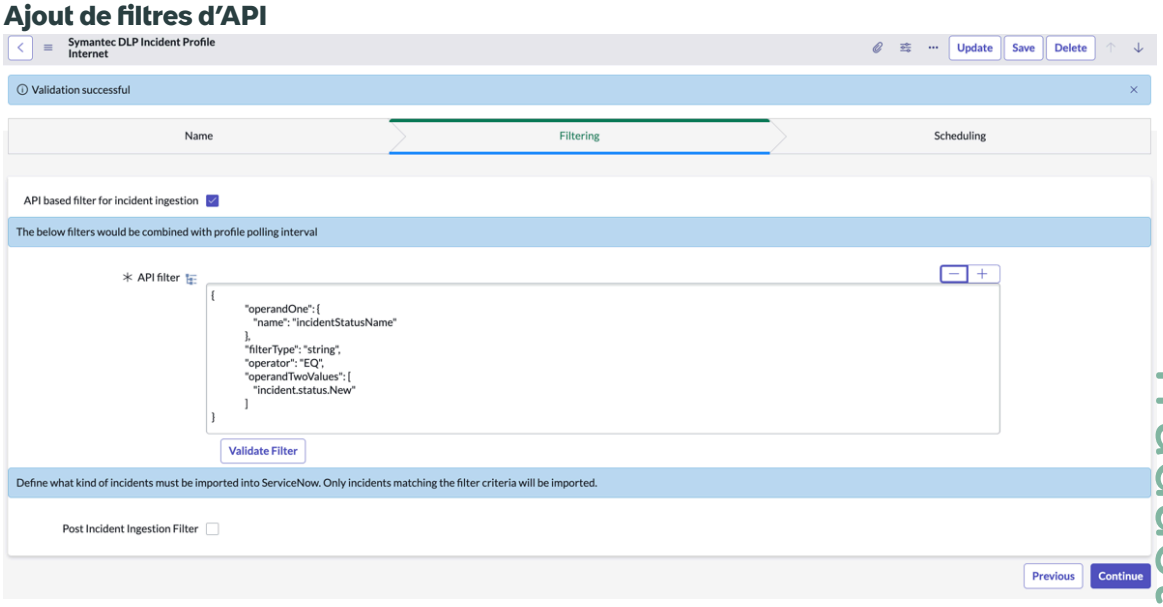
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

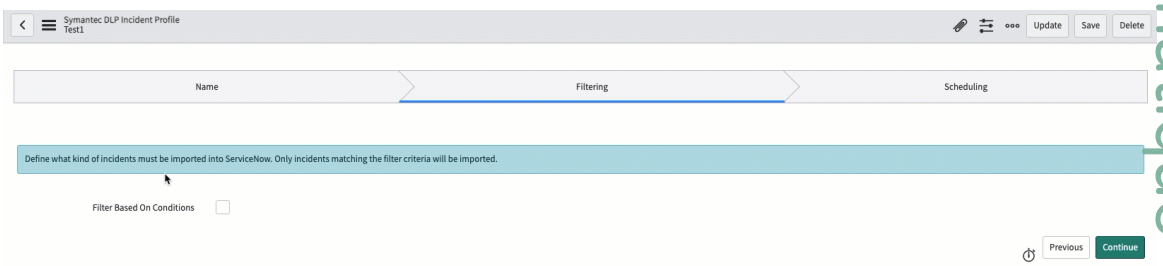
3. Cliquez sur **Valider le filtre** après avoir appliqué les filtres API.

> **Remarque :** Si la validation échoue, un message d'erreur s'affiche indiquant que la validation a échoué, ce qui se produit lorsque les filtres ne sont pas correctement saisis conformément aux API Symantec.

Ajout de filtres d'API



4. Cochez la case **Filtre d'ingestion post-incident** pour définir les critères qu'un incident Symantec DLP entrant doit satisfaire pour qu'un incident DLP soit créé.
   Les options du premier champ des Conditions de filtre correspondent aux champs disponibles dans l'incident DLP. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.
5. Dans le générateur de conditions, définissez les filtres dans le champ **Conditions de filtre** .



6. Pour ajouter d'autres conditions, cliquez sur **ET** ou **OU**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
- Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

Que faire ensuite
Pour configurer le calendrier, cliquez sur **Continuer**.

Configurer le stockage des fichiers de preuves

Configurez le stockage des fichiers de preuves pour stocker en toute sécurité le fichier de preuves pour les incidents DLP.

Avant de commencer
Rôle requis : sn_dlir.admin

Vérifiez que l'utilisateur Symantec que vous configurez pour ServiceNow L'intégration DLP Symantec doit avoir les options Corps, Pièces jointes et Message d'origine activées à partir de la page de configuration des rôles sur le portail Symantec DLP. Pour plus d'informations, consultez la section Attributs d'affichage disponible sur le document Configuration des rôles .



Pourquoi et quand exécuter cette tâche
Vous pouvez configurer le stockage des fichiers de preuves pour stocker les fichiers en toute sécurité. Cela fournit une option de stockage interne dans l'instance ServiceNow, garantissant que les fichiers sont stockés et chiffrés Chiffrement de champà l'aide de l'instance . Pour plus d'informations, consultez la documentation Chiffrement de champ sur Now Platform.

Lorsque l'analyste DLP effectue l'action Télécharger les fichiers de preuves pour les incidents DLP à partir d'Analyst Workspace, le fichier est téléchargé à partir du stockage sélectionné si l'option de stockage des fichiers de preuves est activée. Sinon, le fichier sera téléchargé directement à partir de la source Symantec et ne sera pas conservé dans l'instance ServiceNow.

Remarque : Lorsqu'un analyste DLP effectue l'action Télécharger les fichiers de preuves pour les incidents DLP à partir d'Analyst Workspace, le fichier est téléchargé à partir du stockage sélectionné si l'option de stockage des fichiers de preuves est activée. Sinon, le fichier sera téléchargé directement à partir de la source Symantec et ne sera pas conservé dans l'instance ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Intégration DLP Symantec** > **Profil d'incident**.
2. Cliquez sur la section **Stockage des preuves** dans le formulaire de profil d'incident.
3. Cochez la case **Stockage des fichiers de preuves** pour activer le stockage des fichiers.
4. Sélectionnez le type de stockage préféré.

Type	Description
Stockage des fichiers de preuves	Option permettant d'activer le stockage des fichiers de preuves.
Type de stockage	Option permettant de sélectionner le type de stockage préféré. **Remarque : Stockage ServiceNow** : cela stockera les fichiers de preuves dans l'instance ServiceNow dans un format chiffré.

5. Cliquez sur **Continuer** et passez à la section **Planification** .

Résultats

Les fichiers de preuves sont stockés conformément à la configuration, une fois l'ingestion de l'incident terminée.

Télécharger les fichiers de preuves

Téléchargez des fichiers de preuves d'incidents DLP qui enfreignent la politique DLP sur Symantec.

Avant de commencer

Téléchargez ce fichier sur votre ordinateur local à partir de l'espace de travail de l'analyste DLP IR et de l'espace de travail de l'utilisateur final DLP IR. L'action Télécharger les fichiers n'est disponible que pour les approbateurs sur l'espace de travail de l'utilisateur final DLP IR.

Rôle requis :

- sn_dlir.analyste
- sn_dlir.secure_file_download (tout approbateur disposant de ce rôle)

Procédure

1. Accédez à la **Tous** > **Intégration DLP Symantec** > **Paramètre**.
2. Activer **Si le téléchargement du fichier de violation de l'incident signalé est autorisé** .
   Une fois cette propriété activée, vous pourrez désormais voir l'action **Télécharger le fichier** dans DLP Analyst Workspace pour tout incident Symantec DLP.
3. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
4. Ouvrez un enregistrement d'incident DLP qui est ingéré à partir de la source Symantec.
5. Cliquez sur **Télécharger le fichier**.

Remarque : Le fichier qui a enfreint la politique DLP sur Symantec sera téléchargé sur l'ordinateur local de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour que l'approbateur affiche l'action Télécharger le fichier, procédez comme suit :

6. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'utilisateur DLP**.
   La page Mes incidents DLP s'affiche dans un nouvel onglet.
7. Sélectionnez **le module Mes approbations** disponible sous le module Mes incidents DLP.
   La vue de liste Mes approbations s'affiche.
8. Ouvrez un enregistrement de demande d'approbation qui est déclenché pour un incident Symantec DLP.
9. Cliquez sur l'icône d'informations (i) disponible dans le champ Incident DLP de la vue de formulaire.
10. Cliquez sur **Télécharger le fichier**.

Résultats

Après avoir effectué cette action, le fichier de preuves au format ZIP (si l'incident comporte des violations dans plusieurs composants et/ou si les données du message d'origine sont également disponibles) ou un fichier unique (si l'incident comporte des violations dans un seul composant ou si seules les données du message d'origine sont disponibles) est téléchargé sur l'ordinateur local de l'utilisateur.

Remarque : En tant qu'administrateur DLP, vous pouvez contrôler l'accès à l'action **Télécharger le fichier** en désactivant l'option Le **téléchargement du fichier de violation de l'incident signalé doit-il être autorisé**à partir de la page **Paramètres avancés** . Pour plus d'informations, voir Configurer les paramètres avancés pour Data Loss Prevention Incident Response .

Prévisualiser les fichiers de preuves

Prévisualisez Data Loss Prevention Incident Response les fichiers de preuves dans l'espace de travail de l'analyste DLP IR.

Avant de commencer

Important : Lors de l'utilisation de l'action Fichiers de preuves dans l'espace de travail de l'analyste DLP, les fichiers de preuves sont temporairement stockés dans la base de données ServiceNow dans un format non chiffré. Si vous ne souhaitez pas stocker les fichiers de preuves, désactivez la fonctionnalité d'aperçu des fichiers de preuves. Pour plus d'informations, consultez Configurer les paramètres avancés.

Rôle requis : sn_dlir.analyst

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez un enregistrement d'incident DLP.
3. Dans la barre latérale contextuelle, sélectionnez l'icône Fichiers de preuves ( ).
4. Dans l'onglet **Fichiers de preuves** , sélectionnez la carte **Fichier de preuves** pour afficher un aperçu des fichiers de preuves dans la visionneuse de documents.

   La fonctionnalité d'aperçu est différente pour chaque type de fichier, comme indiqué dans le tableau suivant.

Format de fichier	Extension de fichier
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg et .webp. Les fichiers image s'ouvrent en mode visionneuse de documents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Format de fichier	Extension de fichier
Microsoft Fichiers Office	.doc, .docx, .ppt, .pptx, .xls et .xlsx Les fichiers Office s'ouvrent en mode visionneuse de documents.
Fichiers texte	.txt Les fichiers texte s'ouvrent en mode éditeur de texte.
Fichiers courrier	.Eml **Remarque :** La taille du fichier doit être inférieure à 5 Mo. Vous devez d'abord télécharger le fichier pour prévisualiser son contenu.
Fichiers PDF	.PDF ○ Saisissez un mot clé pour rechercher le document. ○ Fonctions de zoom avant et arrière pour ajuster la vue et améliorer la lisibilité. ○ Faites pivoter la page dans le sens des aiguilles d'une montre ou dans le sens inverse des aiguilles d'une montre pour afficher le contenu plus clairement.

Remarque :

Les fichiers binaires ne seront pas rendus et devront être téléchargés pour prévisualiser leur contenu. La fonctionnalité d'aperçu du fichier de preuve fonctionne également pour les incidents archivés.

Planifier la récupération de l'incident Symantec DLP

Définissez un calendrier pour récupérer les données d'incident et ingérer les Symantec incidents DLP qui correspondent aux critères du profil. Configurez le calendrier pour définir comment et quand extraire des incidents de Symantec.

Avant de commencer
Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche
Vous pouvez planifier la fréquence à laquelle vous interrogerez les incidents futurs qui correspondent à la configuration de profil d'incident. Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Le profil peut être configuré pour effectuer une récupération ponctuelle à l'aide de la case à cocher **Récupération ponctuelle** . La date historique peut aller jusqu'aux trois derniers mois à compter de la date actuelle.

L'intervalle d'interrogation est configuré individuellement pour chaque profil. Les différents intervalles d'interrogation peuvent avoir un impact sur les performances de l'intégration Symantec des incidents DLP. Lors de la planification, prévoyez d'équilibrer la charge du système par rapport à l'urgence d'un incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

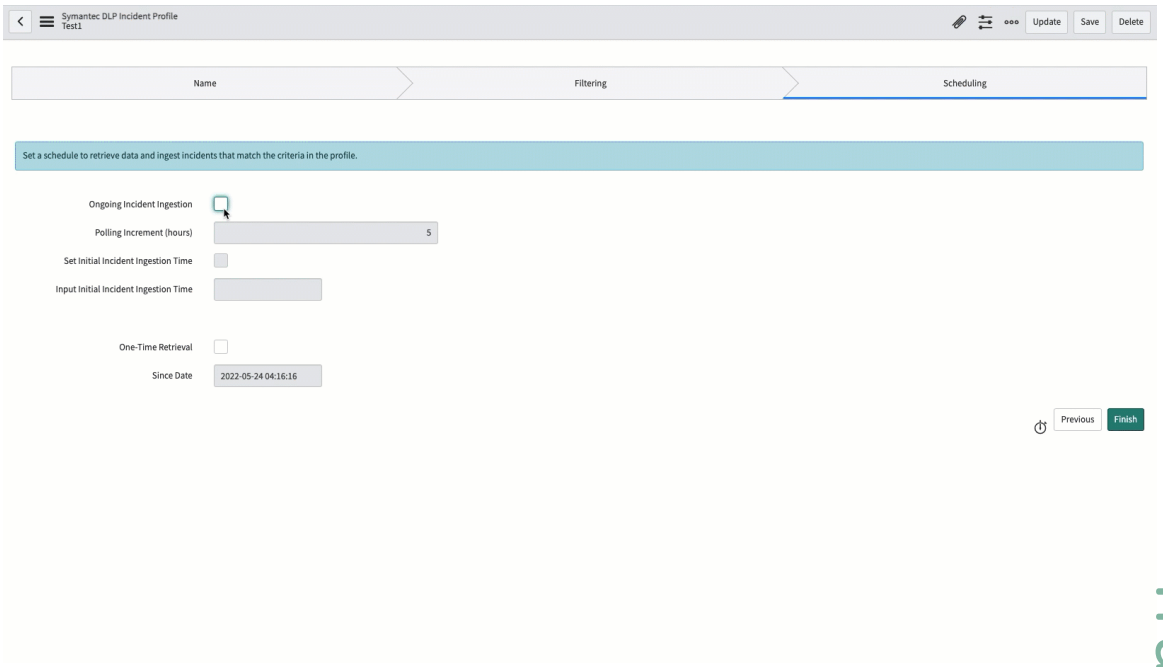
1. Définissez un calendrier pour récupérer les données et ingérer les incidents qui correspondent aux critères du profil.
2. Renseignez les champs du formulaire.

Calendrier de l'incident DLP

Champ	Description
Intégration de l'incident en cours	L'ingestion d'incidents en cours que l'instance extrait de Symantec ServiceNow AI Platform pour les nouveaux incidents. Les incidents DLP sont créés si des incidents déclenchés sont détectés et que les critères de filtrage de génération d'incidents correspondent.
Incrémentation du sondage (minutes)	La fréquence d'interrogation définie en minutes. Ce champ est automatiquement défini sur 300 minutes.
Définir le délai d'intégration de l'incident initial	Option permettant de définir une date et une heure pour l'ingestion initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation.
Délai d'intégration de l'incident initial d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.
Délai d'intégration de l'incident initial	Première fois que les données sont ingérées. Vous pouvez voir que ces valeurs commencent à s'afficher lorsque le délai d'intégration de l'incident initial est défini.
Délai d'intégration de l'incident suivant (estimé)	Période suivante pour une ingestion d'incident estimée.
Récupération ponctuelle	Option permettant d'activer l'extraction unique des données historiques. Si ce champ est sélectionné, les données historiques sont extraites de Symantec DLP en fonction de la date ajoutée dans le champ **Depuis la date** .
Date de début	Date à partir de laquelle les données sont censées être récupérées à partir de Symantec. Ce champ peut être défini sur trois mois au maximum.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Pour enregistrer la configuration du profil créé, cliquez sur **Terminer** dans la fenêtre contextuelle.
4. Pour activer le profil, ouvrez le profil créé.
5. Activer **l'option Actif** .
6. Cliquez sur **Mettre à jour**.

Résultats

Une fois la création et l'activation du profil réussies, les incidents sont récupérés périodiquement selon la configuration définie dans le profil et ajoutés à la table des incidents DLP.

Mappage Symantec des états des incidents DLP avec ServiceNow l'état de l'incident

Synchronisez l'état des incidents DLP ingérés sur le ServiceNow avec les incidents DLP du Symantec. Mappez le champ **État des incidents ServiceNow** avec le champ **État des incidents Symantec** .

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

L'état de l'incident est récupéré dynamiquement à partir de la source du Symantec point de terminaison qui est ajoutée au mappage. Vous devez effectuer un mappage de l'état des incidents un à un.

Procédure

1. Accédez à la **Intégration DLP Symantec** > **Mappage de l'état des incidents**.
2. Fournissez un **nom** pour identifier le mappage.
3. Sélectionnez l'intégration **source** à partir de laquelle vous souhaitez récupérer l'état.
4. Mappez **l'état de l'incident DLP** avec **l'état de l'incident Symantec**.

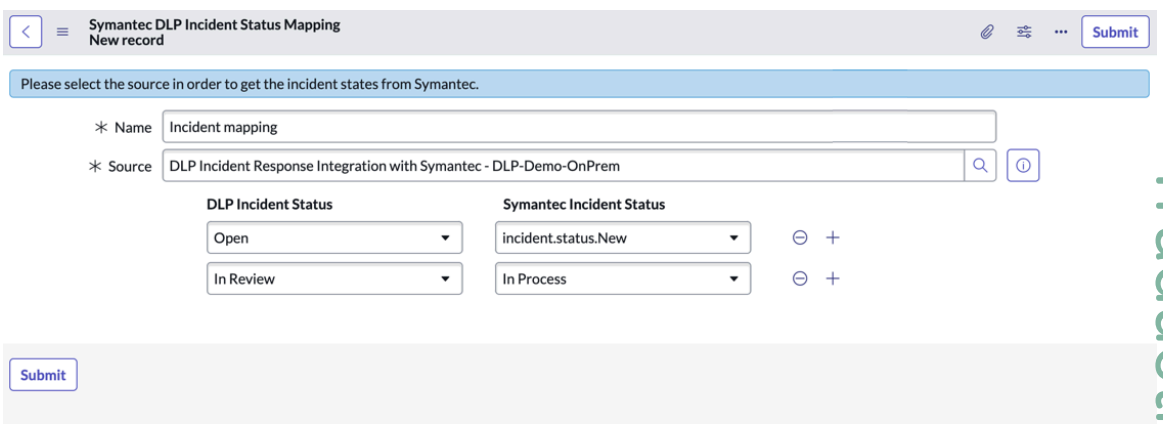
> **Remarque :** Il n'est pas nécessaire de mapper tous les états, vous pouvez mapper uniquement les états requis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage du statut des incidents Symantec DLP

Champ	Description
Nom	Nom de l'enregistrement du mappage.
Source	Source Symantec Endpoint configurée à partir de laquelle vous souhaitez extraire l'état de l'incident.
État des incidents DLP	Liste des états des incidents DLP.
État des incidents Symantec	Liste des états récupérés à partir de la source (point de terminaison Symantec).



5. Cliquez sur **Envoyer**.

Résultats
Une fois l'enregistrement créé avec succès pour mapper les états des incidents, l'état des incidents est synchronisé avec Symantec l'état ServiceNow des ServiceNow incidents DLP.

Si vous modifiez le statut d'un incident DLP sur votre ServiceNow instance, le statut des incidents DLP associés Symantec sera modifié sur la plateforme source Symantec en fonction du mappage défini dans l'enregistrement.

Mappage de gravité entre les incidents Symantec DLP et les incidents ServiceNow

Utilisez la fonctionnalité de mappage de gravité pour configurer et synchroniser le mappage entre Symantec les incidents et ServiceNow AI Platform® les incidents.

Avant de commencer
Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche
Le mappage de gravité DLP vous permet de mapper la gravité de la source avec la gravité de l'incident DLP. Vous pouvez personnaliser et définir la valeur de gravité de la source et la mapper à la valeur de gravité d'incident DLP souhaitée.

Procédure

1. Accédez à la **Intégration DLP Symantec** > **Mappage de sévérité d'incident**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Traduction automatique

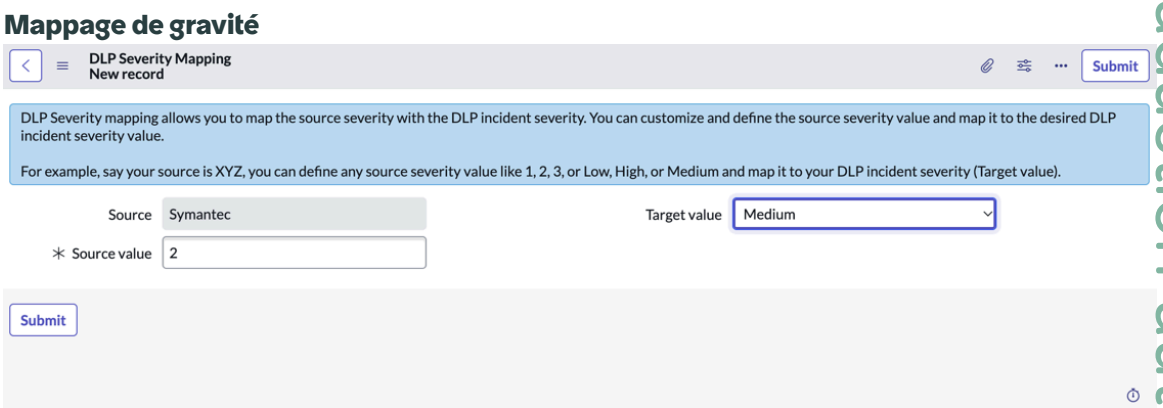
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de gravité DLP

Champ	Description
Source	Source de point de terminaison Symantec configurée à partir de laquelle vous souhaitez extraire l'incident.
Valeur cible	La valeur cible est l'ID de gravité de l'incident DLP. Les valeurs disponibles sont Critique, Élevé, Moyen, Faible et Information (utilisé comme sévérité des informations dans Symantec).
Valeur source	La valeur source est la gravité de l'incident Symantec.

Remarque : Dans le système de base, quatre mappages de gravité sont envoyés aux utilisateurs DLP.

4. Cliquez sur **Envoyer**.



Configurer des règles de réponse intelligente

Configurez la ou les règles de réponse intelligente Symantec pour effectuer des actions de réponse sur les incidents Symantec DLP ingérés.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Vérifiez que l'utilisateur Symantec que vous configurez pour ServiceNow Symantec DLP Integration doit avoir ces règles de réponse intelligente sélectionnées sur la page **de configuration des rôles** . Pour plus d'informations, consultez la section **Actions** disponible dans le document Configuration des rôles .

Pour la ou les règles de réponse intelligente extraites, l'administrateur DLP peut créer la ou les règles d'option de réponse aux incidents et les mappages d'options de réponse pour configurer la ou les actions de réponse à effectuer sur les incidents Symantec DLP ingérés.

Procédure

1. Accédez à la **Tous** > **Intégration DLP Symantec** > **Règles de réponse intelligente**.
   Vous pouvez afficher toutes les options de réponse intelligente disponibles pour chaque configuration d'intégration configurée. Pour plus d'informations, Installer et configurer l'intégration DLP pour la protection

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

contre la Symantec perte de données consultez et suivez la procédure expliquée configurer la source de configuration de l'intégration Symantec si elle n'est pas configurée)

2. Cliquez sur l'une des règles de réponse intelligente pour ouvrir sa vue de formulaire.

   Suivez Créer des règles pour les options de réponse aux incidents pour créer des règles d'option de réponse aux incidents et des mappages d'options de réponse pour afficher cette règle de réponse intelligente sur le modal Répondre de l'espace de travail DLP.

3. Créez les règles d'approbation pour la règle de réponse intelligente à l'aide de l'onglet **Règles d'approbation** de la liste connexe ou en suivant la procédure expliquée dans la section Configurer les règles d'approbation.
   Les règles d'approbation pour chaque règle de réponse intelligente seront visibles dans la liste connexe Règles d'approbation.
4. Après avoir créé la ou les règles d'option de réponse aux incidents, vous pouvez voir l'enregistrement dans la liste connexe de l'enregistrement Règle de réponse intelligente.
5. Utilisez le bouton **Actualiser la règle de réponse intelligente** dans la vue de liste pour mettre à jour manuellement la source.
   Les règles de réponse intelligente ajouteront, mettront à jour ou supprimeront automatiquement chaque jour pour chaque source.

Exécuter les règles de réponse intelligente

Utilisez cette fonctionnalité pour exécuter des règles de réponse intelligente pour les incidents Symantec DLP.

Avant de commencer

Vous devez configurer les règles de réponse intelligente en suivant la procédure expliquée ici dans cette section, Configurer des règles de réponse intelligente.

Rôle requis : sn_dlir.admin

Remarque :

Les options de réponse sur l'espace de travail sont disponibles pour l'utilisateur final, l'analyste ou le gestionnaire en fonction de la configuration mentionnée dans la section Configurer l'option de réponse pour vos incidents DLP.

Procédure

1. Accédez à la **Tous** > **DLP** > **Espace de travail de l'utilisateur DLP**.
2. Ouvrez un incident Symantec DLP.
3. Cliquez sur **Répondre**.
4. Sélectionnez l'option de réponse dans la liste déroulante Réponse.
   Les options de réponse seront visibles en fonction de la configuration de la **règle de l'option de réponse aux incidents** et des **mappages d'options de réponse**.
5. Cliquez sur **Envoyer**.

Remarque : Vous pouvez également configurer la ou les règles d'approbation pour les options de réponse en suivant la procédure expliquée dans la Créer des règles d'approbation section. Lorsqu'une règle d'approbation est configurée pour la règle de réponse intelligente, le flux d'approbation est déclenché en premier et, après avoir reçu toutes les approbations, le flux d'options de réponse intelligente est déclenché. L'état de l'incident DLP est mis à jour en fonction de l'état cible du mappage d'options de réponse après l'exécution réussie de l'option de réponse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer les paramètres d'intégration Symantec DLP

Modifiez les propriétés système par défaut de l'intégration Symantec DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

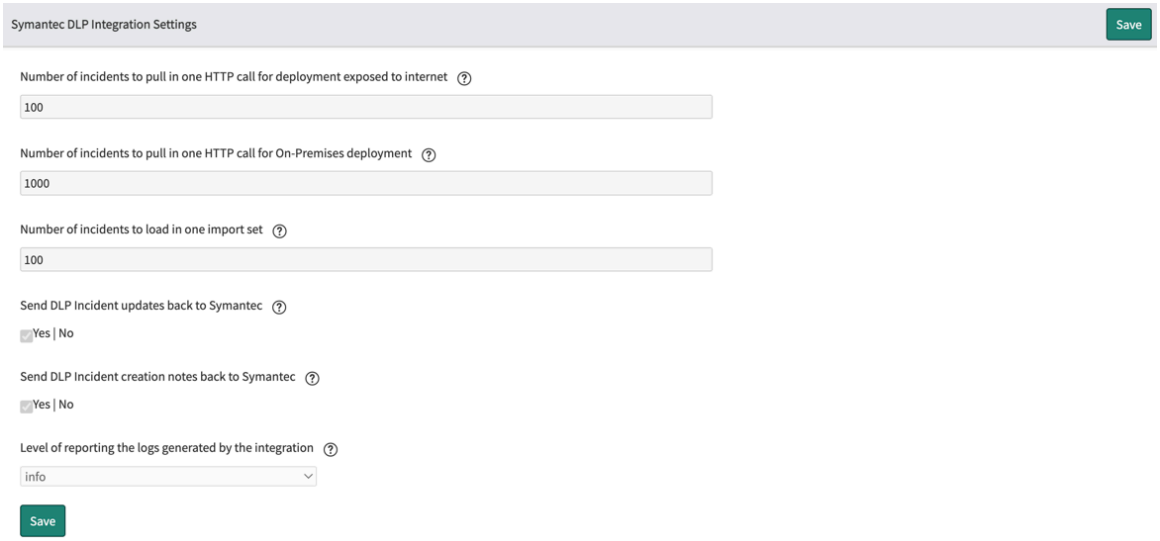
1. Accédez à la **Intégration DLP Symantec** > **Paramètres**.
2. Modifiez les paramètres suivants selon vos besoins.

Paramètres

Champ	Description
Appliquer une limite au Nombre d'incidents à extraire dans un appel HTTP pour un déploiement sur site sn_sym_dlp.page_size_on_prem	Nombre maximal d'incidents à extraire dans un seul appel HTTP pour le déploiement sur site de Symantec. ○ Type : nombre entier ○ Valeur par défaut : 1 000
Appliquer une limite sur le nombre d'incidents à extraire dans un appel HTTP pour un déploiement exposé à Internet sn_sym_dlp.page_size_on_internet	Nombre maximum d'incidents à extraire dans un seul appel HTTP pour Symantec un déploiement exposé à Internet. ○ Type : nombre entier ○ Valeur par défaut : 100
Nombre d'incidents à charger dans un jeu d'importation sn_sym_dlp.incidents_per_attachment	Nombre d'enregistrements à stocker dans un fichier pièce jointe pour traitement. ○ Type : nombre entier ○ Valeur par défaut : 100
Envoyer les mises à jour des incidents DLP à Symantec sn_sym_dlp.incident_update	Cette propriété vous permet de restreindre toute synchronisation d'état entre ServiceNow les Symantec incidents DLP. ○ Type : booléen ○ Valeur par défaut : **vrai**
Envoyer des notes de création d'incidents DLP à Symantec sn_sym_dlp.incident_creation_notes	Cette propriété vous permet de renvoyer une note à Symantec dès qu'un incident est créé dans ServiceNow. ○ Type : booléen ○ Valeur par défaut : **vrai**
Niveau de génération de rapports des journaux générés par l'intégration sn_sym_dlp.logging.verbosity	Propriété qui définit le reporting des journaux générés par l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur **Enregistrer**.

Séparation en domaines dans l'intégration Symantec DLP

Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Prise en charge : Basique.

Comment fonctionne Séparation de domaine avec Symantec l'intégration DLP

Pour procéder à la séparation en domaines, procédez comme suit :

- Créez un utilisateur avec le rôle requis dans le domaine respectif.
- Effectuez les procédures d'intégration Symantec DLP dans le domaine approprié.

Intégration de Data Loss Prevention Incident Response avec Proofpoint

L'intégration Proofpoint DLP prend en charge l'ingestion des incidents de prévention des pertes de données créés sur le déploiement de la protection contre la Proofpoint perte de données. Après l'ingestion, vous pouvez utiliser les fonctionnalités de gestion des incidents pour corriger les incidents DLP.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Vue d'ensemble et fonctionnalités principales

L'intégration Proofpoint DLP aide les entreprises à suivre l'utilisation et le mouvement des données sensibles sur différentes plateformes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette intégration comprend les fonctionnalités clés suivantes :

- Création de plusieurs profils pour différents Proofpoint points de terminaison.
- Automatisation de la création des incidents DLP
- Mappage du champ État de l'incident DLP au champ État de l'incident Proofpoint DLP.
- Filtrage des Proofpoint incidents DLP.
- Ingestion des incidents dans votre ServiceNow instance dès leur création sur Proofpoint le locataire DLP.
- Proofpoint L'intégration DLP prend en charge les points de terminaison et les types d'incidents de type e-mail.
- Mises à jour automatiques pour le statut de l'incident DLP et les commentaires pour la création d'incidents DLP, ainsi que pour le changement d'état et la Proofpoint fermeture du ServiceNow côté.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Proofpoint Site web de la documentation produit	Documentation produit Proofpoint
ServiceNow® Site web de la documentation produit	Site web de la documentation produit ServiceNow

Mise en route Proofpoint de l'intégration pour la protection contre la perte de données

L'intégration Proofpoint DLP prend en charge l'ingestion des incidents de prévention de la perte de données créés sur le locataire de protection contre la Proofpoint perte de données. Après l'ingestion, les fonctionnalités de gestion des incidents qui corrigent les incidents DLP seront utilisées.

Liste de vérification

Passez en revue les informations suivantes avant de commencer à configurer votre Proofpoint intégration DLP pour la protection contre la perte de données.

Liste de vérification

Champ	Description
Vérifiez que vous avez affecté les rôles requis ServiceNow AI Platform et Data Loss Prevention Incident Response d'application.	Les rôles suivants sont utilisés dans l'intégration Proofpoint DLP sur :ServiceNow AI Platform • L'administrateur (admin) installe les applications à partir de et ServiceNow® Store affecte l'administrateur de la prévention des pertes de données (sn_dlir.admin). • L'utilisateur disposant du rôle sn_dlir.admin peut configurer l'intégration et configurer les profils d'incident. • Les utilisateurs disposant du rôle sn_dlir.analyst ont des rôles de lecture dans l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Champ	Description
Affectez les rôles d'utilisateur DLP requis Proofpoint .	Passez en revue les rôles et autorisations d'intégration Proofpoint DLP.
Vérifiez que vous utilisez Proofpoint DLP 1.0.1 ou une version ultérieure.	L'intégration Proofpoint DLP pour la protection contre la perte de données est testée avec Proofpoint la protection contre la perte de données, version 1.0.1 ou ultérieure.
Vérifiez que l'application principale de l'utilisateur final requise pour prendre en charge l'intégration Proofpoint DLP est installée et activée.	Vérifiez que les applications DLP et les applications courantes de prise en charge de la sécurité suivantes sont installées et activées à partir du ServiceNow magasin. Si ce n'est pas le cas, installez-le et activez-le sur l'application. • Security Support Common • Data Loss Prevention Incident Response

Installer et configurer l'intégration pour la protection contre la Proofpoint perte de données

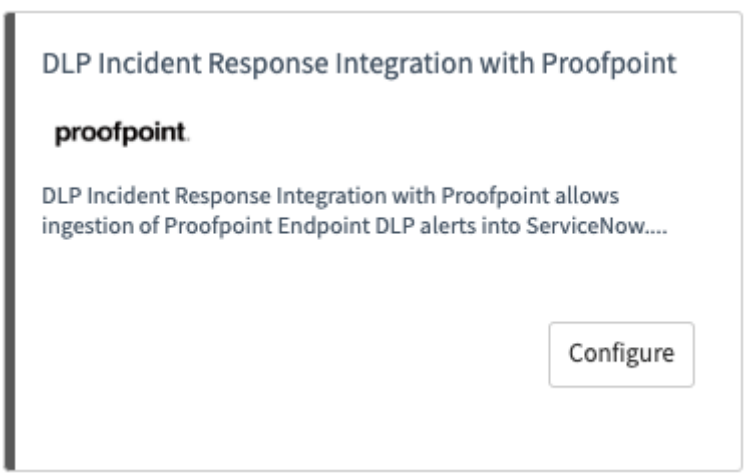
Installez et configurez l'intégration Proofpoint DLP sur ServiceNow® Store votre ServiceNow AI Platform instance. Commencez à enquêter sur les incidents DLP à l'aide des données d'incident Proofpoint DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Téléchargez l'intégration Proofpoint DLP à partir de et ServiceNow® Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette Intégration de Proofpoint à Réponse aux incidents DLP , puis cliquez sur **Configurer**.



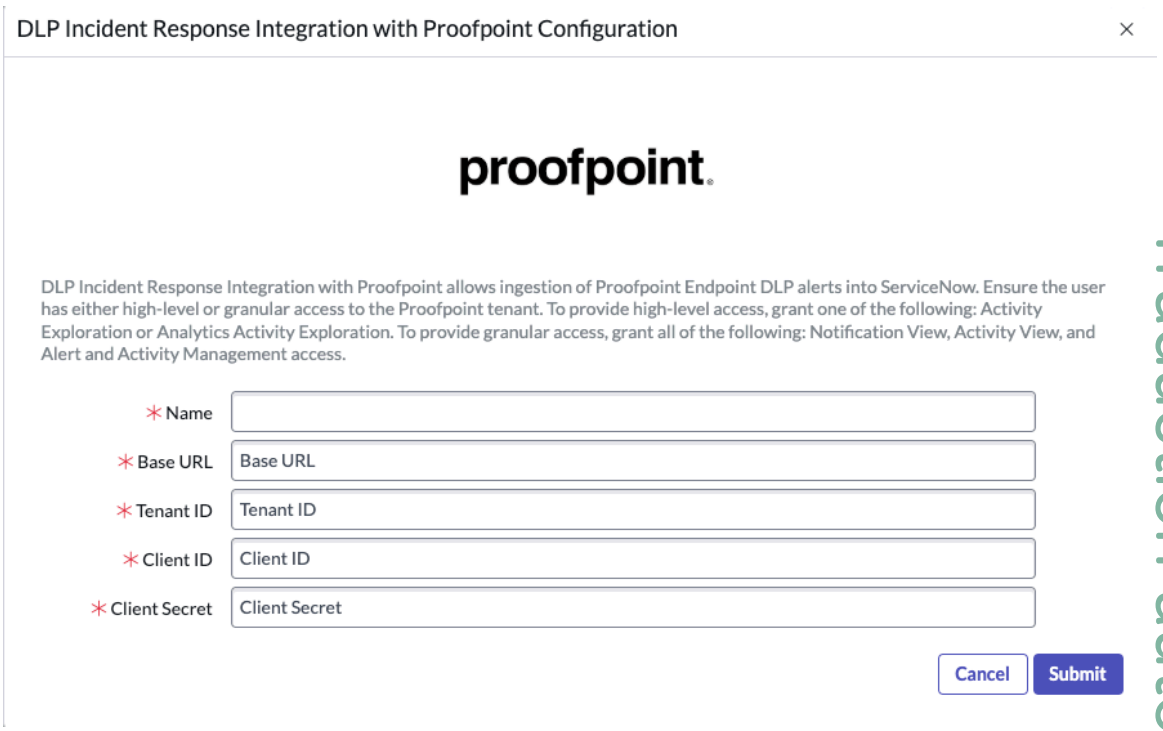
4. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Proofpoint Formulaire Configuration de l'intégration DLP

Champ	Description
Nom	Nom de la configuration de l'intégration Proofpoint DLP.
URL de base	URL qui Proofpoint sert de point de terminaison REST.
ID client	L'ID du Proofpoint client à utiliser.
Secret client	Le secret configuré pour votre compte utilisateur sur Proofpoint.



Remarque : Pour les clients existants, nous continuons à prendre en charge l'authentification de base afin de garantir que les tuiles enfants existantes qui ont une authentification de base fonctionnent comme prévu. Toutefois, si un client souhaite ajouter OAuth à une vignette enfant, il ne doit pas supprimer les informations d'identification d'authentification de base existantes (nom d'utilisateur et mot de passe). Bien qu'ils puissent remplacer ces valeurs par des entrées factices, laisser les champs vides empêchera la soumission de la tuile.

5. Cliquez sur **Envoyer**.

Résultats
Une fois que vous avez validé et soumis la configuration, l'intégration Proofpoint DLP est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

Configurer le webhook sur le locataire DLP pour les Proofpoint notifications d'alerte sur ServiceNow

Configurez un webhook à Proofpoint l'aide du point de terminaison REST API pour commencer à recevoir les alertes du Proofpoint locataire DLP. Votre ServiceNow instance crée des incidents DLP à partir de ces alertes. L'intégration Proofpoint DLP fournit un point de terminaison d'API REST permettant aux utilisateurs finaux de configurer le webhook.

Avant de commencer
Rôle requis : sn_pp_dlp.api_integration_user

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Connectez-vous à **Proofpoint**.
2. Accédez à la **Locataire Proofpoint** > **Application d'administration** > **Intégration** > **Politiques de notification**.
3. Créez une politique de notification avec un nom approprié.
4. Cliquez sur la **politique de notification** et gérez les webhooks configurés dans la politique de notification.
5. Créez une configuration de webhook en cliquant sur **Ajouter des webhooks**.
6. Sélectionnez le type de webhook **Générique**.
7. Dans l'entrée URL, saisissez une URL au format suivant : `https://<Instance_Name>.service-now.com/api/sn_pp_dlp/proofpointalertapi/getalerts`.
8. Gardez la méthode sur **POST.**
9. Ajoutez les en-têtes suivants au webhook :
   - ```
     Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow instance user>
     ```
   - ```
     Name: Content-Type
     Value: application/json
     ```
10. D ne modifiez pas les autres valeurs.
11. Cliquez sur **Enregistrer**.
12. Accédez à la **Locataire Proofpoint** > **Application d'administration** > **Politiques** > **Règles**.
13. Dans la section Actions, sélectionnez les règles pour lesquelles la notification webhook doit être générée.
14. Ajoutez les politiques de notification nouvellement créées pour lesquelles un webhook est configuré.
15. Cliquez sur **Enregistrer**.

Créer une application et Proofpoint obtenir les informations d'identification du client

Créez une application et Proofpoint configurez les paramètres requis pour obtenir les informations d'identification du client. Ces informations d'identification permettent un accès sécurisé à l'API de Proofpoint pour une intégration et une automatisation transparentes.

Avant de commencer

Rôle requis : admin

Procédure

1. Connectez-vous à la Proofpoint console.
   Accédez à la console à l'aide Proofpoint de vos informations d'identification.
2. Créez une application.
   a. Dans la section **Développeur** , sélectionnez Autorisation.
   b. Sélectionnez **Créer**.
   c. Saisissez un nom d'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Dans Périmètres autorisés, ajoutez des périmètres à votre application selon vos besoins.

e. Dans Autorisations autorisées, sélectionnez **Informations d'identification du client**.

f. Sélectionnez **Enregistrer**.
L'ID client et le secret client sont générés.

3. Configurez les détails de l'application.

a. Sélectionnez l'application nouvellement créée.

b. Dans Politiques d'accès, sélectionnez **Modifier**.

Sélectionnez des politiques d'accès de niveau élevé ou granulaire.

c. Sélectionnez **Terminé**.

Résultats

Utilisez l'ID client et le secret client générés pour configurer l'intégration dans l'application DLP Proofpoint (PPT) et commencer à l'utiliser.

Créer un profil pour Proofpoint l'intégration DLP

Créez un profil d'incident dans votre ServiceNow AI Platform instance. Déterminez les Proofpoint incidents DLP qui se prêtent à la création d'incidents DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Configurer les pour renseigner les ServiceNow AI Platform alertes DLP de Proofpoint. Stockez les alertes en tant qu'incidents DLP dans votre ServiceNow instance.

Procédure

1. Accédez à la **Intégration DLP Proofpoint** > **Profil d'incident**.

2. Cliquez sur **Nouveau**.

3. Renseignez les champs de la section **Nom** du formulaire.

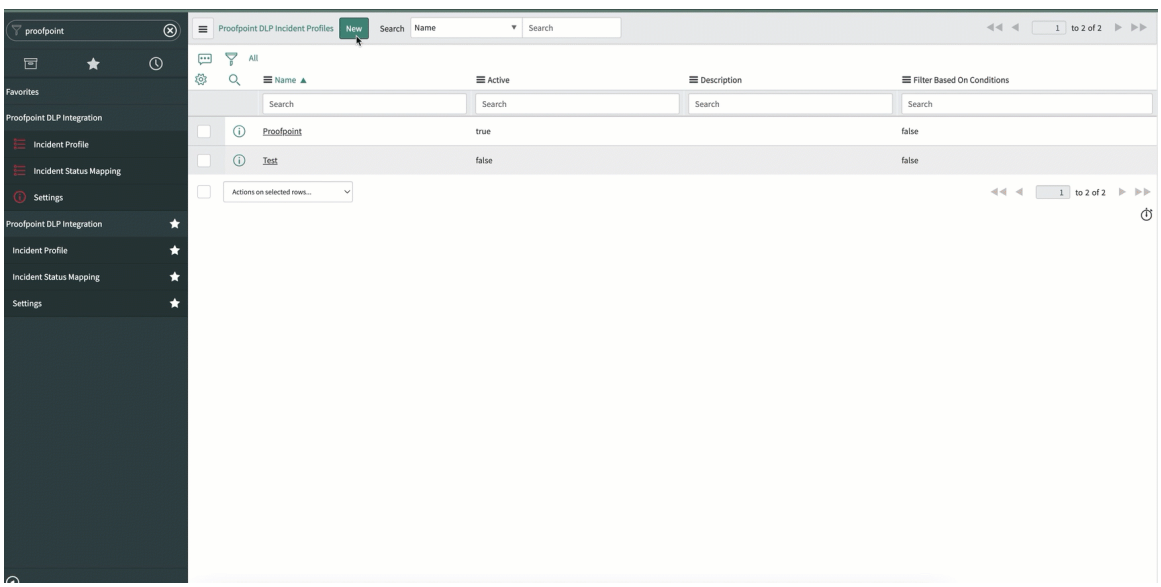
Formulaire Créer un profil pour Proofpoint l'intégration DLP

Champ	Description
Nom	Nom du profil. Ce nom vous permet d'identifier le profil. **Remarque :** Le nom doit être unique pour chaque profil.
Source	Instance Proofpoint DLP que vous avez configurée pour ingérer des incidents. Si vous avez configuré plusieurs instances, sélectionnez l'instance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	appropriée pour les types d'incidents que vous prévoyez d'ingérer pour le profil.
Actif	Option pour rendre le profil actif. Lorsque le profil est actif, votre ServiceNow AI Platform instance est prête à recevoir les incidents de Proofpoint.
Description	Description permettant de distinguer ce profil des autres profils.



4. Cliquez sur **Continuer** et passez à la section Filtrage.

Définir les filtres à appliquer pour la création d'incident

Définissez et définissez des conditions de filtre pour filtrer les incidents DLP entrants Proofpoint . Contrôlez les incidents DLP à créer ServiceNow®.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Ce type de filtrage vous aide à isoler les incidents DLP et à limiter le nombre d'incidents DLP que vous créez. Si des critères de filtrage supplémentaires sont définis, seuls les incidents qui correspondent aux conditions sont créés.

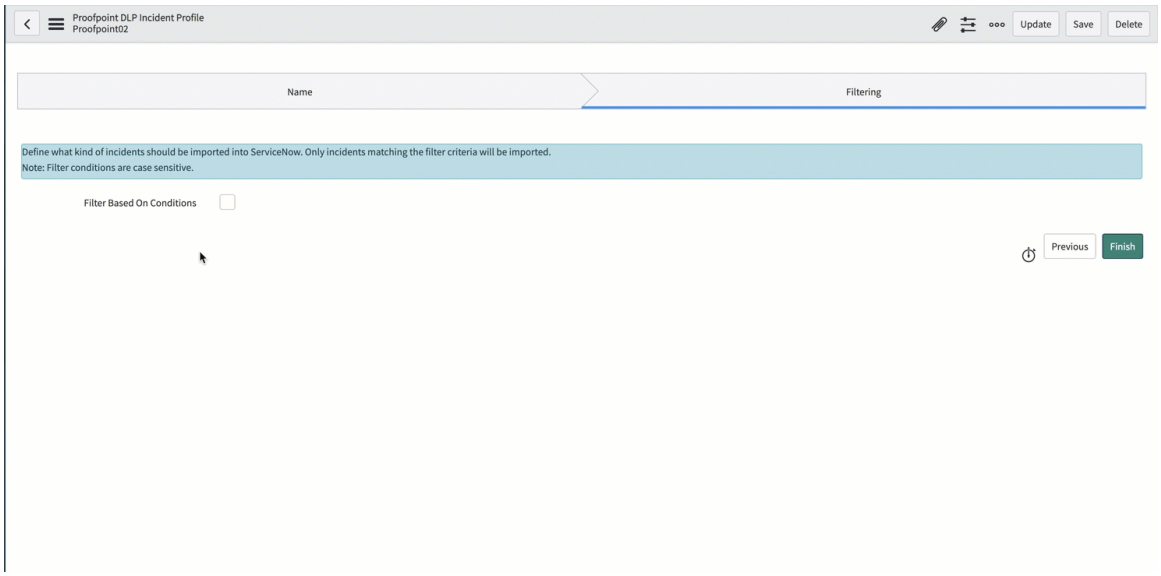
Procédure

1. Sélectionnez l'option **Filtrer en fonction des conditions** et définissez les critères qu'un incident DLP entrant Proofpoint doit satisfaire pour qu'un incident de sécurité soit créé.
2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres dans le champ **Conditions de filtre** .

   Les options du premier champ des **conditions de filtre** correspondent aux champs disponibles dans l'incident DLP. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Ajoutez d'autres conditions en cliquant sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Cliquez sur **Terminer**.

Prévisualiser les fichiers de preuves

Prévisualisez Data Loss Prevention Incident Response les fichiers de preuves dans l'espace de travail de l'analyste DLP IR.

Avant de commencer

Important : Lors de l'utilisation de l'action Fichiers de preuves dans l'espace de travail de l'analyste DLP, les fichiers de preuves sont temporairement stockés dans la base de données ServiceNow dans un format non chiffré. Si vous ne souhaitez pas stocker les fichiers de preuves, désactivez la fonctionnalité d'aperçu des fichiers de preuves. Pour plus d'informations, consultez Configurer les paramètres avancés.

Rôle requis : sn_dlir.analyst

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez un enregistrement d'incident DLP.
3. Dans la barre latérale contextuelle, sélectionnez l'icône Fichiers de preuves ( ).
4. Dans l'onglet **Fichiers de preuves** , sélectionnez la carte **Fichier de preuves** pour afficher un aperçu des fichiers de preuves dans la visionneuse de documents.

   La fonctionnalité d'aperçu est différente pour chaque type de fichier, comme indiqué dans le tableau suivant.

Format de fichier	Extension de fichier
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg et .webp.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Format de fichier	Extension de fichier
	Les fichiers image s'ouvrent en mode visionneuse de documents.
Microsoft Fichiers Office	.doc, .docx, .ppt, .pptx, .xls et .xlsx Les fichiers Office s'ouvrent en mode visionneuse de documents.
Fichiers texte	.txt Les fichiers texte s'ouvrent en mode éditeur de texte.
Fichiers courrier	.Eml **Remarque :** La taille du fichier doit être inférieure à 5 Mo. Vous devez d'abord télécharger le fichier pour prévisualiser son contenu.
Fichiers PDF	.PDF ○ Saisissez un mot clé pour rechercher le document. ○ Fonctions de zoom avant et arrière pour ajuster la vue et améliorer la lisibilité. ○ Faites pivoter la page dans le sens des aiguilles d'une montre ou dans le sens inverse des aiguilles d'une montre pour afficher le contenu plus clairement.

Remarque :

Les fichiers binaires ne seront pas rendus et devront être téléchargés pour prévisualiser leur contenu. La fonctionnalité d'aperçu du fichier de preuve fonctionne également pour les incidents archivés.

Mapper Proofpoint l'état des incidents DLP avec ServiceNow l'état de l'incident

Synchronisez l'état des incidents DLP ingérés sur votre ServiceNow instance et les incidents DLP du Proofpoint. Mappez l'état de l'incident ServiceNow avec l'état de l'incident Proofpoint .

Avant de commencer
Rôle requis : sn_dlir.admin

Procédure

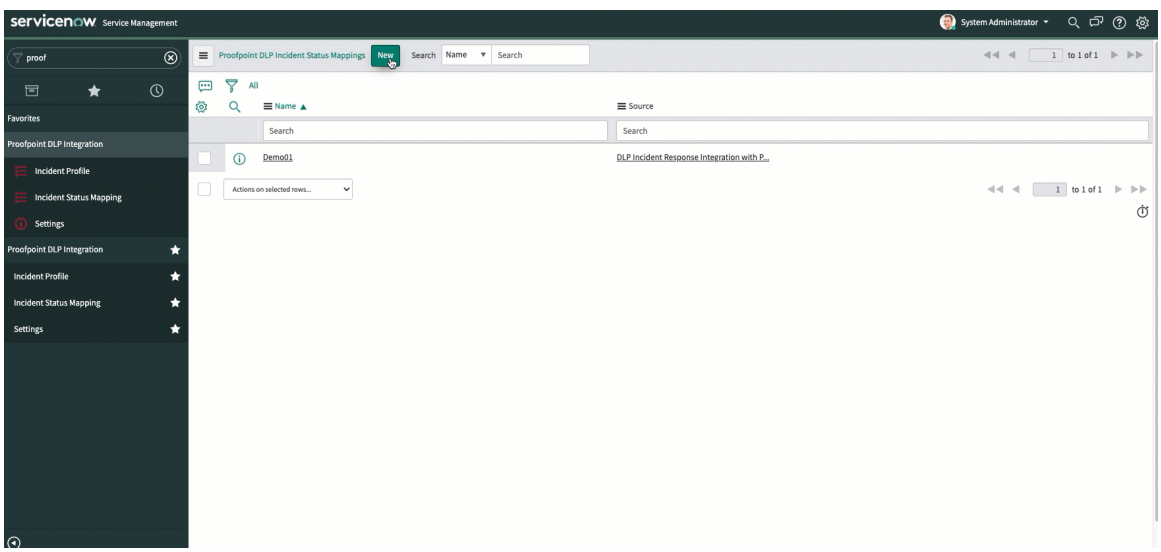
1. Accédez à la **Intégration DLP Proofpoint** > **Incident** > **Mappage de l'état des incidents**.
2. Fournissez un **nom** pour identifier le mappage.
3. Sélectionnez la tuile **Source** (configuration de l'intégration) à laquelle le mappage d'état doit être appliqué.
4. Mappez **l'état de l'incident DLP ServiceNow** avec **l'état de l'incident Proofpoint**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mapper l'état des incidents DLP Proofpoint avec le formulaire d'état d'incident ServiceNow

Champ	Description
Nom	Espace réservé pour l'enregistrement de mappage.
Source	Source de point de terminaison configurée Proofpoint à partir de laquelle vous souhaitez extraire l'état de l'incident.
État des incidents ServiceNow	Liste des états des incidents DLP.
État des incidents Proofpoint	Valeurs mappées par défaut pour les états par défaut disponibles dans les incidents DLP. Pour les états personnalisés, l'état par défaut Proofpoint est **Nouveau**. Vous pouvez modifier et ajouter l'état requis Proofpoint dans le champ d'entrée.



5. Cliquez sur **Envoyer**.

Résultats

Un enregistrement pour le mappage est créé avec succès. Les états des incidents sont synchronisés avec Proofpoint les ServiceNow incidents DLP.

Lorsque vous modifiez l'état d'un incident DLP sur votre ServiceNow instance, l'état de l'incident DLP associé Proofpoint est modifié sur la plateforme source Proofpoint conformément au mappage défini dans l'enregistrement.

Configurer les Proofpoint paramètres d'intégration DLP

Modifiez les propriétés système par défaut de l'intégration Proofpoint DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Accédez à la **Intégration DLP Proofpoint** > **Paramètres**.
2. Modifiez les paramètres suivants selon vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Délai d'expiration maximal pour les appels HTTP sn_pp_dlp.maximum_http_time_out	Délai d'expiration maximal pour les appels HTTP (en secondes). ○ Type : nombre entier ○ Valeur par défaut : 30
Envoyer les mises à jour des incidents DLP à Proofpoint sn_pp_dlp.incident_update	Cette propriété permet de restreindre toute synchronisation de votre ServiceNow instance aux Proofpoint incidents DLP. ○ Type : booléen ○ Valeur par défaut : true
Niveau de génération de rapports des journaux générés par l'intégration sn_pp_dlp.logging.verbosity	Niveau des journaux de génération de rapports générés par l'intégration.

3. Cliquez sur **Enregistrer**.

Résultats

Vos paramètres d'intégration modifiés sont appliqués dans l'intervalle d'interrogation suivant, tel que défini dans le profil.

Séparation en domaines dans l'intégration Proofpoint DLP

Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Prise en charge : Basique.

Comment fonctionne Séparation de domaine avec Proofpoint l'intégration DLP

Pour procéder à la séparation en domaines, procédez comme suit :

- Créez un utilisateur avec le rôle requis dans le domaine respectif.
- Effectuez les procédures d'intégration Proofpoint DLP dans le domaine approprié.

Intégration de Data Loss Prevention Incident Response avec Netskope

L'intégration Netskope DLP prend en charge l'ingestion des incidents de prévention des pertes de données créés sur le déploiement de la protection contre la Netskope perte de données. Netskope DLP aide les entreprises à suivre l'utilisation et le mouvement des données sensibles sur diverses plateformes.

Après l'ingestion, vous pouvez utiliser les fonctionnalités de gestion des incidents pour corriger les incidents DLP.

Fonctionnalités principales

Cette intégration comprend les fonctionnalités clés suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Création de plusieurs profils pour différents Netskope locataires.
- Automatisation de la création d'incidents DLP ServiceNow à partir d'incidents Netskope DLP
- Filtrage des Netskope incidents DLP.
- Ingestion planifiée d'incidents DLP qui créent des Netskope incidents DLP dans ServiceNow.
- Mettez automatiquement à jour l'état de l'objet Netskope lorsque l'état DLP change dans votre instance ServiceNow.
- Affichez les détails d'expertise (contenu en infraction) de l'incident DLP sur l'espace de travail de l'analyste DLP IR et l'espace de travail de l'utilisateur final DLP.

  Remarque : Le contenu en infraction ne persiste pas dans ServiceNow. Le contenu est extrait lorsque l'incident est ouvert dans l'espace de travail.

- Téléchargement du fichier de preuves directement à partir de la Netskope demande.

  Remarque : Le fichier de preuves ne persiste pas dans ServiceNow. Le fichier de preuves est extrait lorsque l'analyste clique sur Télécharger le **fichier** dans l'espace de travail.

- Notification par e-mail aux utilisateurs administrateurs DLP à l'expiration Netskope du jeton.
- Une notification par e-mail est envoyée aux utilisateurs administrateurs DLP en cas de dépassement de la limite définie pour les nouvelles tentatives d'échecs d'appels API d'incidents.
- Netskope prend également en charge le processus d'exécution de l'intégration. Pour plus d'informations, consultez Surveiller le processus d'exécution de l'intégration DLP.

Mise en route de l'intégration Netskope DLP pour la protection contre la perte de données

Passez en revue les informations suivantes avant de commencer à configurer votre Netskope intégration DLP pour la protection contre la perte de données.

Tâche de configuration	Description
Vérifiez que vous avez affecté la Now Platform requise, l'application de prévention des pertes de données.	Les rôles suivants sont utilisés dans l'intégration Netskope DLP sur :ServiceNow AI Platform • L'administrateur (admin) installe les applications à partir de et ServiceNow Store affecte l'administrateur de la prévention des pertes de données (sn_dlir.admin). • L'utilisateur disposant du rôle sn_dlir.admin peut configurer l'intégration et configurer les profils d'incident. • Les utilisateurs ayant le rôle sn_dlir.analyst auront des rôles de lecture dans l'intégration.
Affectez les privilèges requis pour Netskope le jeton d'API v2.	Les privilèges de point de terminaison suivants sont utilisés dans la création de jetons de l'API Netskope v2.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de configuration	Description
	• Lecture : /api/v2/incidents/dlpincidents • Lecture : /api/v2/events/dataexport/events/incident • Lecture + écriture : /api/v2/incidents/update
Vérifiez que l’application principale de l’utilisateur final requise pour prendre en charge l’intégration Netskope DLP est installée et activée.	Vérifiez que les applications DLP et les applications courantes de prise en charge de la sécurité suivantes sont installées et activées à partir du ServiceNow magasin. Si ce n’est pas le cas, installez-le et activez-le sur l’application. • Security Support Common • Data Loss Prevention Incident Response

Installer et configurer l’intégration DLP pour la protection contre la Netskope perte de données

Installez et configurez l’intégration DLP à partir de ServiceNow StoreServiceNow AI Platform l’instanceNetskope. Vous pouvez commencer à enquêter sur les incidents DLP à l’aide des données d’incident Netskope DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

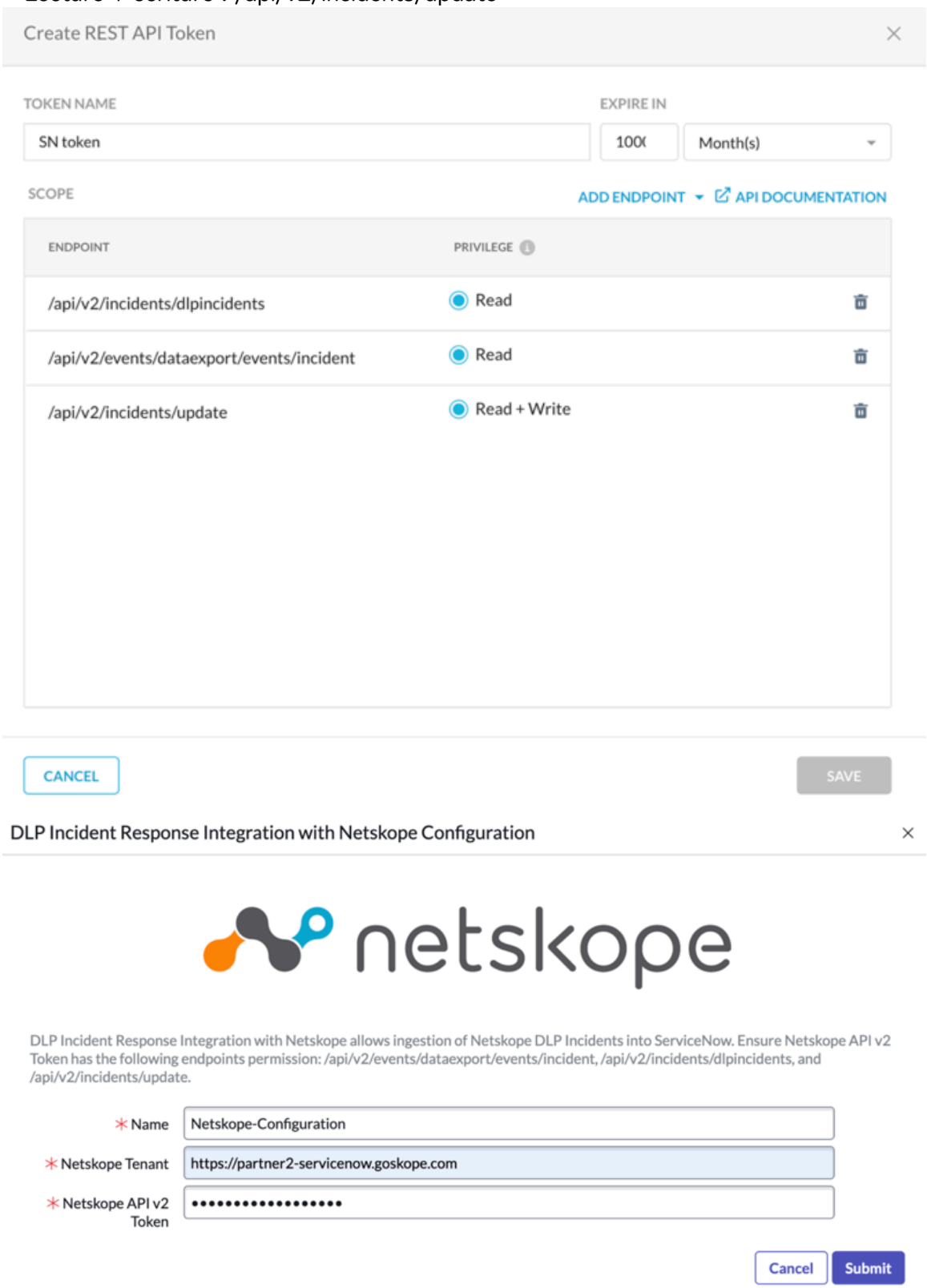
1. Téléchargez l’intégration Netskope DLP à partir de et ServiceNow Store installez-la.
2. Accédez à **Opérations de sécurité** > **Intégrations** > **Configurations d'intégration**
3. Recherchez la vignette Intégration de DLP Incident Response avec Netskope , puis cliquez sur **Configurer**.
4. Remplissez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Assurez-vous que votre Netskope jeton d'API v2 dispose des privilèges de point de terminaison ci-dessous :

- Lecture : /api/v2/incidents/dlpincidents
- Lecture : /api/v2/events/dataexport/events/incident
- Lecture + écriture : /api/v2/incidents/update



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom de la configuration de l'intégration Netskope DLP.
Locataire Netskope	L'URL Netskope de base du Netskope locataire.
Jeton d'API Netskope v2	Jeton configuré pour l'API REST v2 sur votre compte d'utilisateur à l'adresse .Netskope

5. Cliquez sur **Envoyer**.

Résultats

Remarque : Veuillez connecter netskope sub prod à la sous-production ServiceNow. Gardez tous les noms d'utilisateur et mots de passe synchronisés entre les instances pour éviter que les comptes ne soient déconnectés.

Une fois que vous avez validé et soumis la configuration, l'intégration Netskope DLP est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

Créer un profil pour Netskope l'intégration DLP

Créez un profil d'incident dans votre ServiceNow AI Platform instance.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Configurez ServiceNow AI Platform pour récupérer les incidents DLP à Netskope partir du point de terminaison. Stockez les incidents dans votre ServiceNow instance en tant qu'incidents DLP.

Procédure

1. Accédez à la **Intégration DLP Netskope** > **Profil d'incident**.
2. Cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire.

Créer un profil

Champ	Description
Nom	Nom du profil. Le nom doit être unique pour chaque profil. Ce nom vous permet d'identifier le profil.
Source	Netskope Instance DLP que vous avez configurée pour ingérer des incidents. Si vous avez configuré plusieurs instances, sélectionnez l'instance appropriée pour les types d'incidents que vous prévoyez d'ingérer pour le profil. **Remarque :** Un seul profil actif est autorisé par source.
Actif	Indique que le profil est actif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Ce champ n'est disponible qu'après avoir cliqué sur **Terminer** dans la dernière section Planification. Lorsque le profil est actif, votre ServiceNow AI Platform instance interroge activement les Netskope incidents DLP. Les incidents DLP correspondants sont créés en tant qu'incidents DLP ServiceNow lorsque les conditions de filtrage sont mises en correspondance en fonction des paramètres de planification que vous avez fournis.
Ordre	Ordre d'exécution du profil. Le profil avec l'ordre le plus bas considéré comme la priorité la plus élevée. Par défaut, la valeur est 100.
Description	Description permettant de distinguer ce profil des autres profils.

4. Cliquez sur **Continuer** et passez à la section Filtrage.

Définir les filtres à appliquer pour la création d'incident

Définissez et définissez des conditions de filtre pour filtrer les incidents DLP entrants Netskope . Contrôlez lesquels de ces incidents doivent être créés en tant qu'incidents DLP sur votre ServiceNow instance.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Ce type de filtrage vous aide à isoler les incidents DLP et à limiter le nombre d'incidents DLP que vous créez. Si des critères de filtrage supplémentaires sont définis, seuls les incidents qui correspondent aux conditions sont créés.

Procédure

1. Sélectionnez l'option **Filtrer en fonction des conditions** et définissez les critères qu'un incident DLP Netskope entrant doit satisfaire pour qu'un incident DLP soit créé.
2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres dans le champ **Conditions de filtre** .

   Les options du premier champ des **conditions de filtre** correspondent aux champs disponibles dans la table **d'importation d'incidents DLP Netskope** . Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.
3. Ajoutez d'autres conditions en cliquant sur **ET** ou **OU**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
- Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.

4. Cliquez sur **Continuer** et passez à la section Planification.

Planifier la récupération des Netskope incidents DLP

Définissez un calendrier pour récupérer Netskope les incidents DLP qui correspondent aux critères du profil.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier la fréquence à laquelle vous interrogerez pour rechercher de nouveaux Netskope incidents nets qui correspondent à la configuration du profil d'incident. Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Le profil peut être configuré pour effectuer une récupération ponctuelle à l'aide de la case à cocher **Récupération ponctuelle** . La date historique peut être jusqu'à un mois dans le passé.

Procédure

1. Configurez le calendrier pour définir comment et quand extraire des incidents de Netskope.
2. Remplissez les champs du formulaire.

Planifier les Netskope incidents DLP

Champ	Description
Intégration de l'incident en cours	Ingestion d'incidents en cours à partir de Netskope laquelle votre ServiceNow AI Platform instance extrait pour les nouveaux incidents. Si des incidents déclenchés correspondent aux critères de filtrage d'incidents, des incidents DLP sont créés.
Incrémentation du sondage (minutes)	Fréquence d'interrogation définie en minutes. Cette valeur par défaut est définie sur **5**.
Définir le délai d'intégration de l'incident initial	Option permettant de définir l'ingestion d'incident initial en fonction de la date et de l'heure configurées. Vous pouvez utiliser cette option pour définir une date et une heure spécifiques pour l'ingestion initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation.
Délai d'intégration de l'incident initial d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.
Délai d'intégration de l'incident initial	La première fois que des données sont ingérées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : La valeur n'est visible que si l'option **Définir le délai d'intégration de l'incident initial** est sélectionnée.
Délai d'intégration de l'incident suivant (estimé)	Délai d'intégration estimé de l'incident suivant
Récupération ponctuelle	Option permettant d'activer l'extraction unique des données historiques. **Remarque :** Si cette option est sélectionnée, les données historiques sont extraites de DLP en fonction de Netskope la date ajoutée dans **Date de début**.
Date de début	Date à partir de laquelle les données sont extraites à partir de Netskope. **Remarque :** Les données des 30 derniers jours peuvent être extraites au maximum à partir de Netskope.

3. Cliquez sur **Terminer**.
4. Dans la fenêtre contextuelle, enregistrez la configuration de profil créée en cliquant sur **Terminer**.
5. Activez le profil.
   a. Ouvrez le profil créé.
   b. Définir **Actif** sur **vrai**.
   c. Cliquez sur **Mettre à jour**.

Résultats
Une fois l'activation du profil créée, les incidents sont extraits périodiquement conformément à la configuration définie dans le profil. Les incidents sont ajoutés à la table des incidents DLP.

Mapper l'état de l'incident DLP avec Netskope

La section de mappage de l'état des incidents permet aux utilisateurs de fournir les mappages entre l'état de l'incident DLP dans ServiceNow et Netskope l'état de l'objet.

Avant de commencer
Le mappage est utilisé lors de l'ingestion d'un incident DLP depuis Netskope vers ServiceNow, ainsi que lors de la synchronisation de tout changement d'état d'un incident DLP dans ServiceNow vers Netskope.

Synchronisez l'état des incidents DLP ingérés sur ServiceNow avec l'incident DLP de Netskope. Mappez le champ État de l'incident ServiceNow avec le champ État de l'objet Netskope .

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche
Vous devez créer un mappage de l'état des incidents de un à un et de Netskope l'état ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Intégration DLP Netskope** > **Mappage de l'état des incidents**.
2. Fournissez un nom pour identifier le mappage.
3. Sélectionnez l'intégration source.
4. Mappez l'état de l'incident DLP avec Netskope l'état de l'objet (l'état en Netskope double peut également être mappé).
   La synchronisation de l'état de ServiceNow vers Netskope sera désactivée si vous ne créez pas d'enregistrement de mappage.

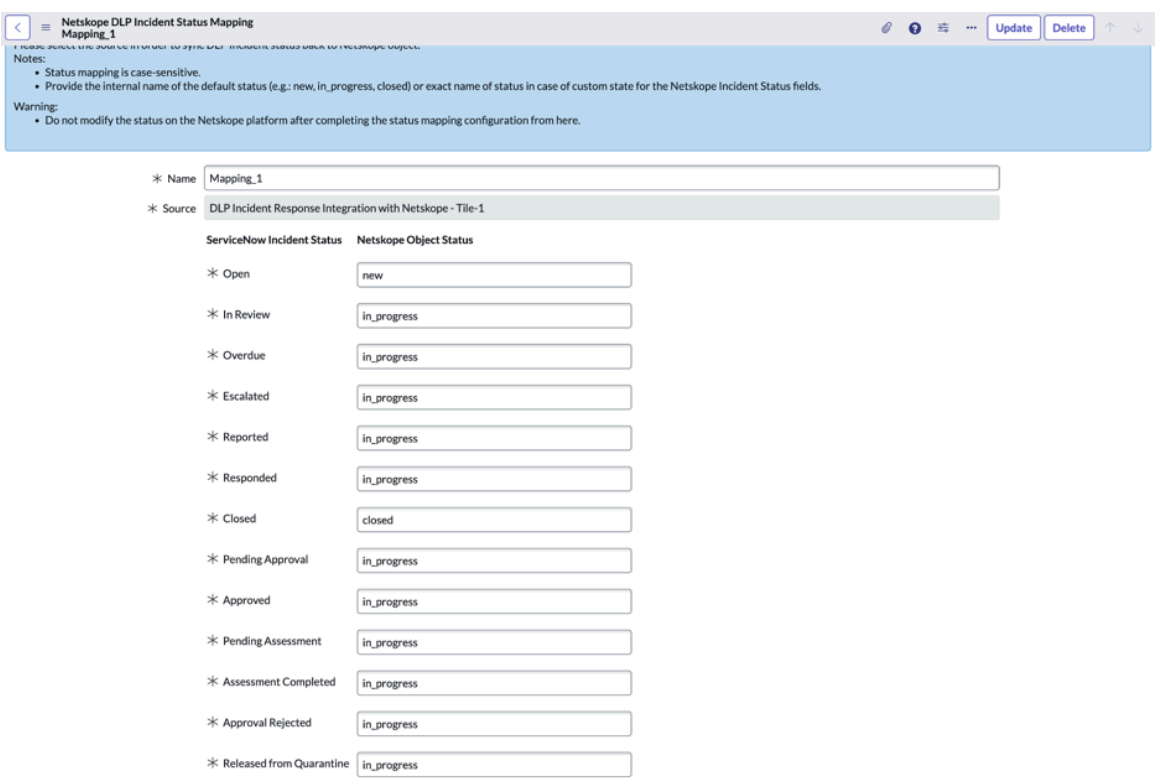
Important : Vous devez mapper tous les états d'objet Netskope à tous les états ServiceNow. Sélectionnez la source afin de resynchroniser l'état de l'incident DLP avec l'objet Netskope .

Les informations et messages d'alerte suivants s'affichent lorsque vous mappez l'état de l'incident, examinez les messages et poursuivez :

Remarque :

- Le mappage de statut est sensible à la casse.
- Fournissez le nom interne de l'état par défaut (par exemple : nouveau, in_progress, fermé) ou le nom exact de l'état en cas d'état personnalisé pour les champs État de l'objet Netskope .

Avertissement : Ne modifiez pas l'état sur la Netskope plateforme après avoir terminé la configuration du mappage d'état d'ici.



Netskope Mappage de l'état des incidents DLP

Champ	Description
Nom	Nom de l'enregistrement du mappage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Source	Source de point de terminaison configurée Netskope à partir de laquelle vous souhaitez synchroniser l'état de l'incident.
État des incidents DLP	Indique la liste des états des incidents DLP.
Netskope Statut de l'objet	Indique la liste des états de l'objet Netskope .

5. Cliquez sur **Envoyer**.

Résultats

Une fois l'enregistrement créé avec succès pour le mappage d'état, chaque fois qu'il y a une mise à jour sur l'état d'un incident DLP ServiceNow, il est automatiquement répercuté sur Netskope le côté selon le mappage.

Remarque : Si vous modifiez l'état d'un incident DLP directement sur Netskope le locataire, la synchronisation de l'état de SN vers Netskope ne fonctionne pas compte tenu des limitations de l'API. Assurez-vous de mapper soigneusement tous les états des incidents DLP avec Netskope l'état des objets.

Configurer les Netskope paramètres d'intégration DLP

Modifiez les propriétés système par défaut de l'intégration Netskope DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Accédez à la **Intégration DLP Netskope** > **Paramètres**.
2. Modifiez les paramètres suivants selon vos besoins.

Configurer les Netskope paramètres d'intégration DLP

Champ	Description
Le téléchargement du fichier de violation de l'incident signalé doit-il être autorisé sn_ns_dlp.enable_file_download.	Option permettant de choisir si vous souhaitez activer le téléchargement du fichier. Par défaut, cette option est activée.
Délai d'expiration maximal pour les appels HTTP, en secondes sn_ns_dlp.maximum_http_time_out.	Délai d'expiration maximal pour les appels HTTP, en secondes. Ce champ est automatiquement défini sur 30.
Nombre maximal de nouvelles tentatives à effectuer pour les défaillances d'API. sn_ns_dlp.maximum_retry.	Nombre maximal de nouvelles tentatives à effectuer pour les défaillances d'API. La valeur par défaut est 3.
Niveau de génération de rapports des journaux générés par l'intégration sn_ns_dlp.logging.verbosity.	Définissez le niveau des journaux de génération de rapports générés par l'intégration. Ce champ est automatiquement défini sur **informations**.

3. Cliquez sur **Enregistrer**.

Résultats

Vos paramètres d'intégration modifiés sont appliqués dans l'intervalle d'interrogation suivant, tel que défini dans le profil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Télécharger les fichiers de preuves

Téléchargez des fichiers qui enfreignent la politique DLP sur Netskope. Téléchargez ce fichier sur votre ordinateur local à partir de l'espace de travail de l'analyste DLP IR et de l'espace de travail de l'utilisateur final DLP IR pour les approbateurs.

Avant de commencer

Rôle requis :

- sn_dlir.analyste
- sn_dlir.secure_file_download (tout approbateur disposant de ce rôle)

Pourquoi et quand exécuter cette tâche

Vous devez activer le téléchargement des fichiers avant Netskope de continuer.

Procédure

1. Accédez à la **Tous** > **Intégration DLP Netskope** > **Paramètres**.
2. Activez la propriété **Le téléchargement du fichier en infraction de l'incident signalé doit-il être autorisé** ?
   Vous pourrez voir le bouton Télécharger le **fichier** dans l'espace de travail de l'analyste DLP IR et l'espace de travail de l'utilisateur final DLP IR.
3. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
4. Ouvrez un enregistrement d'incident DLP qui est ingéré à partir de la Netskope source.
5. Cliquez sur **Télécharger le fichier**.
   Le fichier qui enfreint la politique DLP sur le Netskope sera téléchargé sur l'ordinateur local de l'utilisateur.

> **Remarque :** L'administrateur DLP peut contrôler l'accès à l'action **Télécharger le fichier** pour toutes les intégrations en désactivant l'option **Le téléchargement du fichier de violation de l'incident signalé doit-il être autorisé** à partir de la page **Paramètres avancés** de l'administration DLP. Pour plus d'informations, consultez Configurer les paramètres avancés.

Prévisualiser les fichiers de preuves

Prévisualisez les fichiers de preuves d'incidents DLP dans l'espace de travail de l'analyste DLP IR.

Avant de commencer

- Accédez à la **Tous** > **Administration DLP** > **Paramètres avancés**.
- Assurez-vous que la propriété **sn_ns_dlp.enable_evidence_file_preview** est déjà activée.

> **Important :** Lors de l'utilisation de l'action Fichiers de preuves dans l'espace de travail de l'analyste DLP, les fichiers de preuves sont temporairement stockés dans la base de données ServiceNow dans un format non chiffré pendant la durée que vous avez sélectionnée à l'aide de la propriété **sn_dlir.preview_temp_files_cleanup_interval** de la page **Paramètres avancés** . Vous pouvez désactiver la fonctionnalité d'aperçu des **fichiers de preuves** si vous ne souhaitez pas stocker de données dans la base de données ServiceNow. Pour plus d'informations, consultez Configurer les paramètres avancés.

Rôle requis : sn_dlir.analyst

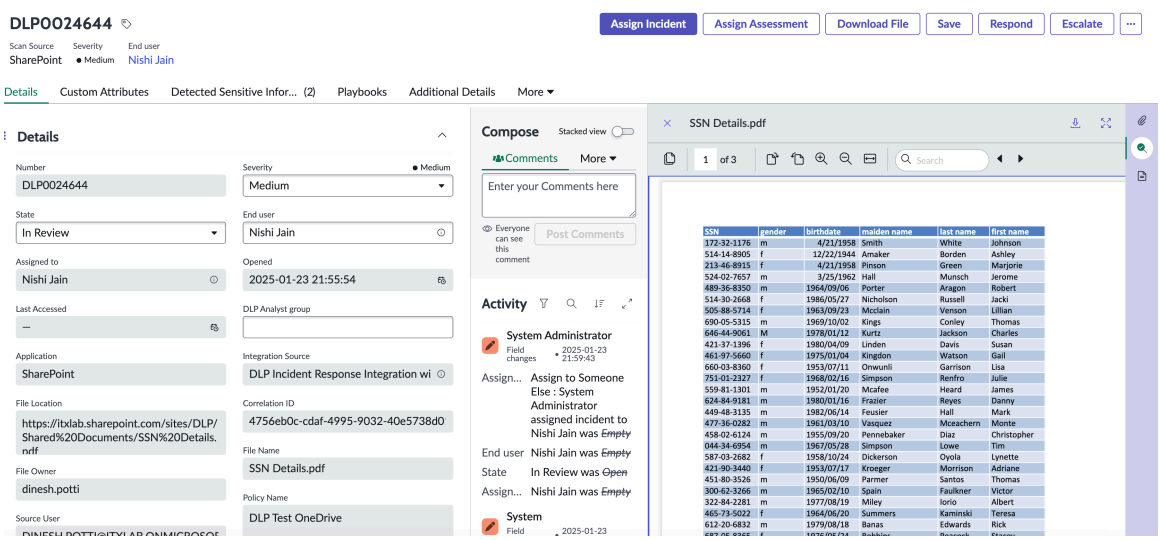
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez un enregistrement d'incident DLP.
3. Sélectionnez l'icône **Fichiers de preuves** , disponible dans le menu contextuel.
   Un onglet s'ouvre et récupère tous les fichiers de preuves. Une fois le téléchargement terminé, vous pouvez afficher tous les fichiers de preuves dans l'onglet **Fichiers de preuves** .
4. Sélectionnez la carte **Fichier de preuves** que vous souhaitez prévisualiser.
   La fonction d'aperçu est différente pour chaque type de fichier.
5. Prévisualisez le PDF et les documents Office dans la visionneuse de documents en sélectionnant l'icône **Développer** en haut à droite du fichier de preuves pour ouvrir le PDF en plein écran.
   Les extensions Office pour lesquelles la visionneuse de documents ouvre les fichiers de preuves incluent : doc, docx, ppt, pptx, xls, xlsx.
   a. Localisez la barre de recherche et entrez le mot-clé que vous recherchez.
   b. Utilisez les fonctions de zoom avant et arrière pour ajuster la vue et améliorer la lisibilité.
   c. Faites pivoter la page dans le sens des aiguilles d'une montre ou dans le sens inverse des aiguilles d'une montre pour afficher le contenu plus clairement.

   Ces options de contrôle améliorent votre capacité à comprendre le dossier de preuves de manière exhaustive. Seul le PDF comporte des options de contrôle dans l'en-tête.

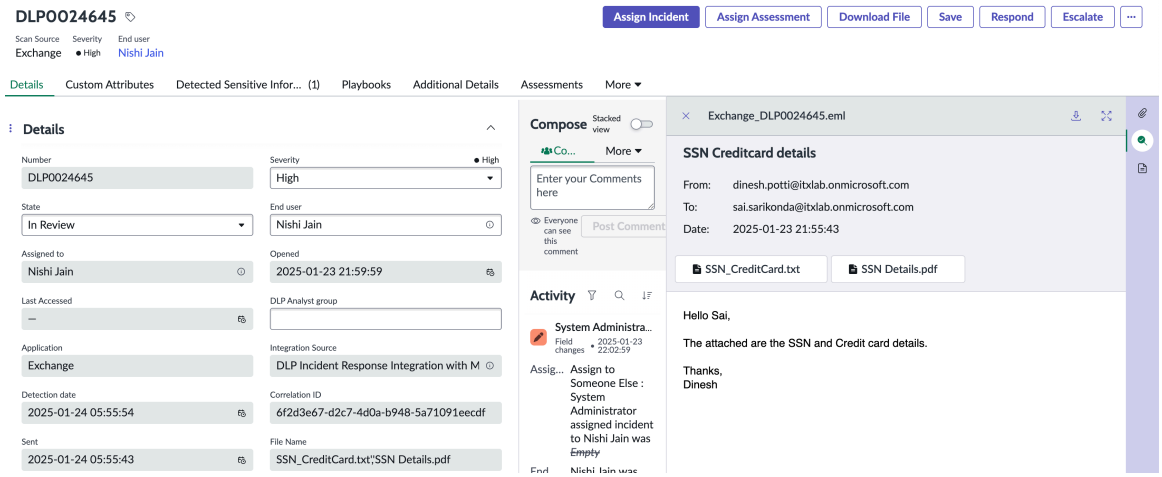


6. Prévisualiser les fichiers EML.
   Sélectionnez les pièces jointes dans l'e-mail et prévisualisez-les.

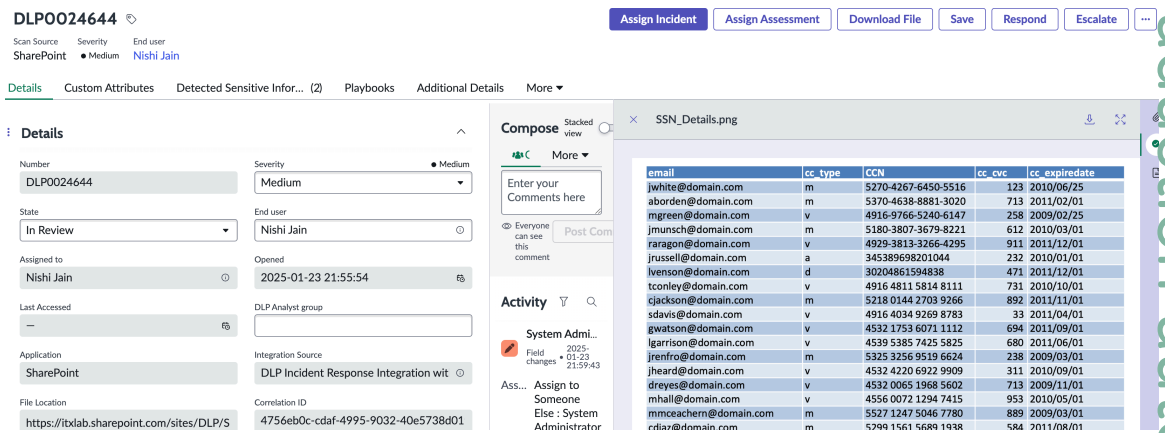
> **Remarque :** Si le fichier de preuve sélectionné dépasse la limite de 5 Mo, il ne peut pas être prévisualisé dans Analyst Workspace. Vous devez télécharger le fichier pour prévisualiser son contenu. Cette limite ne concerne que les fichiers .eml.

Traduction automatique

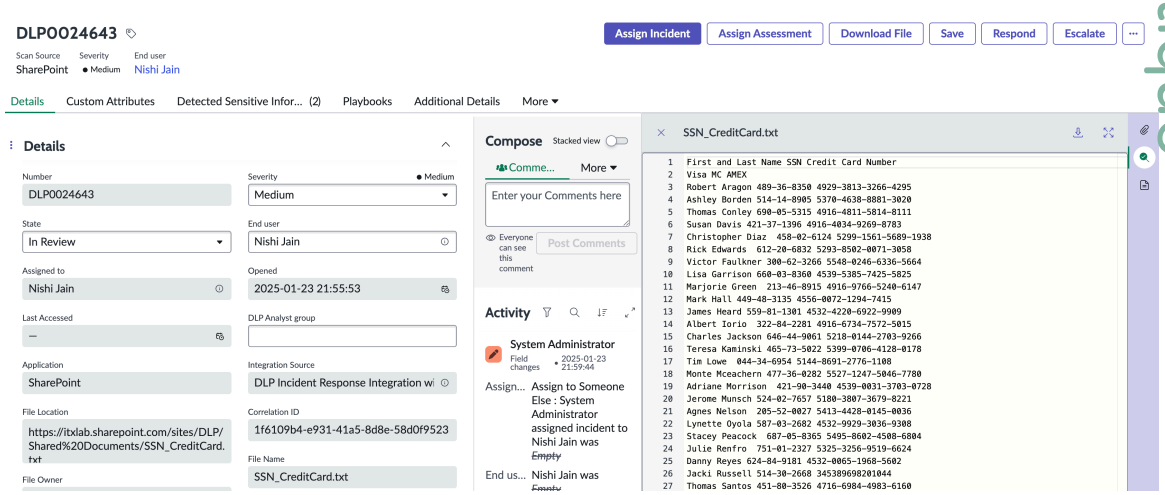
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Prévisualisez les images dans l'espace de travail de l'analyste DLP.
Seules les images avec les extensions .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg et .webp sont prises en charge.



8. Prévisualisez les fichiers texte dans l'éditeur de texte en sélectionnant l'icône **Développer** en haut à droite du fichier de preuve.



Remarque : Les fichiers de preuves, à l'exception des documents Office, des fichiers EML, du texte et des extensions d'image, ne seront pas pris en charge pour l'aperçu. Les fichiers binaires ne seront pas rendus et devront être téléchargés pour prévisualiser leur contenu. La fonctionnalité d'aperçu du fichier de preuve fonctionne également pour les incidents archivés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notifications pour les utilisateurs sur le mécanisme de nouvelle tentative

Netskope l'intégration réessaie le nombre configuré de fois en cas d'échec de l'API lors de l'ingestion d'incident DLP.

Une fois la limite maximale de nouvelles tentatives dépassée, Netskope l'intégration envoie une notification par e-mail aux utilisateurs qui ont le rôle d'administrateur DLP (sn_dlir.admin).

Une fois que vous avez terminé l'installation et la configuration de l'intégration, fournissez le rôle d'administrateur DLP (sn_dlir.admin) aux utilisateurs qui doivent être informés lorsque la limite maximale de nouvelles tentatives dépasse.

Une fois la limite maximale de nouvelles tentatives dépassée, le profil ignore l'ingestion pendant une durée pouvant aller jusqu'à une heure. Le nombre maximal de nouvelles tentatives est configuré à l'aide de la propriété suivante : Nombre maximal de nouvelles tentatives à effectuer pour les défaillances d'API. Pour plus d'informations, consultezConfigurer les Netskope paramètres d'intégration DLP.

Notifications par e-mail à l'expiration des informations d'identification

Lorsque le jeton utilisé dans l'instance expire, Netskope l'intégration ServiceNow envoie une notification par e-mail aux utilisateurs ayant le rôle d'administrateur DLP (sn_dlir.admin).

Une fois la configuration de l'intégration terminée, fournissez le rôle d'administrateur DLP (sn_dlir.admin) aux utilisateurs qui doivent être informés si le jeton a expiré.

Si le jeton expire, l'ingestion de données pour les profils associés sera suspendue jusqu'à ce que la configuration de l'intégration Netskope soit mise à jour avec un jeton valide.

Vous devez créer un jeton ou renouveler l'ancien Netskope le , puis mettre à jour le jeton sur l'instance ServiceNow . Si vous renouvelez le jeton en prolongeant le délai d'expiration, l'application Netskope détecte automatiquement le renouvellement et poursuit la collecte de données. Si vous créez un jeton, vous devez le mettre à jour dans la configuration.

Séparation en domaines dans l'intégration Netskope DLP

Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Prise en charge : Basique.

Comment fonctionne Séparation de domaine avec Netskope l'intégration DLP

Pour procéder à la séparation en domaines, procédez comme suit :

- Créez un utilisateur avec le rôle requis dans le domaine respectif.
- Effectuez les procédures d'intégration Netskope DLP dans le domaine approprié.

Intégration ICAP (Internet Content Adaption Protocol) pour DLP IR

L'intégration DLP ICAP (Internet Content Adaption Protocol) prend en charge l'ingestion d'alertes, permet l'extraction du contenu des Data Loss Prevention Incident Response correspondances et des fichiers de preuves à partir d'Amazon S3 créés sur le déploiement pris en charge Data Loss Prevention Incident Response ICAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois les alertes ingérées, vous pouvez utiliser l'espace de travail DLP pour afficher les informations clés requises, telles que le contenu des correspondances, la gravité des alertes et diverses fonctionnalités de gestion des incidents afin de corriger les incidents DLP.

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Vue d'ensemble et fonctionnalités principales

L'intégration ICAP (Internet Content Adaption Protocol) vous aide à suivre l'utilisation et le mouvement des données sensibles sur différentes plateformes.

Cette intégration comprend les fonctionnalités clés suivantes :

- Ingestion d'alertes DLP : les utilisateurs seraient en mesure de configurer et de planifier l'ingestion d'alertes DLP à partir de catégories Amazon S3 spécifiées. Cela inclut la possibilité d'effectuer des importations delta pour s'assurer que seules les nouvelles données sont ingérées.
- Afficher les alertes ingérées dans l'espace de travail DLP : une fois les alertes ingérées, elles doivent être affichées dans l'espace de travail DLP, en fournissant des détails clés sur chaque alerte, tels que le contenu de la correspondance, la gravité de l'alerte et les métadonnées pertinentes.
- Contenu de correspondance : les enregistrements d'informations sensibles sont créés lors de l'ingestion, le contenu de correspondance est récupéré lorsque l'enregistrement est ouvert.
- Téléchargement des fichiers de preuves : le système permettrait aux utilisateurs de télécharger les fichiers de preuves associés directement depuis l'espace de travail DLP pour une enquête ou un examen plus approfondi.
- Possibilité de personnaliser et de définir le mappage de gravité entre les incidents DLP ICAP et les incidents ServiceNow.

Premiers pas avec l'intégration DLP ICAP pour la protection contre la perte de données

Avant de pouvoir utiliser l'intégration, vous devez la télécharger à partir du ServiceNow® Store

Liste de vérification

Passez en revue les informations suivantes avant de commencer à configurer l'intégration DLP ICAP de votre fournisseur pour la protection contre la perte de données.

Liste de vérification

Champ	Description
Vérifiez que vous avez affecté les rôles requis de ServiceNow AI Platform l'application de prévention des pertes de données.	Les rôles suivants sont utilisés dans l'intégration DLP ICAP sur :ServiceNow AI Platform • L'administrateur (administrateur) installe les applications à partir de et ServiceNow® Store affecte l'administrateur de la prévention des pertes de données (sn_dlir.admin).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Champ	Description
	• L'utilisateur disposant du rôle sn_dlir.admin peut configurer l'intégration et configurer les profils d'incident. • Les utilisateurs disposant du rôle sn_dlir.analyst auront des rôles de lecture dans les configurations d'intégration.
Vérifiez que vous avez affecté les politiques de compartiment Amazon S3 requises.	Vous pouvez suivre la documentation officielle d'AWS pour la création et la gestion des utilisateurs, des politiques et des autorisations IAM via les liens suivants : • Création d'un utilisateur IAM • Création de politiques IAM • Autorisations Amazon S3 **Remarque :** À l'aide des liens ci-dessus, vous pouvez en savoir plus sur les instructions détaillées et les autres options de gestion des utilisateurs IAM et des autorisations S3 dans AWS, ainsi que sur la création d'un utilisateur IAM dans votre compte AWS - AWS Identity and Access Management, et la vue d'ensemble de base du processus utilisé pour créer un utilisateur IAM et des informations d'identification dans AWS Identity and Access Management.
Vérifiez que ServiceNow® l'application principale requise pour prendre en charge l'intégration DLP ICAP est installée et activée.	Vérifiez que les applications DLP et les applications courantes de support de sécurité suivantes sont installées et activées à partir de ServiceNow Store. Si ce n'est pas le cas, installez-le et activez-le sur l'application. • Security Support Common • Composants communs de l'espace de travail Gestion des tickets de sécurité. • Data Loss Prevention Incident Response

Installer et configurer l'intégration DLP ICAP

Installez et configurez l'intégration DLP ICAP du fournisseur à partir de ServiceNow® Store sur votre ServiceNow AI Platform instance. Commencez à enquêter sur les incidents DLP à l'aide des données d'incident DLP ICAP du fournisseur.

Avant de commencer
Rôle requis : sn_dlir.admin

Traduction automatique

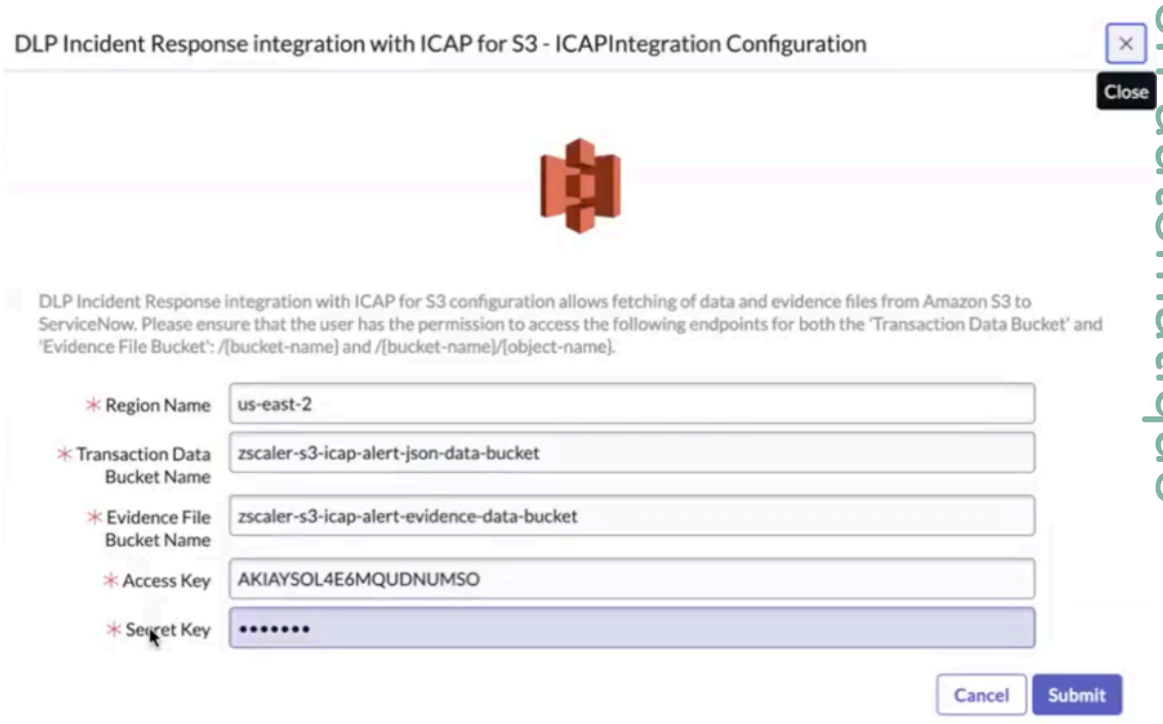
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Téléchargez l'intégration DLP ICAP du fournisseur à partir de et ServiceNow® Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Recherchez la vignette DLP Incident Response Integration with ICAP et cliquez sur **Configurer**.
4. Remplissez les champs du formulaire.

Formulaire Configuration de l'intégration DLP ICAP

Champ	Description
Nom de la région	Nom de la région du nom de la catégorie Amazon S3.
Nom de catégorie de données de transaction	Le nom de la catégorie de données de transaction est la catégorie dans laquelle une transaction de violation DLP a eu lieu.
Nom de la catégorie de fichier de preuves	Le nom de la catégorie de fichier de preuves est la catégorie dans laquelle vous pouvez trouver le fichier DLP à l'origine de l'infraction.
Clé d'accès	Clé d'accès AWS IAM pour la configuration ICAP.
Clé secrète	Clé secrète AWS IAM pour la configuration ICAP.



5. Cliquez sur **Envoyer**.

Résultats

Remarque : Veuillez connecter la sous-production ICAP à la sous-production ServiceNow. Gardez tous les noms d'utilisateur et mots de passe synchronisés entre les instances pour éviter que les comptes ne soient déconnectés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois que vous avez validé et soumis la configuration, les configurations de l'intégration ICAP DLP sont enregistrées.

Créer un profil pour l'intégration DLP ICAP

Créez un profil d'incident dans votre ServiceNow AI Platform instance. Déterminez les alertes DLP ICAP adaptées à la création d'incidents DLP.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Configurez NowPlatform pour extraire les alertes DLP à partir de la configuration Amazon S3. Stockez ces alertes dans votre instance ServiceNow en tant qu'incidents DLP.

Procédure

1. Accédez à la **Tous** > **Intégration DLP ICAP** > **Profil d'incident**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs de la section Nom du formulaire.

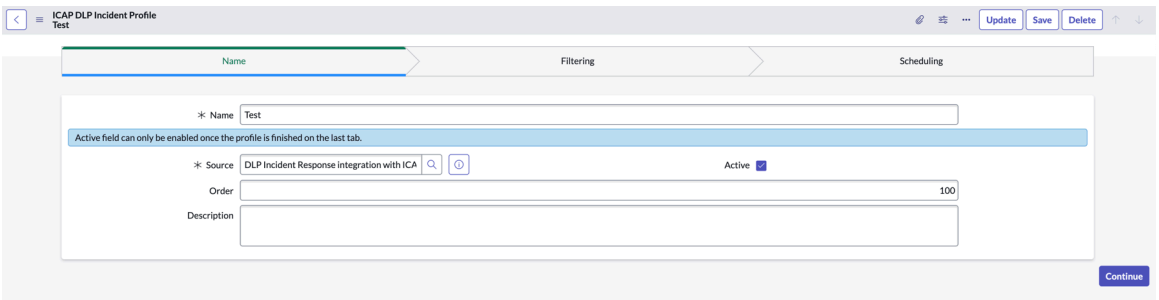
Créer un profil

Champ	Description
Nom	Nom du profil. Ce champ vous permet d'identifier le profil. **Remarque :** Le nom doit être unique pour chaque profil.
Source	Configuration Amazon S3 que vous avez configurée pour ingérer des incidents. Si plusieurs sources sont configurées, sélectionnez la source appropriée pour le type d'incident que vous prévoyez d'ingérer pour le profil. **Remarque :** Une seule source est autorisée pour le profil actif.
Actif	Option permettant d'indiquer si le profil est actif. Ce champ ne peut être activé qu'une fois que vous avez cliqué sur **Terminer** dans la section Planification. Lorsque le profil est actif, cela implique qu'il ServiceNow AI Platform interroge activement les alertes DLP ICAP. Les alertes DLP correspondantes sont créées dans DLP lorsque les conditions de filtrage sont mises en correspondance en fonction des paramètres de planification que vous avez fournis.
Ordre	Ordre d'exécution du profil. Le profil avec l'ordre le plus bas considéré comme la priorité la plus élevée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par défaut, la valeur est 100.
Description	Description de ce profil.



Que faire ensuite

Pour passer à la section Filtrage, cliquez sur **Continuer**.

Définir les filtres à appliquer pour la création d'incident

Définissez et définissez des conditions de filtre pour filtrer les alertes DLP entrantes. Déterminez les alertes qui doivent être créées en tant qu'incidents DLP dans ServiceNow.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Le filtrage vous aide à isoler les alertes DLP et à limiter le nombre d'alertes DLP que vous créez. Si des critères de filtrage supplémentaires sont définis, seules les alertes qui correspondent aux conditions sont créées.

Procédure

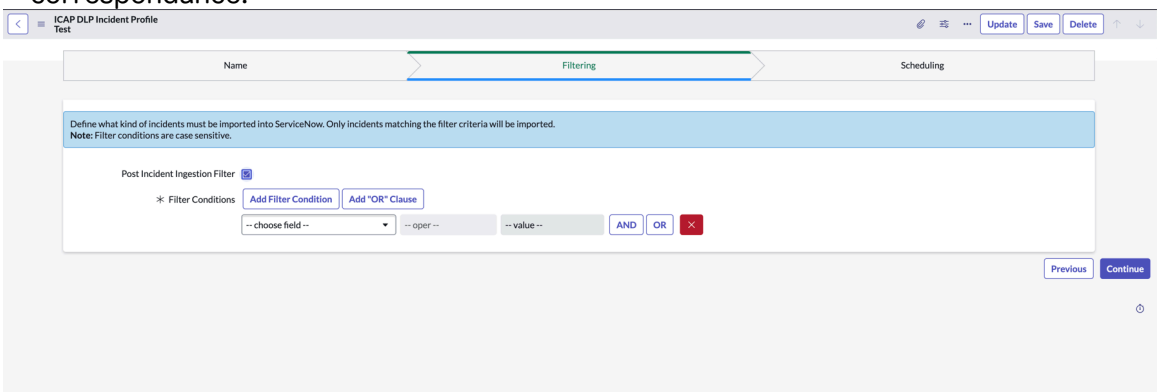
1. Cochez la case **Filtre d'ingestion post-incident** pour appliquer les filtres d'ingestion post-incident et récupérer les incidents qui correspondent aux critères de filtre.
2. Sélectionnez l'option **Filtrer en fonction des conditions** et définissez les critères qu'un incident DLP ICAP entrant doit satisfaire pour qu'un incident DLP soit créé.
3. Définissez les filtres dans le champ **Conditions de filtre** .

   Les options de la liste déroulante **Conditions de filtre** correspondent aux champs disponibles dans la table **d'importation d'incidents DLP ICAP** . Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'incident.
4. Ajoutez d'autres conditions en cliquant sur **ET** ou **OU**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
- Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.



Que faire ensuite

Pour configurer le calendrier, cliquez sur **Continuer**.

Planifier la récupération des incidents DLP ICAP

Définissez un calendrier pour récupérer les alertes DLP ICAP qui correspondent aux critères du profil.

Avant de commencer

Rôle requis : sn_dlir.admin

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier la fréquence à laquelle vous interrogerez les nouveaux incidents ICAP nets qui correspondent à la configuration du profil d'incident. Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Le profil peut être configuré pour effectuer une récupération ponctuelle à l'aide de la case à cocher **Récupération ponctuelle** .

Procédure

1. Configurez le calendrier pour définir comment et quand extraire des incidents d'ICAP.
2. Remplissez les champs du formulaire.

Planifier les incidents DLP ICAP

Champ	Description
Intégration de l'incident en cours	Ingestion d'incidents en cours que votre ServiceNow AI Platform instance extrait d'ICAP pour les nouveaux incidents. Si des incidents déclenchés correspondent aux critères de filtrage d'incidents, des incidents DLP sont créés.
Incrémentation du sondage (minutes)	Fréquence d'interrogation définie en minutes. Cette valeur par défaut est définie sur **5**.
Définir le délai d'intégration de l'incident initial	Option permettant de définir l'ingestion d'incident initial en fonction de la date et de l'heure configurées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Vous pouvez utiliser cette option pour définir une date et une heure spécifiques pour l'ingestion initiale. Les ingestions suivantes sont basées sur la période de l'intervalle d'interrogation.
Délai d'intégration de l'incident initial d'entrée	Date et heure que vous spécifiez pour l'ingestion de l'incident.
Délai d'intégration de l'incident initial	La première fois que des données sont ingérées. **Remarque :** La valeur n'est visible que si l'option **Définir le délai d'intégration de l'incident initial** est sélectionnée.
Délai d'intégration de l'incident suivant (estimé)	Délai d'intégration estimé de l'incident suivant
Récupération ponctuelle	Option permettant d'activer l'extraction unique des données historiques. **Remarque :** Si cette option est sélectionnée, les données historiques sont extraites du DLP ICAP en fonction de la date ajoutée dans **Date de début**.
Nom du dossier	Nom du dossier à partir duquel vous souhaitez récupérer les données. Tous les dossiers dont le nom est lexicographiquement supérieur au nom de dossier fourni seront ingérés lors d'une récupération unique.

3. Cliquez sur **Terminer**.
4. Dans la fenêtre contextuelle, enregistrez la configuration de profil créée en cliquant sur **Terminer**.
5. Activez le profil.
   a. Ouvrez le profil créé.
   b. Définir **Actif** sur **vrai**.
   c. Cliquez sur **Mettre à jour**.

Résultats
Une fois l'activation du profil créée, les incidents sont extraits périodiquement conformément à la configuration définie dans le profil. Les alertes sont ajoutées à la table d'incidents DLP.

Afficher les informations sensibles pour les alertes DLP

Affichez les informations sensibles détectées pour les alertes DLP.

Avant de commencer
Certaines règles et politiques sont configurées dans l'intégration respective et si vous enfreignez les politiques définies, un incident DLP est créé et le contenu de la correspondance affiche ces informations violées dans la section Informations sensibles de cet enregistrement d'incident DLP.

Rôle requis : sn_dlir.analyst

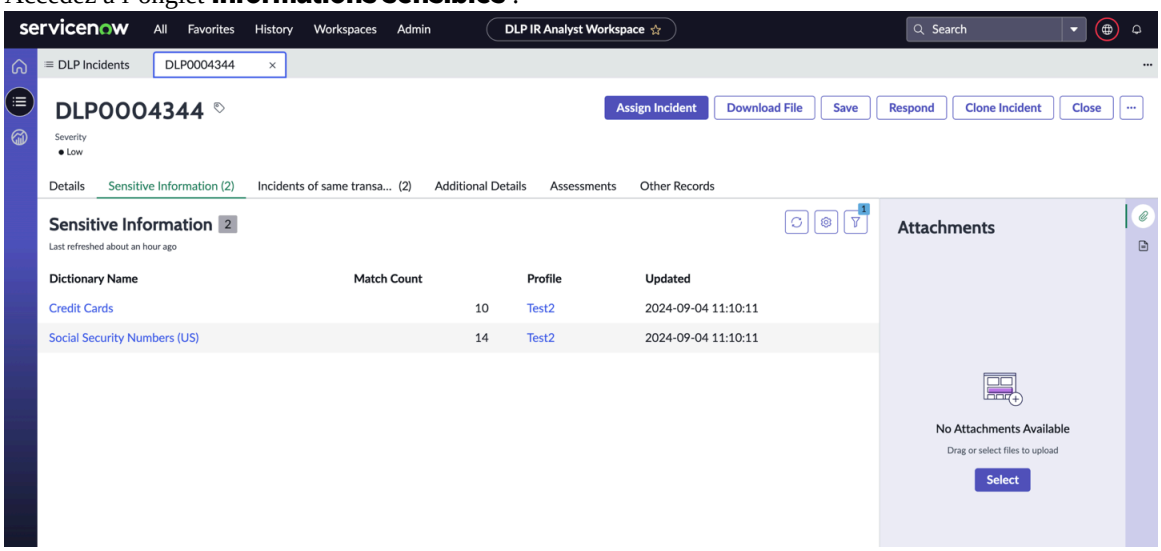
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

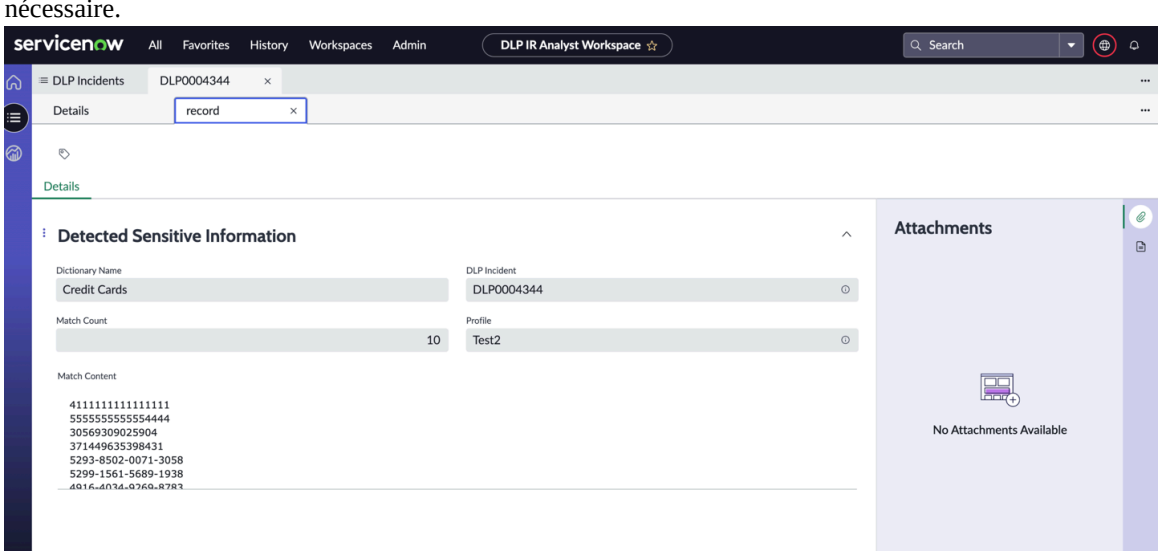
Remarque : Les utilisateurs finaux peuvent également consulter les informations sensibles en se connectant à l'espace de travail de l'utilisateur DLP.

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
   La page Espace de travail DLP : mes incidents s'affiche dans l'Espace de travail de l'analyste DLP pour les analystes.
2. Ouvrez n'importe quel incident DLP.
3. Accédez à l'onglet **Informations sensibles** .



4. Cliquez sur l'enregistrement violé.
5. Consultez les informations de contenu de la correspondance et prenez les mesures correspondantes si nécessaire.



Télécharger des fichiers de preuves pour les alertes DLP

Téléchargez des fichiers qui enfreignent la politique DLP sur le fournisseur qui prend en charge ICAP. Téléchargez ce fichier sur votre ordinateur local à partir de l'espace de travail de l'analyste DLP IR et de l'espace de travail de l'utilisateur final DLP IR pour les approbateurs.

Avant de commencer

Rôle requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sn_dlir.analyst et les approbateurs peuvent télécharger

Pourquoi et quand exécuter cette tâche

Vous devez activer le téléchargement de fichiers pour ICAP avant de poursuivre.

Procédure

1. Accédez à la **Tous** > **Intégration DLP ICAP** > **Paramètres**.
2. Activez la propriété sn_icap_dlp.enable_file_download **L'activation de cette propriété permet de télécharger le fichier de preuves de l'incident ICAP signalé**.
   Vous pourrez voir le bouton Télécharger le **fichier** sur l'espace de travail de l'analyste DLP IR et l'espace de travail de l'utilisateur final DLP IR.
3. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
4. Ouvrez un enregistrement d'incident DLP qui est ingéré à partir de la source du fournisseur ICAP.
5. Cliquez sur **Télécharger le fichier**.

> **Remarque :** L'administrateur DLP peut contrôler l'accès à l'action **Télécharger le fichier** pour toutes les intégrations en désactivant l'option **Le téléchargement du fichier de violation de l'incident signalé doit-il être autorisé** à partir de la page **Paramètres avancés** de l'administration DLP. Pour plus d'informations, consultez Configurer les paramètres avancés.

Prévisualiser les fichiers de preuves pour ICAP

Prévisualisez les fichiers de preuves d'incidents DLP dans l'espace de travail de l'analyste DLP IR.

Avant de commencer

- Accédez à la **Tous** > **Administration DLP** > **Paramètres avancés**.
- Assurez-vous que la propriété **sn_icap_dlp.enable_evidence_file_preview** est déjà activée.

> **Important :** Lors de l'utilisation de l'action Fichiers de preuves dans l'espace de travail de l'analyste DLP, les fichiers de preuves sont temporairement stockés dans la base de données ServiceNow dans un format non chiffré pendant la durée que vous avez sélectionnée à l'aide de la propriété **sn_dlir.preview_temp_files_cleanup_interval** de la page **Paramètres avancés** . Vous pouvez désactiver la fonctionnalité d'aperçu des **fichiers de preuves** si vous ne souhaitez pas stocker de données dans la base de données ServiceNow. Pour plus d'informations, consultez Configurer les paramètres avancés.

Rôle requis : sn_dlir.analyst

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez un enregistrement d'incident DLP.
3. Sélectionnez l'icône **Fichiers de preuves** , disponible dans le menu contextuel.
   Un onglet s'ouvre et récupère tous les fichiers de preuves. Une fois le téléchargement terminé, vous pouvez afficher tous les fichiers de preuves dans l'onglet **Fichiers de preuves** .
4. Sélectionnez la carte **Fichier de preuves** que vous souhaitez prévisualiser.
   La fonction d'aperçu est différente pour chaque type de fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

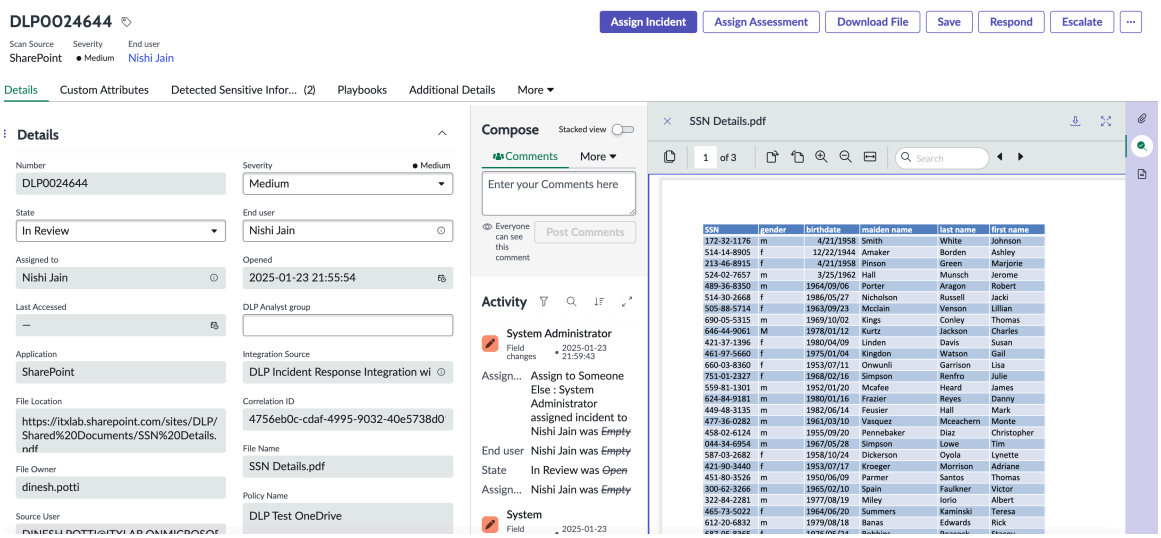
5. Prévisualisez le PDF et les documents Office dans la visionneuse de documents en sélectionnant l'icône **Développer** en haut à droite du fichier de preuves pour ouvrir le PDF en plein écran.
Les extensions Office pour lesquelles la visionneuse de documents ouvre les fichiers de preuves incluent : doc, docx, ppt, pptx, xls, xlsx.

a. Localisez la barre de recherche et entrez le mot-clé que vous recherchez.

b. Utilisez les fonctions de zoom avant et arrière pour ajuster la vue et améliorer la lisibilité.

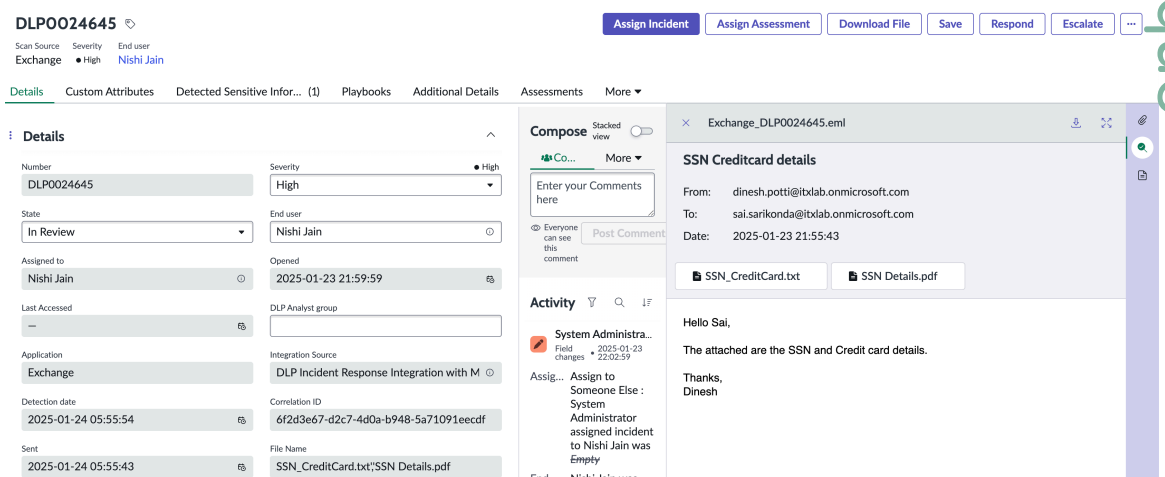
c. Faites pivoter la page dans le sens des aiguilles d'une montre ou dans le sens inverse des aiguilles d'une montre pour afficher le contenu plus clairement.

Ces options de contrôle améliorent votre capacité à comprendre le dossier de preuves de manière exhaustive. Seul le PDF comporte des options de contrôle dans l'en-tête.



6. Prévisualiser les fichiers EML.
Sélectionnez les pièces jointes dans l'e-mail et prévisualisez-les.

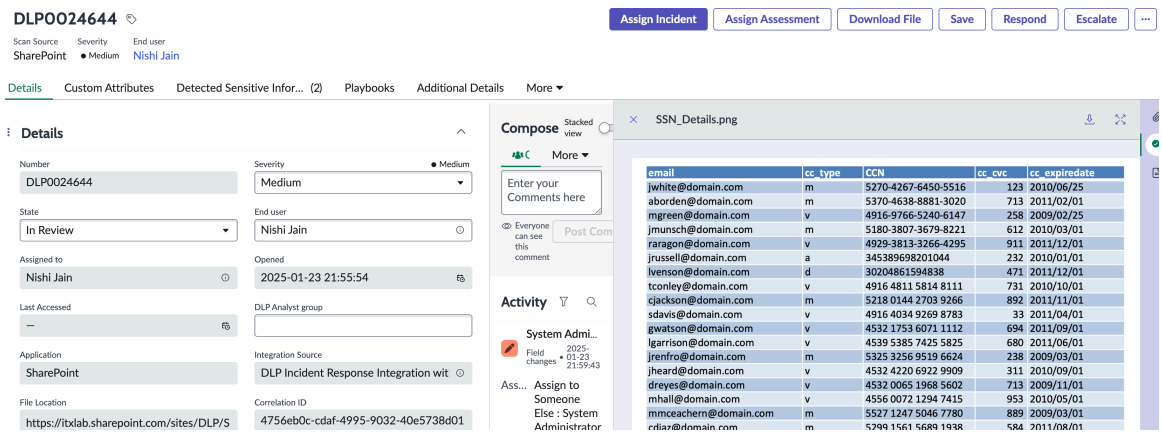
Remarque : Si le fichier de preuve sélectionné dépasse la limite de 5 Mo, il ne peut pas être prévisualisé dans Analyst Workspace. Vous devez télécharger le fichier pour prévisualiser son contenu. Cette limite ne concerne que les fichiers .eml.



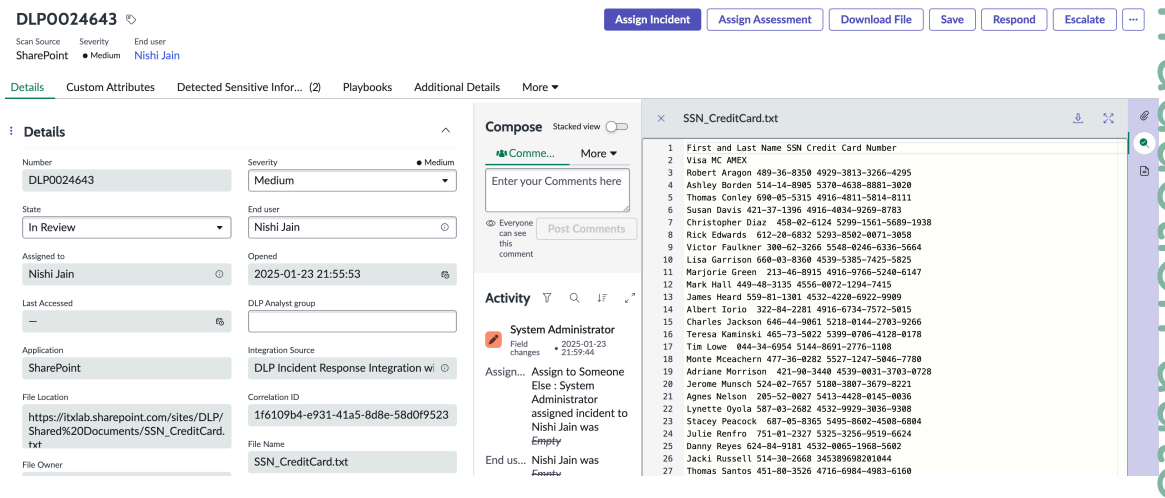
7. Prévisualisez les images dans l'espace de travail de l'analyste DLP.
Seules les images avec les extensions .bmp, .gif, .ico, .jpeg, .jpg, .png, .svg et .webp sont prises en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Prévisualisez les fichiers texte dans l'éditeur de texte en sélectionnant l'icône **Développer** en haut à droite du fichier de preuve.



Remarque : Les fichiers de preuves, à l'exception des documents Office, des fichiers EML, du texte et des extensions d'image, ne seront pas pris en charge pour l'aperçu. Les fichiers binaires ne seront pas rendus et devront être téléchargés pour prévisualiser leur contenu. La fonctionnalité d'aperçu du fichier de preuve fonctionne également pour les incidents archivés.

Passer en revue les paramètres d'intégration ICAP DLP

Passez en revue les paramètres d'intégration ICAP DLP du fournisseur et modifiez les propriétés système par défaut en fonction de votre environnement.

Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Accédez à la **Tous** > **Intégration DLP ICAP** > **Paramètres**.
2. L'examen et la modification des paramètres sont requis.

Nom de la propriété	Description
sn_icap_dlp.maximum_retry	Option permettant de choisir le nombre maximal de nouvelles tentatives à effectuer pour les défaillances d'objets AWS Get.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de la propriété	Description
sn_icap_dlp.logging.verbosité	Définissez le niveau de génération de rapports des journaux générés par l'intégration. La valeur par défaut est définie sur 4.
sn_icap_dlp.enable_file_download	L'option permettant d'activer cette propriété permet de télécharger le fichier de preuves de l'incident ICAP signalé. Par défaut, cette option est activée.
sn_icap_dlp.presigned_file_expiry_time	Spécifiez la durée, en secondes, pendant laquelle le fichier présigné sera disponible au téléchargement ou en prévisualisation. Le fichier ne sera accessible que pendant cette période. Ce champ est automatiquement défini sur 300.

Data Loss Prevention Incident Response avec Microsoft

Microsoft ll Data Loss Prevention Incident Response fournit un cadre de travail de base pour importer des incidents de protection contre la perte de données (DLP) à partir de plusieurs sources, telles que Microsoft les applications d'aperçu (Microsoft Teams, Exchange Online, SharePoint Online, OneDrive Entreprise) et d'autres types d'événements. Les appareils de point de terminaison permettent un workflow de rattrapage impliquant les utilisateurs finaux, les responsables et l'équipe des opérations DLP avec une affectation et des remontées automatisées des incidents.

Demander des applications dans l'App Store

Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Store notes de publication relatives à l'historique des versions .

Fonctionnalités principales

Utilisez les fonctionnalités clés de cette intégration pour effectuer les actions suivantes :

- Créez plusieurs profils pour différents comptes.
- Automatiser la création d'incidents DLP IR .
- Mappez les champs d'événement sur DLP IR les Microsoft DLP IR champs d'incident.
- Filtrer Microsoft DLP IR les événements.
- Planifiez l'ingestion d'événements qui créent DLP IR périodiquement des DLP IR incidents.
- Stockez le contenu correspondant de chaque événement DLP Microsoft dans un stockage cloud externe.
- Supprimer le contenu correspondant au stockage cloud externe lors de la suppression de l'incident dans ServiceNow.DLP IR
- Télécharger des fichiers pour DLP IR les incidents de type Exchange, OneDrive et SharePoint.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus sur cette intégration

Identificateur de document	Titre de document
Microsoft Site web de la documentation produit	Site web de la documentation produit Microsoft
ServiceNow Site web de la documentation produit	Site web de la documentation produit ServiceNow

Premiers pas avec l'intégration Microsoft DLP IR pour la protection contre la perte de données

Examinez les informations suivantes avant de commencer à configurer votre Microsoft DLP IR intégration pour la protection contre la perte de données.

Liste de vérification

Tâche de configuration	Description
Obtenez les informations d'identification Microsoft Purview pour extraire les données de l'événement et les informations d'identification du compte de stockage AWS/Azure pour stocker le contenu de la correspondance Enregistrer une application auprès de la plateforme d'identité Microsoft	Enregistrez une application sur la plateforme Microsoft Azure à partir d'ici pour obtenir l'ID client, le secret client et l'ID de locataire. Pour plus d'informations sur les rôles requis pour créer une application, consultez Prérequis . Pour plus d'informations sur les autorisations/rôles d'API requis sur une application Microsoft Azure pour la configurer sur ServiceNow l'intégration de Microsoft DLP, reportez-vous au tableau suivant.
Autorisations requises pour que l'utilisateur Azure accède à l'objet blob en lecture/écriture/suppression sur le stockage Azure	L'utilisateur Azure doit avoir le rôle **Contributeur de données Blob de stockage** pour lire, écrire et supprimer des objets blob sur le stockage Azure.
Autorisations requises pour que l'utilisateur AWS obtienne l'accès à l'objet de lecture/d'écriture/de suppression sur le stockage AWS	Une politique doit être créée pour donner l'accès à la liste, à la lecture, à l'écriture et à la suppression de l'objet dans AWS S3 Storage.
Affectez et vérifiez si vous disposez des rôles requis pour ServiceNow AI Platform les rôles d'administration des pertes de données.	Les rôles suivants sont requis pour la configuration et la vérification des résultats attendus : • Le rôle administrateur installe l'intégration à partir de et ServiceNow Store attribue le rôle sn_dlir.admin. • Le rôle sn_dlir.admin effectue les tâches suivantes : ○ Configure l'intégration. ○ Configure les profils d'incident.
Vérifiez que les ServiceNow applications principales requises pour prendre en charge l'intégration Microsoft DLP IR sont installées et activées avant de configurer cette intégration.	Vérifiez que les applications courantes et les applications courantes de prise en charge de la sécurité suivantes DLP IR sont installées et activées à partir de la ServiceNow boutique. Si elle n'est pas installée, installez-la et activez-la sur l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Liste de vérification (suite)

Tâche de configuration	Description
	• Security Support Common • Data Loss Prevention Incident Response

Autorisations/rôles d'API requis sur une application Microsoft Azure

Vous avez besoin des autorisations/rôles d'API suivants sur une application Microsoft Azure pour la configurer sur **ServiceNow** *l'intégration DLP de Microsoft.*

API	Nom d'autorisation	Type	Description	Quelle fonctionnalité ServiceNow est-elle requise ?	Le consentement de l'administrateur est-il requis ?
Office 365 Management API	FluxActivité.Lecture.All	Application	Lire les événements de politique DLP, y compris les données sensibles détectées.	Pour ingérer les événements DLP de MSFT Purview vers ServiceNow. **Remarque :** Cette autorisation est indispensable pour obtenir les données MSFT dans ServiceNow.	Oui
Microsoft Graph API	Fichiers.Lecture.Tout	Application	Lisez les fichiers dans toutes les collections de sites auxquelles vous pouvez accéder.	Télécharger le fichier : pour télécharger la pièce jointe sur l'instance ServiceNow à l'origine de l'événement DLP à partir de OneDrive ou SharePoint **Remarque :** Ceci est facultatif. Vous pouvez ignorer cette autorisation d'API si vous ne souhaitez pas autoriser les analystes à télécharger la pièce jointe à l'origine de l'événement DLP.	Oui
	Courrier.Lecture	Application	Lire les e-mails dans toutes les boîtes aux lettres.	Télécharger le fichier : pour télécharger le contenu de l'e-mail (corps et pièce jointe) sur l'instance ServiceNow à l'origine de	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisations/rôles d'API requis sur une application Microsoft Azure
Vous avez besoin des autorisations/rôles d'API suivants sur une application Microsoft Azure pour la configurer sur **ServiceNow** *l'intégration DLP de Microsoft.*

(suite)

API	Nom d'autorisation	Type	Description	Quelle fonctionnalité ServiceNow est-elle requise ?	Le consentement de l'administrateur est-il requis ?
				l'événement DLP à partir d'Exchange. **Remarque :** Ceci est facultatif. Vous pouvez ignorer cette autorisation d'API si vous ne souhaitez pas autoriser les analystes à télécharger le contenu de l'e-mail (corps, pièce jointe) à l'origine de l'événement DLP.	
	Utilisateur.Lire	Délégué	Connectez-vous et lisez le profil d'utilisateur.	Il s'agit de l'autorisation par défaut qui sera disponible pour toutes les nouvelles applications.	Non

Informations sensibles détectées (facultatif)

Le contenu de la correspondance est stocké en externe dans le stockage Azure Blob ou la catégorie Amazon S3 et est extrait du stockage externe lorsque l'utilisateur visualise un incident.

L'une des autorisations suivantes est nécessaire si les utilisateurs souhaitent afficher le contenu de la correspondance/les informations sensibles détectées dans l'application DLP Core :

1. Si vous êtes un Microsoft Azure utilisateur, vous devez avoir le rôle Contributeur de données Blob de stockage pour lire, écrire et supprimer des objets blob sur Stockage Azure.
2. Si vous êtes un utilisateur Amazon S3, vous devez créer une stratégie qui donne l'accès à la liste, à la lecture, à l'écriture et à la suppression de l'objet dans le stockage Amazon S3.

Installer et configurer l'intégration DLP de Microsoft

Installez et configurez l'intégration de DLP Incident Response avec Microsoft DLP à partir de ServiceNow® Store sur votre ServiceNow AI Platform instance. Commencez à enquêter sur les incidents DLP à l'aide des données d'événements Microsoft DLP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

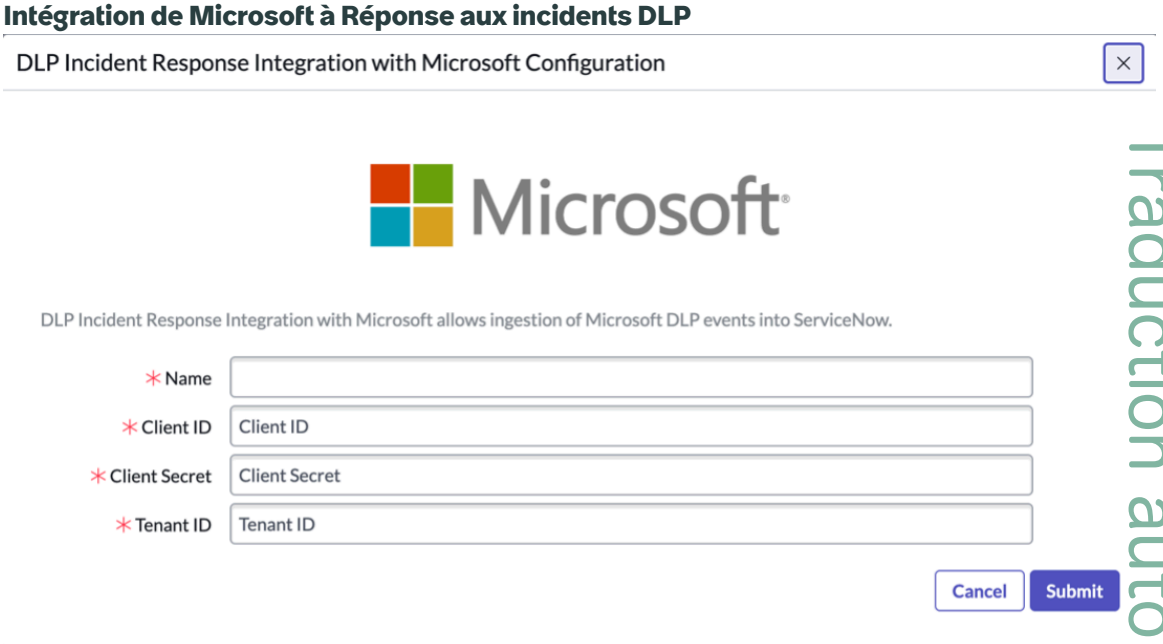
Avant de commencer

Rôle requis : sn_dlir.admin

Procédure

1. Téléchargez l'intégration Microsoft DLP à partir de et ServiceNow® Store installez-la.
2. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration**.
3. Configurez l'intégration DLP Microsoft .
   a. Recherchez la vignette **DLP Incident Response Integration with Microsoft** et cliquez sur **Configurer**.

Intégration de Microsoft à Réponse aux incidents DLP



   b. Remplissez les champs du formulaire.

Formulaire Configuration de l'intégration DLP Microsoft

Champ	Description
Nom	Nom de la configuration de l'intégration Microsoft DLP.
ID client	ID client de l'application créée sur le portail Microsoft Azure.
Secret client	Secret client de l'application créée sur le portail Microsoft Azure.
ID de locataire	ID de locataire de l'utilisateur.

   c. Cliquez sur **Envoyer**.

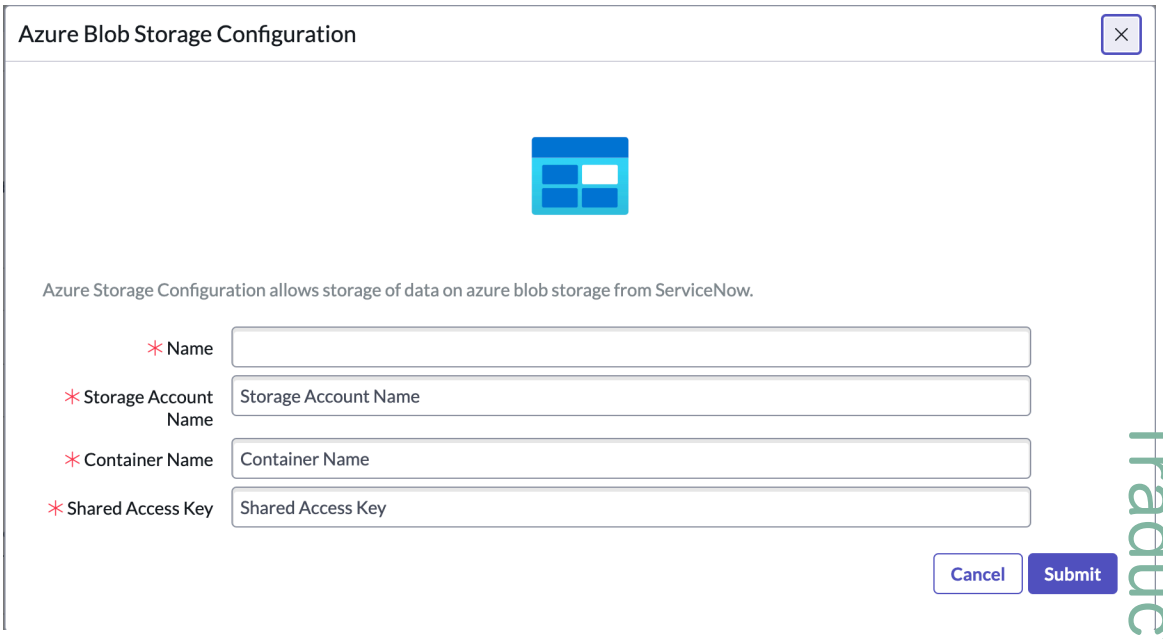
   Une fois que vous avez validé et soumis la configuration, l'intégration Microsoft DLP est enregistrée sur la page Intégrations de sécurité sous forme de tuile.
4. Mettez à jour la configuration de stockage Azure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sur la page Intégrations de sécurité, recherchez la vignette **Configuration du stockage Azure** .

b. Dans la vignette Configuration du stockage Azure, cliquez sur **Mettre à jour**.



c. Remplissez les champs du formulaire.

Formulaire de configuration du stockage Azure

Champ	Description
Nom	Nom de la configuration de stockage Azure.
Nom du compte de stockage	Nom du compte de stockage créé sur le portail Azure
Nom du conteneur	Nom du conteneur créé dans le compte de stockage sur le portail Azure.
Clé d'accès partagé	Clé d'accès partagé pour le compte de stockage.

d. Cliquez sur **Envoyer**.

Une fois que vous avez validé et soumis la configuration, la configuration de stockage Azure est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

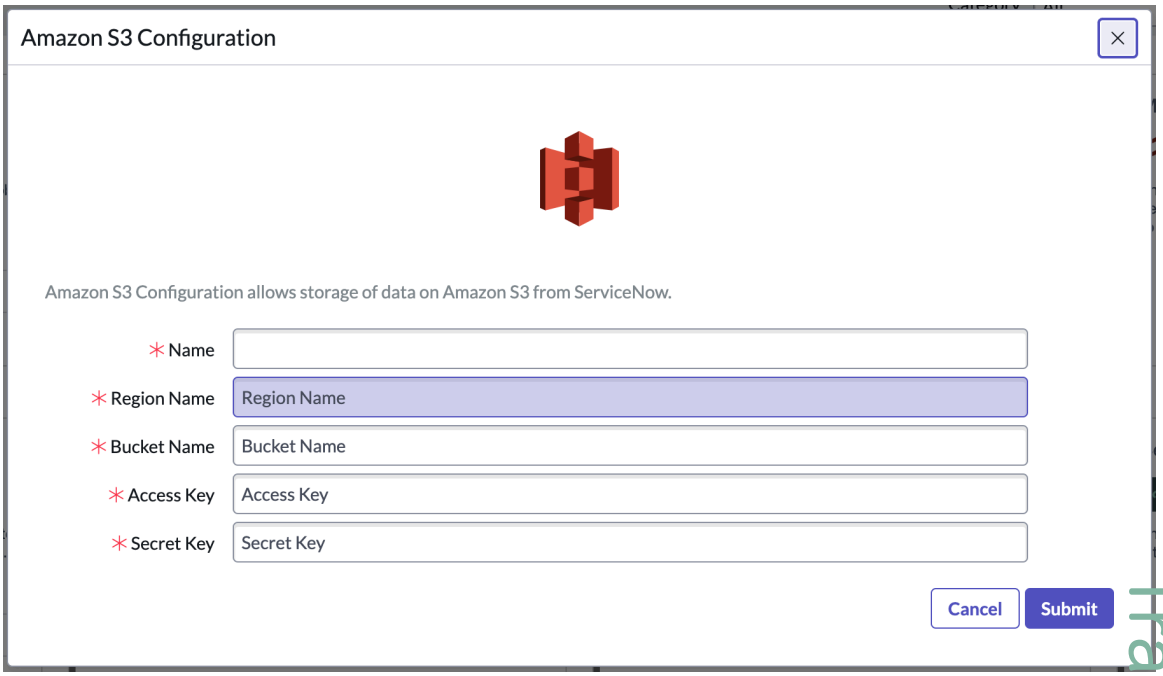
5. Mettez à jour la configuration de stockage AWS.

a. Sur la page Intégrations de sécurité, recherchez la vignette **Configuration du stockage AWS** .

b. Dans la vignette AWS Storage Configuration, cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



c. Remplissez les champs du formulaire.

Formulaire de configuration du stockage AWS

Champ	Description
Nom	Nom de la configuration de stockage AWS.
Nom de la région	Nom de la région du compte de stockage AWS.
Nom du compartiment	Nom de la catégorie créée sur le portail AWS.
Clé d'accès	Clé d'accès avec accès en lecture, en écriture et en suppression.
Clé secrète	Clé partagée avec accès en lecture, en écriture et en suppression

d. Cliquez sur **Envoyer**.

Résultats

Une fois que vous avez validé et soumis la configuration, la configuration AWS S3 est enregistrée sur la page Intégrations de sécurité sous forme de tuile.

Créer un profil d'incident pour Microsoft l'intégration DLP

Créez un profil d'incident dans votre ServiceNow AI Platform instance pour récupérer les données à partir de Microsoft Purview et ajouter les données dans la table d'incidents ServiceNow DLP IR .

Avant de commencer

Rôle requis : sn_dlir.admin(Créer, modifier et supprimer)

sn_dlir.analyst : vue (lecture seule)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Configurez le ServiceNow AI Platform® pour récupérer les événements à partir de Purview Microsoft . Stockez ces événements dans la DLP IR table Incident de votre ServiceNow® instance.

Procédure

1. Accédez à la **Intégration DLP Microsoft** > **Profil d'incident**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs de la section Nom du formulaire.

Formulaire Créer un profil

Champ	Description
Nom	Nom du profil. Ce champ vous permet d'identifier le profil. **Remarque :** Le nom doit être unique pour chaque profil.
Source	Instance Microsoft DLP IR que vous avez configurée pour ingérer des incidents. Si vous disposez de plusieurs configurations d'intégration, sélectionnez l'enregistrement de configuration d'intégration approprié pour les types d'incidents que vous prévoyez d'ingérer pour le profil.
Actif	Option permettant d'indiquer si le profil est actif. Ce champ ne peut être activé qu'une fois que vous avez cliqué sur le champ **Terminer** dans la section Planification. Lorsque le profil est actif, cela implique qu'il ServiceNow AI Platform interroge Microsoft DLP IR activement les événements en fonction de la configuration définie dans le profil.
Ordre	Ordre d'exécution du profil. Le profil avec l'ordre le plus bas considéré comme la priorité la plus élevée. Par défaut, la valeur est 100.
Description	Description unique pour le profil.

Que faire ensuite

Pour passer à la section Filtrage, cliquez sur **Continuer**.

Configuration du stockage des points de terminaison Microsoft Purview

La configuration du stockage des fichiers de preuves de points de terminaison Microsoft Purview vous indique où les fichiers de preuves de points de terminaison sont stockés par les environnements de stockage personnalisé ou de stockage géré par Microsoft.

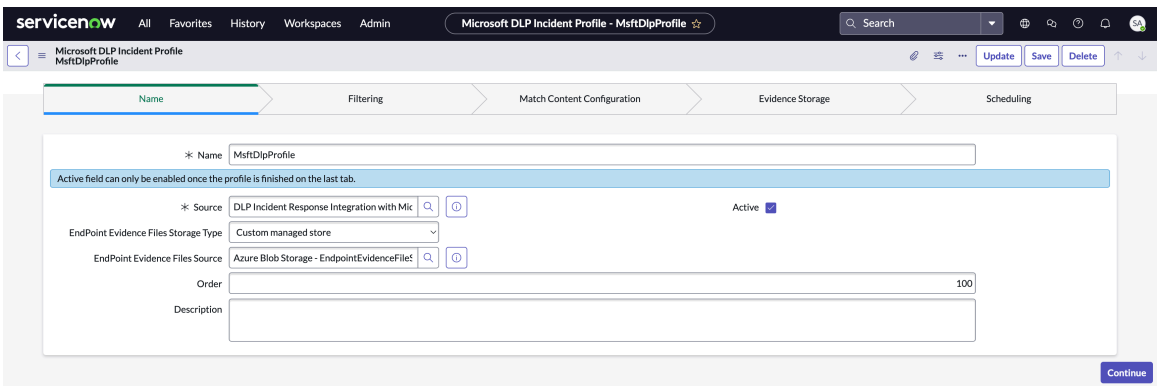
Dans le cas d'un magasin géré par Microsoft, Microsoft lui-même stocke les fichiers de preuves à un certain emplacement et pour le magasin géré personnalisé, vous devez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

spécifier le conteneur dans lequel les fichiers de preuves seront stockés par le domaine lorsqu'une alerte est générée.

Sélectionnez l'un des deux types de stockage en fonction de ce qui est configuré à l'extrémité du champ d'application pour que le système récupère les fichiers de preuves des incidents DLP de point de terminaison correspondants.



Remarque : Nous vous recommandons d'utiliser le **magasin géré personnalisé** , car Microsoft ne fournit actuellement aucune API permettant de récupérer les fichiers de preuves à partir du **magasin géré Microsoft**. Par conséquent, la fonctionnalité d'aperçu et de téléchargement n'est pas prise en charge pour les preuves stockées dans le Microsoft Managed Store. Nous avons soulevé un cas auprès de Microsoft concernant cette limitation.

Définir les filtres à appliquer pour la création d'incident

Définissez et définissez des conditions de filtre pour filtrer les événements DLP Microsoft entrants. Contrôlez lesquels de ces événements doivent être créés en tant qu'incidents DLP IR sur votre ServiceNow instance.

Avant de commencer

Rôle requis : sn_dlir.admin(Créer, modifier et supprimer)

sn_dlir.analyst : vue (lecture seule)

Pourquoi et quand exécuter cette tâche

Ce type de filtrage vous permet d'isoler les événements DLP Microsoft afin de limiter le nombre d'incidents DLP IR que vous créez. Si les critères de filtrage sont définis, seuls les événements qui correspondent aux conditions sont créés en tant qu'incidents DLP.

Procédure

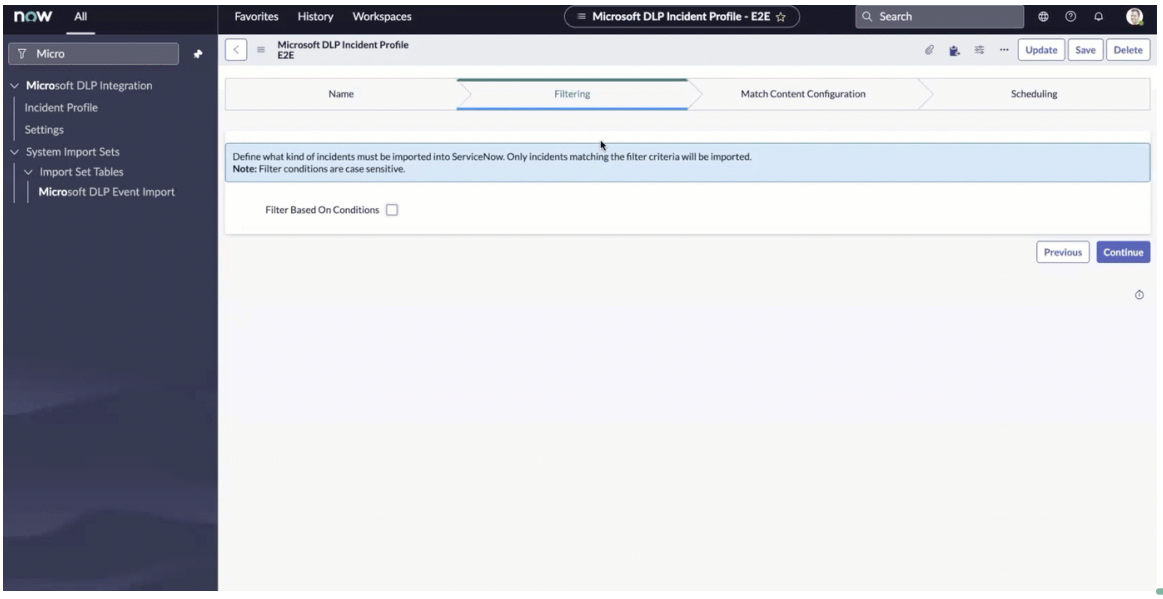
1. Sélectionnez l'option **Filtrer en fonction des conditions** .
2. À l'aide des listes et des champs du générateur de conditions, définissez les filtres dans le champ **Conditions de filtre** .

   Définissez les critères qu'un événement DLP entrant Microsoft doit satisfaire pour qu'un incident DLP soit créé.

   Les options du premier champ des **Conditions de filtre** correspondent aux champs disponibles dans l'événement DLP Microsoft. Les critères que vous saisissez sont sensibles à la casse. Vérifiez que les critères que vous définissez correspondent aux valeurs de l'événement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Ajoutez d'autres conditions en cliquant sur **ET** ou **OU**.
   - Si **ET** est sélectionné, toutes les conditions doivent être mises en correspondance.
   - Si **OU** est sélectionné, l'une ou l'autre des conditions peut être mise en correspondance.
4. Cliquez sur **Continuer** et passez à la section Configuration du contenu de la correspondance. Auparavant, le UserID était mappé uniquement au champ Utilisateur source, mais le champ UserID est actuellement disponible en tant qu'attribut de recherche pour tous les événements Purview, y compris les événements de point de terminaison.

Configurer le contenu de correspondance pour l'incident

Fournissez la configuration pour stocker les informations sensibles sur le stockage cloud externe tel que le stockage Azure ou la catégorie AWS S3 afin de récupérer ce contenu lors d'un chargement tout en accédant à l'incident DLP IR.

Avant de commencer

Rôle requis : sn_dlir.admin(Créer, modifier et supprimer)

sn_dlir.analyst : vue (lecture seule)

Procédure

1. Dans la barre de progression, cliquez sur l'étape **Configuration du contenu correspondant** .
2. Remplissez les champs du formulaire.

Faire correspondre la configuration du contenu

Champ	Description
Stocker le contenu correspondant	Option permettant de stocker le contenu correspondant sur le stockage en nuage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Important : Si cette option n'est pas sélectionnée, le contenu de correspondance de politique pour les incidents DLP ne peut pas être vu dans l'espace de travail DLP. L'activation de cette option garantit que le contenu des correspondances renvoyé dans les incidents DLP est stocké dans le stockage cloud externe (par exemple, Azure, AWS). Vous pouvez également récupérer et afficher le contenu de la correspondance chaque fois qu'un incident DLP est ouvert dans l'espace de travail. Pour en savoir plus sur la configuration du stockage externe dans le cloud, reportez-vous à la section Installer et configurer l'intégration DLP de Microsoft.
Supprimer le contenu de la correspondance à la suppression de l'incident	Option permettant de supprimer le contenu de la correspondance d'incident du stockage cloud externe. Cette option n'est visible que lorsque le champ **Stocker le contenu correspondant** est sélectionné.
Informations d'identification externes dans le cloud	Le stockage cloud externe où le contenu de la correspondance est stocké. Vous pouvez vous référer aux informations d'identification externes dans le cloud ajoutées pour la configuration de stockage. Cette option n'est visible que lorsque le champ **Stocker le contenu correspondant** est sélectionné.

3. Cliquez sur **Continuer** et passez à la section Planification.

Planifier la récupération de l'incident DLP IR Microsoft

Définissez un calendrier pour récupérer les données d'incident et ingérer les Microsoft DLP IR incidents qui correspondent aux critères du profil. Configurez le calendrier pour définir comment et quand extraire des incidents de Microsoft.

Avant de commencer

Rôle requis : sn_dlir.admin(Créer, modifier et supprimer)

sn_dlir.analyst : vue (lecture seule)

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier la fréquence à laquelle vous interrogerez les incidents futurs qui correspondent à la configuration du profil d'incident. Pour activer l'ingestion automatisée d'incidents, vous devez configurer la planification et la récupération des incidents avant d'activer le profil. Le profil peut être configuré pour effectuer une récupération ponctuelle à l'aide de la case à cocher **Récupération ponctuelle** . La date historique peut aller jusqu'aux trois derniers mois à compter de la date actuelle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’intervalle d’interrogation est configuré individuellement pour chaque profil. Les différents intervalles d’interrogation peuvent avoir un impact sur les performances de l’intégration Microsoft DLP IR des incidents. Lors de la planification, prévoyez d’équilibrer la charge du système par rapport à l’urgence d’un incident.

Procédure

1. Définissez un calendrier pour récupérer les données et ingérer les incidents qui correspondent aux critères du profil.
2. Remplissez les champs du formulaire.

Calendrier du formulaire d’incident DLP

Champ	Description
Intégration de l'incident en cours	L’ingestion d’incidents en cours que l’instance extrait de Microsoft pour les nouveaux incidents. DLP IR Les incidents sont créés si des ServiceNow AI Platform incidents déclenchés sont trouvés et si les critères de filtrage de génération d’incidents correspondent.
Incrémentation du sondage (minutes)	Fréquence d’interrogation de Microsoft. Ce champ est automatiquement défini sur 300 minutes.
Définir le délai d'intégration de l'incident initial	Option permettant de définir une date et une heure pour l’ingestion initiale. Les ingestions suivantes sont basées sur la période de l’intervalle d’interrogation. Cette option n’est visible que lorsque le champ **Ingestion d’incident en cours** est sélectionné.
Délai d'intégration de l'incident initial d'entrée	Date et heure que vous spécifiez pour l’ingestion de l’incident. ○ Si la valeur est définie, la récupération des données auprès de Microsoft commencera à partir de la date ultérieure ajoutée. ○ Ce champ n’est visible que lorsque **l’option Définir le délai d’ingestion initial** est sélectionnée.
Délai d'intégration de l'incident initial	Première fois que les données sont ingérées. Vous pouvez voir que ces valeurs commencent à s’afficher lorsque le délai d’intégration de l’incident initial est défini.
Délai d'intégration de l'incident suivant (estimé)	Période suivante pour une ingestion d’incident estimée.
Récupération ponctuelle	Option permettant d’activer les extractions ponctuelles de données historiques. Si ce champ est sélectionné, les données historiques sont extraites de Microsoft DLP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	IR en fonction de la date ajoutée dans le champ **Date de début** .
Date de début	Date à partir de laquelle les données sont censées être récupérées à partir de Microsoft. Ce champ peut être défini sur un maximum de 7 jours.

3. Enregistrez la configuration de profil créée en cliquant sur **Terminer** dans la fenêtre contextuelle.
4. Activez le profil.
   a. Ouvrez le profil créé.
   b. Activez l'option **Actif** .
   c. Cliquez sur **Mettre à jour**.

Résultats
Une fois le profil créé et activé avec succès, les incidents sont récupérés périodiquement selon la configuration définie dans le profil et ajoutés à la table des incidents DLP.

Configurer les paramètres d'intégration Microsoft DLP IR

Modifiez les propriétés système par défaut de l'intégration Microsoft DLP IR .

Avant de commencer
Rôle requis : sn_dlir.admin

Procédure
1. Accédez à la **Intégration DLP de Microsoft** > **Paramètres**.
2. Modifiez les propriétés suivantes au besoin.

Paramètres de l'intégration DLP de Microsoft

Champ	Description
Délai d'expiration maximal pour les appels HTTP (sn_pp_dlp.maximum_http_time_out)	Délai d'expiration maximal pour les appels HTTP (en secondes). ○ Type : nombre entier ○ Valeur par défaut : 30
Niveau de génération de rapports des journaux générés par l'intégration (sn_pp_dlp.logging.verbosity)	Niveau des journaux de génération de rapports générés par l'intégration, c'est-à-dire le nom du type d'information. Vous pouvez également mettre à jour la valeur dans les options suivantes : ○ **erreur** ○ **avertir** ○ **info** ○ **debug** ○ **de**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par défaut, la valeur est **info**.
Destination de génération de rapports des journaux générés par l'intégration (sn_pp_dlp.logging.destination)	La destination des journaux générés par l'intégration. Vous pouvez également mettre à jour la valeur dans les options suivantes : ○ **Db** ○ **fichier** ○ **aucun** Par défaut, la valeur est **db**.

3. Cliquez sur **Enregistrer**.

Résultats

Vos paramètres d'intégration modifiés sont appliqués dans l'intervalle d'interrogation suivant, tel que défini dans le profil.

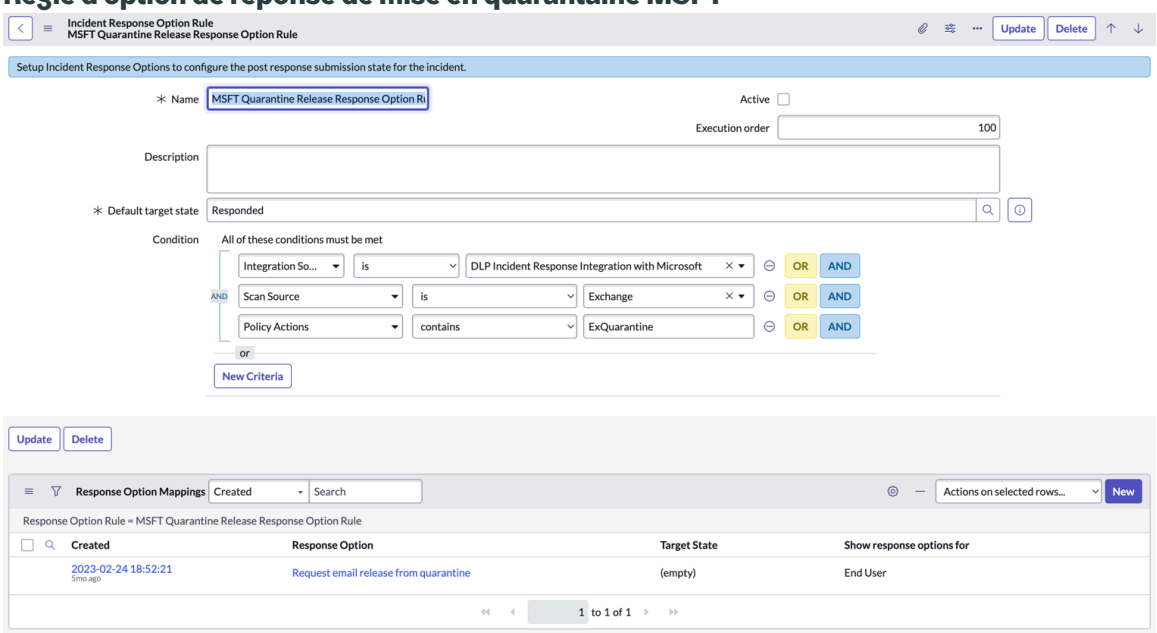
Demander un e-mail de libération de la quarantaine

Utilisez cette fonctionnalité pour libérer les e-mails mis en quarantaine à partir du portail de conformité Microsoft Purview.

Avant de commencer

Par défaut, le système de base propose l'option de réponse **Demander la libération de la quarantaine de l'e-mail** et la **règle d'option de réponse de libération de la quarantaine MSFT** pour libérer l'e-mail de la quarantaine. La **règle d'approbation de mise en quarantaine** est configurée dans cet enregistrement par défaut afin de tirer parti de la fonctionnalité d'approbation de cette action. Pour en savoir plus, consultez Créer des règles pour les options de réponse aux incidents, Configurer l'option de réponse pour vos incidents DLP et Créer des règles d'approbation.

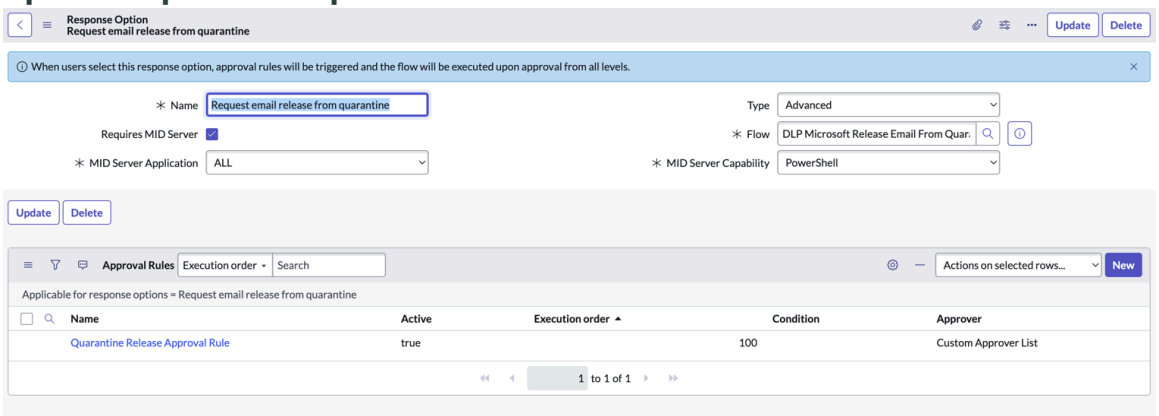
Règle d'option de réponse de mise en quarantaine MSFT



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option de réponse MSFT par défaut



Conditions préalables :

1. Le module Exchange Online PowerShell doit être installé sur le Serveur MID. Pour plus d'informations, voir Installer et gérer Exchange Online PowerShell .
2. Le serveur MID doit communiquer avec le serveur Exchange, qui est également un service cloud. Par conséquent, le serveur MID nécessite un accès Internet continu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si vous utilisez cette option de réponse, assurez-vous que le Serveur MID est opérationnel avec l'aptitude PowerShell. Si un serveur MID n'est pas opérationnel et ne dispose pas de l'aptitude PowerShell, l'utilisateur final ne pourra pas sélectionner l'action **Demander la libération de la quarantaine par e-mail** à partir de l'espace de travail des utilisateurs DLP. Pour plus d'informations, consultez Créer des règles pour les options de réponse aux incidents et Configurer l'option de réponse pour vos incidents DLP.

- Si vous voulez un serveur MID spécifique dans la liste, vous devez configurer l'application MID et la rendre visible dans la liste. Ensuite, au moins un serveur MID configuré doit être opérationnel à partir des applications MID sélectionnées et doit avoir l'aptitude Power Shell.
- Pour utiliser l'option Sortir de quarantaine, vous avez besoin d'autorisations d'API. Sur la page des autorisations d'API Microsoft, vérifiez **Office 365 Exchange Online** > **Exchange.ManageAsApp** est répertorié et contient les valeurs suivantes :
  - **Type** : **Application**.
  - **Consentement de l'administrateur requis** : **oui**.
  - **État** : la valeur incorrecte actuelle **n'est pas accordée pour <Organisation>** pour l'entrée **Office 365 Exchange Online** > **Exchange.ManageAsApp** et modifiez la valeur d'état. Pour en savoir plus sur les autorisations d'API, consultez Attribuer des autorisations d'API à l'application sur le site de documentation de Microsoft.

    Remarque : Cette étape est nécessaire pour se connecter à Exchange Online à l'aide du principe de service.

- Vous devez également avoir le rôle **d'administrateur de sécurité** dans le principe de service,
  - **Recherchez les rôles et les administrateurs Microsoft Entra ID** dans le portail Microsoft Azure, puis ajoutez une affectation à l'application enregistrée (Principe de service), puis suivez la procédure expliquée dans la documentation Microsoft sur la façon d'attribuer un rôle .
- Cette option ne s'applique qu'aux incidents Microsoft Exchange dont la vue de formulaire d'incident comporte l'option **Action de politiqueExQuarantine** .

Rôle requis : utilisateur final

La procédure suivante explique comment soumettre cette action à partir de l'espace de travail de l'utilisateur DLP.

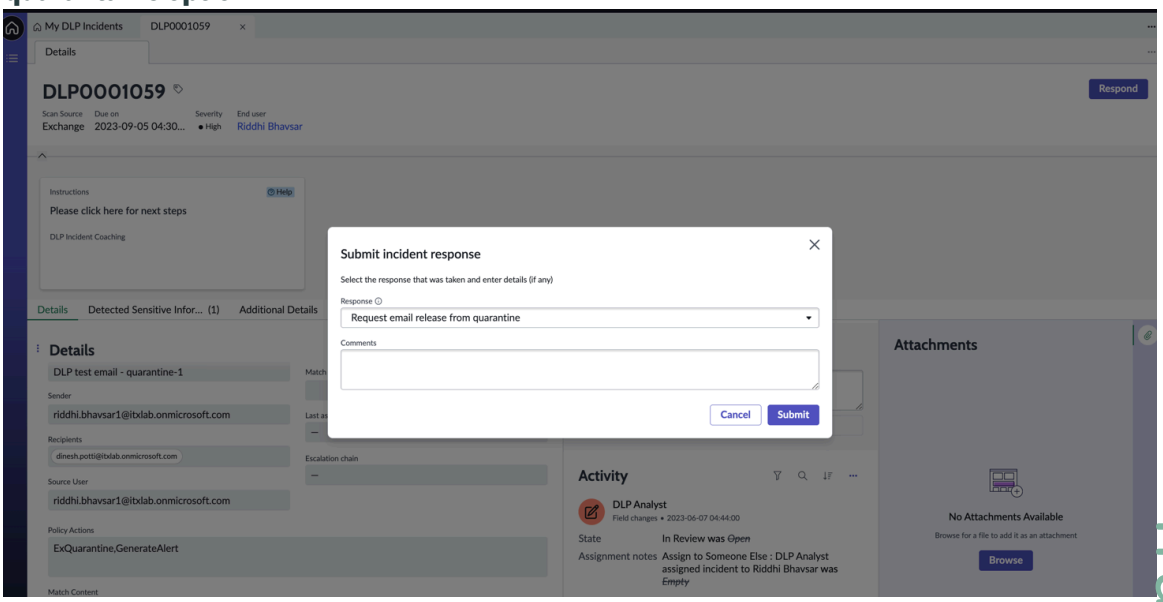
Procédure

1. Accédez à la **DLP** > **Espace de travail de l'utilisateur DLP**.
2. Ouvrez n'importe quel incident DLP Microsoft Exchange.
   Vérifiez que **l'action de politique** d'incident est définie sur ExQuarantine.
3. Cliquez sur **Répondre**.
4. Sélectionnez **l'option Demander le déblocage du courrier à partir de la quarantaine** dans la liste déroulante Réponse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Soumettre la réponse à un incident : demander un e-mail sortant de la quarantaine option



5. Cliquez sur **Envoyer**.

> **Remarque :** Lorsqu'une règle d'approbation est configurée pour cette action, le flux d'approbation est déclenché en premier et, après réception de toutes les approbations, le flux Demander la sortie de quarantaine de l'e-mail est déclenché et l'e-mail est sorti de la quarantaine. L'état de l'incident DLP est mis à jour sur **Sorti de quarantaine après la** mise en production.

Télécharger des fichiers pour les incidents DLP de type Exchange Online, OneDrive et SharePoint

Téléchargez des fichiers ou des e-mails qui enfreignent la politique DLP sur Microsoft Purview. Téléchargez ce fichier ou envoyez-le par e-mail à votre ordinateur local à partir de la DLP IR vue Incident. Vous pouvez télécharger les fichiers pour DLP IR les incidents de type Source d'analyse Exchange Online, OneDrive et SharePoint.

Avant de commencer

Rôle requis :

- sn_dlir.admin, sn_dlir.analyst
- Tout approbateur valide

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez un enregistrement d'incident DLP de type Analyser la source Exchange Online, OneDrive ou SharePoint qui est ingéré à partir de la source Microsoft.
3. Cliquez sur **Télécharger le fichier**.
   Le fichier ou l'e-mail qui a violé la stratégie DLP du côté de Microsoft Purview sera téléchargé sur l'ordinateur local de l'utilisateur.

> **Remarque :** L'administrateur DLP peut contrôler l'accès à l'action **Télécharger le fichier** en désactivant le paramètre **Faut-il autoriser le téléchargement du fichier de violation de l'incident signalé** à partir de la page Paramètres avancés. Pour plus d'informations, consultez Configurer les paramètres avancés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prévisualiser les fichiers de preuves pour les incidents DLP de type Exchange Online, OneDrive et SharePoint

Prévisualisez Data Loss Prevention Incident Response les fichiers de preuves dans l'espace de travail de l'analyste DLP IR.

Avant de commencer

Important : Lors de l'utilisation de l'action Fichiers de preuves dans l'espace de travail de l'analyste DLP, les fichiers de preuves sont temporairement stockés dans la base de données ServiceNow dans un format non chiffré. Si vous ne souhaitez pas stocker les fichiers de preuves, désactivez la fonctionnalité d'aperçu des fichiers de preuves. Pour plus d'informations, consultez Configurer les paramètres avancés.

Rôle requis : sn_dlir.analyst

Procédure

1. Accédez à la **Tous** > **Gestion des incidents DLP** > **Espace de travail de l'analyste DLP**.
2. Ouvrez un enregistrement d'incident DLP.
3. Dans la barre latérale contextuelle, sélectionnez l'icône Fichiers de preuves ( ).
4. Dans l'onglet **Fichiers de preuves** , sélectionnez la carte **Fichier de preuves** pour afficher un aperçu des fichiers de preuves dans la visionneuse de documents.

   La fonctionnalité d'aperçu est différente pour chaque type de fichier, comme indiqué dans le tableau suivant.

Format de fichier	Extension de fichier
Image	.bmp, .gif, .ico, .jpeg, .jpg, .png, .svg et .webp. Les fichiers image s'ouvrent en mode visionneuse de documents.
Microsoft Fichiers Office	.doc, .docx, .ppt, .pptx, .xls et .xlsx Les fichiers Office s'ouvrent en mode visionneuse de documents.
Fichiers texte	.txt Les fichiers texte s'ouvrent en mode éditeur de texte.
Fichiers courrier	.Eml **Remarque :** La taille du fichier doit être inférieure à 5 Mo. Vous devez d'abord télécharger le fichier pour prévisualiser son contenu.
Fichiers PDF	.PDF ○ Saisissez un mot clé pour rechercher le document. ○ Fonctions de zoom avant et arrière pour ajuster la vue et améliorer la lisibilité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Format de fichier	Extension de fichier
	○ Faites pivoter la page dans le sens des aiguilles d'une montre ou dans le sens inverse des aiguilles d'une montre pour afficher le contenu plus clairement.

Remarque :

Les fichiers binaires ne seront pas rendus et devront être téléchargés pour prévisualiser leur contenu. La fonctionnalité d'aperçu du fichier de preuve fonctionne également pour les incidents archivés.

Séparation de domaine dans l'intégration Microsoft DLP

Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez ensuite contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge

Prise en charge : Basique.

Comment fonctionne Séparation de domaine avec Microsoft l'intégration DLP

Pour procéder à la séparation en domaines, procédez comme suit :

- Créez un utilisateur avec le rôle requis dans le domaine respectif.
- Effectuez les procédures d'intégration Microsoft DLP dans le domaine approprié.

Opérations de sécurité Fonctionnalité commune

Chaque fois que l'un des modules d'extension des applications principales Opérations de sécurité (Réponse aux incidents de sécurité, Réponse aux vulnérabilités, Renseignements sur les menaces ou Configuration Compliance) est activé, le module d'extension Security Support Common est activé. Ce module d'extension charge divers modules qui fournissent des fonctionnalités communes à toutes les Opérations de sécurité applications.

Remarque : Seuls les utilisateurs disposant du module [sn_sec_cmn.admin] peuvent afficher et utiliser le Opérations de sécurité module. Ce rôle est hérité lorsqu'un rôle administratif vous est affecté dans l'une Opérations de sécurité des applications.

Security Operations Modules

Fonctionnalité	Description
Référence de Security Operations Integrations, Intégrations de Renseignements sur les menaces, Intégrations de Réponse aux vulnérabilités	Plusieurs intégrations sont incluses dans les Opérations de sécurité applications (Réponse aux incidents de sécurité, Renseignements sur les menaces, et Réponse aux vulnérabilités). Cette section fournit des instructions pour activer les modules d'extension et configurer les intégrations ServiceNow tierces. Vous y trouverez également des instructions de base pour développer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalité	Description
	vos propres intégrations, ainsi que des détails sur des intégrations spécifiques incluses dans le système de base.
Opérations de sécurité Traitement des e-mails	Vous pouvez configurer l'intégration des informations provenant de systèmes de détection externes, fournir une granularité dans le traitement des enregistrements d'opérations de sécurité, traiter les e-mails sans correspondance et empêcher la duplication des enregistrements à l'aide Traitement des e-mailsde .
Groupes	• **Groupes de filtres** Créez et utilisez des groupes de filtres pour localiser les enregistrements à partir de n'importe quelle table de votre instance. Par exemple, vous pouvez créer un groupe de tous les ordinateurs du même fabricant. Vous pouvez également filtrer les éléments de configuration (CI) qui présentent des vulnérabilités similaires ou qui se trouvent dans une plage d'adresses IP de sous-réseau particulière. • **Escalades** Vous pouvez créer un chemin d'escalade des incidents de sécurité pour les problèmes nécessitant plus d'attention ou d'expertise. Lorsqu'un groupe d'escalade existe, un bouton apparaît sur tous les incidents de sécurité de ce groupe.
Balises de sécurité	**Balises** : les règles de balise de sécurité fournissent un filtrage pour l'accès aux balises de sécurité.
Workflows	• **Voir les workflows de sécurité** Vous pouvez afficher les nombreux workflows inclus dans les applications Security Operations. Vous pouvez créer des workflows à partir de modèles et dans l'éditeur de workflow. • **Déclencheurs de workflow** Opérations de sécurité Les déclencheurs de workflow contiennent une condition dans une table. Tous les workflows joints à l'enregistrement de déclencheur de workflow s'exécutent lorsque la condition est remplie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalité	Description
Utilités	• **Mappage des données d'enrichissement** Mappage des données d'enrichissement Transforme les données de XML, JSON ou Propriétés de fichiers en ServiceNow enregistrements. Opérations de sécurité Les workflows utilisent des cartes de données d'enrichissement et fournissent des données de sortie aux incidents de sécurité. • **Transformations de valeurs de champs** Transforme les valeurs de champ client uniques en valeurs de champ reconnues par Opérations de sécurité l'analyse des e-mails, l'enrichissement des données ou les tables à l'aide de cartes de champs. Prend en charge les champs de choix, les références et aligne les données externes sur la terminologie et le format standard de votre nouvel enregistrement. • **Mappage de champs** Opérations de sécurité Les tables peuvent être mappées vers et à partir d'autres tables, liant un incident de sécurité à un ticket du service clientèle ou un problème à d'autres parties du Opérations de sécurité système. Par exemple, vous pouvez intégrer un module d'extension à une Réponse aux incidents de sécurité tâche. • **Orchestration sur demande** Au cours Réponse aux incidents de sécurité de l'analyse, un analyste de sécurité peut vouloir effectuer une tâche qui est pilotée par un workflow d'incident de sécurité. Par exemple, exécutez un vidage de processus sur un CI particulier. Cela peut être accompli avec l'orchestration à la demande. • **Groupes de systèmes d'exploitation** N/A. • **Registre des applications SecOps** N/A.
CMDB	**Règles d'identificateur de CI** : les identificateurs de CI sont des règles utilisées pour rechercher un élément de configuration (CI) dans la CMDB qui contient des informations correspondantes à partir d'une intégration tierce. Ces règles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalité	Description
	définissent les champs qui contiennent des données correspondantes et l'ordre de priorité de leur évaluation. La valeur **de commande** la plus basse est évaluée en premier.

Créer et définir des groupes de filtres dans Security Operations

Créez et utilisez des groupes de filtres pour localiser les enregistrements à partir de n'importe quelle table de votre instance. Par exemple, vous pouvez créer un groupe de tous les ordinateurs du même fabricant. Vous pouvez également filtrer les éléments de configuration (CI) qui présentent des vulnérabilités similaires ou qui se trouvent dans une plage d'adresses IP de sous-réseau particulière.

Avant de commencer

Rôle requis : sn_sec_cmn.write

Pourquoi et quand exécuter cette tâche

Les groupes de filtres peuvent contenir des enregistrements mis à jour dynamiquement, une série d'enregistrements statiques qui ne sont pas filtrés à l'aide de conditions, ou une combinaison d'enregistrements statiques et mis à jour dynamiquement. Certains groupes de filtres sont inclus dans le système de base, par exemple, les exclusions de CI.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Groupes** > **Groupes de filtres**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Le nom du groupe de filtres.
Actif	Case pour activer le groupe.
Description	Description du groupe de filtres.
Adresses IP de réseau	Adresse IP de réseau qui contient les adresses IP des CI que vous souhaitez ajouter au groupe. Ce champ s'affiche uniquement si vous avez sélectionné Élément de configuration [cmdb_ci] ou une table qui étend l'élément de configuration dans le champ **Table** .
Masque de sous-réseau	Sous-réseau qui contient les adresses IP des CI que vous souhaitez ajouter au groupe, par exemple, 255.255.255.0. Ce champ s'affiche uniquement si vous avez sélectionné Élément de configuration [cmdb_ci] ou une table qui étend l'élément de configuration dans le champ **Table** .
Table	La table à filtrer.
Condition	Utilisez le générateur de conditions pour définir les critères à filtrer.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un onglet **Conditions avancées** s'affiche.

D'autres onglets s'affichent en fonction du type de table que vous avez spécifié dans le champ **Table** , comme suit :

Table	Onglets affichés
Élément de configuration [cmdb_ci] ou table qui étend la table d'éléments de configuration	**CI ajoutés manuellement** et **CI correspondants**
Tâche [task] ou table qui étend la table de tâches	**Tâches ajoutées manuellement** et **tâches correspondantes**
Une table non associée à un CI ou à une tâche	**Enregistrement ajouté manuellement**

5. Pour définir plus de conditions pour votre groupe de filtres :
   a. Cliquez sur **Conditions avancées**.
   b. Insérez une nouvelle ligne dans la liste incorporée Conditions de **groupes de filtres supplémentaires** pour sélectionner d'autres groupes de filtres prédéfinis que vous souhaitez combiner avec le groupe de filtres en cours de mise à jour.
   Si vous souhaitez que le groupe de filtres sélectionné filtre les enregistrements en fonction d'un champ de référence, un champ mappé est automatiquement sélectionné lorsque l'enregistrement actuel est enregistré.

   Remarque : La valeur du **champ Mappé** ne peut pas être modifiée à partir de la liste incorporée **Conditions du groupe de filtres supplémentaires** . Pour modifier le champ, cliquez sur l'icône ⓘ ouvrir l'enregistrement.

   c. Cliquez sur **Mettre à jour**.
6. Pour ajouter manuellement d'autres CI ou tâches au groupe de filtres :
   a. Cliquez sur l'onglet **CI ajoutés manuellement** ou **Tâches ajoutées manuellement** .
   b. Cliquez sur **Modifier**.
   c. Sélectionnez les CI ou les tâches que vous souhaitez ajouter.
   d. Cliquez sur **Enregistrer**.
7. Pour afficher les CI ou les tâches qui correspondent à vos critères de sélection :
   a. Cliquez sur l'onglet **Correspondance des CI** ou **Mise en correspondance des tâches** .
   b. Si vous avez modifié les critères, actualisez la liste en cliquant avec le bouton droit dans l'en-tête du formulaire et en sélectionnant **Actualiser la liste**.

Transformation des données partagées

Les modules d'extension Réponse aux incidents de sécurité, Réponse aux vulnérabilités, et Renseignements sur les menaces partagent des caractéristiques communes pour les données de relation et les règles de duplication, utilisées pour importer des informations externes et internes dans Opérations de sécurité.

Analyse des e-mails, Règles de duplicationet Mappage de champs prenez des données d'entrée (un e-mail, un fichier JSON ou XML, ou un enregistrement) et transformez-les au format

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

approprié pour créer un nouvel enregistrement. Chacune de ces fonctionnalités extrait les données à sa manière, mais celles-ci sont transformées en nouvel enregistrement à l'aide de plusieurs des mêmes processus.

Données de relation

Lorsque vous ajoutez des informations à une liste connexe (par exemple, un observable associé dans un incident de sécurité), vous pouvez créer un enregistrement de relation composé d'une table m2m. Parfois, il existe des données supplémentaires sur cet enregistrement de relation à définir. Par exemple, un observable étant une adresse IP source (par opposition à une adresse IP de destination). Ces informations se trouvent dans le champ **Données de relation** du formulaire **Transformation de champ** utilisé par **l'analyse des e-mails** ou dans une liste connexe **Champs de mappage de champs** du formulaire **Mappage de champs** .

Le champ **Données de relation** est généralement vide. Il est le plus souvent utilisé pour les adresses IP sur les observables dans **l'analyse des e-mails**.

Vous pouvez transformer les données de n'importe quel ServiceNow enregistrement en n'importe quel autre ServiceNow enregistrement à l'aide des **champs de mappage de champs** de la fonctionnalité **Mappage de champs** . Par exemple, pour transformer les données d'un incident en incident de sécurité, ou d'un incident de sécurité en PRB.

Règles de duplication Security Operations

Utilisez cette fonction Règles de duplication pour gérer les enregistrements en double pour la sécurité, la vulnérabilité, les IoC, et ainsi de suite.

Les règles de duplication ont deux objectifs. Elles empêchent la création d'un trop grand nombre d'enregistrements en double et, lorsqu'un doublon est détecté, elles spécifient les champs de l'enregistrement à mettre à jour. Seuls les doublons actifs sont recherchés. Si l'enregistrement n'est pas actif, par exemple, si l'incident est fermé, tout nouveau problème identique devient un nouvel incident.

Les règles de duplication sont utilisées par **l'analyse des e-mails**, le **mappage de champs** et **le mappage d'enrichissement des données**.

Information associée

Créer des analyseurs d'e-mails dans Security Operations

Mapper les tables aux tables avec le mappage de champs Security Operations

Créer des règles de duplication dans Opérations de sécurité

Vous pouvez les utiliser Règles de duplication pour identifier les nouveaux e-mails, les données d'enrichissement ou les cartes de champs contenant des enregistrements en double actifs et les traiter de manière appropriée.

Avant de commencer

Rôle requis : sn_sec_cmn.write

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Règles de duplication**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire, selon vos besoins :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règle de duplication

Champ	Description
Nom	Nom de la règle de duplication.
Table	Table où les enregistrements sont créés et utilisés pour déterminer les doublons.
Identification des champs	Sélectionnez un ensemble de champs qui indiquent un incident de sécurité, un observable, une vulnérabilité, etc., lorsque les valeurs de ces champs sont identiques.
Action relative à la duplication	Régit la façon de gérer les e-mails en double. Les choix possibles sont les suivants : **Créer en tant qu'enfant** Crée un enregistrement en tant qu'enfant de l'original. Le champ liant l'enfant au parent est le champ **Parent**. **Ne pas créer ni mettre à jour des enregistrements** (par défaut) Ne fait rien. Ignore les doublons. **Mettre à jour l'enregistrement en double** Met à jour les champs dans l'enregistrement existant tel que spécifié dans **Actions de duplication.** **Remarque :** Si vous choisissez **Mettre à jour l'enregistrement en double**, la liste connexe **Actions de duplication** s'affiche.
Actif	Cochez cette case pour activer la règle.
Description	Décrit le but et l'application de cette règle de duplication ; quand il doit être utilisé, par exemple une règle conçue pour les observables basés sur IP ou les incidents de sécurité du pare-feu.

4. Cliquez avec le bouton droit dans l'en-tête de l'enregistrement et sélectionnez **Enregistrer** ou cliquez sur **Mettre à jour**.
5. Pour définir des actions de duplication, si vous avez choisi **Mettre à jour l'enregistrement en double**, cliquez sur **Nouveau** pour créer des actions de duplication pour chaque champ que vous souhaitez mettre à jour dans l'incident.
6. Remplissez ou modifiez les champs du formulaire pour décrire la façon de mettre à jour le champ :

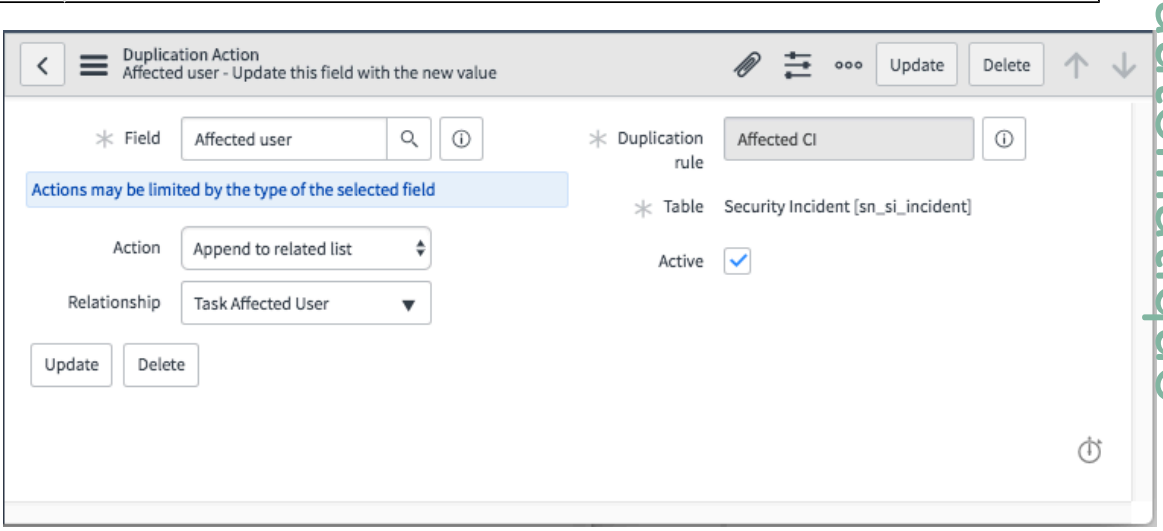
Actions de duplication

Champ	Description
Champ	Le nom du champ à utiliser pour l'action de duplication.
Action	Les actions prises en charge varient selon le type de champ. Les choix possibles sont les suivants : **Mettre à jour ce champ avec la nouvelle valeur** Remplace la valeur précédente dans l'enregistrement existant par cette valeur. **Ajouter la nouvelle valeur à une liste séparée par des virgules, si elle est unique** Traite la valeur comme une entrée dans une liste séparée par des virgules et ajoute les nouvelles données (le cas échéant) comme nouvelle entrée dans cette

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

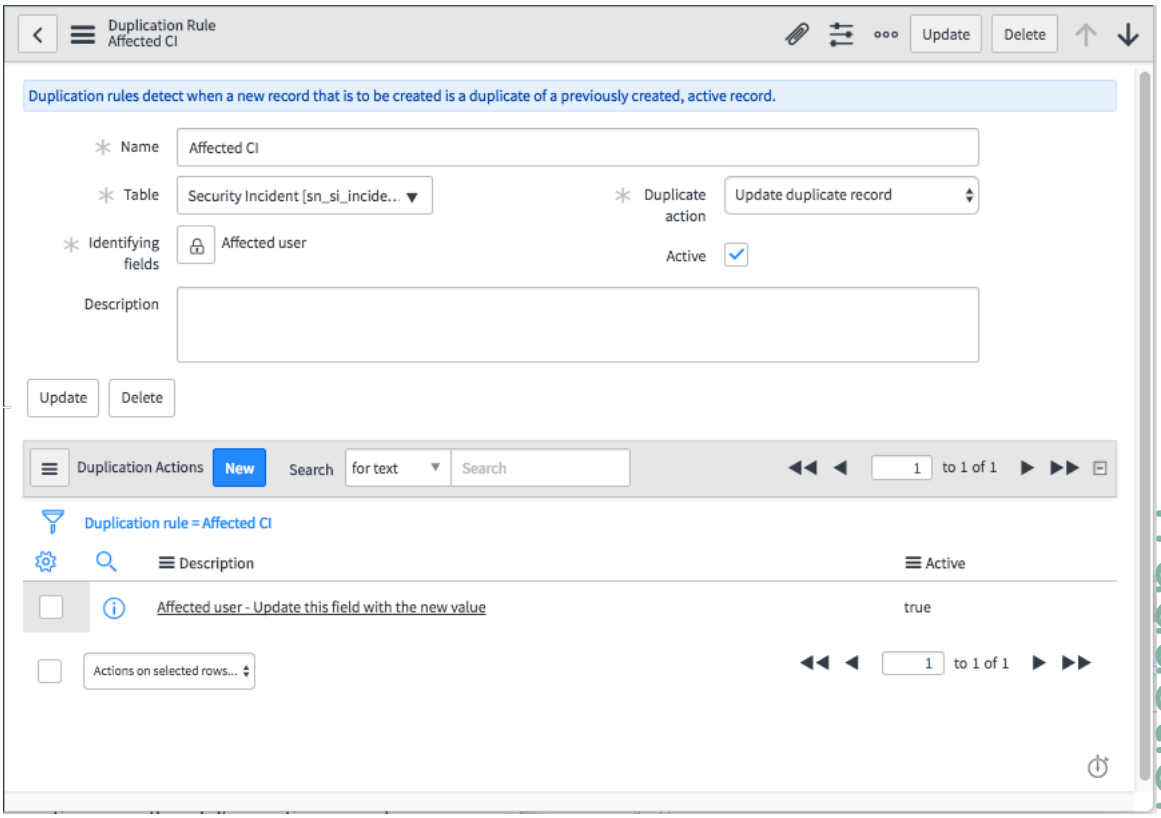
Champ	Description
	liste. Si les données figurent déjà dans la liste, elles ne sont pas ajoutées deux fois. **Ajouter la nouvelle valeur à ce champ** Ajoute la nouvelle valeur à la fin du texte existant dans le champ. **Ajouter un à un champ de compteur** Ajoute un au champ numérique. **Définir le champ à la date d'aujourd'hui** Définit le champ à la date et à l'heure actuelles. **Ajouter à la liste connexe** Ajoute l'enregistrement connexe avec cette valeur à la liste connexe de l'enregistrement actuel. Apparaît lorsqu'il existe une table de plusieurs à plusieurs, avec une colonne du même type, liée à la table en cours de mise à jour. Par exemple, **CI affecté** ou **Utilisateur affecté**.
Relation	[Facultatif] Ce champ s'affiche uniquement lorsque l'action **Ajouter à la liste connexe** est choisie. Il s'agit du nom de la liste connexe que vous souhaitez associer à cette règle.
Règle de duplication	Règle à laquelle cette action fait partie.
Table	Table où les enregistrements sont créés. S'affiche à titre d'information uniquement.
Actif	Cochez cette case pour activer l'action.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Envoyer**.



Opérations de sécurité Traitement des e-mails

Vous pouvez configurer l'intégration des informations provenant de systèmes de détection externes, fournir une granularité dans le traitement des enregistrements d'opérations de sécurité, traiter les e-mails sans correspondance et empêcher la duplication des enregistrements à l'aide Traitement des e-mailsde .

Traitement des e-mails Se compose de ces fonctionnalités :

Fonctionnalité	Description
Analyse des e-mails	Générez de nouveaux Opérations de sécurité enregistrements à partir d'e-mails système externes.
Règles de duplication	Identifie les nouveaux e-mails contenant des incidents connus et les traite de manière appropriée.
Propriétés	Spécifie les comptes utilisés comme entrée pour Analyse des e-mails la sécurité, la vulnérabilité et les IoC. Assure la granularité dans le traitement des Opérations de sécurité enregistrements.
E-mails sans correspondances	Répertorie les e-mails qui ne correspondent à aucun Opérations de sécurité enregistrement.

Propriétés d'e-mail Opérations de sécurité

L'e-mail Propriétés spécifie les boîtes de réception utilisées comme entrée pour Analyse des e-mails importer des informations à partir de systèmes de détection externes afin de créer des enregistrements pour la sécurité, la vulnérabilité et les IoC. Vous pouvez configurer un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

compte général pour tous les systèmes de détection externes à utiliser, ou des comptes de messagerie individuels pour Réponse aux incidents de sécurité, Renseignements sur les menaces ou Réponse aux vulnérabilités.

Créer des Opérations de sécurité propriétés d'e-mail

Vous pouvez spécifier des adresses e-mail pour les rapports et contrôler le comportement automatique des e-mails à l'aide de l'e-mail Propriétés.

Avant de commencer

Rôle requis : sn_sec_cmn.admin

Configurez des outils de détection externes pour envoyer des e-mails dans votre boîte de réception d'analyse des e-mails.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Traitement des e-mails** > **Propriétés**.
2. Saisissez vos boîtes aux lettres des destinataires comme il convient :
   Il s'agit d'adresses e-mail entrantes à traiter par **analyse des e-mails**, plutôt que par **actions entrantes**.

Propriétés d'analyse des e-mails

Champ	Description
Boîte de réception des Opérations de sécurité outils	Adresse e-mail complète pour Opérations de sécurité. Par exemple, secops_support@yourcompany.com.
Boîte de réception des outils des incidents de sécurité	Adresse e-mail complète pour Réponse aux incidents de sécurité. Par exemple, sir_support@your.company.com.
Boîte de réception des Réponse aux vulnérabilités outils	Adresse e-mail complète pour Réponse aux vulnérabilités. Par exemple, vuln_resp@yourcompany.com.
Boîte de réception des Renseignements sur les menaces outils	Adresse e-mail complète pour Renseignements sur les menaces. Par exemple, threat_intel@yourcompany.com.

3. Cliquez sur **Enregistrer**.

Opérations de sécurité Analyse des e-mails

Générez de nouveaux Opérations de sécurité enregistrements à partir de systèmes de détection externes à l'aide de Analyse des e-mails. Cette fonctionnalité fournit une méthode pour intégrer des informations provenant d'outils externes tels que la détection de programmes malveillants, la détection de vulnérabilité, les pare-feu, la connaissance des menaces, et autres.

Façon dont les e-mails sont analysés

Tout système capable d'envoyer un e-mail peut créer Opérations de sécurité des enregistrements, par exemple, incidents de sécurité, demandes, éléments vulnérables, vulnérabilités, observables d'incident de sécurité, méthodes d'attaque, etc.

Tous les Opérations de sécurité modules d'extension (Réponse aux incidents de sécurité, Renseignements sur les menaces, et Réponse aux vulnérabilités) ont une propriété (**email_to**) qui définit l'adresse e-mail à laquelle les intégrations externes doivent envoyer des e-mails, afin qu'ils soient analysés par les analyseurs d'e-mails. Reportez-vous à **Traitement des e-mails** > **Propriétés** pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'e-mail envoyé à l'une Opérations de sécurité des adresses e-mail est stocké dans une table d'événements d'e-mail. Ces e-mails sont traités pour déterminer s'ils correspondent à un analyseur d'e-mail.

Les e-mails qui ont une correspondance sont marqués et les règles de transformation et de duplication créent ou mettent à jour un Opérations de sécurité enregistrement. L'e-mail est lié à cet enregistrement et marqué comme correspondant.

Les e-mails qui ne correspondent pas sont répertoriés en E-mails sans correspondances tant qu'enregistrement Opérations de sécurité . Ils peuvent être examinés pour aider à créer des analyseurs d'e-mails pour traiter ces e-mails. Une action de retraitement vous permet d'exécuter à nouveau l'e-mail sans correspondance dans les analyseurs. Le journal d'e-mails d'origine est lié à cet enregistrement.

Les règles de duplication de la transformation d'e-mail permettent de gérer plusieurs e-mails relatifs au même problème. Ces règles définissent ce qui constitue un enregistrement en double et peuvent empêcher la création d'enregistrements en double. Lorsqu'un doublon est détecté, la règle spécifie l'action à entreprendre : aucune action (ne pas créer de nouvel enregistrement), créer le nouvel enregistrement en tant qu'enregistrement enfant de l'enregistrement existant ou mettre à jour l'enregistrement existant. Lors de la mise à jour de la règle de duplication, spécifie les champs de l'enregistrement existant qui sont mis à jour.

Remarque : Un Opérations de sécurité analyseur d'e-mails fonctionne conjointement avec les actions entrantes de la plateforme et ne les remplace pas. Il ne prend pas en charge la définition de valeurs sur les champs indirects, par exemple, **sys_journal_field** entrées.

Par défaut, les événements par e-mail sont supprimés au bout de 30 jours.

Enregistrements multiples

Les systèmes de détection externes (détecteurs de logiciels malveillants, vulnérabilités, etc.) peuvent envoyer des e-mails qui signalent plusieurs éléments à la fois. L'analyseur d'e-mails prend en charge les séparateurs dans l'e-mail.

Par exemple, un détecteur de logiciels malveillants peut vous envoyer un rapport par e-mail sur tous les systèmes de votre réseau infectés par un logiciel malveillant particulier avec des informations sur le logiciel malveillant en premier, suivi d'une liste des systèmes touchés.

Exemple d'e-mail malveillant

```
Subject: EvilChocolateBunny detected on multiple systems
Malware Hash: 20380285098260923490723
Malware Name: Evil Chocolate Bunny
Type: Keylogger
==========
System: WIN-GHARRISON
IP: 123.45.67.888
Status: File present, not infected
==========
System: WIN-ATUTER
IP: 123.45.67.889
Status: Infected
==========
System: WIN-BANGLIN
IP: 123.45.67.899
Status: File present, not infected
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dans cet exemple, lorsque le **séparateur d'enregistrements** est défini dans votre **transformation d'e-mail**comme **==========**, il divise l'e-mail en quatre sections qui sont évaluées séparément. Cela crée un incident de sécurité pour chacun des trois systèmes affectés.

Remarque : La section d'en-tête est détectée, mais aucun système n'est affecté. Elle est donc utilisée dans les trois enregistrements et ne crée pas de quatrième enregistrement.

Les transformations de champ extraient les données de chaque section. Si quelque chose dans l'en-tête ou le pied de page de l'e-mail s'applique à tous les enregistrements, tels que Hachage de programme malveillant, Nom du programme malveillant et Type dans cet exemple, la transformation de champ pour eux doit définir la **valeur Rechercher sur** une valeur qui effectue une recherche dans le corps de l'e-mail soit **Au début d'une ligne dans le corps de l'e-mail** , soit **N'importe où dans le corps de l'e-mail**.

Les transformations de champdoivent être définies sur rechercher **Au début d'une ligne dans la section des enregistrements** ou sur **Sec** pour les données définies dans chaque section, telles que Système, Adresse IP ou État. Les options de section d'enregistrement ne sont disponibles que lorsqu'un séparateur d'enregistrement est défini dans la transformation d'e-mail.

Lors de l'analyse d'un e-mail avec un séparateur défini, les enregistrements ne sont créés que pour les sections comportant au moins une donnée spécifique à la section.

Dans cet exemple, trois enregistrements sont créés, même si quatre sections sont définies. La première section est un en-tête, et il lui manque quelque chose de spécifique à un seul système. Si l'un des champs de la première section était rempli (Système, Adresse IP ou État), un enregistrement serait également créé pour cette section.

Information associée

Créer des analyseurs d'e-mails dans Security Operations

Opérations de sécurité Mappage des données d'enrichissement

Opérations de sécurité Mappage de champs

Créer des analyseurs d'e-mails dans Security Operations

Analyse des e-mails Crée des Opérations de sécurité enregistrements à partir de votre e-mail pour la sécurité, la vulnérabilité et les observables afin d'accélérer la réponse aux menaces et la correction.

Avant de commencer

- Configurez des outils de détection externes pour envoyer des e-mails à une adresse e-mail centrale.
- Définissez l'adresse e-mail dans les propriétés de Security Operations. Pour plus d'informations, consultez Créer des Opérations de sécurité propriétés d'e-mail.
- Affectez un compte d'utilisateur à cette adresse e-mail et donnez à cet utilisateur des contrôles d'accès de sécurité pour créer et mettre à jour les enregistrements d'événements d'e-mail.
- Ayez une copie de l'e-mail concerné de votre outil de détection externe devant vous.
- Décidez du type d'enregistrement que vous souhaitez créer, un incident de sécurité, un enregistrement de vulnérabilité, une tâche, etc. Ce choix détermine la table que vous sélectionnez.

Rôle requis : sn_sec_cmn.admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Analyse des e-mails**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

> **Remarque :** Si plusieurs champs sont spécifiés, tous les champs doivent correspondre à l'e-mail pour créer un enregistrement.

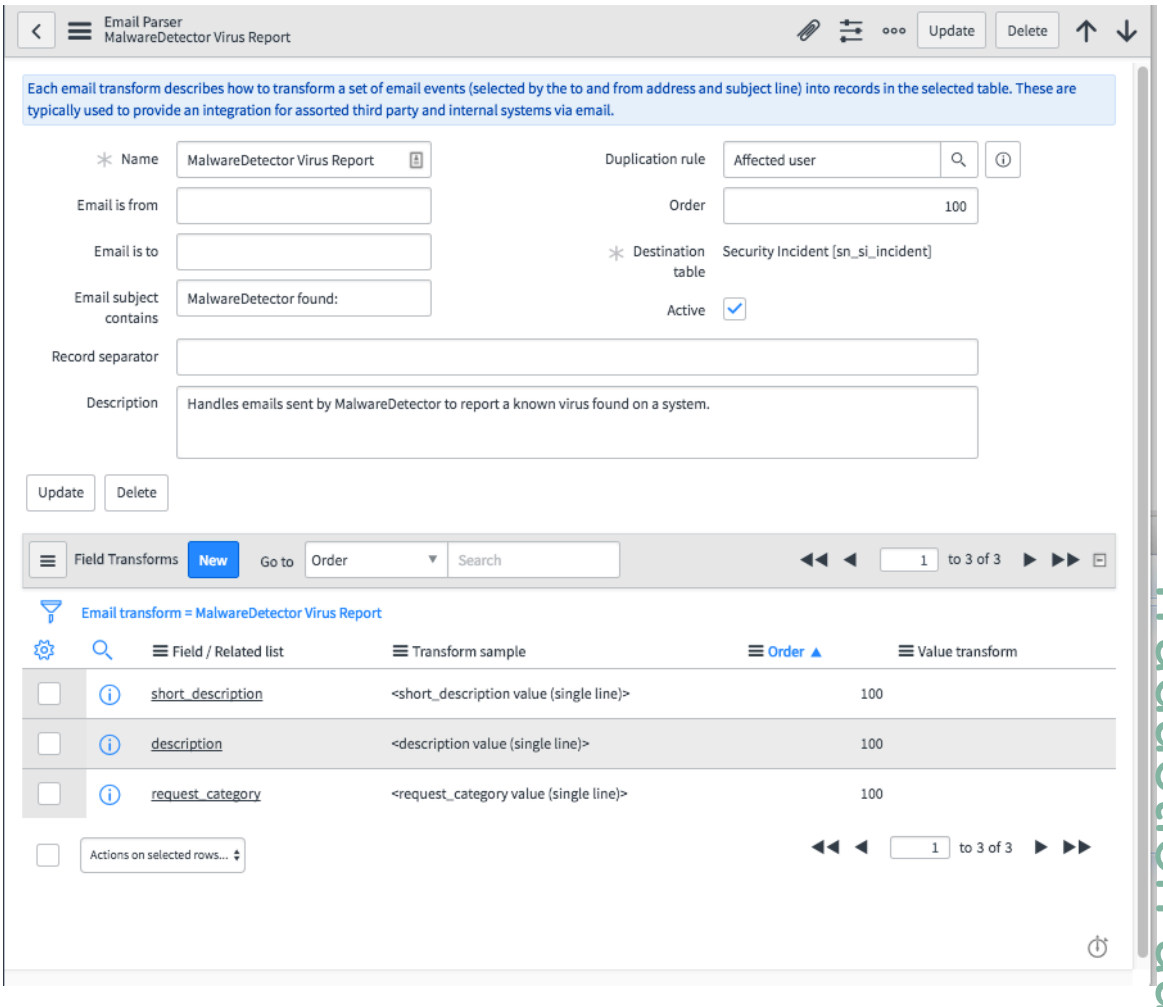
Analyseur d'e-mails

Champ	Description
Nom	Le nom de l'analyseur d'e-mails.
L'e-mail provient de	S'ils sont remplis, seuls les e-mails de cette adresse sont transformés par cet analyseur d'e-mails.
L'e-mail est destiné à	S'ils sont remplis, seuls les e-mails de cette adresse sont transformés par cet analyseur d'e-mails.
L'objet de l'e-mail contient	S'ils sont remplis, seuls les e-mails dont l'objet contient cette phrase sont transformés par cet analyseur d'e-mails.
Règle de duplication	Régit la façon de gérer les e-mails en double pour tout e-mail traité par cette transformation. Pour plus d'informations, consultez Transformation des données partagées.
Ordre	Dans quel ordre considérer les transformations. La première transformation d'e-mail correspondante est utilisée. En règle générale, vous souhaitez configurer les analyseurs d'e-mails les plus spécifiques dans les numéros inférieurs, avec un certain secours. Attribuez des numéros de **commande** plus élevés aux analyseurs d'e-mails fourre-tout afin qu'ils s'exécutent si rien d'autre ne correspond. La valeur par défaut est 100. Lorsque tout correspond, l'analyseur d'e-mails le plus spécifique (**correspondances de**, **à** et **objet**) est utilisé.
Table de destination	Table dans laquelle vous souhaitez créer des enregistrements.
Actif	Indique si cette transformation est active, en cours d'utilisation ou inactive. Si cette option n'est pas cochée, aucun e-mail n'est transformé avec ce code.
Séparateur d'enregistrements	Lorsque les e-mails traités par cet analyseur d'e-mail créent plusieurs enregistrements, ce champ contient le séparateur entre les informations de ces enregistrements. Consultez Opérations de sécurité Analyse des e-mails pour plus d'informations.
Description	Description de cet analyseur d'e-mails, outil avec lequel il fonctionne, objectif, etc.

4. Lorsque vous avez terminé vos entrées, faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
   Un onglet **Transformations de champ** s'affiche. Cet onglet montre comment les champs individuels de la table de destination sont définis en fonction du contenu de l'e-mail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Pour ajouter **des transformations de champ**, effectuez les étapes suivantes.
   a. Dans l'onglet **Transformations de champ** , cliquez sur **Nouveau**.
   b. Renseignez les champs du formulaire comme il convient.

Option	Description
Champ	**Description**
Stocker la valeur dans un champ ou une liste connexe	Sélectionnez où trouver la valeur. Les choix sont les suivants : ○ Stocker la valeur dans un champ du nouvel enregistrement ○ Lier à cette valeur dans une liste connexe ○ Lier à cette valeur, ce qui crée un nouvel enregistrement si un enregistrement correspondant n'existe pas **Remarque :** Si la table de destination ne possède pas de listes connexes, ce champ ne s'affiche pas.
Champ	Sélectionnez le champ pour compléter cette valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Pour les champs de choix, les correspondances sont effectuées avec les choix existants à l'aide de l'étiquette ou de la valeur de choix sous-jacente. Si aucune correspondance n'est trouvée, le champ est défini, mais aucune nouvelle entrée n'est ajoutée à la liste de choix. Pour plus d'informations, consultez Listes de choix . Pour les champs de référence, une entrée n'est définie que lorsqu'une valeur correspondant au nom d'affichage de l'enregistrement ou à un sys_id valide est trouvée. Pour plus d'informations, consultez Champs de référence .
Liste connexe	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou Lier à cette valeur, ce champ spécifie la liste connexe à laquelle ajouter des informations, si **un enregistrement correspondant n'existe pas**.
Champ de valeur	Lorsque **l'option Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier à cette valeur,** ce champ spécifie le champ dans la table affichée dans la liste connexe. Il est utilisé pour rechercher et trouver un enregistrement existant. Par exemple, si votre liste connexe est **constituée de CI affectés**, ce champ **peut contenir** Nom ou **Nom de domaine complet**, ou tout autre champ dans l'enregistrement de CI à utiliser pour rechercher le CI ajouté à la liste **des CI affectés** .
Données de relation	Lorsque **l'option Stocker la valeur dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe**, un enregistrement est créé pour lier cet enregistrement (tel qu'un incident de sécurité) à la valeur (un CI, un observable, etc.). Ce champ spécifie toutes les informations supplémentaires (paires de valeurs et de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	champs) à ajouter à l'enregistrement de liaison. Par exemple, pour l'ajout d'un observable pour une adresse IP source, spécifiez que cette adresse IP est l'adresse IP source et non l'adresse IP de destination. Pour plusieurs valeurs, utilisez un séparateur ^, par exemple, type= IP source^Active=true.
Données de nouvel enregistrement	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur, un nouvel enregistrement est créé si aucun enregistrement correspondant n'existe**. Si aucun enregistrement connexe correspondant à la valeur analysée n'est trouvé, un enregistrement est créé. Ce champ spécifie les données statiques à ajouter à cet enregistrement. Pour les **CI affectés**, si aucun CI correspondant n'est trouvé, un enregistrement de CI est créé. Lorsque cela se produit, la valeur trouvée dans l'e-mail est définie sur le champ **Valeur** dans l'enregistrement CI. Vous pouvez définir des données supplémentaires : une note indiquant la raison de création du CI, des informations sur le type de CI avec lequel vous travaillez, etc. Un exemple serait : description=Créé par Analyseur d'e-mails du scanner de programmes malveillants^type=autodetect.
Rechercher la valeur	Sélectionnez l'emplacement dans l'e-mail à rechercher. Les choix sont les suivants : ○ **Au début d'une ligne dans le corps de l'e-mail** ○ **N'importe où dans le corps de l'e-mail** ○ **Dans la ligne d'objet de l'e-mail** ○ **Toujours la valeur statique** Lorsque vous avez défini un **séparateur d'enregistrements**, d'autres options (**n'importe où dans la sectiondes enregistrements et au début d'une ligne dans la section des enregistrements) vous permettent d'effectuer une** recherche uniquement dans la section actuelle et non dans l'ensemble du corps de l'e-mail (voir Opérations de sécurité Analyse des e-mails pour plus d'informations. Les informations qui se trouvent dans un en-tête ou un pied de page, s'appliquant à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	tous les enregistrements, sont recherchées dans l'ensemble du corps de l'e-mail. Les informations qui diffèrent entre les enregistrements ne sont recherchées que dans la section.
Séparateur de valeur	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier à cette valeur, ce champ spécifie** le séparateur à utiliser pour les listes d'éléments. par exemple, une virgule ou un point-virgule lorsque les données de l'e-mail sont une liste d'adresses IP.
Préfixe de valeur	Texte qui précède toujours la valeur placée dans ce champ à extraire.
Fin de la valeur	Sélectionnez ce qui indique la fin de la valeur. Les choix incluent : **Fin de ligne**, **Fin de l'e-mail** (apporte tout le texte restant dans l'e-mail), ou **Jusqu'à** (s'arrête lorsqu'il trouve le texte spécifié) ou **Jusqu'à** (s'arrête lorsqu'il trouve le texte spécifié).
Suffixe de valeur	Lorsque la **fin de la valeur** est définie sur **Jusqu'à**, ce champ spécifie le texte qui suit toujours la valeur placée dans ce champ. Par exemple, la recherche d'une valeur qui vient après « L'ordinateur affecté est » et avant « . » analysera « AB123 » à partir de « Le virus du lapin dément a été trouvé. L'ordinateur concerné est AB123. L'heure estimée de l'infection était de 15h45" dans un e-mail.
Transformation de valeur	Choisissez l'entrée de transformation de champ à appliquer. Convertit la valeur trouvée dans l'e-mail en une valeur différente, utilisée pour remplir les champs de choix, parfois les champs de référence et autres.
Ordre	Ordre dans lequel s'exécutent les transformations de champ, du plus bas au plus haut. Une transformation de champ avec une entrée d'ordre de 100 est tentée en premier. Ce n'est que si cette transformation de champ ne parvient pas à trouver une valeur qu'une transformation de champ d'ordre supérieur (200) sur le même champ s'exécute.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Transformation d'e-mail	Transformation à laquelle appartient la transformation de ce champ.
Table de destination	Table de destination de la transformation d’e-mail. Il contient des données d’information provenant de la transformation d’e-mail.
Actif	La valeur par défaut est cochée. Lorsque cette option est activée, la transformation de champ est activée. Décochez cette case pour désactiver la transformation de champ.

a. Cliquez sur **Envoyer**.
Le nouvel enregistrement est utilisé pour analyser les informations contenues dans l’e-mail dans un nouvel enregistrement.

Information associée

Créer des règles de duplication dans Opérations de sécurité

Créer des Opérations de sécurité transformations de valeurs de champs

Définir les Réponse aux vulnérabilités notifications par e-mail

Modifier des enregistrements d’e-mail dans Opérations de sécurité

Ajoutez ou créez des transformations dans vos enregistrements d’événements d’e-mail existants.

Avant de commencer

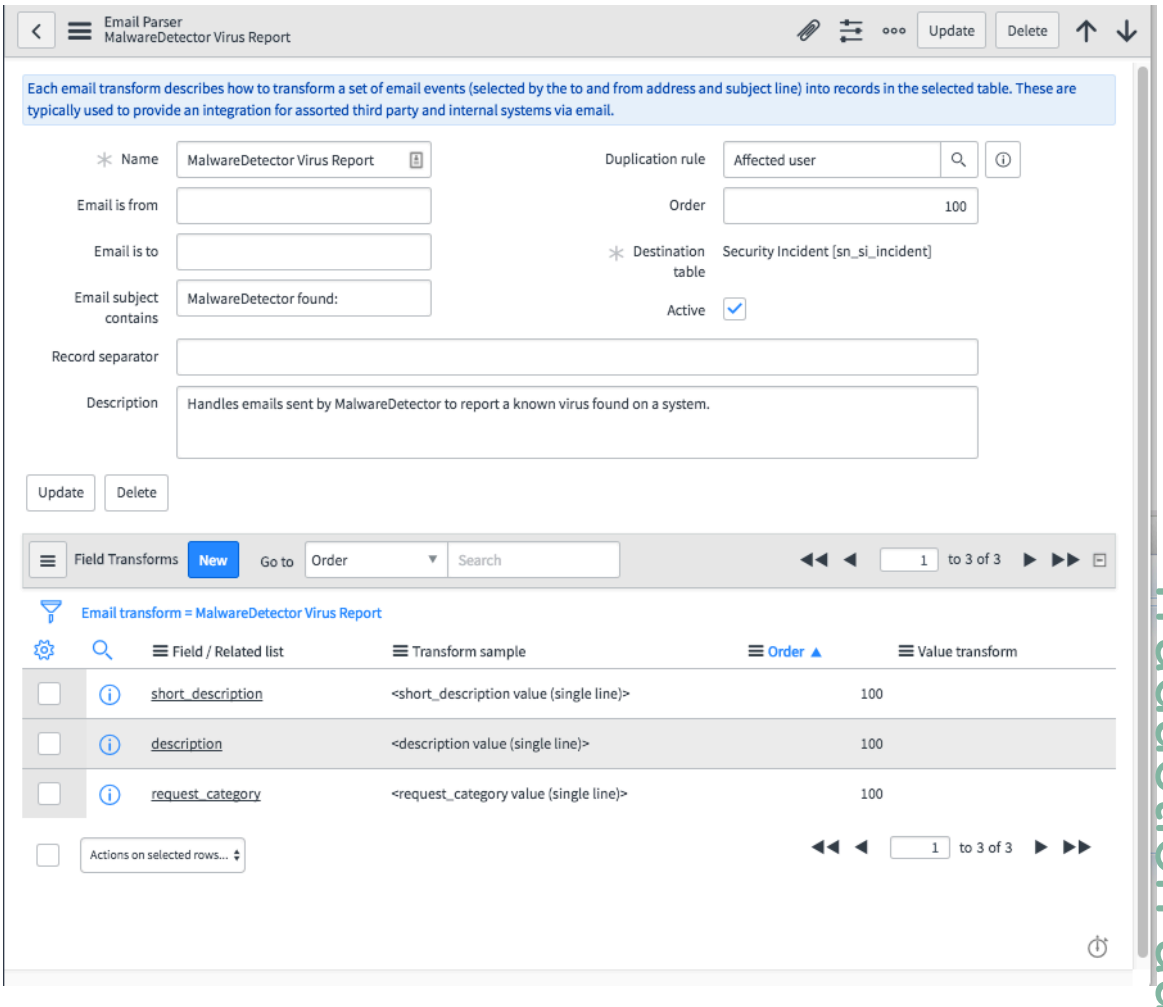
Rôle requis : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Analyse des e-mails**.
2. Cliquez sur l’analyseur d’e-mails pour modifier.
Si l’enregistrement est en lecture seule, cliquez sur le lien ici dans le message d’en-tête.
Vous êtes redirigé vers la forme modifiable de la transformation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Modifiez les champs comme il convient.
4. Pour modifier les **transformations de champ**, cliquez sur le champ et modifiez-le selon vos besoins.
5. Cliquez sur **Mettre à jour.**

Événements d'e-mail sans correspondance Opérations de sécurité

Le marqueur « correspondant » des événements par e-mail qui ne correspondent pas à un analyseur d'e-mail n'est pas défini. Vous pouvez afficher ces enregistrements d'événements d'e-mails à partir de la liste, afin de révéler les systèmes de détection externes dont les E-mails sans correspondances e-mails ne sont pas encore analysés.

Lorsque vous créez des analyseurs d'e-mails, vous pouvez tenter de retraiter l'événement d'e-mail (à partir du formulaire ou de la liste) pour valider un nouvel analyseur d'e-mail.

Afficher et traiter à nouveau les e-mails Security Operations sans correspondance

Vous pouvez examiner E-mails sans correspondances les filtres abandonnés ou en tant que candidats pour un nouveau filtre afin de maintenir ou d'améliorer le taux auquel vous interceptez les menaces par e-mail.

Avant de commencer
Rôle requis : sn_sec_cmn.read

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **E-mails sans correspondances**.
   Si des e-mails sans correspondance ont été trouvés, ils sont répertoriés.
2. Les champs du formulaire sont les suivants :

Événements d'e-mail de sécurité

Champ	Description
De	Adresse e-mail de l'expéditeur.
À	Adresse e-mail des destinataires.
Objet	Ligne d'objet dans l'e-mail.
Détails	Contenu du corps de l'e-mail.
En correspondance	Indique si cet événement par e-mail a été mis en correspondance.

3. Pour traiter à nouveau cet e-mail, créez un enregistrement d'e-mail ou modifiez un enregistrement d'e-mail existant pour qu'il corresponde aux informations contenues dans cet e-mail.
   Consultez Créer des analyseurs d'e-mails dans Security Operations.
4. Revenir à **Security Operations** > **E-mails sans correspondances**.
5. Cliquez sur **Retraiter l'événement d'e-mail** pour tenter de traiter cet e-mail.
   Cela vous renvoie à la E-mails sans correspondances liste principale. Si le nouvel enregistrement d'e-mail correspond, l'événement d'e-mail ne figure plus dans la liste. Un message indique s'il a été mis en correspondance ou non.

Opérations de sécurité Mappage de champs

Opérations de sécurité Les tables peuvent être mappées vers et à partir d'autres tables, liant un incident de sécurité à un ticket du service clientèle ou un problème à d'autres parties du Opérations de sécurité système.

Le mappage de champs définit le mappage utilisé lorsqu'un enregistrement de la table source est utilisé pour créer un nouvel enregistrement dans la table de destination. Généralement utilisées pour créer un incident de sécurité à partir d'un autre enregistrement, ces cartes définissent les champs d'un incident de sécurité qui sont insérés dans un nouveau problème ou les champs d'un incident client existant qui renseignent un nouvel incident de sécurité.

Mapper les tables aux tables avec le mappage de champs Security Operations

Opérations de sécurité vous offre une granularité de mappage de champ plus fine afin que vous puissiez mapper une Opérations de sécurité table à n'importe quelle autre table.

Avant de commencer

Rôle requis : sec_cmn.write

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Mappage de champs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

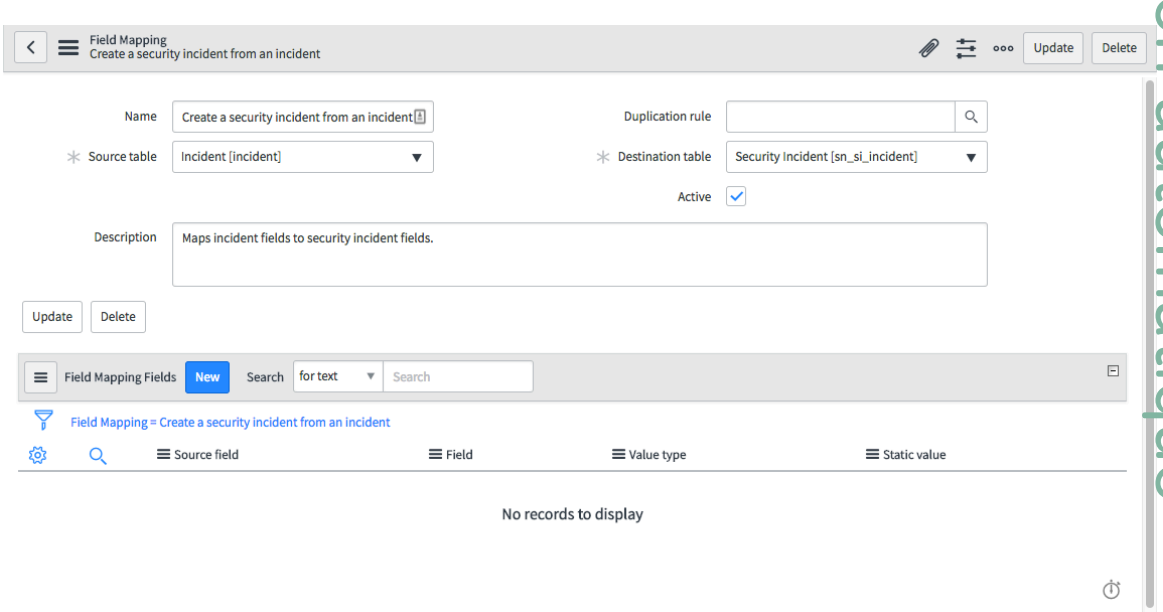
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mappage de champs

Champ	Description
Nom	Nom de la carte de champs.
Table source	Table qui fournit les données à utiliser pour créer un enregistrement dans la table de destination.
Règle de duplication	Régit la façon de gérer les enregistrements sources qui génèrent un enregistrement en double. Pour plus d'informations, consultez Transformation des données partagées.
Table de destination	Table où les nouveaux enregistrements sont créés.
Actif	Cochez cette case pour activer le mappage. **Remarque :** Un seul mappage entre les tables peut être actif à la fois. Si deux cartes contiennent les mêmes tables, l'ancienne version est automatiquement désactivée.
Description	Description de la carte de champs.

4. Lorsque vous avez terminé vos entrées, faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
L'onglet Champs de mappage de champs s'affiche. Cet enregistrement définit quelles données sont placées dans le champ cible, dans les enregistrements créés par cette transformation de champ.



5. Cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire comme il convient.

Option	Description
Champ	**Description**
Stocker la valeur dans un champ ou une liste connexe	Sélectionnez où trouver la valeur. Les choix sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	○ Ajouter une nouvelle valeur dans un champ de l'enregistrement ○ Lier à cette valeur dans une liste connexe ○ Lier à cette valeur, ce qui crée un enregistrement si un enregistrement correspondant n'existe pas **Remarque :** Si la table de destination ne possède pas de listes connexes, ce champ ne s'affiche pas.
Champ	Lorsque **l'option Stocker la valeur dans un champ ou une liste connexe** est définie sur **Ajouter une nouvelle valeur dans un champ de l'enregistrement** , ce champ indique le champ à remplir. **Remarque :** Pour les champs de choix, les correspondances sont effectuées avec les choix existants à l'aide de l'étiquette ou de la valeur de choix sous-jacente. Si aucune correspondance n'est trouvée, le champ est défini, mais aucune nouvelle entrée n'est ajoutée à la liste de choix. Pour plus d'informations, consultez Listes de choix . Pour les champs de référence, une entrée n'est définie que lorsqu'une valeur correspondant au nom d'affichage de l'enregistrement ou à un `sys_id` valide est trouvée. Pour plus d'informations, consultez Champs de référence .
Liste connexe	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou Lier à cette valeur, ce champ spécifie la liste connexe à laquelle ajouter des informations, si **un enregistrement correspondant n'existe pas**.
Champ de valeur	Lorsque **l'option Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier à cette valeur, ce qui crée un nouvel enregistrement si un enregistrement correspondant n'existe pas**, ce champ spécifie le champ de la table affichée dans la liste connexe, qui est utili–

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	sé pour rechercher et rechercher un enregistrement existant. Par exemple, si votre liste connexe est **constituée de CI affectés**, ce champ **peut contenir** Nom ou **Nom de domaine complet**, ou tout autre champ dans l'enregistrement CI qui doit être utilisé pour rechercher que le CI est ajouté à la liste **des CI affectés** .
Données de relation	Lorsque **l'option Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe**, un nouvel enregistrement est créé pour lier cet enregistrement (par exemple, un incident de sécurité) à la valeur (un CI, un observable, etc.). Ce champ spécifie toutes les informations supplémentaires (paires de valeurs et de champs) à ajouter à cet enregistrement de liaison. Par exemple, en ajoutant un observable pour une adresse IP source, vous pouvez spécifier que cette adresse IP est l'adresse IP source plutôt que l'adresse IP de destination. Pour les valeurs multiples, utilisez un séparateur ^, par exemple, type= IP source^active=true.
Données de nouvel enregistrement	**Lorsque la valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur, un nouvel enregistrement est créé si aucun enregistrement correspondant n'existe**. Un nouvel enregistrement est créé si aucun enregistrement connexe correspondant à la valeur analysée n'est trouvé. Ce champ spécifie les données statiques à ajouter à cet enregistrement. Par exemple, pour **les CI affectés**, si nous ne trouvons pas le CI, ce paramètre indique qu'un nouveau CI est créé. La valeur trouvée dans l'enregistrement source est définie sur le champ **Valeur** dans l'enregistrement CI. Vous pouvez définir des données supplémentaires : une note indiquant la raison de création de ce CI, des informations sur le type de CI avec lesquels vous travaillez. Par exemple : description=Créé par programme malveillant rapport d'incident^type=détection automatique
Séparateur de valeur	Lorsque la **valeur Stocker dans un champ ou une liste connexe** est définie sur **Lier à cette valeur dans une liste connexe** ou **Lier à cette valeur, ce qui crée un nouvel enregistrement si un enregistrement correspondant n'existe pas**, ce champ spécifie le séparateur à utiliser pour les listes d'éléments,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	généralement une virgule ou un point-virgule.
Type de valeur	Lorsque **l'option Stocker la valeur dans un champ ou une liste connexe** est définie sur **Ajouter une nouvelle valeur dans un champ de l'enregistrement** , ce champ spécifie le type de valeur. Les choix sont les suivants : ○ **Enregistrement du champ source** ○ **Ajouter au champ en tant que nouvelle ligne** ○ **Valeur statique** ○ **Valeur statique plus valeur du champ d'enregistrement source**
Champ source	Choisissez le champ source qui contient la valeur à placer dans le champ de destination ou dans la liste connexe sélectionnée.
Champ statique	Valeur statique pour le champ.
Transformation de valeur	Choisissez l'entrée de transformation de la valeur de champ à appliquer. Il est utilisé pour mapper les champs de choix entre les enregistrements, par exemple, en convertissant l'ensemble de choix de **catégorie** pour un incident de sécurité dans le champ **Type** approprié pour une demande de changement.
Table de destination	Rempli automatiquement avec la table de destination.
Mappage de champs	Rempli automatiquement avec la carte de champs parente.
Table source	Rempli automatiquement avec la table source.

7. Cliquez sur **Envoyer**.

Opérations de sécurité Transformations de valeurs de champs

Transforme les valeurs de champ client uniques en valeurs de champ reconnues par Opérations de sécurité l'analyse des e-mails, l'enrichissement des données ou les tables à l'aide de cartes de champs. Prend en charge les champs de choix, les références et aligne les données externes sur la terminologie et le format standard de votre nouvel enregistrement.

Vous pouvez mapper des données pour des champs tels que Catégorie, État ou Groupe d'affectation en valeurs utilisées dans la table Security Operations. Par exemple, mappez « En cours d'analyse » vers « Travail en cours ».

Créer des Opérations de sécurité transformations de valeurs de champs

L'option Transformations de valeurs de champs définit une transformation entre les données sources fournies et la valeur de remplacement à utiliser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : sn_sec_cmn.basic ou sn_si.basic

Pourquoi et quand exécuter cette tâche
Définissez chaque entrée de transformation à appliquer soit lorsqu'il y a une correspondance avec la valeur de recherche, soit lorsque la valeur de recherche est contenue dans les données sources fournies ou lorsqu'aucune correspondance n'est trouvée. Définissez une valeur par défaut lorsqu'aucune correspondance n'est trouvée. Si aucune valeur par défaut n'est définie et qu'aucune correspondance n'est trouvée, les données sources d'origine sont utilisées.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Transformations de valeurs de champs**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Transformations de valeurs de champs

Champ	Description
Nom	Nom de la transformation de la valeur de champ.
Description	Description de la carte de champs.
Entrées de transformation de la valeur de champ	Liste des entrées de la table. **a.** Sous **Remplacer les données**, double-cliquez sur « Insérer une nouvelle ligne ». **b.** Choisissez l'une des options suivantes : Quand la date de ce champ correspond Lorsque les données de ce champ contiennent Lorsqu'aucune autre entrée de transformation ne correspond aux données (par défaut) **c.** Cliquez sur la coche verte. **d.** Double-cliquez sous **Valeur de recherche**, ajoutez votre valeur de recherche. **e.** Cliquez sur la coche verte. **f.** Double-cliquez sous **Valeur de remplacement** , puis ajoutez la ServiceNow valeur correspondante. **g.** Répétez l'opération si nécessaire.
Actif	Cochez cette case pour activer la transformation.
Application	Périmètre de l'application.

4. Cliquez sur **Envoyer**.

Opérations de sécurité Mappage des données d'enrichissement

Mappage des données d'enrichissement Transforme les données de XML, JSON ou Propriétés de fichiers en ServiceNow enregistrements. Opérations de sécurité Les workflows utilisent des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

cartes de données d'enrichissement et fournissent des données de sortie aux incidents de sécurité.

Opérations de sécurité comprend plusieurs cartes de données d'enrichissement, déclenchées par divers workflows, par exemple, Intégrations Security Operations : obtenir le flux des statistiques réseau et Intégration des commandes du système Security Operations : obtenir le flux d'exécution des processus. La sortie du mappage des données d'enrichissement à partir des Opérations de sécurité workflows est affichée dans l'onglet **Données d'enrichissement** du formulaire d'incident de sécurité.

Créer un Opérations de sécurité mappage de données d'enrichissement

Transformez les données à partir du format JSON, XML ou Propriétés fichier en enregistrements à ServiceNow l'aide de cartes de données d'enrichissement.

Avant de commencer

Rôle requis : sn_sec_cmn.write

Pourquoi et quand exécuter cette tâche

Les mappages de données d'enrichissement existants sont utilisés par les workflows fournis dans Opérations de sécurité. Vous pouvez afficher la liste sous **Mappage des données d'enrichissement**. Pour utiliser une carte, vous avez besoin d'un déclencheur, soit une règle métier, soit un workflow.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Mappage des données d'enrichissement**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient.

Création d'un mappage de données d'enrichissement

Champ	Description
Nom	Nom de cette carte de données d'enrichissement.
Format d'entrée	Choisissez un format dans la liste : JSON (par défaut) XML Format du fichier de propriétés

Clé de préfixe	Utilisez cette propriété pour limiter l'ensemble de données d'entrée à une clé spécifiée. La racine de l'ensemble de données d'entrée est définie sur cette touche. Dans cet exemple, si vous avez saisi file_info, les valeurs d'entrée seront limitées aux valeurs comprises dans file_info.
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<malware>`
	`<version>2.0</version>`
	`<file_info>`
	`<malware>yes</malware>`
	`<sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1>`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	<filetype>PE</filetype> <sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a9300</sha256> <md5>ee8c91751b3010e38c479cf9ab09827a</md5> <size>546304</size> </file_info> </malware>
Application	Périmètre de l'application.
Règle de duplication	Règle définissant quand un enregistrement est considéré comme un doublon et les actions à entreprendre avec les enregistrements en double.
Table de destination	Choisissez une table dans la liste.
Actif	Cochez cette case pour activer la carte.
Description	Entrez une description de la carte de données d'enrichissement.

4. Cliquez sur **Envoyer**.
   L'onglet Champs de mappage des données d'enrichissement s'affiche.
5. Cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire comme il convient.

Champs de mappage des données d'enrichissement

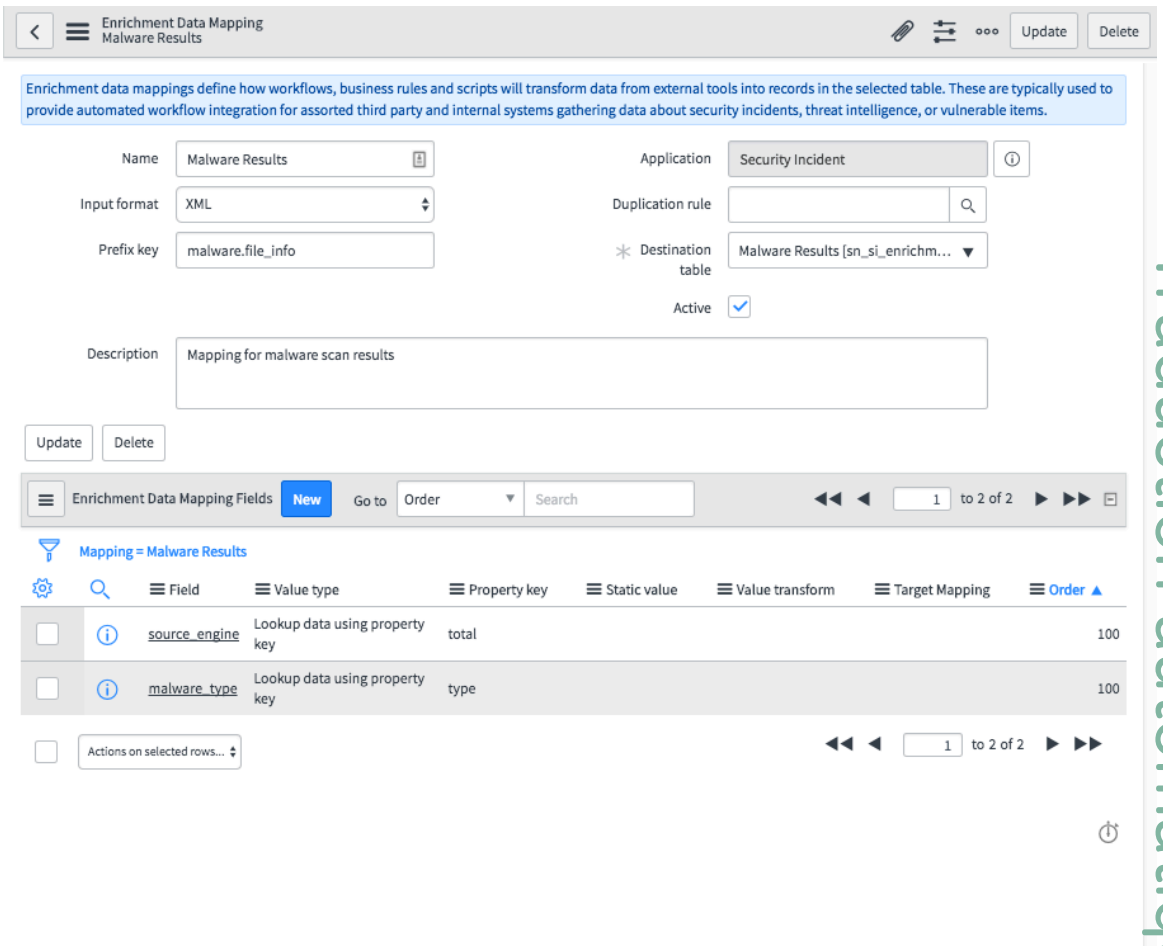
Champ	Description
Champ	Nom de la carte des données d'enrichissement.
Type de valeur	Choisissez dans la liste : Rechercher des données à l'aide de la clé de propriété Valeur statique Valeur statique plus données de la clé de propriété Le champ est un tableau ou un objet (imbrication de données brutes) Chaque choix a des entrées différentes. Les valeurs de champ et les tableaux ou objets nécessitent une clé de propriété.
Clé de propriété	Détermine la clé de la recherche de données d'entrée et la valeur écrite dans le champ cible.
Transformation de valeur	Transformation de valeur de champ qui mappe une valeur à une autre.
Application	Périmètre de l'application.
Ordre	Dans quel ordre considérer le mappage. La première correspondance est utilisée. La valeur par défaut est 100.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Mappage	Nom de la carte des données d’enrichissement.
Table de destination	Table à laquelle vont les champs à mapper.

7. Cliquez sur **Envoyer**.
   Voici un exemple de mappage de données d’enrichissement.



Traduction automatique

Opérations de sécurité Escalade définie par l’utilisateur

Vous pouvez créer un chemin d'escalade des incidents de sécurité pour les problèmes nécessitant plus d'attention ou d'expertise. Lorsqu’un groupe d’escalade existe, un bouton apparaît sur tous les incidents de sécurité de ce groupe.

Créer un groupe d’escalade Opérations de sécurité défini par l’utilisateur

Escaladez un incident de sécurité à tout groupe associé à l’incident à l’aide des escalades.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Groupes** > **Escalades**.
2. Cliquez sur**Nouveau**.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

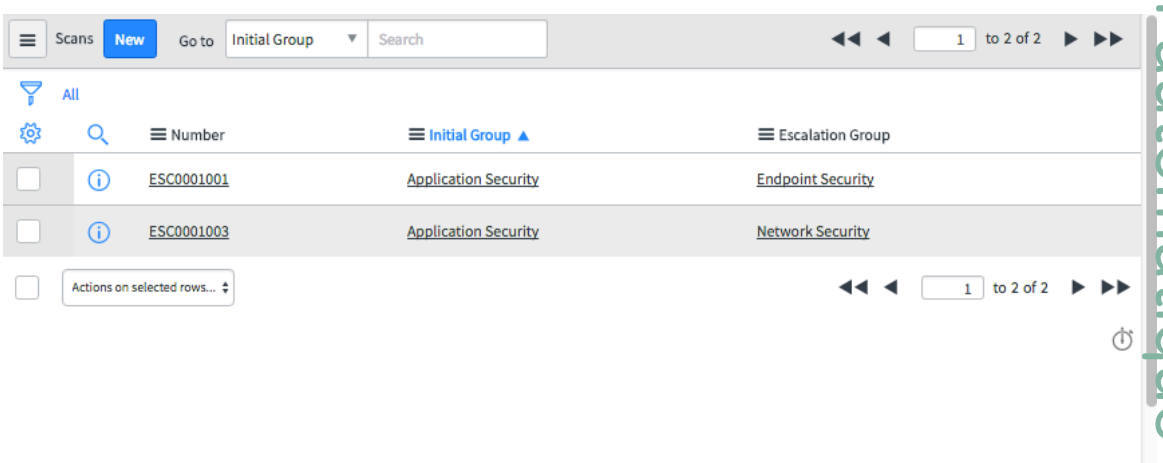
3. Renseignez les champs du formulaire comme il convient.

Escalades

Champ	Description
Numéro	Numéro d'incident d'escalade (le champ est généré automatiquement).
Groupe initial	Sélectionnez le groupe auquel appartient cet incident de sécurité.
Groupe d'escalade	Sélectionnez le groupe auquel escalader l'incident de sécurité.



4. Cliquez sur **Envoyer**.
Un groupe d'escalade est disponible pour tous les incidents de sécurité du groupe initial. Vous pouvez créer plusieurs groupes.



Traduction automatique

Créer des remplacements de propriétés séparées par domaine

Lorsque vous utilisez Séparation de domaine, vous pouvez créer des remplacements des propriétés Security Operations existantes qui vous permettent de personnaliser les fonctions des applications dans chacun de vos domaines.

Avant de commencer

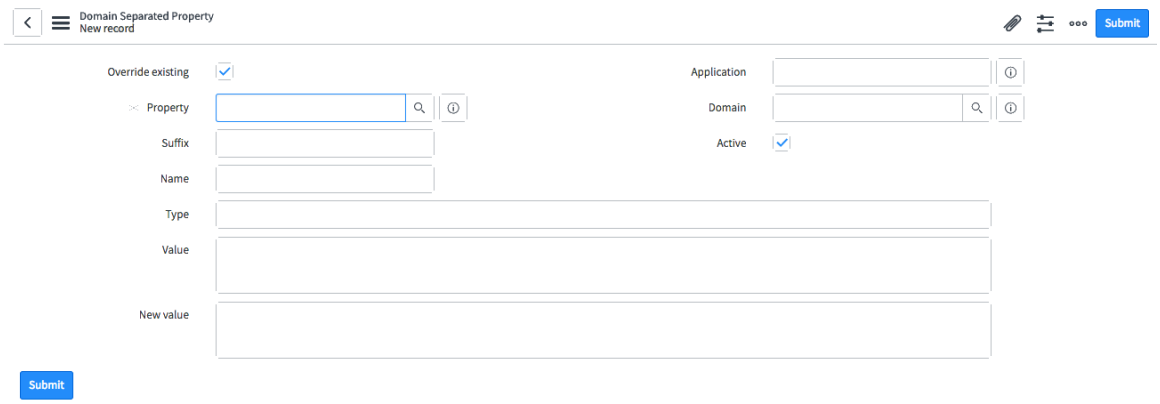
Nécessite l'activation de Prise en charge de domaine : extensions de domaine . Vous pouvez également en savoir plus sur la visionneuse de remplacement de domaine .

Rôle requis : admin

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Propriétés séparées par les domaines**.
2. Cliquez sur **Nouveau**.



3. Remplissez les champs du formulaire.

Formulaire de propriété de séparation en domaines

Champ	Description
Remplacer l'existant	Cochez cette case pour créer une valeur spécifique au domaine pour une propriété existante.
Application	Sélectionnez l'application qui contient la propriété que vous souhaitez remplacer.
Propriété	Sélectionnez la propriété de l'application sélectionnée pour laquelle vous souhaitez créer un remplacement spécifique au domaine.
Domaine	Sélectionnez le domaine pour lequel vous créez ce remplacement de propriété.
Actif	Activer ou désactiver le remplacement.
Suffixe	Affiche le suffixe de la propriété.
Nom	Affiche le nom de la propriété.
Type	Affiche le type de propriété.
Valeur	Affiche la valeur actuelle définie pour la propriété.
Nouvelle valeur	Entrez une nouvelle valeur pour la propriété à appliquer à ce domaine.

4. Cliquez sur **Envoyer**.
   Le remplacement de propriété est appliqué à la propriété sélectionnée dans le domaine spécifié. Lorsque la logique de cette propriété est déclenchée, le système recherche les remplacements de propriétés séparées par domaine. Si un remplacement du domaine est trouvé, la nouvelle valeur est utilisée. Sinon, la valeur du domaine par défaut est utilisée.

Information associée

Présentation de la séparation de domaine

Créer un groupe de systèmes d'exploitation

Les groupes de systèmes d'exploitation sont utilisés pour mapper un système d'exploitation à des types de processus et de scripts spécifiques dans Réponse aux incidents de sécurité les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

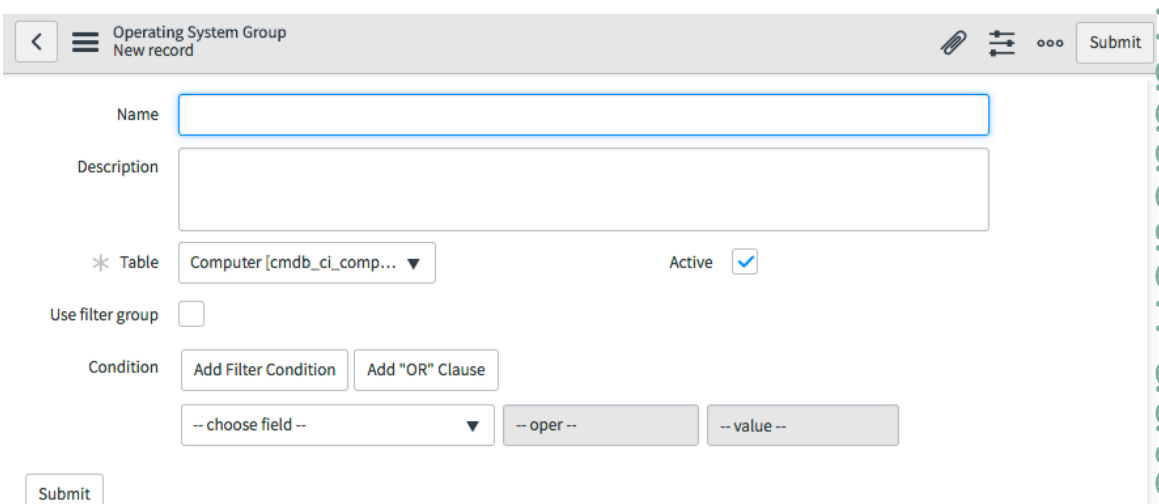
workflows. Les scripts définissent la manière dont les processus en cours d'exécution pour les groupes de systèmes d'exploitation définis sont récupérés. De nouveaux systèmes d'exploitation peuvent être ajoutés si nécessaire.

Avant de commencer

Rôle requis : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Groupes de systèmes d'exploitation**.
   Le système de base comprend des scripts pour trois systèmes d'exploitation :
   - Système d'exploitation BSD
   - Système d'exploitation basé sur POSIX
   - SE Windows
2. Cliquez sur **Nouveau**.



3. Renseignez les champs nécessaires.

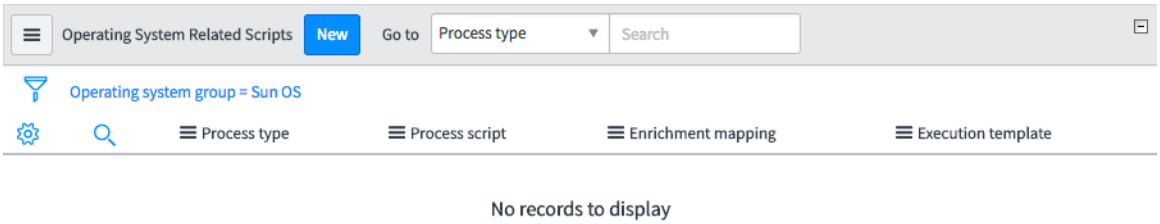
Champ	Description
Nom	Nom du groupe de systèmes d'exploitation.
Description	Description du groupe de systèmes d'exploitation.
Table	La table affectée.
Actif	Cochez cette case pour activer le groupe de systèmes d'exploitation.
Utiliser un groupe de filtres	Cochez cette case pour utiliser un groupe de filtres afin de localiser les enregistrements correspondants dans la table sélectionnée.
Groupe de filtres	Sélectionnez le groupe de filtres pour localiser les enregistrements correspondants dans la table sélectionnée. Ce champ s'affiche uniquement si vous avez coché la case **Utiliser un groupe de filtres** .
Condition	Le champ Les champs du générateur de conditions s'affichent uniquement si vous n'avez pas coché la case **Utiliser un groupe de filtres**.

4. Faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La liste connexe Scripts associés au système d'exploitation s'ouvre.



5. Cliquez sur **Nouveau**.
6. Sélectionnez les scripts qui correspondent aux workflows que vous utilisez pour obtenir des exécutions de processus, de services et/ou de statistiques réseau.
7. Cliquez sur **Envoyer**.

Information associée

Joindre un fichier de script à un fichier synchronisé Serveur MID

Configurer des groupes de balises et des balises de sécurité

Vous pouvez affecter des balises aux incidents de sécurité, aux tâches de réponse, aux éléments vulnérables, aux observables, aux IoC et aux tickets de sécurité pour créer des métadonnées sur l'enregistrement de réponse et définir qui doit avoir accès à des types spécifiques de contenu de sécurité. Les balises peuvent être ajoutées à des groupes de sécurité pour les organiser.

Avant de commencer

Rôle requis : sn_si.admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Balises de sécurité** > **Groupes**.
   Trois groupes de classification par défaut sont inclus dans le système de base.
   - **Liste d'autorisation d'enrichissement/liste de refus** : ce groupe définit si un enregistrement doit être traité comme un enregistrement de liste d'autorisation ou de liste de refus. Les enregistrements de liste d'autorisation sont généralement moins importants, ils peuvent donc être ignorés. Les enregistrements de la liste de refus sont généralement plus intéressants.
   - **Balise META** : ce groupe est fourni en tant que données de démonstration. Vous pouvez l'utiliser pour créer des balises de classification personnalisées utilisées par les applications des opérations de sécurité.
   - **Traffic Light Protocol** : Ce groupe est utilisé pour s'assurer que les informations sensibles sont partagées avec la bonne audience. Il utilise quatre couleurs (blanc, vert, ambre et rouge) pour indiquer différents degrés de sensibilité. Pour chaque couleur, vous pouvez attribuer les rôles d'accès en lecture/écriture appropriés. Lors du partage d'observables dans un cercle de sécurité approuvé, la balise affectée au profil de cercle de sécurité approuvé détermine quels observables balisés TLP peuvent être partagés avec le cercle, comme suit :
     - **TLP : BLANC :** Seuls les observables avec TLP :WHITE peuvent être partagés avec un profil TLP :WHITE.
     - **TLP : VERT :** Les observables avec TLP : GREEN et TLP :WHITE peuvent être partagés avec un profil TLP :GREEN.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **TLP : AMBRE :** Les observables avec TLP : AMBER, TLP : GREEN et TLP : WHITE peuvent être partagés avec un profil TLP : AMBER.
- **TLP : ROUGE :**Tous les observables, quelle que soit leur balise TLP, peuvent être partagés avec un profil TLP :RED, car TLP :RED est la balise TLP la mieux classée.

Remarque : Vous pouvez ajouter d'autres couleurs TLP, mais celles qui s'ajoutent aux quatre couleurs incluses sont considérées comme non valides par le Forum for Incident Response and Security Teams (FIRST).

2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Entrez le nom du groupe de sécurité.
Autoriser les sélections multiples	Cochez cette case si vous souhaitez pouvoir affecter plusieurs balises de sécurité à un enregistrement qui partage un groupe.
Actif	Activer ou désactiver le groupe.
Description	Entrez une description de ce groupe.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
   La liste connexe Balises de sécurité s'affiche.
5. Dans la liste connexe aux balises de sécurité, cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Nom de la balise de classification.
Groupe de balises de sécurité	Si la balise a été créée à l'aide du bouton **Nouveau** dans la liste connexe du groupe, ce champ est par défaut le groupe actuel. Si nécessaire, vous pouvez ajouter la balise à un autre groupe, mais cette opération est facultative.
Ordre	Indiquez l'ordre dans lequel la balise apparaît sur les formulaires ou dans une liste.
Couleur	Sélectionnez la couleur de cette balise.
Appliquer l'accès restreint	Cochez cette case pour affecter des rôles de lecture et/ou d'écriture requis par les utilisateurs pour lire ou écrire sur des enregistrements qui ont cette balise de sécurité.
Actif	Activer ou désactiver la balise.
Description	Description de cette balise.
Rôles (accès en lecture)	Pour affecter un accès en lecture à une balise de sécurité, cliquez sur l'icône de verrouillage, sélectionnez les rôles d'accès appropriés, puis cliquez à nouveau sur l'icône de verrouillage. Ce champ s'affiche uniquement si vous avez coché la case **Appliquer l'accès restreint** .
Rôles (accès en écriture)	Pour affecter un accès en écriture à une balise de sécurité, cliquez sur l'icône de verrouillage, sélectionnez les rôles d'accès appropriés, puis cliquez à nouveau sur l'icône de verrouillage. Ce champ s'affiche uniquement si vous avez coché la case **Appliquer l'accès restreint** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Répétez l'opération au besoin pour créer d'autres balises de sécurité.
8. Cliquez sur **Mettre à jour**.

> **Remarque :** Vous pouvez également créer de nouvelles balises en accédant à **Security Operations** > **Balises de sécurité** > **Balises**. La procédure est la même.

Créer des règles de balise de sécurité

Les règles de balise de sécurité permettent de filtrer l'accès aux balises de sécurité.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Balises de sécurité** > **Balises**.
2. Choisissez ou créez une balise de sécurité.
3. Dans l'onglet **connexe à Règles de balise de sécurité** , cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Le nom de la règle de balise de sécurité.
Balise de sécurité	La balise de sécurité à joindre à la règle.
Actif	Activer ou désactiver la balise de sécurité.
Description	Description de cette règle.

5. Déterminez **le filtrage des enregistrements.**
6. Renseignez les champs du formulaire comme il convient.

Champ	Description
Utiliser un groupe de filtres	Associe le groupe de filtres à la règle.
Table	La table qui doit contenir la règle.
Condition	Ajoutez une ou plusieurs conditions de filtre.

7. Cliquez sur **Envoyer**.

Importer les règles de balise de sécurité

Vous pouvez importer des règles de balise de sécurité à partir d'autres tables de votre déploiement.

Avant de commencer

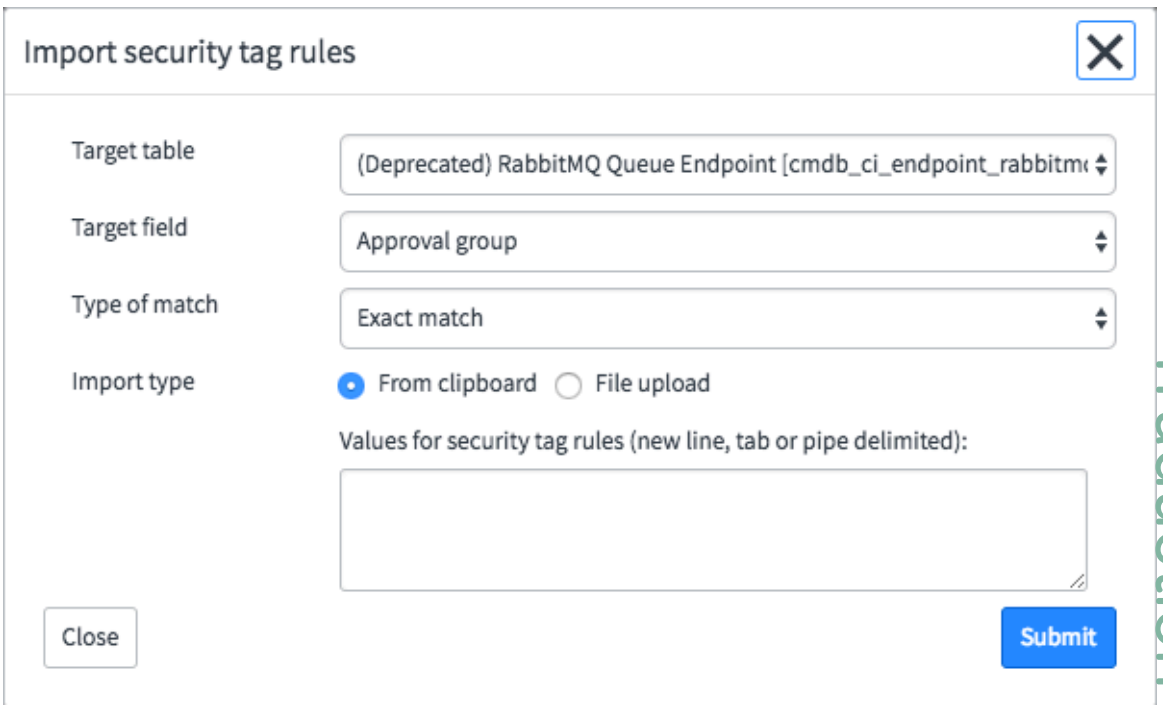
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Balises de sécurité** > **Balises**.
2. Choisissez ou créez une balise de sécurité.
3. Cliquez sur le lien connexe **Importer les règles de balise de sécurité** .



4. Renseignez les champs du formulaire comme il convient.

Champ	Description
Table cible	Choisissez la table à utiliser pour importer les règles.
Champ cible	Choisissez le champ à utiliser pour importer les règles.
Type de correspondance	Choisissez comment faire correspondre les règles importées aux **balises de sécurité** à partir de : Correspondance exacte (par défaut) Contient Commence par Se termine par Expression régulière
Type d'importation	Choisir: **À partir du presse-papiers** Copiez une liste de valeurs délimitées dans la zone de texte. Les valeurs sont analysées en balises de sécurité. **À partir du chargement du fichier** Chargez un fichier avec des valeurs délimitées. Les valeurs sont analysées en balises de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Ajoutez des valeurs pour les règles de balise de sécurité à l'aide de nouveaux délimiteurs de ligne ou de barre verticale.

5. Cliquez sur **Envoyer**.

Annotations de sécurité

Une annotation de sécurité est une note d'explication ou de commentaires ajoutée à un élément de configuration, à un observable ou à une utilisation sur un incident de sécurité.

Plusieurs annotations de sécurité sont disponibles pour les utilisateurs et les observables (nécessite le module d'extension Renseignements sur les menaces). Des rapports sur les annotations de sécurité sont également disponibles.

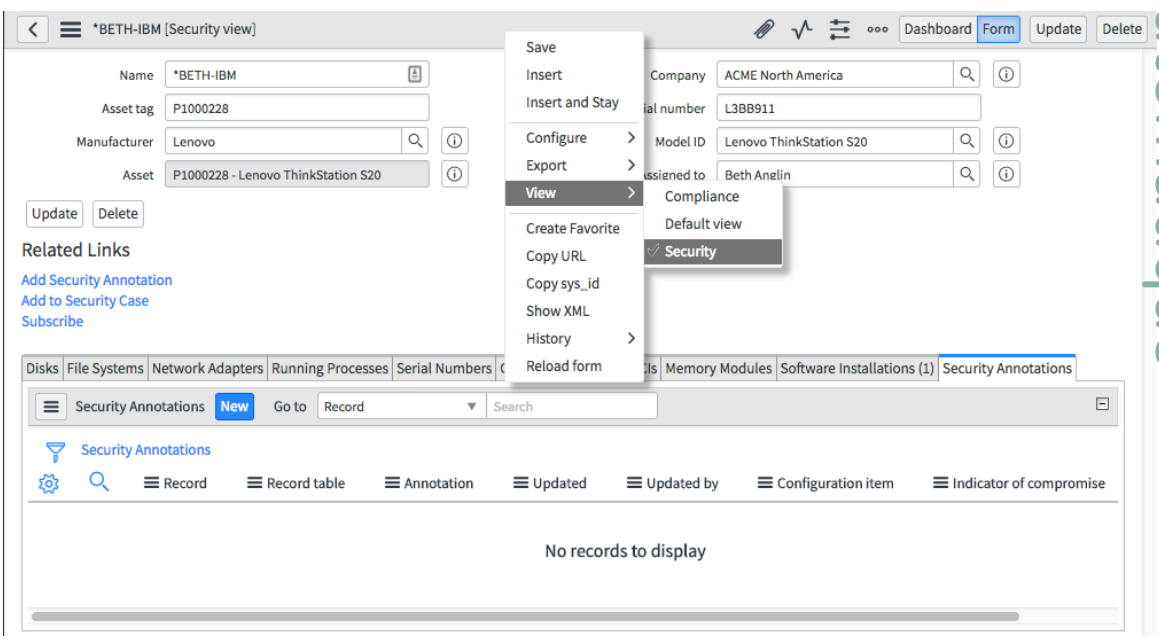
Créer des annotations de sécurité pour les CI

Les annotations sur les CI vous permettent de suivre l'activité sur tous les incidents. Vous pouvez ajouter des annotations à un ou plusieurs CI.

Avant de commencer
Rôle requis : admin

Procédure

1. Depuis un incident de sécurité ou la table Élément de configuration, ouvrez un CI.
2. Faites un clic droit dans l'en-tête et choisissez **Vue** > **Sécurité**.



3. Dans l'onglet connexe **Annotations de sécurité** , cliquez sur **Nouveau**.
4. Saisissez une annotation.
   Les annotations peuvent être dans n'importe quel format de texte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cliquez sur **Envoyer**.

> **Remarque :** Vous pouvez ajouter la même annotation à plusieurs CI en sélectionnant des CI dans la liste, en choisissant **Ajouter une annotation de sécurité**, en entrant une annotation dans n'importe quel format de texte et en cliquant sur **Soumettre**.

Créer des annotations de sécurité pour les observables

Vous pouvez sélectionner un ou plusieurs observables et leur appliquer des annotations de sécurité à l'aide du menu **de choix Actions sur les lignes sélectionnées** .

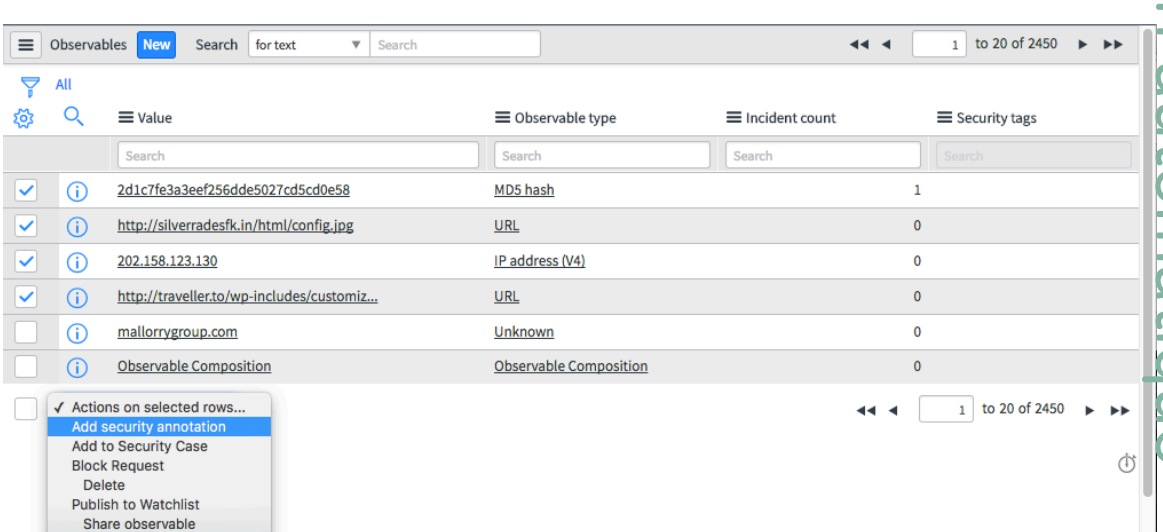
Avant de commencer

- Nécessite le module d'extension et l'activation Renseignements sur les menaces . Le module d'extension Renseignements sur les menaces est disponible sous la forme d'un abonnement distinct.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Renseignements sur les menaces** > **Observables**
2. Sélectionnez un ou plusieurs observables dans la liste.
3. Dans le menu déroulant **Actions sur les lignes sélectionnées** , choisissez **Ajouter une annotation de sécurité**.



4. Saisissez une annotation.
   Les annotations peuvent être dans n'importe quel format de texte.
5. Cliquez sur **Envoyer**.

Créer des annotations de sécurité pour les utilisateurs

Vous pouvez sélectionner un ou plusieurs utilisateurs et leur appliquer des annotations de sécurité à l'aide du menu **de choix Actions sur les lignes sélectionnées** .

Avant de commencer

Nécessite le module d'extension et l'activation Renseignements sur les menaces . Le module d'extension Renseignements sur les menaces est disponible sous la forme d'un abonnement distinct.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Administration utilisateurs** > **Utilisateurs**
2. Sélectionnez un ou plusieurs utilisateurs dans la liste.
3. Dans le menu déroulant **Actions sur les lignes sélectionnées** , choisissez **Ajouter une annotation de sécurité**.
4. Saisissez une annotation.
   Les annotations peuvent être dans n'importe quel format de texte.
5. Cliquez sur **Envoyer**.

Afficher les rapports d'annotations de sécurité

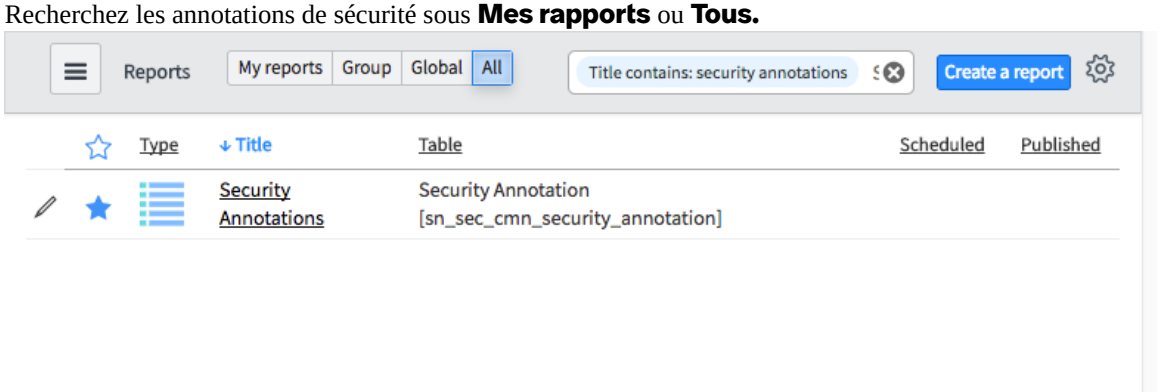
Le rapport Annotations de sécurité présente les détails stockés dans la table Annotations de sécurité [sn_sec_cmn_security_annotations]. Vous pouvez personnaliser les colonnes du rapport et regrouper les données de la manière qui vous convient.

Avant de commencer

Rôle requis : admin

Procédure

1. Accédez à la **Tous** > **Rapports** > **Afficher/Exécuter**.
2. Recherchez les annotations de sécurité sous **Mes rapports** ou **Tous.**



Information associée

Afficher la liste des rapports

Composants installés avec Security Support Common

Plusieurs types de composants sont installés avec Security Support Common. Ils fournissent des fonctionnalités communes à utiliser dans les différentes applications de sécurité, telles que Réponse aux incidents de sécurité.

Localisation et affichage des composants installés

Pour Afficher les composants installés avec Security Support Common plus d'informations sur la localisation et l'affichage des composants installés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les composants installés avec Security Support Common

Plusieurs types de composants sont installés lorsque vous activez le module d'extension, y compris, mais sans s'y Security Support Common limiter, les tables, les rôles d'utilisateur et les modules.

Localisation des composants

Remarque : La table Fichiers d'application répertorie les composants installés avec cette application. Pour savoir comment accéder à cette table, consultez Trouver les composants installés avec une application .

Si vous souhaitez limiter la liste des composants installés aux rôles, aux travaux planifiés et aux tables de l'application Security Support Common, procédez comme suit :

Afficher les listes filtrées des composants installés avec une application

Filtrez la table Fichiers d'applications afin de n'afficher que les rôles, les travaux planifiés et les tables installés avec une application. L'application pour laquelle vous souhaitez afficher ces composants doit être installée afin que ses fichiers soient chargés dans l'instance et dans la table de métadonnées. Suivez ces étapes pour afficher les listes filtrées à partir de la table Fichiers d'applications.

1. Dans le navigateur de filtre, saisissez **sys_metadata.list** pour accéder à la table de métadonnées.
2. Sélectionnez le générateur de conditions (icône de filtre), puis sélectionnez **Application** > **est** suivi du nom de votre application.
3. Dans le générateur de conditions, pour ajouter un deuxième filtre, cliquez sur **ET,** puis sélectionnez **Classe** > **est un** et choisissez l'une des classes suivantes dans la liste : **Rôle**, **Tâche planifiée** ou **Table**.
4. Sélectionnez **Exécuter**.

Les résultats de la classe que vous avez sélectionnée sont affichés dans une liste filtrée.

Rechercher Opérations de sécurité

Vous pouvez trouver rapidement des informations dans n'importe quelle Opérations de sécurité application à l'aide de l'icône de recherche située dans l'en-tête de l'écran. Zing est le moteur d'indexation et de recherche de texte qui effectue toutes les recherches de texte dans votre instance.

Avant de commencer

Rôle requis : sn_si.read ou supérieur

Procédure

1. Cliquez sur l'icône de recherche ( ) dans le coin supérieur droit de l'écran.
2. Tapez les critères selon lesquels vous souhaitez effectuer la recherche, puis appuyez sur **Entrée**.
   Si vous avez activé le module d'extension Réponse aux incidents de sécurité , les critères de recherche que vous avez entrés présentent tout texte de brève description, CI, adresse IP ou URL correspondant dans vos incidents de sécurité, Réponse aux incidents de sécurité tâches ou demandes de sécurité. Si vous avez activé les modules d'extension Réponse aux vulnérabilités OR Renseignements sur les menaces , les résultats de la recherche incluent les vulnérabilités, les éléments vulnérables, les entrées vulnérables, les observables, les IoC et les modes/méthodes d'attaque.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Introduction à la recherche

Recherche de texte Zing

Référence de Security Operations Integrations

Les développeurs et les partenaires ServiceNow peuvent utiliser les informations contenues dans cette section pour mieux comprendre les fonctionnalités sous-jacentes des intégrations tierces, y compris les directives de développement, les options d'intégration et les workflows.

ServiceNow Opérations de sécurité Directives pour le développement des intégrations

La ServiceNow plateforme fournit plusieurs mécanismes pour développer des intégrations avec des systèmes externes. La ServiceNow Opérations de sécurité suite de produits ajoute des capacités d'intégration destinées à rationaliser le processus d'intégration avec des systèmes externes axés sur la sécurité.

La plupart des concepts de ce guide supposent une certaine familiarité avec les fonctionnalités standard ServiceNow . Pour s'intégrer à la Opérations de sécurité suite, une connaissance minimale des concepts suivants ServiceNow est requise :

- Includes de script
- Services Web entrants/sortants
- Sources de données
- Ensembles de données à importer
- Cartes de transformation

Programme de partenariat technologique

Toutes les exigences relatives à la certification des applications ou les directives données dans la documentation du programme de partenariat technologique remplacent les informations contenues dans ce guide. Ce guide ne remplace pas la documentation du programme de partenariat technologique et sert uniquement de complément à la documentation existante.

Pour plus d'informations, consultez l'article de blog du cours de formation du programme de partenariat technologique .

Types d'intégrations ServiceNow fournies

Les Opérations de sécurité applications (Réponse aux incidents de sécurité, Renseignements sur les menaces et Réponse aux vulnérabilités) peuvent être intégrées de manière transparente à d'autres applications afin d'améliorer ServiceNow leurs fonctionnalités.

Les intégrations suivantes sont fournies dans le système de Opérations de sécurité base.

Security Incident Response – Intégration Event Management

Les fonctionnalités de l'application Gestion des événements ont été étendues pour prendre en charge Réponse aux incidents de sécurité. Le Réponse aux incidents de sécurité Gestion des événements module d'extension Support analyse automatiquement le contenu des événements pour Gestion des événements renseigner les champs des incidents de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation couvert :

Création d'événements de sécurité dans le système à partir d'informations de sécurité et Gestion des événements d'outils Gestion des événements (SIEM)

Options utiles fournies :

- Fonctionnalité de gestion des événements : corrélation d'événements, règles d'événements et règles d'alerte
- Mappage automatique des valeurs de additional_information à l'incident de sécurité résultant

Ressources:

Documentation d'appui sur la gestion des événements d'incident de sécurité

Documentation d'Event Management

Security Incident Response - Intégration de l'API de jeu d'importation

En plus de l'utiliser Gestion des événements pour transmettre par push des événements liés à la sécurité, l'application Réponse aux incidents de sécurité fournit une API de jeu d'importation qui permet la création directe d'incidents de sécurité. Le point de terminaison REST pour le jeu d'importation de l'incident de sécurité est http://localhost:8080/api/now/import/sn_si_incident_import.

Cette technique d'intégration est utile lorsque a) Gestion des événements n'est pas installé, ou b) il est souhaité de créer simplement des incidents de sécurité sans passer par l'événement > le flux d'alerte > d'incident de sécurité requis lors de l'utilisation de Gestion des événements.

Cas d'utilisation couvert :

Création d'incidents de sécurité directement à partir des outils SIEM.

Options utiles fournies :

Correspondance automatique de CI lors de la création d'un incident de sécurité en fonction du nom IP, NetBIOS ou de domaine complet.

Ressources:

Documentation de l'API des jeux d'importation de plateforme

Documentation sur les jeux d'importation de service web d'incidents de sécurité

Renseignements sur les menaces : rechercher l'intégration de la source

Les sources de recherche offrent la possibilité d'envoyer des données à des sources de recherche externes afin de déterminer si ces données sont malveillantes. Généralement, ces données sont une adresse IP, une URL, un fichier ou un hachage de fichier.

Cas d'utilisation couvert :

Recherchez une adresse IP, une URL, un fichier ou un hachage auprès d'un service de recherche externe.

Options utiles fournies :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Moyen cohérent de demander des recherches à partir d'éléments de catalogue et d'incidents de sécurité.
- Capacités de limitation et d'étranglement du débit fournies avec peu ou pas de codage.
- Création automatique d'entrées observables d'indicateurs de compromis (IoC) pour tous les problèmes trouvés par les sources de recherche.

Threat Intelligence : intégration de la source de menace

Les sources de menace offrent la possibilité d'extraire des données de référentiels externes de renseignements sur les menaces. Ces données sont ensuite importées dans les différentes tables d'indicateurs de compromission qui existent dans le système. Les collections TAXII et les listes de blocage simples sont prises en charge nativement. Pour ajouter de nouvelles collections TAXII (ou profils basés sur un service de découverte ou de gestion de collection), il suffit d'ajouter une entrée. De même, l'ajout d'une nouvelle liste de blocage simple à colonne unique consiste à saisir un nouvel enregistrement et à fournir l'URL de la liste de blocage. Pour les ensembles de données plus complexes, une intégration personnalisée peut être fournie pour passer un appel à une URL et analyser la réponse.

Cas d'utilisation couvert :

Récupérez les données d'une source Threat Intelligence pour les charger dans des tables IoC.

Options utiles fournies :

- Prise en charge de listes de blocage simples et de collectes TAXII sans codage.
- Mécanisme simple d'exécution des messages REST pour récupérer des données.
- Récupération/traitement des données découplées pour la réutilisation des composants d'intégration.
- Prise en charge native du traitement des données transmises renvoyées aux sources de données (et aux jeux d'importation/cartes de transformation).
- Prend en charge plusieurs demandes de données par intégration (pour les appels paginés) avec la possibilité de transmettre le contexte aux appels suivants

Ressources:

Définir une source de menace

Réponse aux vulnérabilités : intégration d'invocation de scanner

L'invocation du scanner de vulnérabilité est un point d'entrée d'intégration léger qui prend en charge l'invocation d'analyses de vulnérabilité à partir de l'instance. Un scanner de vulnérabilité tiers est appelé de façon asynchrone pour planifier une analyse des éléments de configuration ou des adresses IP.

Cas d'utilisation couvert :

Demander à un scanner tiers d'analyser un CI (à l'aide des informations d'hôte dérivées du CI) ou une adresse IP/adresses IP.

Options utiles fournies :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cadre de travail simple pour définir les implémentations de scanner.
- Moyen cohérent de demander des analyses à partir d'éléments de catalogue, d'incidents de sécurité et d'éléments vulnérables.
- Mise à jour automatique des tâches avec le résultat de l'invocation d'analyse.

Vulnerability Response : intégration de données

Les intégrations de données de vulnérabilité sont destinées à récupérer les données de vulnérabilité des systèmes de vulnérabilité tiers. Les résultats attendus de ces intégrations sont les entrées de vulnérabilité et les éléments vulnérables. Cette intégration permet aux scanners de vulnérabilité tiers de fonctionner indépendamment, dans l'espoir que les vulnérabilités puissent être traitées et suivies au sein de l'instance.

Cas d'utilisation couverts :

- Récupérer les bibliothèques de vulnérabilité
- Récupérer les paires vulnérabilité/CI
- Synchroniser les CI avec le système de gestion des vulnérabilités

Options utiles fournies :

- Récupération/traitement des données découplées pour la réutilisation des composants d'intégration.
- Prise en charge native du traitement des données transmises renvoyées aux sources de données (et aux jeux d'importation/cartes de transformation).
- Prend en charge plusieurs demandes de données par intégration (pour les appels paginés) avec la possibilité de transmettre le contexte aux appels suivants.

Ressources:

Documentation sur l'intégration des données de vulnérabilité

Opérations de sécurité Configurations d'intégration

De nombreuses intégrations incluses dans le système de base nécessitent peu ou pas de configuration et fonctionnent de la même manière. Toutefois, certaines intégrations, telles que , Qualys Cloud Platform nécessitent des étapes distinctes pour la configuration de l'intégration. D'autres prennent en charge différents ensembles de types d'analyse et de recherche et différentes limites de taux.

Cette section décrit les différences entre les intégrations prises en charge et vous dirige vers plus de documentation, si nécessaire.

- Intégration Carbon Black: vous permet d'enquêter sur les incidents de sécurité et d'y répondre à l'aide des API Carbon Black pour interroger et interagir avec les points de terminaison associés aux incidents de sécurité.
- Anti-robot Check Point - Intégration de l'analyseur d'e-mail: utilise un analyseur d'e-mails qui utilise les notifications par e-mail de Check Point Anti-bot pour créer des incidents de sécurité.
- Intégration de l'enrichissement des incidents Elasticsearch: recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- Intégration Have I been pwned?: permet de rechercher rapidement la liste des comptes piratés (adresses email et identifiants) via un service RESTful.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- HPE Security ArcSight ESM : intégration de l'analyseur d'e-mails: utilise un analyseur d'e-mails qui utilise les notifications par e-mail de HPE ArcSight ESM pour créer des incidents de sécurité.
- HPE ArcSight Logger - Intégration de l'enrichissement des incidents: recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- IBM QRadar : intégration de l'enrichissement des incidents: recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- McAfee ESM : intégration de l'analyseur d'e-mails: utilise un analyseur d'e-mails qui utilise les notifications par e-mail de McAfee ESM pour créer des incidents de sécurité.
- McAfee ESM : intégration de l'enrichissement des incidents: recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- Vue d'ensemble de l'intégration OPSWAT Metadefender: permet de télécharger les données de menace, détectées par le scanner tiers Metadefender, dans l'application pour le suivi, la hiérarchisation et la Renseignements sur les menaces résolution.
- Intégration Palo Alto Networks - AutoFocus: Palo Alto Networks AutoFocus, un service cloud de renseignements sur les menaces, vous permet de rechercher des informations de session relatives aux observables d'incident de sécurité.
- Intégration Palo Alto Networks - Firewall: Palo Alto Networks Firewall vous permet de configurer et de gérer des pare-feu pour prévenir les menaces connues et inconnues sur le réseau, le cloud et les terminaux.
- Intégration Palo Alto Networks - WildFire: l'intégration de Wildfire vous permet d'interroger par programmation les tâches d'analyse sur Wildfire et de récupérer les résultats historiques via une simple interface d'API XML.
- Présentation de Qualys Vulnerability Integration: Qualys Cloud Platform est utilisé dans Réponse aux vulnérabilités.
- Splunk - Intégration de l'enrichissement pour les incidents: recherche dans vos journaux et ajoute des informations de perception pertinentes à vos incidents de sécurité.
- Intégration de VirusTotal: utilisé dans Renseignements sur les menaces. Pour utiliser cette source de recherche, vous devez activer le module d'extension VirusTotal Integration.
- Configuration de l'intégration de l'API WhoisXML: fournit des données cohérentes et bien structurées à partir d'une recherche Whois. Maintient des données Whois précises accessibles 24h/24 et 7j/7.

Traduction automatique

Activer et configurer des intégrations tierces

Vous pouvez activer les modules d'extension pour les intégrations tierces et les configurer pour les utiliser à partir du même écran.

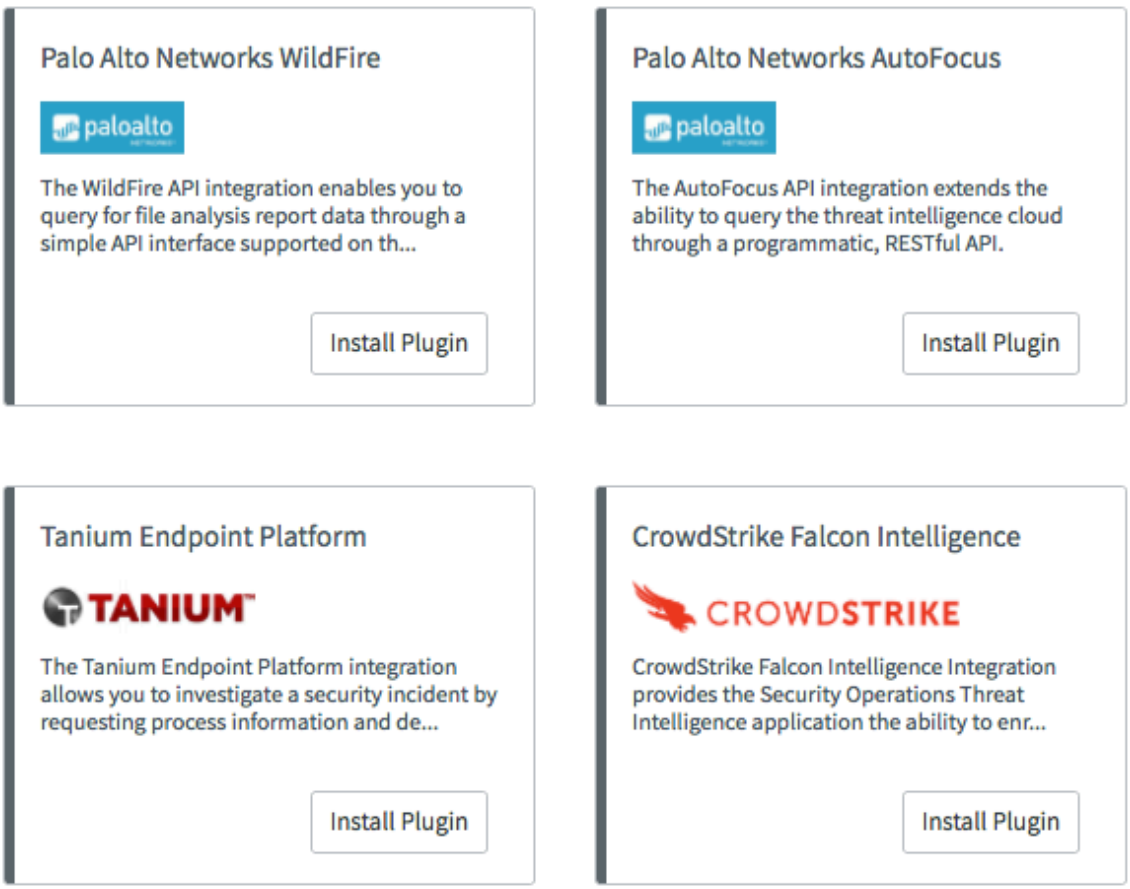
Avant de commencer

Rôle requis : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Configuration de l'intégration**.
   Les intégrations de sécurité disponibles apparaissent sous la forme d'une série de cartes, similaires au groupe de cartes suivant. Vous pouvez pointer vers n'importe quelle carte pour obtenir une description de l'intégration.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

2. Pour installer le module d'extension pour une intégration donnée, cliquez sur **Installer le module d'extension**.

   a. Dans le formulaire Module d'extension système, examinez les détails du module d'extension et cliquez sur le lien connexe **Activer/Mettre à niveau** .

   b. Cliquer sur **Activer**.
   Lorsque l'activation est terminée, l'écran d'intégration de sécurité s'affiche à nouveau et le bouton de l'intégration que vous avez activée est intitulé **Configurer**.

3. Cliquez sur **Configurer**.

   Remarque : Si vous configurez le , reportez-vous à la Qualys Vulnerability Integration section Installation et prise en charge des Réponse aux vulnérabilités applications.

4. Entrez la **clé API**.

5. Cliquez sur **Envoyer**.

Créer une intégration

Vous pouvez créer une intégration et ajouter la carte d'intégration associée à l'écran Intégrations de sécurité. Cette procédure est destinée aux partenaires qui créent des intégrations tierces.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : sn_sec_cmn.admin

Audience: Partenaires qui créent des intégrations tierces.

Procédure

1. Dans le filtre de navigation, tapez sn_sec_core_integration_item.list et appuyez sur la touche **Entrée** .
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

Champ	Description
Nom	Le nom de l'intégration.
ID de module d'extension	Le module d'extension qui doit être activé pour utiliser l'intégration.
Ordre	Indique l'ordre dans lequel cette carte d'intégration apparaît.
Texte de la bannière	Cliquez sur le lien, sélectionnez une image ou un logo à afficher sur la carte d'intégration, puis cliquez sur **OK**.
Installé	Champ en lecture seule indiquant si le module d'extension a déjà été installé.
Configurable	Indique si vous pouvez configurer l'intégration.
Catégories	Utilisé pour filtrer les cartes d'intégration.
Description brève	Description de l'intégration qui apparaît dans l'info-bulle pour la carte.
Description	Une description plus longue de l'intégration.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
   La liste connexe **Intégration et configurations** s'affiche. Vous pouvez utiliser cette liste connexe pour définir les options de configuration de l'intégration. Ces options s'affichent lorsque vous cliquez sur le bouton **Configuration** sur la carte d'intégration associée.
5. Cliquez sur **Nouveau**.
6. Renseignez les champs du formulaire comme il convient.

Champ	Description
Étiquette	Nom de l'élément d'intégration.
Nom	Le module d'extension qui doit être activé pour utiliser l'intégration.
Intégration	Affiche l'intégration pour laquelle vous définissez les éléments d'intégration
Ordre	Indique l'ordre dans lequel cet élément d'intégration apparaît.
Type	Dans la liste, sélectionnez le type de champ : ○ Chaîne ○ Entier ○ Décimal ○ Date ○ Booléen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Mot de passe ○ IPv4 ○ IPv6 ○ URL
Valeur	Entrez la valeur associée au **type** sélectionné. Si une valeur non valide pour le **type** sélectionné est saisie, aucun enregistrement n'est récupéré lors de l'exécution de l'intégration. Par exemple, si vous sélectionnez le type d'URL et saisissez la valeur 12.32.23.10, aucun enregistrement n'est récupéré.

7. Cliquez sur **Envoyer**.

Conseils pour l'écriture d'intégrations

Évitez certains des pièges que vous pouvez rencontrer lors de l'écriture de vos propres intégrations en suivant ces directives.

Utilisez la fonctionnalité de la plateforme ServiceNow dans la mesure du possible

La plupart du temps, les capacités d'intégration intégrées aux Opérations de sécurité applications (Réponse aux incidents de sécurité, Renseignements sur les menaces et Réponse aux vulnérabilités) sont destinées à améliorer ou à rationaliser les fonctionnalités d'intégration de plateforme existantes ServiceNow . Lorsque vous écrivez des intégrations, assurez-vous toujours d'utiliser la fonctionnalité de la plateforme lorsqu'elle existe. Voici quelques fonctionnalités courantes ServiceNow qui peuvent être utilisées plutôt que de « rouler soi-même ».

- Services Web sortants – pour la plupart des interactions avec des systèmes tiers, la communication se fait par le biais de services Web. Dans ce cas, utilisez les services Web sortants de la plateforme (REST et SOAP sont pris en charge).
- Sources de données/jeux d'importation/carte de transformation : pour traiter les données et les insérer dans ServiceNow des tables, le mécanisme préféré consiste à utiliser des sources de données et des composants associés.

Utilisez les cadres de travail d'intégration de Security Operations dans la mesure du possible

Étant donné que Opérations de sécurité les mécanismes d'intégration ont résolu de nombreux problèmes courants, il n'est pas nécessaire de réimplémenter les fonctionnalités de base pour chaque intégration. Par exemple, les cadres de travail des données de vulnérabilité et des sources de menaces prennent en charge le traitement de plusieurs pages et la transmission de ces données à des sources de données/transformations/ensembles d'importation. De même, le cadre de travail d'analyse ou de recherche de source fournit des fonctionnalités de limitation de débit configurables. En règle générale, lors de l'implémentation d'une fonctionnalité ou d'un ensemble de fonctionnalités, vérifiez si le cadre de travail d'intégration existant Opérations de sécurité couvre votre cas d'utilisation. Si oui, utilisez ce cadre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étendre les cadres de travail d'intégration de Security Operations existants selon les besoins

La plupart des tables et des scripts utilisés par Opérations de sécurité les cadres de travail d'intégration étaient destinés à être étendus pour répondre aux besoins futurs. Si un cas d'utilisation est rencontré lors de l'écriture d'une intégration, étendez une table ou un script d'intégration pour mieux répondre à ce cas d'utilisation.

Fournir des commentaires à ServiceNow pour les problèmes rencontrés pendant l'intégration

Au fur et à mesure qu'une intégration est en cours de développement ou de test, assurez-vous de fournir des commentaires lorsque des problèmes sont rencontrés. Même si une solution de contournement est nécessaire, Service client et assistance le personnel peut apporter une amélioration dans les versions futures qui pourrait atténuer le problème pour les intégrations futures.

Testez sous une charge raisonnable

Un problème courant avec les intégrations est qu'elles ne sont pas équipées pour gérer des charges réalistes. Étant donné que chaque intégration est une application incluse dans le périmètre, la plateforme impose davantage de limites pour assurer la stabilité du système. Ces limitations peuvent entraîner l'arrêt de tâches de longue durée ou d'appels d'API. Vous pouvez vous assurer que les processus de longue durée ou les processus qui traitent un grand nombre de données sont gérés correctement en réduisant la durée de chaque appel ou processus (généralement en fournissant un moyen de paginer les demandes d'API ou de mettre en bloc de grands ensembles de données).

Dépannage de l'intégration

Ces suggestions de dépannage peuvent vous aider à résoudre les problèmes courants que vous pouvez rencontrer lors de la configuration ou de l'exécution des intégrations.

Remplacer un certificat SSL tiers non approuvé ou expiré

Lorsqu'une connexion SSL est requise dans une intégration, il arrive que le certificat fourni par le fournisseur tiers ne soit pas encore approuvé ServiceNow ou qu'il ait expiré. Vous pouvez le remplacer ou ajouter un nouveau certificat.

Avant de commencer
Rôle requis : sn_ti.write

Procédure

1. Obtenez le certificat SSL auprès du fournisseur tiers.
   Par exemple, vous pouvez importer un certificat X.509 (PEM) à partir d'un point de terminaison SSL dans le navigateur Firefox, comme suit.

   a. Entrez l'URL du point de terminaison dans la barre d'adresse du navigateur.
   Par exemple : `https://<3rdparty>/`.

   b. Cliquez sur l'icône de verrou dans la ligne d'adresse.

   c. Cliquez sur **Plus d'informations** , puis sur l'onglet **Sécurité** .

   d. Cliquez sur **Afficher le certificat** , puis sur l'onglet **Détail** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Cliquez sur **Exporter** pour enregistrer le PEM dans votre système de fichiers local.

f. Ouvrez le fichier enregistré dans n'importe quel outil d'édition de texte et copiez le contenu dans le presse-papiers.
Il doit commencer par `----- COMMENCER LE CERTIFICAT -----` et se terminer par `----- CERTIFICAT DE FIN -----`.

2. Accédez à la **Définition du système** > **Certificats**.
3. Cliquez sur **Nouveau** et Créez un nouvel enregistrement pour l'intégration.
4. Dans **Certificat PEM**, collez le certificat que vous avez téléchargé et copié dans le presse-papiers précédemment.
5. Cliquez sur **Enregistrer**.
Les autres champs de l'enregistrement sont générés automatiquement.

Cadre de travail des options d'intégration 2.0

Le nouveau Cadre de travail des capacités d'intégration 2.0 a été remanié pour permettre la mise en œuvre des intégrations de manière simple et cohérente. Cela garantit une expérience cohérente pour des types d'intégrations similaires (par exemple : recherche de la réputation de l'observable).

Le nouveau cadre de travail comporte des fonctionnalités implémentées à l'aide de flux .

Les avantages de la mise en œuvre améliorée du cadre comprennent :

- Flux d'aptitude qui incluent uniquement des composants de niveau métier sans logique spécifique à l'implémentation.
- Les flux d'aptitude acceptent désormais un large éventail d'entrées et de formats pour une flexibilité maximale (par exemple, les références d'observables, les références de CI, les tâches, toute combinaison de tables ou de sys_id).
- La limitation ou l'étranglement des exécutions d'intégration sont désormais faciles à configurer (sans avoir à utiliser de code personnalisé ou à modifier les workflows d'implémentation).
- Des fonctionnalités d'audit et de suivi des exécutions améliorées permettent désormais d'améliorer les rapports et de faciliter le dépannage.
- Des fonctions robustes de gestion des erreurs sont intégrées aux flux d'aptitude pour éviter de dupliquer les routines d'implémentation.
- Possibilité de configurer le déclenchement conditionnel des options ou des intégrations. Cela offre la flexibilité nécessaire pour lancer automatiquement des automatisations en fonction de la catégorie d'incident.
- Une condition de filtre par défaut a été introduite sur toutes les options afin de filtrer les observables répertoriés autorisés avant que les entrées ne soient fournies aux intégrations.

Remarque : Ce nouveau cadre d'aptitude ne met pas à niveau le cadre d'aptitude actuel. Les deux cadres peuvent fonctionner en parallèle. Pour obtenir des instructions sur l'exploitation du nouveau cadre de travail d'aptitude, reportez-vous aux sections Utiliser le nouveau cadre de travail d'aptitude avec une intégration installée et Utilisation du nouveau cadre de travail d'aptitude avec un flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégrations et composants pris en charge

Le module d'extension Security Incident Response inclut tous les flux d'aptitude répertoriés dans le Cadre de travail des options d'intégration 2.0, ainsi que des filtres de haut niveau standard que vous pouvez activer ou désactiver en fonction de vos besoins.

Remarque : Si vous souhaitez utiliser le nouveau Cadre de travail d'intégration des aptitudes avec la version New York, vous devez installer le module d'extension ServiceNow Centre d'intégration Starter Pack Installer. Contactez l'assistance clientèle pour obtenir de l'aide sur l'installation.

Versions d'application prises en charge

À partir de Security Incident Response 10.0, les intégrations suivantes sont prises en charge :

Application	Version minimale requise
Intégration de l'analyse hybride Security Operations	10.0.0
Intégration de Security Operations PhishTank	10.0.0
Intégration de ThreatCrowd pour Security Operations	10.0.0
Intégration de Security Operations CrowdStrike Intelligence	10.0.0
Opérations de sécurité : « Ai-je été pwned ? » Intégration	10.0.0
Intégration de Security Operations Metadefender	10.0.0
Intégration future enregistrée par Security Operations	10.0.0
Intégration de Security Operations VirusTotal	10.0.0
Intégration WhoIs inversée de Security Operations	10.0.0

À partir de Security Incident Response 10.4, les intégrations suivantes sont prises en charge :

Application	Version minimale requise
Intégration de RiskIQ pour Opérations de sécurité	10.0.0
Intégration de Security Operations Shodan	10.0.0
Intégration Security Operations WhoIs	10.0.0
Intégration de Security Operations Carbon Black	10.3.1
Intégration de la recherche Splunk pour Security Operations	10.3.0
Intégration de l'enregistreur ArcSight pour Opérations de sécurité	10.3.0
Intégration de Security Operations à McAfee ESM	10.3.0
Intégration de Security Operations Elasticsearch	10.3.0
Opérations de sécurité Intégration IBM QRadar	10.3.1
Opérations de sécurité CrowdStrike Falcon Host	10.3.0

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants inclus

Le nouveau cadre de travail d'intégration de l'aptitude comprend les composants suivants :

- **Options** : toutes les fonctionnalités suivantes qui existent aujourd'hui dans le produit en tant que workflows ont été repensées à l'aide de flux :
  - **Demande de bloc** : fournit un moyen de bloquer les observables associés à un incident de sécurité sur un pare-feu, un proxy web ou un autre point de contrôle. Cette aptitude est utilisée au cours des enquêtes de réponse à un incident pour contenir une menace identifiée.
  - **Recherche et suppression d'e-mails** : fournit un moyen de rechercher un serveur de messagerie pendant un examen de sécurité et, si nécessaire, de supprimer les e-mails du serveur.
  - **Enrichir l'élément de configuration** : fournit un moyen général d'enrichir les éléments de configuration avec des informations supplémentaires tirées de diverses sources. Cette fonctionnalité est utilisée lors des enquêtes de réponse aux incidents pour enrichir les données associées à un incident de sécurité.
  - **Enrichir les observables** : fournit un moyen général d'enrichir les observables avec des informations supplémentaires provenant de diverses sources. Cette aptitude est utilisée au cours des enquêtes de réponse à un incident pour contenir une menace identifiée.
  - **Ingestion d'événements** : fournit un moyen général de créer un incident de sécurité en mappant les événements d'une source d'intégration à un incident de sécurité.
  - **Obtenir les statistiques réseau** : Récupère une liste des connexions réseau actives à partir d'un point de terminaison ou d'un hôte. Cette aptitude est utilisée pour enrichir les incidents au cours des enquêtes.
  - **Obtenir les processus en cours d'exécution** : Récupère une liste des processus en cours d'exécution à partir d'un point de terminaison ou d'un hôte. Cette aptitude est utilisée pour enrichir les incidents au cours des enquêtes.
  - **Isoler l'hôte** : fournit un moyen d'isoler un point de terminaison ou un hôte associé à un incident de sécurité. L'option Isoler l'hôte est exécutée par rapport à un élément de configuration (CI).
  - **Publier dans la liste de surveillance** : fournit un moyen d'ajouter des observables associés à un incident de sécurité à une liste de surveillance qui surveille les événements de sécurité et génère des alertes. Cette aptitude est utilisée dans le cadre de la réponse aux incidents au cours des enquêtes.
  - **Recherche de perceptions** : recherche des instances d'observables dans différents SIEM ou d'autres magasins de journaux. Cette fonctionnalité est utilisée pour déterminer la présence d'IoC malveillants dans votre environnement.
  - **Recherche de menaces** : effectue des recherches de renseignements sur les menaces pour déterminer si un observable donné est associé à une menace de sécurité connue. Cette aptitude est utilisée dans le cadre de la réponse aux incidents au cours des enquêtes.
- **Nouvelles tables** :
  - sn_sec_cmn_capability : aptitude et flux qui implémente l'aptitude.
  - sn_sec_cmn_capability_implementation : flux d'implémentation réel qui fournit les services de l'option.
  - sn_sec_cmn_capability_execution : enregistrement d'exécution d'une option au moment de l'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

  - sn_sec_cmn_capability_implementation_execution : enregistrement d'exécution pour une implémentation d'aptitude au moment de l'exécution.
  - sn_sec_cmn_filter_condition : conditions de filtre qui peuvent être appliquées lors de l'exécution à l'option ou à une implémentation d'aptitude.
- **Inclure le script** : CapabilityProcessor : gère tout le code de traitement pour l'infrastructure.
- **Limite du taux** : Nombre maximal de demandes simultanées par période : définit le nombre d'intégrations pouvant être exécutées en parallèle.
- **Implémentation de l'aptitude du processus de tâche planifiée** : s'exécute toutes les 15 secondes et peut être désactivée dans la page Propriétés de l'administration de la sécurité (**Incident de sécurité** > **Administration** > **Propriétés**.
  - Active ou désactive la tâche planifiée, Implémentations d'aptitudes de processus : cette tâche planifie et gère automatiquement les flux d'exécution de l'implémentation des aptitudes.
  - Active ou désactive les recherches ou les enrichissements automatisés : paramètre qui active ou désactive la tâche planifiée qui effectue une recherche automatisée de menaces ou un enrichissement des observables lorsque des éléments observables sont ajoutés aux incidents de sécurité dans le cadre de travail d'aptitude actuel.
  - Active ou désactive la tâche planifiée, Rechercher les observables d'incident de sécurité : cette tâche planifie automatiquement une tâche de recherche de menace ou d'enrichissement des observables lorsque des éléments observables sont ajoutés à un incident de sécurité.

Configurations dans le nouveau cadre de travail d'aptitude

Cette section décrit les configurations disponibles dans le nouveau cadre de travail.

Avant de commencer

Rôle requis : sn_si.admin, flow_designer action_designer

Procédure

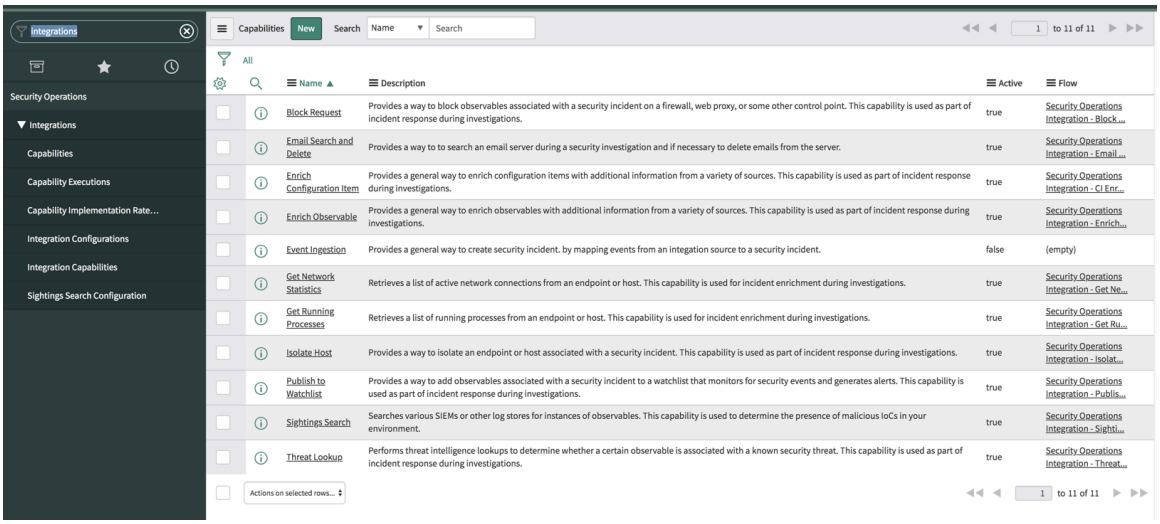
1. Accédez à la **Tous** > **Security Operations** > **Intégrations** > **Options**.

   Remarque : Version 10.4 : à partir de Security Incident Response 10.4, le nom de menu **Options** a été changé en **Options d'intégration (flux).**

2. Les options disponibles avec le système de base s'affichent.

Traduction automatique

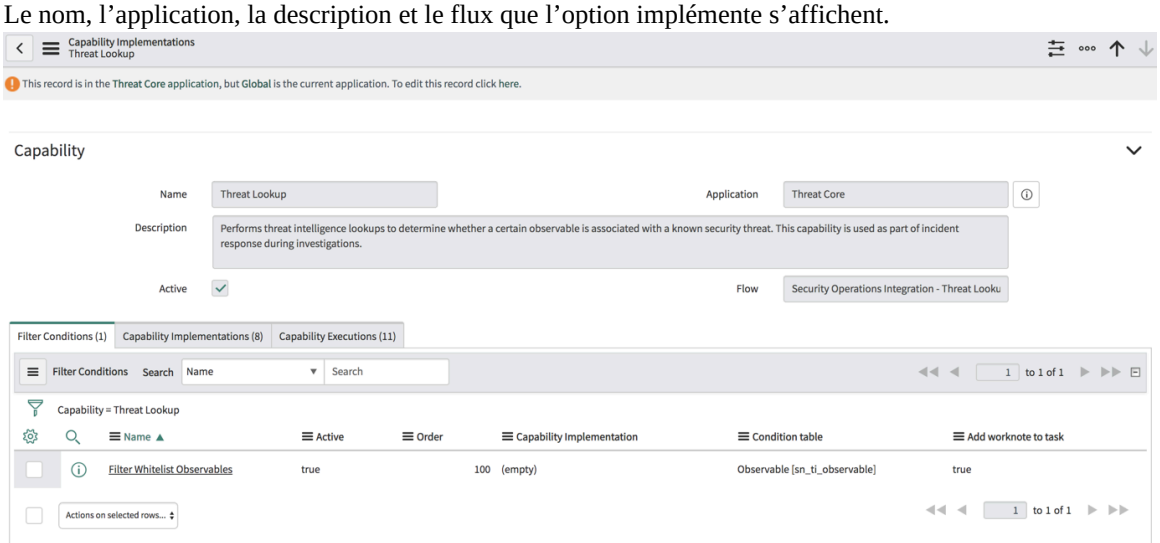
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

Il s'agit des capacités fournies avec le système de base. Vous pouvez utiliser les options ou les personnaliser selon vos besoins. Les étapes suivantes décrivent la configuration d'une option et les intégrations implémentées pour celle-ci.

3. Cliquez sur le lien dans la colonne Nom pour configurer une option.
Le nom, l'application, la description et le flux que l'option implémente s'affichent.



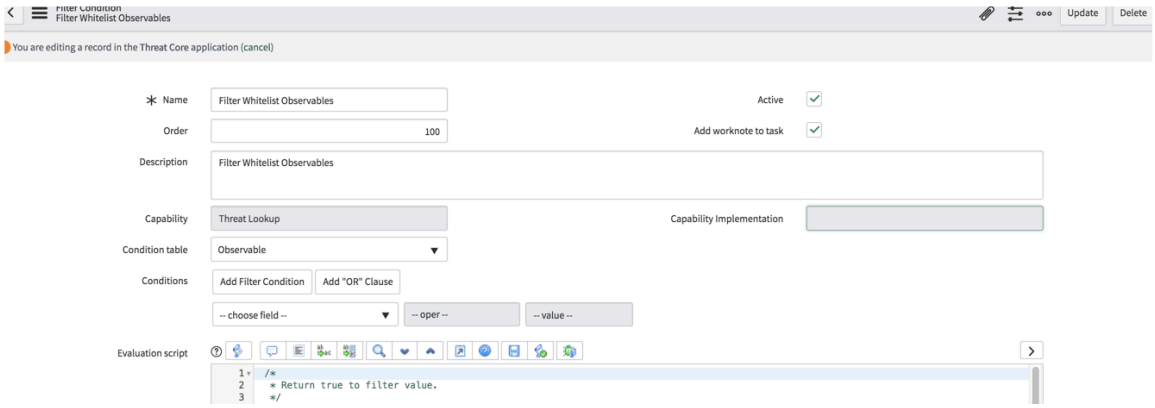
4. Cochez la case **Actif** pour activer l'option.

- **Conditions de filtre au niveau de l'aptitude** : lorsqu'une option d'intégration implémente un flux, les conditions de filtre associées au flux sont exécutées avant le lancement du flux d'aptitude. Par exemple, la fonctionnalité de recherche de menace inclut la condition Filtrer les éléments observables sur liste d'autorisation, comme indiqué ci-dessus. Cliquez sur le lien Nom pour modifier la condition de filtre.

  Remarque : Cochez la case **Ajouter une note de travail à la tâche** pour ajouter des notes de travail afin d'inclure des informations sur les conditions de filtre utilisées.

Traduction automatique

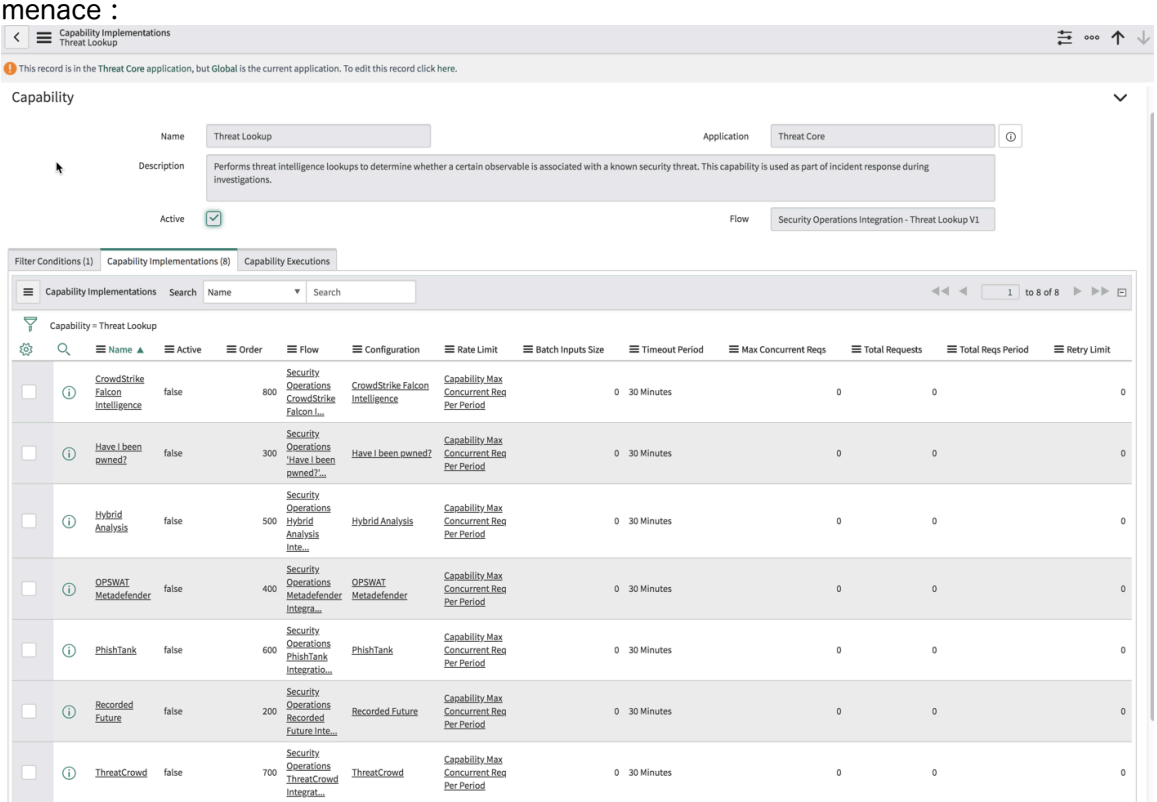
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez définir des conditions de filtre ou un script, ou une combinaison des deux. Dans l'exemple ci-dessus, un script est utilisé pour définir les conditions de filtre. Lorsque le flux d'aptitude est exécuté, le script recherche les observables sur la liste d'autorisation et les supprime de la table.

Remarque : Les conditions de filtre définies ici s'appliquent à toutes les intégrations actives définies dans l'onglet **Implémentations des aptitudes** .

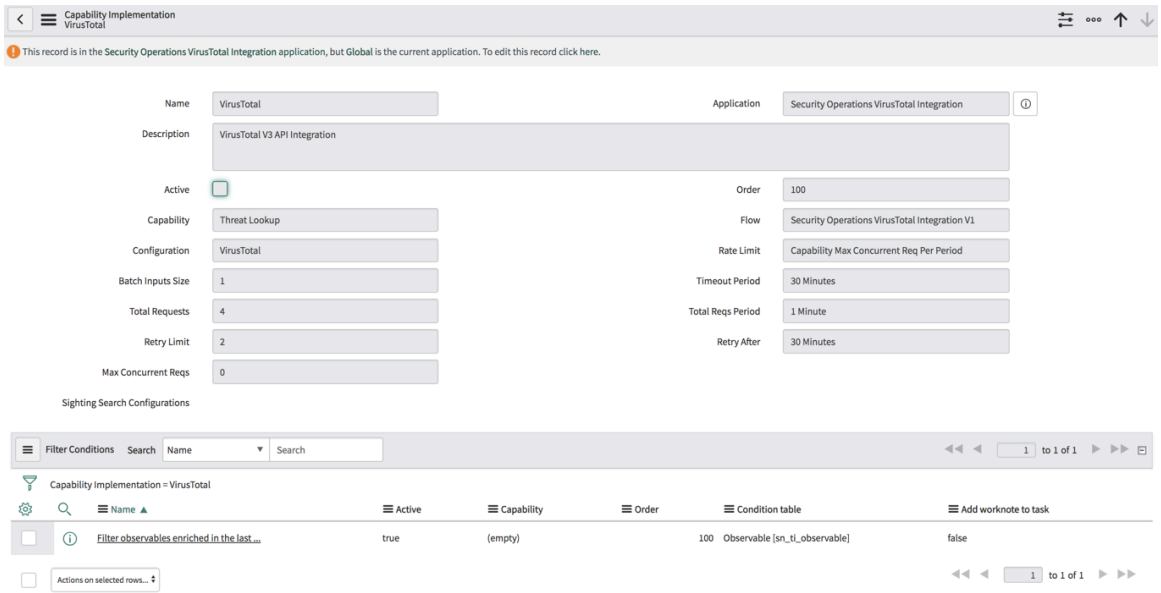
- **Implémentations d'aptitudes** : cliquez sur l'onglet **Implémentations d'aptitudes** . Les implémentations (intégrations) qui ont été configurées pour la fonctionnalité s'affichent. L'exemple ci-dessous montre les intégrations configurées pour l'aptitude Recherche de menace :



5. Cliquez sur le lien Nom pour afficher l'implémentation de l'option.
   Le nom, l'application, la description et le flux que l'option implémente s'affichent.
6. Cochez la case **Actif** pour activer l'aptitude.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez spécifier les détails suivants :

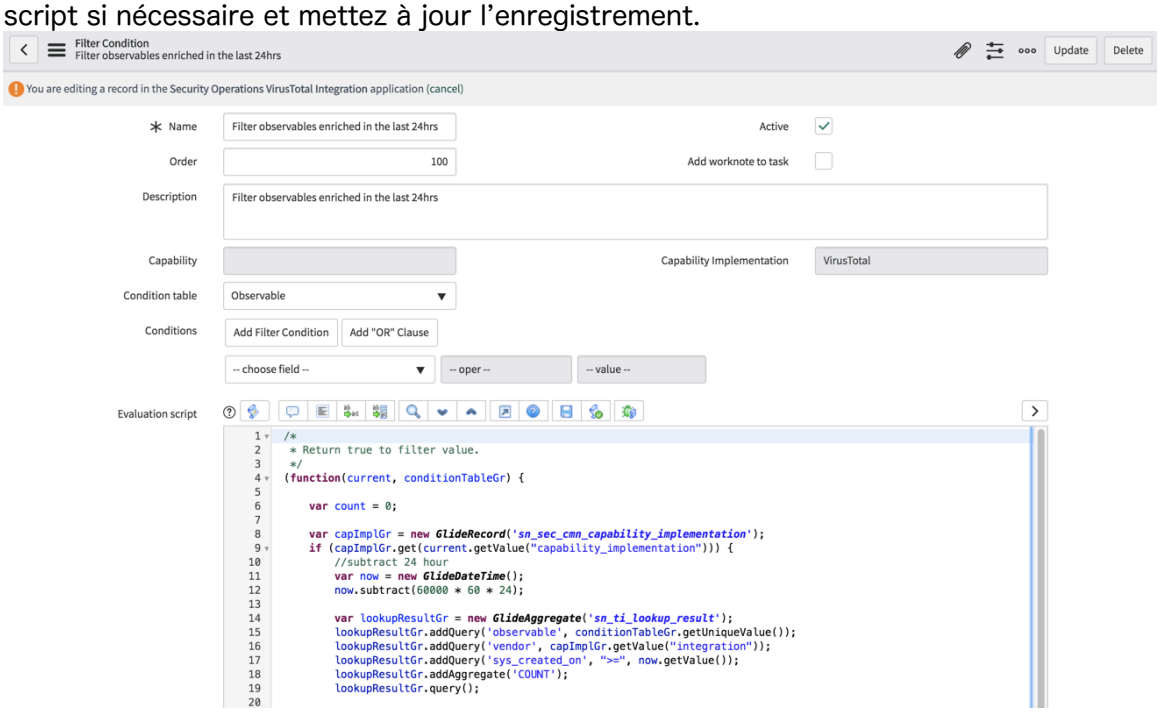
Nom de champ	Description
Actif	Cochez cette case pour activer la désactivation de cette intégration. **Remarque :** Si vous configurez cette intégration à l'aide de la vignette d'intégration dans le **Security Operations** > **Intégrations** > **Configurations des intégrations**, ce marqueur est automatiquement défini sur **Actif**.
Ordre	Indique l'ordre dans lequel les intégrations sont exécutées.
Option	Aptitude implémentée par cette intégration.
Flux	Flux secondaire qui implémente l'aptitude.
Configuration	La configuration d'intégration pour cette option. **Remarque :** La configuration par défaut est initialement définie avec le système de base. Lorsqu'une intégration est configurée à l'aide de la vignette d'intégration sur la page **Configurations d'intégration** , cette valeur est automatiquement réinitialisée sur la nouvelle configuration créée.
Limite du taux	Indique le nombre d'intégrations qui peuvent être exécutées au moment de l'exécution (en parallèle ou par unité de temps).
Taille des entrées par lots	Taille d'entrée du lot pour chaque exécution. Par exemple, pour une intégration de recherche de perceptions, vous pouvez regrouper les observables en lots de 50 afin que les requêtes générées ne deviennent pas trop volumineuses. 0 indique qu'il n'y a pas de limite.
Délai d'expiration	Durée maximale avant l'annulation du flux d'implémentation de l'aptitude. 0 indique qu'il n'y a pas de délai d'expiration.
Nombre total de demandes	Nombre total de demandes d'exécution de l'implémentation. Ce champ, associé au champ Période de demandes totales, peut être utilisé pour limiter

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom de champ	Description
	le nombre de demandes au service. Par exemple, vous pouvez limiter le nombre à 4 demandes par minute.
Nombre total de demandes au cours de la période	Nombre total de demandes d'exécution autorisées par période.
Nombre limite de nouvelles tentatives	Nombre de nouvelles tentatives autorisées pour une demande d'exécution ayant échoué. Cette limite sera applicable si le marqueur **Nouvelle tentative** est défini dans votre intégration pour retenter une demande d'exécution lorsqu'une condition est remplie. Par exemple, une demande de nouvelle tentative est effectuée lorsque vous avez dépassé la limite de votre licence pour ce service pendant une période donnée ou lorsque le service est en panne.
Recommencer après	Période après laquelle une tentative est effectuée de retenter une demande d'exécution ayant échoué.
Nombre maximal de demandes simultanées	Nombre maximal de demandes d'exécution d'implémentation simultanées. 0 indique qu'il n'y a aucune limite.
Configurations de recherche de perceptions	Les requêtes de recherche de perception par défaut qui peuvent être exécutées.

Cliquez sur le lien Nom dans la section Conditions de filtre pour configurer les conditions définies pour l'implémentation. Ajoutez ou supprimez des conditions de filtre, modifiez le script si nécessaire et mettez à jour l'enregistrement.



Utiliser le nouveau cadre de travail d'aptitude avec une intégration installée

Cette section décrit comment utiliser le nouveau cadre de travail d'aptitude pour une intégration existante.

Suivez les étapes ci-dessous pour permettre à une intégration déjà installée et configurée (voir la liste prise en charge des intégrations dans Intégrations et composants pris en charge) d'utiliser le nouveau cadre de travail d'aptitude.

Traduction automatique

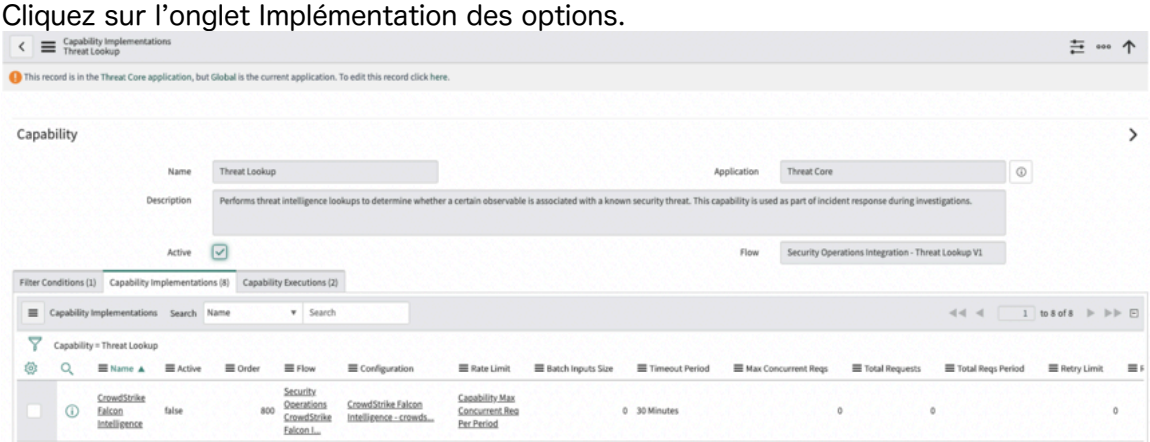
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Cadre de travail **d'aptitude d'intégration** 2.0 disponible avec Réponse aux incidents de sécurité 10.0.2 prend en charge les implémentations des options Recherche de menace et **Enrichir les observables** . Les implémentations d'autres fonctionnalités seront disponibles dans une version ultérieure.

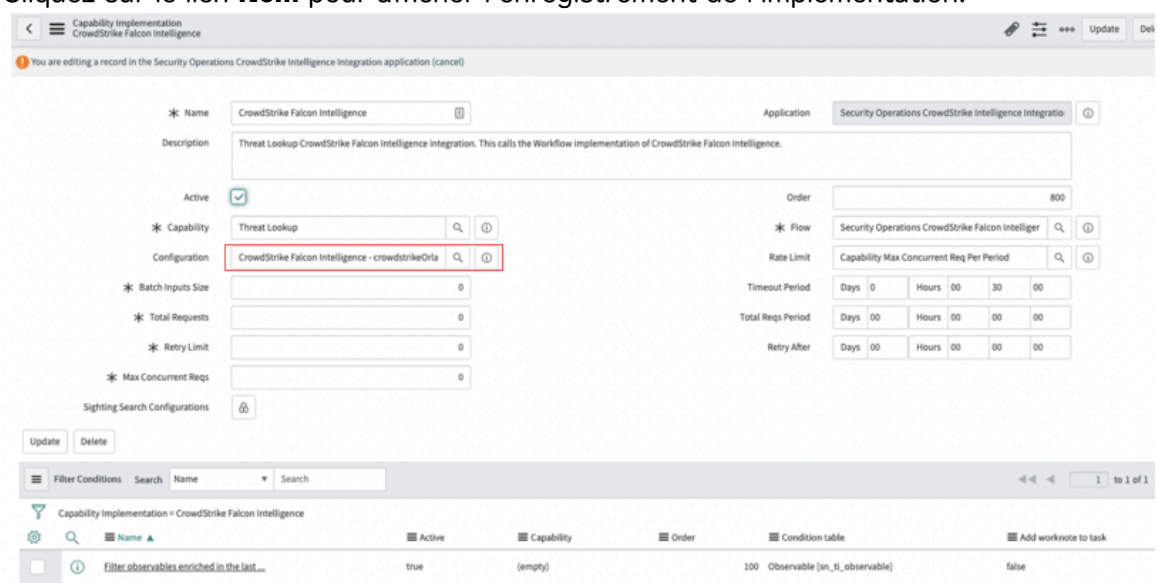
Avant de commencer

- Rôle requis : sn_si.admin
- Réponse aux incidents de sécurité 10.0.2

1. Accédez à la **Security Operations** > **Intégrations** > **Options**.
2. Cliquez sur **l'aptitude de recherche de menace** .
3. Cliquez sur l'onglet Implémentation des options.



4. 4. Affichez l'enregistrement d'implémentation de l'aptitude pour l'intégration de l'élément qui vous intéresse (exemple : Crowdstrike Falcon Intelligence). La colonne **Actif** doit avoir la valeur **Faux**.
5. Cliquez sur le lien **Nom** pour afficher l'enregistrement de l'implémentation.

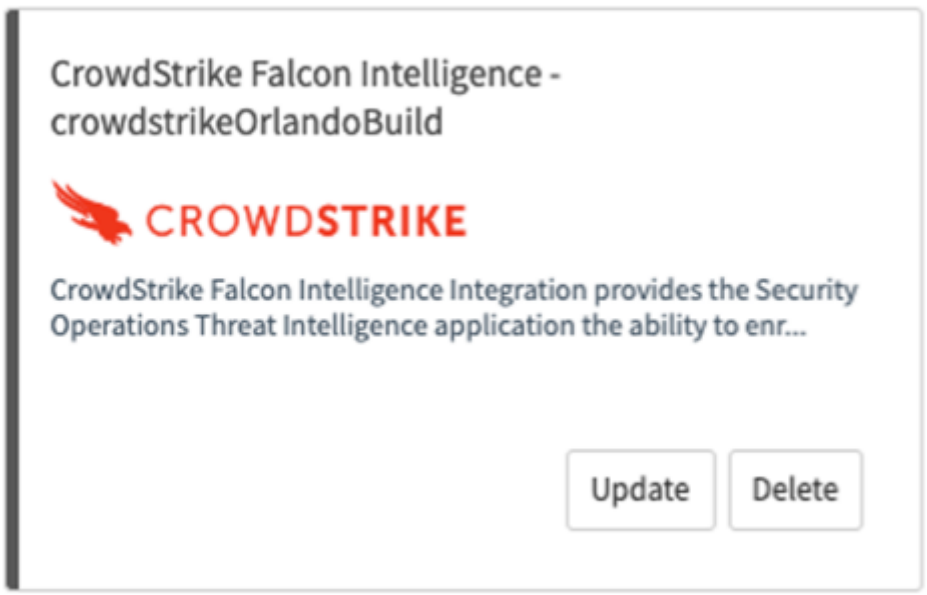


6. Sélectionnez la case à cocher **Activé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Assurez-vous que l'enregistrement d'implémentation pointe vers le bon enregistrement de configuration (le nom de la vignette pour l'intégration dans **Configurations d'intégration** > **Afficher les configurations (oui)**).



8. L'implémentation est activée pour être utilisée avec le nouveau cadre de travail.

Remarque : Toutes les intégrations prises en charge lorsqu'elles sont installées avec Réponse aux incidents de sécurité 10.0.2 seront automatiquement activées dans le nouveau cadre de travail d'aptitude d'intégration.

Utilisation du nouveau cadre de travail d'aptitude avec un flux

Suivez les étapes ci-dessous pour créer un flux et appeler le flux secondaire fourni par le nouveau cadre de travail d'aptitude.

Avant de commencer

- Rôle requis : sn_si.admin, flow_designer action_designer
- Installez l'une des intégrations prises en charge (voir Intégrations et composants pris en charge)

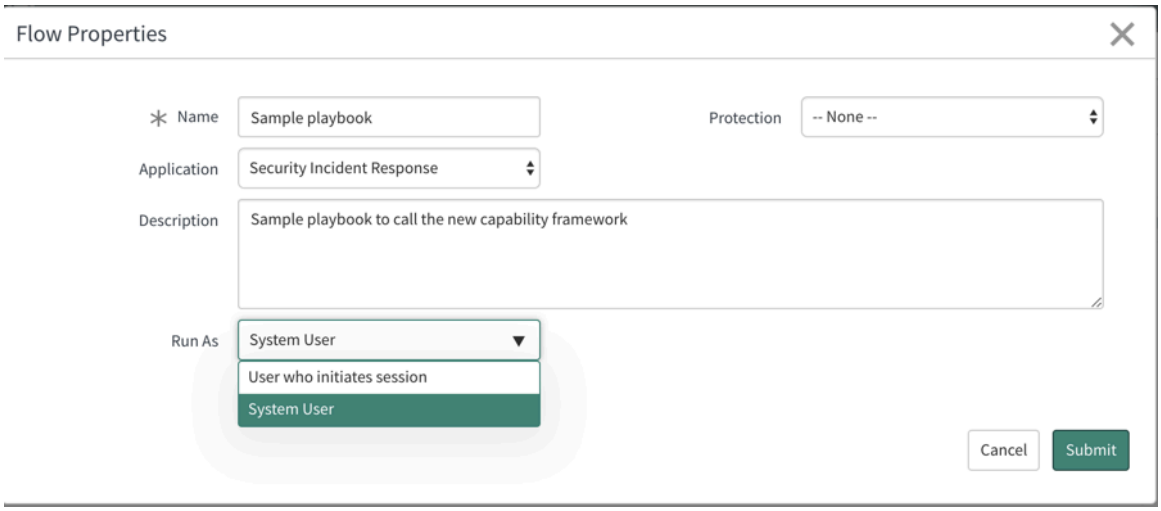
Les étapes ci-dessous décrivent comment créer un exemple de flux et appeler l'un des flux secondaires fournis avec le nouveau cadre de travail d'aptitude.

Procédure

1. Accédez à la **Tous** > **Concepteur de flux** > **Concepteur**.
2. Cliquez sur **Nouveau** pour créer un flux et fournir les informations nécessaires pour les propriétés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

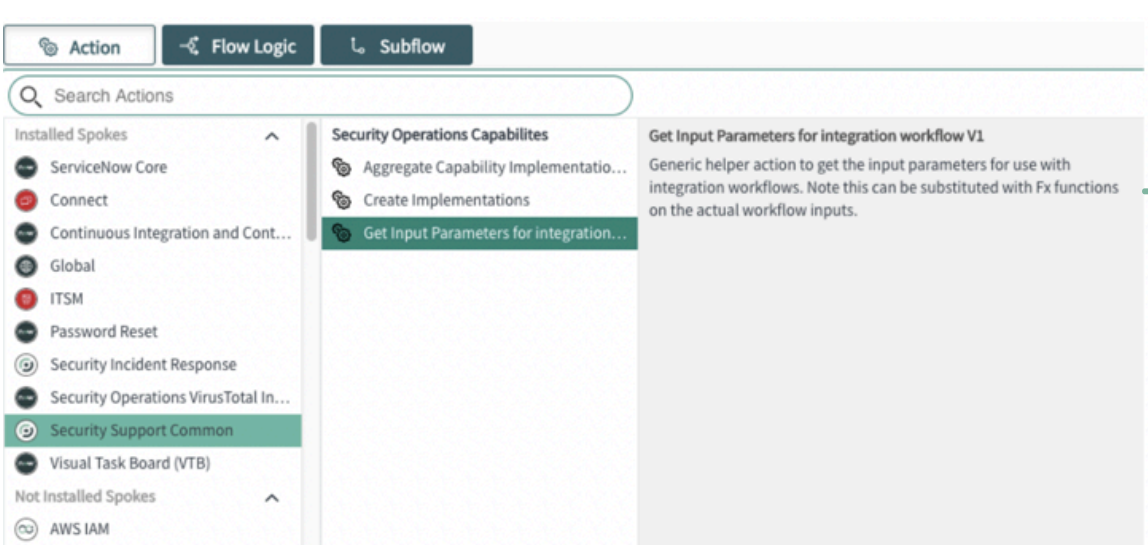


Remarque : Sélectionnez **Utilisateur système** dans la liste de choix Exécuter en tant que, comme illustré dans l'image ci-dessus.

3. Sélectionnez une condition de déclenchement pour le flux (un déclencheur courant est la création d'un enregistrement d'incident de sécurité pour une certaine catégorie d'incidents).



4. À l'étape 1 du flux, sélectionnez une action pour obtenir des entrées de l'incident de sécurité (par exemple, des observables).
   Vous pouvez sélectionner une action parmi les actions fournies avec le système de base avec le spoke commun de prise en charge de la sécurité.



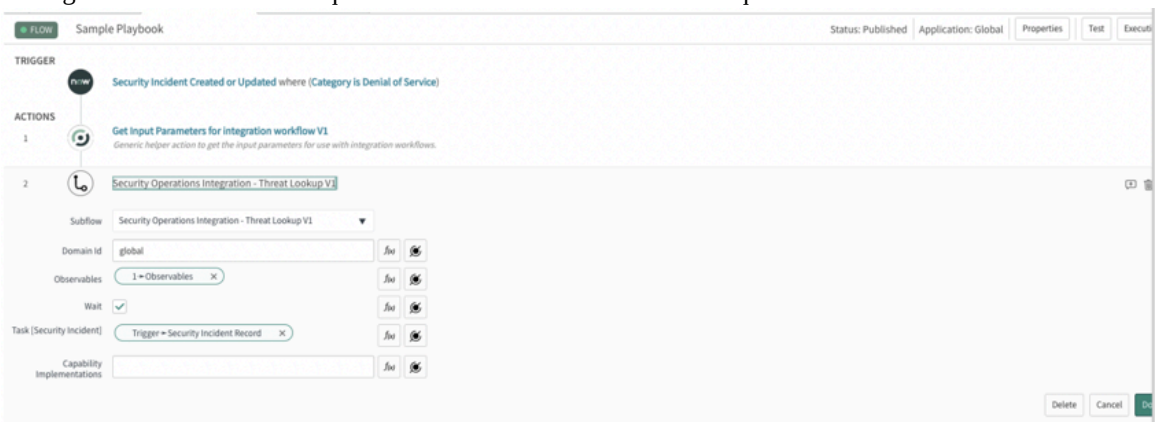
5. À l'étape 2, sélectionnez un flux secondaire (par exemple, Recherche de menace).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Configurez le flux secondaire que vous avez sélectionné comme indiqué ci-dessous :



7. Enregistrez et publiez le flux.

Dépannage des flux d'aptitude d'intégration

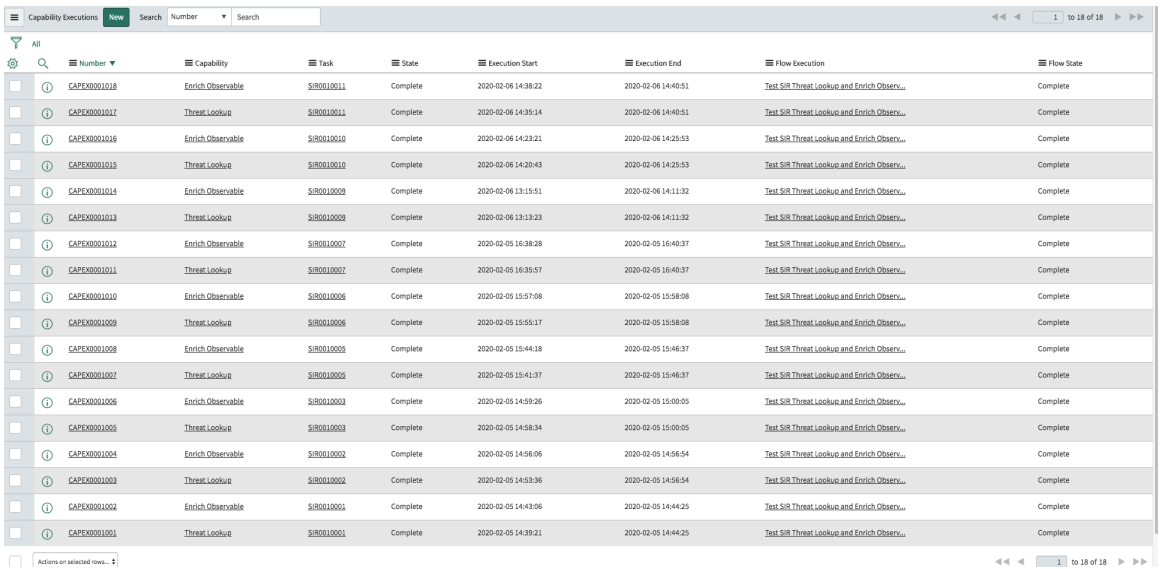
L'option Exécutions des aptitudes fournit des informations détaillées sur chaque aptitude exécutée.

Remarque : Les exécutions terminées sont archivées au bout de 30 jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Security Operations** > **Intégrations** > **Exécutions des aptitudes.**.



2. Cliquez sur le lien Exécutions des aptitudes pour afficher des détails supplémentaires.

`Notes de travail de l'enregistrement de l'incident de sécurité`

Lorsque des observables ont été ajoutés à un incident de sécurité et que la condition de déclenchement du flux est remplie, les flux secondaires Recherche de menace et Enrichissement des observables sont lancés et les notes de travail suivantes sont ajoutées à l'incident de sécurité :

- L'exécution du flux a commencé : Security Operations Integration - Enrichir l'observable V1
- Exécution de flux terminée : Security Operations Integration - Enrichir l'observable V1
- L'exécution du flux a commencé : Security Operations Integration : recherche de menace V1
- Exécution de flux terminée : Security Operations Integration : recherche de menace V1

Pour afficher ces notes de travail, connectez-vous en tant qu'utilisateur avec *`les rôles sn_si.admin`* ou *`sn_si.analyst`*, *`flow_designer`* et *`action_designer`* .

Accédez à la page d'enregistrement de l'incident de sécurité et cliquez sur ces notes de travail pour afficher les détails de l'exécution du flux.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

API REST pour l'intégration tierce avec Security Operations

Le Opérations de sécurité système de base comprend une série d'API REST scriptées qui permettent aux clients et aux partenaires de s'intégrer facilement à un déploiement existant Opérations de sécurité . Les API vous permettent de collecter des données en dehors de votre système (par exemple, un script Python est utilisé pour recevoir des données de VirusTotal) et de les renvoyer à votre instance.

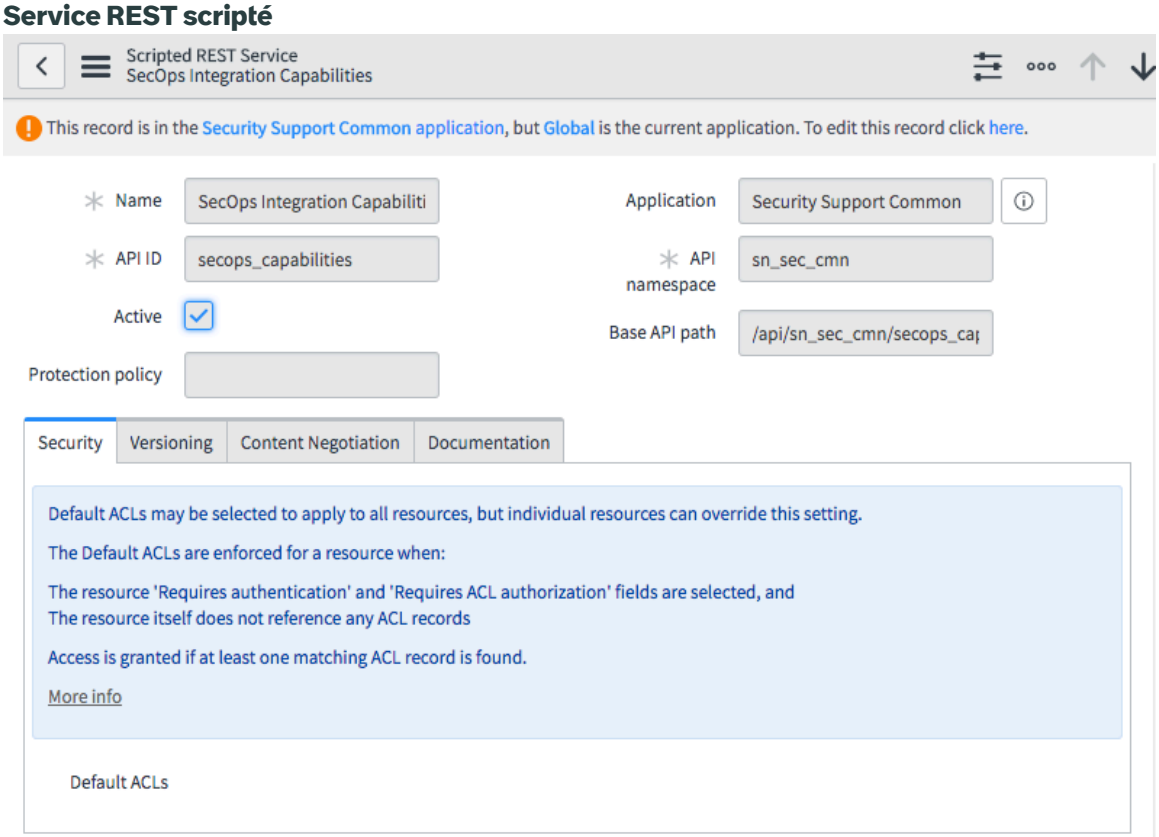
Les scripts écrits dans presque tous les langages (Python, par exemple) peuvent être utilisés avec les API pour effectuer des processus spécifiques au client. Les scripts doivent être écrits dans un langage capable d'effectuer un appel HTTP Post orienté vers l'extérieur. Par exemple, si vous avez une application Java, vous devez utiliser une bibliothèque, telle que le package `java.net.HttpUrlConnection` , pour construire un appel HTTP et transmettre une chaîne JSON en tant que corps du message.

L'API est uniquement utilisée pour ajouter des données qui ont été collectées en dehors de notre système. Par exemple, si vous avez saisi un script Python VT et reçu des données de VT, vous pouvez renvoyer ces données à l'instance SN.

Authentification

Toutes les opérations dans les définitions d'API utilisent l'authentification de plateforme fournie par le Fonctionnalité d'opération des API REST basées sur un script . Pour y accéder, accédez à **Services web du système** > **Services Web basés sur un script** > **API REST basées sur un script** et localisez l'API des **options d'intégration SecOps** .

Service REST scripté



L'utilisateur et le domaine de l'utilisateur sont facilement disponibles dans le contexte de l'API. Les enregistrements peuvent être liés à un utilisateur, un chemin d'audit à établir et la séparation de domaine peut être effectuée. De plus, puisque vous êtes authentifié en tant qu'utilisateur spécifique, vous pouvez utiliser Utilisation de GlideRecordSecure pour empêcher tout accès non autorisé aux données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisation

Pour protéger le processus de création d'enregistrement des utilisateurs extérieurs à l'application Opérations de sécurité , vous devez disposer du rôle sn_sec_cmn.api_write . Seuls les utilisateurs disposant de ce rôle peuvent accéder aux API.

Paramètres de demande de configuration

Les paramètres de demande suivants sont disponibles.

Nom	Par défaut	Description
ignore_mandatory_fields	Faux	Si la valeur est définie sur vrai, l'enregistrement persiste même si les champs obligatoires ne sont pas renseignés.
include_wrap	Faux	Si la valeur est définie sur vrai, la réponse inclut la couche standard fournie par l'instance pour les API REST scriptées.
simple_response	Faux	Si la valeur est définie sur vrai, la réponse indique uniquement si l'opération a réussi.

Réponses d'erreur

Les réponses d'erreur suivantes peuvent se produire.

Message d'erreur	Quand cela se produit-il ?	Solution
Accès insuffisant	L'utilisateur ne dispose pas du rôle sn_sec_cmn.api_write.	Ajoutez le rôle à l'utilisateur.
Corps de publication non valide	Le corps de la demande est vide ou un objet vide.	Conforme à la définition de l'API.
Aucun champ fourni	Les champs de données fournis pour la conservation sont vides.	Conforme à la définition de l'API.
Champs obligatoires manquants : x,y,z	Les champs obligatoires sont manquants.	Conformez-vous à la définition de table de la table cible ou définissez **ignore_mandatory_fields** sur vrai.
Impossible de conserver l'enregistrement	Impossible de conserver l'enregistrement analysé.	Échec de l'insertion de GlideRecord. Une analyse plus approfondie est requise.
Erreur inconnue	Se produit si aucun chemin d'erreur connu n'a été suivi.	Une analyse plus approfondie est nécessaire.

Cas d'utilisation d'enrichissement de CI

À l'aide de vos scripts tiers, vous pouvez écrire dans la table Enrichissement des éléments de configuration [sn_sec_cmn_ci_enrichment_result] pour l'enrichissement des CI. Les enregistrements d'enrichissement sont basés sur des options existantes qui fournissent des informations détaillées sur un enregistrement provenant d'une source tierce.

Des exemples de demandes et de réponses pour le cas d'utilisation d'enrichissement des CI sont affichés ici.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une demande d'enrichissement de CI


```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```


Créer une réponse pour l'enrichissement de CI


```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```


Traduction automatique

Cas d'utilisation de l'enrichissement d'observable

À l'aide de vos scripts tiers, vous pouvez écrire dans la table Résultat de l'enrichissement des observables [sn_ti_observable_enrichment_result] pour l'enrichissement des observables. Les enregistrements d'enrichissement sont basés sur des options existantes qui fournissent des informations détaillées sur un enregistrement provenant d'une source tierce.

Des exemples de demande et de réponses pour le cas d'utilisation d'enrichissement d'observables sont présentés ici.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une demande d'enrichissement de l'observable


```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```


Créer une réponse pour l'enrichissement des observables


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```


Remarque : En plus d'enrichir les enregistrements existants, vous pouvez également Opérations de sécurité Mappage des données d'enrichissement ajouter de nouveaux enregistrements à des tables en transmettant un **enrichment_mapping_id** pour un mappage d'enrichissement existant et une chaîne **de raw_data** correspondante qui peut être analysée par le processus de mappage.

Cas d'utilisation de la recherche de menace

À l'aide de vos scripts tiers, vous pouvez écrire dans la table Résultat de la recherche de menace [sn_ti_lookup_result] pour obtenir les résultats de la recherche de menace. Les enregistrements de recherche sont basés sur les options existantes qui fournissent des informations détaillées sur un enregistrement provenant d'une source tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des exemples de demandes et de réponses pour le cas d'utilisation de la recherche de menaces sont présentés ici.

Créer une demande de recherches de menaces


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une réponse pour les recherches de menaces


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


Options d'intégration

Le Options d'intégration cadre de travail fournit une architecture cohérente pour prendre en charge l'interopérabilité avec les intégrations tierces. Cette interface abstraite et ce modèle de données isolent les intégrations des modifications apportées à l'application principale et garantissent une expérience cohérente pour des types d'intégrations similaires.

Chaque option d'intégration est conservée dans la table Aptitude d'intégration [sn_sec_cmn_integration_capability]. Les flux d'aptitude d'intégration ne peuvent pas être exécutés seuls et nécessitent le lancement d'un flux d'implémentation. Tout module d'extension qui fournit une implémentation de l'aptitude ajoute son implémentation à la table enfant : Implémentation de l'option d'intégration [sn_sec_cmn_integration_capability_implementation].

L'implémentation spécifie le flux à exécuter, l'intégration connexe (ID de module d'extension) et l'aptitude qu'elle implémente. Ces flux peuvent être exécutés en parallèle à l'aide du lanceur de flux parallèle ; Toutefois, l'exécution séquentielle est la valeur par défaut dans le système de base. Si nécessaire, vous pouvez modifier l'ordre d'exécution.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

Security Operations Integration : option Demande de bloc

L'aptitude Bloquer l'action bloque les observables associés à un incident de sécurité sur un pare-feu, un proxy web ou tout autre point de contrôle à l'aide de flux de mise en œuvre. Cette aptitude est utilisée au cours des enquêtes de réponse à un incident pour contenir une menace identifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’aptitude Demande de bloc a un flux, Security Operations Integration - Bloquer le flux de demande, qui exécute la demande de blocage. Ce flux accepte une liste d’observables, recherche toutes les options d’implémentation et exécute la demande en fonction du flux configuré.

Remarque : Si aucune implémentation n’est disponible, les actions d’aptitude ne sont pas affichées dans les menus de produits.

Exécuter une demande de bloc

Bloque la communication avec les observables associés à un incident de sécurité.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

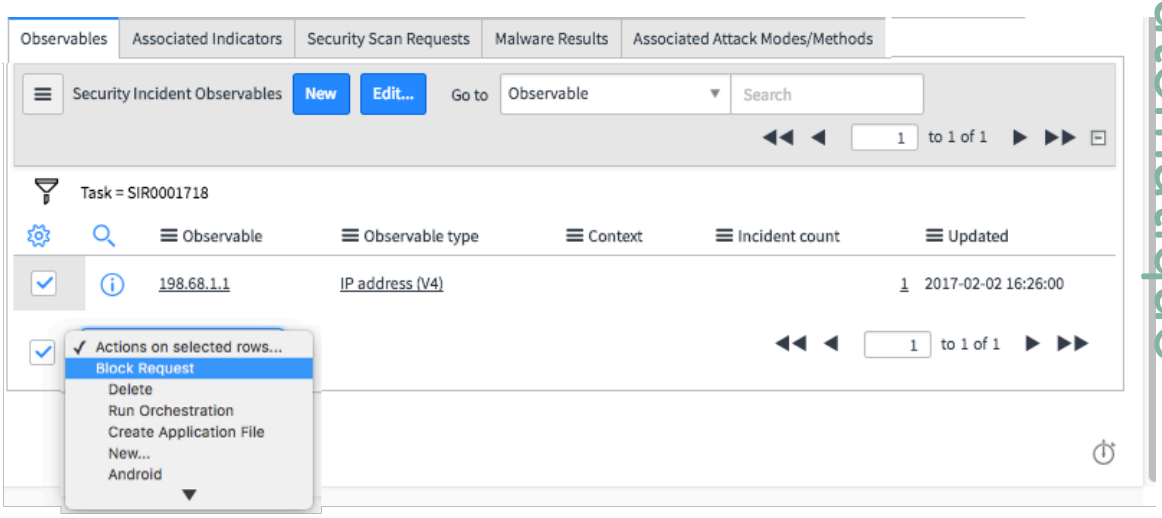
Remarque : Si aucune implémentation n’est disponible, les actions d’aptitude ne sont pas affichées dans les menus de produits.

Le flux Security **Operations Integration - Block Request** peut être déclenché à partir d’un formulaire observable ou de la liste connexe **Observables d’incident de sécurité** sur un incident de sécurité.

Cet exemple montre une demande de bloc à partir d’un incident de sécurité.

Procédure

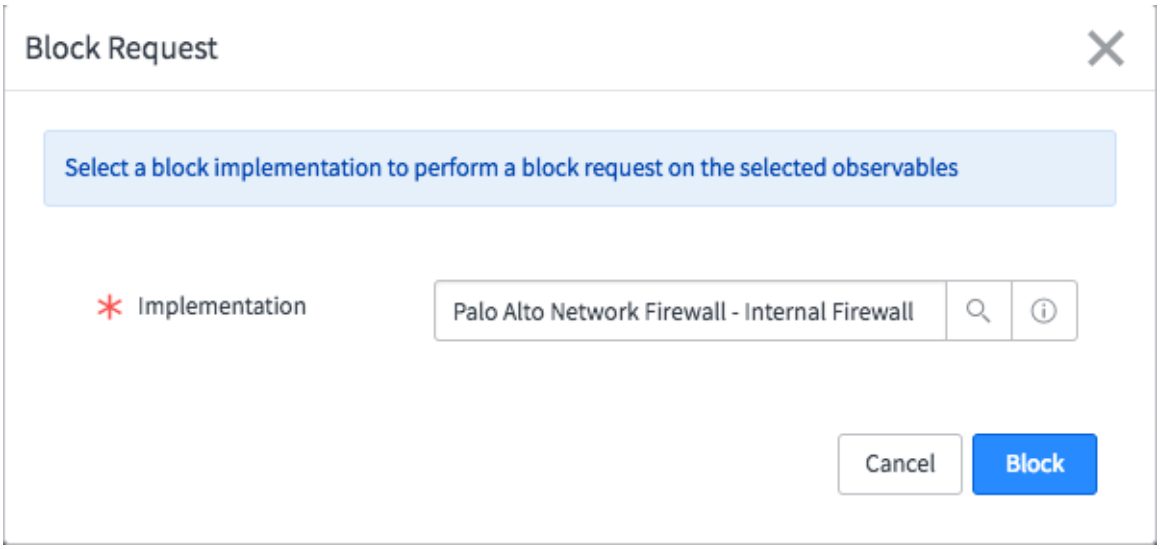
1. Accédez à un incident de sécurité.
2. Sélectionnez des observables dans l’onglet **Liste connexe** .
3. Cliquez sur **Bloquer la demande** dans le menu déroulant **Actions sur les lignes sélectionnées...**



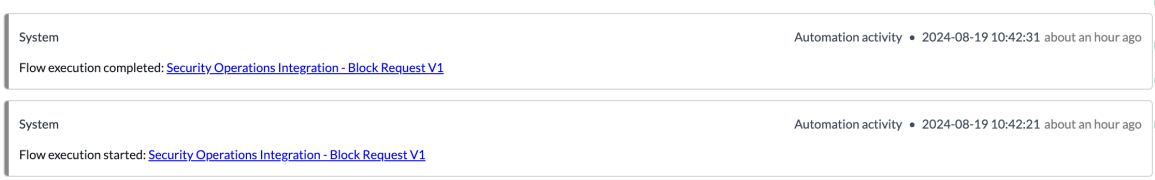
La boîte de dialogue s’affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Choisissez l’implémentation.
5. Cliquez sur **Bloquer**.
   L’audit d’exécution du flux s’affiche dans la section Notes de travail.



Security Operations Integration - Bloquer le flux de demande

Le flux Intégration de Security Operations : demande de bloc est un flux de haut niveau indépendant des intégrations. Il bloque les observables associés à un incident de sécurité. Utilisez-le pour réaliser une intégration telle que Palo Alto Networks - Firewall.

Le flux Security **Operations Integration - Block Request** peut être déclenché sur un formulaire d’observable ou à partir de la liste connexe **Observables d’incident de sécurité** sur un incident de sécurité. Sur une liste, il se trouve dans le menu d’action déroulant. Sur un formulaire, il s’agit d’un lien connexe. Le blocage d’une demande n’est disponible que lorsqu’une implémentation est installée pour l’aptitude de demande de bloc.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Bloquer la demande



Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Security Operations Integration : option de recherche et de suppression d'e-mails

L'option Recherche et suppression d'e-mails renvoie le nombre d'e-mails de menace à partir d'une recherche sur le serveur de messagerie et, éventuellement, renvoie les détails de chaque e-mail trouvé. Une fois la recherche d'e-mails terminée, vous pouvez supprimer les e-mails.

L'option Recherche et suppression d'e-mails comporte un flux qui exécute les processus de recherche et de suppression d'e-mails.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits. En outre, si aucune des implémentations des aptitudes **Recherche et Suppression d'e-mails** n'est active, le lien connexe **Recherche d'e-mails** sur un incident de sécurité ne s'affiche pas.

Security Operations Integration : flux de recherche et de suppression d'e-mails

Le flux Security Operations Integration - Recherche et suppression d'e-mails renvoie le nombre d'e-mails de menace à partir d'une recherche sur le serveur de messagerie et, éventuellement, renvoie les détails de chaque e-mail trouvé. Une fois la recherche d'e-mails terminée, vous pouvez supprimer les e-mails.

Avant de commencer
Rôle requis : sn_si.analyst

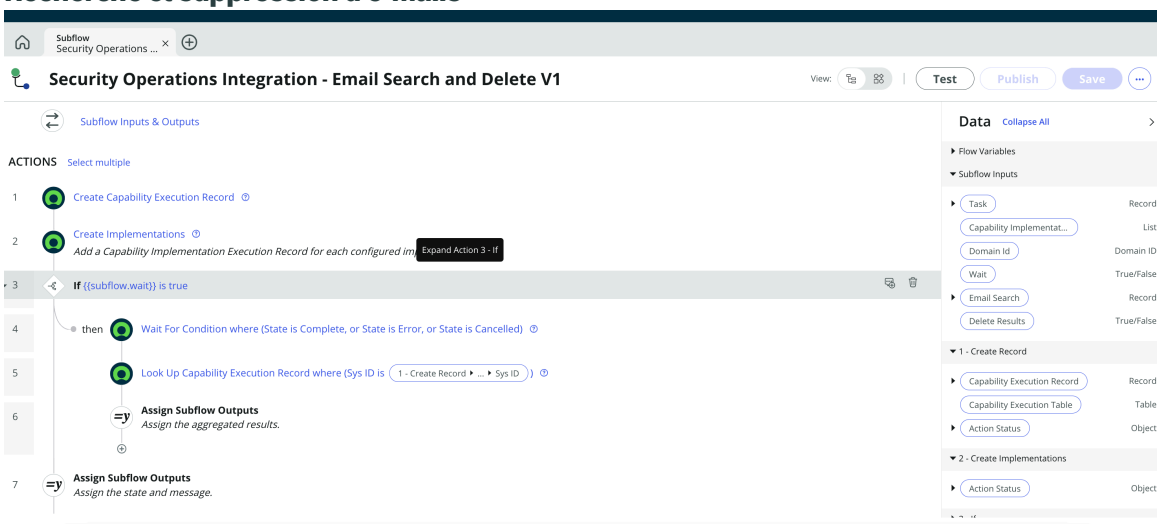
Pourquoi et quand exécuter cette tâche
La requête de recherche peut prendre un certain temps. Une fois le décompte reçu, une approbation est requise pour supprimer les e-mails d'un serveur de messagerie.

Ce flux est déclenché par les boutons **Supprimer des serveurs de messagerie** et **Rechercher sur les serveurs de messagerie** du formulaire **Recherche d'e-mail** dans un incident de sécurité. Pour plus d'informations, consultez Rechercher et supprimer des e-mails d'hameçonnage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche et suppression d'e-mails



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Les activités du processus de flux comprennent :

Suivi des exécutions : action Commencer (recherche de courrier)

L'action d'exécution de l'aptitude Suivi de l'exécution - Commencer (recherche de courrier) crée un enregistrement de suivi de l'exécution et marque l'état de l'enregistrement comme Démarré. Cette action est utilisée par tous les flux d'aptitude et d'implémentation pour suivre leur état.

Résultats

Les résultats possibles pour cette action sont les suivants :

Résultats

Résultat	Description
Réussite	Un enregistrement de suivi des exécutions a été créé.
Échec	Impossible de créer un enregistrement de suivi de l'exécution.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variable	Description
capabilityId	Identificateur système de l'option d'intégration en cours d'exécution.
ID implémentation	Identificateur système de l'implémentation de l'option d'intégration en cours d'exécution.
taskId	Identificateur système pour toute tâche associée au flux.
flowContextId	L'identificateur système de l'enregistrement de contexte de flux associé. Fourni par le système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
nom du flux	Nom du flux. Fourni par le système.
parentCapabilityExcutionId	Identificateur système de l'enregistrement d'audit qui a lancé le flux d'implémentation. Uniquement requis pour les flux d'implémentation de l'option d'intégration, tels que Splunk, Elasticsearch.
emailsearchId	Sysid de l'enregistrement de recherche d'e-mail dans la table Recherche d'e-mail [sn_sec_cmn_email_search].

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
capabilityExecutionId	Identificateur système de l'enregistrement de suivi de l'exécution.

- Action Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune action d'implémentation

Security Operations Integration : enrichir l'aptitude CI

La fonctionnalité Enrichir le CI vous permet d'enrichir les données pour les éléments de configuration associés à un incident de sécurité.

L'aptitude **Enrichir le CI** a un flux, Security Operations Integration - Flux d'enrichissement CI. Lorsque le flux d'aptitude s'exécute, il exécute des flux supplémentaires pour les implémentations activées. Vous pouvez spécifier une implémentation à utiliser pour effectuer l'enrichissement sur les CI sélectionnés, ou vous pouvez effectuer l'enrichissement en utilisant toutes les implémentations.

Remarque : Ces données enrichies ne sont pas le type de données que vous souhaitez stocker dans votre CMDB, car il s'agit de données d'expertise spécifiques à une enquête donnée, par exemple, l'exécution d'un memdump à partir d'un CI. Au lieu de cela, les données sont stockées dans la table Enrichissement des éléments de configuration [sn_sec_cmn_ci_enrichment_result].

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

Security Operations Integration - Flux d'enrichissement CI

Le flux d'enrichissement de CI d'intégration de Security Operations vous permet d'enrichir les données des éléments de configuration (CI) associés à un incident de sécurité.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Ce flux est déclenché de Réponse aux incidents de sécurité deux manières.

Traduction automatique

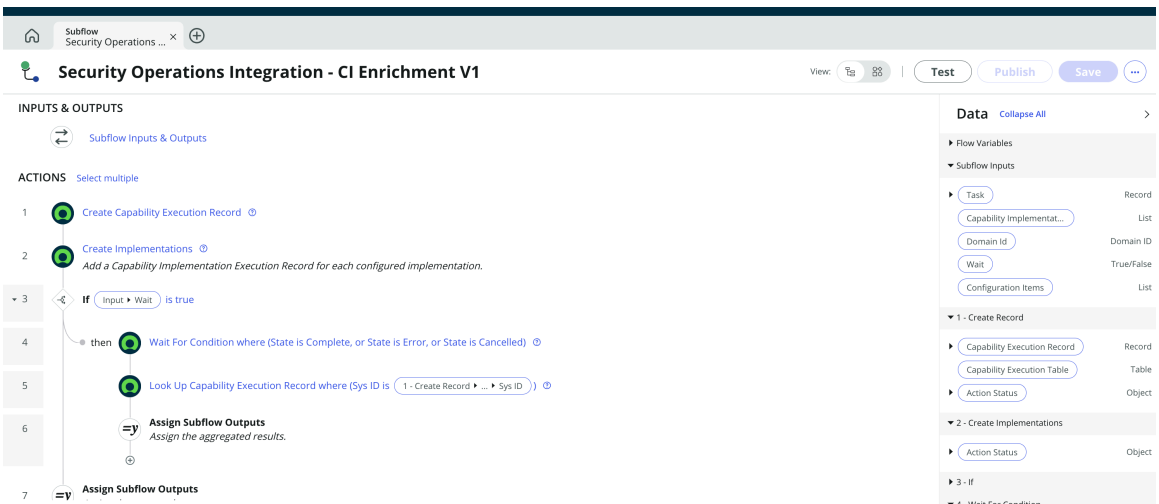
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- en sélectionnant un ou plusieurs CI dans l'onglet **Éléments de configuration** (sous le lien connexe **Éléments affectés**) et en sélectionnant **Exécuter l'enrichissement de CI** dans la liste de choix **Actions sur les lignes sélectionnées** .
- en ouvrant un enregistrement de CI et en cliquant sur le lien connexe **Exécuter l'enrichissement de CI** .

L'une ou l'autre méthode vous permet ensuite de spécifier les implémentations à utiliser pour enrichir les CI sélectionnés. Les flux d'implémentation associés sont exécutés pour effectuer l'enrichissement.

Remarque : Le système de base n'inclut pas de flux d'implémentation pour cette option. Pour enrichir les CI, vous devez créer votre propre flux d'implémentation.

Enrichissement de CI



Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Les actions de processus de flux comprennent :

- Suivi de l'exécution : commencer l'action de flux
- Security Operations Integration - Flux d'enrichissement CI
- Suivi de l'exécution de l'aptitude : aucune action d'implémentation
- Action Obtenir les options de sécurité prises en charge

Security Operations Integration : enrichir l'aptitude des observables

La fonctionnalité Enrichir les observables vous permet d'enrichir les observables avec des informations supplémentaires issues de diverses sources à l'aide de flux de mise en œuvre. Cette aptitude est utilisée au cours des enquêtes de réponse à un incident pour contenir une menace identifiée.

L'aptitude Enrichir l'observable comporte un flux, Security Operations Integration - Enrichir le flux des observables. Lorsque le flux d'aptitude s'exécute, il exécute des flux supplémentaires pour les implémentations activées. Vous pouvez spécifier une implémentation à utiliser pour effectuer un enrichissement sur les observables sélectionnés, ou vous pouvez effectuer l'enrichissement en utilisant toutes les implémentations qui correspondent aux types d'observables pris en charge.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

Security Operations Integration - Enrichir le flux des observables

Le sous-flux Intégration de Security Operations - Enrichir les observables vous permet d'enrichir les observables avec des informations supplémentaires issues de diverses sources à l'aide de Concepteur de flux d'implémentation.

Avant de commencer

Rôle requis : sn_si.analyst

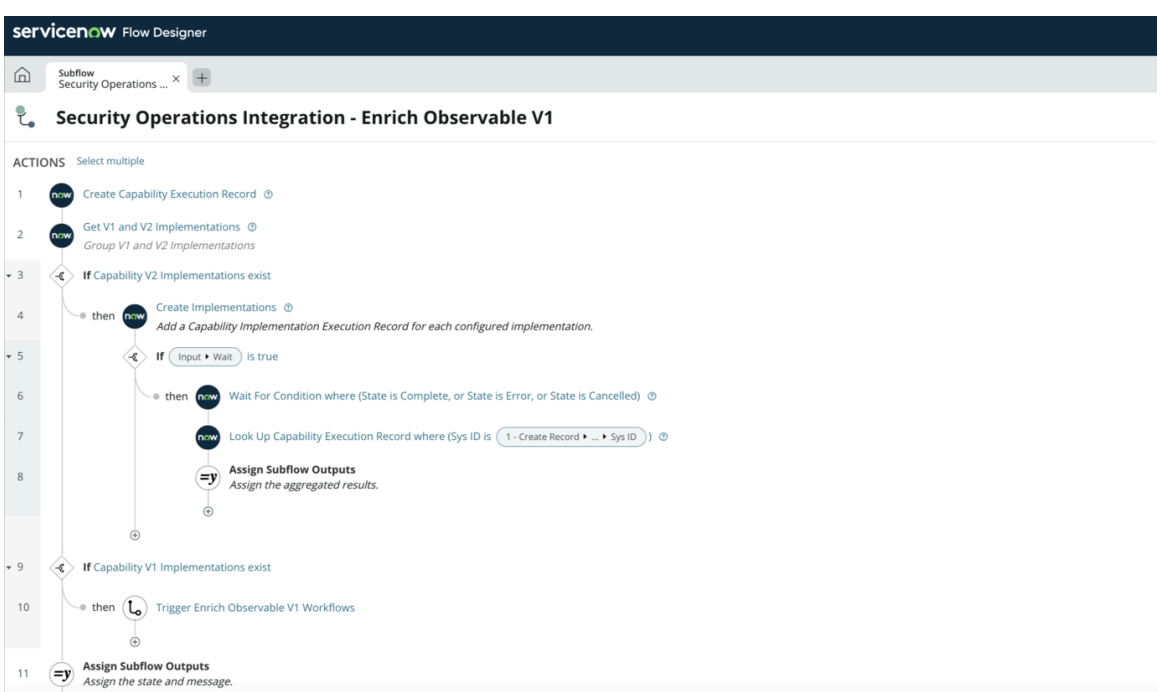
Pourquoi et quand exécuter cette tâche

Ce flux peut être déclenché de deux Réponse aux incidents de sécurité manières ou Renseignements sur les menaces de deux façons.

- en sélectionnant un ou plusieurs observables dans la liste Observables et en sélectionnant **Exécuter l'enrichissement de l'observable** dans la liste de choix **Actions sur les lignes sélectionnées** .
- En ouvrant un enregistrement d'observable et en cliquant sur le lien connexe **Exécuter l'enrichissement de l'observable** .

L'une ou l'autre méthode vous permet ensuite de spécifier les implémentations à utiliser pour enrichir les observables sélectionnés. Les flux d'implémentation associés sont exécutés pour effectuer l'enrichissement.

Enrichir l'observable



Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Les actions de processus de flux comprennent :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Suivi de l’exécution de l’aptitude : aucune action d’implémentation
- Action Obtenir les options de sécurité prises en chargeSuivi de l’exécution de l’aptitude : aucune action d’implémentation

Security Operations Integration : obtenir l’aptitude de statistiques réseau

L’aptitude Obtenir les statistiques réseau récupère une liste des connexions réseau actives à partir d’un hôte ou d’un point de terminaison. Il peut être utilisé pour l’enrichissement des incidents au cours des enquêtes. Cette aptitude est déclenchée automatiquement lorsqu’un élément de configuration est ajouté à un incident de sécurité.

L’aptitude **Obtenir les statistiques réseau** comporte un flux Intégrations Security Operations : obtenir le flux des statistiques réseau qui accepte un ou plusieurs CI et tâches. Le flux itère sur chaque implémentation et chaque CI et invoque à nouveau le flux d’implémentation.

Remarque : Si aucune implémentation n’est disponible, les actions d’aptitude ne sont pas affichées dans les menus de produits.

Intégrations Security Operations : obtenir le flux des statistiques réseau

Le flux Intégrations Security Operations - Obtenir les statistiques réseau récupère une liste des connexions réseau actives à partir d’un hôte ou d’un point de terminaison.

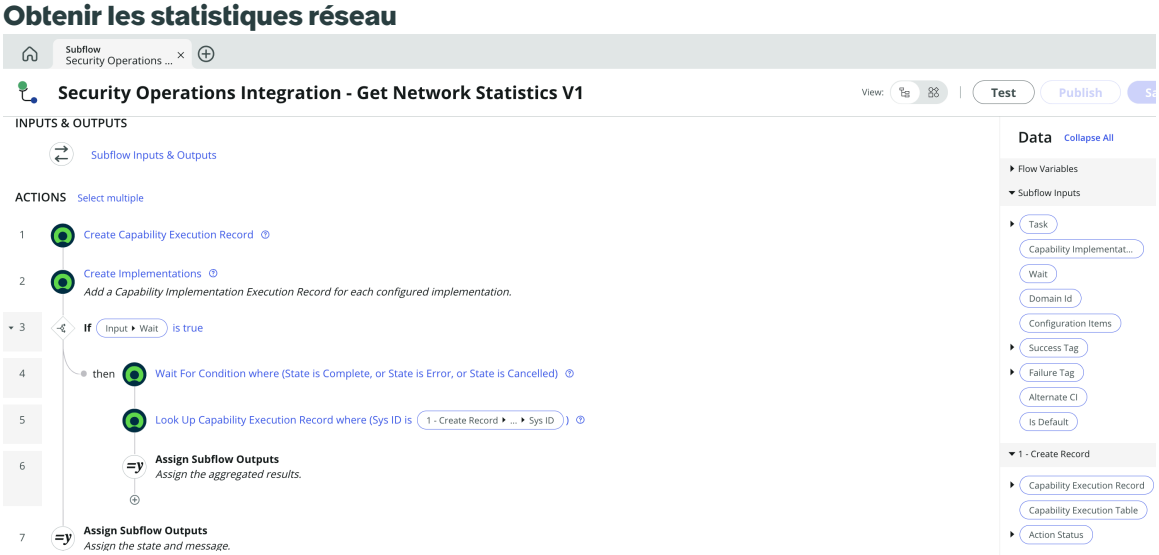
Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Ce flux s’exécute automatiquement lorsqu’un élément de configuration est ajouté à un incident de sécurité.

Obtenir les statistiques réseau



Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d’intégration et activités d’orchestration courants de Security Operations.

Les actions de flux comprennent :

- Aptitude : déterminer l’activité des CI
-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

.

Suivi des exécutions : commencer (CI) Action de flux

L'action de flux Suivi de l'exécution - Commencer (CI) démarre le processus d'audit pour un Opérations de sécurité flux d'intégration qui fonctionne sur les éléments de configuration (CI).

L'action de flux Suivi de l'exécution - Commencer (CI) peut être utilisée avec n'importe quel flux de CI pour commencer à enregistrer la progression du flux dans un audit.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Un enregistrement d'audit est créé.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
capabilityId	Identificateur système de l'option d'intégration en cours d'exécution.
isImpl	Marqueur qui spécifie si l'audit est effectué pour un flux d'aptitude d'intégration ou un flux d'implémentation d'option d'intégration. Les valeurs possibles sont les suivantes : • faux : désigne un audit sur un flux d'aptitude d'intégration abstrait tel que la recherche de perceptions. (par défaut). • vrai : désigne l'audit d'un flux d'implémentation d'option d'intégration. Par exemple, Splunk ou Elasticsearch.
taskId	Identificateur système pour toute tâche associée au flux.

ciList	Un ou plusieurs éléments de configuration (CI) sur lesquels effectuer l'action souhaitée au format suivant :
	`["sysId", "sysId"]`
	ou
	`"sysId"`
	Utilisé comme entrée de flux.

flowContextId	L'identificateur système de l'enregistrement de contexte de flux associé. Fourni par le système.
nom du flux	Nom du flux. Fourni par le système.
parentCapabilityExcutionId	Identificateur système de l'enregistrement d'audit qui a lancé le flux d'implémentation. Uniquement requis pour les flux d'implémentation de l'option d'intégration tels que Splunk, Elasticsearch.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
capabilityExecutionId	Identificateur système de l'enregistrement d'audit.

Les actions de processus de flux comprennent :

- Action Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune action d'implémentation

Security Incident Response - Obtenir le flux de statistiques réseau

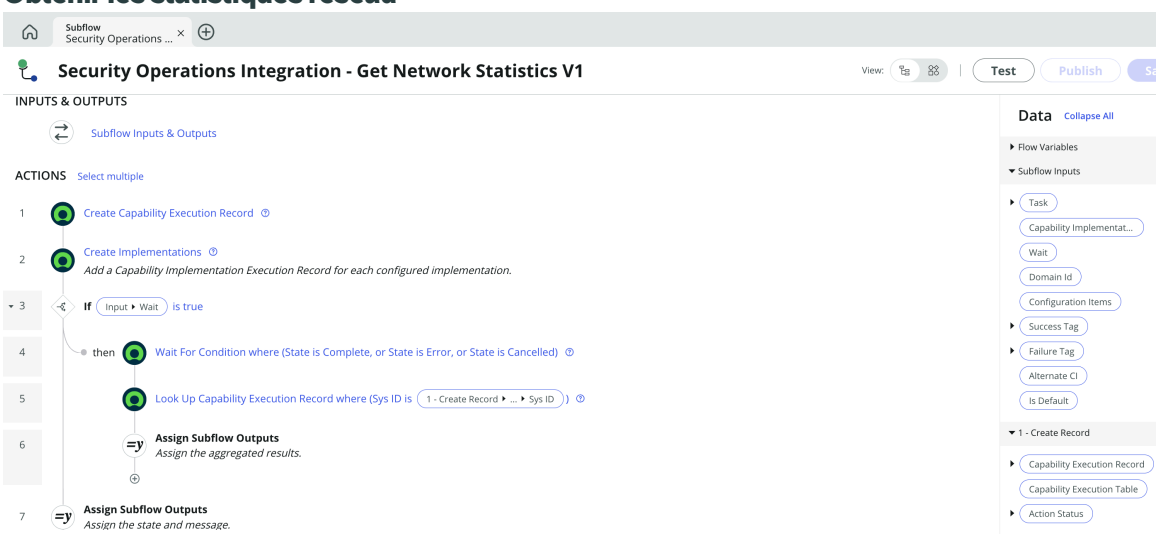
Le champ **Security Incident Response** > **Obtenir les statistiques réseau** le flux récupère les statistiques réseau d'une ressource Windows affectée lorsqu'elle est ajoutée à un incident de sécurité à l'état **Analyse** .

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Pour les nouveaux incidents de sécurité qui contiennent des éléments de configuration, le flux s'exécute automatiquement lorsque l'état passe à **Analyse**

Les incidents de sécurité existants sont automatiquement mis à jour lorsque vous êtes dans l'état **Analyse** et que vous ajoutez un nouvel élément de configuration.

Obtenir les statistiques réseau



Les actions de processus de flux comprennent :

Obtenir le FQDN de l'élément de configuration Action de flux

Déterminer le script Shell par système d'exploitation

Si l'instruction est exécutée par Powershell

Suivi de l'exécution : commencer l'action de flux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Obtenir les statistiques réseau via netstat Action de flux

Suivi de l’exécution de l’aptitude : action de flux d’échec

Créer des enregistrements de données d’enrichissement Action de flux

Suivi de l’exécution de l’aptitude : action de flux d’échec - Renvoie l’ID d’enrichissement.

Suivi de l’exécution de l’aptitude : terminer l’action de flux

Procédure

1. Ouvrez un incident de sécurité.
2. Mettez à jour **l’état** sur **Analyse**, si nécessaire.
3. Ajoutez un élément de configuration (ordinateur, serveur ou similaire).
4. Cliquez sur **Mettre à jour**.
   Orchestration de la réponse aux incidents de sécurité fournit des informations statistiques sur le réseau dans le **Liens connexes** > **Enrichissements des incidents de sécurité** onglet. Pour plus d'informations, reportez-vous à la section Opérations de sécurité Mappage des données d’enrichissement.

   Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d’intégration et activités d’orchestration courants de Security Operations.

Security Operations Integration : obtenir l’aptitude d’exécution des processus

L'option Obtenir l'exécution des processus récupère une liste des processus en cours sur un élément de configuration (CI) à partir d'un point de terminaison ou d'un hôte. Cette aptitude est utilisée pour enrichir les incidents au cours des enquêtes.

L’aptitude Obtenir l’exécution des processus comporte deux flux d’implémentation :

- Intégration de Security Operations Carbon Black : obtenir le flux d’exécution des processus
- Intégration des commandes du système Security Operations : obtenir le flux d’exécution des processus

Remarque : Si aucune implémentation n’est disponible, les actions d’aptitude ne sont pas affichées dans les menus de produits.

Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d’intégration et activités d’orchestration courants de Security Operations.

Intégration de Security Operations Carbon Black : obtenir le flux d’exécution des processus

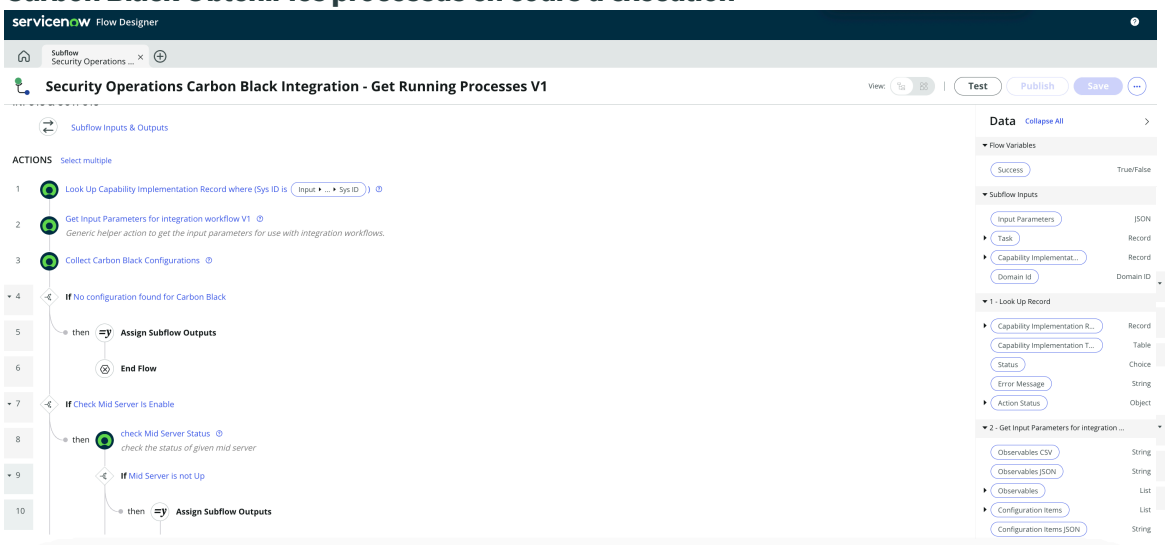
L’intégration de Security Operations Carbon Black : obtenir l’exécution des processus est l’implémentation de l’intégration Carbon Black lancée par le flux Intégration de Security Operations : obtenir l’exécution du processus.

Rôle requis : sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Carbon Black Obtenir les processus en cours d'exécution



Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Collecter les configurations Carbon Black Action de flux

L'action de flux Collecter les configurations Carbon Black rassemble les informations de configuration à utiliser dans le flux.

L'action de flux Collecter les configurations Carbon Black rassemble les informations de configuration de Carbon Black à utiliser dans le flux.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	La configuration a réussi.
Échec	Une erreur s'est produite lors de la tentative de vérification de la configuration. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Il n'existe aucune variable d'entrée pour cette action de flux.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
endpoint_base	URL de base de l'API d'intégration tierce.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
use_mid_server	Détermine si l'activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.
api_token	Clé API d'intégration tierce.

Vérifier l'état du Serveur MID

Détermine si le Serveur MID identifié dans le champ **Hôte du Serveur MID** de la configuration de l'intégration est actif et opérationnel. Si le champ est défini sur **N'importe lequel**, l'action de flux vérifie que n'importe quel serveur MID est actif et opérationnel.

L'action de flux Vérifier l'état du serveur MID peut être utilisée avec n'importe quel flux pour vérifier la présence d'un serveur MID en cours d'exécution dans le flux.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de la session est renvoyé.
Échec	Erreur d'état de la session. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
capabilityExecutionId	ID de l'option en cours d'exécution.
nom du flux	Le nom du flux en cours d'exécution.
mid_server_host	Serveur MID identifié dans la configuration de l'intégration i

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
mid_server_live	Identifie si le Serveur MID identifié dans le champ **Hôte du Serveur MID** de la configuration de l'intégration est actif et opérationnel. Si le champ est défini sur **N'importe lequel**, l'action de flux vérifie que n'importe quel serveur MID est actif et opérationnel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Obtenir l'ID de capteur Action de flux

L'action de flux Obtenir l'ID du capteur rassemble les identificateurs de capteur à utiliser dans le flux.

L'action de flux Obtenir l'ID de capteur peut être utilisée avec n'importe quel flux pour collecter des informations de capteur à utiliser dans le flux.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Identificateurs de capteurs trouvés.
Échec	Aucun capteur trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
api_token	Clé API Carbon Black.
use_mid_server	Détermine si l'activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.
endpoint_base	URL de base de l'API Carbon Black.
ci_ip_address	Adresse IP de l'élément de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code et un message d'erreur HTTP.
Type d'élément de tableau	Variables API.
sensor_detail	Description du capteur Carbon Black au format JSON.

Créer une action de flux de session

L'action Créer un flux de session établit une session Carbon Black à utiliser dans le flux.

L'action Créer un flux de session peut être utilisée avec n'importe quel flux pour créer une session Carbon Black dans le flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Session créée.
Échec	Session non créée. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
sensor_id	Identificateur de capteur.
use_mid_server	Détermine si l'activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code et un message d'erreur HTTP.
sortie	Variables d'API

Vérifier l'action de flux d'état de la session

Détermine l'état d'une session Carbon Black dans le flux.

L'action de flux Vérifier l'état de la session peut être utilisée avec n'importe quel flux pour vérifier l'état de la session Carbon Black dans le flux.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de la session est renvoyé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats (suite)

Résultat	Description
Échec	Erreur d'état de la session. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
session_id	Identificateur de session.
use_mid_server	Détermine si l'activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code et un message d'erreur HTTP.
sortie	Informations sur les processus d'exécution de Carbon Black.

Créer une action de flux de processus de commande

L'action Créer un flux de processus de commande crée un processus de commande Carbon Black à utiliser dans le flux .

L'action Créer un flux de processus de commande peut être utilisée avec n'importe quel flux pour créer un processus de commande Carbon Black dans le flux.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Processus de commande créé.
Échec	Processus de commande non créé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d’entrée déterminent le comportement initial de l’action de flux.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l’API Carbon Black.
session_id	Identificateur de session.
command_id	Identificateur de commande.
use_mid_server	Détermine si l’activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n’est pas le cas, affiche un code et un message d’erreur HTTP.
sortie	Variables d'API

Vérifier le statut de la commande et obtenir l’action du flux de processus

Vérifie l’état de la commande Carbon Black et récupère les processus à utiliser dans le flux.

L’action Vérifier l’état de la commande et obtenir le flux de processus peut être utilisée avec n’importe quel flux pour vérifier l’état d’une commande Carbon Black et obtenir des processus dans le flux.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	État de la commande renvoyé et processus créés.
Échec	État de la commande ou erreur de processus. Plus d’informations sur l’erreur sont disponibles dans l’erreur de sortie de l’action de flux.

Variables d'entrée

Les variables d’entrée déterminent le comportement initial de l’action de flux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
session_id	Identificateur de session.
command_id	Identificateur de commande.
use_mid_server	Détermine si l'activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code et un message d'erreur HTTP.
sortie	Variables d'API

Action de flux de données des processus de mappage

L'action de flux de données de processus de carte mappe les données de processus Carbon Black dans le flux.

L'action Mapper le flux de données des processus peut être utilisée avec n'importe quel flux pour mapper les processus Carbon Black.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Processus mappés
Échec	Processus non mappés. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
affected_ci	Élément de configuration affecté.
implementation_id	Identificateur d'implémentation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
sortie	Données de retour formatées sur l'exécution des processus utilisés par le workflow abstrait.
processus	Liste des processus dans un tableau.

Suivi de l'exécution de l'aptitude : terminer l'action de flux

L'action Suivi de l'exécution de l'aptitude : terminer le flux met à jour l'enregistrement d'audit lorsque le flux est terminé.

L'action Suivi de l'exécution de l'aptitude : terminer le flux peut être utilisée avec n'importe quel flux pour enregistrer l'achèvement du flux.

Remarque : Le tableau Valeur de **retour** de l'action de flux principale du **lanceur parallèle** contient un tableau des résultats de tous les flux d'intégration exécutés et invite à terminer avec succès le suivi des exécutions.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de l'enregistrement d'audit est mis à jour et prend la valeur **Terminé**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
capabilityExecutionId	Identificateur système pour l'enregistrement d'audit. Ce champ était le résultat de l'une des activités Commencer l'audit.
nom du flux	Nom du flux. Fourni par le système.
message	Message d'achèvement.

Variables de sortie

Il n'existe aucune variable de sortie.

Fermer l'action de flux de la session

Ferme une session Carbon Black dans le flux.

L'activité Fermer la session peut être utilisée avec n'importe quel flux pour fermer une session Carbon Black.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	La session est close.
Échec	Session non fermée. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
api_token	Clé API Carbon Black.
endpoint_base	URL de base de l'API Carbon Black.
session_id	Identificateur de session.
use_mid_server	Détermine si l'activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code et un message d'erreur HTTP.
sortie	Variables d'API

Traduction automatique

Intégration des commandes du système Security Operations : obtenir le flux d'exécution des processus

Le flux d'intégration des commandes du système Security Operations : obtenir l'exécution des processus récupère les processus en cours d'exécution d'un élément de configuration lorsqu'il est ajouté ou mis à jour dans un incident de sécurité Windows ou Unix à l'état **Analyse** .

Avant de commencer
Rôle requis : sn_si.analyst

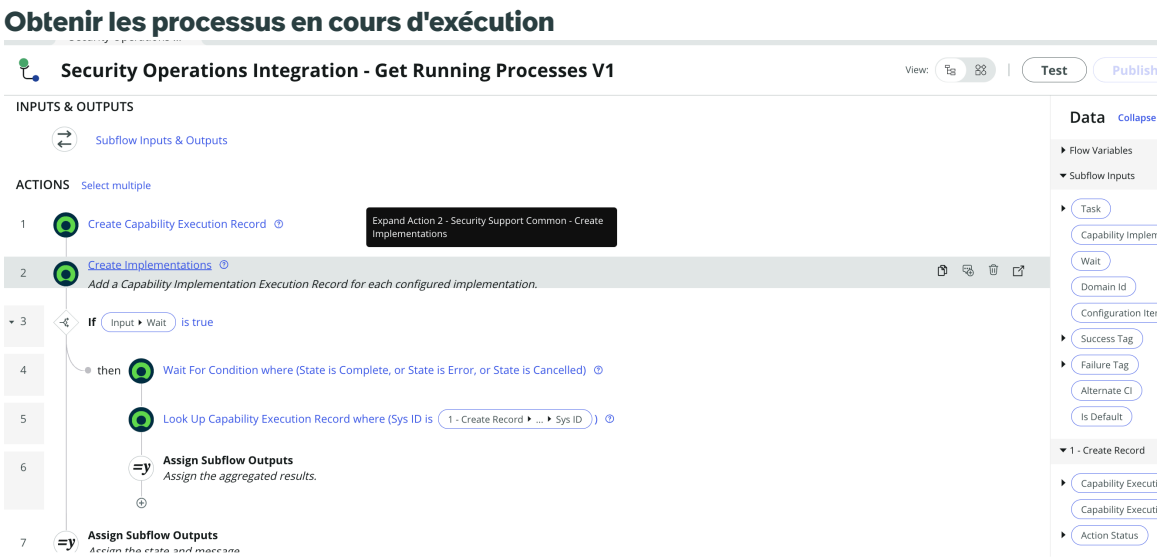
Pourquoi et quand exécuter cette tâche
Pour les nouveaux incidents de sécurité, le flux s'exécute automatiquement lorsque vous soumettez l'incident avec un élément de configuration sélectionné, lorsque l'état passe automatiquement à **Analyse**. S'il reste à l'état **Brouillon** , il ne s'exécute pas.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les incidents de sécurité existants sont automatiquement mis à jour lorsque vous êtes dans l'état **Analyse** et que vous ajoutez un nouvel élément de configuration.

Les actions de processus de flux comprennent :

- Obtenir le FQDN de l'élément de configuration Action de flux
- Déterminer le script Shell par activité du système d'exploitation
- Suivi de l'exécution : commencer l'action de flux
- Obtenir les exécutions de processus via PowerShell
- Exécuter l'activité de script Shell
- Suivi de l'exécution de l'aptitude : action de flux d'échec
- Extraire le script Shell de l'activité de script MID
- Combiner les résultats et les valeurs renvoyées dans un tableau
- Créer des enregistrements de données d'enrichissement Action de flux
- Suivi de l'exécution de l'aptitude : terminer l'action de flux



Procédure

1. Ouvrez un incident de sécurité.
2. Mettez à jour **l'état** sur **Analyse**, si nécessaire.
3. Ajoutez un élément de configuration (ordinateur, serveur ou similaire).
4. Cliquez sur **Mettre à jour**.
   Orchestration de la réponse aux incidents de sécurité Fournit des informations sur le processus en cours d'exécution dans le **Lien connexe** > **Enrichissements des incidents de sécurité**onglet. Pour plus d'informations, consultez Opérations de sécurité Mappage des données d'enrichissement.

   Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Combiner l'activité des résultats

L'activité de workflow Combiner les résultats fusionne les résultats provenant d'intégrations tierces à utiliser dans le workflow.

L'activité Combiner les résultats peut être utilisée avec n'importe quel workflow pour exécuter un script shell de Serveur MID dans le workflow.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Résultats combinés.
Échec	Échec de la combinaison. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
entrée A	Jeu de résultats A
entréeB	Jeu de résultats B
implementation_id	Identificateur d'implémentation.
affected_ci	Élément de configuration

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
résultat	Jeu de résultats A ou Jeu de résultats B en fonction de celui qui est renseigné.

Exécuter l'activité de script Shell

L'activité de workflow Exécuter le script Shell exécute un script shell de Serveur MID dans le workflow.

L'activité Exécuter le script Shell peut être utilisée avec n'importe quel workflow pour exécuter un script shell de Serveur MID dans le workflow.

Résultats

Les résultats possibles de cette activité sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Script Shell trouvé
Échec	Aucun script shell trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
target	Adresse IP ou nom de domaine complet (FQDN) du CI cible.
valeur du script	Script, en tant que valeur de chaîne, exécuté sur un système Unix.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
réponse	Sortie brute. Données des processus en cours d'exécution.

Extraire le script Shell de l'activité de script MID

L'activité de workflow Extraire le script Shell du script MID extrait un script shell de Serveur MID à utiliser dans le workflow.

L'activité Extraire le script Shell du script MID peut être utilisée avec n'importe quel workflow pour extraire un script shell de Serveur MID à inclure dans le workflow.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Script Shell trouvé
Échec	Aucun script shell trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
sysId	Identificateur système

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
valeur du script	Script, en tant que valeur de chaîne, exécuté sur un système Unix.

Obtenir les exécutions de processus via l'activité PowerShell

L'activité de workflow Obtenir l'ID de capteur rassemble les processus en cours d'exécution à l'aide de PowerShell pour les utiliser dans le workflow.

L'activité de workflow Obtenir l'exécution des processus via PowerShell peut être utilisée avec n'importe quel workflow pour récupérer les processus à inclure dans le workflow.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Processus trouvés
Échec	Aucun processus trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
target	Adresse IP ou nom de domaine complet (FQDN) du CI cible.
processingScript	Script ECC exécuté sur un système Windows.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
réponse	Sortie brute. Données des processus en cours d'exécution.

Traduction automatique

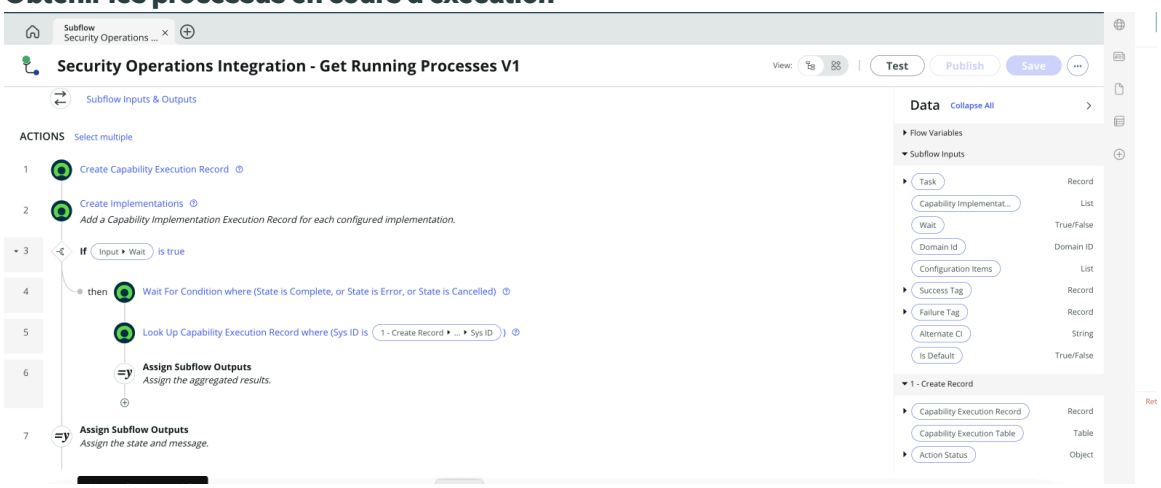
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opérations de sécurité : obtenir le flux d'exécution des processus

Le flux Opérations de sécurité : obtenir l'exécution des processus est un flux de haut niveau indépendant des intégrations. Il récupère une liste des processus en cours d'exécution sur un élément de configuration (CI) à partir d'un hôte. Utilisez-le pour réaliser une intégration, telle que Carbon Black, ou pour un incident de sécurité basé sur Windows.

Rôle requis : sn_si.analyst

Obtenir les processus en cours d'exécution



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Security Operations Integration : capacité d'isolement de l'hôte

La fonctionnalité **Isoler l'hôte** limite les connexions système à d'autres périphériques. L'option Isoler l'hôte est exécutée par rapport à un élément de configuration (CI).

L'aptitude **Isoler l'hôte** comporte un flux Opérations de sécurité : isoler le flux de l'hôte qui accepte un ou plusieurs CI et éventuellement une implémentation. Vous pouvez spécifier une implémentation à utiliser pour isoler l'hôte ou pour que le flux tente d'isoler l'hôte à l'aide de toutes les implémentations.

Remarque : Bien qu'il ne soit pas intégré à une aptitude, Security Operations Carbon Black Integration : supprimer le flux d'isolement de l'hôte un flux est disponible pour l'orchestration afin de restaurer la communication avec un hôte isolé.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

Exécuter Isoler l'hôte

L'option Isoler l'hôte restreint les connexions système à d'autres appareils.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

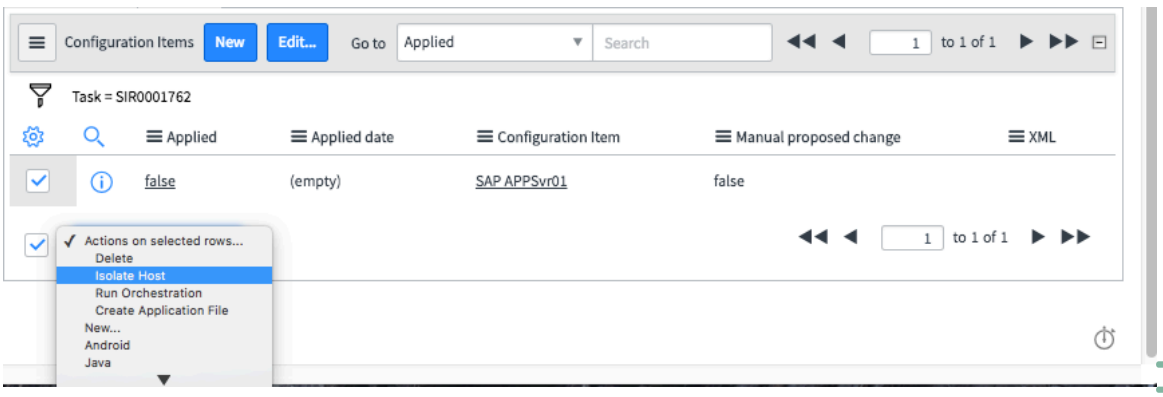
Le flux Security **Operations Integration - Isoler l'hôte ou le point de terminaison** peut être déclenché à partir de la liste connexe sur un incident de sécurité.

Traduction automatique

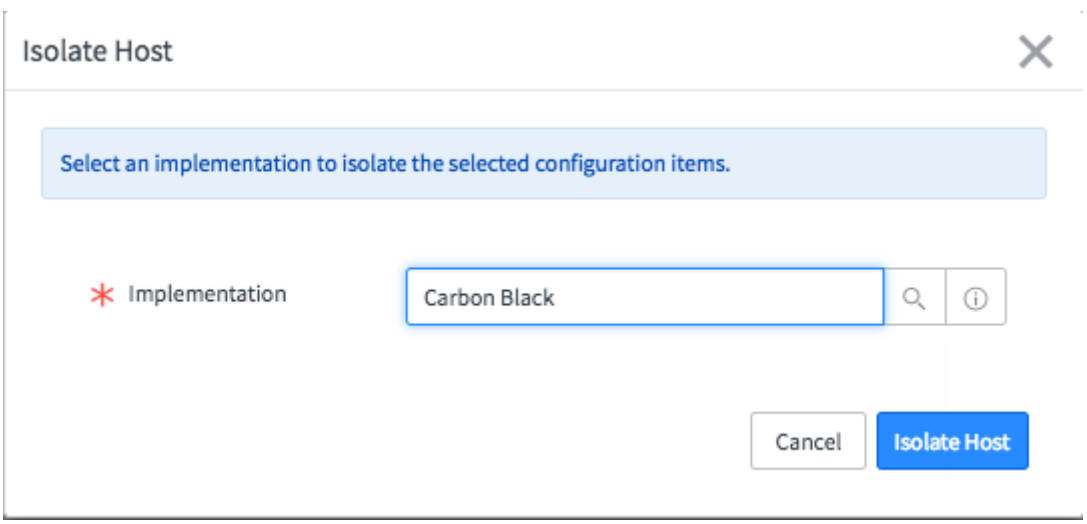
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

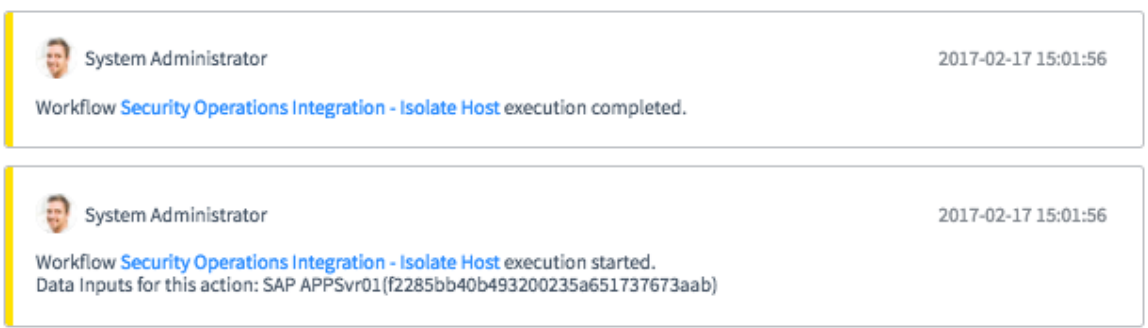
1. Accédez à un incident de sécurité.
2. Sélectionnez **des éléments de configuration** dans l'onglet **Liste connexe** .
3. Cliquez sur **Isoler l'hôte** dans le menu déroulant **Actions sur les lignes sélectionnées...**



La boîte de dialogue s'affiche.



4. Choisissez l'implémentation.
5. Cliquez sur **Isoler l'hôte**.
   L'audit d'exécution du flux s'affiche dans la section Notes de travail.



Traduction automatique

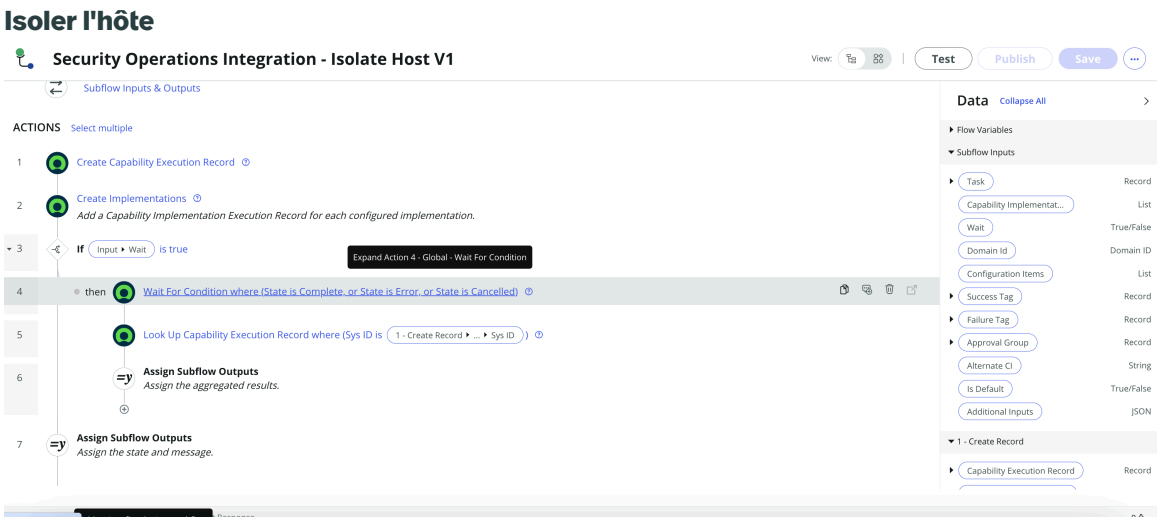
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opérations de sécurité : isoler le flux de l'hôte

Le flux **Security Operations - Isoler l'hôte** est un flux de haut niveau indépendant des intégrations. Il utilise les requêtes configurées pour rechercher un ensemble d'éléments de configuration. Utilisez-le pour réaliser une intégration, telle que Carbon Black.

Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Ce flux est déclenché à partir de l'onglet **Éléments de configuration** d'une liste connexe d'incidents de sécurité.



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Intégration de Security Operations Carbon Black : isoler le flux de l'hôte

L'intégration de Security Operations Carbon Black : isoler l'hôte est l'implémentation de l'intégration Carbon Black lancée par le flux d'intégration de Security Operations : isoler l'hôte.

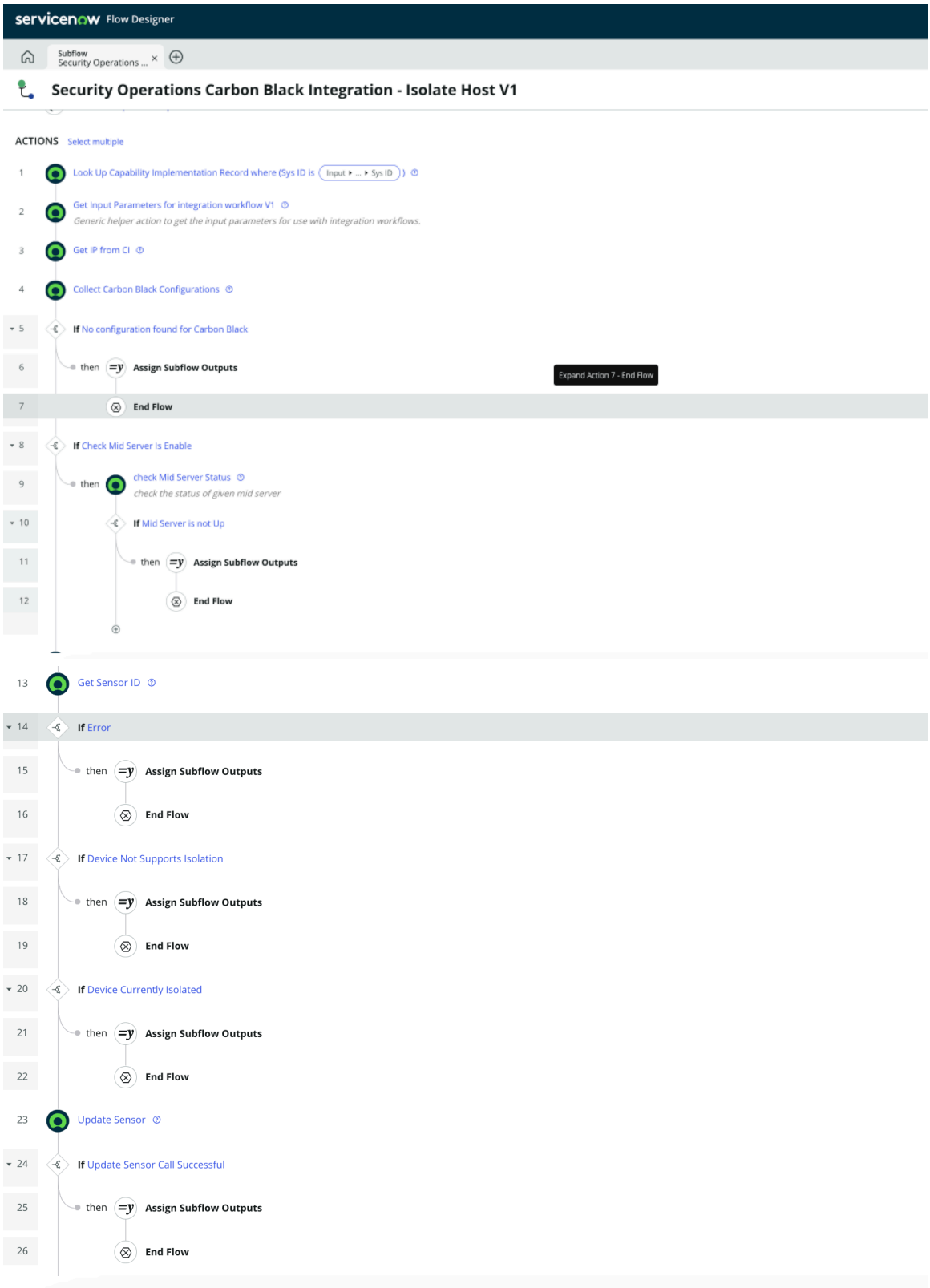
Avant de commencer
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche
Les activités du processus de flux comprennent :

- Suivi des exécutions : commencer (CI) Action de flux
- Obtenir l'adresse IP à partir du CI
- Recueillir les configurations Carbon Black
- Suivi de l'exécution de l'aptitude : action de flux d'échec
- Obtenir l'ID de capteur
- Activité Définir l'isolement réseau activé
- Mettre à jour le capteur : renvoie le résultat Isoler l'hôte.
- Suivi de l'exécution de l'aptitude : terminer l'action de flux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d’intégration et activités d’orchestration courants de Security Operations.

Obtenir l’ID de capteur Action de flux

L’action de flux Obtenir l’ID du capteur rassemble les identificateurs de capteur à utiliser dans le flux.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'action de flux Obtenir l'ID de capteur peut être utilisée avec n'importe quel flux pour collecter des informations de capteur à utiliser dans le flux.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Identificateurs de capteurs trouvés.
Échec	Aucun capteur trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
api_token	Clé API Carbon Black.
use_mid_server	Détermine si l'activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.
endpoint_base	URL de base de l'API Carbon Black.
ci_ip_address	Adresse IP de l'élément de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code et un message d'erreur HTTP.
Type d'élément de tableau	Variables API.
sensor_detail	Description du capteur Carbon Black au format JSON.

Activité Définir l'isolement réseau activé

L'activité de workflow Définir l'isolement réseau activée active l'isolement réseau.

L'activité Définir l'isolement réseau activé peut être utilisée avec n'importe quel workflow pour activer l'isolement réseau.

Résultats

Les résultats possibles de cette activité sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Isolation réseau activée.
Échec	L'isolation du réseau ne peut pas être activée. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
sensor_detail	Description du capteur Carbon Black au format JSON.
Désactiver	Détermine si l'hôte est isolé ou supprime l'isolement de l'hôte. Vrai = désactiver l'isolement Faux = l'isolement reste activé

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
sensor_detail	Description du capteur Carbon Black au format JSON.

Mettre à jour l'activité du capteur

L'activité de workflow Mettre à jour le capteur met à jour le capteur pour isoler les hôtes ou les points de terminaison.

L'activité Capteur de mise à jour peut être utilisée avec n'importe quel workflow pour isoler les hôtes ou les points de terminaison.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Capteur mis à jour.
Échec	Impossible de mettre à jour le capteur. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
api_token	Clé API Carbon Black.
use_mid_server	Détermine si l'activité REST utilise le serveur MID pour interagir avec Carbon Black ou non.
endpoint_base	URL de base de l'API Carbon Black.
sensor_id	Identificateur de capteur.
sensor_detail	Description du capteur Carbon Black au format JSON.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
status_code	Détermine si la demande a abouti. Si ce n'est pas le cas, affiche un code et un message d'erreur HTTP.

Security Operations Carbon Black Integration : supprimer le flux d'isolement de l'hôte

Le flux **d'intégration Security Operations Carbon Black - Supprimer l'isolement de l'hôte** débloque la communication avec un hôte ou un point de terminaison spécifié dans un système Carbon Black.

Avant de commencer
Rôle requis : sn_si.analyst

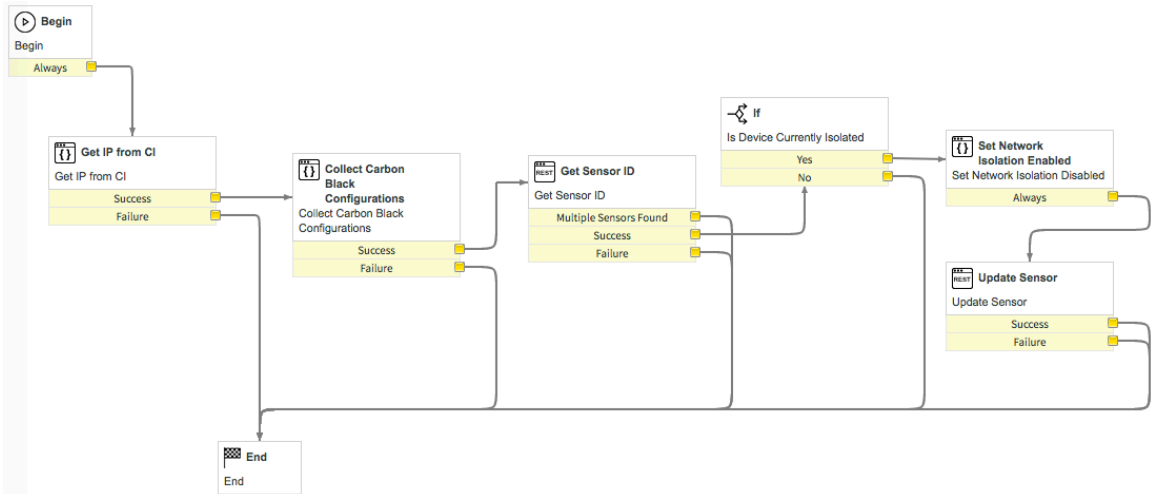
Pourquoi et quand exécuter cette tâche
Ce flux ne fait pas partie d'une option et a besoin d'une orchestration personnalisée pour s'exécuter.
Les activités du processus de flux comprennent :

- Obtenir l'adresse IP à partir de l'activité du CI
- En cas de réussite : Collecter les configurations Carbon Black Action de flux
- Obtenir l'ID de capteur Action de fluxObtenir l'ID de capteur
- Si l'appareil prend en charge l'isolement et l'appareil n'est pas isolé ou désactivé.
- Mettre à jour l'activité du capteur: renvoie le résultat de l'isolement de l'hôte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration Carbon Black : supprimer l'isolation de l'hôte



Security Operations Integration : aptitude de publication dans la liste de surveillance

L'aptitude Publier dans la liste de surveillance ajoute les observables et les indicateurs associés à un incident de sécurité à une liste de surveillance tierce qui surveille les événements de sécurité et génère des alertes. Cette aptitude est utilisée dans le cadre de la réponse aux incidents au cours des enquêtes.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

Security Operations Integration - Flux de publication dans la liste de surveillance

Le flux **d'intégrations Security Operations : publier dans la liste de surveillance** est un flux de haut niveau indépendant des intégrations. Il ajoute des observables à la liste de surveillance tierce qui prend en charge l'aptitude. Utilisez-le pour réaliser une intégration.

Avant de commencer

Rôle requis : sn_si.analyst

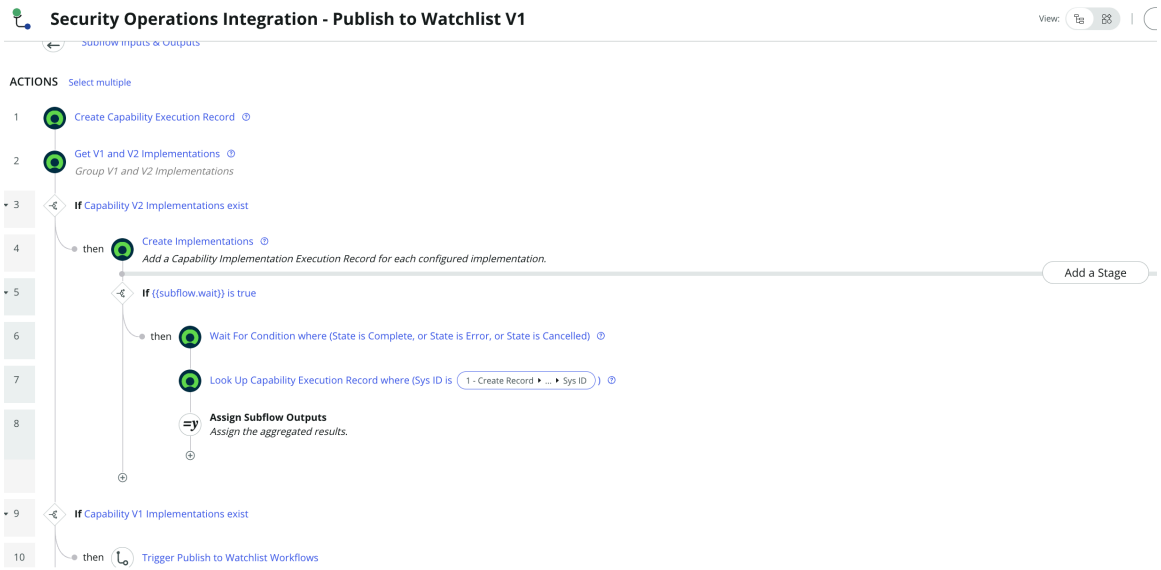
Pourquoi et quand exécuter cette tâche

Ce flux est visible et ne s'exécute que lorsqu'une intégration est disponible. Elle est déclenchée à partir de l'onglet **Observables** ou **Indicateurs associés** sur un incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Publier dans la liste de surveillance



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Security Operations Integration - Option de recherche de perceptions

L'aptitude Recherche de **perceptions** accepte un ensemble d'observables, recherche toutes les intégrations qui prennent en charge une recherche de perceptions, puis exécute ces recherches.

L'aptitude Recherche de perceptions a un workflow, Security Operations Integration - Flux de recherche de perceptions, qui exécute la recherche de perceptions. Ce workflow accepte une liste d'observables, recherche les options d'implémentation, crée les requêtes en fonction des configurations de recherche de perceptions et exécute les recherches en fonction du workflow configuré. Une fois la recherche terminée, une note est ajoutée aux notes de travail de l'incident indiquant si des observations ont été trouvées et, le cas échéant, combien.

Pour afficher les configurations de recherche de perceptions, accédez à **Security Operations** > **Intégrations** > **Configurations de la recherche de perceptions**.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

Créer des enregistrements de configuration de recherche de perceptions

Créez plusieurs enregistrements de configuration de recherche de perceptions et utilisez-les lors de l'interrogation de plusieurs magasins de journaux ou de la variation des paramètres de recherche.

Avant de commencer
Rôle requis : sn_si.admin

- Le module complémentaire CIM doit être installé sur l'instance Splunk.
- Les recherches enregistrées et les requêtes sur place sont prises en charge pour Splunk Integration uniquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous pouvez également créer des enregistrements de configuration de recherche de perceptions pour invoquer les recherches enregistrées dans le magasin de journaux d'entreprise Splunk.

Remarque : Les requêtes de configuration de recherche s'appuient sur les données de journal Splunk pour être conformes à Splunk Common Information Model (CIM).

Avec les configurations de recherche enregistrées, vous pouvez :

- Créez des recherches personnalisées qui combinent plusieurs enregistrements d'événements.
- Des recherches efficaces et efficientes en matière de conception.
- Utiliser les entrées paramétrées dans la recherche enregistrée Splunk.

Le système de base inclut les exemples de configurations, comme illustré dans cette image :

Configurations de recherche enregistrées

	Name	Observable type	Search	Is saved search
	Search	Search	Search	Search
	Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
	Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
	Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

Les requêtes de recherche enregistrées et de configuration sur place sont des exemples de requêtes qui peuvent être remplacées par des paramètres appropriés pour votre environnement. Créez des configurations de recherche enregistrées supplémentaires au besoin. Lorsque vous définissez une configuration de recherche enregistrée, le nom et les paramètres de la requête de recherche doivent correspondre à la configuration enregistrée définie sur votre instance Splunk. Si le nom et les paramètres ne sont pas identiques, vous risquez de ne pas voir de résultats précis lorsque vous effectuez une recherche d'observations.

Remarque : Sur votre instance Splunk, accédez à la page Recherches, rapports et alertes et localisez votre requête de recherche enregistrée. Cliquez sur le lien **Autorisations** pour accéder à la page Autorisations. Sélectionnez la case d'option **Toutes les applications** et activez l'option **Autorisation de lecture** pour **tout le monde**. Cela changera la valeur de la colonne de partage de Privé à Application pour votre requête de recherche enregistrée. Si cette option n'est pas définie, la requête de recherche enregistrée peut ne pas renvoyer de résultats.

Pour vérifier si la configuration de recherche enregistrée correspond à la configuration définie sur votre instance Splunk :

1. Accédez à la **Paramètres** > **Recherches, rapports et alertes**.
2. **Modifiez le contexte de l'application** sur **Tous**.

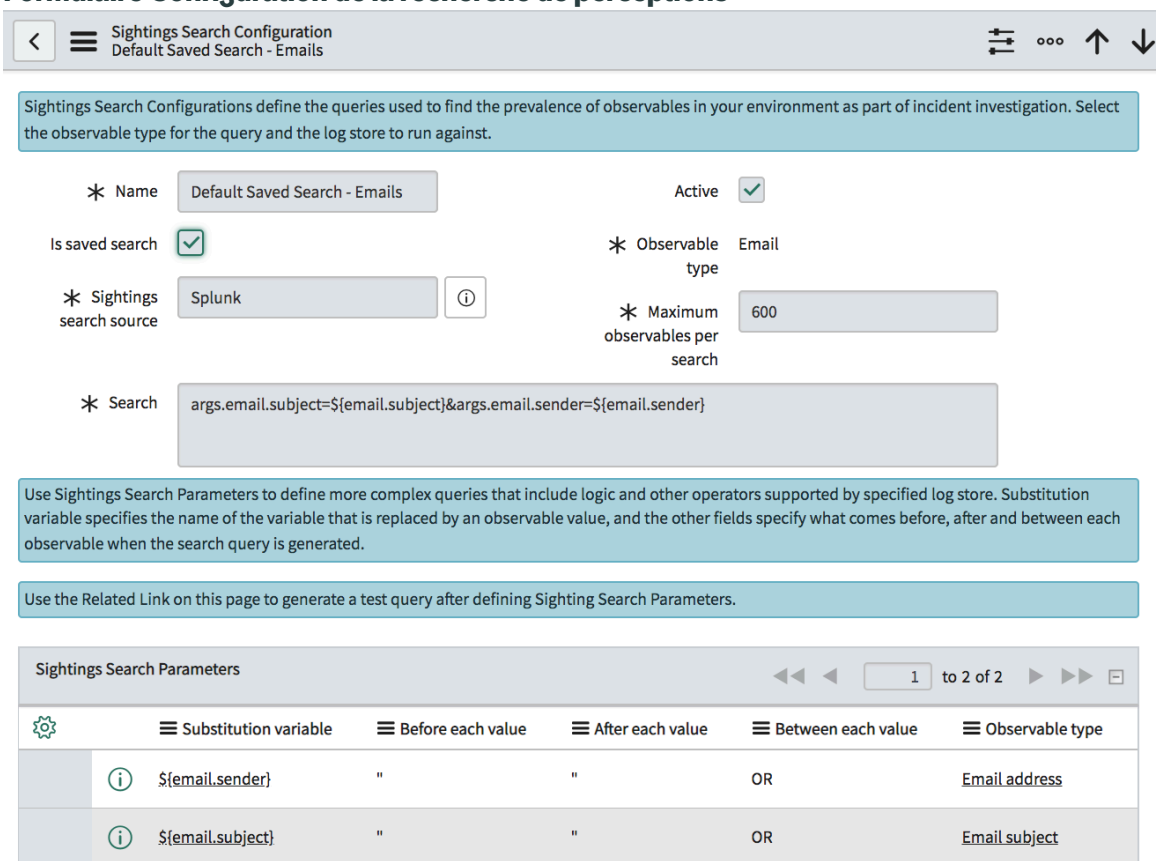
   Une liste de rapports de recherche s'affiche.
3. Confirmez que la requête de recherche enregistrée figure dans la liste.

Par exemple, le formulaire de configuration de la recherche de perceptions contient l'adresse e-mail et l'expéditeur comme paramètres de recherche :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Configuration de la recherche de perceptions



Dans votre instance Splunk, définissez la recherche enregistrée avec le même nom, la recherche enregistrée par défaut - E-mails, et les mêmes paramètres de recherche pour l'adresse e-mail et l'objet de l'e-mail. Si le nom et les paramètres de recherche ne sont pas identiques, la recherche de perceptions ne génère pas de résultat précis.

Procédure

1. Accédez à la **Security Operations** > **Intégrations** > **Configuration de la recherche de perceptions** et créez un nouvel enregistrement (voir la table des descriptions de champ).

Formulaire Configuration de la recherche de perceptions

Champ	Description
Nom	Nom de la configuration.
Est une recherche enregistrée	La configuration de recherche enregistrée est créée si vous sélectionnez cette option.
Source de recherche de perceptions	La source de la recherche d'observations. Sélectionnez le magasin de journaux Splunk comme source.
Actif	Option pour l'état de recherche enregistré. Seules les configurations de recherche actives peuvent être utilisées pour effectuer une recherche de perceptions.
Type d'observable	Le type d'observable peut être n'importe quel type d'observable tel qu'une adresse IP, une valeur de hachage, une URL, un nom de domaine, et ainsi de suite.
Nombre maximum d'observables par recherche	Nombre maximal d'observables à renvoyer à partir de la recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Rechercher	La chaîne de recherche par défaut est `$(observable)`, mais vous pouvez définir votre propre requête de recherche en spécifiant les paramètres pris en charge par le magasin de journaux Splunk.

2. Cliquez sur **Envoyer**.

Résultats
Vous avez créé un enregistrement de configuration de recherche de perceptions.

Que faire ensuite
Après avoir défini la requête de recherche, cliquez sur **Générer une requête de test de recherche de perceptions** et spécifiez une liste de valeurs observables pour générer une requête de test basée sur cette configuration de recherche enregistrée.

Exécuter une recherche de perceptions

Déterminez la prévalence d'une menace dans le temps ou testez les efforts de rattrapage ou d'éradication. Vous pouvez sélectionner un ou plusieurs observables et la plage de dates de votre recherche à partir d'un incident de sécurité. Les résultats sont inclus dans la liste connexe **des observables d'incident de sécurité** .

Avant de commencer
Rôle requis : sn_si.analyst

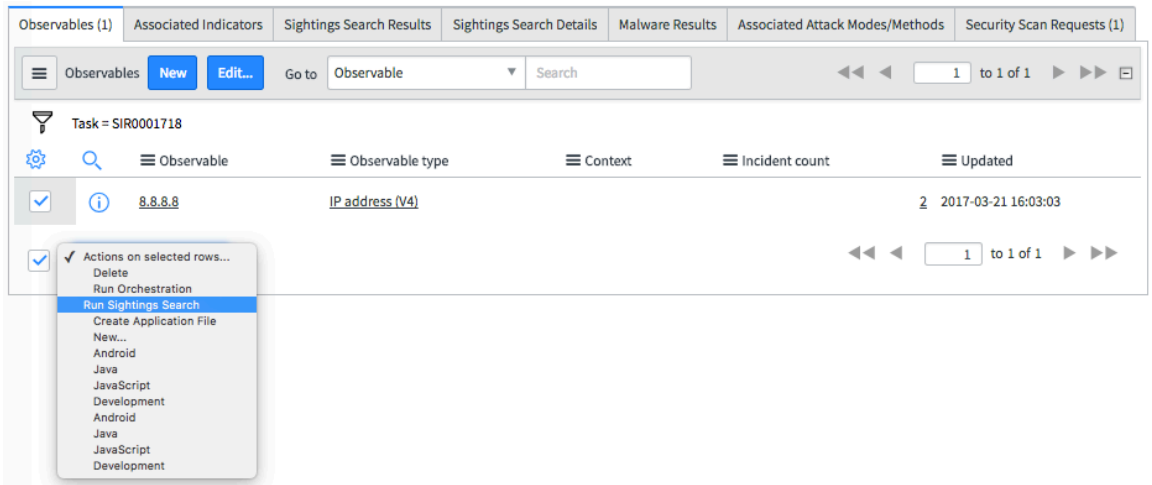
Pourquoi et quand exécuter cette tâche
L'aptitude Recherche de perceptions a un flux, Security Operations Integration - Flux de recherche de perceptions, qui exécute la recherche de perceptions. Ce flux accepte une liste d'observables, recherche toutes les options d'implémentation, crée les requêtes en fonction des configurations de recherche de perceptions et exécute les recherches en fonction du flux configuré.

Remarque : Une implémentation active doit être configurée. La recherche de perceptions prend en charge l'enrichissement des incidents Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger et QRadar. Si aucune implémentation n'est disponible, les actions d'aptitude, telles que **Exécuter la recherche de perceptions**, ne sont pas affichées dans les menus de produit.

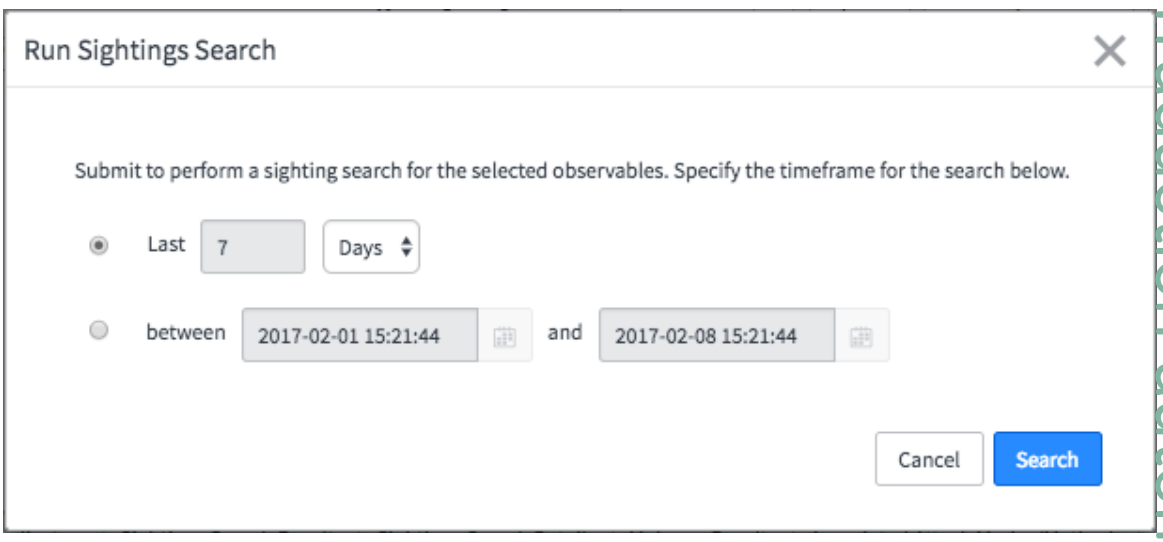
Procédure
1. Accédez à un incident de sécurité.
2. Cliquez sur le lien connexe **Afficher l'IoC** .
3. Sélectionnez **Observables** dans l'onglet Liste connexe.
4. Sélectionnez les observables sur lesquels vous souhaitez effectuer une recherche d'observations.
5. Cliquez sur **Exécuter la recherche de perception** dans le menu déroulant **Actions sur les lignes sélectionnées...**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La boîte de dialogue Exécuter la recherche de perception s'ouvre.



Remarque : Les valeurs saisies dans la boîte de dialogue remplacent les valeurs de configuration d'aptitude pour cette exécution.

6. Choisissez le nombre de jours ou une plage de dates pour rechercher des données.

Option	Description
Dernier	Nombre d'heures ou de jours avant la création de l'incident pour la recherche. La valeur par défaut est de 7 jours. La limite est de 99 heures ou jours.
entre	Plage de dates à rechercher. Les dates par défaut sont les suivantes : Date et heure d'ouverture de l'incident. Date et heure sept jours avant l'ouverture de l'incident.

Remarque : Le dernier est le nombre d'heures ou de jours avant la création de l'incident à rechercher. La valeur par défaut est de 7 jours. La limite est de 99 heures ou jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Rechercher**.
   Un enregistrement de recherche de perceptions est créé. Les données de perception agrégées et associées sont affichées dans l'incident de sécurité sous les onglets **Résultats de recherche de perception** et **Détails de recherche de perception** .

> **Remarque :** Les données des résultats de recherche de perceptions peuvent être partagées avec Trusted Security Circle, à l'exception des données brutes dans le cas des implémentations configurées pour inclure des données brutes.

Résultats de recherche de perceptions

Résultat	Description
Numéro	L'identificateur de la recherche d'observations.
Nombre d'observables	Nombre d'observables recherchés par requête.
Perceptions internes	Nombre de perceptions internes.
Perceptions externes	Nombre de perceptions externes. (Reçu du partage de menaces.)
Éléments de configuration correspondants	Nombre d'éléments de configuration qui correspondent à un enregistrement existant dans votre CMDB pour chaque observable trouvé dans votre environnement.
Plage de dates de démarrage	Il est temps de commencer à chercher des observations.
Plage de dates de fin	Il est temps d'arrêter de chercher des observations.
Mis à jour	Date et heure de la dernière modification.

Note: Si l'implémentation utilisée pour la recherche de perceptions est configurée pour inclure des données brutes et qu'au moins une détection est trouvée, une pièce jointe contenant des échantillons de données brutes apparaît en haut de l'incident de sécurité.

Détails de la recherche de perception

Détail	Description
Recherche de perception	L'identificateur de la recherche d'observations.
Observable	Observable recherché par requête.
Type d'observable	Type d'observable recherché par la requête.
Perceptions internes	Nombre agrégé de perceptions internes.
Perceptions externes	Nombre agrégé de perceptions externes. (Reçu du partage de menaces.)
Mis à jour	Date et heure de la dernière modification.

Security Operations Integration - Flux de recherche de perceptions

Le flux de **recherche de perceptions de Security Operations Integration** est un flux de haut niveau indépendant des intégrations. Elle utilise les requêtes configurées pour rechercher un ensemble d'observables en fonction des intégrations configurées qui prennent en charge l'aptitude. Utilisez-le pour réaliser une intégration telle que Splunk ou Elasticsearch.

Avant de commencer

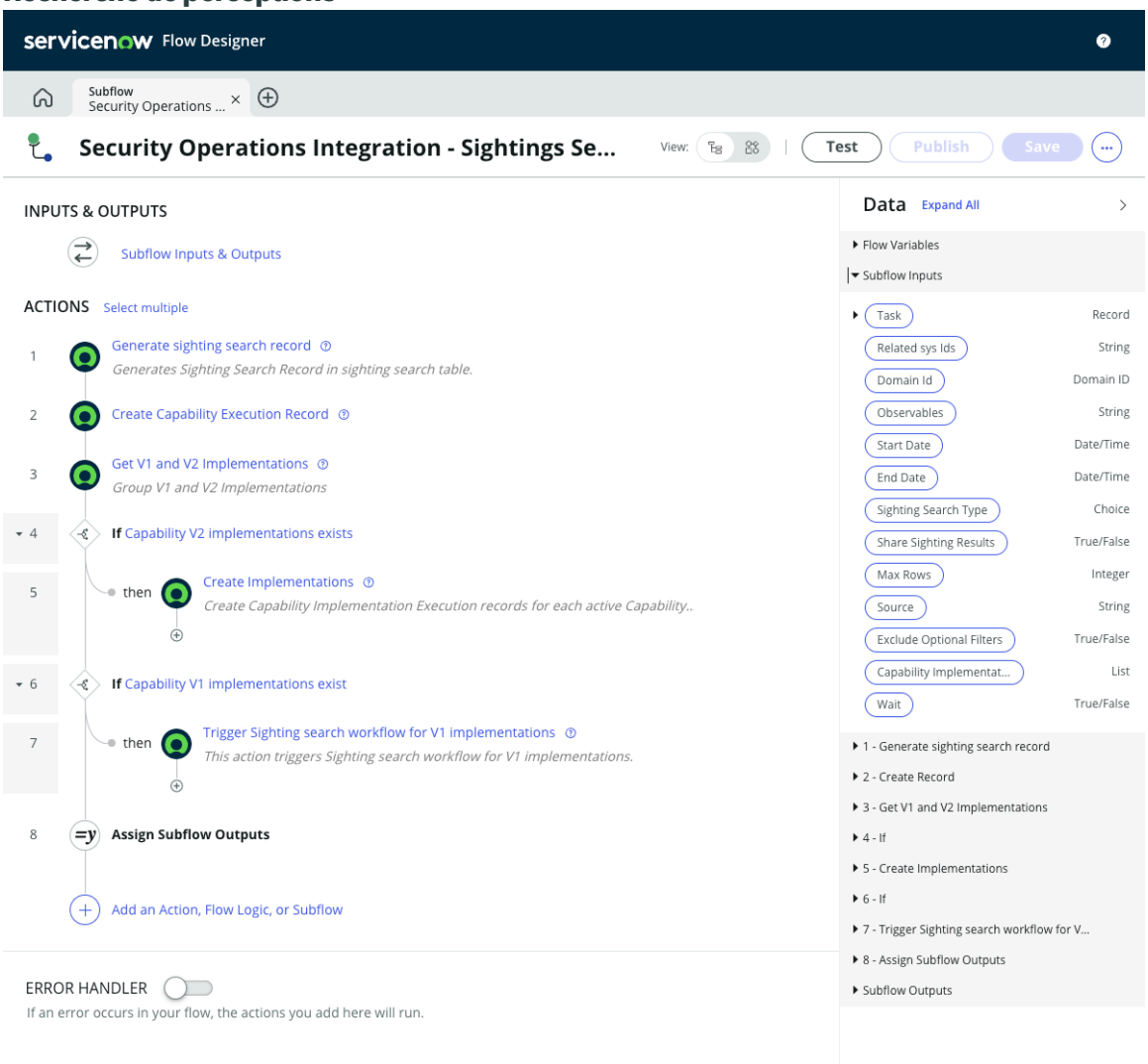
Rôle requis : sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche
Si un observable est associé à un incident de sécurité, ce flux est déclenché lorsque vous cliquez sur **Exécuter la recherche de perception** dans le menu déroulant **Actions sur les lignes sélectionnées...** de l'onglet **Observables d'incident de sécurité** .

Recherche de perceptions



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Recherche de perception : activité Déterminer les observables

L'activité **de workflow Recherche de perceptions - Déterminer les observables** détermine les observables à inclure dans le workflow.

L'activité **Recherche de perceptions - Déterminer les observables** peut être utilisée avec n'importe quel workflow pour déterminer les observables à inclure dans le workflow.

Résultats

Les résultats possibles de cette activité sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Observables trouvés
Échec	Aucun observable trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
task_sys_id	Identificateur de tâche (mappe les incidents de sécurité aux observables).
observables	Adresses IP, hachage, URL, noms de domaine.
workflow_current_sys_id	Identificateur système de l'enregistrement actuel. (Utilisé uniquement si `task_sys_id`, les entrées observables ne sont pas disponibles.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
observables	Observables filtrés

Activité de perceptions observables persistantes

L'activité de workflow **Observations observables persistantes** récupère les observables à partir de l'intégration tierce.

L'activité **Observations d'observables persistants** peut être utilisée avec n'importe quel workflow pour enregistrer les observables trouvés dans l'intégration tierce.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Observables récupérés.
Échec	Une erreur s'est produite lors de la tentative de collecte d'observables. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
sightingsResponse	
taskId	Identificateur de tâche.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
réponse	

Obtenir l'activité des requêtes de perceptions d'observables

L'activité de workflow **Obtenir des requêtes de perception d'observables** récupère les requêtes à partir de la configuration d'intégration.

L'activité **Obtenir des requêtes de perceptions d'observables** peut être utilisée avec n'importe quel workflow pour obtenir des requêtes à envoyer à l'implémentation spécifiée à l'aide du **lanceur de flux parallèle**.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Requêtes trouvées.
Échec	Une erreur s'est produite lors de la tentative d'obtention de requêtes. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
observables	Liste des observables filtrés.
Options	Liste des options prises en charge.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

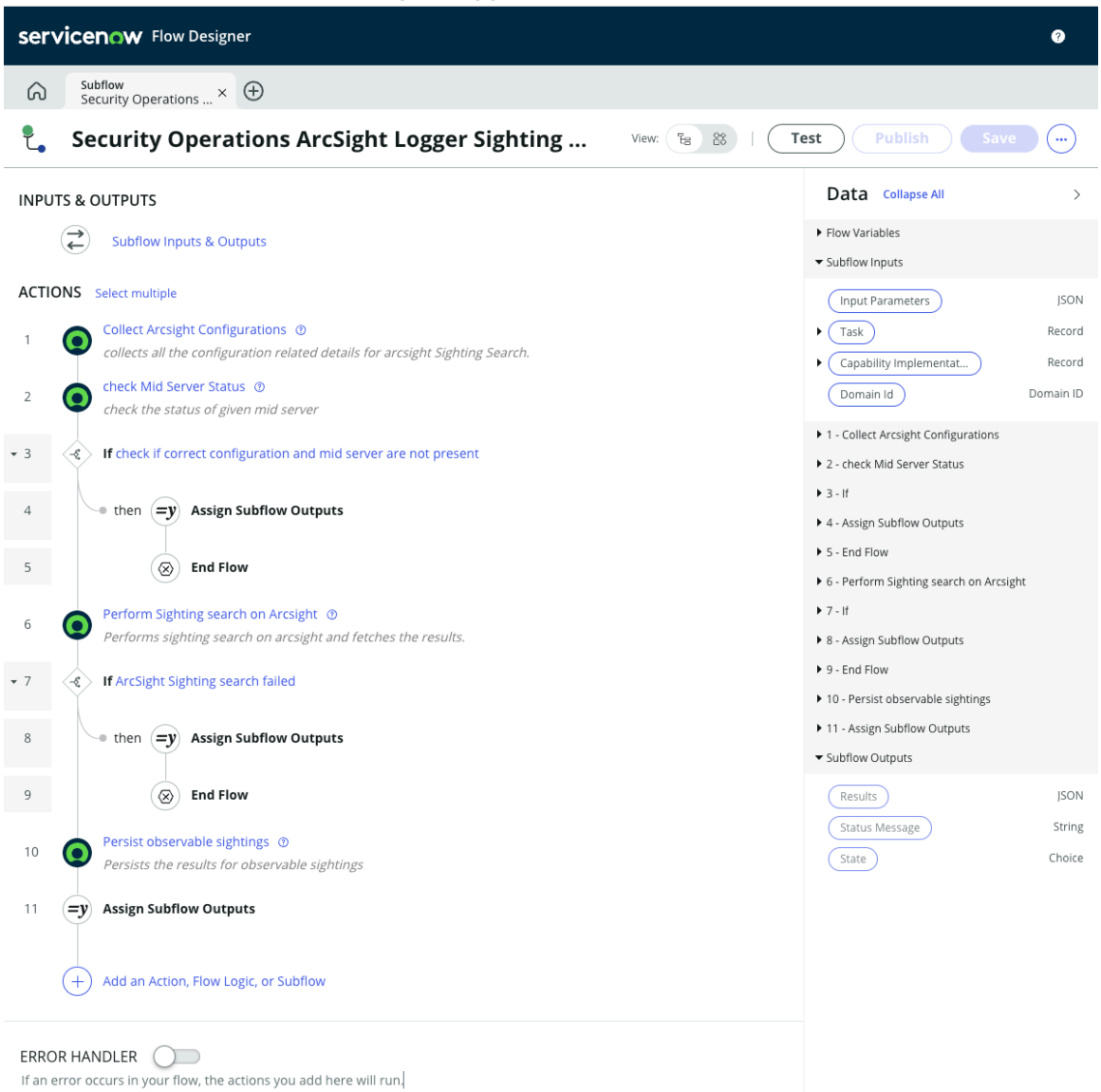
Variable	Description
requêtes	Chaîne de recherche.
nombre de requêtes	Nombre de requêtes à exécuter.

Opérations de sécurité : ArcSight Logger Flux de recherche de perceptions

Le flux Security Operations - ArcSight Logger Sightings Search est l'implémentation de l'intégration Splunk lancée par le flux de **recherche de perceptions de l'intégration Security Operations - Sightings Search Flow**.

Rôle requis : sn_si_analyst

Recherche de perceptions ArcSight Logger



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Traduction automatique

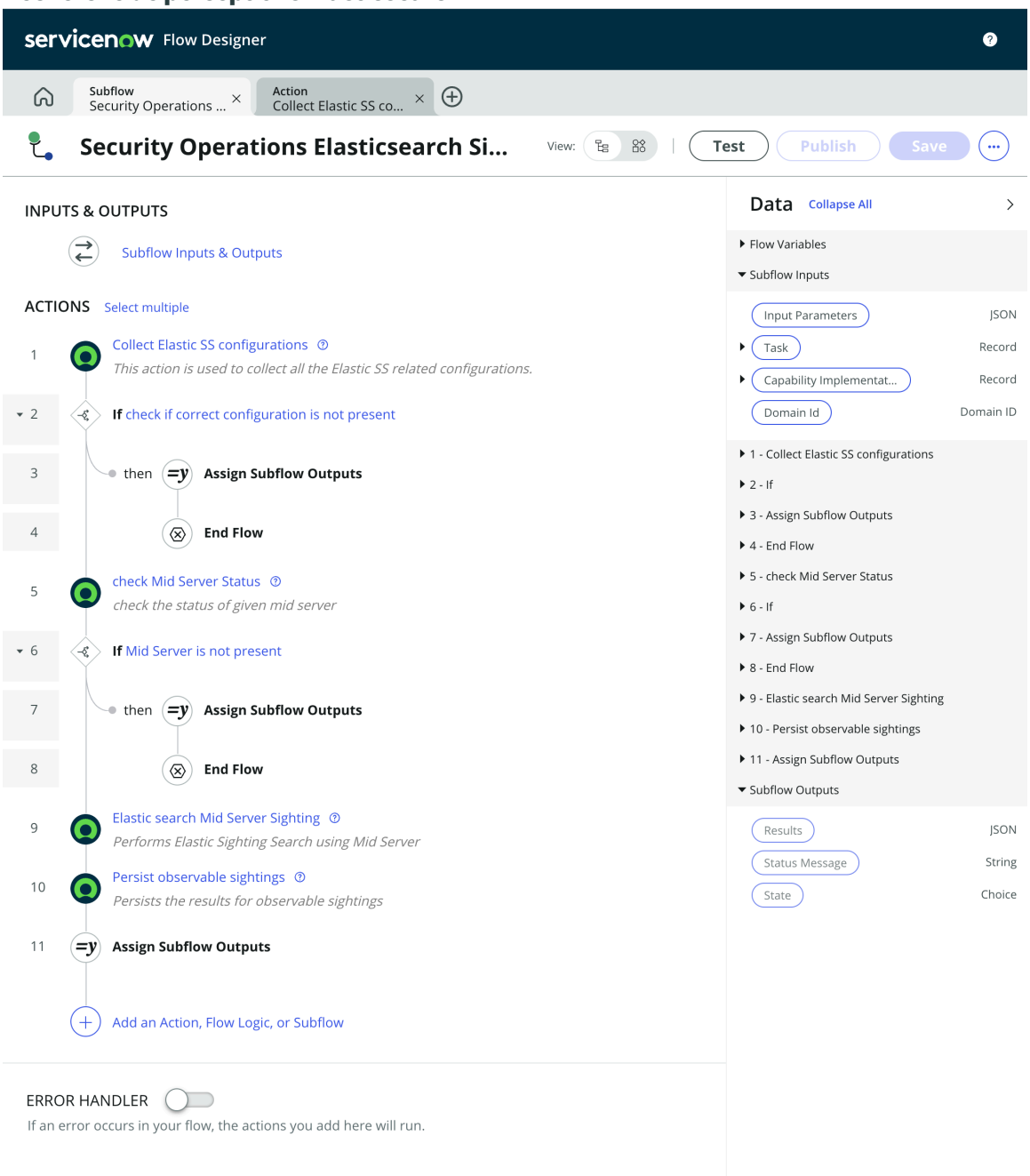
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opérations de sécurité : flux de recherche de perceptions Elasticsearch

Le flux de recherche de perceptions Security Operations - Elasticsearch est l'implémentation d'Elasticsearch lancée par le flux de **recherche de perceptions de l'intégration de Security Operations** .

Rôle requis : sn_si.analyst

Recherche de perceptions Elasticsearch



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Opérations de sécurité - Flux de recherche d'observations McAfee ESM

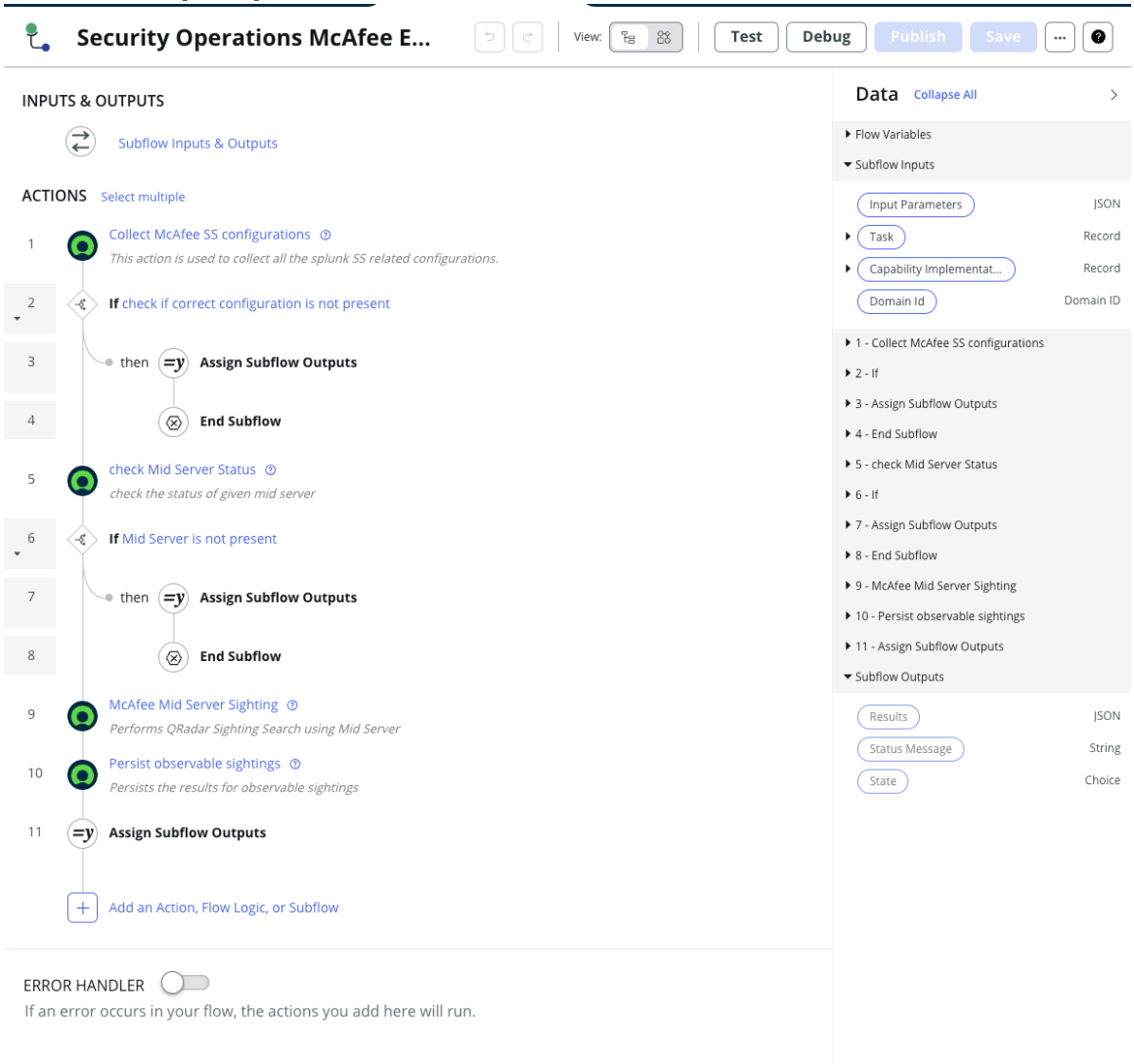
Le flux de recherche de perceptions McAfee ESM est l'implémentation de l'implémentation de la recherche de perceptions McAfee lancée par le **flux de recherche de perceptions de l'intégration de Security Operations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : sn_si_analyst

Recherche de perceptions McAfee ESM



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Opérations de sécurité - Flux de recherche de perceptions QRadar

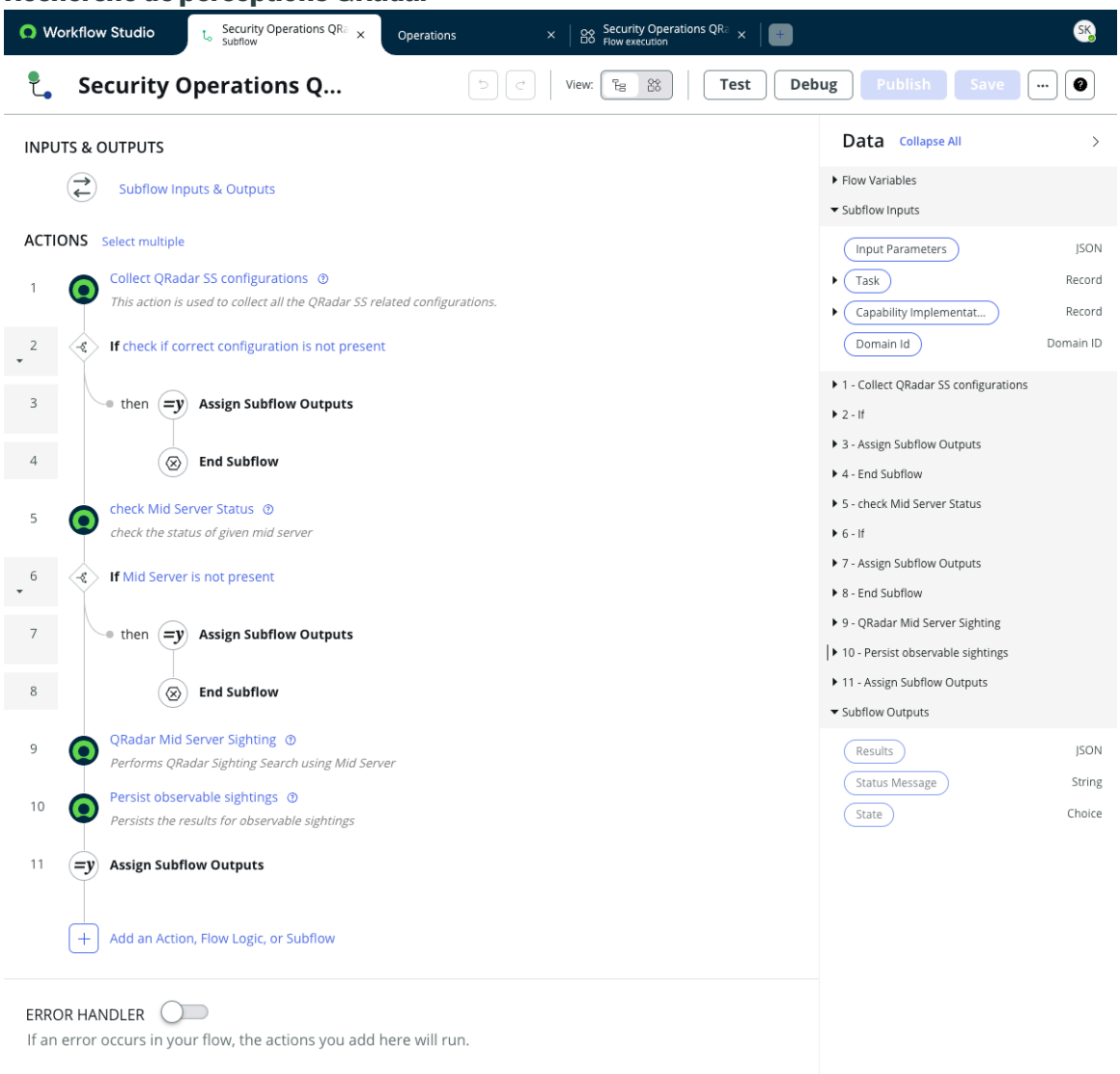
Le flux Security Operations - QRadar Sightings Search est l'implémentation de l'intégration IBM QRadar lancée par le **flux Security Operations Integration - Sightings Search**.

Rôle requis : sn_si_analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche de perceptions QRadar



Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Security Operations Integration - Flux de recherche d'observations Splunk

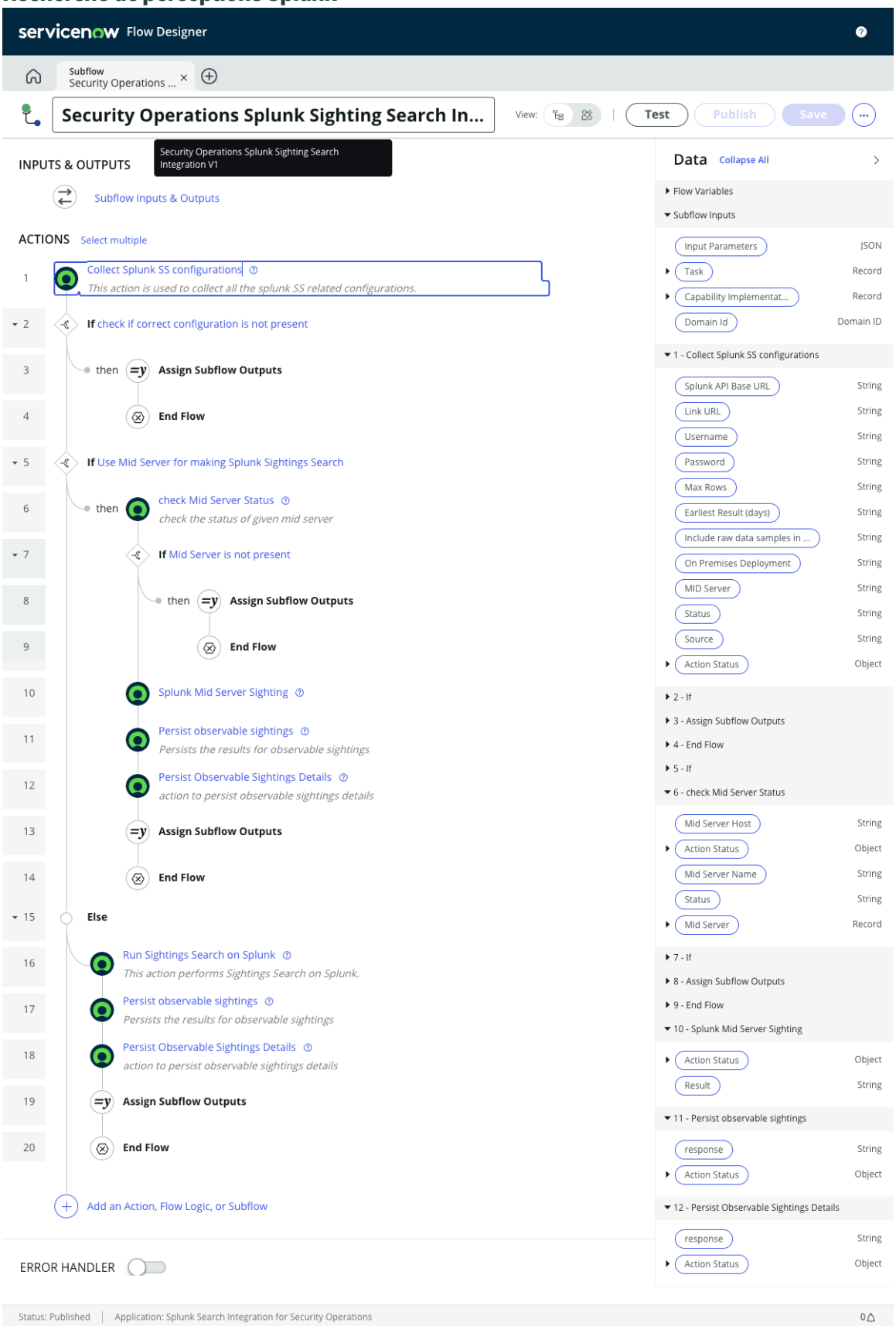
Le flux Security Operations - Recherche de perceptions Splunk est l'implémentation de l'intégration Splunk lancée par le **flux Intégration des opérations de sécurité - Recherche de perceptions**.

Rôle requis : sn_si_analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Recherche de perceptions Splunk



Traduction automatique

Les activités spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres activités, reportez-vous à la section Flux d’intégration et activités d’orchestration courants de Security Operations.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les résultats de recherche de perceptions

Vous pouvez examiner les résultats de la recherche de perceptions pour rechercher des indicateurs malveillants internes et externes.

Avant de commencer

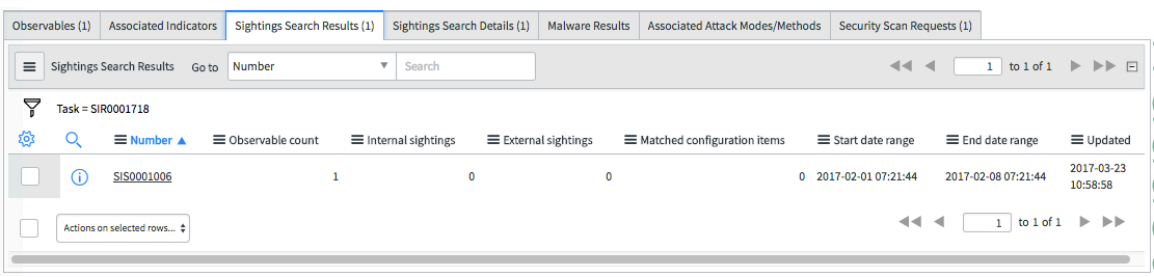
Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

.

Procédure

1. Accédez à un incident de sécurité.
2. Sélectionnez l'onglet **Résultats de recherche de perceptions** dans le groupe Afficher la liste connexe **IoC** pour afficher la liste des recherches de perceptions.



Remarque : Ces données peuvent être partagées avec Trusted Security Circle.

Résultats de recherche de perceptions

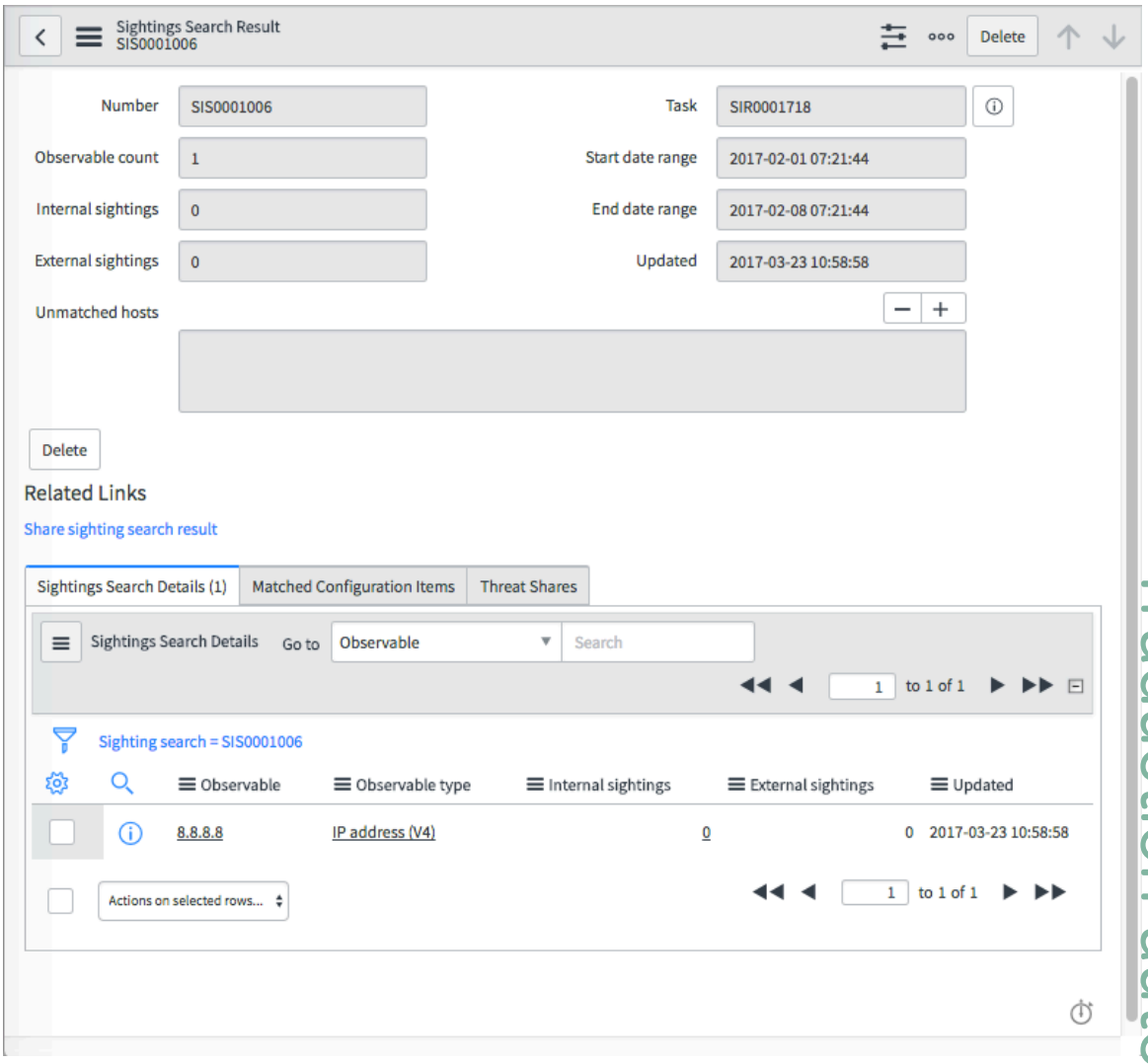
Résultat	Description
Numéro	Identificateur de recherche de perceptions.
Nombre d'observables	Nombre d'observables recherchés.
Perceptions internes	Nombre agrégé de perceptions internes.
Perceptions externes	Nombre agrégé de perceptions externes. (Reçu du partage de menaces.)
Éléments de configuration correspondants	Nombre agrégé d'éléments de configuration qui correspondent à un enregistrement existant dans votre CMDB.
Plage de dates de démarrage	Il est temps de commencer à chercher des observations.
Plage de dates de fin	Il est temps d'arrêter de chercher des observations.
Mis à jour	Date et heure de la dernière modification.

Pour afficher les détails d'une recherche unique :

3. Cliquez sur une recherche de perceptions dans la liste **des résultats de recherche de perceptions** .
Le formulaire Résultats de recherche de perceptions s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Formulaire Résultats de recherche de perceptions

Détail	Description
Numéro	Identificateur de recherche de perceptions internes.
Nombre d'observables	Nombre d'observables recherchés par cette requête.
Perceptions internes	Nombre de perceptions internes pour cette recherche.
Perceptions externes	Nombre de perceptions externes pour cette recherche. (Reçu de Trusted Security Circle.)
Hôtes sans correspondance	Liste des éléments de configuration potentiels pour cette recherche qui n'ont été mis en correspondance avec aucun enregistrement de votre CMDB.
Tâche	Identificateur de tâche d'incident de sécurité.
Plage de dates de démarrage	Heure à laquelle la recherche d'observations a commencé.
Plage de dates de fin	Heure à laquelle la recherche d'observations s'est arrêtée.
Mis à jour	Date et heure de la dernière modification.
Détails de la recherche de perception	Type, nombre d'observations et date de modification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détail	Description
Éléments de configuration correspondants	Nombre d'éléments de configuration qui correspondent à un enregistrement existant dans votre CMDB. Répertorie le CI et l'observation.
Partages de menace	Liste des menaces partagée avec Trusted Security Circle.

Partager les résultats de recherche de perceptions

Vous pouvez partager les observations locales, les détails ou les résultats associés à une recherche particulière avec votre Trusted Security Circle.

Avant de commencer

Rôle requis : sn_si.analyst

Pourquoi et quand exécuter cette tâche

Le partage peut être automatisé à l'aide des **propriétés** Réponse aux incidents de sécurité suivantes.

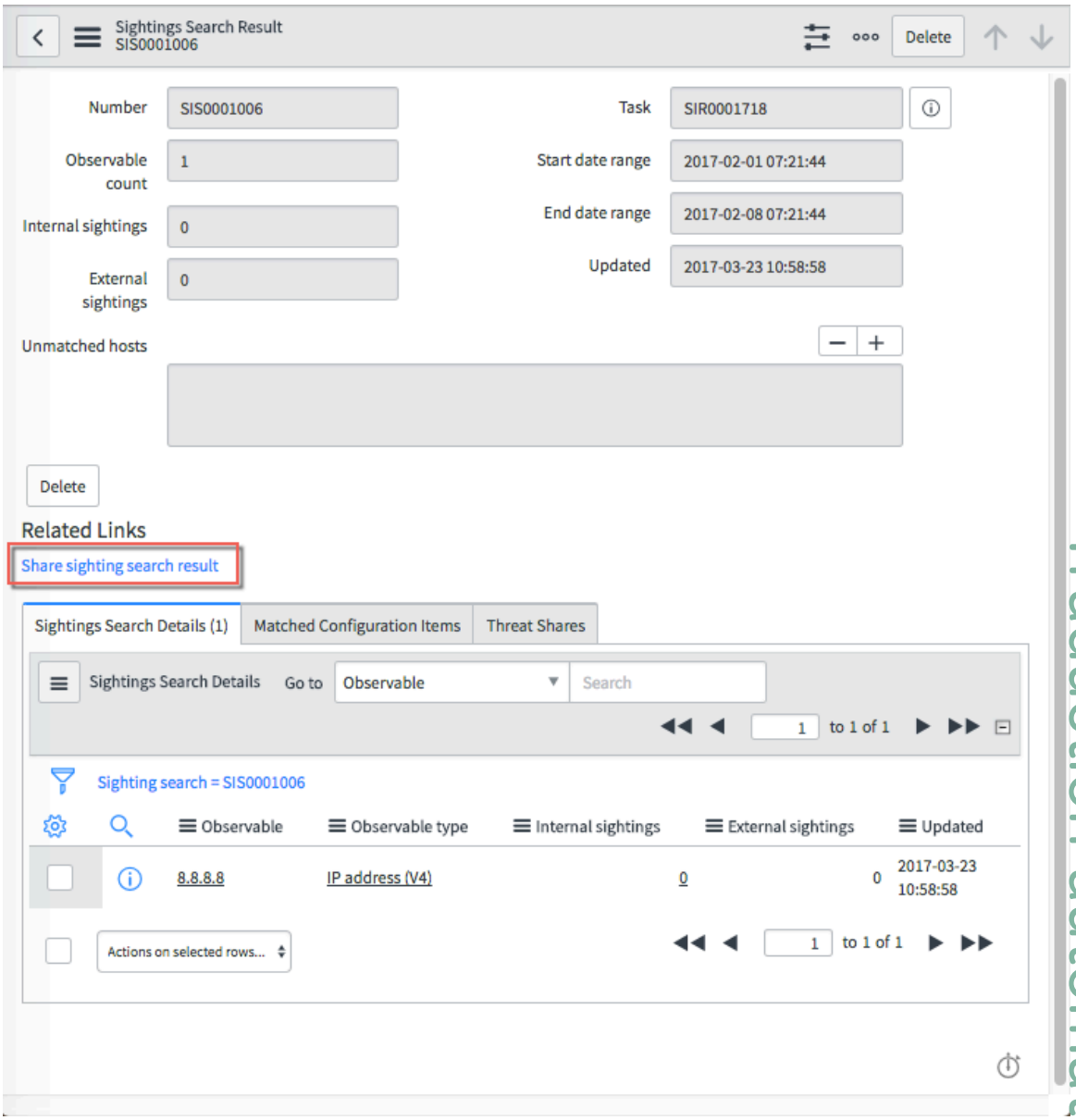
- Partager automatiquement les résultats d'une recherche d'observations avec le cercle de confiance ServiceNow par défaut
- Inclure les observables sans perceptions locales lors du partage automatique des résultats de recherche de perceptions
- Répondre avec des observations locales chaque fois qu'un partage de menace est reçu d'un cercle de confiance

Procédure

1. Accédez à un incident de sécurité.
2. Cliquez sur la liste connexe **Afficher IoC** et sélectionnez l'onglet **Résultats de recherche de perceptions** pour afficher la liste des recherches de perceptions.
3. Cliquez sur un résultat de recherche de perceptions.

Traduction automatique

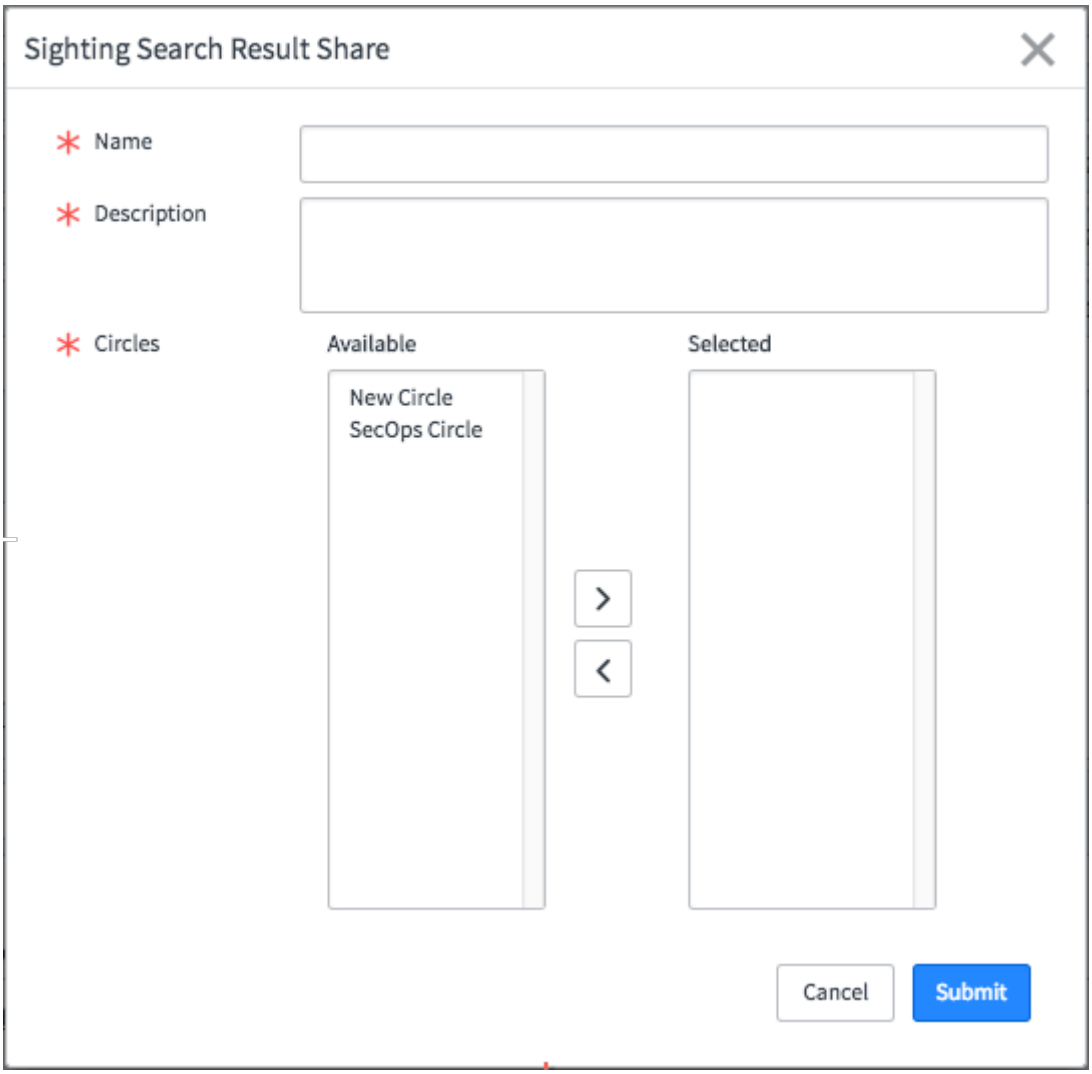
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans le formulaire **Résultat de recherche de perceptions**, cliquez sur le lien connexe **Partager les résultats de recherche de perception** .
   La boîte de dialogue Partage des résultats de recherche de perception s’affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Saisissez un **nom** pour cet enregistrement de partage observable.
6. Saisissez une **description**des observables à partager.
7. Choisissez **les cercles** avec lesquels partager les observables.
8. Cliquez sur **Envoyer**.
   Le ou les observables sont partagés avec le cercle de confiance spécifié.

Partager des observables à partir d'un incident de sécurité

Les observables peuvent être partagés à partir d'un incident de sécurité avec Réponse aux incidents de sécurité les membres de votre cercle de confiance.

Avant de commencer

Rôle requis : sn_si.analyst

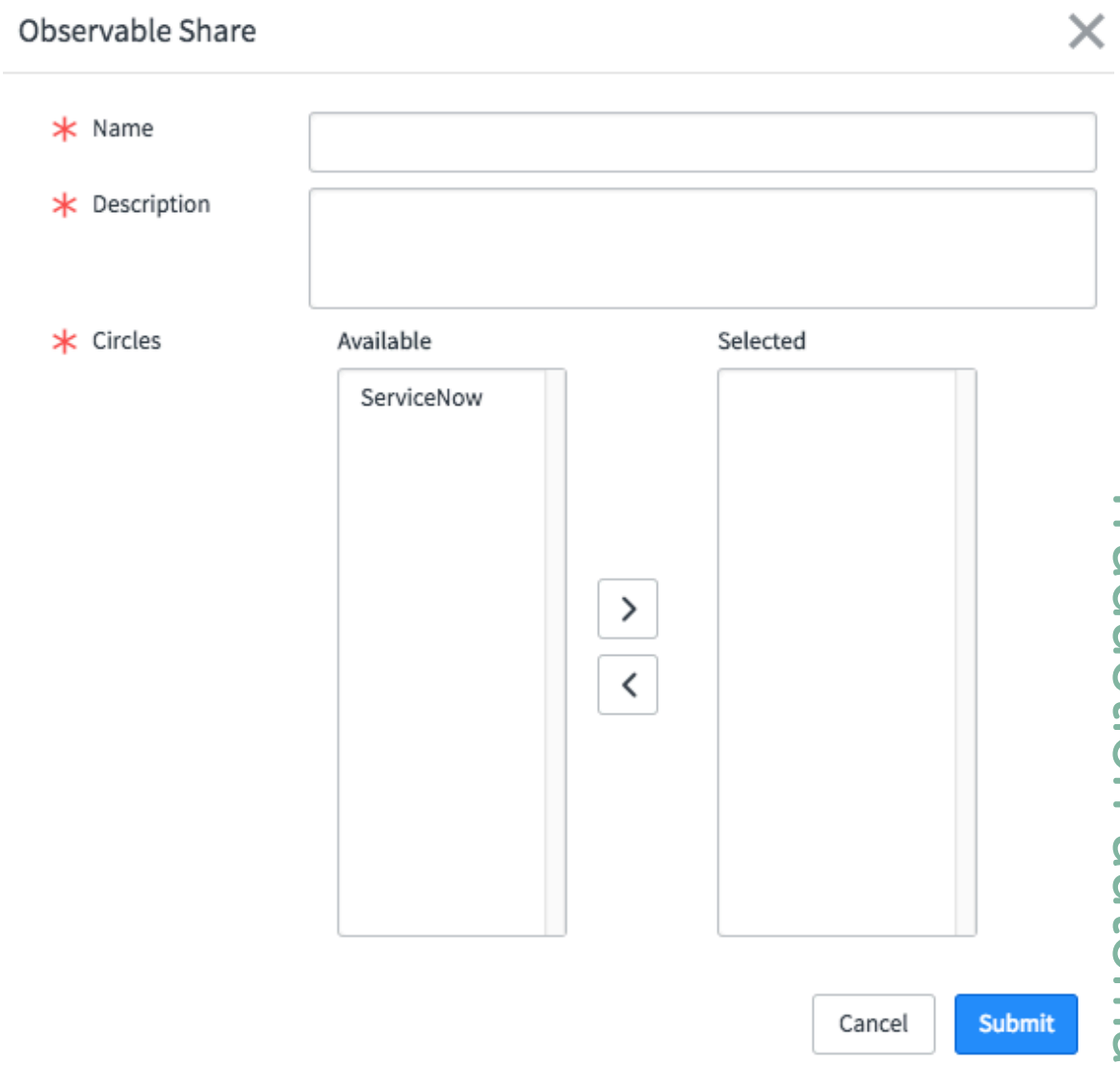
Procédure

1. Accédez à un incident de sécurité.
2. Sélectionnez l'onglet **Observables** dans le groupe Afficher la liste connexe **IoC** .
3. Cliquez sur un observable.
4. Sur le formulaire **Observable** , cliquez sur le lien connexe **Partager l'observable** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La boîte de dialogue Partage observable s’affiche.



5. Entrez un **nom** pour cet enregistrement de partage de menace.
6. Entrez une **description**des observables sélectionnés.
7. Choisissez **les cercles** avec lesquels partager les observables.
8. Cliquez sur **Envoyer**.
   Le ou les observables sont partagés avec le cercle de confiance spécifié.
9. Vous pouvez afficher les enregistrements de partage de menaces en cliquant sur l’onglet **Partages de menaces** .
10. Si l’un des observables partagés contient des observations, celles-ci sont également partagées et peuvent être visualisées en cliquant sur l’onglet **Perceptions** .

Afficher les détails de la recherche de perceptions

Passez en revue les détails agrégés de toutes les recherches d’observations.

Avant de commencer
Rôle requis : sn_si.analyst

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

.

Procédure

1. Accédez à un incident de sécurité.
2. Sélectionnez l'onglet Détails de recherche de **perceptions** dans le groupe Afficher la liste connexe **IoC** pour afficher la liste des recherches de perceptions.

Remarque : Ces données peuvent être partagées avec Trusted Security Circle.

Détails de la recherche de perception

Détail	Description
Observable	Liste de tous les observables recherchés par la requête.
Type d'observable	
Perceptions internes	Nombre de perceptions internes pour toutes les recherches.
Perceptions externes	Nombre de perceptions externes pour toutes les recherches. (Reçu du partage de menaces.)
Recherche de perception	Identificateur de recherche de perceptions.
Mis à jour	Date et heure de la dernière modification.

Afficher les données de recherche de perceptions

Passez en revue les données agrégées de toutes les recherches d'observations.

Avant de commencer

Rôle requis : sn_si.analyst

Procédure

1. Accédez à un incident de sécurité.
2. Sélectionnez l'onglet **Données de recherche de perceptions** du groupe Liste connexe **Afficher toutes les listes connexes** pour afficher la liste des recherches de perceptions.

Remarque : Ces données peuvent être partagées avec Trusted Security Circle.

Données de recherche de perceptions

Résultat	Description
Plage de dates de fin	Il est temps d'arrêter de chercher des observations.
Perceptions externes	Nombre agrégé de perceptions externes. (Reçu du partage de menaces.)
Perceptions internes	Nombre agrégé de perceptions internes.
Est local	Indique si les perceptions proviennent de l'environnement actuel ou d'un environnement partagé.
Observable	Liste de tous les observables recherchés par la requête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultat	Description
Nombre de perception	Nombre de perceptions recherchées.
Recherche de perception	Identificateur de recherche de perceptions.
Détails de la recherche de perception	Regrouper les détails de la recherche d'observations.
Lien de recherche sur la perception	Lien pointant vers le portail de recherche de perceptions. La requête de recherche est automatiquement appliquée lorsque vous cliquez sur le lien de recherche Perception.
Requête de recherche de perception	Requête pour identifier l'instance. 172.10.0.171 est substituable et est substitué dans l'observable sélectionné. (rechercher 172.10.0.171 | tête 10) **Remarque :** La sélection de jours ne sera pas applicable à la recherche enregistrée.

Security Operations Integration - Aptitude de recherche de menace

L'aptitude Recherches de menaces effectue des recherches de renseignements sur les menaces pour déterminer si un ou plusieurs observables sont associés à des menaces de sécurité connues.

L'aptitude Recherches de menaces a un workflow, Security Operations Integration - Flux de recherche de menaces. Lorsque le workflow d'aptitude s'exécute, il exécute des workflows supplémentaires pour les implémentations activées. Vous pouvez spécifier une implémentation à utiliser pour effectuer une recherche sur les observables sélectionnés, ou vous pouvez effectuer la recherche à l'aide de toutes les implémentations.

Remarque : Si aucune implémentation n'est disponible, les actions d'aptitude ne sont pas affichées dans les menus de produits.

Security Operations Integration - Flux de recherche de menaces

Le flux **d'aptitude de Security Operations Integration - Recherche de menace** accède aux implémentations de recherche de menaces disponibles et exécute les flux d'implémentation associés à chacune d'elles pour effectuer des recherches de menaces sur les observables sélectionnés.

Avant de commencer
Rôle requis : sn_ti.write

Pourquoi et quand exécuter cette tâche
Ce flux peut être déclenché de la manière suivante.

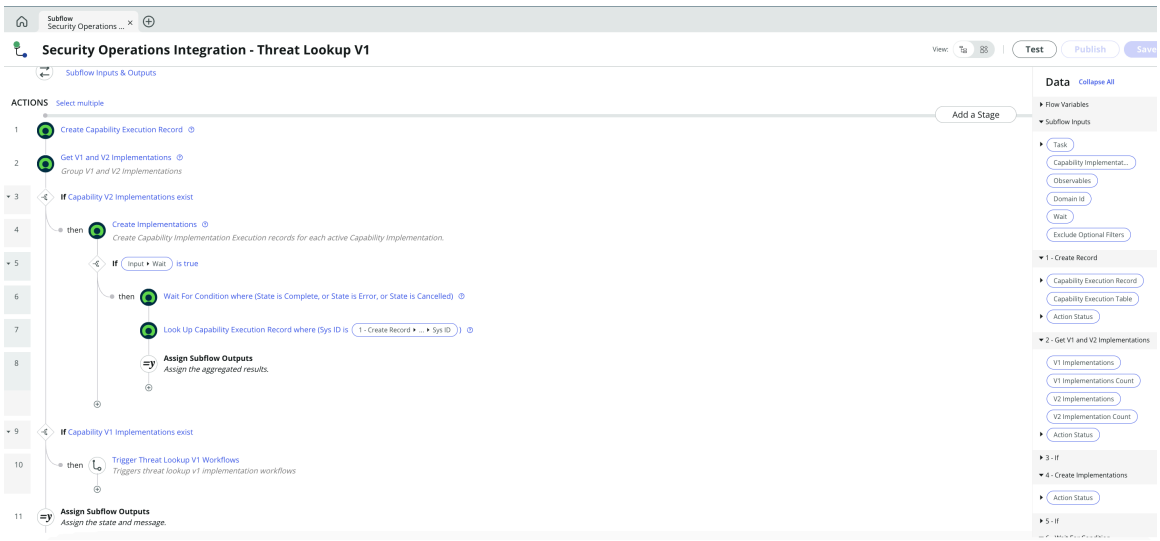
- en sélectionnant un ou plusieurs observables dans la liste Observables et en sélectionnant **Exécuter la recherche de menace** dans la liste de choix **Actions sur les lignes sélectionnées** .
- En ouvrant un enregistrement d'observable et en cliquant sur le lien connexe **Exécuter la recherche de menace** .
- À partir de la liste connexe Observables dans un incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chaque méthode vous permet ensuite de spécifier les implémentations de recherche à utiliser pour analyser les observables sélectionnés. Les flux d'implémentation associés sont exécutés pour effectuer les recherches.

Recherche de menace



Les actions spécifiques à ce flux sont décrites ici. Pour en savoir plus sur les autres actions, reportez-vous à la section Flux d'intégration et activités d'orchestration courants de Security Operations.

Les actions de processus de flux comprennent :

- Action Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune action d'implémentation

Modifier l'ordre d'exécution du flux

Les implémentations de l'option d'intégration spécifient le flux à exécuter. Dans le système de base, les flux sont exécutés séquentiellement, dans l'ordre spécifié dans l'implémentation. Vous pouvez modifier l'ordre selon vos besoins.

Avant de commencer

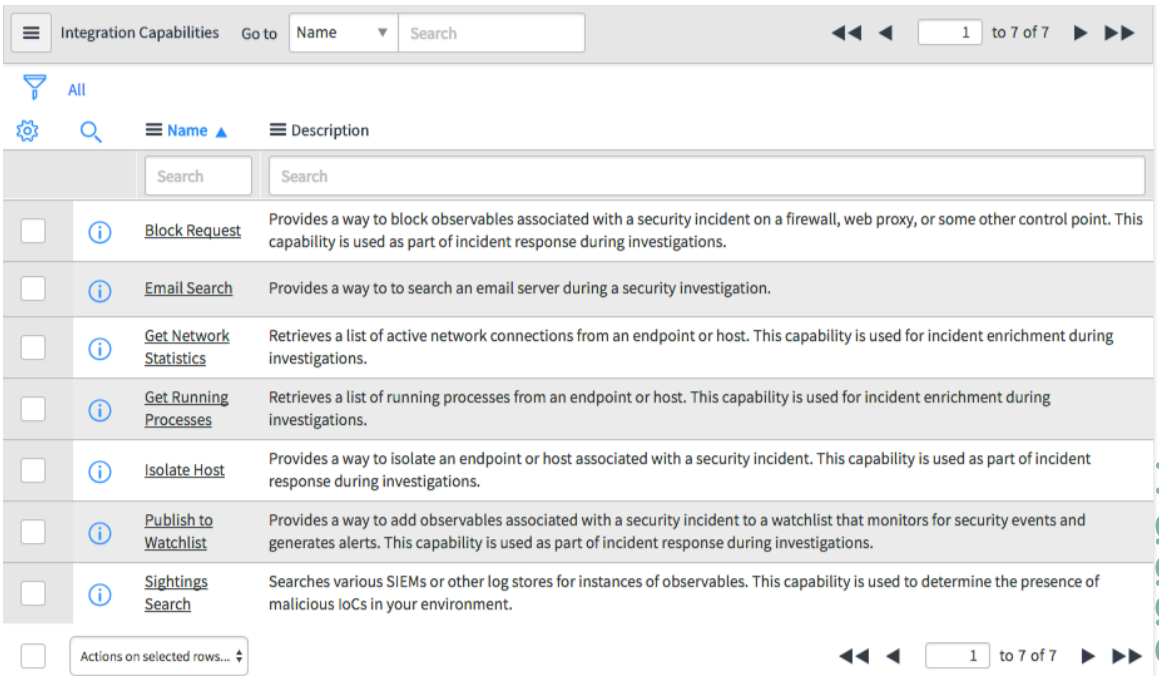
Rôle requis : sn_sec_cmn.write

Traduction automatique

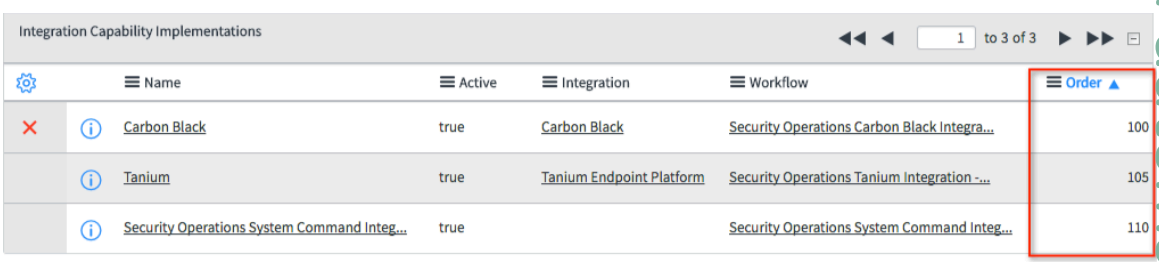
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

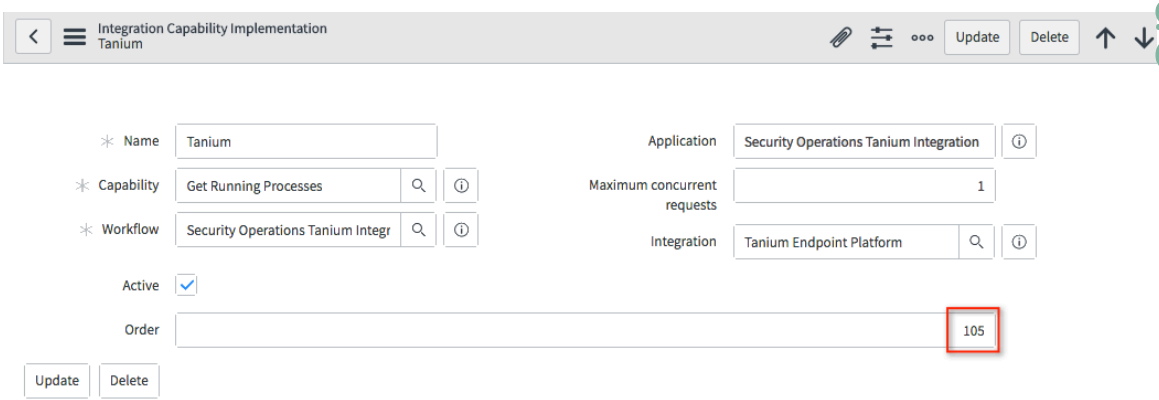
1. Accédez à la **Tous** > **Security Operations** > **Intégrations** > **Options d'intégration**.



2. Sélectionnez l'option d'intégration dont vous souhaitez modifier l'ordre d'exécution.



3. Sélectionnez l'implémentation que vous souhaitez modifier.



4. Modifiez la **commande** pour un nombre supérieur ou inférieur.
   Les nombres inférieurs ont une priorité d'exécution plus élevée.
5. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux d’intégration et activités d’orchestration courants de Security Operations

La plupart des flux associés aux intégrations tierces incluent les mêmes activités. Par exemple, les activités pour commencer et terminer le traitement.

Suivi de l’exécution : commencer l’action de flux

L’action Suivi de l’exécution - Commencer le flux démarre le processus d’audit pour un Opérations de sécurité flux d’intégration qui fonctionne sur les observables.

L’action Suivi de l’exécution - Commencer le flux peut être utilisée avec n’importe quel flux pour commencer à enregistrer la progression du flux dans un audit.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Un enregistrement d’audit est créé.

Variables d'entrée

Les variables d’entrée déterminent le comportement initial de l’action de flux.

Variable	Description
capabilityId	Identificateur système de l’option d’intégration en cours d’exécution.
isImpl	Marqueur qui spécifie si l’audit est effectué pour un flux d’aptitude d’intégration ou un flux d’implémentation d’option d’intégration. Les valeurs possibles sont les suivantes : • faux : désigne un audit sur un flux d’aptitude d’intégration abstrait tel que la recherche de perceptions. (par défaut). • vrai : désigne l’audit d’un flux d’implémentation d’option d’intégration. Par exemple, Splunk ou Elasticsearch.
taskId	Identificateur système pour toute tâche associée au flux.
observableList	Un ou plusieurs SysID observables permettant d’effectuer l’action souhaitée. Utilisé comme entrée de flux.
flowContextId	L’identificateur système de l’enregistrement de contexte de flux associé. Fourni par le système.
nom du flux	Nom du flux. Fourni par le système.
parentCapabilityExcutionId	Identificateur système de l’enregistrement d’audit qui a lancé le flux d’implémentation. Uniquement requis pour les flux d’implémentation de l’option d’intégration tels que Splunk, Elasticsearch et VirusTotal.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
capabilityExecutionId	Identificateur système de l'enregistrement d'audit.

- Action Obtenir les options de sécurité prises en charge
- Suivi de l'exécution de l'aptitude : aucune action d'implémentation

Suivi de l'exécution de l'aptitude : terminer l'action de flux

L'action Suivi de l'exécution de l'aptitude : terminer le flux met à jour l'enregistrement d'audit lorsque le flux est terminé.

L'action Suivi de l'exécution de l'aptitude : terminer le flux peut être utilisée avec n'importe quel flux pour enregistrer l'achèvement du flux.

Remarque : Le tableau Valeur de **retour** de l'action de flux principale du **lanceur parallèle** contient un tableau des résultats de tous les flux d'intégration exécutés et invite à terminer avec succès le suivi des exécutions.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de l'enregistrement d'audit est mis à jour et prend la valeur **Terminé**.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
capabilityExecutionId	Identificateur système pour l'enregistrement d'audit. Ce champ était le résultat de l'une des activités Commencer l'audit.
nom du flux	Nom du flux. Fourni par le système.
message	Message d'achèvement.

Variables de sortie

Il n'existe aucune variable de sortie.

Suivi de l'exécution de l'aptitude : action de flux d'échec

L'action de flux Suivi de l'exécution de l'aptitude : défaillance enregistre une défaillance dans l'enregistrement d'audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’action de flux Suivi de l’exécution de l’aptitude - Défaillance peut être utilisée avec n’importe quel flux pour enregistrer une condition de défaillance.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	L’état de l’enregistrement d’audit est défini sur **Erreur** et un message indiquant que l’erreur est enregistrée.

Variables d'entrée

Les variables d’entrée déterminent le comportement initial de l’action de flux.

Variable	Description
capabilityExecutionId	Identificateur système pour l’enregistrement d’audit. Il s’agit du résultat de toutes les activités Commencer l’audit.
errorMessage	Message indiquant le motif de l’échec.
nom du flux	Nom du flux. Fourni par le système.

Variables de sortie

Il n’existe aucune variable de sortie.

Aptitude : déterminer l’activité des CI

L’activité du workflow Aptitude - Déterminer les CI détermine les éléments de configuration (CI) à inclure dans le workflow.

L’activité Aptitude - Déterminer les CI peut être utilisée avec n’importe quel workflow pour déterminer les CI à inclure dans le workflow.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Éléments de configuration trouvés.
Échec	Aucun CI trouvé. Plus d’informations sur l’erreur sont disponibles dans l’erreur de sortie de l’activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
task_sys_id	Identificateur de tâche (mappe les incidents de sécurité aux CI).
cis_affected	Éléments de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
cis_affected	CI filtrés
task_sys_id	Identificateur de tâche (mappe les incidents de sécurité aux CI).

Créer des enregistrements de données d'enrichissement Action de flux

L'action Créer un flux d'enregistrements de données d'enrichissement crée ou met à jour les enregistrements d'enrichissement à utiliser dans le flux.

L'action **Créer des enregistrements de données d'enrichissement** peut être utilisée avec n'importe quel flux pour mettre à jour les enregistrements d'enrichissement dans le flux.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Enregistrement d'enrichissement mis à jour.
Échec	Enregistrement d'enrichissement non mis à jour. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variable	Description
task_id	Identificateur de tâche.
contenu	Contenu brut (données des processus en cours).
enrichment_mapping_id	Identificateur de mappage d'enrichissement.
ci_id	Identificateur d'élément de configuration.
reference_value	Inutilisé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
résultat	GlideRecords créés à l'aide du script enrichmentUtils.

Obtenir le FQDN de l'élément de configuration Action de flux

Le champ **Orchestration courante de sécurité** > **Obtenir le FQDN de l'élément de configuration** L'action de flux récupère le nom de domaine complet (FQDN) d'un élément de configuration. Cette action de flux peut accélérer le processus d'enquête et de correction.

L'action Obtenir le FQDN de l'élément de configuration peut être utilisée avec n'importe quel flux pour récupérer le nom de domaine complet (FQDN) d'un élément de configuration.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action de flux.

Variables d'entrée

Variable	Description
cmdb_ci.id [chaîne]	L'identificateur système (sys_id) d'un enregistrement d'élément de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
FQDN [chaîne]	Nom de domaine complet (FQDN) de l'élément de configuration.

Remarques supplémentaires

Le champ fqdn de l'élément de configuration doit être renseigné.

Activité Déterminer les observables

L'activité de workflow **Déterminer les observables** détermine l'observable à inclure dans le workflow

L'activité **Déterminer les observables** peut être utilisée avec n'importe quel workflow pour déterminer les observables à inclure dans le workflow.

Résultats

Les résultats possibles de cette activité sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Observables trouvés
Échec	Aucun observable trouvé. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
task_sys_id	Identificateur de tâche (mappe les incidents de sécurité aux observables).
observables	Adresses IP, hachage, URL, noms de domaine.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
observables	Observables filtrés

Action Obtenir les options de sécurité prises en charge

L'action de flux Obtenir les options prises en charge récupère le nom et le nombre d'intégrations qui sont actives et prennent en charge l'aptitude demandée.

L'action Obtenir les options prises en charge peut être utilisée avec n'importe quel flux pour déterminer quelles options sont prises en charge.

Résultats

Les résultats possibles pour cette action sont les suivants :

Résultats

Résultat	Description
Réussite	Intégration qui prend en charge l'aptitude trouvée.
Échec	Une erreur s'est produite lors de la tentative de recherche d'une intégration active qui prend en charge l'aptitude. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variable	Description
capabilityName	Nom de l'option.
taskId	Identificateur système pour toute tâche associée au flux.
domainId	Identificateur système de tout domaine associé au flux.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
SupportedCapabilities	Liste des intégrations qui prennent en charge l'option.
nombre d'aptitudes	Nombre d'intégrations qui prennent en charge l'option.

Suivi de l'exécution de l'aptitude : aucune action d'implémentation

L'action de flux Suivi de l'exécution de l'aptitude - aucune implémentation crée un enregistrement d'erreur lorsqu'aucune implémentation d'aptitude d'intégration n'est trouvée.

L'action Suivi de l'exécution de l'aptitude : aucune implémentation peut être utilisée avec n'importe quel flux d'aptitude d'intégration abstrait pour gérer la condition d'erreur lorsqu'aucune implémentation d'aptitude configurée n'est disponible.

Résultats

Les résultats possibles pour cette action sont les suivants :

Résultats

Résultat	Description
Réussite	L'état de l'enregistrement du suivi des exécutions est défini sur **Erreur** et un message indiquant que l'erreur est enregistrée.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variable	Description
capabilityExecutionId	Identificateur système pour l'enregistrement d'audit. Sortie de l'action utilisée pour commencer le suivi des exécutions.
nom du flux	Nom du flux. Fourni par le système.

Variables de sortie

Il n'existe aucune variable de sortie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une action de recherche de conformité

L'action Créer une recherche de conformité crée une recherche de conformité pour les e-mails dans le ou les serveurs Exchange désignés à l'aide des requêtes de recherche définies et renvoie le nom de la recherche de conformité créée.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variable	Description
search_query	Requête de recherche obligatoire utilisée pour trouver des e-mails dans le serveur Exchange dans toutes les boîtes aux lettres.
Emplacement Exchange	Champ d'emplacement obligatoire utilisé pour effectuer une recherche sur l'ensemble de l'emplacement défini. Les valeurs possibles sont les suivantes : • Tous • Nom de boîte de réception spécifique
targetId	Champ d'identificateur obligatoire de l'hôte cible où se trouve le serveur Exchange.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
réponse	Nom de la recherche de conformité créée.

Conditions de sortie

Les conditions de sortie possibles pour cette action sont les suivantes :

Conditions de sortie

Variable	Description
Échec de la création de la recherche	Lorsque la création de la recherche échoue en raison d'une exception dans le serveur Exchange.
Recherche créée avec succès	Lorsque la création de recherche est réussie.
Échec de la création de la recherche en raison d'une erreur d'analyse	Lorsque la création de la recherche échoue en raison d'un problème d'analyse.
Erreur	Lorsqu'une exception se produit dans l'action de flux.

Obtenir l'adresse IP à partir de l'activité du CI

Cette activité de workflow détermine l'adresse IPV4 associée à un élément de configuration (CI).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’activité **Obtenir l’adresse IP à partir du CI** peut être utilisée avec n’importe quel workflow pour récupérer l’adresse IPv4 d’un CI.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
ci_sys_id [chaîne]	Identificateur système de l’élément de configuration

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
ip_addr [chaîne]	Adresse IPv4. Si l’adresse IP ne peut pas être déterminée, cette valeur est vide.

Conditions de sortie

Les résultats possibles de cette activité sont les suivants :

Conditions

Condition	Description
Réussite	Une adresse IPv4 a été renvoyée.
Échec	Une adresse IPv4 n’a pas pu être déterminée.

Obtenir les statistiques réseau via netstat Action de flux

L’action de flux Orchestration commune de sécurité - Obtenir les statistiques réseau via netstat récupère les statistiques réseau d’une ressource affectée sur un système Windows. Cette action de flux peut accélérer le processus d’enquête et de correction.

L’action Obtenir les statistiques réseau via le flux netstat peut être utilisée avec n’importe quel flux pour récupérer les statistiques réseau d’un système Windows. La machine est interrogée avec la commande **netstat** incluant les paramètres **-a** et **-o** . Pour améliorer les données de sortie, **la commande get-process** est également appelée.

Résultats

Les résultats possibles pour cette action de flux sont les suivants :

Résultats

Résultat	Description
Réussite	Les statistiques du réseau ont été récupérées au format JSON.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats (suite)

Résultat	Description
Échec	Une erreur s'est produite lors de la tentative de récupération des statistiques réseau. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'action de flux.

Variables d'entrée

Variable	Description
Cible [chaîne]	Nom de domaine complet (FQDN) ou adresse IP du système cible.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Réponse [chaîne]	Chaîne JSON représentant les processus en cours d'exécution sur l'ordinateur cible. Les données JSON comprennent : **pid** Identificateur de processus **_port locale** Port local de la transaction réseau **État** État de la connexion TCP. **Remarque :** Ce champ est nul pour les connexions UDP. **local_address** Nom de domaine complet local (FQDN) ou adresse IP **remote_address** Nom de domaine complet (FQDN) ou adresse IP distante **protocol** TCP ou UDP **remote_port** Port distant de la transaction réseau **chemin d'accès** Chemin d'accès au fichier de l'exécutable du processus **hachage** Valeur de hachage de l'exécutable du processus. Le hachage est dans SHA-256 pour PowerShell V4 ou version ultérieure. Sinon, le hachage est dans MD5.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Restrictions

Le Serveur MID doit prendre en charge PowerShell.

Le hachage SHA-256 nécessite PowerShell V4.

Obtenir les processus en cours d'exécution via l'activité WMI

L'activité de workflow**Obtenir l'exécution des processus** récupère les processus en cours d'exécution d'un élément de configuration sur un système Windows. Cette activité peut accélérer le processus d'enquête et de correction.

L'activité **Get Running Processes via WMI** peut être utilisée avec n'importe quel workflow pour récupérer les processus en cours d'exécution sur un système Windows.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
Cible [chaîne]	Nom de domaine complet (FQDN) ou adresse IP du système cible.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Réponse [chaîne]	Chaîne JSON représentant les processus en cours d'exécution sur le système cible. Les données JSON comprennent : **pid** L'identificateur du processus **nom** Nom du processus De plus, si disponible : **Propriétaire** Nom du propriétaire du processus **owner_sid** L'identificateur système du propriétaire du processus **owner_domain** Le domaine du propriétaire du processus **chemin d'accès** Chemin d'accès au fichier de l'exécutable du processus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie (suite)

Variable	Description
	hachage Valeur de hachage de l'exécutable du processus. Le hachage est dans SHA-256 pour PowerShell V4 ou version ultérieure. Sinon, le hachage est dans MD5.

Restrictions

Le Serveur MID doit prendre en charge **PowerShell**.

Le hachage SHA-256 nécessite PowerShell V4.

Vérifier la conformité Action d'état de recherche

L'action Vérifier l'état de la recherche de conformité vérifie l'état de la recherche de conformité créée sur le serveur Exchange et, si l'état est terminé, renvoie les informations relatives à la recherche d'e-mails trouvée pour la recherche de conformité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'action.

Variable	Description
targetId	Champ d'identificateur obligatoire de l'hôte cible où se trouve le serveur Exchange.
searchName	Nom obligatoire de la recherche de conformité créée sur le serveur Exchange.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les actions suivantes.

Variables de sortie

Variable	Description
réponse	Contient l'état de la recherche de conformité et le nombre d'e-mails trouvés sur le serveur Exchange pour la recherche de conformité.

Conditions de sortie

Les conditions de sortie possibles pour cette action sont les suivantes :

Conditions de sortie

Variable	Description
Recherche en cours	Lorsque l'état de la recherche de conformité est en cours.
Recherche terminée : aucun e-mail de menace trouvé	Lorsque l'état de la recherche de conformité est terminé et qu'aucun e-mail n'est trouvé dans le cadre de la recherche de conformité.
Recherche terminée : e-mails de menace trouvés	Lorsque l'état de la recherche de conformité est terminé et que les e-mails sont trouvés dans le cadre de la recherche de conformité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions de sortie (suite)

Variable	Description
Erreur lors de la vérification de l'état	Lorsque la vérification de l'état échoue en raison d'une exception dans le serveur Exchange.
Erreur	Lorsqu'une exception se produit dans l'action de flux.

Mettre à jour l'activité des notes de travail de la tâche

L'activité **de workflow Orchestration commune de sécurité - Mettre à jour les notes de travail de tâche** met à jour la section **Activité** (notes de travail) d'un enregistrement de tâche. Ceci est utile pour les informations de journalisation.

L'activité **Mettre à jour les notes de travail de la tâche** peut être utilisée avec n'importe quel workflow pour mettre à jour les notes de travail de n'importe quel enregistrement de tâche.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
task_id [chaîne]	L'identificateur système (sys_id) d'un enregistrement de tâche.
Contenu [chaîne]	Données inscrites dans les notes de travail d'une tâche.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Résultat [chaîne]	Indique si la mise à jour a réussi.

Déployer les informations de recherche dans l'activité d'incident de sécurité

La recherche **d'informations de déploiement sur l'activité d'incident de sécurité** peut être utilisée avec n'importe quel workflow pour recueillir des informations à partir d'une recherche de menaces et générer un résumé du contenu ainsi que l'ID de l'incident de sécurité d'origine dans les notes de travail de la tâche.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Résumé du rapport de recherche déployé jusqu'à l'incident de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats (suite)

Résultat	Description
Échec	La tâche d'origine et le rapport de résumé de la recherche sont vides.

Variables d'entrée

Variable	Description
scanID[chaîne]	Identificateur de recherche.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
siId[chaîne]	Identificateur d'incident de sécurité.
Réponse [chaîne]	Résumé des résultats de la recherche, y compris la valeur IoC, le résultat, le motif de la défaillance, la référence de recherche, etc.

Workflow Mettre à jour l'incident de sécurité avec les résultats de la recherche

Le workflow **Mettre à jour l'incident de sécurité avec les résultats de la recherche** met à jour les incidents de sécurité existants avec les résultats de la recherche.

Avant de commencer
Rôle requis : sn_si.basic

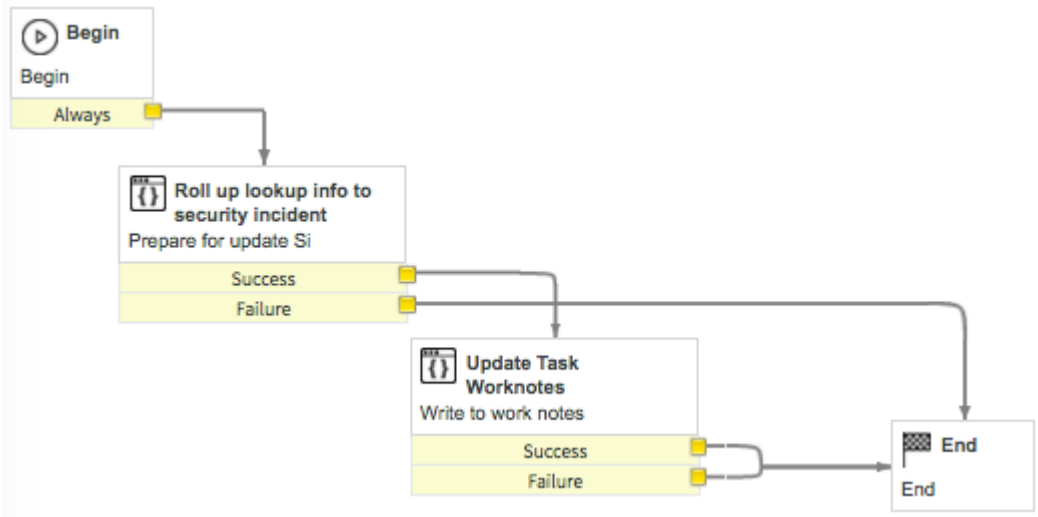
Pourquoi et quand exécuter cette tâche
Ce workflow est déclenché par une règle métier sur la table de recherche qui surveille quand le champ **Résultat** passe à Échec.

Les activités du processus de workflow comprennent :

- Déployer les informations de recherche dans l'activité d'incident de sécurité
- Mettre à jour l'activité des notes de travail de la tâche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Filtrer l'activité des observables sur la liste d'autorisation

L'activité de workflow Observables filtrés sur liste d'autorisation supprime les observables qui peuvent être ignorés de la liste des observables. Cette activité peut accélérer le processus d'enquête et de correction.

L'activité Filtrer les éléments observables sur liste d'autorisation peut être utilisée avec n'importe quel workflow pour filtrer les éléments observables avant d'entreprendre une action.

Résultats

Les résultats possibles de cette activité sont les suivants :

Résultats

Résultat	Description
Réussite	Liste de filtres créée.
Échec	Une erreur s'est produite lors de la tentative de filtrage des observables. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
observables	Liste des observables disponibles.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Variables de sortie

Variable	Description
filteredObservables	Observables filtrés.

Écrire le contenu à enregistrer en tant qu'activité de pièce jointe

Cette activité écrit le contenu transmis à partir d'une entrée et crée une pièce jointe désignée à un enregistrement donné.

L'activité **Écrire du contenu à enregistrer en tant que pièce jointe** peut être utilisée avec n'importe quel workflow pour écrire du contenu et le joindre à un enregistrement.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variables d'entrée

Variable	Description
nom de table [chaîne]	Nom de la table de l'enregistrement. Ce champ d'entrée est obligatoire.
sysid [chaîne]	L'identificateur système (sys_id) d'un enregistrement de tâche. Ce champ d'entrée est obligatoire.
charge utile	Le contenu en texte brut à écrire en tant que pièce jointe. Ce champ d'entrée est obligatoire.
nom de fichier	Nom du fichier de la pièce jointe.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
Résultat [chaîne]	Indique si la mise à jour a réussi.

Obtenir l'adresse IP à partir de l'activité du CI

L'activité Obtenir l'adresse IP à partir du flux CI rassemble l'adresse IP à partir des éléments de configuration (CI) à utiliser dans le flux.

L'activité Obtenir l'adresse IP à partir du CI peut être utilisée avec n'importe quel flux pour collecter des adresses IP d'éléments de configuration (CI) à utiliser dans le flux.

Résultats

Les résultats possibles de cette activité sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Résultat	Description
Réussite	Adresses IP trouvées.
Échec	Aucune adresse IP trouvée. Plus d'informations sur l'erreur sont disponibles dans l'erreur de sortie de l'activité.

Variables d'entrée

Les variables d'entrée déterminent le comportement initial de l'activité.

Variable	Description
ci_sys_id	Identificateur d'élément de configuration.

Variables de sortie

Les variables de sortie contiennent des données qui peuvent être utilisées dans les activités ultérieures.

Variables de sortie

Variable	Description
ip_addr	Adresses IP.

Opérations de sécurité Déclencheurs de workflow

Opérations de sécurité Les déclencheurs de workflow contiennent une condition dans une table. Tous les workflows joints à l'enregistrement de déclencheur de workflow s'exécutent lorsque la condition est remplie.

Créer des Opérations de sécurité déclencheurs de workflow

Créez un déclencheur de workflow qui contient une condition dans une table.

Avant de commencer

Opérations de sécurité contient plusieurs déclencheurs de workflow dans le système de base :

Changements d'élément de configuration sur un incident de sécurité actif

Utilise l'intégration pour enrichir les données liées aux CI à mesure que les éléments de configuration changent.

Analyser de nouveau le groupe vulnérable

Scanne à nouveau un groupe vulnérable à l'aide de , Workflow Analyser la vulnérabilité lorsque vous **fermez/ignorez** le groupe.

Analyser de nouveau l'élément vulnérable

Scanne à nouveau un élément vulnérable à l'aide de la Workflow Analyser l'élément de vulnérabilité touche **Lorsque vous fermez/ignorez** l'élément.

Rôles requis :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lire : sn_sec_cmn.read
- Pour créer ou mettre à jour : sn_sec_cmn.write
- À supprimer : sn_sec_cmn.admin

Procédure

1. Accédez à la **Tous** > **Security Operations** > **Utilités** > **Déclencheurs de workflow**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire comme il convient.

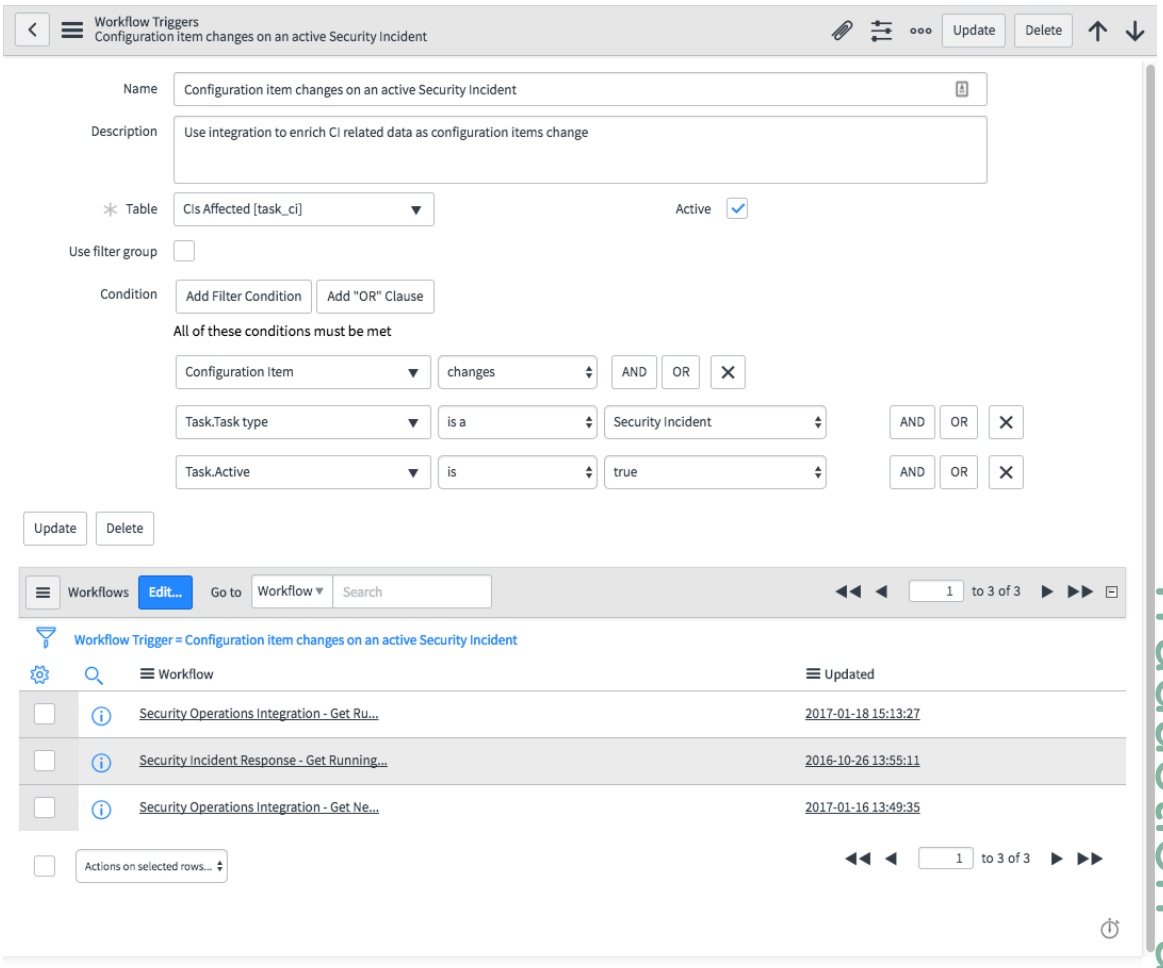
Déclencheurs de workflow

Champ	Description
Nom	Nom du déclencheur de workflow.
Description	Entrez une description pour le déclencheur de workflow.
Table	Table contenant le déclencheur de workflow. Si vous avez coché la case **Utiliser un groupe de filtres** et sélectionné un groupe de filtres, ce champ est défini par défaut sur la table associée au groupe de filtres sélectionné.
Condition	Utiliser le Créateur de conditions permettant de définir les critères du déclencheur de workflow. Si vous avez coché la case **Utiliser un groupe de filtres** et sélectionné un groupe de filtres, les champs **de condition** ne s'affichent pas.
Actif	Cochez cette case pour activer le déclencheur de workflow.
Utiliser un groupe de filtres	Cochez cette case pour utiliser un groupe de filtres prédéfini ou créer un nouveau groupe de filtres pour définir les critères de déclenchement du workflow.
Groupe de filtres	Sélectionnez le groupe de filtres à utiliser pour définir les déclencheurs de workflow. Ce champ s'affiche uniquement si la case **Utiliser des groupes de filtres** est cochée.

4. Lorsque vous avez terminé vos entrées, faites un clic droit dans l'en-tête du formulaire et sélectionnez **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'onglet **Workflows** s'affiche. Il contient des workflows qui sont exécutés lorsque toutes les conditions de filtre ou celles de groupe de filtres sont remplies.

5. Pour ajouter des workflows, procédez comme suit.
   a. Dans l'onglet **Workflows** , cliquez sur **Modifier**.
   b. Utilisez le générateur de conditions, si nécessaire, pour localiser les workflows à sélectionner, ou utilisez la zone de liste double pour sélectionner des workflows et les déplacer vers la liste Workflows.
   c. Cliquez sur **Enregistrer**.
   Les workflows sélectionnés sont ajoutés.
6. Cliquez sur **Mettre à jour**.

Orchestration de Security Operations

Les utilisateurs peuvent interagir et récupérer des données sur des systèmes et environnements Windows ou UNIX à l'aide de packs d'activités et de workflows dans Orchestration des Opérations de sécurité.

Orchestration des Opérations de sécurité permet de gagner du temps en éliminant les processus manuels et en obtenant des informations contextuelles pour corriger les incidents. Les Opérations de sécurité produits ont des packs d'activités et des flux de travail standard qui sont inclus et activés dans chacun des plugins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour créer et accéder à des activités Orchestration supplémentaires qui ne sont pas disponibles avec les produits de l'offre Opérations de sécurité standard, achetez une licence Orchestration complète.

- Orchestration de la réponse aux incidents de sécurité Flux de travail :
  - Security Incident Response - Obtenir le flux de statistiques réseau
  - Intégration des commandes du système Security Operations : obtenir le flux d'exécution des processus
  - Créer une demande de recherche de workflow de changements IoC
  - Security Operations Integration : flux de recherche et de suppression d'e-mails
- Orchestration des renseignements sur les menaces Flux de travail :
  - Renseignements sur les menaces - Exécuter le workflow de recherche IoC
  - Workflow Mettre à jour l'incident de sécurité avec les résultats de la recherche
- Orchestration de la réponse aux vulnérabilités Flux de travail :
  - Workflow Analyser la vulnérabilité
  - Workflow Analyser l'élément de vulnérabilité

Opérations de sécurité et le ServiceNow Store

MadridÀ partir de , toutes les Opérations de sécurité applications et intégrations prises en charge peuvent être téléchargées à partir du ServiceNow Store. Cela vous permet d'obtenir plus rapidement des fonctionnalités nouvelles et mises à jour. Avant de pouvoir utiliser des Opérations de sécurité applications, vous devez vérifier que vous y avez droit (c'est-à-dire que vous disposez de licences valides pour les utiliser), les télécharger à partir de et ServiceNow Store les activer.

La liste toujours croissante des Opérations de sécurité applications disponibles au téléchargement comprend :

- Réponse aux incidents de sécurité (et les intégrations prises en charge)
- Réponse aux vulnérabilités (et les intégrations prises en charge)
- Renseignements sur les menaces (et les intégrations prises en charge)
- Conformité de la configuration
- Trusted Security Circle
- Data Loss Prevention Incident Response

Regardez cette vidéo de cinq minutes pour en savoir plus sur le ServiceNow Store téléchargement des applications Security Operations et GRC à partir du . Cette vidéo de 5 minutes décrit comment télécharger les applications Security Operations et GRC à partir du ServiceNow Store

Le processus que vous utilisez pour obtenir Opérations de sécurité des applications et des intégrations varie selon que vous téléchargez une application pour la première fois, que vous mettez à jour une application que vous avez précédemment téléchargée à partir de ou ServiceNow Store que vous effectuez une mise à niveau d'une version de famille vers la suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Télécharger une application à partir de ServiceNow Store pour la première fois

Le téléchargement d'une application à partir du ServiceNow Store pour la première fois implique un certain nombre d'étapes faciles. Certaines étapes sont effectuées sur le et d'autres ServiceNow Store dans votre instance.

Le vous ServiceNow Store permet de télécharger des produits et applications principaux. Un produit contient une ou plusieurs applications sous licence en tant que groupe. Par exemple, Réponse aux incidents de sécurité est un produit. Le processus comporte les étapes suivantes :

Rôle requis : admin.

- Dans le ServiceNow Store, vous devez vous assurer que vous disposez des droits (ou licences) sur l'application et ses applications dépendantes.

  Remarque : Ce processus s'applique uniquement aux applications qui sont téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de non-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

- Enfin, vous pouvez activer l'application et l'exécuter sur votre instance.

Remarque : À partir des versions précédentes et ultérieures, les modules d'extension de Rome dépendance sont automatiquement activés lorsque vous activez une application principale. Par exemple, lorsque vous activez l'application Réponse aux vulnérabilités , le module d'extension Réponse aux vulnérabilités Dependencies est également activé. Pour plus d'informations, consultez Activer une ServiceNow Store application.

Obtenir une autorisation pour un produit ou une Opérations de sécurité application

La première étape de l'installation d'une Opérations de sécurité application consiste à vérifier que l'application ou le produit et ses applications associées disposent d'autorisations valides ServiceNow .

Avant de commencer

Rôle requis : admin

Les personnes exécutant le droit doivent avoir un compte et avoir l'autorisation de demander des Now Support applications pour les instances à l'étude.

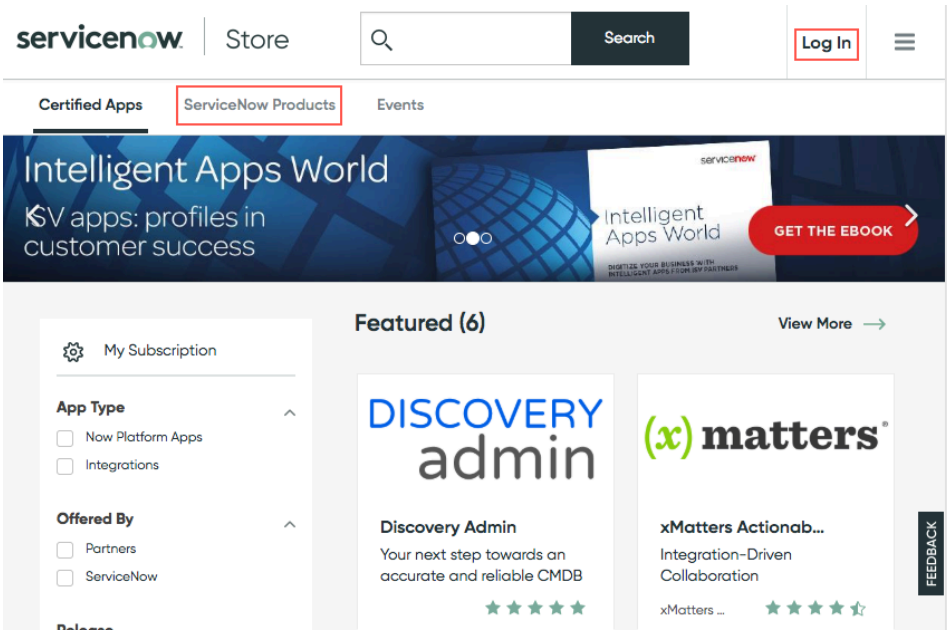
Remarque : Ce processus s'applique uniquement aux applications téléchargées vers les instances de production. Si vous téléchargez des applications vers des instances de sous-production ou de développement, il n'est pas nécessaire d'obtenir des autorisations. Passez à .Activer une ServiceNow Store application

Traduction automatique

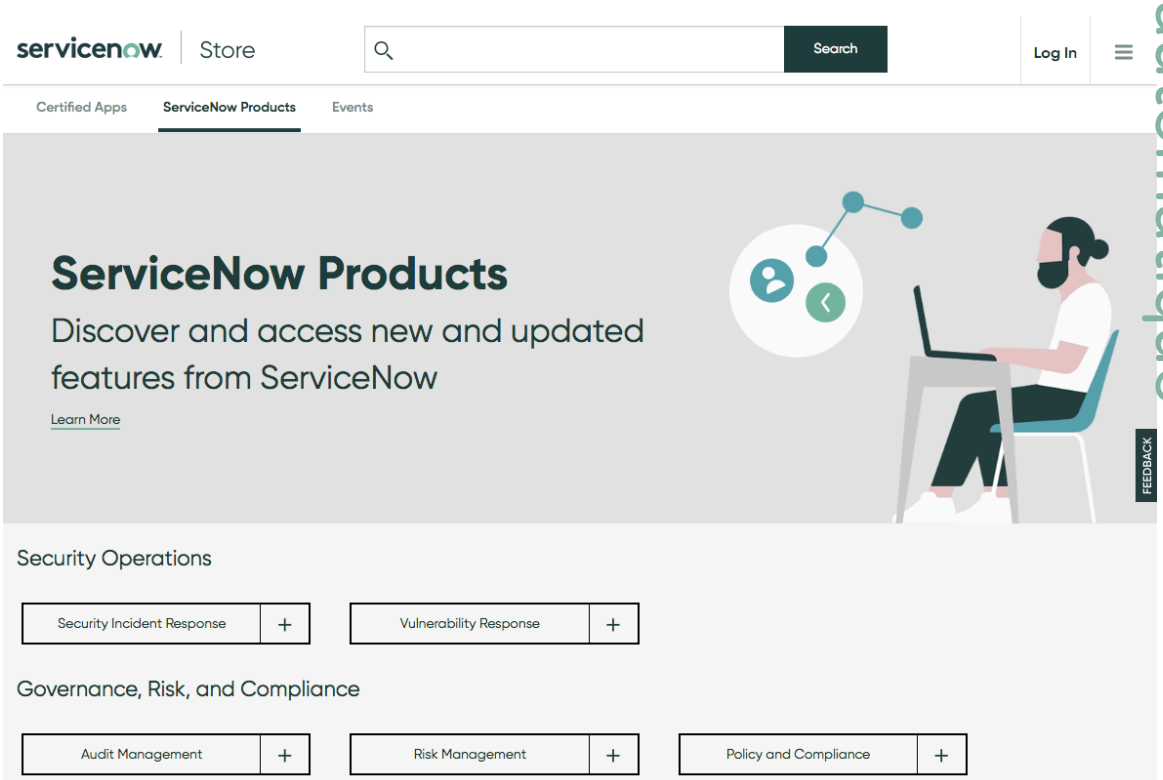
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez au ServiceNow Store .



2. Cliquez sur **Connexion** et connectez-vous à l'aide de vos HI informations d'identification.
3. Cliquez sur l'onglet **Produits ServiceNow** pour afficher tous les produits disponibles ServiceNow . Les intégrations et d'autres types de contenu sont affichés dans l'onglet **Applications certifiées** .



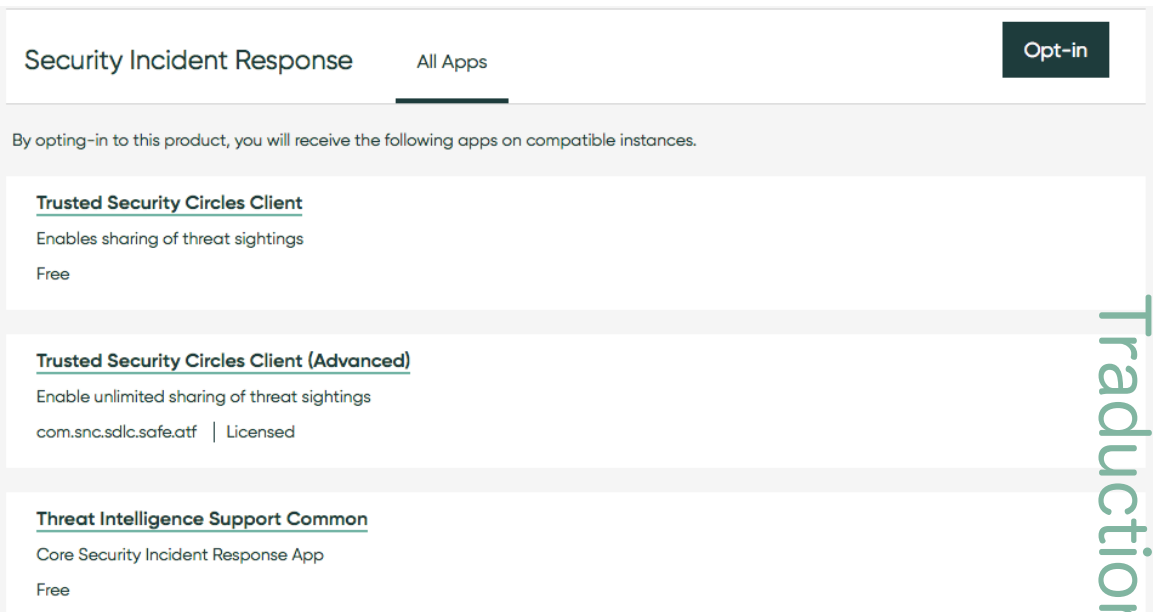
Remarque : Pour les besoins de cet exemple, supposons que vous acquérez une autorisation pour le Réponse aux incidents de sécurité produit.

Traduction automatique

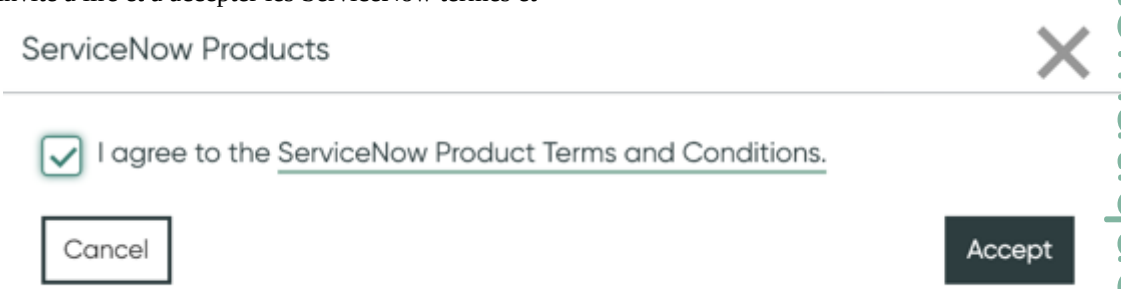
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur le signe plus (+) en regard du nom du produit auquel vous avez droit.
   Toutes les applications associées au produit auquel vous êtes autorisé sont répertoriées. Lorsque vous avez obtenu l'autorisation pour le produit principal, les applications qui y sont répertoriées sont également autorisées.

   Remarque : Vous pouvez également cliquer sur le nom du produit pour afficher plus d'informations sur le produit et ses applications associées.



5. Cliquez sur **Accepter** pour vérifier que vous disposez des droits pour le produit et les applications répertoriées.
   Vous êtes invité à lire et à accepter les ServiceNow termes et



   conditions.

6. Cochez la case et cliquez sur **Accepter**.
7. Notez qu'une coche apparaît en regard du nom du produit et que le bouton Gérer les autorisations s'affiche.

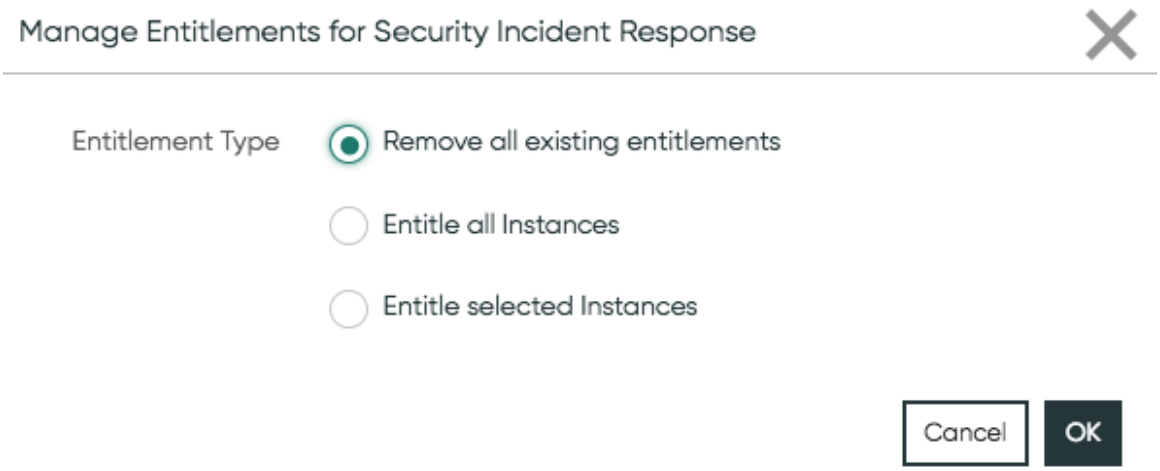


   La coche indique que vous êtes abonné au produit et à ses applications associées. Il est temps de gérer vos droits. Il s'agit d'un processus unique pour ce produit et tous les autres produits que vous souhaitez installer à l'avenir.

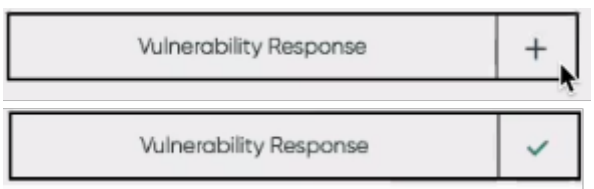
8. **Facultatif :** Vous pouvez cliquer sur **Gérer les autorisations** pour modifier les instances affectées par les applications auxquelles vous avez droit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Une fois que vous avez accepté les ServiceNow conditions générales et géré les droits, vous pouvez autoriser d'autres produits en un seul clic.



Remarque : Vous êtes prêt à activer le produit.

Activer une ServiceNow Store application

Une fois qu'une application a reçu une autorisation, vous devez activer son module d'extension dépendances et activer l'application. Ce processus s'applique également aux applications téléchargées vers des instances de sous-production.

Avant de commencer

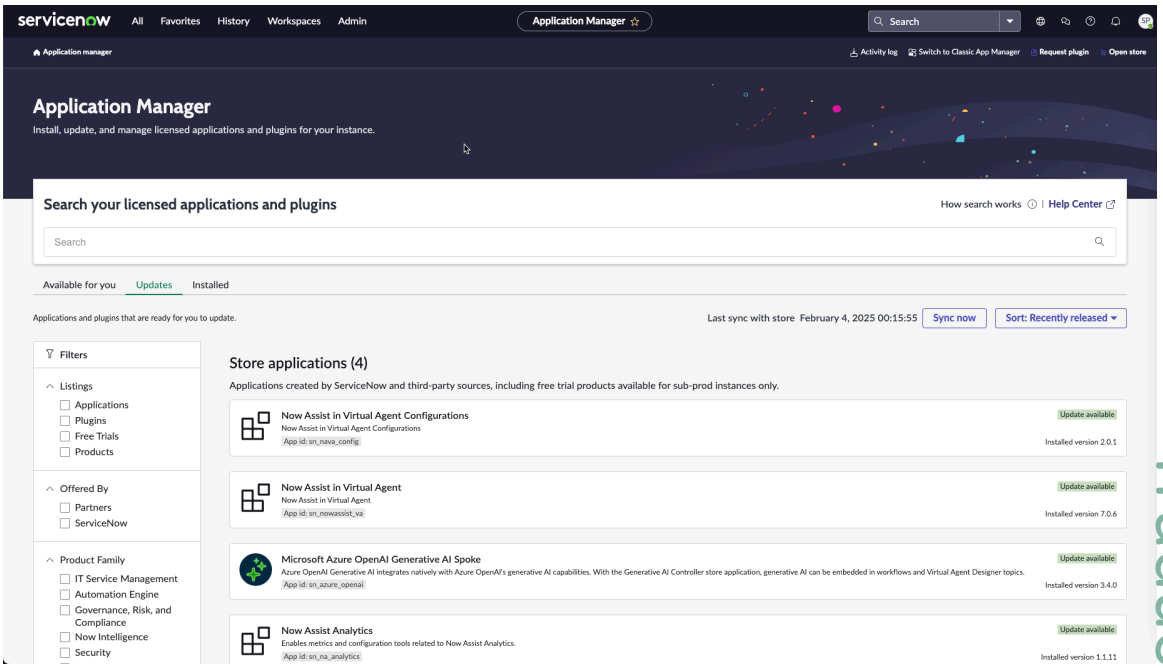
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

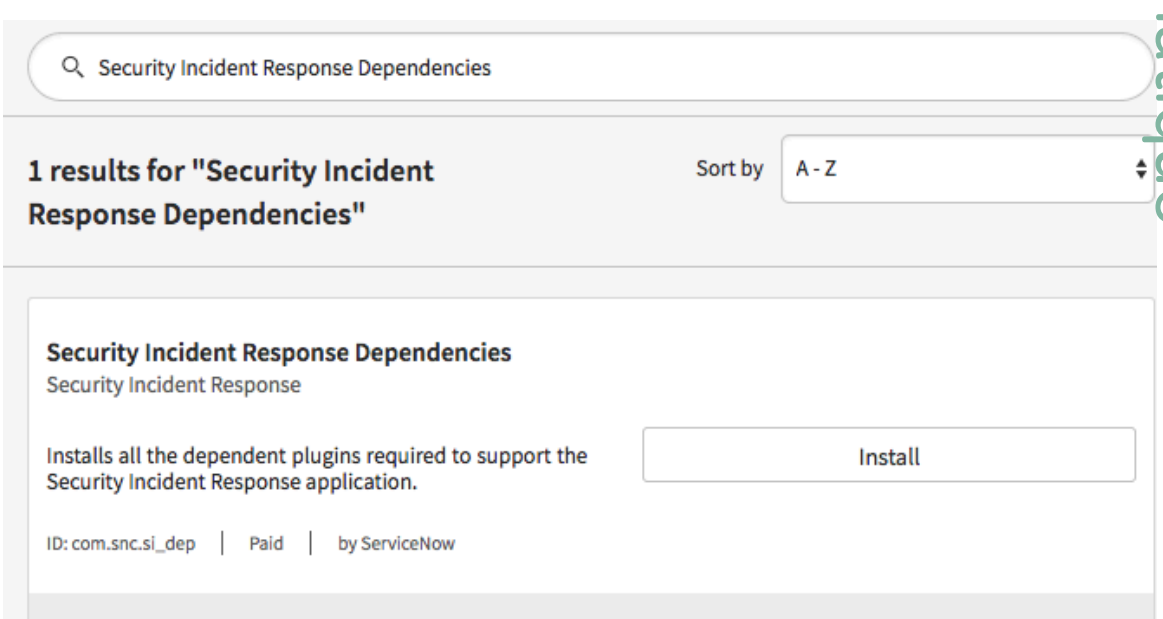
Procédure

1. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous**.



Remarque : À partir d'Orlando, les modules d'extension de dépendance sont automatiquement activés lorsque vous activez une application principale. Par exemple, lorsque vous activez l'application Réponse aux vulnérabilités , le module d'extension Réponse aux vulnérabilités Dependencies est également activé. Par conséquent, les étapes 2 à 5 sont facultatives.

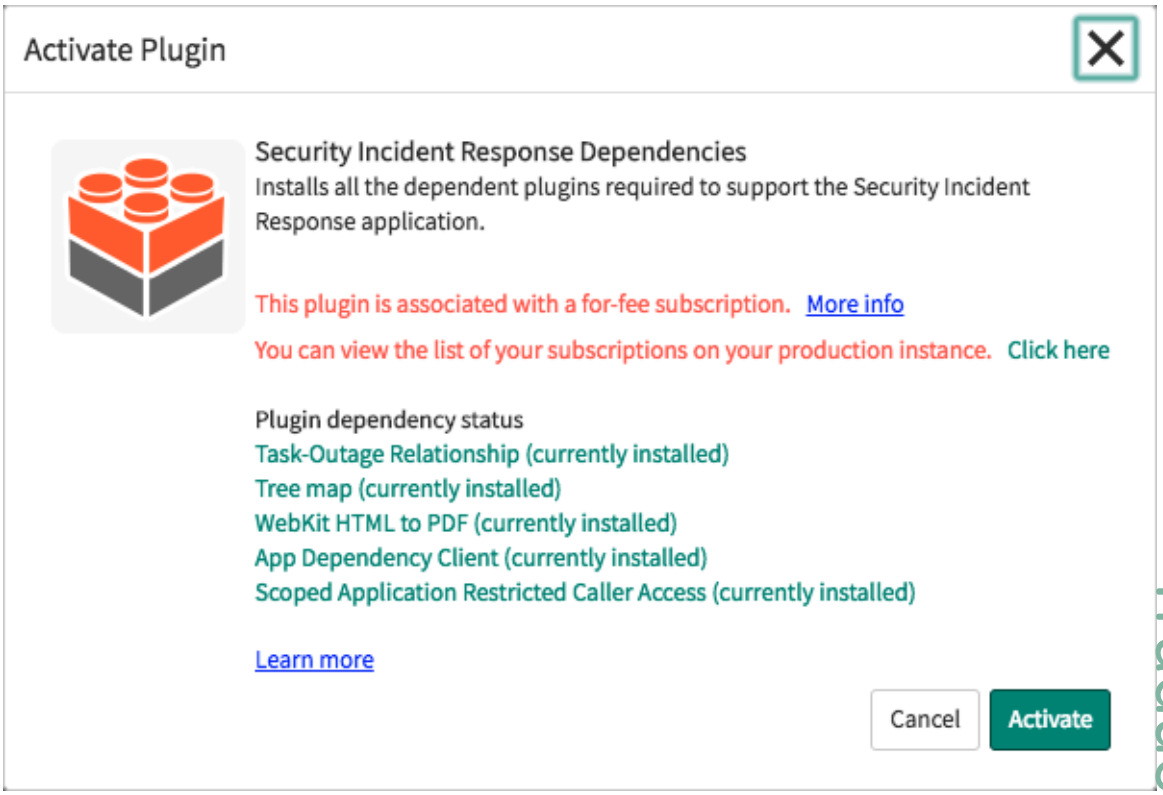
2. Recherchez le module d'extension dépendances de l'application que vous souhaitez activer.
   Par exemple, si vous activez Réponse aux incidents de sécurité, localisez le module d'extension Réponse aux incidents de sécurité Dependencies.



3. Cliquez sur **Installer**.
   La boîte de dialogue Activer le module d'extension s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Dans la boîte de dialogue **Activer le module d'extension** , cliquez sur **Activer**.
5. Lorsque l'activation est terminée, cliquez sur **Fermer et recharger le formulaire**.
6. Localisez maintenant le produit principal que vous activez, cochez la case **Installer avec des données de démonstration** si vous souhaitez charger les données de démonstration, puis cliquez sur **Installer**. Votre application est automatiquement installée sur votre instance.

> **Remarque :** Si vous ne sélectionnez pas la case **à cocher Installer avec des données de démonstration** , les données de démonstration ne seront pas disponibles pour une installation ultérieure à partir du **gestionnaire d'applications** . Pour plus d'informations sur l'installation ou la réinstallation des données de démonstration après l'installation initiale, consultez l'article Solution de contournement pour installer les données de démonstration si l'application est déjà installée [KB0722909] dans la base de HI connaissances.

Installer une Opérations de sécurité intégration

Toutes les ServiceNow intégrations sont disponibles sur le .ServiceNow Store Les applications principales, telles que Réponse aux incidents de sécurité, sont visibles dans l'onglet **Produits ServiceNow** du magasin. Les modules complémentaires d'intégration sont visibles dans l'onglet **Applications certifiées** .

Avant de commencer

Rôle requis : admin

Les installations de stockage nécessitent un compte et une autorisation pour demander des Now Support applications pour les instances à l'étude.

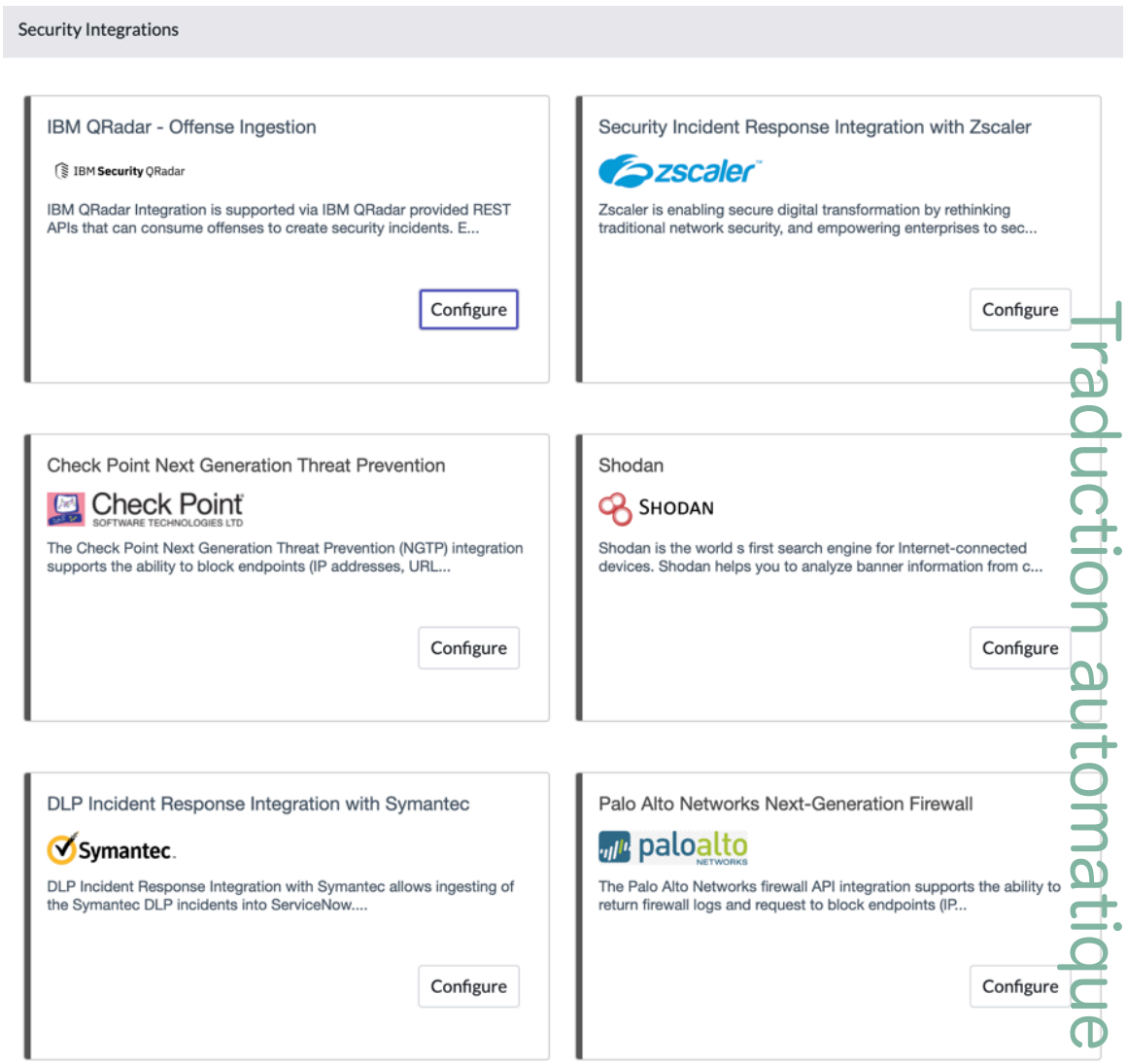
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Security Operations** > **Intégrations** > **Configurations d'intégration** après avoir installé l'application à partir de ServiceNow Store.
   Les tuiles de configuration pour les intégrations s'affichent

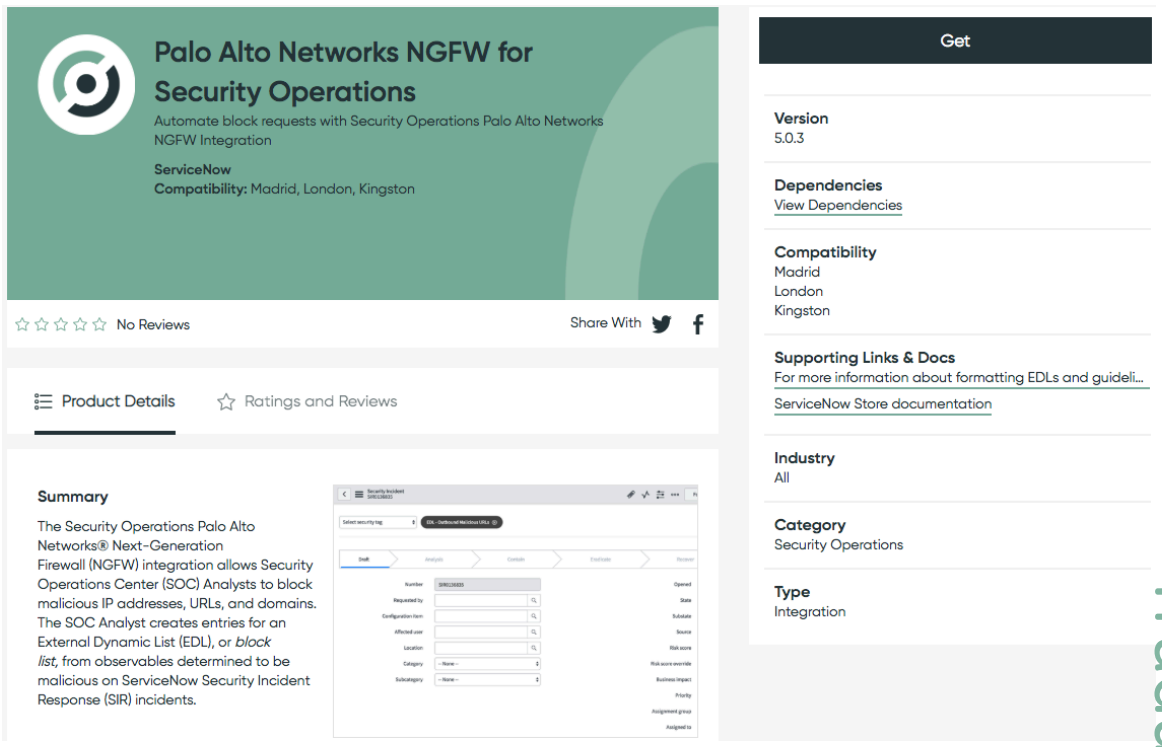
Remarque :



2. Recherchez l'intégration que vous souhaitez installer, puis cliquez sur **Configurer**.
   L'intégration sélectionnée est affichée dans le ServiceNow Store

Traduction automatique

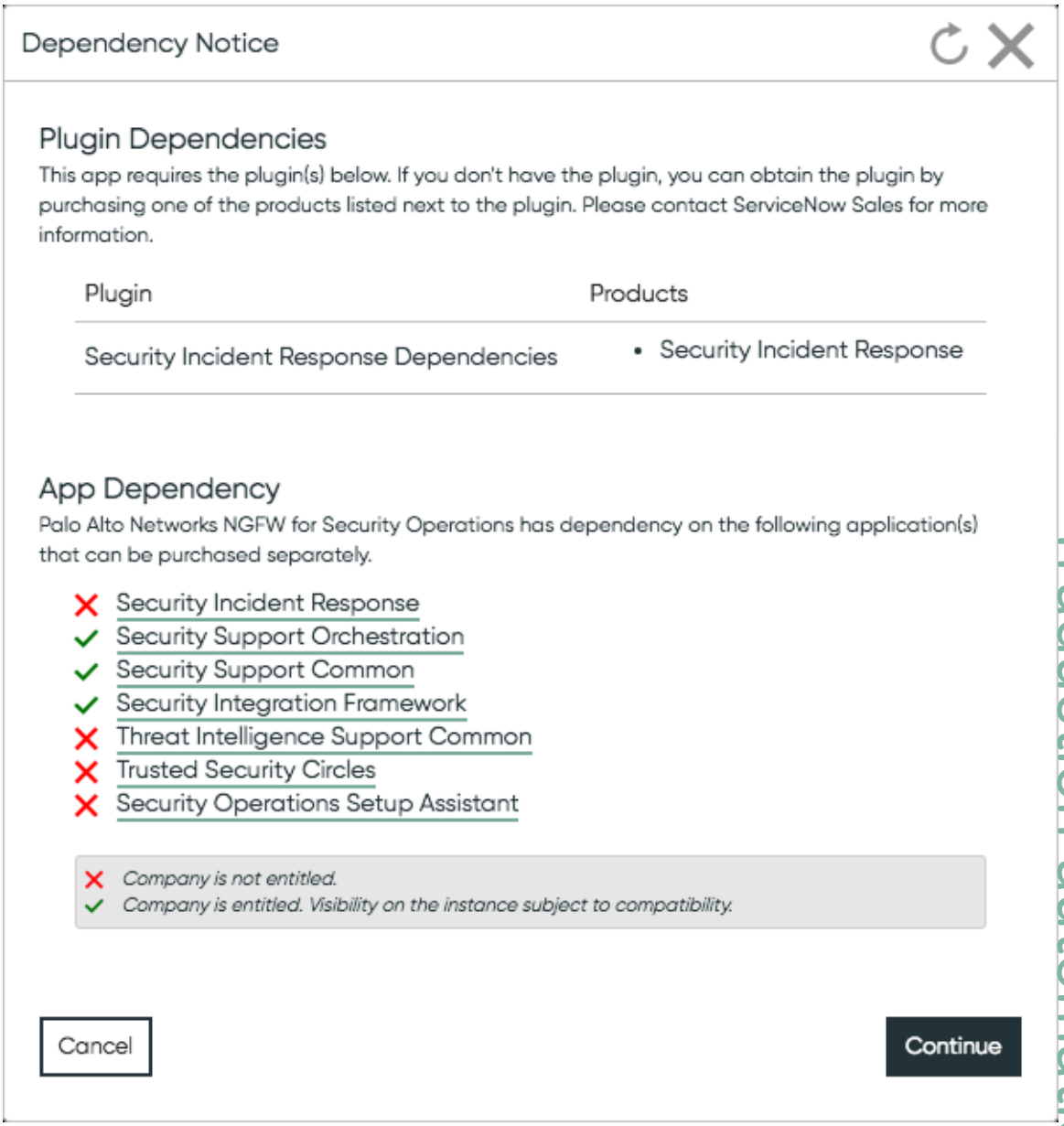
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur **Afficher les dépendances** et passez en revue les dépendances d'application répertoriées.

Traduction automatique

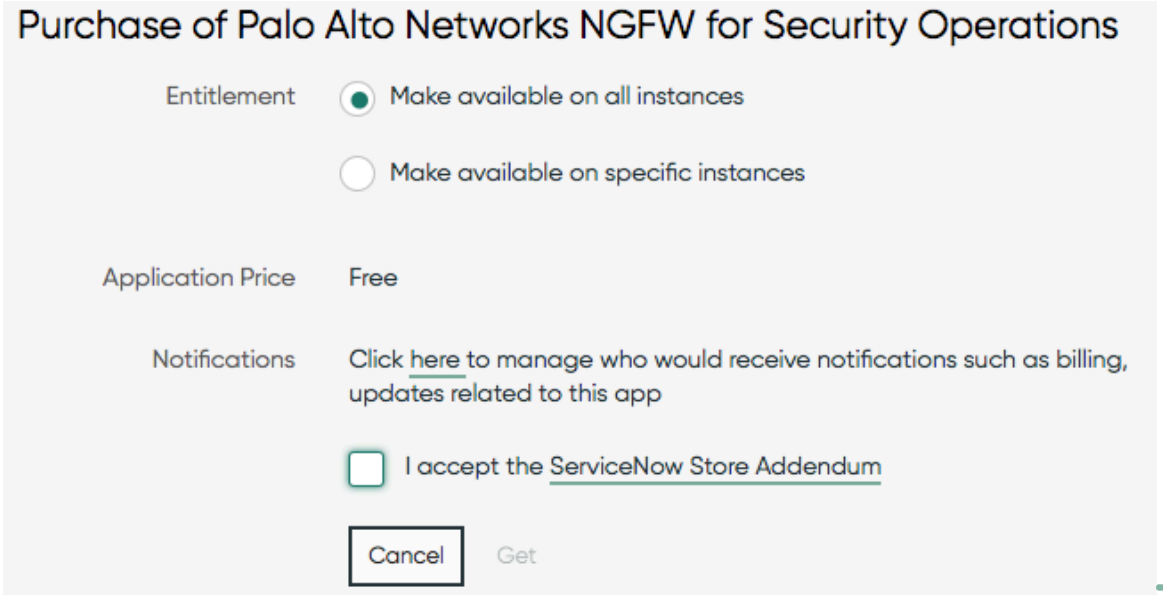
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

4. Si l'intégration comporte des dépendances d'application principales, telles que Réponse aux incidents de sécurité, auxquelles votre société n'est pas encore autorisée :
   a. Suivez ces instructions pour obtenir des autorisations, télécharger les modules d'extension de dépendance et activer les applications.
   b. Revenez à cette procédure.
   c. Cliquez sur **Continuer**.
5. Cliquez sur **Télécharger**.
   Les termes et conditions de ServiceNow s'affichent.
6. Cliquez sur **Continuer**.
   Un écran d'achat similaire au suivant s'ouvre.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Identifiez les instances sur lesquelles vous souhaitez que l'intégration soit disponible, gérez vos notifications et cochez la case **Addendum du ServiceNow Store** .
8. Cliquez sur **Télécharger**.

   Remarque : Si vous téléchargez une demande d'achat, cliquez sur **Acheter**. Si vous téléchargez une application qui nécessite l'approbation préalable du fournisseur, cliquez sur Demander une **application**.

9. Saisissez le nom de l'instance et le motif de la demande, puis cliquez sur **Demander**.
   Vous recevez un e-mail contenant des instructions d'installation détaillées.
10. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous**.
    Une liste des applications disponibles pour l'installation s'affiche.
11. Localisez l'application, sélectionnez-la et cliquez sur **Installer**.
    Votre intégration est automatiquement installée sur votre instance.

Mettre à jour une application précédemment téléchargée à partir de ServiceNow Store

Si vous avez déjà téléchargé une application à partir de et ServiceNow Store qu'une nouvelle version est disponible, vous pouvez la mettre à jour dans votre instance.

Avant de commencer

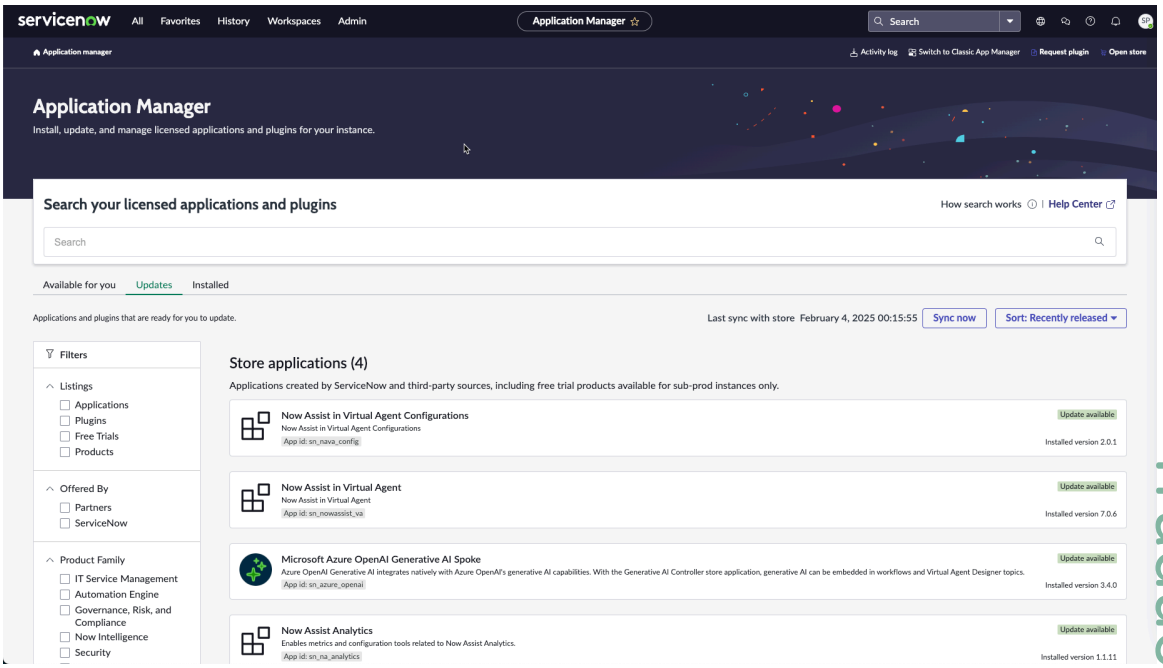
Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tous**.



2. Recherchez l'application que vous souhaitez mettre à jour.
3. Sélectionnez la version vers laquelle vous souhaitez effectuer la mise à niveau, puis cliquez sur **Mettre à jour**.
   Votre application est automatiquement installée sur votre instance.

Mettre à niveau votre instance vers la version de famille suivante

Si vous exécutez actuellement une version de famille et que vous souhaitez effectuer une mise à niveau vers la version suivante, il n'est pas nécessaire d'acquérir les applications à partir ServiceNow Store du . L'application est automatiquement mise à jour lorsque la plateforme est mise à jour vers la version minimale requise.

Rôle requis : admin

Pour plus d'informations, consultez la rubrique Utiliser les notes de version pour savoir comment naviguer dans les notes de version remaniées et trouver les informations que vous recherchez ainsi En savoir plus sur la version Zurich que les nouvelles fonctionnalités.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.